NEC

GVT-074167-001-00 1.10

QX-S5300G 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	2022/03	初版発行（英語版 1.9 版に相当）
1.1	2022/10	・「10-システム管理」の「12 章 NetMiester」に、netmeister management ip コマンドを追加しました。 ・誤記訂正
1.2	2023/01	・「01-はじめに」の「10 章 装置管理」から「10.1.23 display transceiver diagnosis」コマンドを削除しました(誤記修正)。 ・「08-セキュリティ」の「10 章 SSL」に「security-enhanced level」を追加しました。 ・「09-高可用性」の「8 章 Track」の「8.1.5 track nqa」から delay に関するパラメータを削除しました(誤記訂正)。
1.3	2023/05	・「03-アクセス」の「8 章 STP」の「display stp」の表示に説明を追記しました。 ・「04-IP サービス」の「2 章 Gratuitous ARP」に「gratuitous-arp mac-change retransmit」を追加しました。
1.4	2023/07	・「01-はじめに」の「3 章 ログイン」に以下のコマンドを追加しました。 「display ip http」 「display ip https」 「ip http acl」 「ip http enable」 「ip http port」 「ip https acl」 「ip https certificate access-control-policy」 「ip https enable」 「ip https port」 「ip https ssl-server-policy」 ・「01-はじめに」の「10 章 装置管理」の「10.1.50 temperature-limit」コマンドのデフォルト値を修正しました。 ・「03-アクセス」の「8 章 STP」の「bpdu-drop any」の説明に、ドロップするパケットを追記しました。
1.5	2023/09	・「10-システム管理」の「12 章 NetMiester」について、親機モードをサポートしました。また、その他誤記を修正しました。
1.6	2024/05	・「01-はじめに」に「12 章 Auto Config」を追加しました。
1.7	2024/11	・「01-はじめに」に「10.1.25 dying-gasp host」、「10.1.26 dying-gasp source」を追加しました。

版数	日付	改版内容
1.8	2025/07	・表紙ロゴ色、配置の変更 ・「01-はじめに」の「3.1.28 set authentication password」について、デフォルトを変更しました。 ・「06-マルチキャスト」 の「1.1.18 igmp-snooping」コマンドと「1.1.21 igmp-snooping enable」コマンドの説明を追記しました。
1.9	2026/1	・「03-アクセス」の「1.2.4 storm-constrain」について、pps 指定時の storm-constrain の設定例を追記しました。 ・「03-アクセス」の「1.2.4 storm-constrain」について、pps 指定時の storm-constrain の下限値を 0→1 に修正しました。 ・「08-セキュリティ」の「3.1.4 mac-authentication access-user log enable」について、インタフェースビューの設定について追記しました。 ・「08-セキュリティ」の「5.1.14 port-security timer autolearn aging」について、インタフェースビューの設定について追記しました。
1.10	2026/10	・「01-はじめに」の「1.1.12 repeat」コマンドの説明を追記しました。 ・「01-はじめに」の「10.1.18 display power」コマンドの誤記訂正をしました。 ・「02-IRF スタック」の「1.1.16 mad bfd enable」コマンドの誤記訂正をしました。 ・「03-アクセス」の「10.1.9 vlan」コマンドの誤記訂正をしました。 ・「03-アクセス」の「14.1.2 vlan mapping」コマンドの誤記訂正をしました。 ・「04-IP サービス」の「12.1.1 http-redirect https-port」コマンドの誤記訂正をしました。 ・「07-ACL and QoS」の「3.1.1 display qos map-table」コマンドの誤記訂正をしました。 ・「07-ACL and QoS」の「3.1.3 qos map-table」コマンドの誤記訂正をしました。 ・「08-セキュリティ」の「3.1.10 mac-authentication timer」コマンドの誤記訂正をしました。 ・「08-セキュリティ」の「10.1.6 ssl version disable」のデフォルトについて追記しました。 ・「09-高可用性」の「4.1.7 protected-vlan」コマンドの誤記訂正をしました。 ・「10-システム管理」の「12 章 NetMiester」について、下記のコマンドを追加しました。 「netmeister event log enable」 「netmeister event syslog enable」 「netmeister ngn enable」

Copyright © NEC Corporation 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-S5300G 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-S5300G シリーズ Ethernet スイッチ コマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

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

関連マニュアル

次のマニュアルには、QX-S5300G 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-S5300G 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-S5300G 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-S5300G 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-S5300G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

マニュアルの構成

このコマンドマニュアルは以下のセクションで構成されます。

- **はじめに**

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

- **IRF スタック**

  IRF スタックの設定について説明します。

- **アクセス**

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

- **IP サービス**

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

- **ルーティングプロトコル**

各種ルーティングプロトコル（IPv4＆IPv6）の設定について説明します。

- **マルチキャスト**

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

- **ACL and QoS**

  QoS、ACL の設定について説明します。

- **セキュリティ**

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

- **高可用性**

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

- **システム管理**

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

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

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

II. GUI 表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。例えば、<OK>ボタンをクリックします。

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

VI. ネットワークアイコン

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

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 10 個のセクションで構成されています。

01 - はじめに

02 - IRF スタック

03 - アクセス

04 - IP サービス

05 - ルーティングプロトコル

06 - マルチキャスト

07 - ACL and QoS

08 - セキュリティ

09 -高可用性

10 - システム管理

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

1. はじめに

本マニュアルは以下に示す章で構成されています。

01- CLI

02-RBAC

03-ログイン

04-FTP

05-TFTP

06-ファイルシステム管理

07-コンフィグレーションファイル管理

08-ソフトウェア管理

09-ISSU

10-装置管理

11-Python

目次

このセクションのページは **1-x-x** です。

1 章 CLI 1-1
1.1 CLI 設定コマンド 1-1
1.1.1 alias 1-1
1.1.2 display | { begin | exclude | include } 1-3
1.1.3 display | by-linenum 1-4
1.1.4 display > 1-5
1.1.5 display >> 1-6
1.1.6 display alias 1-7
1.1.7 display history-command 1-8
1.1.8 display history-command all 1-9
1.1.9 display hotkey 1-11
1.1.10 hotkey 1-12
1.1.11 quit 1-15
1.1.12 repeat 1-16
1.1.13 return 1-17
1.1.14 screen-length disable 1-18
1.1.15 system-view 1-19

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。コマンド文字列が Syntax の要件を満たしていることを確認します。

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。

システム定義のコマンドエイリアスは削除できません。

1 つのコマンドまたはコマンドの開始キーワードに対して、1 つまたは複数のエイリアスを設定できます。その後、エイリアスを使用してコマンドを実行できます。コマンドに **undo** 形式がある場合は、エイリアスを使用して **undo** コマンドを実行することもできます。

たとえば、エイリアス **shiprt** を **display ip routing-table** に設定する場合、**shiprt** と入力して **display ip routing-table** コマンドを実行できます。エイリアス **ship** を **display ip** に設定する場合、**ship** を使用して **display ip** で始まるすべてのコマンドを実行できます。

- **display ip routing-table** コマンドを実行するには、**ship routing-table** を入力します。
- **display ip interface** コマンドを実行するには、**ship interface** と入力します。

コマンド文字列には最大 9 つのパラメータを含めることができます。各パラメータは、ドル記号（$）と 1～9 の範囲のシーケンス番号で始まります。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 コマンドのエイリアスとして **shiprt** を設定し、設定を確認します。

<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を表示するには、エイリアス **shinc** を使用します。

[Switch] shinc routing-table Static

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

関連コマンド

display alias

1.1.2 display | { begin | exclude | include }

Syntax

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

View

すべての view

定義済みユーザロール

network-admi

network-operator

パラメータ

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

begin: 指定した正規表現の文字列を含む行を含む以降の行を表示します。

exclude: 指定した正規表現の文字列を含まない行を表示します。

include: 指定した正規表現の文字列を含む行を表示します。

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

説明

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

コマンド出力をフィルタリングするには、**display** コマンドで| { **begin** | **exclude** | **include** } *regular-expression* オプションを使用します。正規表現の詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*CLI*”を参照してください。

例

カレントコンフィグレーションで **vlan** を含む行を表示します。

<Switch> display current-configuration | include vlan

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

1.1.3 display | by-linenum

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

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

説明

display | **by-linenum** コマンドは **display** コマンドに行番号をつけて表示します。行番号を使用することで、わかりやすく表示することができます。

行番号は 5 桁で表示され、コロン（:）あるいはハイフン（-）が続きます。

display | **by-linenum** コマンドと **display** | **begin** *regular-expression* コマンドを同時に使用した場合、正規表現に一致しないすべての行はハイフン（-）で表示されます。

例

各出力行を番号で識別して、VLAN 999 設定を表示します。

<Switch> display vlan 999 | by-linenum

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

実行コンフィギュレーションの **user-group** で始まる最初の行と、それに続くすべての行を表示します。

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

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

1.1.4 display >

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

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

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

説明

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

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

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

例

VLAN 1 設定を **vlan.txt** という名前の別のファイルに保存します。

<Switch> display vlan 1 > vlan.txt

vlan.txt ファイルの内容を確認します。

<Switch> more vlan.txt

```
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:  None
 Untagged ports:
   GigabitEthernet1/0/2
```

1.1.5 display >>

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

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

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

説明

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

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

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

例

VLAN 999 設定を vlan.txt ファイルの末尾に追加します。

<Switch> display vlan 999 >> vlan.txt

<Switch>

vlan.txt ファイルの内容を確認します。

<Switch> more vlan.txt

```
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2

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

1.1.6 display alias

Syntax

display alias [*alias*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

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

説明

display alias コマンドはコマンドエイリアスを表示します。

例

すべてのコマンドのエイリアスを表示します。

<Switch> display alias

```
Index     Alias              Command key
1         access-list         acl
2         end                return
3         erase              delete
4         exit               quit
5         hostname           sysname
6         logging            info-center
7         no                 undo
8         shinc              display $1 | include $2
9         show               display
10        sirt               display ip routing-table
11        write              save
```

コマンドエイリアス **shinc** を表示します。

<Switch> display alias shinc

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

関連コマンド

alias

1.1.7 display history-command

Syntax

display history-command

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

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

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

履歴バッファに保存されているコマンドを表示し、再度実行することができます。

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

バッファがいっぱいになったときに新しいコマンドをバッファに入れるには、システムはバッファ内の最も古いコマンド項目を削除します。

現在の CLI セッションのコマンド履歴バッファ内のすべてのコマンドは、ログアウトすると削除されます。

コマンド履歴バッファにパスワード設定コマンドがある場合は、装置のセキュリティを確保するために、パスワードはアスタリスク (*) で表示されます。また、パスワード設定コマンドは、コマンド履歴バッファから再度実行することはできません。

例

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

<Switch> display history-command

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

関連コマンド

history-command max-size

1.1.8 display history-command all

Syntax

display history-command all

View

すべての view

定義済みユーザロール

network-admin

説明

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

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

履歴バッファに保存されているコマンドを表示し、再度実行することができます。

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

ユーザがログアウトしても、システムはすべての CLI セッションの履歴バッファからコマンドを削除しません。

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
03/16/2017 20:03:33 vty0      192.168.1.26    **
Cmd:dis his all

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

表 1-2 コマンド出力

フィールド	説明
Date	コマンドが実行された日付です。
Time	コマンドが実行された時刻です。
Terminal	ユーザが使用しているユーザ回線です。
Ip	ユーザが使用している端末のIPアドレスです。
User	ユーザログイン認証モードが**scheme**の場合にユーザが使用するユーザ名です。ログイン認証モードが**none**または**password**の場合、このフィールドには**が表示されます
Cmd	ユーザが入力したコマンド文字列です。

関連コマンド

display history-command

1.1.9 display hotkey

Syntax

display hotkey

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display hotkey コマンドはホットキー情報を表示します。

例

ホットキー情報を表示します。

<Switch> display hotkey

```
----------------- Hotkeys -----------------
         -Defined function hotkeys-
CTRL_A  Move the cursor to the beginning of the line.
CTRL_B  Move the cursor one character to the left.
CTRL_C  Stop the current command.
CTRL_D  Erase the character at the cursor.
CTRL_E  Move the cursor to the end of the line.
CTRL_F  Move the cursor one character to the right.
CTRL_H  Erase the character to the left of the cursor.
CTRL_K  Abort the connection request.
CTRL_N  Display the next command in the history buffer.
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Redisplay the current line.
CTRL_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

1.1.10 hotkey

Syntax

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

undo hotkey *hotkey*

デフォルト

表 1-3 にデフォルト定義のホットキーを示します。

表 1-3 デフォルト定義のホットキー

ホットキー	機能あるいはコマンド
Ctrl+A	**move_the_cursor_to_the_beginning_of_the_line** 行の先頭にカーソルを移動します。
Ctrl+B	**move_the_cursor_one_character_to_the_left** カーソルを1文字左に移動します。
Ctrl+C	**stop_the_current_command** 現在のコマンドを停止します。
Ctrl+D	**erase_the_character_at_the_cursor** カーソル上の文字を削除します。
Ctrl+E	**move_the_cursor_to_the_end_of_the_line** 行の行末にカーソルを移動します。
Ctrl+F	**move_the_cursor_one_character_to_the_right** カーソルを1文字、右に移動します。
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+H	**erase_the_character_to_the_left_of_the_cursor** カーソルの1つ左の文字を削除します。
Ctrl+K	**abort_the_connection_request** 現在の接続要求を中断します。
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。

ホットキー	機能あるいはコマンド
Ctrl+N	**display_the_next_command_in_the_history_buffer** 履歴バッファの次のコマンドを表示します。
Ctrl+O	**undo debugging all** すべてのデバッグ機能を表示します。
Ctrl+P	**display_the_previous_command_in_the_history_buffer** 履歴バッファの前のコマンドを表示します。
Ctrl+R	**redisplay_the_current_line** 現在の行を再表示します。
Ctrl+T	ー
Ctrl+U	ー
Ctrl+V	**paste_text_from_the_clipboard** クリップボードからテキストを貼り付けます。 このホットキーは、QX-S5300Gシリーズではサポートしていません。
Ctrl+W	**delete_the_word_to_the_left_of_the_cursor** カーソルの左の単語を削除します。
Ctrl+X	**delete_all_characters_from_the_beginning_of_the_line_to_the_cursor** カーソルの左にあるすべての文字を削除します。
Ctrl+Y	**delete_all_characters_from_the_cursor_to_the_end_of_the_line** カーソルから行末までのすべての文字を削除します。
Ctrl+Z	**return_to_the_User_View** user viewに戻ります。
Ctrl+]	**kill_incoming_connection_or_redirect_connection** 現在の接続を終了します。
Esc+B	**move_the_cursor_back_one_word** カーソルを1単語前に移動します。
Esc+D	**delete_all_characters_from_the_cursor_to_the_end_of_the_word** カーソルから単語の最後までのすべての文字列を削除します。
Esc+F	**move_the_cursor_forward_one_word** カーソルを1単語後に移動します。
Esc+N	**move_the_cursor_down_a_line** カーソルを1行下に移動します。**Enter**キーを押す前に、このホットキーを使用できます。 このホットキーは、QX-S5300Gシリーズではサポートしていません。

ホットキー	機能あるいはコマンド
Esc+P	**move_the_cursor_up_a_line** カーソルを1行上に移動します。**Enter**キーを押す前に、このホットキーを使用できます。 このホットキーは、QX-S5300Gシリーズではサポートしていません。
Esc+<	**move_the_cursor_to_the_beginning_of_the_clipboard** カーソルをクリップボードの先頭に移動します。 このホットキーは、QX-S5300Gシリーズではサポートしていません。
Esc+>	**move_the_cursor_to_the_end_of_the_clipboard** カーソルをクリップボードの最後に移動します。 このホットキーは、QX-S5300Gシリーズではサポートしていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

hotkey: ホットキーを指定します。サポートされるホットキーは表 1-3 を参照してください。あるいは **hotkey ?**コマンドを使用してください。

command: ホットキーに割り当てるコマンドを指定します。

function *function*: ホットキーに割り当てられる機能を指定します。サポートされる機能を表示する場合、表 1-3 を参照してください。あるいは **hotkey** *hotkey* **function ?**コマンドを使用してください。

none: ホットキーに割り当てられているコマンドあるいは機能を削除します。ホットキーの割り当てを削除したのち、ホットキーを押下しても、コマンドあるいは機能は実行しません。

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。

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。

ホットキーは 1 つのコマンドあるいは機能のみ対応します。同一のホットキーに複数のコマンドあるいは機能を割り当てた場合、最後に設定したコマンドあるいは機能が適用されます。

コマンドあるいは機能に複数のホットキーを割り当てることができます。コマンドあるいは機能を実行するため、割り当てられたホットキーを使用してください。

端末のソフトウェアから装置と相互に運用する場合、これらのキーは他の操作を実行するために定義されている可能性があります。その場合は、端末のソフトウェアの定義が優先されます。

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 statistics** コマンドを割り当てます。

<Switch> system-view

[Switch] hotkey ctrl_t display tcp statistics

ホットキー**Ctrl+U** に **move_the_cursor_to_the_beginning_of_the_line**（行の先頭にカーソルを移動します。）機能を割り当てます。

<Switch> system-view

[Switch] hotkey ctrl_u function move_the_cursor_to_the_beginning_of_the_line

ホットキー**Ctrl+A** に割り当てられたコマンドあるいは機能を削除します。

<Switch> system-view

[Switch] hotkey ctrl_a none

関連コマンド

display hotkey

1.1.11 quit

Syntax

quit

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

quit コマンドは上位の view に戻ります。

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

例

GigabitEtherne1/0/1 interface view から system view に戻り、次に user view に戻ります。

[Switch-GigabitEthernet1/0/1] quit

[Switch] quit

<Switch>

1.1.12 repeat

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

パラメータ

number: 現在の CLI セッションのコマンド履歴バッファで、繰り返し実行したい直近のコマンド数を指定します。値の範囲は 1～256 です。デフォルトは 1 です。

count *times*: コマンドを実行する回数を指定します。値の範囲は 0～4294967295 です。デフォルトは 0 です。このオプションを指定しない場合、エスケープキーを押して停止するまで実行は継続されます。

delay *seconds*: コマンドを再実行する前にシステムが待機する時間（秒）を指定します。値の範囲は 0～4294967295 です。デフォルトは 1 です。

説明

repeat コマンドを使用すると、現在の CLI セッションのコマンド履歴バッファ内のコマンドを繰り返し実行できます。

コマンドを繰り返す場合、まずそのコマンドのビューに入ります。複数のコマンドを繰り返す場合は、最初のコマンドのビューに入ります。

対話型コマンドを繰り返す際、システムはユーザの操作を待機します。

パスワード設定コマンドはすべてスキップされます。

コマンド履歴バッファで繰り返されるコマンド数は、以下の最小値によって決まります。

· repeat コマンドで指定した直近のコマンド数

· history-command max-size コマンドで指定したコマンド履歴バッファのサイズ

· コマンド履歴バッファ内のコマンド数

例

直近に実行した 2 つのコマンド（display cpu-usage と display clock）を 10 秒間隔で 2 回実行します。

<system> repeat 2 count 2 delay 10

```
<system> display cpu
Unit CPU usage:
     33% in last 5 seconds
     32% in last 1 minute
     33% in last 5 minutes

<system> display clock
07:02:18 UTC Thu 06/19/2017
<AP> display cpu-usage
Unit CPU usage:
     33% in last 5 seconds
     32% in last 1 minute
     33% in last 5 minutes

<system> display clock
07:02:28 UTC Thu 06/19/2017
```

1.1.13 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 interface view から user view に戻ります。

[Switch-GigabitEthernet1/0/1] return

<Switch>

1.1.14 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のとおりです。

- 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 CLI 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 CLI 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 CLI セッションに対してだけ有効です。ログアウトすると、デフォルトに戻ります。

例

現在の CLI セッションの出力画面間の一時停止を無効にします。

<Switch> screen-length disable

関連コマンド

screen-length

1.1.15 system-view

Syntax

system-view

View

User view

定義済みユーザロール

network-admin

network-operator

説明

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

例

user view から system view に移行します。

<Switch> system-view

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

[Switch]

目次

このセクションのページは **1-x-x** です。

2 章 RBAC 2-1
2.1 RBAC 設定コマンド 2-1
2.1.1 description 2-1
2.1.2 display role 2-2
2.1.3 display role feature 2-11
2.1.4 display role feature-group 2-13
2.1.5 feature 2-14
2.1.6 interface policy deny 2-15
2.1.7 permit interface 2-17
2.1.8 permit vlan 2-19
2.1.9 role 2-21
2.1.10 role default-role enable 2-22
2.1.11 role feature-group 2-23
2.1.12 rule 2-24
2.1.13 super 2-29
2.1.14 super authentication-mode 2-30
2.1.15 super default role 2-31
2.1.16 super password 2-32
2.1.17 vlan policy deny 2-34

2章 RBAC

2.1 RBAC設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

User role view

定義済みユーザロール

network-admin

パラメータ

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

説明

description コマンドはユーザロールの説明を設定します。

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

例

ユーザロール **role1** の説明を **labVIP** に設定します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] description labVIP

関連コマンド

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

2.1.2 display role

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

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

説明

display role コマンドはユーザロールの情報を表示します。

例

ユーザロール **123** の情報を表示します。

<Switch> display role name 123

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

すべてのユーザロールに関する情報を表示します。

<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     display security-logfile buffer
  sys-6   deny        command     system-view ; info-center securi
                                ty-logfile directory *
  sys-7   deny        command     security-logfile save
  sys-8   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-16  permit R--   web-menu     -
  sys-17  permit RW-   web-menu     m_device/m_maintenance/m_changep
```

```
                                assword
  sys-18  permit R--   xml-element   -
  sys-19  permit --X   xml-element   useraccounts/changemypassword
  sys-20  permit --X   xml-element   rpc
  sys-21  deny        command      display security-logfile summary
  sys-22  deny        command      display security-logfile buffer
  sys-23  deny        command      system-view ; info-center securi
                                ty-logfile directory *
  sys-24  deny        command      security-logfile save
  sys-25  deny        command      system-view ; local-user-import
                                *
  sys-26  deny        command      system-view ; local-user-export
                                *
  sys-27  permit R--   oid          1
  R:Read W:Write X:Execute

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

Role: level-1
  Description: Predefined level-1 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ----------------------------------------------------------------------
  sys-1   permit      command      tracert *
  sys-2   permit      command      telnet *
  sys-3   permit      command      ping *
```

```
  sys-4   permit      command      ssh2 *
  sys-5   permit      command      display *
  sys-6   permit      command      super *
  sys-7   deny        command      display history-command all
  sys-8   permit      command      mtrace *
  R:Read W:Write X:Execute

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

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

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

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

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

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

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

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

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

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

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

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

```
  VPN instance policy: permit (default)

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

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit      command     *
  sys-2   permit RWX   web-menu     -
  sys-3   permit RWX   xml-element   -
  sys-4   deny        command     display security-logfile summary
  sys-5   deny        command     display security-logfile buffer
  sys-6   deny        command     system-view ; info-center securi
                                 ty-logfile directory *
  sys-7   deny        command     security-logfile save
  sys-8   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      display security-logfile buffer
  sys-4   permit      command      system-view ; info-center securi
                                 ty-logfile directory *
  sys-5   permit      command      security-logfile save
  sys-6   permit      command      cd *
```

```
  sys-7   permit      command      copy *
  sys-8   permit      command      delete *
  sys-9   permit      command      dir *
  sys-10  permit      command      mkdir *
  sys-11  permit      command      more *
  sys-12  permit      command      move *
  sys-13  permit      command      rmdir *
  sys-14  permit      command      pwd
  sys-15  permit      command      rename *
  sys-16  permit      command      undelete *
  sys-17  permit      command      ftp *
  sys-18  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/generateguestaccoun
                                t/
  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 --X   xml-element   useraccounts/changemypassword
  sys-9   permit RWX   xml-element   rpc/
  sys-10  deny        command      *
  R:Read W:Write X:Execute
```

表 2-1 コマンド出力

フィールド	説明
Role	ユーザロール名です。 定義済みのユーザロール名は以下です。 ● network-admin ● network-operator ● level-*n*（*n*は0～15の整数です。） ● security-audit. ● guest-manager. このユーザロールはQX-S5300Gシリーズ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。
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VPNインスタンスポリシーです。 ● **deny**–許可されたVPNインスタンスを除くVPNインスタンス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。 このフィールドは、QX-S5300Gシリーズではサポートしていません。
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、QX-S5300Gシリーズではサポートしていません。

フィールド	説明
Rule	ユーザロール番号です。 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、エンティティフィールドの項目にアクセスできます。 • **deny**–ユーザロールは、エンティティフィールドの項目にアクセスできません。
Type	制御タイプです。 • **R**–Read-onlyです。 • **W**–Writeです。 • **X**–Executeです。
Scope	ルール制御範囲です。 • **command**–コマンドへのアクセスを制御する、あるいはエンティティフィールドで指定されるコマンドです。 • **feature**–エンティティフィールドに指定され、機能のコマンドへのアクセスを制御します。 • **feature-group**–エンティティフィールドに指定され、機能グループの機能の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。このルール制御範囲は、QX-S5300Gシリーズではサポートしていません。 • **xml-element**— XML要素へのアクセスを制御します。 • **oid**— MIBノードへのアクセスを制御します。
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、機能グループです。 • エンダッシュ（–）はすべての機能を示します。 • アスタリスク（*）は0以上の文字を示します。

関連コマンド

role

2.1.3 display role feature

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

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

verbose: 各機能のコマンドを表示します。

説明

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

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

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

フィールド	説明
Feature	機能の名前、概要の説明を表示します。
system-view ; domain *	system viewでの**domain**キーワード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**キーワード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**キーワードで始まるすべてのコマンドです。
system-view ; user-group *	system viewでの**user-group**キーワード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**キーワードで始まるすべてのコマンドとlocal user viewのすべてのコマンドです。
display local-user *	user viewでの**display local-user**キーワードで始まるすべてのコマンドです。

フィールド	説明
display user-group *	user viewでの**display user-group**キーワード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**キーワードで始まるすべてのコマンドです。
debugging local-server *	user viewでの**debugging local-server**キーワードで始まるすべてのコマンドです。
super *	user viewでの**super**キーワードで始まるすべてのコマンドです。
display password-control *	user viewでの**display password-control**キーワードで始まるすべてのコマンドです。
reset password-control *	user viewでの**reset password-control**キーワードで始まるすべてのコマンドです。
system-view ; password-control *	system viewでの**password-control**キーワード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。
(X)	コマンドタイプがexecuteです。execute コマンドは指定した機能を実行します。

関連コマンド

feature

2.1.4 display role feature-group

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

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

verbose: 指定された機能グループの各機能のコマンドを表示します。機能グループを指定しない場合、各機能グループの各機能のコマンドを表示します。**verbose** キーワードを指定しない場合、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

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

<Switch> display role feature-group verbose

```
Feature group: L2
Feature: igmp-snooping  (IGMP-Snooping related commands)
  system-view ; igmp-snooping *    (W)
  system-view ; multicast-vlan *    (W)
  system-view ; vlan * ; igmp-snooping *    (W)
  system-view ; vlan * ; pim-snooping *    (W)
  system-view ; vsi * ; igmp-snooping *    (W)
  system-view ; vsi * ; pim-snooping *    (W)
  system-view ; interface * ; igmp-snooping *    (W)
  system-view ; interface * ; port multicast-vlan *    (W)
  display igmp-snooping *    (R)

...
```

関連コマンド

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

2.1.5 feature

Syntax

feature *feature-name*

undo feature *feature-name*

デフォルト

設定なし

View

Feature group view

定義済みユーザロール

network-admin

パラメータ

feature-name: 機能名を指定します。機能名は小文字で入力する必要があります。

説明

feature コマンドは機能グループに機能を追加します。

undo feature コマンドは機能グループから機能を削除します。

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

例

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

<Switch> system-view

[Switch] role feature-group name security-features

[Switch-featuregrp-security-features] feature aaa

[Switch-featuregrp-security-features] feature acl

関連コマンド

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

2.1.6 interface policy deny

Syntax

interface policy deny

undo interface policy deny

デフォルト

User role はすべてのインタフェースにアクセスできます。

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** コマンドでユーザロールインタフェースポリシーview に移行します。
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**：

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、すべてのインタフェースへのユーザロール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** で 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許可します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] interface policy deny

[Switch-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4

関連コマンド

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

2.1.7 permit interface

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

デフォルト

ユーザロールの interface policy view で許可されているインタフェースはありません。

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: 最大 10 個のインタフェース項目をスペースで区切り、リスト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 **role1** 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)　ユーザロール **role1** で GigabitEthernet 1/0/1、GigabitEthernet 1/0/3～GigabitEthernet 1/0/5 を除いたすべてのインタフェースで動作するユーザロールが使用できないことを確認します。

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

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] quit

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

[Switch] vlan 10

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

[Switch-vlan10] quit

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

[Switch] interface gigabitethernet 1/0/2

```
Permission denied.
```

関連コマンド

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

2.1.8 permit vlan

Syntax

permit vlan *vlan-id-list*

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

デフォルト

ユーザロールの VLAN policy view で許可されている VLAN の設定はありません。

View

User role VLAN policy view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切ることで 10 の VLAN を指定することができます。

各 VLAN は VLAN ID で VLAN を指定あるいは *vlan-id1* **to** *vlan-id2* の形式で指定します。VLAN ID の設定範囲は 1～4094 です。VLAN の範囲を指定する場合、*vlan-id2* は *vlan-id1* よりも大きい値にしてください。

説明

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

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

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

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

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

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

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

例

1) ユーザロール **role1** を設定します。

interface view、VLAN view で有効なすべてのコマンドを実行するため、ユーザロール **role1** を許可します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] rule 1 permit command system-view ; interface *

[Switch-role-role1] rule 2 permit command system-view ; vlan *

VLAN 2、VLAN 4、VLAN 50～VLAN 100 にアクセスするユーザロール **role1** を許可します。

[Switch-role-role1] vlan policy deny

[Switch-role-role1-vlanpolicy] permit vlan 2 4 50 to 100

[Switch-role-role1-vlanpolicy] quit

[Switch-role-role1] quit

2) VLAN 2、VLAN 4、VLAN 50～VLAN 100 を除いたすべての VLAN で動作するユーザロール **role1** が使用できないことを確認します。

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

[Switch] vlan 100

[Switch-vlan100] quit

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

[Switch] interface gigabitethernet 1/0/1

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

[Switch-GigabitEthernet1/0/1] quit

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

[Switch] vlan 101

```
Permission denied.
```

関連コマンド

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

2.1.9 role

Syntax

role name *role-name*

undo role name *role-name*

デフォルト

以下の定義済みユーザロールがあります。

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

View

System view

定義済みユーザロール

network-admin

パラメータ

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

説明

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

undo role コマンドはユーザロールを削除します。

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

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

非 AAA 認証ユーザにセキュリティ検査のロールを割り当てることはできません。

Level-0～level-14 のユーザロールのアクセス許可は、ユーザロールのルールとリソースのアクセスポリシーを使用して変更できます。

ただし、これらのユーザロールの定義済みアクセス権を変更することはできません。

これらのユーザロールのアクセス権を **display history-command all** コマンドに変更することはできません。

例

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

<Switch> system-view

[Switch] role name role1

[Switch-role-role1]

関連コマンド

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

2.1.10 role default-role enable

Syntax

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

undo role default-role enable

デフォルト

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

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザロールはシステムになければなりません。ユーザロールの指定がない場合、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。

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。

AAA 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。

ローカル認証では、**authorization-attribute user role** コマンドを使用してユーザロールをローカルユーザに割り当てない場合、このコマンドが必要です。

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。

例

デフォルトユーザロール機能を有効にします。

<Switch> system-view

[Switch] role default-role enable

関連コマンド

role

2.1.11 role feature-group

Syntax

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

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

デフォルト

ユーザロールグループ **L2**、**L3** が作成されています。

View

System view

定義済みユーザロール

network-admin

パラメータ

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

説明

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

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

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

定義済みの機能グループ **L2**、**L3** に加えて、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、その view に移行します。

<Switch> system-view

[Switch] role feature-group name security-features

[Switch-featuregrp-security-features]

関連コマンド

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

2.1.12 rule

Syntax

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

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。機能を指定するとき、機能名は **display role feature** コマンドで表示される名前と同一にしてください。

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。

oid *oid-string*: MIB ノードの OID を指定します。*oid-string* は OID を表します。OID の設定範囲は 1~255 です。大文字と小文字を区別しない文字列です。OID は、ルートノードからこのノードまでのパスを一意に識別するドット付きの数値文字列です。たとえば、1.3.6.1.4.1.25506.8.35.14.19.1.1 のようになります。

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。

- **Command rule**－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。

- **Feature rule**－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。
- **Feature group rule**－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。
- **OID rule**－ノードタイプによって、指定された MIB ノードとその子ノードへのアクセスを制御します。

ユーザロールは、ユーザロールルールで指定されている許可されたリソースのセットにアクセスできます。

ユーザロールルールには、定義済み（sys-n で識別）およびユーザ定義のユーザロールルールが含まれます。

ユーザロールには最大 256 のユーザ定義ルールを設定できます。

ユーザ定義ユーザロールルールの総数は 1024 以下です。

ユーザロールに対するルールの変更、追加、または削除は、変更後にそのユーザロールでログインしたユーザにのみ有効になります。

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ルールとファイルシステム機能ルールの両方によって制御されます。

ファイルシステムへの出力リダイレクトを伴うコマンドは、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ている場合にのみ許可されます。

以下のガイドラインは、OID 以外のルールに適用されます。

- 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。

以下のガイドラインは、OID ルールに適用されます。

- システムは OID をルールで指定された OID と比較し、最長一致原則を使用して OID のルールを選択します。たとえば、ユーザロールに次のコマンドを使用して設定されたルールが含まれている場合、ユーザロールは OID が 1.3.6.1.4.1.25506.141.3.0.1 の MIB ノードにアクセスできません。
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
  - **rule** *3* **permit read write oid** *1.3.6.1.4*
- 複数のルールに同じ OID が指定されている場合は、ID が大きい方のルールが有効になります。たとえば、ユーザロールに次のコマンドを使用して設定されたルールが含まれている場合、ユーザロールは OID が 1.3.6.1.4.1.25506.141.3.0.1 の MIB ノードにアクセスできます。
  - **rule** *1* **permit read write oid** *1.3.6*

- **rule** *2* **deny read write oid** *1.3.6.1.4.1*
- **rule** *3* **permit read write oid** *1.3.6.1.4.1*

コマンド文字列を指定するとき、表 2-3 のガイドラインに従ってください。

表 2-3 コマンド文字列設定ルール

ルール	ガイドライン
区切り機能はセミコロン（;）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**キーワード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**キーワード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**キーワード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
キーワードの省略ができます。	キーワードの最初の数文字を入力することでキーワード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 キーワード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

OID が 1.1.2 のノードから始まるすべての読み取りおよび書き込み MIB ノードへのアクセスを **role 1** に許可します。

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

関連コマンド

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

2.1.13 super

Syntax

super [*role-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があります。ユーザロールを指定しない場合、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:
User privilege role is network-operator, and only those commands that authorized
to the role can be used.
```

関連コマンド

- **authentication super**(コマンドマニュアルのセクション 8 *セキュリティ*)
- **super authentication-mode**
- **super password**

2.1.14 super authentication-mode

Syntax

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

undo super authentication-mode

デフォルト

local

View

System view

定義済みユーザロール

network-admin

パラメータ

local: ローカルパスワード認証を有効にします。

scheme: リモート AAA 認証を有効にします。

説明

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

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

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

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

local と **scheme** キーワードの両方を指定した場合、最初に指定されたキーワードが適用されます。

- **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、装置はリモート認証を実行します。VTY ユーザ、AUX ユーザは、文字列を入力するか、何も入力しないで別のユーザロールを取得できます。

AAA の詳細は、オペレーションマニュアルのセクション 8 *セキュリティ* “*AAA*”を参照してください。

例

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

<Switch> system-view

[Switch] super authentication-mode local

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

<Switch> system-view

[Switch] super authentication-mode scheme local

関連コマンド

- **authentication super**(コマンドマニュアルのセクション 8 *セキュリティ*)
- **super password**

2.1.15 super default role

Syntax

super default role *role-name*

undo super default role

デフォルト

network-admin

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name: デフォルトターゲットユーザロールの名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があり、セキュリティ監査になることはできません。

説明

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

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

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

例

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

<Switch> system-view

[Switch] super default role network-operator

関連コマンド

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

2.1.16 super password

Syntax

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

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

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

role *role-name*: ユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があり、セキュリティ監査にはなれません。ユーザロールを指定しない場合、**super default role** コマンドを使用して設定される、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。大文字、小文字を区別します。

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

説明

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

undo super password コマンドはデフォルトに戻します。

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

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

異なるユーザロールに異なるパスワードを指定することを推奨します。

例

ユーザロール network-operator のプレーンテキストのパスワード **123456TESTplat&!** を設定します。

<Switch> system-view

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

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

<Switch> system-view

[Switch] super password role network-operator

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

関連コマンド

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

2.1.17 vlan policy deny

Syntax

vlan policy deny

undo vlan policy deny

デフォルト

VLAN へのユーザロールのアクセス可能にします。

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 コマンドはユーザロールの VLAN policy view へのアクセスを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** コマンドでユーザロールの VLAN policy へ移行します。
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

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

VLAN50～VLAN100 を除く VLAN へのユーザロール **role1** のアクセスを拒否します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] vlan policy deny

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

関連コマンド

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

目次

このセクションのページは **1-x-x** です。

3 章 ログイン 3-1
3.1 ログイン設定コマンド 3-1
3.1.1 authentication-mode 3-1
3.1.2 auto-execute command 3-3
3.1.3 databits 3-4
3.1.4 display ip http 3-5
3.1.5 display ip https 3-6
3.1.6 display line 3-7
3.1.7 display telnet client 3-9
3.1.8 display users 3-10
3.1.9 escape-key 3-11
3.1.10 free line 3-13
3.1.11 history-command max-size 3-14
3.1.12 idle-timeout 3-15
3.1.13 ip http acl 3-16
3.1.14 ip http enable 3-17
3.1.15 ip http port 3-18
3.1.16 ip https acl 3-18
3.1.17 ip https certificate access-control-policy 3-19
3.1.18 ip https enable 3-20
3.1.19 ip https port 3-21
3.1.20 ip https ssl-server-policy 3-22
3.1.21 line 3-23
3.1.22 line class 3-24
3.1.23 lock 3-25
3.1.24 parity 3-26
3.1.25 protocol inbound 3-27
3.1.26 screen-length 3-29
3.1.27 send 3-30
3.1.28 set authentication password 3-31
3.1.29 shell 3-32
3.1.30 speed 3-33
3.1.31 stopbits 3-34
3.1.32 telnet 3-35
3.1.33 telnet client source 3-36
3.1.34 telnet ipv6 3-37

3.1.35 telnet server acl 3-38
3.1.36 telnet server dscp 3-39
3.1.37 telnet server enable 3-40
3.1.38 telnet server ipv6 acl 3-41
3.1.39 telnet server ipv6 dscp 3-42
3.1.40 terminal type 3-43
3.1.41 user-role 3-44

3章 ログイン

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。
- 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 の設定はオンラインユーザに影響しません。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。

3.1 ログイン設定コマンド

3.1.1 authentication-mode

Syntax

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

undo authentication-mode

デフォルト

none

View

user line view, user line class view

定義済みユーザロール

network-admin

パラメータ

none: 認証を無効にします。

password: ローカルパスワード認証を行います。

scheme: AAA 認証を行います。AAA の詳細は、オペレーションマニュアルのセクション 8 *セキュリティ "AAA"*を参照してください。

説明

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

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

network-admin、またはレベル 15 のユーザロールを割り当てられたユーザだけがこのコマンドを実行できます。他のユーザは、このコマンドを実行する権限が付与されていても、この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 では、このコマンドは **protocol inbound** コマンドに関連付けられています。

- VTY line view の 2 つのコマンドの設定が両方ともデフォルトの設定である場合、VTY line class view のコマンドの設定が有効になります。
- VTY line view の 2 つのコマンドの設定が両方ともデフォルト以外の設定の場合、VTY line class view のデフォルト以外の設定が有効になります。
- VTY line view にデフォルト以外の設定があるコマンドが 1 つだけの場合、もう一方のコマンドは、VTY line class view の設定に関係なく、デフォルトの設定を使用します。

認証モードの変更は、現在のセッションでは有効になりません。以降のログインセッションで有効になります。

例

user line VTY 0 で認証モードを **none** にします。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] authentication-mode none

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

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] authentication-mode password

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

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

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] authentication-mode scheme

[Switch-line-vty0] quit

[Switch] local-user 123

[Switch-luser-manage-123] password simple 321

[Switch-luser-manage-123] service-type telnet

[Switch-luser-manage-123] authorization-attribute user-role network-admin

関連コマンド

set authentication password

3.1.2 auto-execute command

Syntax

auto-execute command *command*

undo auto-execute command

デフォルト

ログインユーザに対して自動的に実行されるコマンドが指定されていません。

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 コマンドはデフォルトに戻します。

⚠ **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。

ユーザが user line を通じてログインすると、装置は自動的に指定されたコマンドを実行し、コマンド実行後にユーザ接続を閉じます。

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。このコマンドは、user line view と user line class view の両方で使用できます。どちらかの view のデフォルト以外の設定は、他方の view のデフォルトの設定よりも優先されます。user line view のデフォルト以外の設定は、user line class view のデフォルト以外の設定よりも優先されます。

このコマンドで行った設定の変更は、現在のセッションでは有効になりません。以降のログインセッションで有効になります。

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]

設定を確認するには、装置（192.168.1.40）に Telnet 接続します。

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

C:¥> telnet 192.168.1.40

<Switch>

```
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
```

<Switch.41>

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

3.1.3 databits

Syntax

databits { **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

7: データビット数 7

8: データビット数 8

説明

databits コマンドは各文字のデータビット数を指定します。

undo databits コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

この設定は端末のデータビットと同一にしてください。

例

AUX 0 のデータビットを 7 に設定します。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] databits 7

3.1.4 display ip http

Syntax

display ip http

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

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

例

HTTP サービスの設定とステータス情報を表示します。

<Switch> display ip http

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

表 3-1 コマンド出力

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

関連コマンド

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

3.1.5 display ip https

Syntax

display ip https

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

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

例

HTTPS サービスの設定とステータス情報を表示します。

<Switch> display ip https

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

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

表 3-2 コマンド出力

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

関連コマンド

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

3.1.6 display line

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

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

aux: AUX line を指定します。

vty: VTY line を指定します。

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

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

説明

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

例

line 0 の情報を表示します。

<Switch> display line 0

```
  Idx  Type     Tx/Rx      Modem Auth  Int       Location
F 0    AUX 0    9600       -     N     -         1/0

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

表 3-3 コマンド出力

フィールド	説明
Modem	モデムのモードがin/outを示します。デフォルトでは設定されていません。このフィールドには、ハイフン(-)が表示されます。QX-S5300Gシリーズではサポートしていません。
Int	lineの物理ポート。lineに物理ポートがない場合、またはポートがコンソールポートの場合、このフィールドにはハイフン(-)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)。

すべての user line の概要情報を表示します。

<Switch> display line summary

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

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

表 3-4 コマンド出力

フィールド	説明
Line type	user lineのタイプ • **AUX**—AUX line. • **VTY**—VTY line.
number:status	*number*：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*：user line classのuser lineが使用されているかどうかを示します。(**X**は未使用で**U**は使用されています)

3.1.7 display telnet client

Syntax

display telnet client

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display telnet client コマンドはTelnetクライアントのパケットソース設定を表示します。

このコマンドは、装置が **telnet client source** コマンドに応じて、Telnet クライアントが送信 Telnet パケットで使用するように指定された送信元 IPv4 アドレスまたは送信元インタフェースを表示します。

例

Telnet クライアントのパケットソース設定を表示します。

<Switch> display telnet client

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

関連コマンド

telnet client source

3.1.8 display users

Syntax

display users [**all**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: 装置でサポートされるすべての user line を表示します。

説明

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

例

オンライン CLI ユーザの情報を表示します。

<Switch> display users

```
  Idx  Line     Idle      Time            Pid     Type
+ 10   VTY 0    00:00:00   Jan 01 00:33:10   484     TEL
  12   VTY 2    00:06:22   Jan 01 00:33:22   495     TEL

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

表 3-5 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	User type: • **TEL**—Telnet user • **SSH**—SSH user • コンソールポートまたはUSBコンソールポート経由でログインしたユーザの場合、このフィールドには何も表示されません。
+	カレントユーザが使用しているuser lineを示します。
Location	カレントユーザのIPアドレスです。

3.1.9 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。文字(大文字、小文字を区別する(**d** と **D** を除く))、あるいは ASCII コード値を指定できます。設定範囲は 0～127 です。たとえば、**escape-key 1** を設定した場合、キーショートカットは **Ctrl+A** になります。**escape-key a** を設定すると、キーのショートカットは a になります。d または D を指定した場合、実際のショートカットキーは **Ctrl+C** です。**d** または **D** をショートカットキーとして使用するには、文字の ASCII コード値を指定する必要があります。個々の文字の ASCII コード値については、標準 ASCII コード表を参照してください。

default: デフォルトのエスケープキー**Ctrl+C** を復元します。

説明

escape-key コマンドはエスケープキーを指定します。

undo escape-key コマンドはエスケープキーを無効にします。

Esc キーを押すと、実行中のコマンド(**ping** や **tracert** など)を中止できます。デフォルトで **Ctrl+C** でコマンドを中止できるかどうかは、コマンドのソフトウェア実装によって異なります。詳細はコマンドマニュアルのセクション 1 *はじめに* を参照してください。

キーシーケンスを Esc キーとして使用することを推奨します。Esc キーとして単一の文字を定義した場合、コマンドの実行中にキーを押すと、コマンドが停止します。実行中のコマンドがない場合は、キーを押すと共通文字として入力されます。装置からリモート装置に Telnet 接続する場合、キーを押すと、リモート装置の共通文字として文字が入力されます。キーは、次の条件が満たされる場合にのみ、リモート装置で Esc キーとして動作します。

- リモート装置で Esc キーと同じ文字を定義します。
- リモート装置でコマンドを実行しているときにキーを押す。

undo escape-key コマンドは、現在の Esc キーを無効にします。この **undo** コマンドを実行すると、Esc キーは使用できなくなります。

このコマンドは、user line view と user line class view の両方で使用できます。どちらかの view のデフォルト以外の設定は、他方の view のデフォルトの設定よりも優先されます。user line view のデフォルト以外の設定は、user line class view のデフォルト以外の設定よりも優先されます。

user line view の設定は、現在のセッションに対してすぐに有効になります。user line class view の設定は、設定の構成後に確立されるログインセッションに対して有効になります。

現在の Esc キーを表示するには、**display current-configuration** | **include escape-key** コマンドを使用します。

例

VTY line 0 の Esc キーとして設定文字 **a** を使用します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] escape-key a

設定を確認するには、次の手順に従います。

1. IP アドレス 192.168.1.49 に ping を実行し、**-c** キーワードを指定して ICMP エコー要求パケットの数を 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** キーを押します。

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

<Switch>

3.1.10 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 line 1 を解放します。

<Switch> free line vty 1

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

3.1.11 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。コマンド履歴バッファの詳細は、オペレーションマニュアルのセクション 1 *はじめに* 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削除されます。

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 の設定は、現在のセッションに対してすぐに有効になります。user line class view の設定は、設定の構成後に確立されるログインセッションに対して有効になります。

例

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

<Switch> system-view

[Switch] line vty 0

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

3.1.12 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。

アイドルタイムアウト機能を無効にするには、**idle-timeout 0** コマンドを実行します。

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。

どちらかの view のデフォルト以外の設定は、他方の view のデフォルトの設定よりも優先されます。user line view のデフォルト以外の設定は、user line class view のデフォルト以外の設定よりも優先されます。

user line view の設定は、現在のセッションに対してすぐに有効になります。user line class view の設定は、設定の構成後に確立されるログインセッションに対して有効になります。

例

user line VTY 0 のタイムアウト時間を 1 分 30 秒に設定します。

<Switch> system-view

[Switch] line vty 0

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

3.1.13 ip http acl

Syntax

ip http acl *acl-number*

undo ip http acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

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

説明

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

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

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

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

例

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

<Switch> system-view

[Switch] acl basic 2001

[Switch-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[Switch-acl-ipv4-basic-2001] quit

[Switch] ip http acl 2001

関連コマンド

acl（コマンドマニュアルのセクション 7 ***ACL and QoS***）

3.1.14 ip http enable

Syntax

ip http enable

undo ip http enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

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

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

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

例

HTTP サービスを有効にします。

<Switch> system-view

[Switch] ip http enable

関連コマンド

ip https enable

3.1.15 ip http port

Syntax

ip http port *port-number*

undo ip http port

デフォルト

80

View

System view

定義済みユーザロール

network-admin

パラメータ

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

説明

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

undo ip http port コマンドはデフォルトに戻します。

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

例

HTTP サービスのポート番号を 80 に指定します。

<Switch> system-view

[Switch] ip http port 80

3.1.16 ip https acl

Syntax

ip https acl *acl-number*

undo ip https acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

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

説明

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

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

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

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

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

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

例

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

<Switch> system-view

[Switch] acl basic 2001

[Switch-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[Switch-acl-ipv4-basic-2001] quit

[Switch] ip https acl 2001

関連コマンド

acl（コマンドマニュアルのセクション 7 ***ACL and QoS***）

3.1.17 ip https certificate access-control-policy

Syntax

ip https certificate access-control-policy *policy-name*

undo ip https certificate access-control-policy

デフォルト

設定なし

Views

System view

定義済みユーザロール

network-admin

パラメータ

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

説明

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

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

デフォルト：無効

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

例

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

<QX> system-view

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

3.1.18 ip https enable

Syntax

ip https enable

undo ip https enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

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

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

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

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

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

例

HTTPS サービスを有効にします。

<Switch> system-view

[Switch] ip https enable

3.1.19 ip https port

Syntax

ip https port *port-number*

undo ip https port

デフォルト

443

View

System view

定義済みユーザロール

network-admin

パラメータ

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

説明

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

undo ip https port コマンドはデフォルトに戻します。

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

例

HTTPS サービスのポート番号を 8080 に指定します。

<Switch> system-view

[Switch] ip https port 8080

3.1.20 ip https ssl-server-policy

Syntax

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

undo ip https ssl-server-policy

デフォルト

無効

Views

System view

定義済みユーザロール

network-admin

パラメータ

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

説明

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

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

HTTPS サービスは、このコマンドが正常に設定された後、有効になります。

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

例

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

<QX> system-view

[QX] ip https ssl-server-policy myssl

3.1.21 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。値の範囲は 1～73 です。*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。AUX line の設定範囲は 1～9 で、VTY line の設定範囲は 1～63 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

user line VTY 0 の view に移行します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0]

VTY 0～VTY 63 の view に移行します。

<Switch> system-view

[Switch] line vty 0 63

[Switch-line-vty0-63]

関連コマンド

line class

3.1.22 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、次のコマンドを実行できます。

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

user line view と user line class view の両方で使用できるコマンドでは、装置は次のルールに従って使用する設定を決定します。

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

例

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

<Switch> system-view

[Switch] line class vty

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

関連コマンド

line

3.1.23 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 !
```

// ユーザラインはロックされています。ロックを解除するには、**Enter** キーを押してパスワードを入力します。

```
Password:
```

<Switch>

3.1.24 parity

Syntax

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

undo parity

デフォルト

設定されていません。

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

user line AUX 0 で奇数パリティチェックを実行するように設定します。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] parity odd

3.1.25 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 user line で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、つまりレベル 15 ユーザロールが割り当てられたユーザだけが、このコマンドを実行できます。他のユーザは、このコマンドを実行する権限が付与されていても、このコマンドを実行できません。

user line view での設定の変更は、現在のセッションには反映されません。以降のログインセッションで有効になります。

SSH をサポートするように user line を設定する前に、user line の認証モードを **scheme** に設定します。

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両方ともデフォルトの設定である場合、VTY line view のコマンドの設定が有効になります。
- VTY line view の 2 つのコマンドの設定が両方ともデフォルト以外の設定の場合、VTY line view のデフォルト以外の設定が有効になります。
- VTY line view にデフォルト以外の設定があるコマンドが 1 つだけの場合、もう一方のコマンドは、VTY line class view の設定に関係なく、デフォルトの設定を使用します。

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 0～4 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ています。

2) オンライン CLI ユーザの情報を表示します。

<Server> display users

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

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

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

関連コマンド

authentication-mode

3.1.26 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 に設定するか **screen-length disable** コマンドを実行した場合、出力画面のスクロールは停止しません。

説明

screen-length コマンドは出力画面のスクロールの停止を有効にしたとき、画面上に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。

一時停止後にコマンド出力の表示を続けるには、スペースバーを押します。

デフォルトでは、出力画面間の一時停止は有効になっています。

このコマンドは、user line view と user line class view の両方で使用できます。どちらかの view のデフォルト以外の設定は、他方の view のデフォルトの設定よりも優先されます。user line view のデフォルト以外の設定は、user line class view のデフォルト以外の設定よりも優先されます。

user line view の設定は、現在のセッションに対してすぐに有効になります。user line class view の設定は、設定の構成後に確立されるログインセッションに対して有効になります。

例

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

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] screen-length 30

関連コマンド

screen-length disable

3.1.27 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。

このコマンドを使用すると、装置を再起動する前など、ほかのオンラインユーザに影響を与える可能性のある操作を実行する前に、オンラインユーザにメッセージを送信します。

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

装置を再起動する前に、VTY 1 の user に通知するため、メッセージを送信します。

<Switch> send vty 1

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

メッセージは以下の例のようにユーザの設定端末の画面に表示されます。

[Switch]

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

3.1.28 set authentication password

Syntax

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

undo set authentication password

デフォルト

Ver7.4.40 以降では 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: パスワードをハッシュ形式で指定します。

simple: パスワードをプレーンテキスト形式で設定します。セキュリティのため、プレーンテキスト形式で指定されたパスワードは、ハッシュ形式で格納されます。

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

説明

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

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

network-admin、つまりレベル 15 ユーザロールが割り当てられたユーザだけが、このコマンドを実行できます。他のユーザは、このコマンドを実行する権限が付与されていても、この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。

どちらかの view のデフォルト以外の設定は、他方の view のデフォルトの設定よりも優先されます。user line view のデフォルト以外の設定は、user line class view のデフォルト以外の設定よりも優先されます。

パスワードの変更は、現在のセッションでは有効になりません。それ以降のログインセッションで有効になります。

例

user line VTY 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

3.1.29 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。

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、user line VTY 0～VTY 4 の端末サービスを無効にします。

<Switch> system-view

[Switch] line vty 0 4

[Switch-line-vty0-4] undo shell

```
Disable ui-vty0-4 , are you sure? [Y/N]:y
```

[Switch-line-vty0-4]

3.1.30 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

user line AUX 0 で通信速度を 19200 bps に設定します。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] speed 19200

3.1.31 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

user line AUX 0 のストップビットを 1 に設定します。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] stopbits 1

3.1.32 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、小文字を区別しません。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。このオプションを指定しない場合、装置は送信元アドレスとしてサーバへのルートに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 パケットを送信する IP パケットの DSCP 値を指定します。設定範囲は 0～63 です。デフォルトは 48 です。

説明

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

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

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

例

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

<Switch> telnet 1.1.1.2 source ip 1.1.1.1

関連コマンド

telnet client source

3.1.33 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 コマンドはデフォルトに戻します。

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

3.1.34 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 IPv6 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。サーバーアドレスがグローバルユニキャストアドレスの場合、このオプションは指定できません。

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

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

説明

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

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

例

ホスト 5000::1 に Telnet します。

<Switch> telnet ipv6 5000::1

3.1.35 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: レイヤ 2 ACL を指定します。異なるタイプの ACL を指定するには、このキーワードを指定しないでください。

acl-number: ACL を番号で指定します。**mac** を指定した場合、設定範囲は 4000～4999 です。**mac** キーワードを指定しない場合、設定範囲は 2000～3999 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。

デフォルト ACL が作成されていなくても、このコマンドで ACL を指定することができますが、ACL が作成されたのち、フィルタリングが適用されます。

ACL の詳細は、オペレーションマニュアルのセクション 7 *ACL and QoS* “*ACL*”を参照してください。

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。

このコマンドはでデフォルトの Telnet 接続には適用されません。

例

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

<Switch> system-view

[Switch] acl basic 2001

[Switch-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0

[Switch-acl-ipv4-basic-2001] quit

[Switch] telnet server acl 2001

3.1.36 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 IP パケットの ToS フィールドで送信されます。パケットの転送優先度を示します。

例

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

<Switch> system-view

[Switch] telnet server dscp 30

3.1.37 telnet server enable

Syntax

telnet server enable

undo telnet server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

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

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

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

例

Telnet サーバ機能を有効にします。

<Switch> system-view

[Switch] telnet server enable

3.1.38 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: レイヤ 2 ACL を指定します。異なるタイプの ACL を指定するには、このキーワードを指定しないでください。

acl-number: ACL を番号で指定します。**ipv6** を指定した場合、設定範囲は 2000～3999 です。**mac** を指定した場合、設定範囲は 4000～4999 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。

このコマンドには、存在しない ACL を指定できます。ただし、このコマンドは、ACL を作成し、ACL のルールを設定した後でのみ有効になります。

ACL の詳細は、オペレーションマニュアルのセクション 7 *ACL and QoS* “*ACL*”を参照してください。

複数回、コマンドを設定することができますが、最新の設定のみ適用されます。

このコマンドはデフォルトの Telnet 接続には適用されません。

例

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

<Switch> system-view

[Switch] acl ipv6 basic 2001

[Switch-acl6-ipv6-basic-2001] rule permit source 2000::1 128

[Switch-acl6-ipv6-basic-2001] quit

[Switch] telnet server ipv6 acl ipv6 2001

3.1.39 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 サーバで 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 パケットのトラフィッククラスフィールドで送信されます。パケットの転送優先度を示します。

例

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

<Switch> system-view

[Switch] telnet server ipv6 dscp 30

3.1.40 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 と user line class view の両方で使用できます。どちらかの view のデフォルト以外の設定は、他方の view のデフォルトの設定よりも優先されます。user line view のデフォルト以外の設定は、user line class view のデフォルト以外の設定よりも優先されます。

端末の表示タイプの変更は、現在のセッションでは有効になりません。以降のログインセッションで有効になります。

例

端末の表示タイプを VT100 に設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] terminal type vt100

3.1.41 user-role

Syntax

user-role *role-name*

undo user-role [*role-name*]

デフォルト

AUX line 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、小文字を区別しません。設定範囲は 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。定義済みの security-audit および guest-manager ユーザロールはサポートされません。**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、つまりレベル 15 ユーザロールが割り当てられたユーザだけが、このコマンドを実行できます。他のユーザは、このコマンドを実行する権限が付与されていても、このコマンドを実行できません。

このコマンドは、user line view と user line class view の両方で使用できます。どちらかの view のデフォルト以外の設定は、他方の view のデフォルトの設定よりも優先されます。user line view のデフォルト以外の設定は、user line class view のデフォルト以外の設定よりも優先されます。

ユーザロールの変更は、現在のセッションには適用されません。以降のログインセッションで有効になります。

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

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

例

AUX line0 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

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 4-6
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 4-11
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 4-15
4.2.10 dir 4-16
4.2.11 disconnect 4-17
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 4-22
4.2.16 ftp ipv6 4-23
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 4-32
4.2.26 pwd 4-33
4.2.27 quit 4-34
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

オンライン 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。改行される場合のセグメントが左揃えになります。

フィールドの長さ制限は次のとおりです。

- **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。オンラインの 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ユーザにより確立された 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

IP 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 { *advanced-acl-number* | *basic-acl-number* | **ipv6** { *advanced-acl-number* | *basic-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

advanced-acl-number: IPv4 ACL 番号を指定します。設定範囲は 3000～3999 です。

basic-acl-number : 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

ipv6 *advanced-acl-number* : 高度な IPv6 ACL 番号を指定します。設定範囲は 3000～3999 です。

ipv6 *basic-acl-number*: 標準 IPv6 ACL 番号を指定します。設定範囲は 2000～2999 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。存在する 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 ACL2001 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

IPv4 は FTP クライアントに送信される FTP パケットに DSCP 値 0 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

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 サーバの送信 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

IPv6 は、FTP クライアントに送信される FTP パケットに DSCP 値 0 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

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 サーバの送信 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 パケットのトラフィッククラス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: 時間間隔の設定範囲は 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

FTP 接続の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設定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 クライアントがサポートす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てい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 クライアント view で**?**を入力することは、**help** コマンドを実行するのと同じです。

例

#FTP クライアントでサポートされてい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

binary

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。

FTP は以下のいずれかのモードでファイルを転送します。

- **Binary モード**－テキスト以外のファイルを転送します。
- **ASCII モード**－テキストファイルを転送します。

装置が FTP サーバとして動作する場合、転送モードは FTP クライアントによって決定されます。装置が FTP クライアントとして動作する場合は、転送モードを設定できます。転送モードはデフォルトで binary です。

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

binary

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 Binary 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。

FTP サーバにログインした後、実行できます。

FTP は以下のいずれかのモードでファイルを転送します。

- **Binary モード**－プログラムファイルまたは画像を転送します。
- **ASCII モード**－テキストファイルを転送します。

装置が FTP サーバとして動作する場合、転送モードは FTP クライアントによって決定されます。装置が FTP クライアントとして動作する場合は、転送モードを設定できます。デフォルトの転送モードは binary です。

例

転送モードを Binary 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、このコマンドを使って 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。

..: 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。コマンドは現在の作業ディレクトリを変更しません。

/: 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 **folder** 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。

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。

FTP サーバにログインした後のみ実行できます。

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>

FTP サーバ 192.168.0.211 にログインし、FTP クライアントのデバッグを有効にします。

<Switch> ftp 192.168.0.211 –d

```
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 FTP service ready.
User (192.168.0.211:(none)): abc
*Apr 10 09:02:24:139 2017 Switch FTPC/7/EVENT: PAM initialization result: 0.
*Apr 10 09:02:24:150 2017 Switch FTPC/7/EVENT: PAM: Sent a start-accounting request.
Result: 0.
*Apr 10 09:02:24:860 2017 Switch FTPC/7/COMMAND: USER abc
331 Password required for abc.
Password:
*Apr 10 09:02:25:575 2017 Switch FTPC/7/COMMAND: PASS XXXX
230 User logged in.
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> *Apr 10 09:02:25:640 2017 SIMWARE FTPC/7/COMMAND: SYST
```

ftp>

4.2.14 ftp client ipv6 source

Syntax

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

undo ftp client ipv6 source

デフォルト

IPv6 FTP サーバに送信される FTP 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*: 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 IPv6 アドレスは FTP パケットを送信する送信元アドレスです。転送が成功するために、インタフェースが UP し、IPv6 アドレスが設定されていることを確認してください。

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 クライアントによって送信された 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 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。

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 接続のみに適用されます。

例

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 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

IPv4 FTP サーバに送信される FTP パケットの送信元 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

IPv4 FTP サーバに送信される FTP パケットの送信元 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。このオプションは、FTP サーバアドレスがリンクローカルアドレスで、指定された出力インタフェースにリンクローカルアドレスがある場合にのみ使用できます。リンクローカルアドレスについての詳細は、オペレーションマニュアルのセクション 4 *ＩＰサービス* 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 IPv6 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。指定しない場合は、ソースファイルの名前が使用されます。

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、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、ftp コマンドでアクセスする作業ディレクトリにダウンロードしたファイルを保存するには、次のいずれかの操作を行います。

- *localfile* を指定しないでコマンドを実行します。
- *localfile* には、パス情報を含まない、a.cfg のようなファイル名を指定します。

ダウンロードしたファイルを別のディレクトリに保存するには、*localfile* に、flash :/ subdirectory/a.cfg のような完全修飾ファイル名を指定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 1 のフラッシュ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または変更します。

FTP クライアントのローカル作業ディレクトリを表示するには、*directory* または/引数を指定しないでください。

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または保存します。

FTP サーバにログインした後のみ実行できます。

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 *localfile* で指定したローカルファイルに保存します。

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

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を指定します。

localfile: 更新するローカルファイルを指定します。

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。

FTP オペレーションモードが passive の場合、このコマンドを実行するとモードが active に変更されます。

FTP オペレーションモードが active の場合、このコマンドを実行するとモードが passive に変更されます。

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 オペレーションモードを passive に変更します。

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: アップロードするローカルファイルを指定します。

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 サーバに FTP クライアントの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* 引数で 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* 引数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。そうでなければ、このコマンドが失敗します。

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 2 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

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 サーバでサポートされている FTP コマンドを表示します。

rhelp *protocol-command* は FTP サーバでサポートされている FTP コマンドのヘルプ情報を表示します。

この操作は、FTP サーバにログインした後でのみ実行できます。

例

FTP サーバでサポートされている FTP 関連の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	ユーザ名です。
PASS	パスワードです。
NOOP	NULL操作です。
SYST	システムパラメータです。
TYPE	要求タイプです。
CWD	現在の作業ディレクトリを変更します。
XCWD	CWDの意味を持つ拡張コマンド。
PWD	作業ディレクトリを印刷します。
CDUP	ディレクトリを上位ディレクトリに変更します。
XCUP	CDUPの意味を持つ拡張コマンドです。
XPWD	PWDの意味を持つ拡張コマンドです。
LIST	ファイルを一覧表示します。
NLST	ファイルの簡単な説明が表示されます。
MLSD	ファイルの内容を一覧表示します。

フィールド	説明
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	アップロードを追加します。
DELE	ファイルを削除します。
MKD	フォルダを作成します。
XMKD	MKDの意味を持つ拡張コマンドです。
RMD	フォルダを削除します。
XRMD	RMDの意味を持つ拡張コマンドです。
ABOR	転送を中止します。
SIZE	転送ファイルのサイズです。
RNFR	元の名前です。
RNTO	新しい名前です。

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: FTP サーバのディレクトリを指定します。

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。

rmdir コマンドは、指定されたディレクトリのファイルをごみ箱から削除しません。

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 認証を開始します。

FTP サーバにログインした後のみ実行できます。

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 コマンドは装置を有効または無効にして、FTP 動作の詳細情報を表示します。

このコマンドは現在の FTP セッションのみ適用されます。

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、宛先フォルダにファイルのディレクトリを書き込みます。宛先フォルダ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、宛先フォルダ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ォルダにダウンロードされたファイルの書き込みを行います。宛先フォルダ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。転送が成功するためには、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ことを確認してください。
- **ip** *source-ip-address*: IPv4 アドレスを指定します。転送が成功するために、インタフェースが UP でアドレスが IPv4 アドレスであることを確認してください。

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** ファイルとして保存します。

<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.
```

<Switch>

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…	システムはダウンロードしたファイルを記憶媒体に書き込みました。このフィールドは、**get**または**sget**が指定されている場合にのみ表示されます。 操作が成功した場合、このコマンドはこのフィールドの最後に**Done**を表示します。 操作が失敗した場合、このコマンドは**Failed**を表示します。

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

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*: 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。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。転送が成功するために、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。

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 サーバへ送信する TFTP パケットには、2000::1 を送信元 IPv6 アドレスに指定します。

<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

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*: 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。転送が成功するためには、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ことを確認してください。

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 サーバに送信される 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

IPv4 TFTP サーバへ送信する TFTP パケットには、192.168.20.222 を送信元 IP アドレスに指定します。

<Switch> system-view

[Switch] tftp client source ip 192.168.20.222

関連コマンド

tftp

5.1.4 tftp ipv6

Syntax

tftp ipv6 *tftp-server* [**-i** *interface-type interface-number*] { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

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

-i *interface-type interface-number*: 送信インタフェースのタイプと番号を指定します。このパラメータは TFTP サーバアドレスがリンクローカルアドレスで送信インタフェースにリンクローカルアドレスが設定されているときのみ使用されます。リンクローカルアドレスの詳細は、オペレーションマニュアルのセクション 4 *IP サービス* “*IPv6 の基本*” を参照してください。

get: ファイルをダウンロードし、宛先フォルダにファイルのディレクトリを書き込みます。宛先フォルダ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、宛先フォルダ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ォルダにダウンロードされたファイルの書き込みを行います。宛先フォルダがすでに存在する場合、ダウンロードされたファイルは既存のファイルに上書きします。ダウンロードあるいはメモリへの書き込みが失敗すると、既存のファイルは上書きされません。

source-file: 送信元ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。

destination-file: 宛先ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。この引数が指定されない場合、ファイルは送信元ファイル名を使用します。

dscp *dscp-value*: 送信する TFTP パケットの IPv6 パケットの DSCP 値です。パケットを転送する優先度を示します。設定範囲は 0～63 です。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }: 送信する TFTP パケットの送信元アドレスを指定します。キーワードが指定されない場合、装置は自動で RFC3484 によって定義された送信元 IPv6 アドレスを選択します。

送信元 IPv6 アドレスとしてルートの出力インタフェースのプライマリ IPv6 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 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。転送が成功するために、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ことを確認ください。

- **ipv6** *source-ipv6-address*: IPv6 アドレスを指定します。転送が成功するために、インタフェースが UP でアドレスが IPv6 アドレスであることを確認ください。

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 mount 6-15
6.1.13 move 6-16
6.1.14 pwd 6-17
6.1.15 rename 6-17
6.1.16 reset recycle-bin 6-18
6.1.17 rmdir 6-19
6.1.18 tar create 6-20
6.1.19 tar extract 6-21
6.1.20 tar list 6-22
6.1.21 umount 6-23
6.1.22 undelete 6-24

6章 ファイルシステム管理

6.1 ファイルシステム管理設定コマンド

⚠ **注意:**

- 記録媒体、ファイル、ディレクトリを管理する前に、設定が装置に与える影響を確認してから行ってください。
- ピリオド（．）の名前で始まるファイルあるいはディレクトリは、隠しファイルあるいは隠しディレクトリです。ファイルあるいはディレクトリの先頭にピリオド（．）を使用しないでください。
- いくつかの隠しファイルと隠しディレクトリが存在します。ファイルシステムの管理を行う際は、隠しファイルや隠しディレクトリを修正しないでください。

ファイルシステム名、ディレクトリ名、およびファイル名は、命名規則に準拠している必要があります。命名規則および名前の指定方法の詳細は、オペレーションマニュアルのセクション 1 *はじめに*を参照してください。

ファイルシステムで **copy**、**delete**、**fixdisk**、**format**、**gunzip**、**gzip**、**mkdir**、**move**、**rename**、**rmdir**、または **undelete** コマンドを使用する前に、ファイルシステムが書き込み保護されていないことを確認してください。

パーティション分割されている記憶媒体、またはフォーマット中または修復中のファイルシステムにアクセスすることはできません。ファイルシステムにアクセスするには、進行中の操作が完了するのを待ってから、次のいずれかの方法を使用します。

- ファイルまたはディレクトリを指定するには、絶対パスを使用してください。たとえば、**flash:**ファイルシステム内のファイルとディレクトリを表示するには、**dir flash:/**コマンドを使用します。
- ファイルシステム内のファイルまたはディレクトリにアクセスする前に、**cd** コマンドを使用して作業ディレクトリをファイルシステムのルートディレクトリに変更します。たとえば、**flash:**ファイルシステムのルートディレクトリにあるファイルとディレクトリを表示するには、次の作業を行います。
  - 作業ディレクトリをファイルシステムのルートディレクトリに変更するには、**cd flash:/**コマンドを使用します。
  - **dir** コマンドを実行してください。

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 :　宛先ディレクトリを指定します。

.. :　親ディレクトリを指定します。作業ディレクトリがルートディレクトリの場合、cd .. コマンドを実行するとエラーメッセージが表示されます。このキーワードに関するオンラインヘルプ情報はありません。

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: コピーするファイルの名前を指定します。ファイルが装置上ではなく FTP、TFTP、または HTTP サーバ上にある場合は、ファイルの URL を指定してください。URL の大文字と小文字が区別されるかどうかは、サーバによって異なります。

dest-file: 宛先ファイルの名前または URL を指定します。ソースファイルを FTP、TFTP、または HTTP サーバにコピーするには、URL を指定します。URL の大文字と小文字が区別されるかどうかは、サーバによって異なります。

dest-directory: 宛先ディレクトリまたは URL を指定します。ソースファイルを FTP、TFTP、または HTTP サーバにコピーするには、URL を指定します。装置はソースファイルをコピー先の場所にコピーし、ファイルを元のファイル名で保存します。URL の大文字と小文字が区別されるかどうかは、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 あるいは TFTP サーバに保存します。
- FTP あるいは TFTP サーバのファイルをコピーし、ローカルに保存します。

ファイルあるいはディレクトリを指定するため、以下のガイドラインを使用します。

位置	フォーマット	補足
装置	オペレーションマニュアルのセクション1 *はじめに*“*ファイルシステム管理*”の“*ファイル名のガイドライン*”を参照してください。	―
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の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。 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。

位置	フォーマット	補足
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。
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*] .	URLのユーザ名とパスワードは、サーバ上で設定されているユーザ名とパスワードと同じでなければなりません。認証にユーザ名だけが必要な場合は、パスワードを入力する必要はありません。 認証が不要な場合は、ユーザ名やパスワードを入力する必要はありません。 たとえば、**startup.cfg**ファイルは、1.1.1.1のHTTPサーバ上の許可ディレクトリに保存されます。HTTPアカウントのユーザ名とパスワードはそれぞれ**a**と**1**です。ファイルをコピーするには、URL http://a:1@1.1.1.1/startup.cfgを入力します。認証が不要な場合は、URL http://1.1.1.1/startup.cfgを入力してください。

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.
```

**1.cfg** ファイルを flash : ファイルシステムの test ディレクトリから USB ディスクにコピーします。そのコピーを最初のパーティションの **testbackup** ディレクトリに **1backup.cfg** として保存します。

<Switch> copy flash:/test/1.cfg usba0:/testbackup/1backup.cfg

```
Copy flash:/test/1.cfg to usba0:/testbackup/1backup.cfg?[Y/N]:y
Copying file flash:/test/1.cfg to usba0:/testbackup/1backup.cfg...Done.
```

現在のディレクトリに **test.cfg** ファイルをコピーし、**testbackup.cfg** として特定のスロットのファイルシステムのルートディレクトリに保存します。

<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 **test.cfg** をコピーします。コピーをローカルの現在のディレクトリに **testbackup.cfg** として保存します。 FTP のユーザ名は **user** です。 パスワードは非公開です。

<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 の許可ディレクトリから **test.cfg** をコピーします。コピーをローカルの現在のディレクトリに **testbackup.cfg** として保存します。HTTP ログインのユーザ名は **user** です。パスワードは非公開です。

<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.
```

現在のディレクトリから **test.cfg** をコピーします。このコピーを HTTP サーバ 1.1.1.1 上の許可ディレクトリに **testbackup.cfg** として保存します。 HTTP ログインのユーザ名は user です。パスワードは非公開です。

<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 の許可ディレクトリから **test.cfg** をコピーします。コピーをローカルの現在のディレクトリに **testbackup.cfg** として保存します。 HTTP ログインのユーザ名は user です。パスワードは非公開です。

<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。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、“**delete *.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* コマンドは、ファイルを永久に削除します。削除したファイルは復元できません。

/unreserved パラメータを使用しない **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 **1.cfg** ファイルを削除します。

<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 **1.cfg** ファイル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ディレクトリを隠しファイル、隠しディレクトリを含めてすべて表示します。指定しない場合、隠しファイル、隠しディレクトリを除いたファイルとディレクトリが表示されます。

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 : 特定の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にあるファイルとディレクトリを表示します。

説明

dir コマンドはファイルあるいはディレクトリを表示します。

オプションを指定しない場合、現在のディレクトリの隠しファイル、隠しディレクトリを除いたファイルとディレクトリを表示します。

ごみ箱のディレクトリ名は.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。

複数のユーザがファイル操作（ファイルやディレクトリの作成または削除など）を同時に実行した場合、このコマンドの出力は正しくない可能性があります。

例

現在のディレクトリ内のすべてのファイルとディレクトリの情報を表示します。

<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ファイルとディレクトリを表示します。

<Switch> dir /all-filesystems

```
Directory of flash:/
...

Directory of usba0:/
...
```

表 6-1 コマンド出力

フィールド	説明
Directory of	現在のディレクトリです。
0 -rwh 3144 Apr 26 2014 13:45:28 xx.xx	ファイルあるいはディレクトリ情報です。 • **0**—ファイルあるいはディレクトリ番号です。システムによって自動で割り当てられます。 • **-rwh**—ファイルあるいはディレクトリの属性です。最初の文字はディレクトリを示します。dはディレクトリで、ーはファイルです。2番目の文字はファイルあるいはディレクトリ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ディレクトリ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ディレクトリ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ディレクトリで、ーは通常のファイルあるいはディレクトリです。変更、名前の変更、隠しファイル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。ディレクトリはハイフン（ー）が表示されます。 • **Apr 26 2014 13:45:28**—ファイルあるいはディレクトリが変更された最後の日時です。 • **xx.xx**—ファイルあるいはディレクトリ名です。

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: ファイルあるいはディレクトリ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: 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、ディレクトリのプロンプトモードを設定します。

undo file prompt コマンドはデフォルトに戻します。

quiet モードである場合、システムはいかなるファイルあるいはディレクトリ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、ディレクトリ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。

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、ほかのユーザが記憶媒体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フラッシュを修復します。

<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。

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。

この装置では、活線挿抜対応の記憶媒体上のファイルシステムが VFAT である必要があります。装置上で異なるタイプのファイルシステムを使用するには、このコマンドを使用して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.
```

USB メモリをフォーマットします。

<Switch> format usba2:

```
All data on usba2: will be lost, continue? [Y/N]:y
```

```
Formatting usba2:... 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、元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


524288 KB total (184664 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


524288 KB total (184664 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。

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、圧縮ファイルを *file*.**gz** ファイルに保存し、ソース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


524288 KB total (184664 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


524288 KB total (184664 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: ディレクトリを指定します。

説明

mkdir コマンドはディレクトリを作成します。

ディレクトリの名前は親ディレクトリ内で一意である必要があります。

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。

例

現在のディレクトリにディレクトリ **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ディレクトリ **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 mount

Syntax

mount *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。

説明

mount コマンドはファイルシステムをマウントするように設定します

一般に、活線挿抜対応の記憶媒体上のファイルシステムは、その記憶媒体が装置に接続されると自動的にマウントされます。ただし、システムがファイルシステムを認識できない場合は、アクセスする前にファイルシステムをマウントする必要があります。

ファイルシステムの損傷を避けるため、ファイルシステムをマウントしている場合は以下の処理を実行しないでください。

- 装置を再起動、電源の入れ直し、または電源を切ります。
- 記憶媒体の挿入、あるいは取り外しを行います。
- 入れ替えを実行します。

活線挿抜対応の記憶媒体をデバイスから取り外すときは、最初に記憶媒体上のすべてのファイルシステムをアンマウントする必要があります。マウントされたままで取り外すと、記憶媒体上のファイルや記憶媒体自体が破損する可能性があります。

例

ファイルシステムを USB ディスクにマウントします。

<Switch> mount usba0:

関連コマンド

umount

6.1.13 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: 宛先ディレクトリ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。

ターゲットディレクトリを指定する場合、システムはファイル名を変更しないで指定したディレクトリ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** をディレクトリ **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.
```

6.1.14 pwd

Syntax

pwd

View

User view

定義済みユーザロール

network-admin

説明

pwd コマンドは作業ディレクトリを表示します。

例

作業ディレクトリを表示します。

<Switch> pwd

```
flash:
```

6.1.15 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: ソースディレクトリ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: 宛先ディレクトリ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ディレクトリの名前を変更します。

作業ディレクトリのファイルあるいはディレクトリに変更しようとするファイルあるいはディレクトリ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.
```

6.1.16 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。このオプションを指定しない場合、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

6.1.17 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: ディレクトリを指定します。

説明

rmdir コマンドはディレクトリを削除します。

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

ディレクトリ **subtest** を削除します。

<Switch>rmdir subtest/

```
Remove directory flash:/test/subtest and the files in the recycle-bin under this
directory will be deleted permanently. Continue?[Y/N]:y
Removing directory flash:/test/subtest... Done.
```

6.1.18 tar create

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: ファイルとディレクトリをアーカイブする前に **gzip** コマンドでファイルとディレクトリを圧縮します。指定しない場合、コマンドはファイルとディレクトリを圧縮せずにアーカイブします。

archive-file *dest-file*: アーカイブファイル名を指定します。**gz** 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** 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とディレクトリの名前を表示します。指定しない場合、正常にアーカイブされたファイルおよびディレクトリの名前は表示されません。

source { *source-file* | *source-directory* }&<1-5>: アーカイブされるファイルあるいはディレクトリを指定します。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とディレクトリをアーカイブします。

例

ファイル **1.cfg** とファイル **2.cfg**、およびテストディレクトリを **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** とファイル **2.cfg**、およびテストディレクトリを **b.tar.gz** に圧縮してアーカイブします。

<Switch> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test

```
Creating archive flash:/b.tar.gz Done.
```

ファイルとディレクトリを圧縮、アーカイブします。アーカイブしたファイルとディレクトリを表示します。

<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**

6.1.19 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ディレクトリの名前を表示します。

screen: 画面に解凍したファイルとディレクトリ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*: 解凍したファイルとディレクトリを別のディレクトリに保存します。*directory* はディレクトリを指定します。

説明

tar extract コマンドはファイルとディレクトリを解凍します。

screen キーワードあるいは **to** *directory* オプションを指定しない場合、解凍したファイルとディレクトリを作業ディレクトリに保存します。

このコマンドは、解凍したファイルとディレクトリを元の名前を使用して保存します。解凍したファイルまたはディレクトリと同じ名前のファイルまたはディレクトリが宛先ディレクトリにすでに存在する場合、そのファイルまたはディレクトリは上書きされます。

例

アーカイブファイル **a.tar** からファイルと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 からファイルとディレクトリを解凍し、正常に解凍されたファイルとディレクトリ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** からファイルとディレクトリを解凍し、ファイルの内容を画面に表示します。

<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**

6.1.20 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ディレクトリの名前を表示します。

例

アーカイブしたファイルとディレクトリ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**

6.1.21 umount

Syntax

umount *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。

説明

umount コマンドはファイルシステムをマウント解除します。

記憶媒体上のファイルシステムは、記憶媒体が装置に接続されると自動的にマウントされます。装置から活線挿抜対応の記憶媒体を取り外すには、まずその記憶媒体上のすべてのファイルシステムをマウント解除する必要があります。マウントされている活線挿抜対応の記憶媒体を取り外すと、その記憶媒体またはさらにはその記憶媒体上のファイルが損傷する可能性があります。

記憶媒体をアンマウントする前に、ほかのユーザが記憶媒体にアクセスしていないことを確認してください。さもないとアンマウント処理ができません。

ファイルシステムの損傷を避けるため、記憶媒体をマウントあるいはアンマウントしている場合は以下の処理を実行しないでください。

- 装置を再起動、電源の入れ直し、または電源を切ります。
- 記憶媒体の挿入、あるいは取り外しを行います。
- マスタ/サブの入れ替えを実行します。

例

USB メモリ上のファイルシステムをアンマウントします。

<Switch> umount usba0:

関連コマンド

mount

6.1.22 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。ファイル名の拡張子は.cfg です。ファイル名は、最大 255 文字です。大文字、小文字を区別しません。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

IPv4 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。

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* を指定しない場合、このコマンドはすべてのインタフェースの実行コンフィグレーションを表示します。*interface-type* だけを指定した場合、このコマンドはこのタイプのすべてのインタフェースの実行コンフィグレーションを表示します。

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。

システムがパラメータの設定を自動的に変更した場合、コンフィグ設定された設定に代わって有効となっている設定を表示します。自動的な設定変更は、一般的にシステムの制限により発生します。

例

ローカルユーザの設定を表示します。

<Switch> display current-configuration configuration local-user

```
#
local-user ftp
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ftp
 authorization-attribute user-role network-operator
#
```

```
local-user root
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

VLAN インタフェースの設定を表示します。

<Switch> display current-configuration interface Vlan-interface

```
#
interface Vlan-interface1
 ip address 192.168.1.84 255.255.255
#
Return
```

7.1.3 display current-configuration diff

Syntax

display current-configuration diff

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display current-configuration diff コマンドは現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間の差分の設定を表示します。

例

現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間の差分の設定を表示します。

<Switch> display current-configuration diff

```
--- Startup configuration
+++ Current configuration
@@ -5,7 +5,7 @@
#
```

```
  sysname Switch
 #
-alias dhc display history-command
+alias dh display hotkey
 #
system-working-mode standard
```

<Switch>

表 7-1 コマンド出力

フィールド	説明
--- *A* +++ *B*	● *A*は比較のためのソース設定を表します。スタートアップ設定、現在の設定、またはソース設定ファイルの名前とそのディレクトリ情報を指定できます。次回の起動に使用するコンフィグレーションファイルです。 ● *B*は比較のためのターゲット設定を表します。現在の設定、スタートアップ設定、またはターゲット設定ファイルの名前とそのディレクトリ情報を指定できます。 この例では、スタートアップコンフィグレーションと現在のコンフィグレーションは、それぞれソースとターゲットです。
@@ *-linenumber1,number1* *+linenumber2,number2* @@	異なるコマンドラインの位置の概要です。 ● *-linenumber1,number1*ー違いを含む設定セクション。linenumber1は、セクションの開始行を表します。number1引数は、セクションの開始行と終了行の間の行数を表します。 ● *+linenumber2,number2*ー違いを含む設定セクション。linenumber2は、セクションの開始行を表します。number2は、セクションの開始行と終了行の間の行数を表します。

フィールド	説明
cmd1 *- cmd2* *+ cmd3* *cmd4*	コマンドの違いを表示します。 • *cmd1*と*cmd4*ーコマンドラインの先頭にマイナス（ - ）またはプラス（+）の記号が付いていない場合、コマンドラインはソースとターゲットの両方の設定に含まれています。それらはコマンドラインの違いを見つけるためのコンテキストを提供します。 • *- cmd2*ーコマンドラインがソース設定に含まれていてターゲット設定に含まれていない場合は、コマンドラインの先頭にマイナス記号が付きます。 • + *cmd3*ーターゲット設定に含まれているがソース設定には含まれていない場合は、コマンド行の先頭にプラス記号が付きます。 この例では、**alias dhc display history-command**コマンドはソース設定にのみ含まれ、**alias dh display hotkey**コマンドはターゲット設定にのみ含まれています。

関連コマンド

- **display current-configuration**
- **display diff**
- **display saved-configuration**

7.1.4 display default-configuration

Syntax

display default-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display default-configuration コマンドは工場出荷状態のデフォルトコンフィグレーション設定を表示します。

工場出荷状態のコンフィグレーションはデフォルトコンフィグレーションファイルにあります。製品仕様のデフォルト設定は初期設定と異なります。設定ファイルがない場合

あるいは設定ファイルが壊れている場合、デフォルト設定によって装置が起動し、正常に動作するようにします。

例

デフォルトコンフィグレーション設定を表示します。

<Switch> display default-configuration

7.1.5 display diff

Syntax

display diff configfile *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }

display diff current-configuration { **configfile** *file-name-d* | **startup-configuration** }

display diff startup-configuration { **configfile** *file-name-d* | **current-configuration** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configfile *file-name-s*: 比較元のコンフィグレーションファイルを指定します。

configfile *file-name-d*: 比較先のコンフィグレーションファイルを指定します。

current-configuration: 現在のコンフィグレーションファイルを指定します。**display diff current-configuration** コマンドにおいて、このパラメータは、比較元のコンフィグレーションファイルを指定します。他の 2 つの **display diff** コマンドにおいて、このパラメータは比較先のコンフィグレーションファイルを指定します。

startup-configuration: 次回の起動に使用するコンフィグレーションファイルを指定します。**display diff startup-configuration** コマンドにおいて、このパラメータは比較元のコンフィグレーションファイルを指定します。他の 2 つの **display diff** コマンドにおいて、このパラメータは比較先のコンフィグレーションファイルを指定します。

説明

display diff コマンドは 2 つのコンフィグレーションファイルの設定の相違を表示します。

例

startup.cfg と **test.cfg** の違いを表示します。

<Switch> display diff configfile startup.cfg configfile test.cfg

```
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -5,7 +5,7 @@
 #
  sysname Switch
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
```

<Switch>

出力には、**alias dhc display history-command** コマンドは **startup.cfg** にのみ含まれ、**alias dh display hotkey** コマンドは **test.cfg**.にのみ含まれることが示されています。

実行コンフィグレーションと次回のスタートアップコンフィグレーションの違いを表示します。

<Switch> display diff current-configuration startup-configuration

```
--- Current configuration
+++ Startup configuration
@@ -5,7 +5,7 @@
 #
  sysname Switch
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
```

<Switch>

出力には、**alias dhc display history-command** コマンドは実行コンフィグレーションにのみ含まれ、**alias dh display hotkey** コマンドは次回の起動コンフィグレーションにのみ含まれることが示されています。

コマンド出力の説明については、表 7-1 を参照してください。

関連コマンド

- **display current-configuration**
- **display current-configuration diff**
- **display saved-configuration**

7.1.6 display saved-configuration

Syntax

display saved-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display saved-configuration コマンドは装置が次回に起動に使用するために保存されているコンフィグレーションファイルの内容を表示します。

このコマンドは、装置の次回に起動するときに使用できるように重要な設定がコンフィグレーションファイルに保存されているかどうかを確認することができます。

以下の順番でコンフィグレーションファイルを選択します。

1) メインのコンフィグレーションファイルが有効である場合、メインのコンフィグレーションファイルの内容を表示します。
2) バックアップのコンフィグレーションファイルが有効である場合、バックアップのコンフィグレーションファイルの内容を表示します。
3) メインのコンフィグレーションファイルとバックアップのコンフィグレーションファイルが有効でない場合、何も表示されません。

例

次回に起動するコンフィグレーションファイルの内容を表示します。

<Switch> display saved-configuration

```
#
 version 7.1.070, Release 1201
#
 sysname Switch
#
 ftp server enable
#
 telnet server enable
#
 domain default enable system
#
vlan 1
#
```

```
domain system
#
  ---- More ----
```

関連コマンド

- **reset saved-configuration**
- **save**

7.1.7 display startup

Syntax

display startup

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display startup コマンドは現在のスタートアップコンフィグレーションファイルと次回に起動するコンフィグレーションファイルの名前を表示します。

すべての IRF スタックのメンバは Master と同一の現在のスタートアップコンフィグレーションファイルを使用します。Master とメンバの切り替えが行われた後、現在のスタートアップコンフィグレーションファイルの名前は NULL と表示されます。これはスタートアップコンフィグレーションファイルで再起動するのではなく、新しい Master は現在の設定で動作し続けるためです。

例

スタートアップコンフィグレーションファイルの名前を表示します。

<Switch> display startup

```
Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

表 7-2 コマンド出力

フィールド	説明
Current Startup saved-configuration file	装置が起動した際のコンフィグレーションファイルです。
Next main startup saved-configuration file	次回起動する際に使用するプライマリ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-interface 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指定します。

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指定します。

説明

⚠ **注意:**

すべての IRF スタックのメンバ装置から次回の起動時に使用するコンフィグレーションファイルを完全に削除します。

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。

メインファイル、バックアップファイル、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。

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。

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。このファイルの拡張子で.cfg でなければなりません。ファイル名は、最大 255 文字の大文字、小文字を区別しない文字列です。

説明

restore startup-configuration コマンドは指定した TFTP サーバからコンフィグレーションファイルをダウンロードし、次回の起動時に使用するコンフィグレーションファイルとして指定します。

次回の起動時に使用するコンフィグレーションファイルを指定する前に、以下の要件を確認してください。

- サーバが到達可能です。
- サーバが TFTP サービスを有効にしています。
- サーバへの読み込み、書き込み許可があります。

このコマンドは、各メンバ装置のデフォルト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、そのファイルを次回のメインスタートアップコンフィグレーションファイルとして指定します。パーティション化された USB ディスクがデフォルトの記憶媒体として使用されている場合、設定ファイルは最初のパーティションに保存されます。すべての IRF スタックメンバが同じタイプのデフォルトの記憶媒体を使用していることを確認してください。従属装置がマスタとは異なるタイプのデフォルト記憶媒体を使用する場合、コマンドは設定ファイルを従属装置に伝搬することはできません。例えば、配下装置は USB ディスクを使用しますが、マスタ装置はフラッシュメモリを使用します。このような場合は、手動で下位のメインスタートアップコンフィグレーションファイルを復元する必要があります。

例

IPv4 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: ファイルパス、最大 255 文字の文字列を指定します。ファイルは.cfg ファイルでなければなりません。**all** または **slot** *slot-number* オプションを指定した場合、ファイルパスにメンバ ID を含めることはできません。ファイルパスにフォルダ名が含まれている場合、そのフォルダはすべての IRF スタックメンバにすでに存在している必要があります。

all: すべてのメンバ装置に稼働中の設定を保存します。指定しないあるいは **slot** *slot-number* オプションを指定しない場合、Master 装置のみ稼働中の設定を保存します。

slot *slot-number*: 稼働中の設定をメンバ装置に保存します。*slot-number* は装置の IRF スタックのメンバ ID を示します。このオプションあるいは all を指定しない場合、Master 装置のみ稼働中の設定を保存します。

safely: safe モードでコンフィグレーションファイルを保存します。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。

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** あるいは **main** 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** あるいは **backup** 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。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 IRF スタックメンバにファイルを自動的に保存し、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**] [**changed**]コマンドは、次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

モリ容量の不足またはストレージスペース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。

safe モードは fast モードより遅いですが、より安全です。確実に設定を保存するために **safely** を指定してください。

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.
```

稼働中の設定をデフォルトの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

次回起動時の設定ファイルは指定されていません。

View

User view

定義済みユーザロール

network-admin

パラメータ

cfgfile: 設定ファイルのパスを指定します。最大 255 文字の文字列です。ファイルは“.cfg”ファイルでなければなりません。ファイルパスには、ファイル名のみ、または記憶媒体情報とファイル名を含めることができます。ファイルがデフォルトの記憶媒体にない場合は、記憶媒体情報とともにファイル名を指定する必要があります。

backup: コンフィグレーションファイルをバックアップの次回の起動に使用するコンフィグレーションファイルとして指定します。

main: コンフィグレーションファイルをメインの次回の起動に使用するコンフィグレーションファイルとして指定します。これは、装置が起動時に読み込みを行うメインのコンフィグレーションファイルです。読み込みに失敗した場合、装置はバックアップの次回の起動に使用するコンフィグレーションファイルの読み込みを行います。

説明

⚠ **注意:**

IRF スタックで **undo startup saved-configuration** コマンドを使用する場合は注意してください。IRF スタックあるいは IRF スタックメンバの再起動後に IRF スタックが分裂します。

---

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します。

IRF スタックでは、**startup saved-configuration** コマンドはすべての IRF スタックのメンバに適用します。コマンドを設定するため、各メンバ装置の記憶媒体のルートディレクトリに指定されたファイルがすでに存在していることを確認します。

backup あるいは **main** を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。

メインファイルとバックアップの次回起動時の設定ファイルに異なるファイルを指定します。

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 8-4
8.1.3 display boot-loader 8-5

8章 ソフトウェア管理

8.1 ソフトウェア管理設定コマンド

8.1.1 boot-loader file

Syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] { **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: Boot: イメージファイルを指定します。

system: System イメージファイルを指定します。

feature: 最大 30 個のフィーチャイメージファイルの、スペースで区切られたリストを指定します。

filename: *filesystemname* / *filename***.bin** 形式の.bin ファイルを指定します。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。ファイルシステムの場所セクション(存在する場合)を除き、値の文字列は最大 63 文字です。ファイルの指定の詳細については、オペレーションマニュアルのセクション 1 *はじめに* を参照してください。

ipe-filename: *filesystemname* / *filename***.ipe** 形式の.ipe イメージパッケージファイルを指定します。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保存されている必要があります。ファイルシステムの場所セクションがある場合を除き、設定範囲は最大 63 文字です。ファイルの指定の詳細については、オペレーションマニュアルのセクション 1 *はじめに* を参照してください。

all: すべての IRF スタックのメンバ装置を指定します。

slot *slot-number*: 次回の起動に使用するイメージが指定された装置の IRF スタックのメンバ ID を指定します。

backup: バックアップの次回の起動に使用するファイルを指定します。バックアップの次回の起動に使用するイメージファイルはメインの次回の起動に使用するイメージファイルが有効でないときのみ使用されます。

main: メインの次回の起動に使用するファイルを指定します。装置は起動時には常にメインの次回の起動に使用するファイルで起動を行います。

説明

boot-loader file コマンドは起動イメージファイルを指定します。

boot-loader file コマンドは起動イメージリスト全体を上書きします。新しいスタートアップ機能イメージを追加するには、機能イメージファイルを含むすべての機能イメージファイルを古いスタートアップイメージリストに指定します。 新しい起動イメージリストには、コマンドで指定された機能イメージファイルのみが含まれます。

指定された起動ソフトウェアイメージをロードするには、システムを再起動する必要があります。

アップグレードイメージがアップグレードに指定されたスロットのファイルシステムに見つからない場合、システムは自動的にそのファイルシステムにイメージをコピーします。宛先ディレクトリは、ファイルシステムのルートディレクトリです。宛先ルートディレクトリにアップグレードイメージと同じ名前のスタートアップイメージが既に含まれている場合は、イメージを上書きするかどうかを選択する必要があります。

例

IRF スタックのメンバ 1 のメインスタートアップ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 file flash:/all.ipe on slot 1.....Done.
NEC QX-S5324GT-4X1C images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:Y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:Y
Decompressing file boot.bin to flash:/boot.bin.....Done.
Decompressing file system.bin to
flash:/system.bin.....Done.
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.....Done.
The images that have passed all examinations will be used as the main startup
software images at the next reboot on slot 1.
```

#すべての IRF スタックメンバのメインスタートアップイメージファイルとして **flash：/all.ipe** を指定します。

<Switch> boot-loader file slot1#flash:/all.ipe all main

```
Verifying the file flash:/all.ipe on slot
1.....................................Done.
NEC QX-S5324GT-4X1C Switch images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:y
Decompressing file boot.bin to flash:/boot.bin.......................Done.
Decompressing file system.bin to flash:/system.bin.....................Done.
The images that have passed all examinations will be used as the main startup
software images at the next reboot on slot 1.
File flash:/boot.bin already exists on slot 2.
Do you want to overwrite the file?
 Y: Overwrite the file.
 N: Not overwrite the file.
 A: From now on, overwrite or not overwrite without prompt.
Please make a choice. [Y/N/A]:a
What type of overwrite operation do you want to perform?
 Y: Overwrite without prompt.
 N: Not overwrite or display prompt.
 Q: Return to the previous step.
Please make a choice. [Y/N/Q]:y
An existing file will be overwritten without prompt if it has the same name as
any upgrade file.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
The images that have passed all examinations will be used as the main startup
software images at the next reboot on slot 2.
The images that have passed all examinations will be used as the main startup
software images at the next reboot on slot 3.
Decompression completed.
Do you want to delete flash:/all.ipe now? [Y/N]:n
```

関連コマンド

display boot-loader

8.1.2 bootrom update

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

file *file*: フラッシュの Boot Ware イメージが含まれるファイルを指定します。設定範囲は 1～63 です。

slot *slot-number-list*: IRF スタックのメンバ装置のメンバ ID を半角スペースで区切って 7 つまで指定します。項目は、メンバ ID によって IRF スタックメンバ装置を指定するか、*start-slot-number* **to** *end-slot-number* の形式で IRF スタックメンバ装置の範囲を指定します。終了スロット番号は開始スロット番号以上でなければなりません。

説明

bootrom update コマンドはフラッシュの Boot Ware イメージを、Boot Ware 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 Ware 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 Ware に新しい Boot Ware イメージをアップグレードします。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

ファイル **a.bin** を使用して、Boot Ware イメージをアップグレードします。

<Switch> bootrom update file flash:/a.bin slot 1

```
  This command will update the Boot ROM file on the specified board(s), Continue?
[Y/N]:y
  Now updating the Boot ROM, please wait.............Done.
```

関連コマンド

boot-loader file

8.1.3 display boot-loader

Syntax

display boot-loader [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタック装置のメンバ ID を指定します。メンバ装置が指定されない場合、各 IRF スタック装置のソフトウェアイメージを表示します。

説明

display boot-loader コマンドは現在のソフトウェアイメージと次回の起動に使用するソフトウェアイメージを表示します。

例

現在のソフトウェアイメージと次回の起動に使用するソフトウェアイメージを表示します。

<Switch> display boot-loader

```
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
  flash:/boot.bin
  flash:/system.bin
```

表 8-1 コマンド出力

フィールド	説明
Current software images	Comwareイメージが読み込まれました。
Main startup software images	次回の起動に使用するメインのComwareイメージです。

フィールド	説明
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 ISSU.....9-1
9.1 ISSU 設定コマンド.....9-1
9.1.1 display issu rollback-timer.....9-1
9.1.2 display issu state.....9-2
9.1.3 display version comp-matrix file.....9-5
9.1.4 issu accept.....9-6
9.1.5 issu commit.....9-7
9.1.6 issu load.....9-9
9.1.7 issu rollback.....9-12
9.1.8 issu rollback-timer.....9-13
9.1.9 issu run switchover.....9-14

9章 ISSU

9.1 ISSU設定コマンド

9.1.1 display issu rollback-timer

Syntax

display issu rollback-timer

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display issu rollback-timer コマンドは自動ロールバックタイマの情報を表示します。

ISSU プロセスの処理中に、自動ロールバックタイマの変更が行われても、ISSU プロセスを処理しているプロセスには適用されません。現在のロールバックタイマの残存時間は、設定された自動ロールバックの間隔より大きくなります。

例

issu run switchover コマンドを実行した後、自動ロールバックタイマの情報を表示します。

<Switch> display issu rollback-timer

```
Rollback timer: Working
Rollback interval: 45 minutes
Rollback time remaining : 40 minutes
```

issu accept コマンドを実行した後、自動ロールバックタイマの情報を表示します。

<Switch> display issu rollback-timer

```
Rollback timer: Not working
Rollback interval: 30 minutes
```

ISSU プロセスが行われていないとき、自動ロールバックタイマの情報を表示します。

<Switch> display issu rollback-timer

```
Rollback timer: Not working
Rollback interval: 45 minutes
```

関連コマンド

issu rollback-timer

9.1.2 display issu state

Syntax

display issu state

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display issu state コマンドは ISSU の状態を表示します。

issu コマンドは実行している ISSU プロセス中に、ISSU の状態を確認することができます。次に何を実行するどうかを決定します。

例

アップグレードが行われていないとき、ISSU の状態を表示します。

<Switch> display issu state

```
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot: None
Current version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Current software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
```

issu load コマンドが実行されている間に、ISSU の状態を表示します。

<Switch> display issu state

```
ISSU state: Loading
```

```
Compatibility: Incompatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot:
  slot 1
Previous version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Previous software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
Upgrade version list:
  boot: 7.1.070, Test 0001016
  system: 7.1.070, Test 0001016
  feature1: 7.1.070, Test 0001016
Upgrade software images:
  flash:/boot-t0001016.bin
  flash:/system-t0001016.bin
  flash:/feature1-t0001016.bin
```

表 9-1 コマンド出力

フィールド	説明
ISSU state	ISSUの状態です。 • **Init**—ISSUプロセスが開始されていない、あるいは完了していません。 • **Loading**—システムは**issu load**コマンドを実行しています。 • **Loaded**— **issu load**コマンドが完了しました。 • **Switching**—システムは**issu run switchover**コマンドを実行しています。 • **Switchover**—**issu run switchover**コマンドが完了しました。 • **Accepted**—**issu accept**コマンドが完了しました。 • **Committing**—システムは**issu commit**コマンドを実行しています。 • **Rollbacking**—ロールバック中です。

フィールド	説明
Compatibility	ソフトウェアの互換性を示します。 • **Compatible**－互換性があります。 • **Incompatible**－互換性がありません。 • **Unknown**—アップグレードの必要がありません。
Work state	装置の動作状態です。 • **Normal**—装置が正常に動作しています。 • **Independent active**—互換性のないISSUアップグレード方法を実行するとき、アップグレードが行われたメンバ装置は、**Independent active**状態になります。この動作状態のIRFスタックユニットのメンバ装置は異なるソフトウェアバージョンで稼働しています。
Upgrade method	アップグレードモードです。このフィールドが**Card by card**と表示される場合、アップグレードはメンバ装置ごとに実行されます。
Upgraded slot	アップグレードされたメンバ装置です。
Current upgrading slot	アップグレードされているメンバ装置です。
Current version list	現在実行中のイメージのバージョンです。 このフィールドは、アップグレードが実行されていない場合に表示されます。
Current software images	現在実行中のイメージのファイル名です。 このフィールドは、アップグレードが実行されていない場合に表示されます。
Previous version list	ISSUを行う前に装置で稼働しているソフトウェアバージョンです。
Previous software images	ISSUを行う前に装置で稼働しているソフトウェアイメージです。
Upgrade version list	アップグレードを行うソフトウェアバージョンです。
Upgrade software images	アップグレードを行うソフトウェアイメージです。

関連コマンド

- **issu accept**
- **issu commit**
- **issu load**
- **issu rollback**
- **issu run switchover**

9.1.3 display version comp-matrix file

Syntax

display version comp-matrix file { **boot** *filename* | **system** *filename* } *

display version comp-matrix file ipe *ipe-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

boot: ブートファイルを指定します。

system: システムファイルを指定します。

filename: *filesystemname/filename***.bin** 形式の“.bin”ファイルを指定します。ファイルは、装置上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。ファイルシステムの場所セクションがある場合は、それを除いた値の文字列は最大 63 文字です。ファイルの指定の詳細については、オペレーションマニュアルのセクション 1 *はじめに* "*ファイルシステム管理*"を参照してください。

ipe-filename: *filesystemname/filename***.ipe** の形式の“.ipe”ファイルを指定します。ファイルは、装置上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。ファイルシステムの場所セクションがある場合は、それを除いた値の文字列は最大 63 文字です。ファイルの指定の詳細については、オペレーションマニュアルのセクション 1 *はじめに* "*ファイルシステム管理*"を参照してください。

説明

display version comp-matrix file コマンドは推奨される ISSU 方式を表示します。

1 つ以上のイメージに互換性がない場合は、互換性のないアップグレード方法が適用されます。互換性のないアップグレード中にシステム全体を再起動する必要があります。

例

推奨される ISSU 方式を表示します。この例では、指定されたイメージは実行中のイメージと互換性があります。

<Switch> display version comp-matrix file boot flash:/boot-t0001015.bin system flash:/system-t0001015.bin

```
Verifying the file flash:/boot-t0001015.bin on slot 1.....Done.
Verifying the file flash:/system-t0001015.bin on slot 1.....Done.
Identifying the upgrade methods.........Done.
```

```
Slot     Upgrade Way
1        File Upgrade
```

表 9-2 コマンド出力

フィールド	説明
Verifying the file	システムはファイルの有効性を検証していました。
Upgrade Way	互換性のあるISSUアップグレード方法です。 • **Service Upgrade**—サービスレベルのインクリメントアップグレードです。 • **File Upgrade**—ファイルレベルのインクリメントアップグレードです。 • **Reboot**—アップグレードを行うために全装置を再起動します。 このフィールドは、互換バージョンの場合にのみ表示されます。 ISSUアップグレード方法の詳細は、オペレーションマニュアルのセクション1 *はじめに* “*ISSU*”を参照してください。
Influenced service according to following table	アップグレードによって影響を受けるサービスです。 このフィールドは、互換性のあるアップグレード方法でのみ表示されます。

関連コマンド

issu load

9.1.4 issu accept

Syntax

issu accept

View

User view

定義済みユーザロール

network-admin

説明

issu accept コマンドは互換性のあるバージョンにアップグレードすることを許可し、自動ロールバックタイマを削除します。

issu accept コマンドを実行した後、ISSU プロセスで自動ロールバックを行うことはできませんが、手動でロールバックを行う **issu rollback** コマンドを使用することができます。

issu accept コマンドを実行しないで ISSU プロセスを完了させるため、**issu commit** コマンドを実行することができます。

issu accept コマンドは互換性のない ISSU のアップグレード方法には適用しません。互換性のないアップグレード方法での ISSU プロセスの処理中に、**issu accept** コマンドを実行した場合、エラーメッセージを表示します。

例

互換性のあるバージョンにアップグレードすることを許可します。

<Switch> issu accept

関連コマンド

- **issu load**
- **issu run switchover**

9.1.5 issu commit

Syntax

issu commit 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*: もとのマスタ装置のメンバ ID あるいはアップグレードされていない Standby 装置のメンバ ID を指定します。

説明

issu commit コマンドは互換性のあるアップグレード方法の ISSU プロセスの処理中に、Standby（Subordinate）装置（もとのマスタ装置を含みます）をアップグレードします。

複数のシャーシで構成される IRF スタックユニットでは、1 台ずつ Standby 装置をアップグレードします。別の Standby 装置をアップグレードする前に、アップグレードされた Standby 装置が再度起動し、IRF スタックユニットに加入するまで待つ必要があります。すべてのメンバ装置がアップグレードされた後、ISSU は Init 状態に遷移し、ISSU プロセスは完了します。ロールバックすることができません。

1 台の装置のみで構成される IRF スタックユニットでは、**issu commit** コマンドは ISSU プロセスを完了させます。**issu commit** コマンドが完了したとき、ISSU は Init 状態に遷移し、ISSU プロセスは完了します。ロールバックすることができません。

再起動時、Standby 装置は自動でマスタ装置の設定と状態データの同期化を行います。Standby 装置で **issu commit** コマンドを使用する前に同期化が完了するまで待つ必要があります。同期化の状況を確認する場合、**display device** コマンドを使用します。すべてのメンバ装置が正常な状態である場合、同期化は完了しています。

例

メンバ 2 をアップグレードし、新しいマスタ装置になったのち、もとのマスタ装置（メンバ 3）とほかのアップグレードされていない Standby 装置（メンバ 4、メンバ 1）をアップグレードします。

<Switch> issu commit slot 3

```
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version           New Version
  Test 0001015              Test 0001016

  Slot                    Upgrade Way
  3                       Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

<Switch> issu commit slot 4

```
Verifying the file flash:/feature1.bin on slot 4.............Done.
Copying file flash:/feature1.bin to slot4#flash:/feature1.bin...Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version           New Version
  Test 0001015              Test 0001016

  Slot                    Upgrade Way
  4                       Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

<Switch> issu commit slot 1

```
Verifying the file flash:/feature1.bin on slot 1.............Done.
Copying file flash:/feature1.bin to slot1#flash:/feature1.bin...Done.
Upgrade summary according to following table:
```

```
flash:/feature1.bin
  Running Version           New Version
  Test 0001015              Test 0001016

  Slot                     Upgrade Way
  1                       Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

フィールドの説明は表 9-2 を参照してください。

関連コマンド

- **issu accept**
- **issu load**
- **issu run switchover**

9.1.6 issu load

Syntax

issu load file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number*&<1-9>

issu load file ipe *ipe-filename* **slot** *slot-number*&<1-9>

View

User view

定義済みユーザロール

network-admin

パラメータ

boot: ブートファイルを指定します。

system: システムファイルを指定します。

feature: 最大 30 個の feature イメージファイルのスペース区切りリストを指定します。

filename: *filesystemname/filename***.bin** 形式の“.bin”ファイルを指定します。ファイルは、装置上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。ファイルシステムの場所セクションがある場合は、それを除いた値の文字列は最大 63 文字です。ファイルの指定の詳細については、オペレーションマニュアルのセクション 1 *はじめに* "*ファイルシステム管理*"を参照してください。

ipe-filename: *filesystemname/filename***.ipe** の形式で“.ipe”ファイルを指定します。ファイルは、装置上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。ファイルシステムの場所セクションがある場合は、それを除いた値の文字列は最大 63 文

字です。ファイルの指定の詳細については、オペレーションマニュアルのセクション 1 *はじめに* "*ファイルシステム管理*"を参照してください。

slot *slot-number*: Standby 装置のメンバ ID を指定します。互換性のあるアップグレード方法では 1 つのメンバ ID のみ指定することができます。互換性のないアップグレード方法では空白で区切り、最大 3 つのメンバ ID を指定することができます。IRF スタックユニットが 1 つのメンバ装置のみで構成されている場合、IRF スタックユニット全体をアップグレードするため 1 つのメンバ装置のメンバ ID を指定します。

説明

issu load コマンドは下位メンバのソフトウェアイメージをアップグレードし、それらのメンバのメインスタートアップソフトウェアイメージとして新しいイメージを設定します。

ソフトウェアイメージの全部または一部をアップグレードすることができます。一部のイメージのみをアップグレードする場合は、新しいイメージがアップグレード対象外のイメージと互換性があることを確認してください。競合が存在する場合、アップグレードは失敗します。

issu load コマンドは以下の動作を実行します。

- バージョンの互換性を確認します。
- アップグレード方法を識別します。
- メンバ装置をアップグレードするための新しいイメージをロードします。
- アップグレードが再起動後も存続できるように、新しいスタートアップイメージをメインのスタートアップソフトウェアイメージとして設定します。

再起動時に、下位装置は自動的にマスタ装置の設定とステータスデータを同期します。下位装置で **issu load** コマンドを使用する前に、同期が完了するのを待つ必要があります。同期が完了したかどうかを確認するには、**display system stable state** コマンドを使用します。**System State** フィールドに **Stable** と表示されれば、同期は完了です。

ISSU アップグレード方法の詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*ISSU*”を参照してください。

例

メンバ装置 1（下位メンバ）を system イメージファイル **flash:/ soft-system-V714.bin**、boot イメージファイル **flash : / soft-boot-V714.bin**、および feature イメージファイル **soft-freeradius-V714.bin** でアップグレードします。この例では、イメージは実行中のイメージと互換性があります。

<Switch> issu load file boot flash:/soft-boot-V714.bin system flash:/soft-system-V714.bin feature flash:/soft-freeradius-V714.bin slot 1

```
This operation will delete the rollback point information for the previous upgrade
and maybe get unsaved configuration lost. Continue? [Y/N]:y
Verifying the file flash:/soft-freeradius-V714.bin on slot 1...Done.
Verifying the file flash:/soft-boot-V714.bin on slot 1...Done.
Verifying the file flash:/soft-system-V714.bin on slot 1........Done.
```

```
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/soft-boot-V714.bin
  Running Version           New Version
  7.1.3                    7.1.4

flash:/soft-system-V714.bin
  Running Version           New Version
  7.1.3                    7.1.4

flash:/soft-freeradius-V714.bin
  Running Version           New Version
  7.1.3                    7.1.4

  Slot                     Upgrade Way
  1                       Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait.....
```

表 9-3 コマンド出力

フィールド	説明
Verifying the file	システムはファイルの有効性を検証していました。
Copying file	システムはアップグレードファイルを下位メンバにコピーしていました。このフィールドは、コマンドに従属メンバを指定した場合に表示されます。
Upgrade Way	ISSUアップグレード方法です。 • **Service Upgrade**—サービスインクリメントアップグレードです。 • **File Upgrade**—ファイルレベルインクリメントアップグレードです。 • **Reboot**—アップグレードを完了させるため、全装置の再起動が必要です。 ISSUアップグレード方法の詳細は、オペレーションマニュアルのセクション1 *はじめに* “*ISSU*”を参照してください。

🕮 **メモ：**

ISSU でソフトウェアをアップグレードする場合、boot パッケージと system パッケージのみをアップグレードすることはできません。同時に Freeradius パッケージをアップグレードする必要があります。**issu load file boot** *filename* **system** *filename* **feature** *filename* **slot** *slot-number* コマンドを使用してください。
QX-S5300G シリーズは、Radius サーバ機能をサポートしていません。

9.1.7 issu rollback

Syntax

issu rollback

View

User view

定義済みユーザロール

network-admin

説明

issu rollback コマンドは ISSU を中断し、もとのソフトウェアバージョンにロールバックします。

装置は自動ロールバックと手動のロールバックをサポートします。**issu rollback** コマンドは手動でロールバックを行います。

ISSU が以下のいずれかの状態の場合、手動でロールバックを行うことができます。

- **Loaded**－**issu load** コマンドが完了しました。
- **Switching**－(互換性のあるアップグレード方法を行っている間)、システムは **issu run switchover** コマンドを実行しています。
- **Switchover**－(互換性のあるアップグレード方法を行っている間)、**issu run switchover** コマンドが完了しました。
- **Accepted**－**issu accept** コマンドが完了しました。

Switching 状態では、再起動アップグレード中のロールバックと互換性のないアップグレード中の自動ロールバックにより、次の状況が発生する可能性があります。

- アップグレードされた下位メンバが再起動します。
- マスタ/メンバの切り替えが原因でマスタが再起動し、サービスが停止することもあります。
- ロールバック後、メンバ装置はアップグレード前に実行していたソフトウェアを実行しますが、それらのマスタ/下位ロールは以前と同じではない可能性があります。

十分に長い自動ロールバックタイマを指定し、ISSU が Switching 状態の間はロールバックを実行しないでください。

例

もとのソフトウェアバージョンにロールバックします。

<Switch> issu rollback

```
This command will quit the ISSU process and roll back to the previous version.
Continue? [Y/N]:y
```

関連コマンド

- **issu accept**
- **issu commit**
- **issu load**
- **issu run switchover**

9.1.8 issu rollback-timer

Syntax

issu rollback-timer *minutes*

undo issu rollback-timer

デフォルト

45 分

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes: 自動ロールバックタイマの間隔を指定します。設定範囲は 0～120 分です。0 分に指定すると自動ロールバックを無効にします。

説明

issu rollback-timer コマンドは自動ロールバックタイマを設定します。

undo issu rollback-timer コマンドはデフォルトに戻します。

自動ソフトウェアバージョンのロールバックは、互換性のあるアップグレード方法を用い、複数の装置から構成される IRF スタックユニットでのみ有効です。

自動ロールバックがサポートされる状態で、**issu run switchover** コマンドを実行したとき、自動ロールバックタイマが開始します。タイマが終了する前に **issu accept** コマンドあるいは **issu commit** コマンドを実行しない場合、システムは ISSU を行う前に自動でソフトウェアバージョンをロールバックします。

ISSU プロセスの処理中に、自動ロールバックタイマの変更が行われても、ISSU プロセスを処理しているプロセスには適用されません。

例

自動ロールバックタイマを 50 分に設定します。

<Switch> system-view

[Switch] issu rollback-timer 50

関連コマンド

issu rollback

9.1.9 issu run switchover

Syntax

issu run switchover

View

User view

定義済みユーザロール

network-admin

説明

issu run switchover コマンドはマスタ/メンバの切り替えを実行します。アップグレードを行う前のソフトウェアバージョンとアップグレード後のソフトウェアバージョンで互換性がない場合、**issu run switchover** コマンドは、まだアップグレードされていないすべてのメンバをアップグレードします。

issu run switchoverコマンドは複数の装置から構成される IRF スタックユニットで有効です。

- 互換性のあるアップグレード方法の場合、**issu run switchover** コマンドは ISSU アップグレード方法に依存した動作を実行します。
  - **インクリメントアップグレード**－プロセスレベルのマスタ/メンバの切り替えを実行します。
  - **リブートアップグレード**－古いソフトウェアで動作する現在のマスタをリブートします。その結果、アップグレードされた Standby 装置が新しいマスタとして選択されます。
- 互換性のないアップグレード方法の場合、**issu load** コマンドは IRF スタックユニットを 2 つの IRF スタックユニットに分割します。アップグレードされたメンバは新しい IRF スタックユニットを形成します。コマンドは古い IRF スタックユニットのメンバをアップグレードイメージで再起動します。起動後、メンバは Standby 装置として新しい IRF スタックユニットに加入します。

再起動時、Standby 装置は自動でマスタ装置の設定と状態データの同期化を行います。Standby 装置で **issu run switchover** コマンドを使用する前に同期化が完了するまで待つ必要があります。同期化の状況を確認する場合、**display device** コマンドを使用します。すべてのメンバ装置が正常な状態である場合、同期化は完了しています。

例

複数の装置から構成される IRF スタックユニットで、ISSU 中に互換バージョンへのマスタ/メンバを実行します。

<Switch> issu run switchover

```
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version           New Version
  Test 0001015              Test 0001016

  Slot                     Switchover Way
  1                       Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

複数の装置から構成される IRF スタックユニットで、マスタ/メンバの切り替えを実行し、ISSU 中にアップグレードされていないメンバ（メンバ 1 とメンバ 2）を互換性のないバージョンにアップグレードします。

<Switch> issu run switchover

```
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version           New Version
  Test 0001015              Test 0001016

  Slot                     Upgrade Way
  1                       Reboot
  2                       Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

表 9-4 コマンド出力

フィールド	説明
Switchover Way	切り替え方法です。 ● **Active standby process switchover**—アクティブプロセスからStandbyプロセスに切り替えます。 ● **Master subordinate switchover**—マスタからStandbyに切り替えます。

ほかのフィールドについては表 9-2 を参照してください。

関連コマンド

issu load

目次

このセクションのページは **1-x-x** です。

10 章 装置管理 10-1
10.1 装置管理設定コマンド 10-1
10.1.1 clock datetime 10-1
10.1.2 clock protocol 10-2
10.1.3 clock summer-time 10-3
10.1.4 clock timezone 10-5
10.1.5 command 10-6
10.1.6 copyright-info enable 10-7
10.1.7 display clock 10-8
10.1.8 display cpu-usage 10-9
10.1.9 display cpu-usage configuration 10-10
10.1.10 display cpu-usage history 10-11
10.1.11 display device 10-13
10.1.12 display device manuinfo 10-14
10.1.13 display diagnostic-information 10-15
10.1.14 display environment 10-17
10.1.15 display fan 10-19
10.1.16 display memory 10-20
10.1.17 display memory-threshold 10-22
10.1.18 display power 10-23
10.1.19 display scheduler job 10-25
10.1.20 display scheduler logfile 10-26
10.1.21 display scheduler reboot 10-27
10.1.22 display scheduler schedule 10-28
10.1.23 display transceiver interface 10-29
10.1.24 display version 10-30
10.1.25 dying-gasp host 10-31
10.1.26 dying-gasp source 10-33
10.1.27 fan prefer-direction 10-34
10.1.28 header 10-35
10.1.29 job 10-36
10.1.30 memory-threshold 10-37
10.1.31 monitor cpu-usage enable 10-38
10.1.32 monitor cpu-usage interval 10-39
10.1.33 monitor cpu-usage threshold 10-40
10.1.34 monitor resend cpu-usage 10-41

10.1.35 monitor resend memory-threshold 10-43
10.1.36 parity-error monitor log enable 10-44
10.1.37 parity-error monitor period 10-45
10.1.38 parity-error monitor threshold 10-46
10.1.39 password-recovery enable 10-46
10.1.40 reboot 10-47
10.1.41 reset scheduler logfile 10-49
10.1.42 resource-monitor minor resend enable 10-50
10.1.43 resource-monitor output 10-50
10.1.44 resource-monitor resource 10-52
10.1.45 scheduler job 10-54
10.1.46 scheduler logfile size 10-55
10.1.47 scheduler reboot at 10-56
10.1.48 scheduler reboot delay 10-57
10.1.49 scheduler schedule 10-58
10.1.50 shutdown-interval 10-59
10.1.51 sysname 10-60
10.1.52 temperature-limit 10-61
10.1.53 time at 10-62
10.1.54 time once 10-63
10.1.55 time repeating 10-65
10.1.56 usb disable 10-67
10.1.57 user-role 10-67

10章 装置管理

10.1 装置管理設定コマンド

10.1.1 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。

正しいシステム時間は、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、システム時刻を正しく設定する必要があります。

装置がローカルシステム時刻を使用するには、**clock protocol none** コマンドとこのコマンドを順番に実行します。指定したシステム時刻がただちに有効になります。その後、装置は内蔵の水晶発振器によって生成されたクロック信号を使用してシステム時間を維持します。

装置の電源を入れ直すと、ローカルシステムの時刻がデフォルトに戻ります。装置の電源を入れ直した後、このコマンドを再度実行してローカルシステムの時刻を設定する必要があります。

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**

10.1.2 clock protocol

Syntax

clock protocol { **none** | **ntp** }

undo clock protocol

デフォルト

NTP から UTC 時刻を取得します。

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 を使用して UTC 時刻を取得します。NTP を正しく設定する必要があります。

NTP の詳細は、オペレーションマニュアルのセクション 11 *システム管理 “NTP”* を参照してください。

説明

clock protocol コマンドはシステムクロックソースを指定します。

undo clock protocol コマンドはデフォルトに戻します。

正しいシステム時間は、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、システム時刻を正しく設定する必要があります。

装置はローカルに設定されたシステム時間を使用するか、またはネットワーク上のタイムソースから UTC 時間を取得してシステム時間を計算できます。

clock protocol none コマンドを設定した場合、装置はローカルに設定されたシステム時間を使用します。装置は内蔵の水晶発振器で生成されたクロック信号を使用してシステム時間を維持します。

clock protocol ntp コマンドを設定すると、装置は NTP を介して UTC 時刻を取得し、システム時刻を計算します。その後、装置は UTC 時間を定期的に同期させてシステム時間を再計算します。

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

10.1.3 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。

正しいシステム時間は、ネットワーク管理と通信に不可欠です。装置をネットワークで実行する前に、システム時刻を正しく設定する必要があります。

サマータイムを設定した後、装置はシステム時間を再計算します。システム時間を表示するには、**display clock** コマンドを使用します。

ネットワーク上のすべての装置がローカルタイムと同じ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**

10.1.4 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、小文字が区別されます。

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。

正しいシステム時間は、ネットワーク管理と通信に不可欠です。装置をネットワーク上で実行する前に、システム時刻を正しく設定する必要があります。

タイムゾーンを設定した後、装置はシステム時間を再計算します。システム時間を表示するには、**display clock** コマンドを使用します。

ネットワーク上のすべての装置がローカルタイムと同じ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**

10.1.5 command

Syntax

command *id command*

undo command *id*

デフォルト

設定なし

View

job view

定義済みユーザロール

network-admin

パラメータ

id: コマンドの ID を指定します。設定範囲は 0～4294967295 です。コマンドの ID は job を一意に識別します。job のコマンドは昇順で実行されます。

command: job に割り当てられたコマンドを指定します。

説明

command コマンドは job にコマンドを割り当てます。

undo command コマンドは取り消します。

コマンド（command A）を job に割り当てるには、最初にその job に command A の view に移行するためのコマンドを割り当てる必要があります。

デフォルトのコマンドの ID を別のコマンドに指定した場合は、デフォルトのコマンドが置き換えられます。

スケジュール内のすべてのコマンドがコマンド Syntax に準拠していることを確認してください。コマンドを job に割り当てると、システムは Syntax を調べません。

コマンドが「はい」または「いいえ」の回答を必要とする場合、システムは常に **Y** または **Yes** が入力されたと見なします。コマンドが文字列入力を必要とする場合、システムはデフォルト文字列（もしあれば）または null が入力されたと見なします。

job に **telnet**、**ftp**、**ssh2**、または **monitor process** コマンドを含めることはできません。

例

backupconfig の job にコマンドを割り当てて、TFTP サーバ 192.168.100.11 に startup.cfg ファイルをバックアップします。

<Switch> system-view

[Switch] scheduler job backupconfig

[Switch-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg backup.cfg

GigabitEthernet 1/0/1.をシャットダウンするために、**shutdownGE** job にコマンドを割り当てます。

<Switch> system-view

[Switch] scheduler job shutdownGE

[Switch-job-shutdownGE] command 1 system-view

[Switch-job-shutdownGE] command 2 interface gigabitethernet 1/0/1

[Switch-job-shutdownGE] command 3 shutdown

関連コマンド

scheduler job

10.1.6 copyright-info enable

Syntax

copyright-info enable

undo copyright-info enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

copyright-info enable コマンドは著作権情報の表示を有効にします。

undo copyright-info enable コマンドは著作権情報の表示を無効にします。

10.1.7 display clock

Syntax

display clock

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display clock コマンドはシステムの現在時刻、日付、タイムゾーン、サマータイムを表示します。

例

ローカルタイムゾーンが指定されていないとき、システム時間を表示します。

<Switch> display clock

```
10:09:00.258 UTC Fri 03/16/2015
```

時間は hour:minute:second.milliseconds 形式です。

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

```
15:10:00.152 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

```
15:11:00.211 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

関連コマンド

- **clock datetime**
- **clock timezone**
- **clock summer-time**

10.1.8 display cpu-usage

Syntax

display cpu-usage [**slot** *slot-number* [**cpu** *cpu-number*]]

display cpu-usage [**control-plane** | **data-plane**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

control-plane: コントロールプレーンの CPU 使用率統計情報を表示します。**control-plane** または **data-plane** を指定しないと、CPU 使用率の合計統計情報が表示されます。

data-plane: データプレーンの CPU 使用率統計情報を表示します。**data-plane** または **control-plane** を指定しないと、CPU 使用率の合計統計情報が表示されます。

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのオプションが指定されない場合、すべての IRF スタックのメンバ装置の CPU 使用率の統計情報を表示します。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 でなければなりません。

重要:

- **control-plane** または **data-plane** を指定しない場合、コマンドは CPU 使用率の合計統計情報を表示します。
- CPU 使用率の合計統計情報の最大値は 100%です。
- コントロールプレーンが 45%、データプレーンが 5%の場合、CPU 使用率の合計統計情報は 25%です。

説明

display cpu-usage コマンドは現在の CPU 使用率の統計情報を表示します。

起動後、装置は以下の間隔で CPU 使用率の平均を記録します。

- 5 秒
- 1 分
- 5 分

このコマンドは、最後の 5 秒、1 分、5 分間における平均の CPU 使用率の統計情報を表示します。

例

現在の CPU 使用率の統計をテキスト形式で表示します。

<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
```

現在の CPU 使用率の統計を表形式で表示します。

<Switch> display cpu-usage

```
Slot CPU       Last 5 sec       Last 1 min       Last 5 min
1    0         17%              29%              28%
```

表 10-1 コマンド出力

フィールド	説明
% in last 5 seconds Last 5 sec	最後の5秒のCPUまたはCPUコア使用率の平均です。
% in last 1 minute Last 1 min	最後の1分のCPUまたはCPUコア使用率の平均です。
% in last 5 minutes Last 5 min	最後の5分のCPUまたはCPUコア使用率の平均です。

10.1.9 display cpu-usage configuration

Syntax

display cpu-usage configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置の CPU 使用率監視設定を表示します。

cpu *cpu-number*: CPU を番号で指定します。*cpu-number* は 0 でなければなりません。

説明

display cpu-usage configuration コマンドは CPU 使用率モニタリング設定を表示します。

例

CPU 使用率モニタリング設定を表示します。

<Switch> display cpu-usage configuration

```
CPU usage monitor is enabled.
Current monitor interval is 60 seconds.
Current severe alarm threshold is 90%.
Current minor alarm threshold is 80%.
Current recovery-threshold is 40%.
```

関連コマンド

- **monitor cpu-usage enable**
- **monitor cpu-usage interval**
- **monitor cpu-usage threshold**

10.1.10 display cpu-usage history

Syntax

display cpu-usage history [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job *job-id*:プロセスを ID で指定します。*job-id* の値の範囲は 1 から 2147483647 です。プロセスを指定しない場合、このコマンドはシステム全体の CPU 使用率（全プロセスの合計 CPU 使用率）の統計を表示します。実行中のプロセスの ID と名前を表示するには、**display process** コマンドを使用します。詳細については、オペレーションマニュアルのセクション 11 *システム管理* を参照してください。

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。プロセスを指定してメンバ装置を指定しない場合、このコマンドは Master 装置のプロセスの統計情報を表示します。オプションを指定しなかった場合、このコマンドはすべてのメンバ装置上のすべてのプロセスの統計情報を表示します。

cpu *cpu-number*: CPU を番号で指定します。*cpu-number* は 0 でなければなりません。プロセスを指定して CPU を指定しない場合、このコマンドはデフォルト CPU の統計を表示します。プロセスまたは CPU を指定しないと、このコマンドはすべての CPU の履歴統計を表示します。

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を有効にすると、システムは定期的に CPU 使用率をサンプリングし、そのサンプルを履歴レコードバッファに保存します。このコマンドでは、座標系の最新の 60 サンプルが次のように表示されます。

縦軸は CPU 使用率を表します。統計が使用率のステップの倍数でない場合は、最も近い使用率のステップの倍数に切り上げまたは切り下げられます。たとえば、CPU 使用率のステップが 5%の場合、統計値 53%は 55%に切り上げられ、統計値 52%は 50%に切り捨てられます。

横軸は時間を表します。

シャープ記号(#)は CPU 使用率を示します。特定の時間における一番上のポンド記号の縦軸の値は、その時間の CPU 使用率を表します。

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)
```

出力は最後の 60 分間の全システムの CPU 使用率を示します。システム名は SYSTEM です。

出力には次の項目が表示されます。

プロセス名。**SYSTEM** という名前は、システム全体を表します。

プロセスを保持している CPU：スロット 1 の CPU 0。

過去 60 分間のシステム全体の CPU 使用率統計情報の履歴です。

- 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**

10.1.11 display device

Syntax

display device [**usb**] [**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

usb: USB インタフェースに接続する機器を指定します。

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の情報を表示します。

verbose : 詳細なハードウェア情報を表示します。このキーワードがない場合、概要情報を表示し、ファイアウォールカードの情報を表示しません。

説明

display device コマンドは装置情報を表示します。

usb キーワードを指定しない場合は、このコマンドはメンバ装置に関する情報を表示します。

例

装置情報を表示します。

<Switch> display device

```
Slot 1
Slot Type            State    Subslot  Soft Ver           Patch Ver
1    QX-S5328GT-4X2Q Master   1       1115              None
```

表 10-2 コマンド出力

フィールド	説明
Type	装置のタイプです。
State	IRFスタックユニットにおける装置の役割です。 **Master**–装置はマスタです。 **Standby**–装置は下位メンバです。
Soft Ver	ソフトウェアバージョンです。
Patch Ver	装置のパッチバージョン。パッチがインストールされていない場合、このフィールドには**None**と表示されます。

10.1.12 display device manuinfo

Syntax

display device manuinfo [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのオプションが指定されない場合、すべての IRF スタックユニットのラベル情報を表示します。

説明

display device manuinfo コマンドは装置のラベル情報を表示します。

ラベル情報は、固定構成データまたはアーカイブ情報とも呼ばれており、デバック中あるいはテスト中に装置の記憶媒体に書き込まれます。ベンダ名、装置のシリアル番号、製造日、MAC アドレス、装置の名前を含む情報です。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

装置のラベル情報を表示します。

<Switch> display device manuinfo

...

10.1.13 display diagnostic-information

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **service**] [*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

hardware: ハードウェア関連の稼働情報を指定します。

infrastructure: 基本機能の運用情報を指定します。

l2: レイヤ 2 機能の運用情報を指定します。

service: レイヤ 4 および上位レイヤ機能の動作情報を指定します。

filename : 情報をファイルに保存します。*filename* には、拡張子**.tar.gz** を使用する必要があります。指定しない場合、情報をファイルに保存するか、情報を表示するかを選択するようにプロンプトが出されます。

説明

display diagnostic-information コマンドは機能およびハードウェアモジュールの操作情報を表示または保存します。

次のいずれかの方法を使用して、診断とトラブルシューティングのために稼働統計を収集できます。

- 機能ごとまたはモジュールごとに機能情報を収集するには、別々の表示コマンドを使用します。
- **display diagnostic-information** コマンドを使用して、複数またはすべての機能とハードウェアモジュールの動作情報を収集します。

記憶域を節約するために、このコマンドは情報をファイルに保存する前に自動的に情報を圧縮します。

1) **tar extract** コマンドを使用してファイルを抽出します。
2) **gunzip** コマンドを使用して、抽出したファイルを解凍します。
3) **more** コマンドを使用して、解凍されたファイルの内容を表示します。

display diagnostic-information コマンドを中止した場合、**gunzip** コマンドは抽出ファイルを解凍できない可能性があります。抽出されたファイルを解凍するには、Linux を実行している PC に抽出されたファイルをエクスポートし、**gunzip-c** コマンドを使用します。

コマンドにファイル名を指定しないと、情報を表示するか保存するかを選択するようにプロンプトが出されます。情報を保存することを選択した場合、システムは自動的にファイル名を割り当て、そのファイル名を大括弧内に表示します。ファイル名の一意性のために、ファイル名には装置名と現在のシステム時刻が含まれています。

装置名に次のいずれかの特殊文字が含まれている場合、スラッシュ(/)、バックスラッシュ、コロン(:)、アスタリスク(*)、疑問符(?)、小なり記号(<)、大なり記号(>)、パイプライン記号(|)、および引用符(")です。例えば、装置名 **A/B** はファイル名の **A_B** に変わります。**flash:/diag_A_B_20160101-000438.tar.gz.**

機能パラメータを指定しない場合、このコマンドはすべての機能とモジュールの動作情報を表示または保存します。

このコマンドは、|、**>**、および**>>**オプションをサポートしません。

装置がこのコマンドを実行している間は、他のコマンドを実行しないでください。他のコマンドを実行すると、収集した運用情報に影響を与える可能性があります。

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===============
...
```

運用情報をデフォルトファイルに保存します。

<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_
Switch_20160101-024601.tar.gz]:
Diagnostic information is outputting to flash:/diag_
Switch_20160101-024601.tar.gz.
Please wait...
Save successfully.
```

ファイル名を入力するように求められたら、**Enter** キーを押します。

test.tar.gz にすべての機能とモジュールの操作情報を保存してください。

<Switch> display diagnostic-information test.tar.gz

```
Diagnostic information is outputting to flash:/test.tar.gz.
Please wait...
Save successfully.
```

関連コマンド

- **gunzip**
- **more**
- **tar extract**

10.1.14 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*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の温度情報を表示します。

説明

display environment コマンドは装置の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 31           0      63       68     NA
 1     hotspot 2 0            0      110      130    137
```

表 10-3 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	ホットスポットに固定されている温度センサです。
Slot	センサ位置です
Temperature	現在の温度です。
Lower	下限温度です。装置がこのフィールドをサポートしていない場合、このフィールドには**NA**が表示されます。
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、このフィールドには**NA**が表示されます。
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、このフィールドには**NA**が表示されます。
Shutdown	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、このフィールドには**NA**が表示されます。

10.1.15 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*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置のファントレイの動作ステータス情報を表示します。

fan-id: ファントレイを ID で指定します。ファントレイを指定しない場合、このコマンドは指定された位置にあるすべてのファントレイの動作ステータス情報を表示します。

説明

display fan コマンドはファントレイの動作ステータス情報を表示します。

例

#すべてのファントレイの動作状態を表示します。

<Switch> display fan

```
Slot 1:
Fan 1:
State    : Normal
Airflow Direction: Port-to-power
Prefer Airflow Direction: Port-to-power
```

表 10-4 コマンド出力

フィールド	説明
Slot 1	メンバ装置の番号です。
Fan 1	ファントレイの番号です。

フィールド	説明
State	ファンの稼働状態を示します。 • **Absent**–スロットにはファントレイが取り付けられていません。 • **Fault**–ファンに問題があります。 • **Normal**–ファンが正常に動作しています。 • **FanDirectionFault**–実際のエアーフロー方向は推奨方向ではありません。
Airflow Direction	現在のファンの風向きを示します。 • **Port-to-power**–ポート側から電源側へ。 • **Power-to-port**–電源側からポート側へ。
Prefer Airflow Direction	好ましい風向きを示します。 • **Port-to-power**–ポート側から電源側へ。 • **Power-to-port**–電源側からポート側へ。

10.1.16 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*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置のメモリ使用量を表示します。

cpu *cpu-number*: CPU を番号で指定します。*cpu-number* は 0 でなければなりません。

説明

display memory コマンドは装置のメモリ使用量を表示します。

例

メモリ使用量を表示します。

<Switch> display memory

```
Memory statistics are measured in KB:
Slot 1:
           Total     Used     Free    Shared   Buffers    Cached   FreeRatio
Mem:      2036536   496116  1540420        0     1436    113644      75.7%
-/+ Buffers/Cache:   381036  1655500
Swap:           0        0        0
LowMem:   1651512   279856  1371656       --       --       --      83.1%
HighMem:   385024   216260   168764       --       --       --      43.8%
```

表 10-5 コマンド出力

フィールド	説明
Mem	メモリ使用量です。
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、カーネル管理およびISSU機能にのみ使用されます。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。 このフィールドがサポートされていない場合は、2つのハイフン(--)が表示されます。
Buffers	バッファで使用されている物理メモリです。 このフィールドがサポートされていない場合は、2つのハイフン(--)が表示されます。
Cached Caches	キャッシュで使用されている物理メモリです。 このフィールドがサポートされていない場合は、2つのハイフン(--)が表示されます。
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。

フィールド	説明
LowMem	メモリ使用量の少ない情報です。
HighMem	メモリ使用量の多い情報です。

10.1.17 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*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置のメモリ使用量しきい値と統計情報を表示します。

cpu *cpu-number*: CPU を番号で指定します。*cpu-number* は 0 でなければなりません。

説明

display memory-threshold コマンドはメモリアラームのしきい値と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 または **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 thresholds:
   Minor: 96M
   Severe: 64M
   Critical: 48M
   Normal: 128M
   Early-warning: 192M
   Secure: 304M
```

```
Current free-memory state: Normal (secure)
Free-memory event statistics:
 [Back to secure state]
   First notification: 0.0
   Latest notification: 0.0
   Total number of notifications sent: 0
 [Entered early-warning state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Back to normal state]
   First notification: 0.0
   Latest notification: 0.0
   Total number of notifications sent: 0
 [Entered minor alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Back to minor alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Entered severe alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Back to severe alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Entered critical alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
```

10.1.18 display power

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*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の電源ユニット情報を表示します。

power-id: 電源ユニットを ID で指定します。このオプションを指定しない場合、指定されたメンバ装置の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       Absent   --       --          --          --
 2       Normal   AC       --          --          --
```

表 10-6 コマンド出力

フィールド	説明
PowerID	電源ユニットIDです。
State	電源ユニットのステータスです。 • **Absent**–スロットに電源ユニットが取り付けられていません。 • **Fault**–電源ユニットに障害があります。 • **Normal**–電源ユニットは正常に動作しています。
Mode	電源のモードです • **AC**–AC電源ユニット • **DC**–DC電源ユニット
Current(A)	電源ユニットの出力電流（アンペア単位）です。 このフィールドは未サポートです。

フィールド	説明
Voltage(V)	電源ユニットの出力電圧（ボルト単位）です。 このフィールドは未サポートです。
Power(W)	電源ユニットの出力電力（ワット単位）です。 このフィールドは未サポートです。

10.1.19 display scheduler job

Syntax

display scheduler job [*job-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job-name: job の名前を指定します。設定範囲は 1～47 文字で、大文字、小文字を区別します。このオプションを指定しない場合、すべての job の設定情報を表示します。

説明

display scheduler job コマンドはスケジュール自動実行機能の job の設定情報を表示します。

例

すべての job の設定情報を表示します。

<Switch> display scheduler job

```
Job name: saveconfig
 copy startup.cfg backup.cfg

Job name: backupconfig

Job name: creat-VLAN100
 system-view
 vlan 100
```

// 出力では、装置は 3 つの job があることを示します。最初のジョブには 1 つのコマンドがあります。2 番目の job にはコマンドがありません。3 番目の job には 2 つのコマンドがあります。job は空白行で区切られます。

10.1.20 display scheduler logfile

Syntax

display scheduler logfile

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display scheduler logfile コマンドはスケジュール自動実行機能の実行された job のログ情報を表示します。

例

実行された job のログ情報を表示します。

<Switch> display scheduler logfile

```
Logfile Size: 1902 Bytes.

Job name       : shutdown
Schedule name   : shutdown
Execution time  : Tue Dec 27 10:44:42 2015
Completion time : Tue Dec 27 10:44:47 2015
---------------------------------                  Job                    output
-----------------------------------
```

<Switch>system-view

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

[Switch]interface rang gigabitethernet 1/0/1 to gigabitethernet 1/0/3

[Switch-if-range]shutdown

表 10-7 コマンド出力

フィールド	説明
Logfile Size	ログファイルのサイズです。byteで表示されます。
Schedule name	jobが所属するスケジュールです。
Execution time	jobが開始されたときの時間です。

フィールド	説明
Completion time	jobが完了したときの時間です。jobが実行されなかった、あるいはjobにコマンドがない場合、このフィールドは表示されません。
Job output	jobのコマンドと出力です。

関連コマンド

reset scheduler logfile

10.1.21 display scheduler reboot

Syntax

display scheduler reboot

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display scheduler reboot コマンドはスケジュール再起動機能のユーザが設定した装置の再起動時刻を表示します。

例

装置の再起動時刻を表示します。

<Switch> display scheduler reboot

```
System will reboot at 16:32:00 05/23/2015 (in 1 hours and 39 minutes).
```

関連コマンド

- **scheduler reboot at**
- **scheduler reboot delay**

10.1.22 display scheduler schedule

Syntax

display scheduler schedule [*schedule-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

schedule-name: スケジュール名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。このオプションが指定されない場合、すべてのスケジュールの情報を表示します。

説明

display scheduler schedule コマンドはスケジュール自動実行機能のスケジュール情報を表示します。

例

すべてのスケジュールの情報を表示します。

<Switch> display scheduler schedule

```
Schedule name       : shutdown
Schedule type       : Run once after 0 hours 2 minutes
Start time         : Tue Dec 27 10:44:42 2015
Last execution time  : Tue Dec 27 10:44:42 2015
Last completion time : Tue Dec 27 10:44:47 2015
Execution counts    : 1
------------------------------------------------------------------------
Job name                                    Last execution status
shutdown                                    Successful
```

表 10-8 コマンド出力

フィールド	説明
Schedule type	スケジュールが実行される時間です。実行時間が指定されていない場合、このフィールドは表示されません。
Start time	初回にスケジュールが実行される時間です。実行時間が指定されていない場合、このフィールドは表示されません。

フィールド	説明
Last execution time	スケジュールが実行されたときの最後の時間です。実行時間が指定されていない場合、このフィールドは表示されません。スケジュールが実行されていない場合、"Yet to be executed"と表示されます。
Last completion time	スケジュールが完了した最後の時間です。実行時間が指定されていない場合、このフィールドは表示されません。
Execution counts	スケジュールが実行された回数です。実行時間が指定されていない場合、このフィールドは表示されません。
Job name	スケジュールのjob名です。
Last execution status	最後に実行された結果です。 • **Successful** • **Failed** • **Waiting**–装置はスケジュールを実行し、jobが実行待ちです。 • **In process**–jobが実行されています。 • **-NA**-–実行時間になっていません。 jobのコマンドが実行されたかどうかについての情報および実行結果を表示するには、**display scheduler logfile**コマンドを実行してください。

10.1.23 display transceiver interface

Syntax

display transceiver interface [i*nterface-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。このオプションが指定されない場合、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

インタフェース 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 1/0/1

...

10.1.24 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

...

表 10-9 コマンド出力

フィールド	説明
Last reboot reason	最後の再起動の理由です。 • **User reboot**—再起動は、CLIやSNMPなどのユーザインタフェースから手動で開始されました。 • **Cold reboot**—再起動は電源の再投入が原因でした。 • **Kernel abnormality reboot**—再起動はカーネルの例外が原因でした。 • **DeadLoop reboot**—再起動はカーネルスレッドのデッドループが原因でした。 • **DEV HandShake reboot**—装置管理ハンドシェイクの失敗によるものです。 • **SlaveSwitch reboot**—再起動は、マスタ/下位切り替えが原因で発生しました。 • **IRF Merge reboot**—再起動はIRFマージが原因でした。 • **Auto Update reboot**—再起動はソフトウェアの自動アップグレードによるものです。 • **Memory exhaust reboot**—再起動は、カードメモリ不足のイベントによって発生しました。

10.1.25 dying-gasp host

Syntax

dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **snmp-trap version** { **v1** | **v2c** | **v3** [**authentication** | **privacy**] } **securityname** *security-string*

dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **syslog**

undo dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] { **snmp-trap** | **syslog** }

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：デバイスが電源オフアラームを送信する宛先ホストの IPv4 アドレスを指定します。

ipv6 *ipv6-address*：デバイスが電源オフアラームを送信する宛先ホストの IPv6 アドレスを指定します。

vpn-instance *vpn-instance-name*: 宛先ホストが属する **MPLS L3VPN** インスタンスを指定します。*vpn-instance-name* 引数は VPN インスタンス名を表し、大文字と小文字を区別する 1～31 文字の文字列です。宛先ホストがパブリックネットワークに属する場合は、このオプションを指定しないでください。

snmp-trap: SNMP 通知を使用して電源オフアラームを送信します。

version: SNMP バージョンを指定します。

- **v1**:SNMPv1 を指定
- **v2c**:SNMPv2c を指定
- **v3**:SNMPv3 を指定。もし **authentication** または **privacy** パラメータを指定しない場合、認証または暗号化を実施しません。
  - **authentication**: パケットの認証のみを行う。
  - **privacy**: パケットに対して認証と暗号化の両方を実行する。

securityname *security-string*：SNMPv1 または SNMPv2c のコミュニティ名、または SNMPv3 のユーザー名を、大文字と小文字を区別して 1～32 文字で指定します。

syslog：ログメッセージを使用して電源オフアラームを送信します。

説明

dying-gasp host を使用して、電源オフアラームの宛先ホスト設定を行います。

undo dying-gasp host を使用して、パワーオフアラームの宛先ホスト設定を削除します。

デバイスは、SNMP 通知とログメッセージのいずれか、または両方を使用して電源オフアラームを送信できます。

デバイスは、複数の宛先ホストに同時に電源オフアラームを送信できます。

SNMP v3 トラップでパワーオフアラームを NMS に送信するようにデバイスを設定する場合、SNMP v3 ユーザを作成するために **snmp-agent usm-user** コマンドを実行します。SNMP v3 ユーザが属するグループの認証モードが、**dying-gasp host** コマンドで設定した認証モードと同じであることを確認してください。さらに、認証および暗号化パラメータは、NMS 側で設定されたものと一致している必要があります。これを怠ると、デバイスは SNMP v3 トラップで電源切断アラームを NMS に送信できません。

例

SNMPv1 通知を使用して、1.1.1.1 のホストにパワーオフアラームを送信するように デバイスを設定する場合の例（コミュニティ名は **public** を設定）

<Sysname> system-view

[Sysname] dying-gasp host 1.1.1.1 snmp-trap version v1 securityname public

関連コマンド

dying-gasp source

10.1.26 dying-gasp source

Syntax

dying-gasp source *interface-type* { *interface-number* | *interface-number.subnumber* }

undo dying-gasp source

デフォルト

設定なし

IPv4 ネットワークでは、デバイスは宛先ホストへのルートの出力インタフェースのプライマリ IPv4 アドレスをソースアドレスとして使用します。

IPv6 ネットワークでは、デバイスは RFC 3484 で定義されているソース 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-type {*interface-number* | *interface-number.subnumber*} : レイヤ 3 インタフェースを指定します。

interface-type 引数でインタフェースの種類を指定します。*interface-number* 引数はインタフェース番号を指定します。

subnumber 引数は、サブインタフェース番号を指定し、1 から 4094 の範囲で指定します。

*interface-number.subnumber 引数の*サポートは、デバイス・モデルに依存します。

説明

電源オフアラームの送信元インタフェースを指定するには、**dying-gasp source** を使用します。

デフォルトの状態に戻す場合は **undo dying-gasp** source を使用します。

デバイスは、発信電源オフアラームパケットのソースアドレスとして、指定されたソースインタフェースの IPv6 アドレスまたはプライマリ IPv4 アドレスを使用します。宛先ホストは、このアドレスを使用して、デバイスから受信した SNMP 通知またはログメッセージを識別します。

指定したソースインタフェースにアドレスが設定されていない場合、このコマンドは有効になりません。このコマンドを有効にするには、ソースインタフェースにアドレスを割り当てます。

例

Vlan-interface 1 インタフェースを電源オフアラームの送信元インタフェースとして使用する場合

<Sysname>system-view

[Sysname]dying-gasp source vlan-interface 1

関連コマンド

dying-gasp host

10.1.27 fan prefer-direction

Syntax

fan prefer-direction slot *slot-number* { **port-to-power** | **power-to-port** }

undo fan prefer-direction slot *slot-number*

デフォルト

推奨されるエアーフローの方向は、ポート側から電源側です。

View

System 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。

port-to-power: ポート側から電源装置側へのエアーフローの方向を指定します。

power-to-port: 電源装置側からポート側へのエアーフローの方向を指定します。

説明

fan prefer-direction コマンドは装置の推奨エアーフロー方向を指定します。

undo fan prefer-direction コマンドはデフォルトに戻します。

例

メンバ装置 1 の推奨エアーフロー方向を **port-to-power** に設定します。

<Switch> system-view
[Switch] fan prefer-direction slot 1 port-to-power

関連コマンド

display fan

10.1.28 header

Syntax

header { **legal** | **login** | **motd** | **shel**l } *text*

undo header { **legal** | **login** | **motd** | **shell** }

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

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。2 つの形式で入力できます。詳細はオペレーションマニュアルのセクション 1 *はじめに* “*装置管理*”を参照してください。

説明

header コマンドはバナーを作成します。

undo header コマンドはバナーを削除します。

例

legal バナー、login バナー、MOTD バナー、shell 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%
```

10.1.29 job

Syntax

job *job-name*

undo job *job-name*

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

job-name: job 名を指定します。設定範囲は 1～47 文字で、大文字、小文字を区別します。

説明

job コマンドはスケジュール自動実行機能のスケジュールに job を割り当てます。

undo job コマンドは job を削除します。

スケジュールに複数の job を割り当てることができます。スケジュールの job は連続して実行されます。

スケジュールに割り当てられる job はあらかじめ作成されている必要があります。job を作成する場合、**scheduler job** コマンドを使用します。

例

スケジュール **saveconfig** に job 名が **save-job** の job を割り当てます。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] job save-job

関連コマンド

- **scheduler job**
- **scheduler schedule**

10.1.30 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：96 MB.

Severe：64 MB.

Critical：48 MB.

Normal：128 MB.

View

System view

定義済みユーザロール

network-admin

パラメータ

minor *minor-value*: **minor** アラームしきい値を指定します。このしきい値の値の範囲を表示するには、*minor-value* の代わりに疑問符（？）を入力します。このしきい値を 0 に設定すると、**minor** アラーム機能が無効になります。

severe *severe-value*: **severe** アラームしきい値を指定します。このしきい値の値範囲を表示するには、*severe-value* の代わりに疑問符（？）を入力します。このしきい値を 0 に設定すると、**severe** アラーム機能が無効になります。

critical *critical-value*: **critical** アラームしきい値を指定します。このしきい値の値の範囲を表示するには、*critical-value* 引数の代わりに疑問符（？）を入力してください。このしきい値を 0 に設定すると、**critical** アラーム機能が無効になります。

normal *normal-value*: **normal** アラームのしきい値を指定します。このしきい値の値の範囲を表示するには、normal-value の代わりに疑問符（？）を入力してください。

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置の空きメモリしきい値を設定します。

cpu *cpu-number*: CPU を番号で指定します。*cpu-number* は 0 でなければなりません。

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。

正しい動作を保証し、メモリ効率を向上させるために、システムは空きメモリ容量をリアルタイムでモニタします。空きメモリスペースの量が minor、severe、または critical アラームしきい値以下になると、システムは影響を受けるサービスモジュールまたはプロセスにアラームを発行します。

early-warning は、メモリ不足状態に近づいていることを警告します。

しきい値の詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*装置管理*”を参照してください。

例

minor アラーム、severe アラームクリティカルアラーム、および通常状態のしきい値をそれぞれ 64 MB、48 MB、32 MB、および 96 MB 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

10.1.31 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*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置の CPU 使用率モニタリングを有効にします。

cpu *cpu-number*: CPU を番号で指定します。*cpu-number* は 0 でなければなりません。

説明

monitor cpu-usage enable コマンドは CPU 使用率の監視を有効にします。

undo monitor cpu-usage enable コマンドは CPU 使用率の監視を無効にします

CPU 使用率モニタリングが有効になった後、システムは **monitor cpu-usage interval** コマンドで指定された間隔で CPU 使用率をサンプリングして保存します。**display cpu-usage history** コマンドを使用して、最近の CPU 使用率を表示できます。

例

CPU 使用率の監視を有効にします。

<Switch> system-view

[Switch] monitor cpu-usage enable

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage interval**

10.1.32 monitor cpu-usage interval

Syntax

monitor cpu-usage interval *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage 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 使用率監視のサンプリング間隔を指定します。有効値は、大文字、小文字を区別しません。**5Sec**（5 秒）、**1Min**（1 分）、**5Min**（5 分）です。

slot *slot-number*： IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置の間隔を設定します。

cpu *cpu-number*：CPU を番号で指定します。*cpu-number* は 0 でなければなりません。

説明

monitor cpu-usage interval コマンドは CPU 使用率をモニタするサンプリング間隔を設定します。

undo monitor cpu-usage interval コマンドはデフォルト設定に戻します。

例

CPU 使用率監視のサンプリング間隔を 5 秒に設定します。

<Switch> system-view

[Switch] monitor cpu-usage interval 5Sec

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage enable**

10.1.33 monitor cpu-usage threshold

⚠ **重要:**

- **monitorcpu-usage threshold** コマンドは、CPU 使用率の合計統計情報をチェックします。
- CPU 使用率の合計統計情報の最大値は 100%です。
- コントロールプレーンが 45%、データプレーンが 5%の場合、CPU 使用率の合計統計情報は 25%です。

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

- severe CPU 使用率アラームしきい値は 99%
- minor CPU 使用率アラームしきい値は 80%

- CPU 使用率回復しきい値は 60%

View

System view

定義済みユーザロール

network-admin

パラメータ

severe-threshold : severe CPU 使用率アラームしきい値をパーセントで指定します。設定範囲は 2～100 です。

minor-threshold *minor-threshold* : minor CPU 使用率アラームしきい値をパーセントで指定します。設定範囲は、1～severe CPU 使用率アラームしきい値-1 までです。

recovery-threshold *recovery-threshold*: CPU 使用率回復しきい値をパーセントで指定します。設定範囲は、0～minor CPU 使用率アラームしきい値-1 までです。

slot *slot-number* : IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置の CPU 使用率しきい値を設定します。

cpu *cpu-number*: CPU を番号で指定します。

説明

monitor cpu-usage threshold コマンドは CPU 使用率アラーム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設定に戻します。

装置は 1 分間隔で CPU 使用率をサンプリングします。サンプルが CPU 使用率しきい値よりも大きい場合、装置はトラップを送信します。

例

severe CPU 使用率アラームしきい値を 90%に、minor CPU 使用率アラームしきい値を 80%、CPU 使用率回復しきい値を 70%に設定します。

<Switch> system-view

[Switch] monitor cpu-usage threshold 90 minor-threshold 80 recovery-threshold 70

関連コマンド

display cpu-usage configuration

10.1.34 monitor resend cpu-usage

Syntax

monitor resend cpu-usage { **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend cpu-usage [**minor-interval** | **severe-interval**] [**slot** *slot-number* [**cpu** *cpu-number*]]

デフォルト

minor アラームの再送信間隔は 300 秒です。severe アラームの再送信間隔は 60 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

minor-interval *minor-interval*: minor アラームの再送信間隔を 10～3600 の範囲で 5 の倍数で指定します。（秒単位）

severe-interval *severe-interval*: severe アラームの再送信間隔を 10～3600 の範囲の 5 の倍数で指定します。（秒単位）

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置の CPU 使用率アラームの再送信間隔を設定します。

cpu *cpu-number*: CPU を番号で指定します。

説明

monitor resend cpu-usage コマンドは CPU 使用率アラームの再送信間隔を設定します。

undo monitor resend cpu-usage コマンドはデフォルト設定に戻します。

装置は、定期的に CPU 使用率をサンプリングし、そのサンプルを CPU 使用率のしきい値と比較します。サンプルがアラームしきい値を超えると、CPU 使用率はアラーム状態になり、装置はアラームを送信します。

CPU 使用率が minor アラーム状態にある間、装置は、CPU 使用率が severe しきい値を超えるか、minor アラームが削除されるまで、minor アラームを定期的に送信します。

CPU 使用率が severe アラーム状態にある間、装置は、severe アラームが削除されるまで、定期的に severe アラームを送信します。

このコマンドを使用すると、CPU 使用率アラームの再送間隔を変更できます。

minor-interval または **severe-interval** を指定しない場合、**undo monitor resend cpu-usage** コマンドは、minor アラームと severe アラームの再送信間隔の両方のデフォルト設定を復元します。

例

スロット 1 の CPU0 に対する CPU 使用率 minor アラームの再送間隔を 60 秒に設定します。

<Switch> system-view

[Switch] monitor resend cpu-usage minor-interval 60 slot 1 cpu 0

10.1.35 monitor resend memory-threshold

Syntax

monitor resend memory-threshold { **critical-interval** *critical-interval* | **early-warning-interval** *early-warning-interval* | **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend memory-threshold [**critical-interval** | **early-warning-interval** | **minor-interval** | **severe-interval**] * [**slot** *slot-number* [**cpu** *cpu-number*]]

デフォルト

- Early warning 再送信間隔：1 時間
- Minor アラーム再送信間隔：12 時間。
- Severe アラーム再送信間隔：3 時間
- Critical アラーム再送信間隔：1 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

critical-interval *critical-interval*: **critical** アラームの再送信間隔を指定します。設定範囲は 1～48 です。単位は時間です。

early-warning-interval *early-warning-interval*: **early-warning** の再送間隔を指定します。設定範囲はです。単位は時間です。

minor-interval *minor-interval*: **minor** アラームの再送信間隔を指定します。設定範囲は 1～48 です。単位は時間です。

severe-interval *severe-interval*: **severe** アラームの再送信間隔を指定します。設定範囲は 1～48 です。単位は時間です。

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置のアラーム再送信間隔を設定します。

cpu *cpu-number*: CPU を番号で指定します。

説明

monitor resend memory-threshold コマンドはメモリ不足アラームの再送信間隔を設定します。

undo monitor resend memory-threshold コマンドはデフォルトに戻します。

装置は、定期的に空きメモリ容量をサンプリングし、そのサンプルを空きメモリしきい値と比較します。サンプルがしきい値以下になると、装置はメモリ不足アラーム状態に入り、アラームを送信します。

critical アラーム状態では、装置は critical アラームが削除されるまで定期的に critical アラーム通知を送信します。

低いアラーム状態では、装置は高いアラーム状態になるか、または現在のアラームが削除されるまで、アラーム状態の通知を定期的に送信します。

このコマンドを使用して、アラームの再送間隔を変更できます。

例

スロット 1 の CPU0 の minor メモリ不足アラームの再送間隔を 12 時間に設定します。

<Switch> system-view

[Switch] monitor resend memory-threshold minor-interval 12 slot 1 cpu 0

10.1.36 parity-error monitor log enable

Syntax

parity-error monitor log enable

undo parity-error monitor log 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

parity-error monitor log enable コマンドは転送チップのエントリのパリティエラーログを有効にします。

undo parity-error monitor log enable コマンドは転送チップのエントリのパリティエラーログを無効にします。

パリティエラーログ機能は、検出されたパリティエラーのログを生成します。

例

パリティエラーログ機能を有効にします。

<Switch> system-view

[Switch] parity-error monitor log enable

10.1.37 parity-error monitor period

Syntax

parity-error monitor period *value*

undo parity-error monitor period

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

value: パリティエラーの統計情報の収集間隔を指定します。1～86400 秒の範囲で指定します。

説明

parity-error monitor period コマンドは転送チップのエントリのパリティエラー統計間隔を設定します。

undo parity-error monitor period コマンドはデフォルトに戻します。

パリティエラーを検出し、設定された間隔でパリティエラーの統計情報を収集します。

例

間隔を 120 秒に指定します。

<Switch> system-view

[Switch] parity-error monitor period 120

関連コマンド

parity-error monitor threshold

10.1.38 parity-error monitor threshold

Syntax

parity-error monitor threshold *value*

undo parity-error monitor threshold

デフォルト

5000

View

System view

定義済みユーザロール

network-admin

パラメータ

value: パリティエラーのアラームしきい値を指定します。1～1000000 の範囲で指定します。

説明

parity-error monitor threshold コマンドは転送チップのエントリのパリティエラーアラームしきい値を設定します。

undo parity-error monitor threshold コマンドはデフォルトに戻します。

パリティエラーの統計を検出して収集します。パリティエラー統計間隔内のパリティエラーの数がパリティエラーアラームのしきい値を超えると、システムはアラームを送信します。

例

パリティエラーアラームのしきい値を 8000 に指定します。

<Switch> system-view

[Switch] parity-error monitor threshold 8000

関連コマンド

parity-error monitor period

10.1.39 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 BootWare 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

10.1.40 reboot

Syntax

reboot [**slot** *slot-number*] [**force**]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのオプションが指定されない場合、すべての IRF スタックの装置を再起動します。

force: ソフトウェアの確認を行わず、すぐさま装置を再起動します。このキーワードが指定されていない場合、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

reboot コマンドは装置を再起動します。

⚠ **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** キーワードは、装置に障害が発生した場合、または **force** キーワードを指定しないで **reboot** コマンドを実行しても再起動が正しく実行されない場合にのみ使用してください。**force** キーワードを指定した再起動コマンドは、データ保護を実行しないため、ファイルシステムが破損する可能性があります。

メインのスタートアップソフトウェアイメージが破損しているか存在しない場合は、**reboot** コマンドを実行する前に、メインのスタートアップソフトウェアイメージのセットを再指定する必要があります。

データセキュリティのため、装置がファイル操作を実行している間に装置を再起動しても、装置は再起動しません。

IRF スタックユニットにメンバ装置が 1 つしかない場合は、メンバ装置を再起動すると IRF スタックユニット全体が再起動されます。IRF スタックユニットに下位メンバがあり、そのメンバが正しく動作している場合は、Master を再起動すると Master /下位切り替えが発生します。

IRF スタックユニットおよびメンバ装置を正しく動作させるために、下位のメンバ装置が **Stable** 状態にない場合は、Master を再起動して切り替えを引き起こすことはありません。配下のメンバ装置の状態を確認するには、**display system stable state** コマンドを実行してください。

例

装置を再起動してください。プロンプトで実行コンフィギュレーションを保存します。

<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 mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

ソフトウェアチェックを実行せずに、直ちに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...
```

10.1.41 reset scheduler logfile

Syntax

reset scheduler logfile

View

User view

定義済みユーザロール

network-admin

説明

reset scheduler logfile コマンドはスケジュール自動実行機能のログ情報の削除を行います。

例

ログ情報のクリアを行います。

<Switch> reset scheduler logfile

関連コマンド

display scheduler logfile

10.1.42 resource-monitor minor resend enable

Syntax

resource-monitor minor resend enable

undo resource-monitor minor resend 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

resource-monitor minor resend enable コマンドは minor リソース不足アラームの再送信を有効にします。

undo resource-monitor minor resend enable コマンドは minor リソース不足アラーム再送信の設定を無効にします。

リソースタイプが minor アラームのままの状態であるか、severe から minor のアラーム状態になると、装置は minor リソース不足アラーム再送機能が有効になっているかどうかを識別します。機能が無効になっている場合、装置は追加のアラームを発行しません。有効になっている場合は、minor アラームを定期的に送信し続けます。

例

minor リソース不足アラームの再送を有効にします。

<Switch> system-view

[Switch] resource-monitor minor resend enable

関連コマンド

- **display resource-monitor**
- **resource-monitor output**
- **resource-monitor resource**

10.1.43 resource-monitor output

Syntax

resource-monitor output { **netconf-event** | **snmp-notification** | **syslog** } *

undo resource-monitor output [**netconf-event** | **snmp-notification** | **syslog**] *

デフォルト

NETCONF、SNMP、information center

View

System view

定義済みユーザロール

network-admin

パラメータ

netconf-event: リソース不足アラームを、NETCONF 機能に送信して NETCONF イベントにカプセル化します。詳細はオペレーションマニュアルのセクション 11 *システム管理* “*NETCONF*”を参照してください。

snmp-notification: リソース不足アラームを、SNMP 機能に送信して SNMP trap と inform にカプセル化します。詳細はオペレーションマニュアルのセクション 11 *システム管理* “*SNMP*”を参照してください。

syslog: リソース不足アラームを、information center に送信してログメッセージにカプセル化します。information center の詳細は、オペレーションマニュアルのセクション 11 *システム管理* “*information center*”を参照してください。

説明

resource-monitor output コマンドはリソース不足アラームの送信先を指定します。

undo resource-monitor output コマンドはリソース不足アラームの送信先を削除します。

undo resource−monitor output コマンドは、キーワードの指定がない場合は、リソース不足アラームの出力を無効化します。

例

#リソース不足アラームの出力先を information center モジュールに設定します。

<Switch> system-view

[Switch] resource-monitor output syslog

関連コマンド

- **resource-monitor minor resend enable**
- **resource-monitor resource**

10.1.44 resource-monitor resource

Syntax

resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number* **by-percent minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

undo resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number*

デフォルト

リソースのタイプによってデフォルトの設定が異なりますので、**display resource-monitor** コマンドを使用してリソース不足しきい値を表示してください。

View

System view

定義済みユーザロール

network-admin

パラメータ

resource-name: リソースタイプを名前で指定します。大文字、小文字を区別しません。パラメータの値は完全に入力する必要があります。表 10-10 にモニタ可能なリソースタイプを示します。

表 10-10 モニタ可能なリソースタイプ

リソースタイプ	説明
ac	Ethernetサービスインスタンスのリソースです。
agg_group	アグリゲーショングループのリソースです。
ecmpgroup	ECMPグループリソースです。
mqcin	受信MQCリソースです。
mqcout	発信MQCリソースです。
nexthoppool1	アンダレイネットワークのNext-hop poolリソースです。 nexthoppool1(Tunnel関連)はQX-S5300Gシリーズではサポートしていません。
openflowin	OpenFlowリソースです。 openflowin(OpenFlow関連)はQX-S5300Gシリーズではサポートしていません。
pbr	PBRリソースです。
pfilterin	受信パケットフィルタリソースです。

リソースタイプ	説明
pfilterout	発信パケットフィルタリソースです。
rport	レイヤ3 Ethernetインタフェースのリソースです。
subrport	レイヤ3 Ethernetサブインタフェースのリソースです。
vlan	VLANリソースです。
vlaninterface	VLANインタフェースのリソースです。
vrf	VPNインスタンスのリソースです。 vrf(MCE関連)はQX-S5300Gシリーズではサポートしていません。
vsi	VSI（Virtual Switch Instance 仮想スイッチインスタンス)リソースです。 vsi(EVPN関連)はQX-S5300Gシリーズではサポートしていません。
vsiintf	VSIインタフェースのリソースです。 vsiintf(EVPN関連))はQX-S5300Gシリーズではサポートしていません。

slot *slot-number*: メンバ ID で、IRF メンバ装置を指定します。

cpu *cpu-number*: 番号で CPU を指定します。

by-percent: リソース不足のしきい値をパーセントで指定します

minor-threshold *minor-threshold*: minor リソース不足のしきい値を指定します。値の範囲を表示するには、*minor-threshold* 引数の代わりに疑問符(?)を入力します。

severe-threshold *severe-threshold*: servere リソース不足のしきい値を指定します。値の範囲を表示するには、*severe-threshold* 引数の代わりに疑問符(?)を入力します。

説明

resource-monitor resource コマンドはリソース不足のしきい値を設定します。

undo resource-monitor resource コマンドはリソース不足のしきい値の設定を無効にします。

このコマンドを設定すると、装置は使用可能なリソースタイプの量をモニタします。装置は、定期的に使用可能量をサンプリングしてリソース不足のしきい値と比較し、リソース不足状況を識別します。そして設定通りアラームを送信します。

例

スロット 1 の ARP エントリリソースの minor リソース不足のしきい値を 30%、severe リソース不足のしきい値を 10%に設定します。

<Switch> system-view

[Switch] resource-monitor resource arp slot 1 cpu 0 by-percent minor-threshold 30 severe-threshold 10

関連コマンド

- **display resource-monitor**
- **resource-monitor minor resend enable**
- **resource-monitor output**

10.1.45 scheduler job

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

job-name: job 名を指定します。設定範囲は 1～47 文字です。大文字、小文字を区別します。

説明

scheduler job コマンドは job を作成して job view に移行、あるいは既存の job の view に移行します。

undo scheduler job コマンドは job を削除します。

job は複数のスケジュールから割り当てることができます。job view で job にコマンドを割り当てることができます。

例

job 名が **backupconfig** の job を作成し、job view に移行します。

<Switch> system-view

[Switch] scheduler job backupconfig

[Switch-job-backupconfig]

関連コマンド

- **command**
- **scheduler schedule**

10.1.46 scheduler logfile size

Syntax

scheduler logfile size *value*

デフォルト

16KB

View

System view

定義済みユーザロール

network-admin

パラメータ

value: job を実行するログファイルのサイズを設定します。設定範囲は 16～1024KB です。

説明

scheduler logfile size コマンドはスケジュール自動実行機能の job を実行するログファイルのサイズを設定します。

job を実行するログファイルは、job が実行される情報を保存します。ファイルの容量が一杯である場合、古い記録が削除され、新しい記録が保存されます。もしファイルサイズよりもログファイルのサイズが大きい場合、実行される情報はファイルに保存されません。

例

job を実行するログファイルのサイズを 32KB に設定します。

<Switch> system-view

[Switch] scheduler logfile size 32

関連コマンド

display scheduler logfile

10.1.47 scheduler reboot at

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 再起動する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

date: 再起動する日時を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。*YYYY* の設定範囲は 2000～2035 です。*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。

説明

scheduler reboot at コマンドはスケジュール再起動機能の日時、時間を指定します。

undo scheduler reboot コマンドはスケジュール再起動機能の設定を削除します。

⚠ **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。

日時が指定されていないとき、以下の動作を行います。

- 再起動時間が現在時刻より遅い場合、再起動は当日の再起動時間に行われます。
- 再起動時間が現在時刻より早い場合、再起動は次の日の再起動時間に行われます。

データ保護のため、ファイルの操作を実行している間、システムは装置の再起動を行いません。

装置はスケジュール再起動機能を 1 回のみサポートします。もし **schedule reboot delay** コマンドと **scheduler reboot at** コマンドの両方が設定されている場合、あるいはどちらかのコマンドを複数回設定した場合、最後に設定したコマンドが適用されます。

データセキュリティのため、ファイル操作が実行されている場合、システムは再起動時に再起動しません。

例

装置を PM12:00 に再起動します。現在時刻は 2015 年 6 月 6 日の 11:43 であると仮定します。

<Switch> scheduler reboot at 12:00

```
Reboot system at 12:00:00 06/06/2015 (in 0 hours and 16 minutes). Confirm? [Y/N]:
```

関連コマンド

scheduler reboot delay

10.1.48 scheduler reboot delay

Syntax

scheduler reboot delay *time*

undo scheduler reboot

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 再起動する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。引数は 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。

説明

scheduler reboot delay コマンドはスケジュール再起動機能の再起動遅延時間を指定します。

undo scheduler reboot コマンドはスケジュール再起動機能の再起動遅延時間を削除します。

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。

装置はスケジュール再起動機能を 1 回のみサポートします。もし **schedule reboot delay** コマンドと **scheduler reboot at** コマンドの両方を実行した場合、あるいはどちらかのコマンドを複数回実行した場合、最後に実行したコマンドが有効になります。

例

装置を 88 分後に再起動します。現在時刻は 2015 年 6 月 6 日の 11:48 であると仮定します。

<Switch> scheduler reboot delay 88

```
Reboot system at 13:16 06/06/2015(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

10.1.49 scheduler schedule

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

schedule-name: スケジュール名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。

説明

scheduler schedule コマンドはスケジュールを作成してその view に移行、あるいは既存スケジュールの view に移行します。

undo scheduler schedule コマンドはスケジュールを削除します。

管理者を妨げることなく、装置が自動で一つあるいは一連のコマンドを実行するように、job のスケジュールを設定することができます。

スケジュールを設定するには以下を行います。

1) **scheduler job** コマンドを使用して job を作成します。
2) job view で **command** コマンドを使用して job にコマンドを割り当てます。
3) **scheduler schedule** コマンドを使用してスケジュールを作成します。

4) schedule view で **job** コマンドを使用してスケジュールに job を割り当てます。複数の job をスケジュールに割り当てることができます。job はすでに作成している必要があります。
5) **user-role** コマンドを使用してスケジュールにユーザロールを割り当てます。一つのスケジュールには最大 64 のユーザロールを割り当てることができます。
6) **time at** コマンド、**time once** コマンド、**time repeating** コマンドを使用して、スケジュールを実行する時間を指定します。1 つのスケジュールに 1 つの実行時間のみ指定することができます。

例

スケジュール名が **saveconfig** のスケジュールを作成します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

関連コマンド

- **job**
- **time at**
- **time once**

10.1.50 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

interval: 検出間隔を指定します。設定範囲は 1～300 秒です。0 秒を設定すると、検出機能は無効になります。

説明

shutdown-interval コマンドは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。

プロトコルによってポートがシャットダウンすると、装置はポート状態の検出タイマを開始します。タイマが終了すると、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 します。
- もし T>=T1 の場合、ポートはすぐさま UP します。

たとえば、タイマが 30 秒に設定されている場合。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。ポートのシャットダウンから 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

ポート状態検出タイマを 100 秒に設定します。

<Switch> system-view

[Switch] shutdown-interval 100

10.1.51 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]

10.1.52 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

Switch	センサ	警告温度の推奨値	警告温度のデフォルト値	アラーム温度の推奨値	アラーム温度のデフォルト値
QX-S5324GT-4X1C	Hotspot 1	52	66	57	71
QX-S5348GT-4X1C	Hotspot 1	57	61	63	66

🕮 **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お勧めします。

View

System view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。

hotspot: ホットスポットセンサの温度アラームしきい値を設定します。ホットスポットセンサは通常、高温となるチップの側に置かれ、チップをモニタします。

sensor-number: 番号でセンサを指定します。各番号は装置の温度センサを示します。番号の最小は 1 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。

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。

センサの番号の設定範囲としきい値は、モデルによって異なります。設定範囲は、CLI オンラインヘルプを使用して確認してください。

装置の温度が下限温度を下回った、あるいは高温時のワーニング温度に到達したとき、装置は以下の動作を行います。

- ログメッセージとトラップを送信します。
- 装置の前面にある LED 表示で通知します。

例

ホットスポットセンサ 1 の温度アラームしきい値をスロットに設定します。

Set temperature alarm thresholds for hotspot sensor 1 in a slot.

<Switch> system-view

[Switch] temperature-limit slot 1 hotspot 1 -10 50 60

関連コマンド

display environment

10.1.53 time at

Syntax

time at *time date*

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

time: スケジュールを自動で実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

date: スケジュールを自動で実行する実行日を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。YYYY の設定範囲は 2000～2035 です。MM の設定範囲は 1～12 です。DD の設定範囲は月によって変わります。

説明

time at コマンドは非周期のスケジュール実行日時を指定します。

undo time コマンドは非周期のスケジュール実行日時の設定を削除します。

指定時間（実行日と時間）は現在時刻よりも、後にする必要があります。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

2015 年 5 月 11 日の AM01:01 にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time at 1:1 2015/05/11

関連コマンド

scheduler schedule

10.1.54 time once

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

month-date *month-day*: 今月の日を指定します。設定範囲は 1～31 です。今月の日で指定した日が存在しない場合、次の月の該当する日が適用されます。

week-day *week-day*&<1-7>: スケジュールを実行する曜日を指定します。半角スペースで区切り、最高 7 週間まで Mon、Tue、Wed、Thu、Fri、Sat、Sun を指定します。

delay *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。引数は 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。

説明

time once コマンドは非定期スケジュールの 1 つ以上の実行日と実行時間を指定します。

undo time コマンドは非定期スケジュール実行日時の設定を削除します。

指定された時間が過ぎている場合、次の日の指定された時間が適用されます。

指定された月日が過ぎている場合、次の月の指定された日が適用されます。

指定された曜日が過ぎている場合、次の週の指定された曜日が適用されます。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

15:00 にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time once at 15:00

Schedule starts at 15:00 5/11/2011.

今月の 15 日後の 15:00 にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time once at 15:00 month-date 15

次の月曜日、金曜日の PM12:00 にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time once at 12:00 week-day mon fri

10 分後にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time once delay 10

関連コマンド

scheduler schedule

10.1.55 time repeating

Syntax

time repeating [**at** *time* [*date*]] **interval** *interval*

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。このオプションを指定しない場合、現在のシステム時間が指定されます。

date: スケジュールを定期的に自動で実行する開始日を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。YYYY の設定範囲は 2000～2035 です。MM の設定範囲は 1～12 です。DD の設定範囲は月によって変わります。このオプションを指定しない場合、指定した時間になったときの最初の日が指定されます。

interval *interval*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。引数は 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。形式が *mm* である場合、引数は 1 分以上にする必要があります。

month-date [*month-day* | **last**]: 実施日を 1～31 の範囲で指定します。指定した日が当月に存在しない場合、次の月の該当日が適用されます。

week-day *week-day*&<1-7>: スケジュールを実行する曜日を最高 7 曜日まで指定できます。半角スペースで区切り、Mon、Tue、Wed、Thu、Fri、Sat、Sun を指定します。

説明

time repeating コマンドは定期的にスケジュールを実行する時間テーブルを指定します。

undo time コマンドはスケジュール自動実行機能の時間の設定を削除します。

time repeating [**at** *time* [*date*]] **interval** *interval-time* コマンドは 1 日内の指定した時間で定期的にスケジュールを実行するように設定します。

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>] コマンドは月あるいは曜日内の指定した日で定期的にスケジュールを実行するように設定します。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

本日の 8:00 から 1 時間ごとにスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 8:00 interval 60

毎日の PM12:00 にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 12:00

毎月の 5 日の AM8:00 にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 8:00 month-date 5

毎月の最終日の AM8:00 にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 8:00 month-date last

各金曜日と各土曜日の AM8:00 にスケジュール **saveconfig** を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 8:00 week-day fri sat

関連コマンド

scheduler schedule

10.1.56 usb disable

Syntax

usb disable

undo usb disable

デフォルト

有効.

View

System view

定義済みユーザロール

network-admin

説明

usb disable コマンドは USB インタフェースを無効にします。

undo usb disable コマンドは USB インタフェースを有効にします。

ファイルのアップロードやダウンロードで USB インタフェースが使用できます。

このコマンドを実行する前に、**umount** コマンドですべての USB 機器をアンマウントに設定してください。

例

USB インタフェースを有効にします。

<Switch> system-view

[Switch] undo usb disable

10.1.57 user-role

Syntax

user-role *role-name*

undo user-role *role-name*

デフォルト

スケジュールには、スケジュール作成者のユーザロールがあります。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

role-name : ユーザロール名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。ユーザロールは、ユーザ定義または事前定義済みにすることができます。定義済みのユーザロールには、network-admin、network-operator、および level-0～level-15 があります。

説明

user-role コマンドはユーザロールをスケジュールに割り当てます。

undo user-role コマンドはスケジュールからユーザロールを削除します。

スケジュールには 1 つ以上のユーザロールが必要です。スケジュール内のコマンドは、スケジュールの 1 つ以上のユーザ役割によって許可されていれば実行できます。ユーザロールの詳細については、オペレーションマニュアルのセクション 1 *はじめに*“*RBAC*”を参照してください。

スケジュールは最大 64 のユーザ役割を持つことができます。制限に達すると、追加のユーザ役割をスケジュールに割り当てることはできません。

例

スケジュールテストにユーザロール **rolename** を割り当てます。

<Switch> system-view

[Switch] scheduler schedule test

[Switch-schedule-test] user-role rolename

関連コマンド

- **command**
- **scheduler schedule**

目次

このセクションのページは **1-x-x** です。

11 章 Python 11-1
11.1 Python 設定コマンド 11-1
11.1.1 exit() 11-1
11.1.2 python 11-1
11.1.3 python filename 11-2

11章 Python

11.1 Python設定コマンド

11.1.1 exit()

Syntax

exit()

View

Python shell

定義済みユーザロール

network-admin

説明

exit()コマンドは Python シェルを終了します。

Python シェルから user view に戻る場合、**quit** コマンドは使用できません。**exit()**コマンドを使用する必要があります。

例

Python シェルを終了します。

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> exit()
```

<Switch>

11.1.2 python

Syntax

python

View

User view

定義済みユーザロール

network-admin

説明

python コマンドは Python シェルに移行します。

Python シェルでは、次の項目を使用できます。

- Python 2.7 コマンド
- Python 2.7 標準 API
- Comware7 拡張 API

例

Python シェルを開始します。

<Switch> python

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

11.1.3 python filename

Syntax

python *filename* [*param*]

View

User view

定義済みユーザロール

network-admin

パラメータ

filename: 装置の記憶媒体上の Python スクリプトの名前を指定します。スクリプト名は大文字、小文字を区別します。拡張子.py を使用する必要があります。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。複数のパラメータを入力するには、区切り文字としてスペースを使用します。

説明

python filename コマンドは Python スクリプトを実行します。

Python スクリプトの実行中は、操作を実行できません。

スクリプト内のステートメントが構文の要件を満たしていることを確認します。Syntax エラーのあるステートメントが見つかると、システムは Python スクリプトの実行を停止します。

スクリプトの実行時には、対話型ステートメントのデフォルトが使用されます。人間が入力してもシステムは停止しません。

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']

目次

このセクションのページは **1-x-x** です。

12 章 Auto Config 12-1
12.1 Auto Config コマンド 12-1
12.1.1 autodeploy udisk enable 12-1

12章 Auto Config

12.1 Auto Configコマンド

12.1.1 autodeploy udisk enable

Syntax

autodeploy udisk enable

undo autodeploy udisk 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

autodeploy udisk enable コマンドは USB ベース Auto Config を有効にします。

undo autodeploy udisk enable コマンドは USB ベース Auto Config を無効にします。

例

USB ベース Auto Config を無効にします。

<Switch> system-view

[Switch] undo autodeploy udisk enable

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

2.IRF スタック

本マニュアルは以下に示す章で構成されています。

01-IRF スタック

目次

このセクションのページは **2-x-x** です。

1 章 IRF スタック 1-1
1.1 IRF スタック設定コマンド 1-1
1.1.1 display irf 1-1
1.1.2 display irf configuration 1-2
1.1.3 display irf link 1-3
1.1.4 display irf topology 1-5
1.1.5 display mad 1-6
1.1.6 irf auto-update enable 1-9
1.1.7 irf domain 1-10
1.1.8 irf link-delay 1-11
1.1.9 irf mac-address persistent 1-12
1.1.10 irf member description 1-14
1.1.11 irf member priority 1-15
1.1.12 irf member renumber 1-15
1.1.13 irf-port 1-17
1.1.14 irf-port-configuration active 1-18
1.1.15 mad arp enable 1-19
1.1.16 mad bfd enable 1-21
1.1.17 mad enable 1-23
1.1.18 mad exclude interface 1-25
1.1.19 mad ip address 1-26
1.1.20 mad restore 1-27
1.1.21 port group interface 1-28

1章 IRF スタック

1.1 IRFスタック設定コマンド

1.1.1 display irf

Syntax

display irf

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf コマンドは IRF スタックユニットの情報を表示します。

例

表 1-1 に、IRF スタックユニット情報のフィールドを示します。

表 1-1 コマンド出力

フィールド	説明
MemberID	IRFスタックのメンバIDです。 ● メンバIDはアスタリスク（*）で表示されます。 ● ログインしている装置のメンバIDは(+)で表示されます。
Role	IRFスタックユニットのメンバ装置の役割です。 ● **Standby**—メンバ装置です。 ● **Master**—Master装置です。 ● **Loading**—装置がソフトウェアイメージを読み込んでいます。
Priority	IRFスタックのメンバのプライオリティです。
CPU-MAC	装置のCPU-MACアドレスです。

フィールド	説明
Description	メンバ装置の説明です。 ● 説明が設定されていない場合、ハイフン線（-----）と表示されます。 ● 文字の最大数を超過している場合、超過している個所が省略され、（...）と表示されます。すべての説明を表示する場合、**display current-configuration**コマンドを使用します。
Auto upgrade	ソフトウェアオートアップグレード機能の状態です。 ● **yes**—有効です。 ● **no**—無効です。
MAC persistent	IRFスタックのBridge MACアドレスを保持する設定です。 ● **6 min**—Master装置が離脱したのち、IRFスタックユニットのBridge MACアドレスは6分間変更しません。 ● **always**—Masterが離脱した後、IRFスタックユニットのBridge MACアドレスは変更しません。 ● **no**—Masterが離脱した後、すぐに新しいMasterのBridge MACアドレスに切り替わります。
Domain ID	IRFスタックユニットのドメインIDです。IRFスタックユニットに割り当てたドメインIDは、IRFスタックユニットを識別するために使用されます。

関連コマンド

- **display irf configuration**
- **display irf topology**

1.1.2 display irf configuration

Syntax

display irf configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf configuration コマンドは基本的な IRF スタックの設定を表示します。

例

すべてのメンバの基本的な IRF スタックの設定を表示します。

<Switch> display irf configuration

```
MemberID  NewID    IRF-Port1                IRF-Port2
 1        1        Ten-GigabitEthernet1/0/49   Ten-GigabitEthernet1/0/51
 2        2        Ten-GigabitEthernet2/0/49   Ten-GigabitEthernet2/0/51
                   Ten-GigabitEthernet2/0/50
 4        4        Ten-GigabitEthernet4/0/49   Ten-GigabitEthernet4/0/51
                                               Ten-GigabitEthernet4/0/52
```

表 1-2 コマンド出力

フィールド	説明
MemberID	装置の現在のメンバIDです。
NewID	装置に割り当てられたメンバIDです。メンバIDは再起動後に適用されます。
IRF-Port1	IRFスタックポート1に関連付けられたIRFスタック物理ポートです。IRFスタック物理ポートがIRFスタックポート1に関連付けられていない場合、**disable**と表示されます。
IRF-Port2	IRFスタックポート2に関連付けられたIRFスタック物理ポートです。IRFスタック物理ポートがIRFスタックポート2に関連付けられていない場合、**disable**と表示されます。

関連コマンド

- **display irf**
- **display irf topology**

1.1.3 display irf link

Syntax

display irf link

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf link コマンドは IRF スタックのリンク情報を表示します。

Examples

IRF スタックのリンク情報を表示します。

<Switch> display irf link

```
Member 1
 IRF Port    Interface                        Status
 1           disable                         --
 2           Ten-GigabitEthernet1/0/49          UP
             Ten-GigabitEthernet1/0/50          ADM
Member 2
 IRF Port    Interface                       Status
 1           Ten-GigabitEthernet2/0/49          UP
             Ten-GigabitEthernet2/0/50          DOWN
 2           disable                         --
```

表 1-3 コマンド出力

フィールド	説明
Member ID	IRFスタックのメンバIDです。
IRF Port	IRFスタックポート番号です。 ● **1**－IRFスタックポート1です。 ● **2**－IRFスタックポート2です。
Interface	IRFスタックポートに関連付けられたIRFスタック物理ポートです。IRFスタック物理ポートがIRFスタックポートに関連付けられていない場合、**disable**と表示されます。
Status	IRFスタック物理ポートのリンク状態です。 ● **UP**－リンクがUP状態です。 ● **DOWN**－リンクがDOWN状態です。 ● **ADM**－ポートが**shutdown**コマンドにより手動でシャットダウンしています。 ● **ABSENT**－ホストの拡張インタフェースカードがありません。

1.1.4 display irf topology

Syntax

display irf topology

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf topology コマンドは IRF スタックユニットのトポロジ情報を表示します。

例

表 1-4 に、IRF スタックユニット情報のフィールドを示します。

表 1-4 コマンド出力

フィールド	説明
IRF-Port1	リンク状態、隣接情報を含むIRFスタックポート1の情報です。
IRF-Port2	リンク状態、隣接情報を含むIRFスタックポート2の情報です。
MemberID	IRFスタックのメンバIDです。
Link	IRFスタックポートのリンク状態です。 • **UP**—IRFスタックのリンクがUP状態です。 • **DOWN**—IRFスタックのリンクがDOWN状態です。ポートの物理リンクがない、あるいは**irf-port-configuration active**コマンドで動作していません。 • **DIS**—IRFスタックポートに関連付けられたIRFスタック物理ポートがありません。 • **TIMEOUT**—IRFスタックのhelloパケットの送信がタイムアウトしています。 • **ISOLATE**—装置はIRFスタックユニットから絶縁されています。この問題は、次のような理由で発生する可能性があります。 ■ IRFスタックユニットは装置モデルをサポートしません。 ■ メンバ装置の最大数が上限を超えました。

フィールド	説明
neighbor	装置のIRFスタックのメンバIDがIRFスタックポートに接続しています。 装置がポートに接続されていない場合、このフィールドには3つのハイフン（---）が表示されます。
Belong To	IRFスタックユニットがあります。IRFスタックユニットのMasterのCPU-MACアドレスで示します。

関連コマンド

- **display irf**
- **display irf configuration**

1.1.5 display mad

Syntax

display mad [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: 詳細な MAD 情報を表示します。指定しない場合、MAD の設定が有効あるいは無効のみを表示します。

説明

display mad コマンドは MAD の状態と設定を表示します。

例

MAD 情報の概要を表示します。

<Switch> display mad

```
MAD ARP enabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD disabled.
```

MAD 情報の詳細を表示します。

<Switch> display mad verbose

```
Multi-active recovery state: No
Excluded ports (user-configured):
  Bridge-Aggregation4
  Vlan-interface999
Excluded ports (system-configured):
  IRF physical interfaces:
    Ten-GigabitEthernet1/0/49
    Ten-GigabitEthernet1/0/50
    Ten-GigabitEthernet1/0/51
    Ten-GigabitEthernet1/0/52
  BFD MAD interfaces:
    GigabitEthernet1/0/10
    GigabitEthernet2/0/10
    Vlan-interface3
  Member interfaces of excluded interface Bridge-Aggregation 4:
    GigabitEthernet1/0/11
    GigabitEthernet2/0/11
MAD ARP enabled interface:
  Vlan-interface2
MAD ND enabled interface:
  Vlan-interface2
MAD LACP enabled interface: Bridge-Aggregation 1
  MAD status              : Normal
  Member ID      Port                   MAD status
  1              GigabitEthernet1/0/1      Normal
  2              GigabitEthernet2/0/1      Normal
MAD BFD enabled interface: VLAN-interface 3
  MAD status              : Normal
  Member ID   MAD IP address      Neighbor    MAD status
  1          192.168.1.1/24      2          Normal
  2          192.168.1.2/24      1          Normal
```

表 1-5 コマンド出力

フィールド	説明
MAD ARP enabled.	ARP MADの状態です。 ARP MADが無効な場合、このフィールドには**MAD ARP disabled**が表示されます。
MAD LACP enabled.	LACP MADの状態です。 LACP MADが無効になっている場合、このフィールドには**MAD LACP disabled**と表示されます。

フィールド	説明
MAD BFD enabled.	BFD MADの状態です。 BFD MADが無効の場合、このフィールドには**MAD BFD disabled**と表示されます。
Multi-active recovery state	IRFスタックユニットがRecovery状態であるかどうかを示します。 ● **Yes**—IRFスタックユニットがRecovery状態です。IRFスタックユニットが複数のIRFスタックユニットに分裂したとMADが検出したとき、1つのIRFスタックユニットにトラフィックを転送します。ほかのすべてのIRFスタックユニットがRecovery状態に設定されます。Recovery状態ではMADは、IRFスタック物理ポートとシャットダウンに設定されていないポートを除いてIRFスタックユニットのすべてのIRFスタック物理ポートをシャットダウンします。 ● **No**—IRFスタックユニットがRecovery状態でありません。アクティブでトラフィックを転送できます。
Excluded ports(user-configured)	IRFスタックユニットがRecovery状態へ遷移時にシャットダウンしないよう、手動で設定されたポートです。
Excluded ports(system-configured)	IRFスタックユニットがRecovery状態へ遷移時にシャットダウンしないよう、デフォルトで設定されたポートです。このポートはユーザが設定することができません。 ● IRF物理インタフェースです。 ● BFD MADインタフェース： 　■ BFD MADおよびVLAN内のレイヤ2イーサネットポートに使用されるVLANインタフェース。 　■ BFD MADに使用される管理イーサネットポート。 ● アグリゲートインタフェースがMADシャットダウンアクションから除外されている場合は、レイヤ2アグリゲートインタフェースのIRFスタックメンバインタフェースです。
MAD ARP enabled interface:	ARP MADが有効になっているインタフェースです。
MAD ND enabled interface:	ND MADが有効になっているインタフェースです。
MAD LACP enabled interface	LACP MADが有効になっているインタフェースです。このフィールドは、LACP MADで有効になっている各インタフェースに対して表示されます。

フィールド	説明
MAD status	LACP MAD動作モードの状態です。 • **Normal**— LACP MADが正常に動作しています。 • **Faulty**—LACP MADがインタフェースあるいはポートで正常に動作していません。インタフェースあるいはポートの接続あるいは設定を確認してください。 ■ LACP MADリンクのポートが起動していることを確認します。 ■ 中間装置が拡張LACPDUをサポートしていることを確認してください。 ■ すべてのメンバ装置にLACP MAD用のIRFスタックメンバポートがあることを確認します。
Member ID Port MAD status	LACP MADの詳細です。 • **Member ID**—装置のIRFメンバIDです。 • **Port**—LACP MADに使用されるアグリゲートインタフェースのメンバポートです。 • **MAD status**—IRFスタックメンバポートのLACP MAD動作ステートです。オプションには**Normal**と**Faulty**があります。
MAD BFD enabled interface:	BFD MADが有効になっているインタフェースです。
MAD status	BFD MAD動作の状態です。 • **Normal**—BFD MADは正常に動作しています。 • **Faulty**—BFD MADが正しく動作していません。BFD MADリンクの接続を確認してください。 • **N/A**—BFD MADリンク状態を検出できません。管理イーサネットポートでBFD MADが有効になっている場合、このフィールドには**N/A**と表示されるのが普通です。
Member ID MAD IP address Neighbor MAD status	BFD MADの詳細状態です。 • **Member ID**—ローカル装置のIRFメンバIDです。 • **MAD IP address**—IRFスタックメンバ装置のMAD IPアドレスです。 • **Neighbor**—隣接メンバ装置のIRFスタックメンバIDです。 • **MAD status**—BFD MADリンクス状態です。オプションには**Normal**と**Faulty** があります。

1.1.6 irf auto-update enable

Syntax

irf auto-update enable

undo irf auto-update enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

irf auto-update enable コマンドはすべての IRF スタックユニットのメンバのソフトウェアを自動で更新する機能を有効にします。

undo irf auto-update enable コマンドはソフトウェア自動更新機能を無効にします。

このコマンドで、IRF スタックユニットの Master 装置の現在のソフトウェアイメージを IRF スタックユニットに追加するすべての装置に自動的に伝えます。

ソフトウェア自動更新機能を有効にする場合、装置に新しいシステムソフトウェアのための有効な領域があることを確認してください。適切な領域がない場合、装置は現在のソフトウェアイメージを自動的に削除します。もし再利用された空き領域が十分でない場合、装置はソフトウェア自動更新機能を完了することができません。装置を再起動し、ファイルを削除するために Boot メニューに移行してください。

例

ソフトウェア自動更新機能を有効にします。

<Switch> system-view

[Switch] irf auto-update enable

1.1.7 irf domain

Syntax

irf domain *domain-id*

undo irf domain

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-id: IRF スタックユニットのドメイン ID を指定します。設定範囲は 0～4294967295 です。

説明

irf domain コマンドは IRF スタックユニットにドメイン ID を割り当てます。

undo irf domain コマンドはデフォルトの IRF スタックのドメインの設定に戻します。

1 つの IRF スタックユニットは 1 つの IRF スタックのドメインを形成します。IRF スタックは IRF スタックユニットを一意に識別し、別の IRF スタックユニットからの干渉を防ぐために IRF スタックのドメイン ID を使用します。

1 つの IRF スタックユニットが LACP MAD、ARP MAD の中間装置として別の IRF スタックユニットを使用する場合、IRF スタック分裂の検出失敗を避けるために、中間装置と異なるドメイン ID を割り当てなければなりません。間違って検出されると、IRF スタックの分裂を引き起こします。

IRF スタックユニットは IRF スタックのドメイン ID が 1 つのみあります。**irf domain**、**mad enable**、**mad arp enable** コマンドで IRF スタックのドメイン ID を変更することができます。これらのコマンドで設定された IRF スタックのドメイン ID は互いに上書きされます。

例

IRF スタックのドメイン ID を 10 に設定します。

<Switch> system-view

[Switch] irf domain 10

1.1.8 irf link-delay

Syntax

irf link-delay *interval*

undo irf link-delay

デフォルト

500 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: リンクレイヤが IRF スタックポートのリンクダウンのイベントを報告する遅延時間です。設定範囲は 0～10000 ミリ秒です。0 に設定した場合、遅延なくリンクダウンのイベントが報告されます。

説明

irf link-delay コマンドは IRF スタックポートのリンクダウンのイベントを報告する遅延時間を設定します。

undo irf link-delay コマンドは 4000 ミリ秒を設定します。

設定をデフォルトに戻す場合は、**irf link-delay 500** コマンドを実行してください。**undo irf link-delay** は 4000 ミリ秒で動作します。

IRF スタックのリンクダウンのレポート遅延（Link-delay）の設定をするとき、以下の制限とガイドラインに従ってください。

- IRF スタックの Link-delay が上位レイヤプロトコル（たとえば、CFD）のタイムアウトの設定よりも短いことを確認してください。この上位プロトコルのタイムアウトの時間は、上位レイヤプロトコルでリンクがダウンしたと認識する間隔です。もし Link-delay がプロトコルのタイムアウト時間より長い場合、不必要な再計算が発生する可能性があります。
- 以下の状況では Link-delay を 0 秒に設定してください。
  - IRF スタックユニットが Master/メンバあるいは IRF スタックリンクの素早い切り替えが必要である場合
  - RRPP、BFD あるいは GR が使用されている場合
  - IRF スタックの IRF スタック物理ポートをシャットダウンする、あるいは IRF スタックのメンバ装置を再起動する場合（操作を完了したのち、ネットワークの状況に従って遅延を再設定します。）

例

IRF スタックポートのリンクダウンのイベントを報告する遅延時間を 300 ミリ秒に設定します。

<Switch> system-view

[Switch] irf link-delay 300

1.1.9 irf mac-address persistent

Syntax

irf mac-address persistent { **always** | **timer** }

undo irf mac-address persistent

デフォルト

Master 装置が離脱した後、IRF スタックユニットの Bridge MAC アドレスは 6 分間変更されません。

View

System view

定義済みユーザロール

network-admin

パラメータ

always: IRF スタックユニットの Bridge MAC アドレスを変更しません。新しい Master の選定が行われたのち IRF スタックユニットは Bridge MAC アドレスを変更しません。

timer: 新しい Master の選定が行われたのち IRF スタックユニットの Bridge MAC アドレスは 6 分間変更しません。時間以内に IRF スタックユニットに装置が再加入した場合、IRF スタックの Bridge MAC アドレスを変更しません。時間以内に IRF スタックユニットに装置が再加入しない場合、IRF スタックユニットは新しい Master の Bridge MAC アドレスを使用します。

説明

irf mac-address persistent コマンドは IRF スタックの Bridge MAC アドレスを保持するように設定します。

undo irf mac-address persistent コマンドは IRF Bridge MAC 永続性を無効にします。

IRF スタックの Bridge MAC アドレスは Master の再選定後に、IRF スタックユニットが Bridge MAC アドレスとして古い Master の Bridge MAC アドレスを使用し続ける時間を指定します。

ARP MAD が使用される場合、IRF スタックの Bridge MAC アドレスの保持を無効にするため、**undo irf mac-address persistent** コマンドを使用します。

以下の状況で **irf mac-address persistent always** コマンドを設定します。

- IRF スタックがデイジーチェーン構成を使用する場合
- IRF スタックが上位または下位の装置とリンクアグリゲーションで接続されている場合

Bridge MAC アドレスの変更によって Master の再選定で転送遅延やパケットロスを引き起こさないように **irf mac-address persistent always** コマンドを設定してください。

デフォルトで IRF スタックユニットは Master 装置の Bridge MAC アドレスを使用します。LACP のようなレイヤ 2 プロトコルは IRF スタックユニットを識別するため、Bridge MAC アドレスを使用します。LAN スイッチでは Bridge MAC アドレスは一意にする必要があります。

Bridge MAC アドレスの重複を防ぐため、IRF スタックユニットは Master の離脱後、自動的に Bridge MAC アドレスを変更することができます。しかし変更を行うとサービス

の中断を引き起こします。ネットワークの状況に依存して、Master の離脱後に IRF スタックユニットの Bridge MAC アドレスを保持するか変更するかを設定することができます。

2 つの IRF スタックユニットが同じ Bridge MAC アドレスを持っている場合、結合することができません。

例

IRF スタックの Bridge MAC アドレスの保持時間を永久保持に設定します。

<Switch> system-view

[Switch] irf mac-address persistent always

1.1.10 irf member description

Syntax

irf member *member-id* **description** *text*

undo irf member *member-id* **description**

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。

text: 説明を設定します。設定範囲は 1～127 文字です。

説明

irf member description コマンドは IRF スタックのメンバの説明を設定します。

undo irf member description コマンドはデフォルトに戻します。

例

IRF スタックのメンバ 1 の説明を F1Num001 に設定します。

<Switch> system-view

[Switch] irf member 1 description F1Num001

1.1.11 irf member priority

Syntax

irf member *member-id* **priority** *priority*

undo irf member *member-id* **priority**

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。IRF スタックのメンバ ID の設定範囲は 1～10 です。

priority: プライオリティを指定します。設定範囲は 1～32 です。プライオリティの値が高い場合、プライオリティは高くなります。Master はプライオリティが高い装置が優先されます。

説明

irf member priority コマンドは IRF スタックのメンバのプライオリティを変更します。

undo irf member priority コマンドはデフォルトに戻します。

IRF スタックのメンバの ID、プライオリティを表示する場合、**display irf** コマンドを使用します。

例

IRF スタックのメンバ 2 のプライオリティを 32 に設定します。

<Switch> system-view

[Switch] irf member 2 priority 32

1.1.12 irf member renumber

Syntax

irf member *member-id* **renumber** *new-member-id*

undo irf member *member-id* **renumber**

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。設定範囲は 1～10 です。

new-member-id: IRF スタックのメンバに新しい ID を割り当てます。設定範囲は 1～10 です。

説明

注意:

IRF スタックのメンバ ID の変更を行うと、再起動により IRF スタック物理ポートの設定を含むメンバ ID に関する設定が変更され、パケットロスが発生する可能性があります。

irf member renumber コマンドは装置の IRF スタックのメンバ ID を変更します。

undo irf member renumber コマンドは装置の IRF スタックのメンバ ID をもとに戻します。

メンバ ID を適用する場合、IRF スタックのメンバの再起動が必要です。メンバ装置を再起動する前に IRF スタックのメンバ ID の変更をキャンセルするには、**undo irf member renumber** コマンドを使用します。コマンドで、新しい IRF スタックのメンバ ID を古い IRF スタックのメンバ ID と同じになるように設定します。

装置を IRF スタックユニットに追加するとき、装置に一意の IRF スタックのメンバ ID を割り当てる必要があります。IRF スタックのメンバ ID が IRF スタックユニットで使用されている場合、装置は IRF スタックユニットに加入することができません。

IRF スタックのメンバ装置間のメンバ ID の置換は、予期しない設定の変更やデータロスを引き起こす可能性があります。たとえば、Device A、Device B の IRF スタックのメンバ ID がそれぞれ 2、3 であるとします。メンバ ID を置換した後、ポートの設定も変更されます。

例

IRF スタックのメンバ ID を 1 から 2 に変更します。

<Switch> display irf

[Switch] irf member 1 renumber 2

```
Renumbering the member ID may result in configuration change or loss.
Continue?[Y/N]Y
```

装置を再起動する前に、前の例の変更を取り消してください。

[Switch] undo irf member 1 renumber

```
Renumbering the member ID may result in configuration change or loss.
Continue?[Y/N]y
```

irf member 1 renumber 2 コマンドの実行後に装置を再起動すると、システムの再起動時に装置メンバ ID が 2 に変わります。**undo irf member 1 renumber** を使用しても、メンバ ID を 1 に復元することはできません。メンバ ID を再設定するには、**irf member 2 renumber 1** コマンドを使用する必要があります。

1.1.13 irf-port

Syntax

irf-port *member-id/irf-port-number*

undo irf-port *member-id/irf-port-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ装置をそのメンバ ID で指定します。

irf-port-number: メンバ装置の IRF ポートを指定します。*irf-port-number* 引数は IRF ポートインデックスを表し、1 または 2 である必要があります。

説明

irf-port コマンドは IRF port view に移行します。

undo irf-port コマンドは IRF スタックポートのすべてのポートの割り当てを削除します。

IRF スタック接続の IRF スタックポートに IRF スタック物理ポートを割り当てるため、IRF port view に移行する必要があります。

例

IRF ポート 2/1 view に入ります。

<Switch> system-view

[Switch] irf-port 2/1

[Switch-irf-port2/1]

関連コマンド

port group interface

1.1.14 irf-port-configuration active

Syntax

irf-port-configuration active

View

System view

定義済みユーザロール

network-admin

説明

irf-port-configuration active コマンドは装置に設定したすべての IRF スタックポートの設定を有効にします。

2 つの装置間の IRF スタック物理ポートを接続し、IRF スタックポートに関連付けたのち、IRF スタックポートの設定を有効にするために、このコマンドを使用します。このコマンドは 2 つの装置を 1 つの IRF スタックユニットに結合します。

システムは以下の状況において自動で IRF スタックポートの設定を有効にします。

- 装置が起動するコンフィグレーションファイルが IRF スタックポートの関連付けを含みます。
- IRF スタックが形成したのち、IRF スタックポートに IRF スタック物理ポートを関連付けます。

例

ポートが DIS 状態のときに IRF スタックポート 1/2 を設定して有効にするには、次の手順を実行します。

IRF スタックポート 1/2 を Ten-GigabitEthernet 1/0/49 に関連付けます。

<Switch> system-view

[Switch] interface ten-gigabitethernet 1/0/49

[Switch-Ten-GigabitEthernet1/0/49] shutdown

[Switch-Ten-GigabitEthernet1/0/49] quit

[Switch] irf-port 1/2

[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/49

IRF スタックのセットアップを行うため、以下の作業を行います。

IRF スタックの設定を完了した後、設定を保存します。

irf-port-configuration active コマンドを実行し、IRF スタックポートを有効にします。

[Switch-irf-port1/2] quit

[Switch] interface ten-gigabitethernet 1/0/49

[Switch-Ten-GigabitEthernet1/0/49] undo shutdown

[Switch-Ten-GigabitEthernet1/0/49] quit

再起動後に IRF スタックポートの設定が適用されるように設定を保存します。

[Switch] save

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.....................
Saved the current configuration to mainboard device successfully.
```

IRF スタックポートを有効にします。

[Switch] irf-port-configuration active

1.1.15 mad arp enable

Syntax

mad arp enable

undo mad arp enable

デフォルト

無効

View

Management Ethernet interface view

VLAN interface view

定義済みユーザロール

network-admin

説明

mad arp enable コマンドは ARP MAD を有効にします。

undo mad arp enable コマンドは ARP MAD を無効にします。

ARP MAD は拡張 ARP パケットを使用して、multi-active 衝突を検知します。

ARP MAD を LACP MAD または BFD MAD と一緒に設定しないでください。衝突の処理方法が異なるためです。

VLAN インタフェースに ARP MAD を設定するときは、次の制限事項とガイドラインに従ってください。

カテゴリ	制限とガイドライン
ARP MAD VLAN	• VLANインタフェース1でARP MADを有効にしないでください • 中間装置を使用している場合は、次の作業を行います。 　■ IRFスタックユニットと中継装置の両方で、ARP MAD用のVLANを作成します。 　■ IRFスタックユニットと中継装置の両方で、ARP MADリンクのポートをARP MAD VLANに割り当てます。 　■ IRFスタックユニットで、ARP MAD VLAN用のVLANインタフェースを作成します。 • ARP MAD VLANを他の目的に使用しないでください。
ARP MADと機能設定	中継装置を使用する場合は、次の要件を満たしていることを確認します。 IRFスタックユニットと中継装置の間のスパニングツリー機能を実行して、転送状態にあるARP MADリンクが1つだけであることを確認します。スパニングツリー機能とその設定についての詳細は、オペレーションマニュアルのセクション3 *アクセス* を参照してください。 • アドレスの所有者が離れるとすぐに、IRFスタックユニットがブリッジMACアドレスを変更できるようにします。 • 中継装置もIRFスタックユニットの場合は、スプリットを正しく検出できるように、2つのIRFスタックユニットに異なるドメインIDを割り当てます。

管理 Ethernet ポートを使用する ARP MAD を設定する場合は、次の制限およびガイドラインに従ってください。

カテゴリ	制限とガイドライン
ARP MAD用管理イーサネットポート	各メンバ装置の管理Ethernetポートを中継装置の共通Ethernetポートに接続します。
ARP MAD VLAN	中継装置で、ARP MAD用のVLANを作成し、ARP MADに使用するポートをそのVLANに割り当てます。IRFスタックユニットでは、VLANに管理Ethernetポートを割り当てる必要はありません。

カテゴリ	制限とガイドライン
ARP MADと機能設定	• アドレスの所有者が離れるとすぐに、IRFスタックユニットがブリッジMACアドレスを変更できるようにします。 • 中継装置もIRFスタックユニットの場合は、スプリットを正しく検出できるように、2つのIRFスタックユニットに異なるドメインIDを割り当てます。

mad arp enable コマンドを使用するとき、システムはドメイン ID を入力するように画面が表示されます。現在のドメイン ID を変更しない場合、Enter キーを押下します。

IRF スタックユニットは 1 つの IRF スタックのドメイン ID のみサポートします。**irf domain**、**mad enable**、**mad arp enable** のコマンドを使用して IRF スタックのドメイン ID を変更することができます。設定された IRF スタックのドメイン ID は、相互に上書きします。

例

VLAN インタフェース 3 で ARP MAD を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] mad arp enable

```
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

関連コマンド

irf domain

1.1.16 mad bfd enable

Syntax

mad bfd enable

undo mad bfd enable

デフォルト

無効

View

VLAN interface view

Management Ethernet interface view

定義済みユーザロール

network-admin

説明

mad bfd enable コマンドは BFD MAD を有効にします。

undo mad bfd enable コマンドは BFD MAD を無効にします。

BFD MAD を ARP MAD と一緒に設定しないでください。衝突の処理方法が異なるためです。

VLAN インタフェースで BFD MAD を設定するとき、以下のガイドラインに従います。

カテゴリ	制限とガイドライン
BFD MAD VLAN	• VLANインタフェース1でBFD MADを有効にすることはできません。 • 中継装置を使用する場合、次の作業を行います。 ■ IRFスタック装置と中継装置の両方でBFD MADのVLANを作成します。 ■ IRFスタック装置と中継装置の両方でBFD MADリンクのポートBFD MAD VLANに割り当てます。 ■ IRFスタックユニットで、BFD MAD VLANのVLANインタフェースを作成します。 ■ ネットワークの IRF スタックユニットは異なる BFD MAD VLAN を使用してください。 • 正しいトラフィックの転送を行うため、BFD MAD VLANはBFD MADリンクのポートのみを使用してください。もしBFD MADリンクのポートでない場合、BFD MAD VLANからのポートを取り除いてください。たとえば**port trunk permit vlan all**コマンドですべてのVLANにポートが割り当てられている場合、BFD MAD VLANからポートを除外するため、**undo port trunk permit**コマンドを使用してください。
BFD MAD VLANと機能の互換性	BFD MAD のVLANをほかの用途で使用しないでください。 • BFD MADで使用されるVLANインタフェースでは**mad bfd enable**コマンドと**mad ip address**コマンドのみ設定できます。もしほかの機能を設定する場合、BFD MADとインタフェースのほかの機能の両方は正常に動作しない可能性があります。 • BFD MADのVLANのポートでは、スパニングツリー機能を無効にしてください。MAD機能はスパニングツリー機能と同時に使用することはできません。

カテゴリ	制限とガイドライン
MAD IPアドレス	• BFD MADを有効にしたVLANインタフェースでMADのIPアドレスを設定する場合、**ip address**コマンドの代わりに**mad ip address**コマンドを使用してください。 • BFD MAD が有効なVLANインタフェースのすべてのMAD IPアドレスは、同じサブネット上にある必要があります。

管理イーサネットポートを使用する BFD MAD を設定する場合は、次の制限事項とガイドラインに従ってください。

カテゴリ	制限とガイドライン
BFD MAD用管理Ethernetポート	各メンバ装置の管理Ethernetポートを中継装置の共通Ethernetポートに接続します。
BFD MAD VLAN	• 中継装置で、BFD MAD用のVLANを作成し、BFD MADに使用されるポートをVLANに割り当てます。IRFスタックユニットでは、VLANに管理Ethernetポートを割り当てる必要はありません。 • ネットワーク上のIRFスタックユニットが異なるBFD MAD VLANを使用していることを確認します。 • 中継装置のBFD MAD VLANに、BFD MADリンクのポートだけが含まれていることを確認します。
MAD IPアドレス	• BFD MAD対応の管理イーサネットポートでMAD IPアドレスを設定するには、**ip address**コマンドの代わりに**mad ip address**コマンドを使用します。 • すべてのMAD IPアドレスが同じサブネット上にあることを確認します。

例

VLAN インタフェース 3 で BFD MAD を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] mad bfd enable

1.1.17 mad enable

Syntax

mad enable

undo mad enable

デフォルト

無効

View

Aggregate interface view

定義済みユーザロール

network-admin

説明

mad enable コマンドは LACP MAD を有効にします。

undo mad enable コマンドは LACP MAD を無効にします。

LACP MAD は、ARP MAD とは異なる方法で衝突を処理します。競合を避けるために、IRF スタックユニットで ARP MAD と一緒に LACP MAD を有効にしないでください。

LACP MAD には、中間装置として機能するために拡張 LACP DU をサポートする NEC 装置が必要です。IRF スタックユニットと中間装置間のすべての IRF スタックメンバ装置に接続するダイナミックリンクアグリゲーショングループを設定する必要があります。ダイナミックリンクアグリゲーションを有効にするため、アグリゲーションインタフェースで **link-aggregation mode dynamic** コマンドを設定します。

1 つの IRF スタックユニットが、LACP MAD の中間装置として別の IRF スタックユニットを使用する場合、正しく検出を行うため、異なるドメイン ID の 2 つの IRF スタックユニットを割り当てる必要があります。そうでない場合、IRF スタックの分裂の検出が誤って行われます。

mad enable コマンドを使用するとき、システムはドメイン ID を入力するように画面が表示されます。現在のドメイン ID を変更しない場合、Enter キーを押下します。

IRF スタックユニットは 1 つの IRF スタックのドメイン ID のみサポートします。**irf domain**、**mad enable**、**mad arp enable** のコマンドを使用して IRF スタックのドメイン ID を変更することができます。設定された IRF スタックのドメイン ID は、相互に上書きします。

例

Bridge-Aggregation 1 でレイヤ 2 ダイナミックアグリゲートインタフェースに LACP MAD を有効にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] link-aggregation mode dynamic

[Switch-Bridge-Aggregation1] mad enable

```
You need to assign a domain ID (range: 0-4294967295)
```

```
[Current domain is: 0]: 1
The assigned  domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
```

関連コマンド

irf domain

1.1.18 mad exclude interface

Syntax

mad exclude interface *interface-type interface-number*

undo mad exclude interface *interface-type interface-number*

デフォルト

IRF スタック物理ポートとコンソールポートを除いて Recovery 状態の IRF スタックユニットのすべてのネットワークポートがシャットダウンされます。システムは自動的に次のサービスインタフェースをシャットダウンから除外します。

- IRF スタック物理インタフェース
- BFD MAD に使用されるインタフェース
- アグリゲートインタフェースがシャットダウンから除外されている場合は、アグリゲートインタフェースのメンバインタフェース。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ポートのタイプと番号でサービスインタフェースを指定します。

説明

mad exclude interface コマンドは multi-active 衝突の検出により Recovery 状態の IRF スタックユニットのすべてのネットワークポートをシャットダウンしないように設定します。

undo mad exclude interface コマンドは multi-active 衝突の検出時にインタフェースが Recovery 状態に移行したときにインタフェースをシャットダウンするように IRF スタックユニットを設定します。

Telnet 接続のような特別の目的のためにポートの状態を UP に継続する必要がある場合、シャットダウンを行うアクションからポートを除外します。不正なトラフィックの転送を防ぐため、Telnet で使用するポートを除いたポートを除外しないことを推奨します。

メンバ装置が再起動して回復した IRF スタックユニットに参加すると、MAD によってシャットダウンされたサービスインタフェースが起動します。IRF リンクが回復する前にアクティブ IRF スタックユニットに障害が発生した場合は、非アクティブ IRF スタックユニットで **mad restore** コマンドを使用して、非アクティブ IRF スタックユニットを回復します。このコマンドはまた MAD によってシャットダウンされたすべてのサービスインタフェースを始動させます。

例

MAD が Recovery 状態に遷移したときにシャットダウンとならないように GigabitEthernet 1/0/1 を除外します。

<Switch> system-view

[Switch] mad exclude interface gigabitethernet 1/0/1

関連コマンド

mad restore

1.1.19 mad ip address

Syntax

mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

undo mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

デフォルト

設定なし

View

VLAN interface view

Management Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: ドットが付いた 10 進数で IP アドレスを指定します。

mask: ドットが付いた 10 進数でサブネットマスクを指定します。

mask-length: サブネットマスク長を指定します。設定範囲は 0～32 です。

member *member-id*: IRF スタックのメンバ ID を指定します。

説明

mad ip address コマンドは BFD MAD の IRF スタックメンバに MAD IP アドレスを割り当てます。

undo mad ip address コマンドは IRF スタックメンバの MAD IP アドレスを削除します。

BFD MAD を使用するため、各 IRF スタックのメンバの BFD MAD が有効な VLAN インタフェースで MAD IP アドレスを設定します。すべての MAD IP アドレスが同一サブネット上にある必要があります）

ip address コマンドを使用して MAD IP アドレスを設定したり、BFD MAD 対応ポートまたはインタフェースに VRRP 仮想アドレスを設定したりしないでください。

Master は送信元 IP アドレスとして MAD IP アドレスを使用することで、ほかのメンバ装置と BFD セッションを確立しようとします。

- もし IRF スタックユニットが正常に動作しているとき、Master の MAD IP アドレスのみが有効です。Master はほかのメンバと BFD セッションを確立することができません。**display bfd session** コマンドを実行した場合、BFD セッションの状態は Down です。
- IRF スタックユニットが分裂しているとき、分裂した IRF スタックユニットの Master の IP アドレスが適用されます。Master は BFD セッションを確立することができます。**display bfd session** コマンドを実行した場合、2 つの装置間の BFD セッションの状態は **Up** です。

例

VLAN インタフェース 3 の IRF スタックのメンバ 1 に MAD IP アドレスを割り当てます。

<Switch> system-view

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] mad ip address 192.168.0.1 255.255.255.0 member 1

VLAN インタフェース 3 の IRF スタックのメンバ 2 に MAD IP アドレスを割り当てます。

[Switch-Vlan-interface3] mad ip address 192.168.0.2 255.255.255.0 member 2

関連コマンド

mad bfd enable

1.1.20 mad restore

Syntax

mad restore

View

System view

定義済みユーザロール

network-admin

説明

mad restore コマンドは Recovery 状態にある IRF スタックユニットの正常な MAD を回復します。

IRF スタックの分裂が回復する前にアクティブの IRF スタックユニットが故障した場合、**mad restore** コマンドを使用して Recovery 状態の IRF スタックユニットを回復します。

回復した IRF スタックユニットはアクティブの IRF スタックユニットの役割を引き継ぎます。

例

Recovery 状態にある IRF スタックユニットの正常な MAD を回復します。

<Switch> system-view

[Switch] mad restore

```
This command will restore the device from multi-active conflict state. Continue?
[Y/N]:Y
Restoring from multi-active conflict state, please wait...
```

1.1.21 port group interface

Syntax

port group interface *interface-type interface-number*

undo port group interface *interface-name*

デフォルト

設定なし

View

IRF port view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: IRF スタック物理ポートのタイプと番号を指定します。

interface-name: *interface-type interface-number* の形式で IRF スタック物理ポートを指定します。*interface-type interface-number* の間に半角スペースは入りません。

説明

port group interface コマンドは IRF スタックポートに IRF スタック物理ポートを割り当てます。

undo port group interface コマンドは IRF スタック物理ポートと IRF スタックポートの割り当てを削除します。

IRF スタック接続を行うため、IRF スタックポートに最低 1 つの IRF スタック物理ポートを関連付けてください。最大 4 つの IRF スタック物理ポートを IRF スタックポートに関連付けることができます。

このコマンドを複数回実行して、複数の IRF スタック物理インタフェースを IRF スタックポートに関連付けます。最大 4 つの IRF スタック物理インタフェースを IRF スタックポートに関連付けることができます。

IRF スタックポートから IRF スタック物理ポートに関連付ける、あるいは関連付けを削除する前に、ポートグループのすべてのポートを **shutdown** コマンドでシャットダウンします。関連付け、あるいは削除の処理が完了した後、すべての IRF スタック物理ポートを **undo shutdown** コマンドでアップします。

IRF スタックリンクが切断されたとしても IRF スタック物理ポートと IRF スタックポート間の関連付けを直接削除することはできません（たとえば、IRF スタックリンクが切断された状態は、トランシーバが取り外され、IRF スタック物理ポートが削除されたままとなっている場合が該当します）。関連付けを削除するため、**undo port group interface** コマンドを使用します。

IRF ポート関連付けの要件の詳細はオペレーションマニュアルのセクション 2 *IRF スタック* を参照してください。

例

IRF メンバ 1 の IRF ポート 1/1 に Ten-GigabitEthernet 1/0/49 ををを割り当てます。

<Switch> system-view

[Switch] interface ten-gigabitethernet 1/0/49

[Switch-Ten-GigabitEthernet1/0/49] shutdown

[Switch-Ten-GigabitEthernet1/0/49] quit

[Switch] irf-port 1/1

[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/49

[Switch-irf-port1/1] quit

[Switch] interface ten-gigabitethernet 1/0/49

[Switch-Ten-GigabitEthernet1/0/49] undo shutdown

関連コマンド

irf-port

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

3. アクセス

本マニュアルは以下に示す章で構成されています。

01-Ethernet インタフェース

02-ループバックインタフェースと Null インタフェース

03-Interface range

04-MAC アドレステーブル

05-MAC Information

06-リンクアグリゲーション

07-Port Isolation

08-STP

09-ループ検出

10-VLAN

11-Private VLAN

12-Voice VLAN

13-QinQ

14-VLAN マッピング

15-LLDP

16-L2PT

目次

このセクションのページは **3-x-x** です。

1 章 Ethernet インタフェース 1-1
1.1 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 1-2
1.1.3 description 1-4
1.1.4 display counters 1-4
1.1.5 display counters rate 1-6
1.1.6 display interface 1-8
1.1.7 duplex 1-21
1.1.8 eee enable 1-22
1.1.9 flow-control 1-22
1.1.10 flow-interval 1-23
1.1.11 interface 1-24
1.1.12 jumboframe enable 1-25
1.1.13 link-delay 1-26
1.1.14 loopback 1-28
1.1.15 multicast-suppression 1-30
1.1.16 port auto-power-down 1-31
1.1.17 reset counters interface 1-32
1.1.18 shutdown 1-33
1.1.19 speed 1-34
1.1.20 unicast-suppression 1-35
1.1.21 using fortygige 1-37
1.1.22 using tengige 1-38
1.2 レイヤ２ Ethernet インタフェース設定コマンド 1-39
1.2.1 display storm-constrain 1-39
1.2.2 mdix-mode 1-41
1.2.3 speed auto 1-42
1.2.4 storm-constrain 1-43
1.2.5 storm-constrain control 1-45
1.2.6 storm-constrain enable log 1-46
1.2.7 storm-constrain enable trap 1-47
1.2.8 storm-constrain interval 1-48
1.2.9 virtual-cable-test 1-49

1章 Ethernet インタフェース

1.1 Ethernetインタフェース設定コマンド

1.1.1 broadcast-suppression

Syntax

broadcast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo broadcast-suppression

デフォルト

Ethernet インタフェースでは、ブロードキャストトラフィックは抑制されません。

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: ブロードキャスト抑制しきい値をインタフェース帯域幅のパーセンテージとして設定します。設定範囲は 0～100 です。値が小さいほど、許可されるブロードキャストトラフィックが少なくなります。

pps *max-pps*: インタフェースが毎秒転送できるブロードキャストパケットの最大数を指定します。*max-pps*（pps 内）の設定範囲は、0～1.4881×インタフェース帯域幅である。

kbps *max-kbps*: Ethernet インタフェースが転送できるブロードキャストトラフィックの最大キロビット/秒を指定します。設定範囲（kbps の場合）は、0～インタフェース帯域幅です。

説明

broadcast-suppression コマンドはブロードキャスト抑制しきい値を設定し、ブロードキャスト抑制を有効にします。

undo broadcast-suppression コマンドはブロードキャスト抑制を無効にします。

ブロードキャストストーム抑制機能は、ブロードキャストトラフィックのサイズをインタフェース上のしきい値に制限します。インタフェース上のブロードキャストトラフィックがこのしきい値を超えると、トラフィックがこのしきい値を下回るまで、システムはパケットを破棄します。

storm-constrain コマンドと **broadcast-suppression** コマンドはどちらも、ポートでのブロードキャストストームを抑制できます。**broadcast-suppression** コマンドは、チップを使用してブロードキャストトラフィックを物理的に抑制します。ソフトウェアを使用してブロードキャストトラフィックを抑制する **storm-constrain** コマンドよりも、装置のパフォーマンスへの影響は少なくなります。

トラフィックの抑制結果を判定するには、インタフェースで **storm-constrain broadcast** コマンドと **broadcast-suppression** コマンドの両方を設定しないでください。

抑制しきい値を pps で設定する場合、実際の抑制しきい値は、次のように設定されたしきい値と異なる場合があります。

- 設定値が 125 より小さい場合は、125 の値が有効になります。
- 設定値が 125 より大きく 125 の倍数でない場合は、設定値より大きく、かつ最も近い 125 の倍数が有効になります。

抑制しきい値を kbps で設定する場合、実際の抑制しきい値は、次のように設定されたしきい値と異なる場合があります。

- 設定値が 64 より小さい場合は、64 の値が有効になります。
- 設定値が 64 より大きく 64 の倍数でない場合は、設定値より大きく、かつ最も近い 64 の倍数が有効になります。

無効にするしきい値については、装置のプロンプトを参照してください。

例

GigabitEthernet 1/0/1 のブロードキャスト抑制しきい値を 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.

この出力では、チップがサポートしているのはステップ 64 だけなので、有効な値は 10048kbps(64 の 157 倍）です。

関連コマンド

- **multicast-suppression**
- **unicast-suppression**

1.1.2 combo enable

Syntax

combo enable { **auto** | **copper** | **fiber** }

デフォルト

v7.1.8 を含むそれ以前

copper

v7.2.16 を含むそれ以降

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auto*:* 挿入されたメディアを自動的に識別し、対応するコンボポートをアクティブにします。

copper: 銅線コンボポートをアクティブにします。この場合は、ツイストペアを使用してポートを接続します。

fiber: ファイバコンボポートをアクティブにします。この場合、光ファイバを使用してポートを接続します。

説明

combo enable コマンドはコンボインタフェースの銅線またはファイバコンボポートをアクティブにします。

コンボインタフェースは、装置パネルに 1 つのファイバコンボポートと 1 つの銅線コンボポートを物理的に含む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します。その結果、同時に作業することはできません。いずれかのポートをアクティブにすると、もう一方のポートは自動的に無効になります。銅線コンボポートまたはファイバコンボポートを選択してアクティブにできます。

このコマンドを使用する前に、装置パネルのマークに従って以下を実行してください。

- 装置のコンボインタフェースを決定します。
- 各コンボインタフェースに属する 2 つの物理インタフェースを識別します。

例

コンボインタフェース GigabitEthernet 1/0/1 の銅線コンボポートをアクティブにします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] combo enable copper

コンボインタフェース GigabitEthernet 1/0/1 のファイバコンボポートをアクティブにします。

<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** に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] description lan-interface

1.1.4 display counters

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信トラフィックの統計情報を表示します。

outbound: 送信トラフィックの統計情報を表示します。

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

説明

display counters コマンドはインタフェースのトラフィックの統計情報を表示します。

このコマンドは **flow-interval** コマンドで指定されたポートの統計情報を収集する間隔内のトラフィックの統計情報を表示します。

Ethernet インタフェースのトラフィックの統計情報を削除する場合、**reset counters interface** コマンドを使用します。詳細はコマンドマニュアルのセクション 3 *アクセス*“*Ethernet インタフェース*”の“*reset counters interface*”を参照してください。

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

すべてのインタフェースの受信トラフィック統計を表示する

<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。

フィールド	説明
Total (pkts)	インタフェースを通して送受信したパケットの総数です。
Broadcast (pkts)	インタフェースを通して送受信したブロードキャストパケットの総数です。
Multicast (pkts)	インタフェースを通して送受信したマルチキャストパケットの総数です。
Err (pkts)	インタフェースを通して送受信したエラーパケットの総数です。
Overflow: More than 14 digits (7 digits for column "Err")	以下のときに**Overflow**と表示します。 • エラーフィールド値のデータ長が10進数で7桁を超えました。 • 非エラーフィールド値のデータ長が10進数で14桁を超えました。
--: Not supported	統計情報をサポートしていません。

関連コマンド

- **flow-interval**
- **reset counters interface**

1.1.5 display counters rate

Syntax

display counters rate { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信トラフィックレートの統計情報を表示します。

outbound: 送信トラフィックレートの統計情報を表示します。

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

説明

display counters rate コマンドは最後のサンプリング間隔からの up 状態のインタフェースのトラフィックレートの統計情報を表示します。

統計情報は up 状態のインタフェースのみ適用されます。

インタフェースタイプを指定した場合、最後のサンプリング間隔からの up 状態の指定タイプ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ない場合、最後のサンプリング間隔からの up 状態の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。

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

すべてのインタフェース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                  0           0              --              --

 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におけるインタフェースの帯域幅使用率です。単位は%です。
Total (pkts/sec)	最後のサンプリング間隔の中に送受信したユニキャストパケットの平均レートです。単位はppsです。
Broadcast (pkts/sec)	最後のサンプリング間隔の中に送受信したブロードキャストパケットの平均レートです。単位はppsです。
Multicast (pkts/sec)	最後のサンプリング間隔の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。

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。

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。

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。

現在のシステム時刻と、インタフェースの物理ステータスが UP / DOWN に変更された時刻を表示します。

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。

例

レイヤ 2 インタフェース GigabitEthernet 1/0/1 の詳細情報を表示します。

```
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: 10000
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: Automdix
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Port priority: 2
Last link flapping: 6 hours 39 minutes 25 seconds
Last clearing of counters:  14:34:09 Tue 11/01/2011
 Peak input rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Peak output rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Last 300 second input:  0 packets/sec 0 bytes/sec -%
 Last 300 second output:  0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
       0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, 0 bytes
       0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
       0 CRC, 0 frame, 0 overruns, 0 aborts
       0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
       0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
```

```
Output (normal): 0 packets, 0 bytes
     0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, 0 buffer failures
     0 aborts, 0 deferred, 0 collisions, 0 late collisions
     0 lost carrier, 0 no carrier
```

表 1-3 コマンド出力

フィールド	説明
Current state	インタフェースの物理リンクの状態です。 • **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。（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**)—インタフェースが属するアグリゲートインタフェースは、**shutdown**コマンドを使用してシャットダウンしています。 • **Link-Flap DOWN**—リンクフラッピング保護機能によってインタフェースがシャットダウンされました。 • **mac-address moving down**—インタフェースはMACアドレス移動抑制機能によってシャットダウンされました。 • **MAD ShutDown**—インタフェースはIRF MADによってシャットダウンされました。この状態は、インタフェースがIRF分割後にリカバリ状態になった場合に発生します。 • **Storm-Constrain**—インタフェースがシャットダウンされています。これは、未知の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、またはブロードキャストトラフィックが上限しきい値を超えていることをStorm制御機能が検出したためです。 • **STP DOWN**—BPDUガード機能によってインタフェースがシャットダウンされました。 • **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 (DLDP DOWN)**—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。 ● **DOWN (LAGG DOWN)**—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。 ● **DOWN (OAM DOWN)**—OAMがリモートリンクの障害を検出したため、インタフェースがリンクレイヤでdownしています。 ● **DOWN (BFD)**—リンク障害を検出したため、データリンクレイヤで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アドレスが割り当てられていないため、IPパケットを処理できません。
Internet address	インタフェースのIPアドレスです。**primary**属性は、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フォーマットです。
Hardware Address	インタフェースのMACアドレスです。
IPv6 packet frame type	IPv6パケットのフレーミング形式です。
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。
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。
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。

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。
100Mbps-speed mode	インタフェースが100Mbpsで動作しています。
1000Mbps-speed mode	インタフェースが1000Mbpsで動作しています。
10Gbps-speed mode	インタフェースが10Gbpsで動作しています。
40Gbps-speed mode	インタフェースが40Gbpsで動作しています。
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の通信モードで動作しています。
full-duplex mode	インタフェースがfullの通信モードで動作しています。
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	インタフェースが**speed auto**コマンドで設定されています。
Link speed type is force link	インタフェースが**speed**コマンドで設定されています。
link duplex type is autonegotiation	インタフェースが**duplex auto**コマンドで設定されています。
link duplex type is force link	インタフェースが**duplex**コマンドで設定されています。
Flow-control is not enabled	汎用フロー制御はインタフェースで無効になっています。
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	インタフェースはジャンボフレームをサポートしています。
Broadcast MAX-	ブロードキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
Multicast MAX-	マルチキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
Unicast MAX-	ユニキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
PVID	インタフェースのポートVLANのID（PVID）です。

フィールド	説明
MDI type	ケーブルタイプです。（設定に依存します） ● 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。（設定に依存します） ● 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	ポートによってパケットを転送できるVLAN。VLANが作成されている必要があります。
VLAN permitted	ポートによってパケットが許可されているVLANです。
Trunk port encapsulation	トランクポートのカプセル化プロトコルタイプです。
Last link flapping	インタフェースで最後に物理状態の変化があった以降の時間です。**Never**はインタフェース状態が変化していないことを示します。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 seconds input: 0 packets/sec 0 bytes/sec 0% Last 300 seconds output: 0 packets/sec 0 bytes/sec 0%	過去300秒以内の平均受信または送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	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。 ユニキャストパケット、ブロードキャスト、マルチキャスト、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	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、正常なpauseフレームがカウントされます。 ユニキャストパケット、ブロードキャスト、マルチキャスト、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。

フィールド	説明
input errors	受信エラーパケットの統計情報です。
runts	不正なフォーマット、CRCが有効なフォーマットでの64バイト長未満の受信フレーム数です。
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、1518バイト（VLANタグなし）よりも長いフレームあるいは1522バイト（VLANタグつき）よりも長いフレームを示します。 ● 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
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、jabberフレームは1518バイト（VLANタグなし）あるいは1522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	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。 ユニキャストパケット、ブロードキャスト、マルチキャスト、pauseフレームの送信数です。 ハイフン（-）はサポートしてないことを示します。
Output(normal) : 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	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、正常なpauseフレームがカウントされます。 ユニキャストパケット、ブロードキャスト、マルチキャスト、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。

フィールド	説明
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	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が発生したときのピーク時における受信トラフィックのピークレートです。単位はbpsです。
Peak output rate	送信トラフィックレートが発生したときのピーク時における送信トラフィックのピークレートです。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   auto    F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaa
```

インタフェースの詳細な説明を含む、GigabitEthernet 1/0/3 に関する簡単な情報を表示します。

<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   auto    F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

DOWN 状態のインタフェースとその原因に関する情報を表示します。

<Switch> display interface brief down

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
GE1/0/1            DOWN Not connected
Vlan2              DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
GE1/0/2            DOWN Not connected
```

表 1-4 コマンド出力

フィールド	説明
Brief information on interfaces in route mode:	レイヤ3インタフェースの概要情報です。
Interface	インタフェース名です。

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しています。 ● **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。
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。
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	**description**コマンドによって設定された一部あるいは完全なインタフェースの説明です。 ● **display interface brief**コマンドで**description**が指定されていない場合、インタフェースの説明の最初の27文字のみが表示されます。 ● **display interface brief**コマンドで**description**が指定されている場合、すべてのインタフェースの説明が表示されます。
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。
Speed	インタフェースの速度（bps）です。 速度が自動的にネゴシエートされる場合、このフィールドは速度の横に（a）フラグを表示します。 インタフェースが速度を自動ネゴシエーションするように設定されていても、オートネゴシエーションが開始されていない場合、このフィールドにはautoと表示されます。
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。

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。 ● **F**—full通信モードです。 ● **F(a)**—full通信モードでオートネゴシエートされています。 ● **H**—half通信モードです。 ● **H(a)**—half通信モード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ために、**undo shutdown**コマンドを実行します。 ● **DOWN (Link-Aggregation interface down)**—アグリゲートインタフェースがシャットダウンしているとき、アグリゲートインタフェースのすべてのメンバポートの物理状態がdownです。 ● **DOWN (Loopback detection down)**—ループバック検出モジュールがループバックを検出したため、ポートがシャットダウンしています。 ● **DOWN (Monitor-Link uplink down)**—モニタリンクモジュールがアップリンクのダウンを検出したため、ポートがシャットダウンしています。 ● **MAD ShutDown**—IRFスタックの分裂後、IRFスタックの除外ポートを除くすべてのインタフェースがdownになりました。 ● **Not connected**—物理接続がありません。（ネットワークが切断された、あるいは故障している可能性があります） ● **Storm-Constrain**—不明なユニキャストトラフィック、マルチキャストトラフィック、ブロードキャストトラフィックが上限を超過したため、ポートがシャットダウンしています。 ● **STP DOWN**—STP BPDUガード機能によってポートがシャットダウンしています。 ● **Port Security Disabled**—ポートが不正なパケットを受信したため、侵入検出機能によってポートがシャットダウンしています。 ● **Standby**—Standby状態のバックアップインタフェースです。

関連コマンド

reset counters interface

1.1.7 duplex

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auto: ピアとの通信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 full 通信モード（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 half 通信モード（半 2 重モード）に設定します。ファイバポート、1000Mbps Ethernet インタフェース、および 10000Mbps Ethernet インタフェースはこのキーワードをサポートしていません。

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。

デュプレックスモードは接続する装置と同じ設定にしてください。

例

GigabitEthernet 1/0/1 を full 通信モードに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] duplex full

1.1.8 eee enable

重要:

ファイバポートはこのコマンドをサポートしていません。

Syntax

eee enable

undo eee enable

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

eee enable コマンドは 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。

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。

flow-control コマンドが設定されると、インタフェースでフローコントロールのフレームの送受信を行うことができます。

- 混雑したとき、インタフェースはピアにフローコントロールのフレームを送信します。
- ピアからフローコントロールの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。

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 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]

1.1.12 jumboframe enable

Syntax

jumboframe enable [*size*]

undo jumboframe enable [*size*]

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

size: 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。値は偶数の整数である必要があります。

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。

undo jumboframe enable *size* コマンドはデフォルトに戻します。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

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

1.1.13 link-delay

Syntax

v7.1.8 を含むそれ以前

link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]
undo link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

v7.2.16 を含むそれ以降

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

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

デフォルト

ポートの物理リンクが **up** または **down** するたびに、インタフェースは変更を即座に CPU に報告します。

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

v7.1.8 を含むそれ以前

msec: 物理状態の変更を抑制する間隔をミリ秒単位で有効にします。指定しない場合、抑制間隔は秒単位の精度です。

delay-time: インタフェースで物理状態の変更を抑制する間隔を設定します。0 に設定すると、インタフェースは物理状態の変更があったときに、すぐに CPU に通知し、抑制しません。

- **msec** キーワードを指定しない場合、値の範囲は 0～120 秒です。
- **msec** キーワードを指定する場合、値の範囲は 0～10000 ミリ秒で、値は 100 の倍数にする必要があります。

mode up: リンクアップイベントを抑制します。

mode updown: リンクアップイベントとリンクダウンイベントの両方を抑制します。

v7.2.16 を含むそれ以降

down: リンクダウンイベントを抑制します。

up: リンクアップイベントを抑制します。

msec: 物理状態の変更を抑制する間隔をミリ秒単位で有効にします。指定しない場合、抑制間隔は秒単位の精度です。

delay-time: インタフェースで物理状態の変更を抑制する間隔を設定します。0 に設定すると、インタフェースは物理状態の変更があったときに、すぐに CPU に通知し、抑制しません。

- **msec** キーワードを指定しない場合、値の範囲は 0～120 秒です。
- **msec** キーワードを指定する場合、値の範囲は 0～10000 ミリ秒で、値は 100 の倍数にする必要があります。

説明

link-delay コマンドは Ethernet インタフェースの物理状態の変更を抑制する間隔を設定します。

undo link-delay コマンドはデフォルトに戻します。

v7.1.8 を含むそれ以前

この機能を設定すると、リンクダウンイベントのみ、リンクアップイベントのみ、またはその両方を抑制するように設定できます。

指定したタイプのイベントが抑制期間の終了時にも存在する場合は、そのイベントがレポートされます。

この機能を設定するときは、次のガイドラインに従ってください。

- リンクダウンイベントのみを抑制するには、**link-delay** [**msec**] *delay-time* コマンドを設定します。
- リンクアップイベントのみを抑制するには、**link-delay** [**msec**] *delay-time* **mode up** コマンドを設定します。
- リンクダウンイベントとリンクアップイベントの両方を抑制するには、**link-delay** [**msec**] *delay-time* **mode updown** コマンドを設定します。

インタフェースでは、リンクアップイベントとリンクダウンイベントに対して異なる抑制間隔を設定できます。リンクアップまたはリンクダウンイベントに対して **link-delay** 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。

RRPP、スパニングツリープロトコル、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。

v7.2.16 を含むそれ以降

この機能を設定すると、リンクダウンイベントのみ、リンクアップイベントのみ、またはその両方を抑制するように設定できます。

指定したタイプのイベントが抑制期間の終了時にも存在する場合は、そのイベントがレポートされます。

この機能を設定するときは、次のガイドラインに従ってください。

- リンクダウンイベントを抑制するには、**link-delay down** コマンドを設定します。
- リンクアップイベントを抑制するには、**link-delay up** コマンドを設定します。

インタフェースでは、リンクアップイベントとリンクダウンイベントに対して異なる抑制間隔を設定できます。インタフェースで **link-delay** コマンドを複数回実行する場合は、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は別々に設定できます。
- リンクアップイベントまたはリンクダウンイベントについて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。

RRPP、スパニングツリープロトコル、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。

例

v7.1.8 を含むそれ以前

GigabitEthernet 1/0/1 のリンクダウンイベント抑制間隔を 8 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] link-delay 8

GigabitEthernet 1/0/1 のリンクアップイベント抑制間隔を 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 msec 800 mode up

v7.2.16 を含むそれ以降

GigabitEthernet 1/0/1 のリンクダウンイベント抑制間隔を 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 のリンクアップイベント抑制間隔を 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

1.1.14 loopback

重要:

Ethernet インタフェースでループバックテストを有効にすると、インタフェースはデータトラフィックを転送しません。

Syntax

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

undo loopback

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

external: Ethernet インタフェースの外部ループバックテストを実行します。

internal: Ethernet インタフェースの内部ループバックテストを実行します。

説明

loopback コマンドは Ethernet インタフェースでループバックテストを有効にします。

undo loopback コマンドは Ethernet インタフェースでループバックテストを無効にします。

Ethernet インタフェースでループバックテストを有効にすると、Ethernet インタフェースは全二重モードに切り替わります。ループバックテストを無効にすると、Ethernet インタフェースはデュプレックス設定に戻ります。

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実行します。

Ethernet インタフェースが正常に動作しないとき、問題を識別するため、ループバックテストを実行することができます。

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**、**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実行します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] loopback internal

1.1.15 multicast-suppression

Syntax

multicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo multicast-suppression

デフォルト

Ethernet インタフェースでは、マルチキャストトラフィックは抑制されません。

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: マルチキャスト抑制しきい値をインタフェース帯域幅のパーセンテージで設定します。設定範囲は 0～100 です。値が小さいほど、通過できるマルチキャストトラフィックが少なくなります。

pps *max-pps*: インタフェースが毎秒転送できるマルチキャストパケットの最大数を指定します。*max-pps*（pps 内）の設定範囲は、0～1.4881×インタフェース帯域幅である。

kbps *max-kbps*: Ethernet インタフェースが転送できるマルチキャストトラフィックの最大キロビット/秒を指定します。設定範囲（kbps の場合）は、0 からインタフェース帯域幅です。

説明

multicast-suppression コマンドはマルチキャストストーム抑制を有効にし、マルチキャストストーム抑制しきい値を設定します。

undo multicast-suppression コマンドはマルチキャストストーム抑制を無効にします。

マルチキャストストーム抑制機能は、マルチキャストトラフィックのサイズをインタフェースのしきい値に制限します。インタフェース上のマルチキャストトラフィックがこのしきい値を超えると、トラフィックがこのしきい値を下回るまで、システムはパケットを破棄します。

storm-constrain コマンドと **multicast-suppression** コマンドはどちらも、ポートでのマルチキャストストームを抑制できます。マルチキャスト抑制コマンドは、チップを使用してマルチキャストトラフィックを物理的に抑制します。ソフトウェアを使用してマルチキャストトラフィックを抑制する **storm-constrain** コマンドよりも、装置のパフォーマンスへの影響は少なくなります。

トラフィックの抑制結果を判定するには、インタフェースで **storm-constrain multicast** コマンドと **multicast-suppression** コマンドの両方を設定しないでください。

抑制しきい値を pps で設定する場合、実際の抑制しきい値は、次のように設定されたしきい値と異なる場合があります。

- 設定値が 125 より小さい場合は、125 の値が有効になります。
- 設定値が 125 より大きく 125 の倍数でない場合は、設定値より大きく、かつ最も近い 125 の倍数が有効になります。

抑制しきい値を kbps で設定する場合、実際の抑制しきい値は、次のように設定されたしきい値と異なる場合があります。

- 設定値が 64 より小さい場合は、64 の値が有効になります。
- 設定値が 64 より大きく 64 の倍数でない場合は、設定値より大きく、かつ最も近い 64 の倍数が有効になります。

有効な抑制しきい値を決定するには、スイッチのプロンプト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.

この出力では、チップがサポートしているのはステップ 64 だけなので、有効な値は 10048kbps（64 の 157 倍）です。

関連コマンド

- **broadcast-suppression**
- **unicast-suppression**

1.1.16 port auto-power-down

重要:

ファイバポートはこのコマンドをサポートしていません。

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 Ethernet インタフェースで自動電源切断を有効にします。

undo port auto-power-down コマンドは Ethernet インタフェースで自動電源切断を無効にします。

自動電源切断が有効のインタフェースが特定の期間ダウンしていた場合、次の両方のイベントが発生します。

- インタフェースへの電力供給が自動的に停止します。
- インタフェースが省電力モードに入ります。

期間はチップの仕様によって異なり、設定することはできません。

インタフェースが起動すると、次の両方のイベントが発生します。

- 装置はインタフェースへの電源供給を自動的に回復します。
- インタフェースが正常な状態に戻ります。

例

GigabitEthernet 1/0/1 で自動電源切断を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port auto-power-down

1.1.17 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。

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**
- **display counters interface**
- **display counters rate interface**

1.1.18 shutdown

Syntax

shutdown

undo shutdown

デフォルト

Ethernet 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。

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

1.1.19 speed

Syntax

speed { **10** | **100** | **1000** | **10000** | **40000** | **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。マネジメントポートのみサポートします。

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。

10000: インタフェースの通信速度を 10000Mbps に設定します。

40000: インタフェースの通信速度を 40000Mbps 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。

Ethernet 銅線ポートの場合は、**speed** コマンドを使用して、ピアインタフェースの速度に一致するように速度を設定します。

ファイバポートの場合は、**speed** コマンドを使用して、トランシーバモジュールのレートに一致するようにポートの速度を設定します。

キーワードに対するインタフェースのサポートは、インタフェースの種類によって異なります。詳細については、interface view で **speed ?**コマンドを使用してください。

LSWM4SP2PM または LSWM2XGT2PM インタフェースカードがスイッチに取り付けられている場合、カード上のインタフェースは 10 Gbps でしか動作できません。

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

1.1.20 unicast-suppression

Syntax

unicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo unicast-suppression

デフォルト

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: 未知のユニキャスト抑制しきい値をインタフェース帯域幅のパーセンテージとして設定します。設定範囲は 0～100 です。値が小さいほど、通過できる未知のユニキャストトラフィックが少なくなります。

pps *max-pps*: インタフェースが 1 秒あたりに転送できる未知のユニキャストパケットの最大数を指定します。*max-pps*（pps 内）設定範囲は、0～1.4881×インタフェース帯域幅です。

kbps *max-kbps*: Ethernet インタフェースが 1 秒あたりに転送できる未知のユニキャストトラフィックの最大キロビット数を指定します。設定範囲（kbps の場合）は、0～インタフェース帯域幅です。

説明

unicast-suppression コマンドは未知のユニキャストストーム抑制を有効にし、未知のユニキャストストーム抑制しきい値を設定します。

undo unicast-suppression コマンドは未知のユニキャストストーム抑制を無効にします。

未知のユニキャストストーム抑制機能は、未知のユニキャストトラフィックのサイズをインタフェースのしきい値に制限します。インタフェース上の未知のユニキャストトラフィックがこのしきい値を超えると、システムは未知のユニキャストトラフィックがこのしきい値を下回るまでパケットを破棄します。

storm-constrain コマンドと **unicast-suppression** コマンドはどちらも、ポートでの不明なユニキャストストームを抑制できます。ユニキャスト抑制コマンドは、チップを使用して未知のユニキャストトラフィックを物理的に抑制します。ソフトウェアを使用して未知のユニキャストトラフィックを抑制する **storm-constrain** コマンドよりも、装置のパフォーマンスへの影響は少なくなります。

未知のユニキャストインタフェース抑制の結果を判定するには、トラフィックで **storm-constrain unicast** コマンドと **unicast-suppression** コマンドの両方を設定しないでください。

抑制しきい値を pps で設定する場合、実際の抑制しきい値は、次のように設定されたしきい値と異なる場合があります。

- 設定値が 125 より小さい場合は、125 の値が有効になります。
- 設定値が 125 より大きく 125 の倍数でない場合は、設定値より大きく、かつ最も近い 125 の倍数が有効になります。

抑制しきい値を kbps で設定する場合、実際の抑制しきい値は、次のように設定されたしきい値と異なる場合があります。

- 設定値が 64 より小さい場合は、64 の値が有効になります。
- 設定値が 64 より大きく 64 の倍数でない場合は、設定値より大きく、かつ最も近い 64 の倍数が有効になります。

有効な抑制しきい値を決定するには、スイッチのプロンプトを参照してください。

例

GigabitEthernet 1/0/1 で、未知のユニキャストストーム抑制しきい値を 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.
```

この出力では、チップがサポートしているのはステップ 64 だけなので、有効な値は 10048kbps（64 の 157 倍）です。

関連コマンド

- **broadcast-suppression**
- **multicast-suppression**

1.1.21 using fortygige

Syntax

using fortygige

undo using fortygige

デフォルト

10-GE ブレークアウトインタフェースは分割されておらず、1 つのインタフェースとして動作します。

View

10-GE breakout interface view

定義済みユーザロール

network-admin

説明

using fortygige コマンドは 4 つの 10-GE に分割されたインタフェースを 40-GE インタフェースに統合します。

undo using fortygige コマンドは設定をキャンセルします。

広い帯域が必要な場合、40GE インタフェースを 4 つの 10GE に分割したインタフェースを 40GE インタフェースに結合することができます。4 つの 10GE インタフェースでこのコマンドを有効にするには、10GE インタフェース内の 1 つでこのコマンドを実行してください。装置を再起動する前に、**save** コマンドを実行する必要があります。

例

10GE に分割された Ten-GigabitEthernet 1/1/1:1 から Ten-GigabitEthernet 1/1/1:4 を 40GE インタフェースに結合します。

<Switch> system-view

[Switch] interface ten-gigabitethernet1/1/1:1

[Switch-Ten-GigabitEthernet1/1/1:1] using fortygige

```
The interfaces Ten-GigabitEthernet1/1/1:1 through Ten-GigabitEthernet1/1/1:4
will be deleted. Continue? [Y/N]:y
```

関連コマンド

using tengige

1.1.22 using tengige

Syntax

using tengige

undo using tengige

デフォルト

インタフェースは分割されず、１つのインタフェースとして動作します。

View

40-GE interface view

定義済みユーザロール

network-admin

説明

using tengige コマンドは 40GE インタフェースを複数の 10GE に分割します。

undo using tengige コマンドは設定をキャンセルします。

ポート密度を向上させ、コストを削減し、ネットワークの柔軟性を向上させるために、広帯域幅インタフェースを複数の 10 GE ブレークアウトインタフェースに分割できます。

例:

- 40-GE インタフェース FortyGigE 1/1/1 を、Ten-GigabitEthernet 1/1/1:1 から Ten-GigabitEthernet 1/1/1:4 までの 4 つの 10-GE ブレークアウトインタフェースに分割します。

10-GE ブレークアウトインタフェースは、番号の付け方が異なることを除いて、一般的な 10-GE インタフェースと同じ設定と属性をサポートします。装置を再起動する前に、**save** コマンドを実行する必要があります。

例

40GE インタフェース FortyGigE 1/1/1 を 4 つの 10GE インタフェースに分割します。

<Switch> system-view

[Switch] interface fortygige 1/1/1

[Switch-FortyGigE1/1/1] using tengige

```
The interface FortyGigE 1/1/1 will be deleted. Continue? [Y/N]:y
```

関連コマンド

using fortygige

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。このオプションを指定しない場合、このコマンドはすべてのストームコントロール対応インタフェースのストームコントロール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、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。

例

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を表示します。

<Switch> display storm-constrain

```
Abbreviation: BC - broadcast; MC - multicast; UC - unicast
            KNUC - known unicast; FW - forwarding
Flow Statistic Interval: 5 (in seconds)
Port         Type Lower    Upper    Unit CtrlMode Status   Trap Log SwitchNum
------------------------------------------------------------------------------
```

```
GE1/0/1      MC   100      200      kbps shutdown shutdown off  on  10
```

表 1-5 コマンド出力

フィールド	説明
Flow Statistic Interval	ストーム抑止モジュールのトラフィックポーリング間隔です。単位は秒です。
Port	省略されたポート名です。
Type	ストーム抑止機能が有効なトラフィックタイプです。 ● **BC**—ブロードキャストパケットです。 ● **MC**—マルチキャストパケットです。 ● **UC**—不明なユニキャストパケットです。 ● **KNUC**–既知のユニキャストパケットです。このフィールドは、QX-S5300Gシリーズではサポートしていません。
Lower	ストーム抑止の下限値です。単位はpps、kbps、%です。
Upper	ストーム抑止の上限値です。単位はpps、kbps、%です。
Unit	ストーム抑止のしきい値の単位です。 ● ppsです。 ● kbpsです。 ● %です。
CtrlMode	上限に到達したときの保護動作です。（blockあるいはshutdown） 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ます。 ● **shutdown**—ポートがシャットダウンです。 ● **block**—ポートがトラフィックのタイプを廃棄します。
Trap	ストーム抑止がしきい値に到達した際のトラップの状態です。 ● **on**—ポートはしきい値イベントをトラップします。 ● **off**—ポートはしきい値イベントをトラップしません。
Log	ストーム抑止がしきい値に到達した際のログの状態です。 ● **on**—ポートはしきい値イベントをログに保存します。 ● **off**—ポートはしきい値イベントをログに保存しません。
SwitchNum	インタフェースの転送状態の変更回数です。 カウントが65535に到達したとき、自動でリセットされます。

1.2.2 mdix-mode

> ⚠ **重要:**
>
> ファイバポートはこのコマンドをサポートしていません。

Syntax

mdix-mode { **automdix** | **mdi**| **mdix** }

undo mdix-mode

デフォルト

Ethernet インタフェースは **automdix** モードで動作します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

automdix: インタフェースが相手とピンの役割をネゴシエートするように指定します。

mdi: ピン 1 とピン 2 が送信ピンで、ピン 3 とピン 6 が受信ピンであることを指定します。

mdix: ピン 1 とピン 2 が受信ピンで、ピン 3 とピン 6 が送信ピンであることを指定します。

説明

mdix-mode コマンドは Ethernet インタフェースの Medium Dependent Interface Cross-Over(MDIX)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 または 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: 速度自動ネゴシエーションのオプションとして 10 Mbps を設定します。

100: 速度自動ネゴシエーションのオプションとして 100 Mbps を設定します。

1000: 速度自動ネゴシエーションのオプションとして 1000 Mbps を設定します。

説明

speed auto コマンドは速度自動ネゴシエーションのオプションを設定します。

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** コマンドは互いに優先します。設定した最新のコマンドが有効になります。

例：

- インタフェースで **speed auto 100 1000** を設定してから **speed 100** を設定すると、インタフェースの速度は強制的に 100 Mbps に設定されます。
- インタフェースで **speed 100** を設定してから **speed auto 100 1000** を設定すると、インタフェースはピアとの速度ネゴシエーションを行います。ネゴシエートされる速度は、100 Mbps または 1000 Mbps です。

速度自動ネゴシエーションにより、Ethernet インタフェースからネゴシエートへのピアとの間で、両端でサポートされる最高速度を実現できます。ネゴシエーションの速度オプションリストを絞り込むことができます。ネゴシエーション障害を回避するには、両端で最低 1 つの速度オプションがサポートされていることを確認してください。

例

速度ネゴシエーションに 10Mbps と 1000Mbps を使用するように GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] 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、既知のユニキャスト、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** を指定した場合、*upperlimit* の設定範囲は、1～1.4881×インタフェース帯域幅（kbps）になります。
  例えば、インタフェース帯域幅が 1 Gbps (1,000,000 kbps) の場合、この設定で制御できる範囲は 1 ～ 1.4881 × 1,000,000 kbps = 1 ～ 1,488,100 pps です。
  例えば、インタフェース帯域幅が 10 Gbps (10,000,000 kbps) の場合、この設定で制御できる範囲は 1 ～ 1.4881 × 10,000,000 kbps = 1 ～ 14,881,000 pps です。

例えば、インタフェース帯域幅が 40 Gbps (40,000,000 kbps) の場合、この設定で制御できる範囲は 1 ～ 1.4881 × 40,000,000 kbps = 1 ～ 59,524,000 pps です。

- **kbps** を指定した場合は、*upperlimit* の設定範囲は、1～インタフェース帯域幅になります。
- **ratio** を指定した場合、上限引数の設定範囲は 1～100 です。

lowerlimit: 下限のしきい値を指定します。単位は pps、kbps、%です。

- **pps** を指定した場合、*lowerlimit* の設定範囲は、1～1.4881×インタフェース帯域幅（kbps）になります。
  例えば、インタフェース帯域幅が 1 Gbps (1,000,000 kbps) の場合、この設定で制御できる範囲は 1 ～ 1.4881 × 1,000,000 kbps = 1 ～ 1,488,100 pps です。
  例えば、インタフェース帯域幅が 10 Gbps (10,000,000 kbps) の場合、この設定で制御できる範囲は 1 ～ 1.4881 × 10,000,000 kbps = 1 ～ 14,881,000 pps です。
  例えば、インタフェース帯域幅が 40 Gbps (40,000,000 kbps) の場合、この設定で制御できる範囲は 1 ～ 1.4881 × 40,000,000 kbps = 1 ～ 59,524,000 pps です。
- **kbps** を指定した場合、*lowerlimit* の設定範囲は 1～インタフェース帯域幅までです。
- **ratio** を指定した場合、*lowerlimit* の設定範囲は 1～100 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**

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、10 秒より短いトラフィックポーリング間隔は使用しないでください。

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、ファイバポートでは使用できません。
10M および 100M までのポートリンクではサポートされていません。

Syntax

virtual-cable-test

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

virtual-cable-test コマンドは Ethernet インタフェースのケーブル接続をテストし、テスト結果を表示します。

テスト結果は参照用です。ケーブル長検出誤差は 5m（約 16 フィート）以内です。

テスト項目がない場合は、ハイフン（-）が表示されます。

例

GigabitEthernet 1/0/1 のケーブル接続をテストします

<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**—ケーブルの状態は良好です。 ● **Abnormal**—ケーブルに異常があります。 ● **Abnormal (open)**—オープン回路が検出されました。 ● **Abnormal (short)**—短絡が検出されました。 ● **Failure**—テストに失敗しました。
n metre(s)	ケーブル接続が正常に機能している場合、このフィールドにはケーブルの全長が表示されます。 ケーブル接続に失敗した場合、このフィールドにはローカルポートから障害点までの長さが表示されます。

目次

このセクションのページは **3-x-x** です。

2 章 ループバックインタフェースと Null インタフェース 2-1
2.1 ループバックインタフェースと Null インタフェース設定コマンド.....2-1
2.1.1 description.....2-1
2.1.2 display interface loopback.....2-2
2.1.3 display interface null.....2-5
2.1.4 interface loopback.....2-6
2.1.5 interface null.....2-7
2.1.6 reset counters interface loopback.....2-8
2.1.7 reset counters interface null.....2-9
2.1.8 shutdown.....2-9

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

loopback *interface-number*：ループバックインタフェースを番号で指定します。これは、デフォルトのループバックインタフェースの番号にすることができます。指定しない場合、コマンドは装置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、あるいはすべてのデフォルト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。
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。
Maximum transmission unit	インタフェースのMTUです。
Internet protocol processing: disabled	レイヤ3パケットを処理できないインタフェースを示します。（インタフェースにIPアドレスが設定されていないときに表示されます。）
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、アドレスがプライマリIPアドレスであることを示します。
Physical: Loopback	インタフェースの物理タイプがループバックです。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最新の300秒の平均受信レートです。 ● **bytes/sec**—1秒間に受信した平均バイト数です。 ● **bits/sec**—1秒間に受信した平均ビット数です。 ● **packets/sec**—1秒間に受信した平均パケット数です。

フィールド	説明
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最新の300秒の平均送信レートです。 ● **bytes/sec**—1秒間に送信した平均バイト数です。 ● **bits/sec**—1秒間に送信した平均ビット数です。 ● **packets/sec**—1秒間に送信した平均パケット数です。
Input: 0 packets, 0 bytes, 0 drops	インタフェースの受信パケットの総数とサイズ（単位はバイトです）と廃棄したパケット数です。
Output: 0 packets, 0 bytes, 0 drops	インタフェースの送信パケットの総数とサイズ（単位はバイトです）と廃棄したパケット数です。

すべてのループバックインタフェースの概要情報を表示します。

<Switch> display interface loopback brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP       Description
Loop1              UP   UP(s)    --            forLAN1
```

down 状態のすべてのループバックインタフェースの情報と原因を表示します。

<Switch> display interface loopback brief down

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
Loop1              ADM  Administratively
```

表 2-2 コマンド出力

フィールド	説明
Link	インタフェースの物理リンク状態です。 ● **UP**—リンクがupです。 ● **DOWN**—リンクが物理的にdownしています。 ● **ADM**—リンクが運用上でシャットダウンしています。物理状態を回復するために、**undo shutdown**コマンドを実行します。 ● **Stby**—インタフェースがstandbyインタフェースです。
Protocol	インタフェースのデータリンク層プロトコル状態です。常に**UP(s)**です。**UP(s)**は、インタフェースのデータリンクレイヤプロトコルがアップしているが、リンクがオンデマンドリンクであるか存在しないことを表します。**(s)**属性はなりすましフラグを表します。この値は、ヌルインタフェースおよびループバックインタフェースによく見られます。

フィールド	説明
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 インタフェースの番号は常に 0 です。

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とその原因に関する情報を表示します。指定しない場合、すべての状態のインタフェースの情報が表示されます。

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。

null が指定されない場合、装置のすべてのインタフェースの情報を表示します。

null が指定され、**0** が指定されない場合、Null 0 インタフェースの情報を表示します。これは Null インタフェースには Null 0 のみであるためです。

例

Null 0 インタフェースの詳細情報を表示します。

<Switch> display interface null 0

```
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Null 0 インタフェースの概要情報を表示します。

<Switch> display interface null 0 brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP       Description
NULL0              UP   UP(s)    --
```

コマンド出力は表 2-1 と表 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。

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、以下のことができます。

- 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します。

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。*interface-number* を指定しない場合、このコマンドはすべて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、あるいはすべてのデフォルトのループバックインタフェースの統計情報を削除します。

一定期間、ループバックインタフェースのトラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除するために **reset counters interface** [**loopback** [*interface-number*]]コマンドを使用します。その後、自動で統計情報を収集します。

このコマンドは少なくとも 1 つのループバックインタフェースが作成されている場合のみ有効です。

例

ループバックインタフェース 1 の統計情報を削除します。

<Switch> reset counters interface loopback 1

関連コマンド

display interface loopback

2.1.7 reset counters interface null

Syntax

reset counters interface null [**0**]

View

User view

定義済みユーザロール

network-admin

パラメータ

0 : Null 0 インタフェースを指定します。Null インタフェースの番号は常に 0 です。

説明

reset counters interface null コマンドは Null インタフェースの統計情報を削除します。

一定期間、Null インタフェースのトラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除するために **reset counters interface** [**null** [**0**]]コマンドを使用します。その後、自動で統計情報を収集します。

例

Null 0 インタフェースの統計情報を削除します。

<Switch> reset counters interface null 0

関連コマンド

display interface null

2.1.8 shutdown

Syntax

shutdown

undo shutdown

デフォルト

up

View

Loopback interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはループバックインタフェースをシャットダウンします。

undo shutdown コマンドはループバックインタフェースを up にします。

このコマンドはインタフェースの接続を切断し、通信を行うためのインタフェースを無効にするため、**shutdown** コマンドを使用する際には影響を考慮してください。

例

ループバックインタフェース 1 をシャットダウンします。

<Switch> system-view

[Switch] interface loopback 1

[Switch-LoopBack1] shutdown

目次

このセクションのページは **3-x-x** です。

3 章 Interface range 3-1
3.1 Interface range 設定コマンド 3-1
3.1.1 display interface range 3-1
3.1.2 interface range 3-2
3.1.3 interface range name 3-3

3章 Interface range

3.1 Interface range設定コマンド

3.1.1 display interface range

Syntax

display interface range [**name** *name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *name*: インタフェースレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。指定しない場合、**interface range name** コマンドで作成されたインタフェースレンジの情報を表示します。

説明

display interface range コマンドは **interface range name** コマンドを使用して作成されたインタフェースレンジの情報を表示します。

例

interface range name コマンドを使用して作成されたすべての既存のインタフェースレンジの情報を表示します。

<Switch> display interface range

```
Interface range name t2 GigabitEthernet1/0/1 GigabitEthernet1/0/2
Interface range name test GigabitEthernet1/0/3 GigabitEthernet1/0/4
```

出力は以下のことを示します。

- インタフェースレンジ **t2** に GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 が追加されました。
- インタフェースレンジ **test** に GigabitEthernet 1/0/3 と GigabitEthernet 1/0/4 が追加されました。

関連コマンド

interface range name

3.1.2 interface range

Syntax

interface range *interface-list*

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切り、24 までインタフェースを指定するか、インタフェースの範囲を指定します。インタフェースの範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。*interface-type interface-number1* **to** *interface-type interface-number2* を指定したとき、*interface-number2* は *interface-number1* 以上の値にしてください。

説明

interface range コマンドはインタフェースレンジを作成し、interface range view に移行します。同じ機能を 1 つずつインタフェースに設定する代わりに、interface range view に移行して、複数のインタフェースをまとめて実行することができます。たとえば、インタフェースの範囲をシャットダウンするため、interface range view で **shutdown** コマンドを実行します。

interface range 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。

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コマンドの実行に失敗した場合、他のメンバインタフェースで実行されません。最初に指定したインタフェースではないインタフェースで、コマンドの実行に失敗した場合、システムは system view でコマンドを実行します。

interface range view でコマンド実行後、以下のいずれかの状態がおこるかもしれません。

- システムは interface range view にとどまり、エラーメッセージを表示しません。それは、すべてのメンバインタフェースで実行が成功したことを意味します。
- 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 コマンドにて、それぞれのメンバインタフェースの interface view における設定を確認することができます。また、system view での設定が不要な場合、設定を取り消すために **undo** コマンドを使用してください。

インタフェースレンジの最初に指定したインタフェースの設定を確認する場合、interface range view で **display this** コマンドを実行します。

インタフェースレンジの設定を行う場合、以下のガイドラインに従ってください。

- インタフェース範囲の最初のインタフェースとして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 interface view に入ることが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 までのインタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[Switch-if-range] shutdown
```

3.1.3 interface range name

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name: インタフェースレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

interface-list: インタフェースを指定します。半角スペースで区切り、24 までインタフェースを指定するか、インタフェースの範囲を指定します。インタフェースの範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。*interface-type interface-number1* **to** *interface-type interface-number2* を指定したとき、*interface-number2* は *interface-number1* 以上の値にしてください。

説明

interface range name *name* **interface** *interface-list* コマンドはインタフェースレンジを作成し、インタフェースレンジの名前を設定し、interface range view に移行します。

interface 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 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。最初に指定したインタフェースは **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 でコマンド実行後、以下のいずれかの状態がおこるかもしれません。

- システムは interface range view にとどまり、エラーメッセージを表示しません。それは、すべてのメンバインタフェースで実行が成功したことを意味します。
- 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 コマンドにて、それぞれのメンバインタフェースの interface view における設定を確認することができます。また、system view での設定が不要な場合、設定を取り消すために **undo** コマンドを使用してください。

インタフェースレンジの最初に指定したインタフェースの設定を確認する場合、interface range view で **display this** コマンドを実行します。

インタフェースレンジのメンバインタフェースを表示する場合、**display interface range** コマンドを使用します。

インタフェースレンジの設定を行う場合、以下のガイドラインに従ってください。

- インタフェース範囲の最初のインタフェースとして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 interface view に入ることが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することを推奨します。

例

GigabitEthernet 1/0/1 から GigabitEthernet 1/0/5 までをンタフェースレンジ **myEthPort** に追加し、interface range view に移行します。

<Switch> system-view

[Switch] interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/5

[Switch-if-range-myEthPort]

インタフェースレンジ **myEthPort** の view に移行します。

<Switch> system-view

[Switch] interface range name myEthPort

[Switch-if-range-myEthPort]

関連コマンド

display interface range

目次

このセクションのページは **3-x-x** です。

4 章 MAC アドレステーブル 4-1
4.1 MAC アドレステーブル設定コマンド 4-1
4.1.1 display mac-address 4-1
4.1.2 display mac-address aging-time 4-3
4.1.3 display mac-address mac-learning 4-4
4.1.4 display mac-address mac-move 4-5
4.1.5 display mac-address statistics 4-7
4.1.6 mac-address (interface view) 4-8
4.1.7 mac-address (system view) 4-10
4.1.8 mac-address mac-learning enable 4-12
4.1.9 mac-address mac-move fast-update 4-14
4.1.10 mac-address max-mac-count 4-14
4.1.11 mac-address max-mac-count enable-forwarding 4-15
4.1.12 mac-address mac-roaming enable 4-16
4.1.13 mac-address notification mac-move 4-17
4.1.14 mac-address notification mac-move suppression (interface view) 4-19
4.1.15 mac-address notification mac-move suppression (system view) 4-20
4.1.16 mac-address static source-check enable 4-21
4.1.17 mac-address timer 4-22
4.1.18 snmp-agent trap enable mac-address 4-23

4章 MAC アドレステーブル

本章はスタティック MAC アドレスエントリ、ダイナミック MAC アドレスエントリ、ブラックホール MAC アドレスエントリ、マルチポートユニキャスト MAC アドレスエントリを含むユニキャスト MAC アドレスエントリの設定を示します。スタティックマルチキャスト MAC アドレスエントリの設定については、オペレーションマニュアルのセクション 6 *マルチキャスト* を参照してください。

4.1 MACアドレステーブル設定コマンド

4.1.1 display mac-address

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole** | **multiport**] [**vlan** *vlan-id*] [**count**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: MAC アドレスを指定します。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

dynamic: ダイナミック MAC アドレスエントリを表示します。

static: スタティック MAC アドレスエントリを表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

blackhole: ブラックホール MAC アドレスエントリを表示します。

multiport: マルチポートユニキャスト MAC アドレスエントリを表示します。

count: コマンドで指定したすべてのエントリに一致する MAC アドレスエントリ数のみを表示します。MAC アドレスエントリの詳細は表示されません。たとえば、VLAN 20 のダイナミックエントリ数を表示する場合、**display mac-address vlan** *20* **dynamic count** コマンドを使用します。エントリの属性が指定されない場合、MAC アドレステーブルのエントリ数を表示します。**count** を指定しない場合、指定された MAC アドレスエントリの詳細情報を表示します。

説明

display mac-address コマンドは MAC アドレスエントリを表示します。

MAC アドレスエントリは宛先 MAC アドレス、出力インタフェース、VLAN ID が含まれます。

パラメータを指定しない場合、すべての MAC アドレスエントリを表示します。

アグリゲートインタフェースに少なくとも 1 つの Selected メンバポートがある場合、アグリゲートインタフェースのダイナミック MAC アドレスエントリのみ表示します。

マルチポートユニキャスト MAC アドレスエントリは、MAC アドレスの学習には影響しません。送信元 MAC アドレスがマルチポートユニキャストエントリと一致するフレームを受信した場合、装置は引き続きフレームの MAC アドレスを学習し、ダイナミックエントリを作成できます。ただし、作成されたダイナミックエントリの優先順位は低くなります。装置は、マルチポートユニキャストエントリを使用して、エントリのアドレス宛てのフレームを転送することを優先します。

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。

フィールド	説明
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。 • **OpenFlow**— OpenFlowインスタンスのMACアドレスエントリです。OpenFlowはQX-S5300Gシリーズではサポートしていません。
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	エントリがエージングアウト可能かどうかを示します。 • **Y**—エントリはエージングアウト可能です。 • **N**—エントリはエージングアウトできません。
mac address(es) found	MACアドレスエントリに一致する数です。

関連コマンド

- **mac-address**
- **mac-address timer**

4.1.2 display mac-address aging-time

Syntax

display mac-address aging-time

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-address aging-time コマンドはダイナミック MAC アドレスエントリのエージングタイマを表示します。

例

ダイナミック MAC アドレスエントリのエージングタイマを表示します。

<Switch> display mac-address aging-time

```
MAC address aging time: 300s.
```

関連コマンド

mac-address timer

4.1.3 display mac-address 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 4-2 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。 • Enabled. • Disabled.
Port	インタフェース名です。
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。 • Enabled. • Disabled.

関連コマンド

mac-address mac-learning enable

4.1.4 display mac-address mac-move

Syntax

display mac-address mac-move [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。メンバ装置を指定しない場合、すべての IRF スタックメンバ装置の MAC アドレスの移動記録を表示します。

説明

display mac-address mac-move コマンドは装置が起動した後、MAC アドレスの移動記録を表示します。

指定された 2 つのインタフェース間で MAC アドレスの移動が発生したとき、ネットワークでレイヤ 2 でのループが発生する可能性があります。ループを検出し、位置を特定するために MAC アドレスの移動記録を表示することができます。

MAC アドレスの移動記録では、同一 MAC アドレス、VLAN、送信元ポート、現在のポートの記録が 1 つの記録として認識されます。

IRF スタックメンバ装置は、最大 200 の MAC アドレス移動レコードを作成できます。

例

スロットの MAC アドレス移動記録を表示します。

<Switch> display mac-address mac-move slot 1

```
MAC address    VLAN Current port  Source port   Last time          Times
0000-0001-002c 1    GE1/0/1      GE1/0/2      2013-05-20 13:40:52 1
0000-0001-002c 1    GE1/0/2      GE1/0/1      2013-05-20 13:41:30 1
---  2 MAC address moving records found  ---
```

#すべてのスロットの MAC アドレス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 4-3 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

4.1.5 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:                     32768
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 4-4 コマンド出力

フィールド	説明
Dynamic Unicast Address (Learned) Count	パケットによって発生したダイナミックユニキャストMACアドレスエントリ数です。
Dynamic Unicast Address (Security-service-defined) Count	セキュリティサービスによって発生したダイナミックユニキャストMACアドレスエントリ数です。
Static Unicast Address (User-defined) Count	ユーザによって追加されたスタティックユニキャストMACアドレスエントリ数です。

フィールド	説明
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。

4.1.6 mac-address (interface view)

Syntax

mac-address { **dynamic** | **multiport** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **multiport** | **static** } *mac-address* **vlan** *vlan-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface/Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

dynamic: ダイナミック MAC アドレスエントリを指定します。

static: スタティック MAC アドレスエントリを指定します。

multiport: マルチポート MAC アドレスエントリを指定します。宛先 MAC アドレスがマルチポートユニキャスト MAC アドレスエントリにマッチするフレームは複数のポートに送信されます。

mac-address: MAC アドレスを指定します。マルチキャスト MAC アドレスとすべてが 0 の MAC アドレスを除きます。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: 指定されたインタフェースが所属する既存の VLAN ID を指定します。設定範囲は 1～4094 です。

説明

mac-address コマンドはインタフェースの MAC アドレスエントリを追加あるいは修正します。

undo mac-address コマンドはインタフェースの MAC アドレスエントリを削除します。

一般的に、装置は自動で各インタフェースの受信フレームの送信元 MAC アドレスによって学習された MAC アドレステーブルを構築します。しかし、手動でスタティック MAC アドレスエントリを設定することができます。手動で設定されたスタティック MAC アドレスエントリはダイナミック MAC アドレスエントリよりも優先されます。インタフェースに接続されたユーザの装置のセキュリティを向上するため、ユーザの装置をインタフェースに関連づけるため、スタティックエントリを設定します。ユーザの装置（たとえばホスト A）のフレームは常にインタフェースから送信されます。ホスト A の偽の MAC アドレスを使用するほかのホストはホスト A からのフレームを取得することができません。

MAC アドレスエントリの設定は、設定を保存しないと、再起動により削除されます。ただしダイナミック MAC アドレスエントリは設定の保存に関わらず、再起動により削除されます。

例

VLAN 2 に所属する GigabitEthernet 1/0/1 に MAC アドレス 000f-e201-0101 のスタティック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 1/0/1 に 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。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1

VLAN 2 に所属する GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 で MAC アドレス 0001-0001-0101 のマルチポートユニキャスト MAC アドレスエントリを追加します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address multiport 0001-0001-0101 vlan 2

[Switch-GigabitEthernet1/0/1] quit

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] mac-address multiport 0001-0001-0101 vlan 2

関連コマンド

- **display mac-address**
- **mac-address(system view)**

4.1.7 mac-address (system view)

Syntax

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **vlan** *vlan-id*

mac-address multiport *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [[**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

undo mac-address multiport *mac-address* **interface** *interface-list* **vlan** *vlan-id*
undo mac-address [**multiport**] [[*mac-address*] **vlan** *vlan-id*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dynamic: ダイナミック MAC アドレスエントリを指定します。

static: スタティック MAC アドレスエントリを指定します。

blackhole: ブラックホール MAC アドレスエントリを指定します。パケットの送信元 MAC アドレスあるいは宛先 MAC アドレスがブラックホール MAC アドレスに一致している場合、パケットは廃棄されます。

multiport: マルチポートユニキャスト MAC アドレスエントリを指定します。宛先 MAC アドレスがマルチポートユニキャスト MAC アドレスエントリにマッチするフレームは複数のポートに送信されます。

mac-address: MAC アドレスを指定します。マルチキャスト MAC アドレスとすべてが 0 の MAC アドレスを除きます。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: 指定されたインタフェースが所属する既存の VLAN ID を指定します。設定範囲は 1～4094 です。

interface *interface-type interface-number*: 出力インタフェースのタイプと番号を指定します。

interface interface-list: 最大 4 つのインタフェース項目のリストを指定します。各インタフェース項目は、*interface-type interface-number* の形式の個々のインタフェース、または *interface-type interface-number1* **to** *interface-type interface-number2* の形式の一定範囲のインタフェースです。インタフェースは、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みです。*interface-number2* の値を interface-number1 の値より小さくすることはできません。

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 コマンドはすべての 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。

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 MAC アドレスエントリを設定することができます。

複数のポートから指定した宛先 MAC アドレスのフレームを送信するために、マルチポートユニキャスト MAC アドレスエントリを設定します。最初にコマンドを実行するとき、コマンドは MAC アドレスを追加します。同一の MAC アドレス、同一の VLAN で、異なるインタフェースでコマンドを再度実行した場合、コマンドはエントリの指定されたインタフェースを追加します。

スタティックあるいはブラックホール MAC アドレスエントリはダイナミック MAC アドレスエントリに上書きすることができます。ダイナミック MAC アドレスエントリはスタティックあるいはブラックホール MAC アドレスエントリに上書きすることはできません。

パラメータを指定しないで **undo mac-address** コマンドを実行した場合、すべてのユニキャスト MAC アドレスエントリとスタティックマルチキャスト MAC アドレスエントリを削除します。

指定した VLAN のすべての MAC アドレスエントリ（ユニキャスト MAC アドレスエントリとスタティックマルチキャスト MAC アドレスエントリを含みます）を削除することができます。また特定のタイプ（ダイナミック、スタティック、ブラックホール、マルチポートユニキャスト）の MAC アドレスエントリのみを削除することができます。1 つの

インタフェースのみを選択することで、スタティックマルチキャスト MAC アドレスエントリではなく、対応するユニキャスト MAC アドレスエントリを削除します。

MAC アドレスエントリの設定は、設定を保存しないと、再起動により削除されます。ただしダイナミック MAC アドレスエントリは設定の保存に関わらず、再起動により削除されます。

例

MAC アドレス 000f-e201-0101 のスタティックエントリを追加します。MAC アドレスに関連づけられたすべてのフレームは VLAN 2 に所属する GigabitEthernet 1/0/1 から送信します。

<Switch> system-view

[Switch] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2

MAC アドレス 000f-e201-0101 のマルチポートユニキャスト MAC アドレスエントリを追加します。MAC アドレス向けのすべてのフレームは VLAN 2 に所属する GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 に送信されます。

<Switch> system-view

[Switch] mac-address multiport 000f-e201-0101 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3 vlan 2

関連コマンド

- **display mac-address**
- **mac-address (interface view)**

4.1.8 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/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いっぱいになることを防ぐため、MAC アドレステーブルの学習を無効にすることができます。

たとえば、攻撃者からの異なる送信元 MAC アドレスの大量のパケットを学習しないように、以下のガイドラインに従い、装置で MAC アドレスの学習を無効にすることができます。

- インタフェースごとに MAC アドレスの学習を無効にすることができます。グローバルで MAC アドレスの学習を無効にした場合、すべてのインタフェースで MAC アドレスの学習が無効になります。装置は MAC アドレスの学習を停止し、ダイナミックに MAC アドレステーブルのアップデートを行うことができません。
- MAC アドレスの学習を無効にすると、ブロードキャストストームが発生する可能性あるため、インタフェースで MAC アドレスの学習を無効にしたのち、ブロードキャストストームの抑制を行ってください。ブロードキャストストームの抑制の詳細は、オペレーションマニュアルのセクション 3 *アクセス* “*Ethernet インタフェース*” を参照してください。
- グローバルで MAC アドレスの学習を有効にし、インタフェースあるいは VLAN で MAC アドレスの学習を無効にすることができます。

MAC アドレスの学習を無効にしたとき、装置はインタフェースにある既存のダイナミック MAC アドレスエントリを即座に削除します。

例

グローバルで MAC アドレスの学習を無効にします。

<Switch> system-view

[Switch] undo mac-address mac-learning enable

VLAN 10 で MAC アドレスの学習を無効にします。

<Switch> system-view

[Switch] vlan 10

[Switch-vlan10] undo mac-address mac-learning enable

GigabitEthernet 1/0/1 で MAC アドレスの学習を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo mac-address mac-learning enable

アグリゲートインタフェース Bridge-Aggregation 1 で MAC アドレスの学習を無効にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] undo mac-address mac-learning enable

関連コマンド

display mac-address mac-learning

4.1.9 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

4.1.10 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設定します。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。

インタフェースで学習した MAC アドレスの数が上限に達した場合、インタフェースは MAC アドレスエントリの学習を停止します。

例

GigabitEthernet 1/0/1 で学習できる MAC アドレスエントリの最大数を 600 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address max-mac-count 600

関連コマンド

- **mac-address**
- **mac-address max-mac-count enable-forwarding**

4.1.11 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。

この章では、未知のフレームは、送信元 MAC アドレスが MAC アドレステーブルにないフレームのことを示します。

例

MAC アドレスエントリを最大 600 まで学習できるように GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address max-mac-count 600

GigabitEthernet 1/0/1 で学習できる MAC アドレスの数が制限に到達したのち、GigabitEthernet 1/0/1 で受信された未知のフレームを装置が転送することを無効にします。

[Switch-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding

関連コマンド

- **mac-address**
- **mac-address max-mac-count**

4.1.12 mac-address mac-roaming enable

Syntax

mac-address mac-roaming enable

undo mac-address mac-roaming enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

mac-address mac-roaming enable コマンドは MAC アドレスの同期化を有効にします。

undo mac-address mac-roaming enable コマンドは MAC アドレスの同期化を無効にします。

IRF 環境で、異なる IRF スタックメンバ装置のポートが同じアグリゲーショングループの Selected ポートである場合、MAC アドレスエントリは IRF スタックメンバ装置間で同期化します。この MAC アドレスの同期化は、IRF 環境での MAC アドレスの同期化が有効かどうかにかかわらず行われます。アグリゲーショングループの詳細は、オペレーションマニュアルのセクション 3 *アクセス* を参照してください。

MAC アドレステーブルのサイズは IRF スタックメンバ装置により異なることがあります。MAC アドレスの同期化が有効になっている場合、IRF スタックメンバ装置のテーブルのサイズを超える MAC アドレスエントリは MAC アドレステーブルと同期できません。

例

MAC アドレスの同期機能を有効にします。

<Switch> system-view

[Switch] mac-address mac-roaming enable

4.1.13 mac-address notification mac-move

Syntax

mac-address notification mac-move [**interval** *interval*]

undo mac-address notification mac-move

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

interval *interval*: 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 コマンドはデフォルトに戻します。

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

1 つの MAC アドレスに設定できる MAC アドレス移動記録は 1 つだけです。

MAC アドレスが複数回移動する場合、新しい記録が古い記録を上書きします。

検出間隔内で、IRF スタックメンバ装置は最大 20 の MAC アドレスの移動情報を記録できます。記録は MAC 移動件数の降順にランク付けされます。

新しい記録の MAC 移動カウントが既存の記録の MAC 移動カウントよりも大きい場合、装置は次の処理を実行します。

- MAC 移動カウントが最も小さい記録を破棄します。
- MAC 移動数の多い順に MAC アドレス移動記録をランク付けします。

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 アドレス移動記録を破棄し、MAC 移動記録の生成をもう一度開始します。

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。MAC アドレスの移動記録を、MAC 移動カウントの降順に並べ替えます。

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 Switch MAC/4/MAC_FLAPPING: MAC address 0000-0012-0034
in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

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 MAC 移動検出間隔内に 1 回移動しました。

関連コマンド

display mac-address mac-move

4.1.14 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。

この機能は、MAC アドレスが MAC 移動検出間隔内に抑制しきい値を超えて MAC アドレスとの間で移動された場合、インタフェースをシャットダウンします。シャットダウンインタフェースは、抑制期間が経過すると自動的に起動します。また、**shutdown** コマンドを使用してから **undo shutdown** コマンドを使用して、インタフェースを起動することもできます。

MAC アドレス移動抑制がインタフェースをシャットダウンすると、システムは syslog メッセージのみをインフォメーションセンターモジュールに送信します。**snmp-agent trap enable mac-address** コマンドも実行された場合、システムは SNMP 通知を SNMP モジュールにも送信します。

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)

4.1.15 mac-address notification mac-move suppression (system view)

Syntax

mac-address notification mac-move suppression { **interval** *interval* | t**hreshold** *threshold* }

undo mac-address notification mac-move suppression { **interval** | **threshold** }

デフォルト

抑制間隔は 30 秒です。抑制しきい値は 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*: 抑制されたインタフェースが停止している間の MAC アドレス移動抑制間隔を指定します。*interval-value* 引数の値の範囲は 30 秒～86400 秒です。このオプションを指定しない場合、デフォルトの抑制間隔である 30 秒が使用されます。

threshold *threshold*: MAC 移動検出間隔内に、インタフェースから発信された、またはインタフェースに向けられた MAC アドレス移動の抑制しきい値を指定します。この引数の値の範囲は 0～1024 です。このオプションを指定しないと、デフォルトの抑制しきい値である 3 が使用されます。

説明

mac-address notification mac-move suppression コマンドは MAC アドレスの抑制間隔または制御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。

このコマンドをインタフェースで有効にするには、インタフェースでも MAC アドレス移動抑制を有効にする必要があります。

抑制間隔または抑制しきい値を複数回設定すると、最新の設定が適用されます。抑制間隔の設定は、抑制しきい値の設定とは無関係です。

例

MAC アドレスの抑制間隔を 40 秒に、抑制しきい値を 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)

4.1.16 mac-address static source-check enable

Syntax

mac-address static source-check enable

undo mac-address static source-check enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

定義済みユーザロール

network-admin

説明

mac-address static source-check enable コマンドはスタティック送信元チェック機能を有効にします。

undo mac-address static source-check enable コマンドはスタティック送信元チェック機能を無効にします。

例

GigabitEthernet 1/0/1 のスタティック送信元チェック機能を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo mac-address static source-check enable

4.1.17 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秒単位で指定します。*seconds* の設定範囲は 10～1000000 です。

🕮 **メモ：**

Version 7.1.6 では 10～630 を確立することが可能です。

---

no-aging: ダイナミック MAC アドレスエントリをエージング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います。

- 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

4.1.18 snmp-agent trap enable mac-address

Syntax

snmp-agent trap enable mac-address [**mac-move**]

undo snmp-agent trap enable mac-address [**mac-move**]

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

mac-move: MAC アドレステーブルの MAC アドレス移動に関する通知を指定します。指定しない場合、このコマンドは MAC アドレステーブルのすべてのタイプの SNMP 通知を有効にします。

説明

snmp-agent trap enable mac-address コマンドは MAC アドレステーブルの SNMP 通知を有効にします。

undo snmp-agent trap enable mac-address コマンドは MAC アドレステーブルの SNMP 通知を無効にします。

重要な MAC アドレス移動イベントを NMS に報告するには、MAC アドレステーブルの SNMP 通知を有効にします。MAC アドレス移動イベント通知が正しく送信されるようにするには、装置にも SNMP を設定する必要があります。

MAC アドレステーブルに対して SNMP 通知が無効になっている場合、装置は作成されたログをインフォメーションセンターに送信します。ログを表示するには、インフォメーションセンターでログの送信先と出力ルールの設定を行います。

SNMP およびインフォメーションセンターの設定については、装置のネットワーク管理およびモニタリング設定ガイド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 通知だけをサポートします。MAC アドレスの移動に関する SNMP 通知を有効または無効にすると、MAC アドレステーブルのすべてのタイプの SNMP 通知を有効または無効にすることができます。

例

MAC アドレステーブルで MAC アドレスが移動した場合 SNMP 通知を無効にします。

<Switch> system-view

[Switch] undo snmp-agent trap enable mac-address mac-move

関連コマンド

mac-address notification mac-move

目次

このセクションのページは **3-x-x** です。

5 章 MAC Information 5-1
5.1 MAC Information 設定コマンド 5-1
5.1.1 mac-address information enable (interface view) 5-1
5.1.2 mac-address information enable (system view) 5-2
5.1.3 mac-address information interval 5-2
5.1.4 mac-address information mode 5-3
5.1.5 mac-address information queue-length 5-4

5章 MAC Information

5.1 MAC Information設定コマンド

5.1.1 mac-address information enable (interface view)

Syntax

mac-address information enable { **added** | **deleted** }

undo mac-address information enable { **added** | **deleted** }

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

added: インタフェースで新しい MAC アドレスが学習されたとき、装置が MAC アドレスの変更情報を記録することを有効にします。

deleted: 既存の MAC アドレスが削除されたとき、装置が MAC アドレスの変更情報を記録することを有効にします。

説明

mac-address information enable コマンドは MAC Information 機能をインタフェースで有効にします。

undo mac-address information enable コマンドは MAC Information 機能をインタフェースで無効にします。

インタフェースで MAC Information 機能を有効にするまえに、グローバルで MAC Information 機能を有効にしてください。

例

新しい MAC アドレスを学習したとき、MAC アドレスの変更情報を記録するため、GigabitEthernet 1/0/1 で MAC Information 機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address information enable added

関連コマンド

mac-address information enable (system view)

5.1.2 mac-address information enable (system view)

Syntax

mac-address information enable

undo mac-address information enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

mac-address information enable コマンドは MAC Information 機能をグローバルで有効にします。

undo mac-address information enable コマンドは MAC Information 機能をグローバルで無効にします。

インタフェースで MAC Information 機能を有効にするまえに、グローバルで MAC Information 機能を有効にしてください。

例

MAC Information 機能をグローバルで有効にします。

<Switch> system-view

[Switch] mac-address information enable

関連コマンド

mac-address information enable (interface view)

5.1.3 mac-address information interval

Syntax

mac-address information interval *interval*

undo mac-address information interval

デフォルト

1 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: 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。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、キューに 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ました。
  - キューが一杯になりました。
- MAC アドレスの変更を通知する送信間隔が終了した場合、装置は Syslog メッセージあるいは SNMP トラップメッセージを送信します。

例

MAC アドレスの変更を記録する MAC Information のキューの長さを 600 に指定します。

<Switch> system-view

[Switch] mac-address information queue-length 600

目次

このセクションのページは **3-x-x** です。

6 章 リンクアグリゲーション.....6-1
6.1 リンクアグリゲーション設定コマンド.....6-1
6.1.1 description.....6-1
6.1.2 display interface.....6-2
6.1.3 display lacp system-id.....6-6
6.1.4 display link-aggregation load-sharing mode.....6-7
6.1.5 display link-aggregation member-port.....6-8
6.1.6 display link-aggregation summary.....6-11
6.1.7 display link-aggregation verbose.....6-13
6.1.8 interface bridge-aggregation.....6-16
6.1.9 lacp period short.....6-17
6.1.10 lacp system-priority.....6-18
6.1.11 link-aggregation global load-sharing mode.....6-19
6.1.12 link-aggregation load-sharing mode local-first.....6-20
6.1.13 link-aggregation mode.....6-21
6.1.14 link-aggregation port-priority.....6-22
6.1.15 link-aggregation selected-port maximum.....6-23
6.1.16 link-aggregation selected-port minimum.....6-24
6.1.17 port link-aggregation group.....6-25
6.1.18 reset counters interface.....6-26
6.1.19 reset lacp statistics.....6-27
6.1.20 shutdown.....6-28

6章 リンクアグリゲーション

6.1 リンクアグリゲーション設定コマンド

6.1.1 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋**Interface** です。（たとえばアグリゲートインタフェース Bridge-Aggregation1 のデフォルトは **Bridge-Aggregation1 Interface** です。）

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

description コマンドはインタフェースの説明を設定します。

undo description コマンドはデフォルトに戻します。

例

アグリゲートインタフェース Bridge-Aggregation 1 の説明を **connect to the lab** に設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] description connect to the lab

6.1.2 display interface

Syntax

display interface [**bridge-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation: レイヤ 2 アグリゲートインタフェースを指定します。

interface-number: 既存のアグリゲートインタフェース番号を指定します。

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 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 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 のインタフェース番号を指定した場合、指定したアグリゲートインタフェースの情報を表示します。

例

レイヤ 2 アグリゲートインタフェース Bridge-Aggregation 1 の詳細情報を表示します。

<Switch> display interface bridge-aggregation 1

```
Bridge-Aggregation1
Current state: UP
IP packet frame type: Ethernet II, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000 kbps
2Gbps-speed mode, full-duplex mode
```

```
Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Last clearing of counters: Never
Last 300 seconds input:  6900 packets/sec 885160 bytes/sec    0%
Last 300 seconds output:  3150 packets/sec 404430 bytes/sec    0%
Input (total):  5364747 packets, 686688416 bytes
        2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input (normal):  5364747 packets, 686688416 bytes
        2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
        0 CRC, 0 frame, 0 overruns, - aborts
        - ignored, - parity errors
Output (total): 1042508 packets, 133441832 bytes
        1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
Output (normal): 1042508 packets, 133441832 bytes
        1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        - lost carrier, - no carrier
```

レイヤ 2 アグリゲートインタフェース Bridge-Aggregation 1 の概要情報を表示します。

<Switch> display interface bridge-aggregation 1 brief

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) – auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed   Duplex Type PVID Description
BAGG1              UP   auto    A     A    1
```

表 6-1 コマンド出力

フィールド	説明
Bridge-Aggregation1	レイヤ2アグリゲートインタフェース名です。

フィールド	説明
Current state	アグリゲートインタフェースの状態です。 ● **Administratively DOWN**–**shutdown**コマンドでインタフェースがシャットダウンしています。 ● **DOWN**–**shutdown**コマンドでシャットダウンしていませんが、物理的にdownしています。（イーサネットケーブルが物理的に接続されていない、あるいはリンクに失敗している可能性があります） ● **UP**–インタフェースが運用上も物理的にも起動している状態です。
IP Packet Frame Type	IPv4パケットのフレームフォーマットです。
Description	インタフェースの説明です。
Bandwidth	インタフェースの予期された帯域幅です。 帯域幅が0 kbpsの場合、この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優先度です。
Output queue - Urgent queuing: Size/Length/Discards	緊急出力キューの情報です。 ● **Size**–キュー内のパケット数です。 ● **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**–ドロップされたパケットの数です。
Output queue - Protocol queuing: Size/Length/Discards	プロトコル出力キューの情報です。 ● **Size**–キュー内のパケット数です。 ● **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**–ドロップされたパケットの数です。
Output queue - FIFO queuing: Size/Length/Discards	FIFO出力キューの情報です。 ● **Size**–キュー内のパケット数です。 ● **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**–ドロップされたパケットの数です。
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	指定されたVLANからのパケットがVLANタグをつけてインタフェースに送信されました。

フィールド	説明
Untagged VLANs	指定されたVLANからのパケットがVLANタグなしでインタフェースに送信されました。
Last clearing of counters	**reset counters interface**コマンドがインタフェース統計情報を削除するために最後に使用された時刻。装置の起動以降に**reset counters interface**コマンドがインタフェースで使用されたことがない場合、このフィールドには**Never**と表示されます。
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	インタフェースにはIPアドレスが割り当てられておらず、IPパケットを処理できません。
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**–インタフェースは物理的に起動しています。 • **DOWN**–インタフェースは物理的に停止しています。 • **ADM**–インタフェースは**shutdown**コマンドを使用してシャットダウンされました。インタフェースの物理状態を復元するには、**undo shutdown**コマンドを使用します。 • **Stby**–インタフェースは、スタンバイ状態のバックアップインタフェースです。
Speed	通信速度です。単位はbpsです。 速度が自動的にネゴシエートされる場合、このフィールドには速度の横に（**a**）フラグが表示されます。 インタフェースが速度を自動ネゴシエーションするように設定されているが、自動ネゴシエーションが開始されていない場合、このフィールドには**auto**が表示されます。

フィールド	説明
Duplex	インタフェースのデュプレックスモードです。 • **A**—自動ネゴシエーションです。インタフェースはデュプレックスモードを自動ネゴシエーションするように設定されていますが、自動ネゴシエーションが開始されていません。 • **F**—全二重 • **F(a)**—自動ネゴシエーション全二重 • **H**—半二重 • **H(a)**—自動ネゴシエーション半二重
Type	インタフェースのリンクタイプです。 • **A**—Access. • **H**—Hybrid. • **T**—Trunk.
Protocol	インタフェースのデータリンク層プロトコル状態です。 • **UP**–インタフェースのデータリンクレイヤプロトコルがアップしています。 • **DOWN**–インタフェースのデータリンクレイヤプロトコルがダウンしています。 • **UP(s)**–インタフェースのデータリンクレイヤプロトコルはアップしていますが、リンクはオンデマンドリンクであるか、存在しません。(**s**)属性はスプーフィングフラグを表します。この値は、ヌルインタフェースおよびループバックインタフェースによく見られます。
Cause	インタフェースの物理リンク状態が**DOWN**になる原因です。

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）で設定されます。

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

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 load-sharing mode コマンドはグローバルあるいは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。

例

デフォルトのグローバルリンクアグリゲーションロードシェアリングモードを表示します。

<Switch> display link-aggregation load-sharing mode

```
Link-aggregation load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

設定済みのグローバルリンクアグリゲーションロードシェアリングモードを表示します。

<Switch> display link-aggregation load-sharing mode

```
Link-aggregation load-sharing mode:
destination-mac address, source-mac address
```

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、このフィールドにはレイヤ2およびレイヤ3トラフィックのリンクアグリゲーションロードシェアリングモードが表示されます。 グローバルのリンクアグリゲーションロードシェアリングモードを設定している場合、このフィールドには設定モードが表示されます。
Route-Aggregation10 load-sharing mode	アグリゲーショングループ10のリンクアグリゲーションロードシェアリングモードです。 デフォルトでは、このフィールドにはグローバルリンクアグリゲーションロードシェアリングモードが表示されます。 このアグリゲーショングループに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ている場合、このフィールドには設定モードが表示されます。
Layer 2 traffic: packet type-based sharing	レイヤ2のデフォルトのロードシェアリングモードを示します。この出力のモードはパケットタイプです。
Layer 3 traffic: packet type-based sharing	レイヤ3のデフォルトのロードシェアリングモードを示します。この出力のモードはパケットタイプです。
destination-mac address, source-mac address	設定されたリンクアグリゲーションロードシェアリングモードを示します。この出力例では、トラフィックは送信元と宛先のMACアドレスに基づいています。

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のリストを *interface-type interface-number1* [**to** *interface-type interface-number2*] の形式で指定します。*interface-number2* の値は、*interface-number1* の値以上である必要があります。

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。ビットが1のときは文字が表示され、ビットが0のときには文字は表示されません。 • **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**－送信システムがリンクが集約されたとみなすことを示します。1が集約された、0が集約されていないです。 • **E**－送信システムが、受信フレームを集約しているかどうかを示します。1が集約している、0が集約していないです。 • **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**－送信システムのRXステートマシンがデフォルト状態にあるかどうかを示します。1は、はいを示します。0は、いいえを示します。 • **H**－送信側システムのRXステートマシンが期限切れ状態にあるかどうかを示します。1は、はいを示します。0は、いいえを示します。

フィールド	説明
Aggregate Interface	メンバポートが所属するアグリゲートインタフェースです。
Local	ローカルインタフェースの情報です。
Oper-key	操作キーです。
Flag	LACPプロトコル状態のフラグです。
Remote	ピアエンドの情報です。
System ID	ピアのシステムIDです。システムLACPプライオリティとシステムMACアドレスが含まれます。
Received LACP Packets	受信したLACPパケット数です。
Illegal	異常パケットの総数です。
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
Aggregation 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**－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**－スタティックリンクアグリゲーションです。 ● **D**－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**–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: 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 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。

レイヤ 2 の **bridge-aggregation** のみを指定した場合、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 は、対応するアグリゲートインタフェースが装置に存在する場合にだけ使用できます。

このコマンドは、自動割り当てが有効になっているインタフェースがアグリゲートグループに参加していない場合は表示しません。

例

ダイナミックのアグリゲーショングループであるレイヤ 2 アグリゲーショングループ 10 に関する詳細情報を表示します。

<Switch> display link-aggregation verbose bridge-aggregation 10

```
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation10
Aggregation Mode: Dynamic
```

```
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port              Status   Priority Index    Oper-Key            Flag
  GE1/0/1           S        32768    61       2                   {ACDEF}
  GE1/0/2           S        32768    62       2                   {ACDEF}
  GE1/0/3           S        32768    63       2                   {AG}
Remote:
  Actor             Priority Index    Oper-Key SystemID            Flag
  GE1/0/1(R)        32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2           32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3           32768    113      0        0x8000, 0000-0000-0000 {DEF}
```

スタティックのアグリゲーショングループであるレイヤ 2 アグリゲーショングループ 20 に関する詳細情報を表示します。

<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(R)      S       32768    1
  GE1/0/2         S       32768    1
  GE1/0/3         S       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**–負荷分散を行いません。

フィールド	説明
Port Status	ポートの状態です。 • **Selected** • **Unselected** • **Individual**
Port	ポートのタイプです。 • **Auto port**–ポートは自動割り当てで有効になっています。 • **Management port**–ポートは管理ポートです。この値は、QX-S5300Gシリーズではサポートしていません。 • **Reference port**–ポートは基準ポートです。
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**－送信システムのRXステートマシンがデフォルト状態にあるかどうかを示します。1は、はいを示します。0は、いいえを示します。 • **H**－送信側システムのRXステートマシンが期限切れ状態にあるかどうかを示します。1は、はいを示します。0は、いいえを示します。
Aggregate Interface	アグリゲートインタフェースの名前です。
Aggregation Mode	アグリゲーショングループのタイプです。 • **S**－スタティックです。 • **D**－ダイナミックです。

フィールド	説明
Management VLANs	（このフィールドは、QX-S5300Gシリーズではサポートしていません。）管理VLANです。管理VLANが指定されていない場合、このフィールドには**None**と表示されます。
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。
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です。 • **Priority**–ポートプライオリティです。 • **Index**—ポートインデックスです。 • **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、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。 • **Priority**–ピアポートのプライオリティです。 • **Index**—ピアポートのインデックスです。 • **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。

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短いタイムアウト間隔のショート（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。

ISSU 中のトラフィックの中断を避けるために、ISSU を実行する前に短い LACP タイムアウト間隔を有効にしないでください。詳細はオペレーションマニュアルのセクション 1 *はじめに* “*ISSU*”を参照してください。

例

GigabitEthernet 1/0/1 で短い LACP タイムアウト間隔（3 秒）を有効にします。

<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、パケットタイプに基づいてリンクアグリゲーションロードシェアリングモードを自動的に選択します。

View

System view

定義済みユーザロール

network-admin

パラメータ

destination-ip: 宛先 IP アドレスをもとに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。

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。

system view において、装置は以下のロードシェリングモードの組み合わせをサポートします。

- パケットタイプに基づいて自動的に決定されるロードシェアリングモード
- 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
- 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
- 入力ポート

例

宛先 MAC アドレスをもとにしてグローバル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 load-sharing mode local-first

Syntax

link-aggregation load-sharing mode local-first

undo link-aggregation load-sharing mode local-first

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

link-aggregation load-sharing mode local-first コマンドはリンクアグリゲーションの local-first ロードシェアリングを有効にします。

undo link-aggregation load-sharing mode local-first コマンドはリンクアグリゲーションの local-first ロードシェアリングを無効にします。

local-first ロードシェアリングを無効にすると、すべての IRF スタックメンバ装置のアグリゲートインタフェースのすべての Selected ポート間でパケットのロードシェアリングを行います。

リンクアグリゲーションの local-first ロードシェアリングは既知のユニキャストパケットのみ適用します。

例

リンクアグリゲーションの local-first ロードシェアリングを無効にします。

<Switch> system-view

[Switch] undo link-aggregation load-sharing mode local-first

6.1.13 link-aggregation mode

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

デフォルト

スタティックアグリゲーションモード

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

link-aggregation mode dynamic コマンドはダイナミックアグリゲーションモードで動作するようにアグリゲーショングループを設定し、LACP を有効にします。

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

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。

アグリゲーションモードを変更すると、Selected member ports が Unselected になることがあります。

ダイナミックアグリゲーショングループに自動割り当てが有効になっているメンバポートが含まれている場合、アグリゲーションモードをスタティックに変更すると、選択されたメンバポートが選択解除される可能性があります。同時に、メンバポートでは自動割り当てが自動的に無効になります。ベストプラクティスとして、アグリゲーションモードを変更する前に、ダイナミックアグリゲーショングループにそのようなメンバポートが含まれていないことを確認してください。

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レイヤ 2 アグリゲーショングループ 1 を設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] link-aggregation mode dynamic

6.1.14 link-aggregation port-priority

Syntax

link-aggregation port-priority *priority*

undo link-aggregation port-priority

デフォルト

32768

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

priority: ポートプライオリティを設定します。設定範囲は 0～65535 です。この値が小さいほど、LACP プライオリティが高くなります。

説明

link-aggregation port-priority コマンドはインタフェースのポートプライオリティを設定します。

undo link-aggregation port-priority コマンドはデフォルトに戻します。

例

レイヤ 2 での GigabitEthernet 1/0/1 のポートプライオリティを 64 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] link-aggregation port-priority 64

関連コマンド

lacp system-priority

6.1.15 link-aggregation selected-port maximum

Syntax

link-aggregation selected-port maximum *max-number*

undo link-aggregation selected-port maximum

デフォルト

8

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

max-number: アグリゲーショングループで使用できる Selected ポートの最大数を設定します。設定範囲は 1～8 です。

説明

link-aggregation selected-port maximum コマンドはアグリゲーショングループで使用できる Selected ポートの最大数を設定します。

undo link-aggregation selected-port maximum コマンドはデフォルトに戻します。

このコマンドを実行すると、アグリゲーショングループのいくつかの Selected ポートは Unselected ポートになる可能性があります。

アグリゲーショングループで使用できる Selected ポートの最大数は、ローカルとピアエンドで同一にする必要があります。

アグリゲーショングループで使用できる Selected ポートの最大数は、以下の値の小さい方に制限されます。

- **link-aggregation selected-port maximum** コマンドで設定された最大数
- リンクアグリゲーション機能で許可される Selected ポートの最大数

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。

この場合、アグリゲーショングループでは常に 1 つの Selected ポートだけが許可され、Unselected ポートはバックアップポートとして機能します。

例

アグリゲートインタフェース Bridge-Aggregation 1 に対応するアグリゲーショングループで使用できる Selected ポートの最大数を 5 に設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] link-aggregation selected-port maximum 5

関連コマンド

link-aggregation selected-port minimum

6.1.16 link-aggregation selected-port minimum

Syntax

link-aggregation selected-port minimum *min-number*

undo link-aggregation selected-port minimum

デフォルト

設定なし

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

min-number: アグリゲートインタフェースを UP にするのに必要なアグリゲーショングループで使用できる Selected ポートの最小数を設定します。設定範囲は 1～8 です。

説明

link-aggregation selected-port minimum コマンドはアグリゲーショングループで使用できる Selected ポートの最小数を設定します。

undo link-aggregation selected-port minimum コマンドはデフォルトに戻します。

このコマンドを実行すると、アグリゲーショングループのすべてのメンバポートは Unselected ポートになる可能性があります。

アグリゲーショングループで使用できる Selected ポートの最小数は、ローカルとピアエンドで同一にする必要があります。

例

レイヤ 2 アグリゲーショングループ 1 で使用できる Selected ポートの最小数を 3 に設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] link-aggregation selected-port minimum 3

関連コマンド

link-aggregation selected-port maximum

6.1.17 port link-aggregation group

Syntax

port link-aggregation group *group-id* [**force**]

undo port link-aggregation group

🕮 **メモ：**

force オプションは、V7.2.16 以降で実行可能です。

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。

force: 現在のインタフェースがアグリゲートインタフェースから属性設定を同期できるようにします。指定しない場合、現在のインタフェースは、アグリゲートグループに参加したときにアグリゲートインタフェースのアトリビュート設定を同期しません。レイヤ 2 Ethernet インタフェースでのみサポートされています。

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。

レイヤ 2 Ethernet インタフェースはレイヤ 2 アグリゲートインタフェースグループにのみ割り当てできます。

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。

アグリゲーションインタフェースと異なる属性設定がある場合、インタフェースはアグリゲーショングループに参加できません。アグリゲーショングループに参加した後、インタフェースはアグリゲーションインタフェース上の属性設定を継承します。アグリゲーションインタフェースでのみ属性設定を変更できます。

force キーワードが有効になるのは、インタフェースをアグリゲーショングループに割り当てたときだけです。実行コンフィギュレーションまたはコンフィギュレーションファイルに保存することはできません。

例

レイヤ 2 Ethernet インタフェース GigabitEthernet 1/0/1 をレイヤ 2 アグリゲーショングループ 1 に割り当てます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port link-aggregation group 1

6.1.18 reset counters interface

Syntax

reset counters interface [**bridge-aggregation** | *interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

bridge-aggregation: 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: 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 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* 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 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。

bridge-aggregation は、対応するアグリゲートインタフェースが装置に存在する場合にだけ使用できます。

例

レイヤ 2 のアグリゲートインタフェース Bridge-Aggregation 1 の統計情報を削除します。

<Switch> reset counters interface bridge-aggregation 1

6.1.19 reset lacp statistics

Syntax

reset lacp statistics [**interface** *interface-list*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-list*: リンクアグリゲーションメンバポートのリストを指定します。形式は *interface-type interface-number1* [**to** *interface-type interface-number2*]です。

interface-number1 の値は、i*nterface-number2* の値以上である必要があります。

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。メンバポートを指定しない場合、すべてのメンバポートの LACP の統計情報を削除します。

説明

reset lacp statistics コマンドはリンクアグリゲーションメンバポートの LACP の統計情報を削除します。

例

すべてのリンクアグリゲーションメンバポートの LACP の統計情報を削除します。

<Switch> reset lacp statistics

関連コマンド

display link-aggregation member-port

6.1.20 shutdown

Syntax

shutdown

undo shutdown

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはアグリゲートインタフェースをシャットダウンします。

undo shutdown コマンドはアグリゲートインタフェースを up にします。

例

レイヤ 2 のアグリゲートインタフェース Bridge-Aggregation 1 を up にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] undo shutdown

目次

このセクションのページは **3-x-x** です。

7 章 Port Isolation.....7-1
7.1 Port Isolation 設定コマンド.....7-1
7.1.1 display port-isolate group.....7-1
7.1.2 port-isolate enable.....7-2
7.1.3 port-isolate group.....7-3

7章 Port Isolation

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 ID 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のID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 ID 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 ID 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。

例

アイソレーショングループ 1 を作成します。

<Switch> system-view

[Switch] port-isolate group 1

目次

このセクションのページは **3-x-x** です。

8 章 STP 8-1
8.1 STP 設定コマンド 8-1
8.1.1 active region-configuration 8-1
8.1.2 bpdu-drop any 8-2
8.1.3 check region-configuration 8-2
8.1.4 display stp 8-4
8.1.5 display stp abnormal-port 8-13
8.1.6 display stp bpdu-statistics 8-14
8.1.7 display stp down-port 8-17
8.1.8 display stp history 8-18
8.1.9 display stp region-configuration 8-20
8.1.10 display stp root 8-21
8.1.11 display stp tc 8-22
8.1.12 instance 8-24
8.1.13 region-name 8-25
8.1.14 reset stp 8-26
8.1.15 revision-level 8-27
8.1.16 snmp-agent trap enable stp 8-28
8.1.17 stp bpdu-protection 8-29
8.1.18 stp bridge-diameter 8-30
8.1.19 stp compliance 8-31
8.1.20 stp config-digest-snooping 8-32
8.1.21 stp cost 8-33
8.1.22 stp dispute-protection 8-35
8.1.23 stp edged-port 8-36
8.1.24 stp enable 8-37
8.1.25 stp global config-digest-snooping 8-38
8.1.26 stp global enable 8-39
8.1.27 stp global mcheck 8-40
8.1.28 stp log enable tc 8-41
8.1.29 stp loop-protection 8-42
8.1.30 stp max-hops 8-43
8.1.31 stp mcheck 8-43
8.1.32 stp mode 8-45
8.1.33 stp no-agreement-check 8-46
8.1.34 stp pathcost-standard 8-47

8.1.35 stp point-to-point 8-48
8.1.36 stp port bpdu-protection 8-49
8.1.37 stp port priority 8-50
8.1.38 stp port shutdown permanent 8-51
8.1.39 stp port-log 8-52
8.1.40 stp priority 8-54
8.1.41 stp pvst-bpdu-protection 8-55
8.1.42 stp region-configuration 8-55
8.1.43 stp role-restriction 8-56
8.1.44 stp root primary 8-57
8.1.45 stp root secondary 8-58
8.1.46 stp root-protection 8-59
8.1.47 stp tc-protection 8-60
8.1.48 stp tc-protection threshold 8-61
8.1.49 stp tc-snooping 8-62
8.1.50 stp timer forward-delay 8-63
8.1.51 stp timer hello 8-64
8.1.52 stp timer max-age 8-65
8.1.53 stp timer-factor 8-66
8.1.54 stp transmit-limit 8-67
8.1.55 stp vlan enable 8-69
8.1.56 vlan-mapping modulo 8-70

8章 STP

8.1 STP設定コマンド

8.1.1 active region-configuration

Syntax

active region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

active region-configuration コマンドは MST(multiple spanning tree)リージョン設定をアクティブにします。

MST リージョンパラメータを設定するとき、MSTP は新しいスパニングツリーの計算プロセスを行います。スパニングツリーの計算プロセスが実行されるとネットワークが不安定になります。VLAN-インスタンスマッピングテーブルを設定するときに、よく発生します。このため **active region-configuration** コマンドあるいは **stp global enable** コマンドを実行したのち、MSTP を有効にします。

このコマンドを実行する前に、**check region-configuration** コマンドを使用して MST のリージョンの設定が正しいことを確認してください。MST のリージョンの設定が正しいことが確認できたら、このコマンドを実行してください。

例

MSTI 1 に VLAN 2 をマッピングし、MST リージョンの設定を有効にします。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] instance 1 vlan 2

[Switch-mst-region] active region-configuration

関連コマンド

- **check region-configuration**
- **instance**
- **region-name**
- **revision-level**

- **stp global enable**
- **vlan-mapping modulo**

8.1.2 bpdu-drop any

Syntax

bpdu-drop any

undo bpdu-drop any

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

bpdu-drop any コマンドはポートで BPDU ドロップ機能を有効にします。

undo bpdu-drop any コマンドは BPDU ドロップ機能を無効にします。

この機能を使用することで、装置は以下の BPDU パケットをドロップします。

- EOAM
- GVRP
- LACP
- LLDP
- PVST
- STP（STP、RSTP、MSTP を含みます）

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。

フィールド	説明
Revision level	MSTリージョンのリビジョンレベルです。
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-number 1* [**to** *interface-type interface-number 2*] です。*interface-number 2* は *interface-number 1* 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*: メンバ ID によって IRF スタックメンバ装置を指定します。

メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の情報を表示します。

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、指定した VLAN のすべてのポートに適用します。
- ポートを指定し、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。

ネットワークの収束中、最新のスパニングツリーの情報は表示されません。

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         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	ポートで有効なスパニングツリー保護機能です。 • **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ガードです。 • **LOOP**—Loopガードです。 • **BPDU**—BPDUガードです。 スパニングツリー保護機能が設定されていない場合、またはスパニングツリー保護がトリガーされない場合、**NONE**が表示されます。

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（.）の後の値は装置のMACアドレスを示します。

フィールド	説明
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）
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保護機能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。

フィールド	説明
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。
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時間以内にポートが送信するBPDUの最大数です。
Protection type	スパニングツリー保護がポートに設定されています ● **Config**—スパニングツリーの保護機能を設定します。 ● **Active**—有効なスパニングツリー保護機能です。 スパニングツリー保護の機能は次のとおりです。 ● **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。 スパニングツリー保護機能が設定されていない場合、またはスパニングツリー保護がトリガーされない場合、**NONE**が表示されます。
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。 MSTP運用時に、高速収束が無効の状態になった場合は、「802.1s準拠」から「legacy」に変化します。
Port Config-Digest-Snooping	ポートのDigest Snoopingの状態です。

フィールド	説明
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。
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。 • プライマリルートです。 • 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)	ポート状態の遷移遅延です。（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。

フィールド	説明
TC Snooping	TC snoopingの状態です。 ● 有効 ● 無効

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 STP 保護処理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 または VLAN で、このコマンドを使用すると、スパニングツリー保護機能によってブロックされているポートについて、最大 3 つの履歴レコードを表示できます。

例

MSTP 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ているポートに関する履歴を表示します。

<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 STP 保護処理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]---
   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。
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、フォワーディングまたはラーニング状態の非ブロック指定ポートから、低プライオリティBPDUを受信します。 • **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	保護機能が開始した時間です。

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、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。

フィールド	説明
Type	統計項目です。
Looped-back BPDUs	同じポートで送受信されたBPDUの数です。
Max-aged BPDUs	最大エージングを超過したBPDUの数です。
TCN sent	TCN BPDUの送信数です。
TCN received	TCN BPDUの受信数です。
TCA sent	TCA BPDUs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	Configuration BPDUの送信数です。
RST received	RSTP BPDUの受信数です。
MST sent	RSTP BPDUの受信数です。
MST received	MSTP BPDUの送信数です。
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	検出されたトポロジ変更の数です。
TC sent	TC BPDUの送信数です。
TC received	TC BPDUの受信数です。
PVID inconsistency BPDUs	BPDU受信ポートと一致しないPVIDを持つ受信PVST BPDUの数です。

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 protection**—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*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の情報を表示します。

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 の指定されたスロット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 の指定されたスロットのポートの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	ポートのロール計算の時間です。

8.1.9 display stp region-configuration

Syntax

display stp region-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp region-configuration コマンドは有効な MST リージョンの設定情報を表示します。以下の情報があります。

- リージョン名
- リビジョンレベル
- ユーザ定義の VLAN-インスタンスマッピング

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*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の情報を表示します。

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、コマンド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 モードでは、MSTI 0 のスロット 1 にあるすべてのポートの着信および発信 TC / TCN BPDU 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 モードでは、VLAN 2 のスロット 1 にあるすべてのポートの着信および発信 TC / TCN BPDU 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-id: 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。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。

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-number 1* [**to** *interface-type interface-number 2*] です。*interface-number 2* は *interface-number 1* 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

SNMP notification は、新規ルート選択イベントでは無効になります。

MSTP モードでは、SNMP notification は MSTI 0 で有効です。ほかの MSTI では無効です。

PVST モードでは無効です。

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に、装置が通知を送信できるようにします。このキーワードは、STP、MSTP、および RSTP モードにのみ適用されます。

tc: 装置が TCN BPDU を受信した場合、SNMP notification の送信を有効にします。PVST モードでのみ有効です。

説明

snmp-agent trap enable stp コマンドはスパニングツリートポロジの変更に関する SNMP notification を有効にします。

undo snmp-agent trap enable stp コマンドはスパニングツリートポロジの変更に関する SNMP notification を無効にします。

キーワードを指定しない場合、**snmp-agent trap enable stp** コマンドは、さまざまなイベントの SNMP 通知に次のように適用されます。

- STP、MSTP、および RSTP モードでは、このコマンドは、新規ルート選択イベントの SNMP 通知に適用されます。
- PVST モードでは、このコマンドは、スパニングツリートポロジの変更に関する SNMP 通知に適用されます。

例

スパニングツリートポロジの変更に関する SNMP notification 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 BPDU ガード機能を有効にします。

undo stp bpdu-protection コマンドは BPDU ガード機能を無効にします。

例

#グローバルに BPDU ガードを有効にします。

<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。

undo stp bridge-diameter コマンドはデフォルトに戻します。

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。

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。この設定は、ポートに対して同時に有効になり、ネットワークへの影響を軽減します。

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

Digest Snooping を GigabitEthernet 1/0/1 とグローバルで有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp config-digest-snooping

[Switch-GigabitEthernet1/0/1] quit

[Switch] stp global config-digest-snooping

関連コマンド

- **display stp**
- **stp global config-digest-snooping**

8.1.21 stp cost

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost** *cost-value*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost**

デフォルト

装置は各スパニングツリーのポートのパスコストを、対応する標準にもとづいて自動的に計算します。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

cost-value: ポートのパスコストを指定します。設定範囲は、採用されているパスコスト計算基準によって決まります。

- パスコスト計算に IEEE 802.1d-1998 が選択されている場合、設定範囲は 1～65535 です。
- パスコスト計算に IEEE 802.1t が選択されている場合、設定範囲は 1～200000000 です。
- パスコスト計算にプライベート標準が選択されている場合、コスト範囲は 1～200000 です。

説明

stp cost コマンドはポートのパスコストを設定します。

undo stp cost コマンドはデフォルトに戻します。

パスコストはスパニングツリー計算を行う際の重要な要素です。MSTI のポートに異なるパスコストを設定すると、VLAN トラフィックのフローが異なる物理的リンクを通って転送され、VLAN ベースのロードバランスを行うことができます。

ポートのパスコストの設定はポートの役割に影響します。ポートの役割が変更されたとき、システムはポートの役割を計算し、状態遷移を開始します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

MSTI あるいは VLAN を指定しない場合、このコマンドは MSTP CIST あるいは STP、RSTP スパニングツリーのポートのパスコストを設定します。

例

MSTP モードで MSTI 2 の GigabitEthernet 1/0/1 のパスコストを 200 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp instance 2 cost 200

PVST モードで VLAN 2 の GigabitEthernet 1/0/1 のパスコストを 200 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp vlan 2 cost 200

関連コマンド

- **display stp**
- **stp pathcost-standard**

8.1.22 stp dispute-protection

Syntax

stp dispute-protection

undo stp dispute-protection

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

stp dispute-protection コマンドは Dispute Guard を有効にします。

undo stp dispute-protection コマンドは Dispute Guard を無効にします。

スパニングツリー機能によってポートで単方向リンクが検出された場合、ポートをブロックしてループを防止します。

一部の VLAN ネットワークでは、ダウンストリーム装置のアップリンクポートが PVID からのパケットを拒否するように設定されています。その結果、ダウンストリーム装置はアップストリーム装置から PVID の BPDU を受信できません。

ただし、アップストリーム装置はダウンストリーム装置から BPDU を受信できます。この場合、**dispute guard** はアップストリーム装置の受信ポートをブロックし、トラフィックの中断を引き起こします。

サービスの継続性を確保し、リンクがブロックされないようにするには、**undo stp disput-protection** コマンドを使用して **dispute guard** を無効にします。

例

Dispute guard を無効にします。

<Switch> system-view

[Switch] undo stp dispute-protection

8.1.23 stp edged-port

Syntax

stp edged-port

undo stp edged-port

デフォルト

すべてのポートは非エッジポートです。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp edged-port コマンドはポートを Edge ポートに設定します。

undo stp edged-port コマンドはポートを非 Edge ポートに設定します。

ユーザ端末に直接接続しているポートは別の装置あるいは共有 LAN セグメントに接続されているポートよりも、Edge ポートとして設定されることができます。

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。

レイヤ 2 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。

レイヤ 2 aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 を Edge ポートとして設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp edged-port

関連コマンド

- **stp bpdu-protection**
- **stp loop-protection**
- **stp port bpdu-protection**
- **stp root-protection**

8.1.24 stp enable

Syntax

stp enable

undo stp enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp enable コマンドはスパニングツリー機能を有効にします。

undo stp enable コマンドはスパニングツリー機能を無効にします。

スパニングツリー機能を有効にしたとき、装置はスパニングツリーのモードの設定に従い STP、RSTP、PVST、MSTP モードで動作します。

スパニングツリー機能を有効にしたとき、装置は受信した configuration BPDU にもとづいて VLAN のスパニングツリーの状態を自動で維持します。

スパニングツリー機能を無効にしたとき、装置はスパニングツリーの状態の維持を停止します。

レイヤ 2 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。

レイヤ 2 aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

MSTP モードで、GigabitEthernet 1/0/1 のスパニングツリー機能を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo stp enable

関連コマンド

- **stp global enable**
- **stp mode**
- **stp vlan enable**

8.1.25 stp global config-digest-snooping

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global config-digest-snooping コマンドはグローバルで Digest Snooping を有効にします。

undo stp global config-digest-snooping コマンドはグローバルで Digest Snooping を無効にします。

この設定はグローバル、およびほかのベンダの装置に接続されたポートの両方で有効にする必要があります。影響を最小限にするため、グローバルで有効にする前に関連したポートの機能を有効にしてください。

例

Digest Snooping を GigabitEthernet 1/0/1 とグローバルで有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp config-digest-snooping

[Switch-GigabitEthernet1/0/1] quit

[Switch] stp global config-digest-snooping

関連コマンド

- **display stp**
- **stp config-digest-snooping**

8.1.26 stp global enable

Syntax

stp global enable

undo stp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global enable コマンドはスパニングツリー機能をグローバルで有効にします。

undo stp global enable コマンドはスパニングツリー機能をグローバルで無効にします。

スパニングツリー機能を有効にしたとき、スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

スパニングツリー機能が有効であるとき、装置は受信した configuration BPDU にもとづいて VLAN のスパニングツリーの状態を維持します。スパニングツリー機能が無効であるとき、装置はスパニングツリーの状態の維持を停止します。

例

スパニングツリー機能をグローバルで有効にします。

<Switch> system-view

[Switch] stp global enable

関連コマンド

- **stp enable**
- **stp mode**

8.1.27 stp global mcheck

Syntax

stp global mcheck

View

System view

定義済みユーザロール

network-admin

説明

stp global mcheck コマンドはグローバルで mCheck を実行します。

MSTP、RSTP、PVST のポートが STP 装置に接続し、STP BPDU を受信すると、ポートは自動で STP モードに遷移します。しかし以下の状況ではポートは自動でもとのモードに戻ることができません。

- ピアの STP 装置がシャットダウンあるいは削除されたとき。
- ポートが変更を検出できないとき。

この場合、mCheck を実行して、ポートをもとのモードに強制的に移行させることができます。

スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

装置が MSTP、RSTP、PVST モードで動作しているときのみ **stp global mcheck** コマンドが適用されます。

例

グローバルで mCheck を実行します。

<Switch> system-view

[Switch] stp global mcheck

関連コマンド

- **stp mcheck**
- **stp mode**

8.1.28 stp log enable tc

Syntax

stp log enable tc

undo stp log enable tc

デフォルト

設定なし

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 TC BPDU の検出あるいは受信した場合、ログを作成します。

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 モードでのみ有効です。

例

TC BPDU の検出あるいは受信した場合、ログを作成します。

<Switch> system-view

[Switch] stp log enable tc

8.1.29 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**

8.1.30 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

8.1.31 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、Device A、Device B、Device C が一列に接続されています。Device A は STP を動作し、Device B はスパニングツリープロトコルが動作しておらず、Device C は RSTP、MSTP あるいは PVST で動作します。Device C が Device 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。Device B を Device C と RSTP、MSTP、PVST で動作するように設定した場合、Device B と Device 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**

8.1.32 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、VLAN1 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**

8.1.33 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

8.1.34 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**

8.1.35 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トインタフェースあるいは full 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、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 1/0/1 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

8.1.36 stp port bpdu-protection

Syntax

stp port bpdu-protection { **enable** | **disable** }

undo stp port 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 stp port 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**

8.1.37 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 のポートプライオリティを 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 のポートプライオリティを 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

8.1.38 stp port shutdown permanent

Syntax

stp port shutdown permanent

undo stp port shutdown permanent

デフォルト

ポートステータス検出タイマが期限切れになると、装置は BPDU ガードによってシャットダウンされたエッジポートを再アクティブ化します。

View

System view

定義済みユーザロール

network-admin

説明

stp port shutdown permanent コマンドは BPDU ガードによってシャットダウンされたエッジポートを装置が再アクティブ化しないようにします。

undo stp port shutdown permanent コマンドはデフォルトに戻します。

stp port shutdown permanent コマンドは、設定後に BPDU ガードによってシャットダウンされたエッジポートでのみ有効になります。**undo stp port shutdown permanent** コマンドを実行しても、装置はシャットダウンポートを起動しません。これらのポートを起動するには、**undo shutdown** コマンドを使用する必要があります。

ポートステータス検出タイマの詳細については、オペレーションマニュアルのセクション 1 *はじめに* “*装置管理*”を参照してください。

例

BPDU ガードによってシャットダウンされたエッジポートを装置が再アクティブ化しないようにします。

<Switch> system-view

[Switch] stp port shutdown permanent

8.1.39 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 1～4094 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。

8.1.40 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

8.1.41 stp pvst-bpdu-protection

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp pvst-bpdu-protection コマンドは PVST BPDU ガード機能を有効にします。

undo stp pvst-bpdu-protection コマンドは PVST BPDU ガード機能を無効にします。

ポートが PVST BPDU を受信する場合、MSTP が有効な装置はポートをシャットダウンします。シャットダウンしたポートは検出間隔が終了したのち、up となります。検出間隔を設定する場合、**shutdown-interval** コマンドを使用します。

例

MSTP モードで PVST BPDU ガード機能を有効にします。

<Switch> system-view

[Switch] stp pvst-bpdu-protection

関連コマンド

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

8.1.42 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]

8.1.43 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

8.1.44 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**

8.1.45 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**

8.1.46 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**

8.1.47 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

8.1.48 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

8.1.49 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 スヌーピングを有効にします。

undo stp tc-snooping コマンドは TC スヌーピングを無効にします。

TC スヌーピングとスパニングツリー機能は相互に排他的です。TC スヌーピングを有効にする前に、スパニングツリー機能をグローバルに無効にする必要があります。

例

スパニングツリー機能をグローバルに無効にし、TC スヌーピングを有効にします。

<Switch> system-view

[Switch] undo stp global enable

[Switch] stp tc-snooping

関連コマンド

stp global enable

8.1.50 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**

8.1.51 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**

8.1.52 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**

8.1.53 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。

安定したネットワークでは、各非ルートブリッジは、hello 時間の間隔で設定 BPDU を周辺の装置に転送し、リンクで障害が発生しているかどうかを判別します。hello 時間の 9 回以内に装置がアップストリーム装置から BPDU を受信しない場合、アップストリーム装置に障害が発生したと見なされます。その後、新しいスパニングツリー計算プロセスが開始されます。

次の状況では、タイムアウト係数を 5、6、または 7 に設定することを推奨します。

- 望ましくないスパニングツリーの計算を防止します。アップストリーム装置がビジー状態のため、設定 BPDU を時間内に転送できない場合があります。たとえば、多くのレイヤ 2 インタフェースがアップストリーム装置に設定されています。この場合、ダウンストリーム装置はタイムアウト期間内に BPDU を受信できず、望ましくない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上のネットワークリソースを節約します。

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

8.1.54 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。

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

8.1.55 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。

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**

8.1.56 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、次の式に従い、VLAN をマッピングする MSTI の ID を決定します。

ID ＝ (VLAN ID － 1) %*modulo* ＋ 1

(VLAN ID － 1) %*modulo* は (VLAN ID － 1)に対してモジュロ演算を行うことを意味します。モジュロの値が 15 である場合、VLAN 1 は MSTI 1 に、VLAN 2 は MSTI 2 に、VLAN 15 は MSTI 15 に、VLAN 16 は MSTI 16 のようにマッピングされます。

例

VLAN を MSTI にモジュロ 8 でマッピングします。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] vlan-mapping modulo 8

関連コマンド

- **active region-configuration**
- **check region-configuration**

- **display stp region-configuration**
- **region-name**
- **revision-level**

目次

このセクションのページは **3-x-x** です。

9 章 ループ検出.....9-1
9.1 ループ検出設定コマンド.....9-1
9.1.1 display loopback-detection.....9-1
9.1.2 loopback-detection action.....9-2
9.1.3 loopback-detection enable.....9-4
9.1.4 loopback-detection global action.....9-5
9.1.5 loopback-detection global enable.....9-6
9.1.6 loopback-detection interval-time.....9-7

9章 ループ検出

9.1 ループ検出設定コマンド

9.1.1 display loopback-detection

Syntax

display loopback-detection

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display loopback-detection コマンドはループバック検出の設定と状態を表示します。

例

ループバック検出の設定と状態を表示します。

<Switch> display loopback-detection

```
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
 Interface              Action mode     VLANs
 GigabitEthernet1/0/1    Shutdown        10
```

表 9-1 コマンド出力

フィールド	説明
Action mode	ループガードのアクションです。 • **Block**—ポートでループが検出されたとき、装置は次の動作を実行します。 　• ログを生成します。 　• 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。 • **Shutdown**—ポートでループが検出されたとき、装置は次の操作を実行します。 　• ログを生成します。 　• ポートをシャットダウンして、ポートがフレームを送受信できないようにします。装置は、一定時間後に自動的にポートをフォワーディングステートに設定します。**shutdown-interval**コマンドを使用して時間間隔を設定します。詳細はコマンドマニュアルのセクション1 *はじめに* “*装置管理*”を参照してください。
VLANs	インタフェースが属するVLAN、およびループが検出されたVLANです。

9.1.2 loopback-detection action

Syntax

Layer 2 Ethernet interface view：

loopback-detection action { **block** | **no-learning** | **shutdown** }

undo loopback-detection action

Layer 2 aggregate interface view：

loopback-detection action shutdown

undo loopback-detection action

デフォルト

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。ループが検出された場合、装置は次の操作を実行します。

- ログを生成します。
- 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。

レイヤ 2 アグリゲートインタフェースはこのキーワードをサポートしません。

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: shutdown モードを有効にします。ループを検出すると、装置はログを出力し、すべてのフレームの送受信を無効にするためポートをシャットダウンします。装置は検出タイマが終了すると、自動でポートをアップします。**shutdown-interval** コマンドで検出タイマを設定することができます。詳細はコマンドマニュアルのセクション 1 *はじめに* “*装置管理*”を参照してください。

説明

loopback-detection action コマンドはポートのループ保護のアクションを設定します。

undo loopback-detection action コマンドは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 **shutdown** 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: 最大 10 個の VLAN 項目のスペース区切りリストを指定します。各項目は、*vlan-id1* から *vlan-id2* の形式で、VLAN ID または VLAN ID の範囲を指定します。VLAN ID の値の範囲は 1～4094 です。*vlan-id2* の ID は、*vlan-id1* の ID 以上でなければなりません。

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。

ループ検出はグローバルに、またはポートごとに有効にできます。ポートがいずれかの VLAN で検出フレームを受信すると、ループ検出が有効になっているかどうかに関係なく、そのポートでループ保護アクションがトリガされます。

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: shutdown 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、自動でポートをアップします。**shutdown-interval** コマンドで検出タイマを設定することができます。詳細はコマンドマニュアルのセクション 1 *はじめに* “*装置管理*”を参照してください。

説明

loopback-detection 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。

例

グローバルでループ保護のアクションを **shutdown** 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

すべての VLAN で有効

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: 最大 10 個の VLAN 項目のスペース区切りリストを指定します。各項目は、*vlan-id1* から *vlan-id2* の形式で、VLAN ID または VLAN ID の範囲を指定します。VLAN ID の設定範囲は 1～4094 です。*vlan-id2* の ID は、*vlan-id1* の ID 以上である必要があります。

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。

ループ検出は、グローバルに有効にすることも、ポート単位で有効にすることもできます。ポートが通信を許可している VLAN の検出フレームを受信すると、設定されているループ保護アクションを実行します。ループ検出が有効になっているかどうかは関係ありません。

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 30 秒に戻します。

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。

undo loopback-detection interval-time コマンドを使用しても、デフォルトに戻すことはできません。interval-time を再設定するには、**loopback-detection interval-time5** コマンドを使用する必要があります。

例

ループ検出間隔を 10 秒に設定します。

<Switch> system-view

[Switch] loopback-detection interval-time 10

関連コマンド

display loopback-detection

目次

このセクションのページは **3-x-x** です。

10 章 VLAN 10-1
10.1 VLAN 設定コマンド 10-1
10.1.1 description 10-1
10.1.2 display interface vlan-interface 10-2
10.1.3 display vlan 10-5
10.1.4 display vlan brief 10-7
10.1.5 interface vlan-interface 10-8
10.1.6 name 10-9
10.1.7 reset counters interface vlan-interface 10-10
10.1.8 shutdown 10-11
10.1.9 vlan 10-12
10.2 ポートベース VLAN 設定コマンド 10-13
10.2.1 display port 10-13
10.2.2 port 10-14
10.2.3 port access vlan 10-15
10.2.4 port hybrid pvid 10-16
10.2.5 port hybrid vlan 10-17
10.2.6 port link-type 10-19
10.2.7 port trunk permit vlan 10-19
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 10-23
10.3.3 mac-vlan enable 10-24
10.3.4 mac-vlan mac-address 10-25
10.3.5 mac-vlan trigger enable 10-26
10.3.6 port pvid forbidden 10-27
10.3.7 vlan precedence 10-28
10.4 IP サブネットベース VLAN 設定コマンド 10-29
10.4.1 display ip-subnet-vlan interface 10-29
10.4.2 display ip-subnet-vlan vlan 10-31
10.4.3 ip-subnet-vlan 10-32
10.4.4 port hybrid ip-subnet-vlan 10-33
10.5 プロトコルベース VLAN 設定コマンド 10-34
10.5.1 display protocol-vlan interface 10-34
10.5.2 display protocol-vlan vlan 10-36

10.5.3 port hybrid protocol-vlan 10-37
10.5.4 protocol-vlan 10-39

10章 VLAN

10.1 VLAN設定コマンド

10.1.1 description

Syntax

description *text*

undo description

デフォルト

VLAN の説明は **VLAN** *vlan-id* です。*vlan-id* は 4 桁で VLAN ID を指定します。VLAN ID が 4 桁未満の場合、先頭に 0 が付加されます。たとえば、VLAN 100 の VLAN のデフォルト説明は **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 および VLAN インタフェースを効率的に管理するには、VLAN および VLAN インタフェースの機能または接続に基づいて、VLAN および VLAN インタフェースの説明を設定します。

例

VLAN 2 の説明を **sales-private** に設定します。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] description sales-private

VLAN インタフェース 2 の説明を **linktoPC56** に設定します。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] quit

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] description linktoPC56

関連コマンド

- **display interface vlan-interface**
- **display vlan**

10.1.2 display interface vlan-interface

Syntax

display interface vlan-interface [*interface-number*] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-interface *interface-number*: VLAN インタフェース番号を指定します。指定しない場合、すべての VLAN インタフェースの情報を表示します。

brief: インタフェースの概要情報を表示します。このキーワードを指定しない場合、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。このキーワードを指定しない場合、説明の最初の 27 文字のみを表示します。

down: VLAN インタフェースが down 状態で、その原因が表示されます。このキーワードを指定しない場合、コマンドはすべての状態の VLAN インタフェースに関する情報を表示します。

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 10 の情報を表示します。

<Switch> display interface vlan-interface 10

```
Vlan-interface10
Current state: UP
Line protocol state: UP
Description: Vlan-interface10 Interface
Bandwidth: 100000kbps
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。

フィールド	説明
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 transmission unit	VLANインタフェースのMTUです。
Internet protocol processing : disabled	VLANインタフェースにはIPアドレスが割り当てられておらず、IPパケットを処理できません。
Internet Address	VLANインタフェースのIPアドレスです。プライマリ属性は、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の送信フレームの形式です。
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の送信フレームの形式です。
Last clearing of counters	**reset counters interface vlan-interface**コマンドが実行された最新の時刻です。このコマンドを実行したことがない場合、このフィールドには**Never**と表示されます。
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。

フィールド	説明
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。この状態はリンクが準備できていないとき、装置がオンデマンドリンクのセットアップを初期化します。
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 を指定します。このキーワードを指定すると、コマンドは、ダイナミック VLAN の総数と各ダイナミック VLAN ID を表示します。ダイナミック VLAN は、RADIUS サーバによって割り当てられます。

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 を指定します。このキーワードを指定すると、コマンドは、スタティック VLAN の総数と各スタティック VLAN 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。

フィールド	説明
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。VLANインタフェースにIPv4アドレスが設定されている場合にのみ表示されます。 VLANインタフェースにセカンダリIPv4アドレスも設定されている場合は、次のいずれかのコマンドを使用して、セカンダリIPv4アドレスを表示できます。 • **display interface vlan-interface** • **display this （VLAN interface view）**
Subnet mask	プライマリIPv4アドレスのサブネットマスクです。(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使用可能です)
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 に移行あるいはデフォルトの VLAN インタフェースの view に移行します。

undo interface vlan-interface コマンドは指定された 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。

サブ VLAN の VLAN インタフェースを作成することはできません。サブ VLAN はサポートしていません。

以下に示す、セカンダリ VLAN の VLAN インタフェースを作成することはできません。

- 同一プライマリ VLAN に関連しています。
- プライマリ VLAN インタフェースの VLAN interface view のレイヤ 3 通信で有効になっています。

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

VLAN *vlan-id* です。*vlan-id* は 4 桁の VLAN ID です。VLAN ID が 4 桁未満の場合、先頭に 0 が付加されます。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。

802.1 X または MAC アドレス認証の場合、名前または ID によって認可 VLAN を指定できます。多数の VLAN が設定されている場合は、VLAN 名を使用して VLAN を識別します。

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 インタフェースを番号で指定します。指定しない場合、すべての VLAN インタフェースの統計情報を削除します。

説明

reset counters interface vlan-interface コマンドは VLAN インタフェース上の統計情報を削除します。

期間内に統計情報を収集する前に履歴統計情報を削除するには、このコマンドを使用します。

例

VLAN インタフェース 2 で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。VLAN の 1 つ以上のポートが up である場合、VLAN インタフェースは up になり、VLAN のすべてのポートが down である場合、VLAN インタフェースは down します。

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。

shutdown コマンドでシャットダウンした 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。

故障したインタフェースを修理するため、**shutdown** コマンドを使用し、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-id-list* | **all** }

undo vlan { *vlan-id-list* | **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-id-list: 最大 32 の VLAN 項目のスペース区切りリストを指定します。

各項目は VLAN または VLAN の範囲を vlan-id1 [to vlan-id2]の形式で指定します。

vlan-id2 の値は、*vlan-id1* の値以上である必要があります。*vlan-id* の設定範囲は、1～4094 です。

all: 予約された VLAN を除くすべての VLAN を指定します。

装置上に作成できる VLAN の最大数が 4094 未満の場合、このキーワードはサポートされません。

説明

vlan *vlan-id-list* コマンドは予約済み VLAN を除いて VLAN をバッチで作成します。

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(VLAN1)または予約済み VLAN を作成または削除することはできません。

アプリケーションによってロックされているダイナミック VLAN または VLAN を削除する前に、VLAN から設定を削除する必要があります。

例

VLAN 2 を作成し、その view に移行します。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2]

VLAN2 および、VLAN 4～VLAN 100 を作成します。

<Switch> system-view

[Switch] vlan 2 4 to 100

関連コマンド

display vlan

10.2 ポートベースVLAN設定コマンド

10.2.1 display port

Syntax

display port { **hybrid** | **trunk** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

hybrid: ハイブリッドポートを指定します。

trunk: トランクポートを指定します。

説明

display port コマンドはハイブリッドポートあるいはトランクポートに関する情報を表示します。

例

ハイブリッドポートの情報を表示します。

<Switch> display port hybrid

```
Interface          PVID  VLAN Passing
GE1/0/1           100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                  2555-2558, 3000, 4000
                        Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                  150-160, 200, 255, 286, 300-302
```

トランクポートの情報を表示します。

<Switch> display port trunk

```
Interface          PVID  VLAN Passing
GE1/0/2            2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                          555, 600-611, 1000, 2006-2008
```

表 10-4 コマンド出力

フィールド	説明
Interface	ポート名です。
PVID	ポートのVLAN IDです。
VLAN Passing	ポートで許可されたVLANです。
Tagged	VLANタグを削除しないでポートがパケットを送信するVLANです。
Untagged	VLANタグを削除した後、ポートがパケットを送信するVLANです。

10.2.2 port

Syntax

port *interface-list*

undo port *interface-list*

デフォルト

VLAN 1

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number1* [**to** *interface-type interface-number2*]です。*interface-number2* は *interface-number1* 以上の値にしてください。

説明

port コマンドは指定したアクセスポートに VLAN を割り当てます。

undo port コマンドは VLAN から指定したアクセスポートを削除します。

このコマンドはアクセスポートのみ適用可能です。

デフォルトですべてのポートはアクセスポートです。ポートタイプを **port link-type** コマンドで設定することができます。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 に VLAN 2 を割り当てます。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3

関連コマンド

display vlan

10.2.3 port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

すべての VLAN は VLAN1 に所属しています。

View

Layer 2 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。

説明

port access vlan コマンドはアクセスポートを指定した VLAN に割り当てます。

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

アクセスポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

例

GigabitEthernet 1/0/1 に VLAN 3 を割り当てます。

<Switch> system-view

[Switch] vlan 3

[Switch-vlan3] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port access vlan 3

10.2.4 port hybrid pvid

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートの PVID はポートが所属している VLAN の ID です。

View

Layer 2 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。

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、**port hybrid vlan** コマンドを使用してハイブリッドポートに PVID を設定してください。

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 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: 最大 32 の VLAN 項目のスペース区切りリストを指定します。各項目は VLAN ID または VLAN ID の範囲を *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-id2* の値は、*vlan-id1* の値以上でなければなりません。指定された VLAN は、装置上にすでに存在している必要があります。

tagged: 指定した VLAN タグを付けるメンバとしてポートを設定します。VLAN タグを削除しないメンバは、VLAN タグを削除せずに VLAN のパケットを送信します。

untagged: 指定した VLAN タグを削除するメンバとしてポートを設定します。VLAN タグを削除するメンバは、VLAN タグを削除して VLAN のパケットを送信します。

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

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、タグを付けて送信するよう VLAN 2、VLAN 4 および VLAN50～VLAN100 に割り当てます。

<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 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

access: ポートのリンクタイプをアクセスとして設定します。

hybrid: ポートのリンクタイプをハイブリッドとして設定します。

trunk: ポートのリンクタイプをトランクとして設定します。

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 コマンドはポートをデフォルトリンクタイプに戻します。

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 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: 最大 32 の VLAN 項目のスペース区切りリストを指定します。各項目は VLAN ID または VLAN ID の範囲を vlan-id1 **to** vlan-id2 の形式で指定します。VLAN ID の設定範囲は 1 から 4094 です。vlan-id2 の値は、vlan-id1 の値以上でなければなりません。

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

トランクポート GigabitEthernet 1/0/1 を VLAN 2、VLAN 4 および VLAN 50 から 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 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。

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、**port trunk permit vlan** コマンドを使用してトランクポートの PVID を設定ください。

例

トランクポート GigabitEthernet 1/0/1 の 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。*mac-address* の形式は H-H-H です。

mask *mac-mask*: MAC から VLAN へのエントリで MAC アドレスを一致させるためのマスクを指定します。*mac-mask* の場合、上位ビットは、2 進表記で連続する 1s か、16 進表記で連続する F でなければなりません。デフォルト値は 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。
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 aggregate interface 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 H-H-H の形式で指定します。MAC アドレスをマルチキャスト MAC アドレスまたはすべて 0 にすることはできません。MAC アドレスを設定する場合、各 H セクションの先頭のゼロは省略できます。たとえば、MAC アドレス 000f-00e2-0001 を設定するには、**f-e2-1** だけを入力します。

mask *mac-mask*: MAC アドレスマスクを指定します。mac-mask の場合、上位ビットは、2 進表記で連続する 1s か、16 進表記で連続する F でなければなりません。デフォルト値は 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*: エントリ-VLAN MAC に固有の VLAN の 802.1p プライオリティを指定します。*priority* の値の範囲は 0~7 で、既定値は 0 です。値が大きいほど、802.1p 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-to-VLAN エントリを指定します。

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 VLAN100 に関連付けて、VLAN100 の 802.1 p プライオリティを 7 に設定します。

<Switch> system-view

[Switch] mac-vlan mac-address 0-1-1 vlan 100 dot1p 7

VLAN100 を、6 つの上位ビットが 121122 である MAC アドレスに関連付けて、このエントリの VLAN100 の 802.1 p プライオリティを 4 に設定します。

<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。

ポートへの VLAN 割り当ては、受信したパケットの送信元エントリアドレスが MAC-to-VLAN MAC アドレスと正確に一致した場合にのみトリガされます。

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 の割り当てにのみ使用します。

例

GigabitEthernet 1/0/1 でパケットの送信元 MAC アドレスが MAC アドレス-VLAN エントリに一致しないとき、PVID でのパケットの転送を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port pvid forbidden

関連コマンド

mac-vlan trigger enable

10.3.7 vlan precedence

Syntax

vlan precedence { **mac-vlan** | **ip-subnet-vlan** }

undo vlan precedence

デフォルト

mac-vlan

View

Layer 2 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

mac-vlan: MAC アドレスベース VLAN を優先します。

ip-subnet-vlan: IP サブネットベース VLAN を優先します。

説明

vlan precedence コマンドは MAC アドレスベース VLAN と IP サブネットベース VLAN の両方がポートに設定されたときの VLAN の優先順位を設定します。

undo vlan precedence コマンドはデフォルトに戻します。

このコマンドは MAC アドレスベース VLAN と IP サブネットベース VLAN でのみ適用されます。

ダイナミック MAC ベース VLAN が有効なとき、MAC ベース VLAN の優先度を保証するため、**vlan precedence mac-vlan** コマンドを設定することを推奨します。**vlan**

precedence ip-subnet-vlan コマンドを使用している場合、このコマンドは適用されません。

例

GigabitEthernet 1/0/1 で MAC アドレスベース VLAN を優先します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] vlan precedence mac-vlan

関連コマンド

mac-vlan trigger enable

10.4 IPサブネットベースVLAN設定コマンド

10.4.1 display ip-subnet-vlan interface

Syntax

display ip-subnet-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number1 **to** *interface-type interface-number2*:インタフェース範囲を指定します。*interface-type interface-number1* と *interface-type interface-number2* は、どちらもインタフェースタイプとインタフェース番号を表します。*interface-number2* の値は、*interface-number1* の値以上である必要があります。

all: すべてのポートを指定します。

説明

display ip-subnet-vlan interface コマンドは指定したポートに関連づけられた IP サブネットベース VLAN の情報を表示します。

例

GigabitEthernet 1/0/1 に関連づけられた IP サブネットベース VLAN の情報を表示します。

<Switch> display ip-subnet-vlan interface gigabitethernet 1/0/1

```
Interface: GigabitEthernet1/0/1
 VLAN ID   Subnet index  IP address      Subnet mask      Status
 3         0             192.168.1.0     255.255.255.0    Active
 4         N/A           N/A             N/A              Inactive
 4094      65535         172.16.1.1      255.255.0.0      Inactive
```

表 10-6 コマンド出力

フィールド	説明
VLAN ID	IPサブネットベースVLANのIDです。
Subnet index	IPサブネットのインデックスです。 IPサブネットベースVLANが設定されていない場合、**N/A**と表示されます。
IP address	サブネットのIPアドレスです。IPアドレスあるいはサブネットアドレスです。 VLANのIPサブネットが設定されていない場合、**N/A**と表示されます。
Subnet mask	IPサブネットのマスクです。 VLANのサブネットマスクが設定されていない場合、**N/A**と表示されます。

Status	IPサブネットベースVLANがポートで適用されているかどうかを示します。
	• **Active**–IPサブネットベースVLANが適用されています
	• **Inactive**–IPサブネットベースVLANが適用されていません。たとえば、以下の状況である場合、表示されます。
	  • IPサブネットベースVLANの設定が完了していません。
	  • ポートがIPサブネットベースVLANを許可していません。

関連コマンド

- **display ip-subnet-vlan vlan**
- **ip-subnet-vlan**
- **port hybrid ip-subnet-vlan**

10.4.2 display ip-subnet-vlan vlan

Syntax

display ip-subnet-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id1: IP サブネットベース VLAN の VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN ID の範囲を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての IP サブネットベース VLAN を指定します。

説明

display ip-subnet-vlan vlan コマンドは IP サブネットベース VLAN の情報を表示します。

例

すべての IP サブネットベース VLAN の情報を表示します。

<Switch> display ip-subnet-vlan vlan all

```
VLAN ID: 3
 Subnet index    IP address      Subnet mask
 0               192.168.1.0     255.255.255.0
```

表 10-7 コマンド出力

フィールド	説明
VLAN ID	IPサブネットベースVLANのVLAN IDです。
Subnet index	IPサブネットのインデックスです。
IP address	サブネットのIPアドレスです。IPアドレスあるいはサブネットアドレスです。
Subnet mask	IPサブネットのマスクです。

関連コマンド

- **display ip-subnet-vlan interface**
- **ip-subnet-vlan**
- **port hybrid ip-subnet-vlan**

10.4.3 ip-subnet-vlan

Syntax

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* [*mask*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

デフォルト

設定なし

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-subnet-index: IP サブネットの開始インデックスです。設定範囲は 0～65535 です。この値はユーザによって設定することができます。またシステムによって IP サブネットあるいは IP アドレスが VLAN に関連づけられた順番にもとづいて自動で番号が付けられます。

ip *ip-address* [*mask*]: サブネットベース VLAN の分類のもとになっている送信元 IP アドレスまたはネットワークアドレスを、ドット区切り 10 進法で指定します。*mask* は、ドット区切り 10 進法の送信元 IP アドレスまたはネットワークアドレスのサブネットマスクで、デフォルト値は 255.255.255.0 です。

to *ip-subnet-end*: IP サブネットインデックスの範囲を指定します。設定範囲は 0～65535 です。*ip-subnet-end* は IP サブネットの開始インデックス以上の値にしてください。

all: VLAN に関連付けられているすべての IP サブネットまたは IP アドレスを指定します。

説明

ip-subnet-vlan コマンドは VLAN と、IP サブネットあるいは IP アドレスを関連づけます。

undo ip-subnet-vlan コマンドは関連づけを削除します。

IP サブネットあるいは IP アドレスはマルチキャストネットワークセグメントあるいはマルチキャストアドレスにすることはできません。

例

VLAN 3 を IP サブネットベース VLAN になるよう設定し、これをサブネット 192.168.1.0/24 に関連づけます。

<Switch> system-view

[Switch] vlan 3

[Switch-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0

関連コマンド

- **display ip-subnet-vlan interface**
- **display ip-subnet-vlan vlan**
- **port hybrid ip-subnet-vlan**

10.4.4 port hybrid ip-subnet-vlan

Syntax

port hybrid ip-subnet-vlan vlan *vlan-id*

undo port hybrid ip-subnet-vlan { **vlan** *vlan-id* | **all** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

all: すべての VLAN を指定します。

説明

port hybrid ip-subnet-vlan コマンドはポートを IP サブネットベース VLAN に関連づけます。

undo port hybrid ip-subnet-vlan コマンドは関連づけを削除します。

このコマンドを有効にするには、次のタスクを実行します。

1. VLAN を作成し、指定した IP サブネットまたは IP アドレスに関連付けます。
2. ポートリンクタイプをハイブリッドに設定します。

3. ポートを設定して、IP サブネットベース VLAN が通過できるようにします。

例

GigabitEthernet 1/0/1 を IP サブネットベース VLAN 3 に関連づけます。

<Switch> system-view

[Switch] vlan 3

[Switch-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0

[Switch-vlan3] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port link-type hybrid

[Switch-GigabitEthernet1/0/1] port hybrid vlan 3 untagged

[Switch-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 3

アグリゲートインタフェース Bridge-aggregation 1 を IP サブネットベース VLAN 3 に関連づけます。

<Switch> system-view

[Switch] vlan 3

[Switch-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0

[Switch-vlan3] quit

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] port link-type hybrid

[Switch-Bridge-Aggregation1] port hybrid vlan 3 untagged

[Switch-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3

関連コマンド

- **display ip-subnet-vlan interface**
- **display ip-subnet-vlan vlan**
- **ip-subnet-vlan**

10.5 プロトコルベースVLAN設定コマンド

10.5.1 display protocol-vlan interface

Syntax

display protocol-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number1 **to** *interface-type interface-number2*: インタフェース範囲を指定します。*interface-type interface-number1* と *interface-type interface-number2* は、どちらもインタフェースタイプとインタフェース番号を表します。*interface-number2* の値は、*interface-number1* の値以上である必要があります。

all: すべてのポートを指定します。

説明

display protocol-vlan interface コマンドは指定されたポートに関連づけられたプロトコルベース VLAN の情報を表示します。

例

GigabitEthernet 1/0/1 に関連づけられたプロトコルベース VLAN の情報を表示します。

<Switch> display protocol-vlan interface gigabitethernet 1/0/1

```
Interface: GigabitEthernet1/0/1
 VLAN ID  Protocol index  Protocol type          Status
 2        0              IPv6                  Active
 2        1               N/A                   Inactive
 4094     65535          IPv4                  Inactive
```

表 10-8 コマンド出力

フィールド	説明
VLAN ID	プロトコルベースVLANのIDです。
Protocol index	プロトコルテンプレートインデックスです。
Protocol type	プロトコルテンプレートで指定されたプロトコルタイプです。 プロトコルタイプが指定されていない場合、**N/A**と表示されます。
Status	プロトコルベースVLANがポートで適用されているかどうかを示します。 • **Active**–プロトコルベースVLANが適用されています • **Inactive**–プロトコルベースVLANが適用されていません。

関連コマンド

- **display protocol-vlan vlan**
- **port hybrid protocol-vlan**
- **protocol-vlan**

10.5.2 display protocol-vlan vlan

Syntax

display protocol-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id1: プロトコルベース VLAN の VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN ID の範囲を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべてのプロトコルベース VLAN を指定します。

説明

display protocol-vlan vlan コマンドはプロトコルベース VLAN の情報を表示します。

例

すべてのプロトコルベース VLAN の情報を表示します。

<Switch> display protocol-vlan vlan all

```
VLAN ID: 2
 Protocol index  Protocol type
 0               IPv4
 65535           IPv6

VLAN ID: 3
 Protocol index  Protocol type
 0               IPv4
 65535           LLC DSAP 0x11 SSAP 0x22
```

表 10-9 コマンド出力

フィールド	説明
VLAN ID	プロトコルベースVLANのIDです。
Protocol index	プロトコルベーステンプレートインデックスです。
Protocol type	プロトコルテンプレートで指定されたプロトコルタイプあるいはカプセル化フォーマットです。

関連コマンド

- **display protocol-vlan interface**
- **port hybrid protocol-vlan**
- **protocol-vlan**

10.5.3 port hybrid protocol-vlan

Syntax

port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

undo hybrid protocol-vlan { **vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } | **all** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

protocol-index: プロトコルテンプレートインデックスの開始インデックスです。設定範囲は 0～65535 です。

to *protocol-end*: プロトコルテンプレート範囲のエンドプロトコルテンプレートインデックスを 0 から 65535 の範囲で指定します。この値は、開始プロトコルテンプレートインデックス以上を指定する必要があります。

all: すべてのプロトコルテンプレートを指定します。

説明

port hybrid protocol-vlan コマンドはハイブリッドポートを VLAN の指定されたプロトコルに関連づけます。

undo port hybrid protocol-vlan コマンドは関連づけを削除します。

このコマンドを有効にするには、次の操作を実行します。

1. VLAN を作成し、指定したプロトコルテンプレートに関連付けます。
2. ポートリンクタイプをハイブリッドに設定します。
3. ポートを設定して、プロトコルベース VLAN が通過できるようにします。

ポートで **undo port hybrid protocol-vlan** コマンドを実行するときは、次のガイドラインに従ってください。

- *vlan-id* と **all** キーワードの両方を指定すると、このコマンドは、指定した VLAN のすべてのプロトコルテンプレートからポートの関連付けを解除します。
- **all** キーワードのみを指定する場合、このコマンドは、すべての VLAN のすべてのプロトコルテンプレートからポートを分離します。

例

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、タグなしメンバとして VLAN 2 に割り当て、それを VLAN 2 のプロトコルテンプレート 1 に関連付けます。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] protocol-vlan 1 ipv4

[Switch-vlan2] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port link-type hybrid

[Switch-GigabitEthernet1/0/1] port hybrid vlan 2 untagged

[Switch-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 2 1

ハイブリッドアグリゲートインタフェース Bridge-Aggregation 1 を VLAN 2 のプロトコルテンプレート 1（IPv4）に関連づけます。

レイヤ 2 aggregate interface Bridge-Aggregation 1 をハイブリッドポートとして設定し、タグなしメンバとして VLAN 2 に割り当て、それを VLAN 2 のプロトコルテンプレート 1 に関連付けます。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] protocol-vlan 1 ipv4

[Switch-vlan2] quit

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] port link-type hybrid

[Switch-Bridge-Aggregation1] port hybrid vlan 2 untagged

[Switch-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 1

10.5.4 protocol-vlan

Syntax

protocol-vlan [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }

undo protocol-vlan { *protocol-index* [**to** *protocol-end*] | **all** }

デフォルト

設定なし

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

at: AppleTalk ベース VLAN を指定します。

ipv4: IPv4 ベース VLAN を指定します。

ipv6: Ipv6 ベース VLAN を指定します。

ipx: IPX ベース VLAN を指定します。キーワード **ethernetii**、**llc**、**raw**、および **snap** は、IPX カプセル化形式を指定します。

mode: VLAN 用の自己定義したプロトコルテンプレートを設定します。**ethernetii**、**llc**、および **snap** は有効なカプセル化フォーマットです。

ethernetii etype *etype-id*: カプセル化形式と指定されたプロトコルタイプ ID に一致します。*etype-id* には、着信パケットのプロトコルタイプ ID を、800、86dd、809b、および 8137 を除く 16 進表記で指定します。設定範囲は 600～ffff です。

llc: 一致する LLC カプセル化フォーマットを指定します。

dsap *dsap-id*: DSAP(Destination Service Access Point)を指定します。16 進表記で設定範囲は 0～ff です。

ssap *ssap-id*: SSAP(Source Service Access Point)を指定します。設定範囲は 0～ff です。16 進数表記で指定します。

snap etype *etype-id*: SNAP カプセル化形式と指定されたプロトコルタイプ値を照合します。*etype-id* には、インバウンドパケットの Ethernet タイプを指定します。設定範囲は 600～ffff です。(8137 を除く)

protocol-index: プロトコルインデックスを指定します。設定範囲は 0～65535 です。指定しない場合、システムは自動的にインデックスを割り当てます。

to *protocol-end*: プロトコルテンプレートの終了インデックスを指定します。設定範囲は 0～65535 です。*protocol-end* は *protocol-index* 以上の値にしてください。

all: VLAN に割り当てられたすべてのプロトコルを削除するよう指定します。

説明

注意:

IP はイーサネットのアドレス解決のため ARP を使用します。通信障害を防止するため、同一の VLAN の IP と ARP のテンプレートを設定し、同一のポートでそれらを関連づけてください。

protocol-vlan コマンドは VLAN をプロトコルベース VLAN およびプロトコルテンプレートに設定します。

undo protocol-vlan コマンドは設定されているプロトコルテンプレートを削除します。

mode を使用した場合、以下のガイドラインに従ってください。

- **ethernetii etype** *etype-id* オプションの *etype-id* には、次の 16 進数値を設定しないでください。
  - **800**–Ethernet II カプセル化の IPv4 プロトコルを指定します。
  - **809b**–Ethernet II カプセル化の AppleTalk プロトコルを指定します。
  - **8137**–Ethernet II カプセル化の IPX プロトコルを指定します。
  - **86dd**–Ethernet II カプセル化の IPv6 プロトコルを指定します。
- *dsap-id* と *ssap-id* の両方に、次のいずれかの 16 進値を設定しないでください。
  - **e0**–IPX パケットの 802.2 LLC カプセル化形式を指定します。
  - **ff**–IPX パケットの 802.3 raw カプセル化形式を指定します。
  - **aa**–802.2 SNAP カプセル化形式を指定します。

dsap-id と *ssap-id* のいずれかが設定されている場合、システムは 16 進数値 aa をもう一方に割り当てます。

- **snap etype** *etype-id* オプションの *etype-id* を 16 進数値の 8137 に設定しないでください。それ以外の場合、テンプレートの形式は IPX プロトコルのものと同じになります。*etype-id* には、16 進数値の 800、809b、または 86dd を設定できます。16 進数値 800、809b、および 86dd は、それぞれ IPv4、AppleTalk、および IPv6 に対応します。

例

Ethernet II カプセル化の ARP パケットと IPv4 パケットを転送用に VLAN3 に割り当てます。(ARP のプロトコルタイプ ID は、16 進数表記で 0806 です。)

<Switch> system-view

[Switch] vlan 3

[Switch-vlan3] protocol-vlan 1 ipv4

[Switch-vlan3] protocol-vlan 2 mode ethernetii etype 0806

関連コマンド

- **display protocol-vlan interface**
- **display protocol-vlan vlan**
- **port hybrid protocol-vlan**

目次

このセクションのページは **3-x-x** です。

11 章 Private VLAN 11-1
11.1 Private VLAN コマンド 11-1
11.1.1 display private-vlan 11-1
11.1.2 port private-vlan host 11-4
11.1.3 port private-vlan promiscuous 11-6
11.1.4 port private-vlan trunk promiscuous 11-8
11.1.5 port private-vlan trunk secondary 11-11
11.1.6 private-vlan (VLAN interface view) 11-15
11.1.7 private-vlan (VLAN view) 11-17
11.1.8 private-vlan isolated 11-18
11.1.9 private-vlan primary 11-20

11章 Private VLAN

11.1 Private VLAN コマンド

11.1.1 display private-vlan

Syntax

display private-vlan [*primary-vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

primary-vlan-id: プライマリ VLAN ID を指定します。設定範囲は 1～4094 です。

プライマリ VLAN を指定しない場合は、すべてのプライマリ VLAN ID と関連するセカンダリ VLAN を表示します。

説明

display private-vlan コマンドはプライマリ VLAN とそれに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 とそれに関連するセカンダリ VLAN の情報を表示します。

<Switch> display private-vlan

```
Primary VLAN ID: 2
Secondary VLAN ID: 3-4

VLAN ID: 2
VLAN type: Static
Private VLAN type: Primary
Route interface: Configured
IPv4 address: 1.1.1.1
IPv4 subnet mask: 255.255.255.0
IPv6 global unicast addresses:
  2001::1, subnet is 2001::/64 [TENTATIVE]
```

```
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:  None
Untagged ports:
  GigabitEthernet1/0/2
  GigabitEthernet1/0/3
  GigabitEthernet1/0/4

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:  None
Untagged ports:
  GigabitEthernet1/0/2
  GigabitEthernet1/0/3

VLAN ID: 4
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged ports:  None
Untagged ports:
  GigabitEthernet1/0/2
  GigabitEthernet1/0/4
```

表 11-1 コマンド出力

フィールド	説明
VLAN type	VLANタイプを示します。Dynamicまたはstaticを表示します。
Private VLAN type	プライベートVLANタイプ示します。 ● **Primary**： プライマリVLAN ● **Secondary**： セカンダリVLAN ● **Isolated secondary**： L2で隔離したセカンダリVLAN
Route interface	VLANインタフェースのありなしを示します。 ● Configured ● Not configured

フィールド	説明
IPv4 address	VLANインタフェースのプライマリIPv4アドレスを示します。このフィールドはIPv4アドレスを設定しているときに表示されます。セカンダリIPv4アドレスについても同様です。 以下のいずれかのコマンドで確認ができます。 • **display interface vlan-interface** • **display this (VLAN interface view)**
IPv4 subnet mask	VLANインタフェースのプライマリIPv4アドレスのサブネットを示します。このフィールドはIPv4アドレスを設定しているときに表示されます。
IPv6 global unicast addresses	VLANインタフェースのグローバルユニキャストIPv6アドレスを示します。このフィールドはIPv6アドレスを設定しているときに表示されます。 IPv6アドレスの状態を以下に示します。 • **TENTATIVE**： 初期状態。DADの処理前か処理中を示します。この状態のアドレスは送信元アドレスまたは宛先アドレスとして使用できません。 • **DUPLICATE**： DADによるアドレス重複検出。アドレスがユニークでないため使用できません。 • **PREFERRED**： アドレスがpreferredで送信元または宛先として使用できます。このコマンドではこのアドレスの状態を表示しません。 • **DEPRECATED**： アドレスがpreferredライフタイムとvalidライフタイムの間にある状態を示します。有効なアドレスですが、新規の通信には使用できません。
Description	VLANの説明を示します。
Name	VLAN名を示します。
Tagged ports	VLANのTaggedメンバを示します。
Untagged ports	VLANのUntaggedメンバを示します。

関連コマンド

- **private-vlan (VLAN view)**
- **private-vlan primary**

11.1.2 port private-vlan host

Syntax

port private-vlan host

undo port private-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

port private-vlan host コマンドはポートをホストポートとして設定します。

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
```

出力は次のことを示します。GigabitEthernet 1/0/1 はブリッジモードで動作しており、ホストポートです。

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
```

出力には次のように表示されます。

- GigabitEthernet 1/0/1 は、セカンダリ VLAN 20 およびプライマリ VLAN 2 の untagged メンバです。
- GigabitEthernet 1/0/1 のポートリンクタイプはハイブリッドで、その PVID は VLAN 20 です。

関連コマンド

- **port private-vlan promiscuous**
- **port private-vlan trunk promiscuous**
- **port private-vlan trunk secondary**
- **private-vlan (VLAN view)**
- **private-vlan primary**

11.1.3 port private-vlan promiscuous

Syntax

port private-vlan *vlan-id* **promiscuous**

undo port private-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。VLAN1 は有効な値の範囲内にありますが、コマンドでは設定できません。

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 に関する情報を表示します。

<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
```

出力はそれを示したものです。

- GigabitEthernet 1/0/1 がプライマリ VLAN 2 から削除されます。
- GigabitEthernet 1/0/1 は、VLAN2 の untagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプと PVID は変更されません。

関連コマンド

- **port private-vlan host**
- **port private-vlan trunk promiscuous**
- **port private-vlan trunk secondary**
- **private-vlan (VLAN view)**
- **private-vlan primary**

11.1.4 port private-vlan trunk promiscuous

Syntax

port private-vlan *vlan-id-list* **trunk promiscuous**

undo port private-vlan *vlan-id-list* **trunk promiscuous**

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list： プライマリ VLAN リストを最大 10 個まで設定します。設定範囲は 1～4094 です。プライマリ VLAN の指定はスペースを空けて指定するか、*vlan-id1* **to** *vlan-id2* の形式で指定します。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**

11.1.5 port private-vlan trunk secondary

Syntax

port private-vlan *vlan-id-list* **trunk secondary**

undo port private-vlan *vlan-id-list* **trunk secondary**

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list： セカンダリ VLAN リストを最大 10 個まで設定します。設定範囲は 1～4094 です。セカンダリ VLAN の指定はスペースを空けて指定するか、*vlan-id1* **to** *vlan-id2* の形式で指定します。v*lan-id2* の値は *vlan-id1* の値と同じか大きな値を指定してください。

VLAN 1 は設定可能な範囲ですが、コマンドによる設定はできません。

説明

port private-vlan trunk secondary コマンドは指定した VLAN のトランクセカンダリポートとしてポートを設定し、これらの VLAN にポートを割り当てます。

undo port private-vlan trunk secondary コマンドは指定した VLAN のポートのトランクセカンダリ属性をキャンセルします。

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** 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 タグなしパケットを転送します。

例

- この例では、VLAN2 と 3 がプライマリ VLAN で、VLAN2 が VLAN20 のセカンダリ VLAN に関連付け、VLAN3 が VLAN30 のセカンダリ VLAN に関連付けされています。

GigabitEthernet 1/0/1 の設定情報を確認します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] display this

```
#
 interface GigabitEthernet1/0/1
#
return
```

GigabitEthernet 1/0/1 を VLAN20 と 30 のトランクセカンダリポートに設定して、設定情報を確認します。

[Switch-GigabitEthernet1/0/1] port private-vlan 20 30 trunk secondary

[Switch-GigabitEthernet1/0/1] display this

```
#
 interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 2 3 20 30 tagged
 port hybrid vlan 1 untagged
 port private-vlan 20 30 trunk secondary
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 は VLAN20 と 30 のトランクセカンダリポートです。
- GigabitEthernet 1/0/1 は VLAN2、3、20、30 の tagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプはハイブリッドです。

undo port private-vlan trunk secondary コマンドを GigabitEthernet 1/0/1 で実行して、設定を確認します。

[Switch-GigabitEthernet1/0/1] undo port private-vlan 20 30 trunk secondary

[Switch-GigabitEthernet1/0/1] display this

```
#
 interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 2 3 tagged
 port hybrid vlan 1 untagged
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 が VLAN20 と 30 から削除されました。
- GigabitEthernet 1/0/1 は VLAN2 と 3 の tagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプと PVID は変更されません。

- この例では、VLAN10 がセカンダリ VLAN ではありません。

GigabitEthernet 1/0/1 の設定情報を確認します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] display this

```
#
 interface GigabitEthernet1/0/1
#
return
```

GigabitEthernet 1/0/1 を VLAN10 のトランクセカンダリポートに設定して、設定情報を確認します。

[Switch-GigabitEthernet1/0/1] port private-vlan 10 trunk secondary

[Switch-GigabitEthernet1/0/1] display this

```
#
 interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 10 tagged
 port hybrid vlan 1 untagged
 port private-vlan 10 trunk secondary
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 は VLAN10 のトランクセカンダリポートです。
- GigabitEthernet 1/0/1 は VLAN10 の tagged メンバポートです。
- GigabitEthernet 1/0/1 のリンクタイプはハイブリッドです。

undo port private-vlan trunk secondary コマンドを GigabitEthernet1/0/1 で実行して、設定情報を確認します。

[Switch-GigabitEthernet1/0/1] undo port private-vlan 10 trunk secondary

[Switch-GigabitEthernet1/0/1] display this

```
#
 interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 1 untagged
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 が VLAN10 から削除されました。
- GigabitEthernet 1/0/1 のリンクタイプと PVID は変更されません。

関連コマンド

- **port private-vlan host**
- **port private-vlan promiscuous**
- **port private-vlan trunk promiscuous**
- **private-vlan (VLAN view)**
- **private-vlan isolated**
- **private-vlan primary**

11.1.6 private-vlan (VLAN interface view)

Syntax

private-vlan secondary *vlan-id-list*

undo private-vlan [**secondary** *vlan-id-list*]

デフォルト

セカンダリ VLAN はレイヤ 3 で隔離されます。

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list： セカンダリ VLAN リストを最大 10 個まで設定します。設定範囲は 1～4094 です。セカンダリ VLAN の指定はスペースを空けて指定するか、*vlan-id1* **to** *vlan-id2* の形式で指定します。v*lan-id2* の値は *vlan-id1* の値と同じか大きな値を指定してください。

VLAN 1 は設定可能な範囲ですが、コマンドによる設定はできません。

説明

private-vlan secondary コマンドはプライマリ VLAN と関連付けられたセカンダリ VLAN 間のレイヤ 3 通信を有効にします。

undo private-vlan コマンドはプライマリ VLAN と関連付けられたセカンダリ VLAN 間のレイヤ 3 通信を無効にします。

このコマンドは以下の条件で動作します。

- コマンドはプライマリ VLAN インタフェースの VLAN interface view で実行されます。
- セカンダリ VLAN はプライマリ VLAN と関連付けられます。
- セカンダリ VLAN には VLAN インタフェースは作成されません。
- IP アドレスはプライマリ VLAN インタフェースに割り当てられます。
- プライマリ VLAN インタフェースのローカルプロキシ ARP が有効です。

レイヤ 3 通信が有効ではないセカンダリ VLAN のために VLAN インタフェースを作成できます。セカンダリ VLAN でレイヤ 3 通信が有効である場合は、この機能のために VLAN インタフェースを作成しないでください。

このコマンドを同じプライマリ VLAN インタフェース上で複数実行した場合、すべての指定されたセカンダリ VLAN がレイヤ 3 で通信が可能です。

undo private-vlan を実行する場合は、以下のガイドラインに従ってください。

- **secondary** *vlan-id-list* オプションを指定する場合は、指定されたセカンダリ VLAN に対するレイヤ 3 通信の設定を削除してください。
- **secondary** *vlan-id-list* オプションを指定しない場合は、プライマリ VLAN のすべてのセカンダリ VLAN に対するレイヤ 3 通信の設定を削除してください。

例

この例の要件を以下に示します。

- VLAN4 はプライマリ VLAN2 に関連付けるセカンダリ VLAN です。
- アップリンクポート(GigabitEthernet 1/0/2)は VLAN2 のプロミスカスポートです。
- ダウンリンクポート(GigabitEthernet 1/0/3 と GigabitEthernet 1/0/4)はそれぞれ VLANs 3 と 4 のホストポートです。
- セカンダリ VLAN3 と 4 はレイヤ 3 通信ができます。

VLAN 2 をプライマリ VLAN に設定してセカンダリ VLAN3 と 4 を関連付けます。

<Switch> system-view

[Switch] vlan 3 to 4

[Switch] vlan 2

[Switch-vlan2] private-vlan primary

[Switch-vlan2] private-vlan secondary 3 to 4

[Switch-vlan2] quit

GigabitEthernet 1/0/2 を VLAN2 のプロミスカスポートに設定します。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] port private-vlan 2 promiscuous

[Switch-GigabitEthernet1/0/2] quit

GigabitEthernet 1/0/3 を VLAN 3 に割り当てホストポートに設定します。

[Switch] interface gigabitethernet 1/0/3

[Switch-GigabitEthernet1/0/3] port access vlan 3

[Switch-GigabitEthernet1/0/3] port private-vlan host

[Switch-GigabitEthernet1/0/3] quit

GigabitEthernet 1/0/4 を VLAN 4 に割り当てホストポートに設定します。

[Switch] interface gigabitethernet 1/0/4

[Switch-GigabitEthernet1/0/4] port access vlan 4

[Switch-GigabitEthernet1/0/4] port private-vlan host

[Switch-GigabitEthernet1/0/4] quit

VLAN インタフェース 2 を作成して、VLAN3 と 4 とのレイヤ 3 通信を有効にします。

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] private-vlan secondary 3 to 4

IP アドレスを VLAN インタフェース 2 に割り当てます。

[Switch-Vlan-interface2] ip address 192.168.1.1 255.255.255.0

ローカルプロキシ ARP を VLAN インタフェース 2 で有効にします。

[Switch-Vlan-interface2] local-proxy-arp enable

関連コマンド

- **private-vlan (VLAN view)**
- **private-vlan primary**

11.1.7 private-vlan (VLAN view)

Syntax

private-vlan secondary *vlan-id-list*

undo private-vlan [**secondary** *vlan-id-list*]

デフォルト

プライマリ VLAN とセカンダリ VLAN の関連付けはありません。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

secondary *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**
- **private-vlan primary**

11.1.8 private-vlan isolated

Syntax

private-vlan isolated

undo private-vlan isolated

デフォルト

同じセカンダリ VLAN に属するポート間でレイヤ 2 通信ができます。

View

VLAN view

定義済みユーザロール

network-admin

説明

private-vlan isolated コマンドは同じセカンダリ VLAN のレイヤ 2 通信を隔離します。

undo private-vlan isolated コマンドは設定をデフォルトに戻します。

このコマンドは以下の条件で動作します。

- セカンダリ VLAN はプライマリ VLAN に関連付けされています。
- ポートはセカンダリ VLAN のホストポートまたはトランクセカンダリポートに設定されています。

このコマンドはプライマリ VLAN、およびサブ VLAN の設定コマンドと相互に排他的です。

例

この例の要件を以下に示します。

- VLAN4 はプライマリ VLAN2 に関連付けられたセカンダリ VLAN です。
- GigabitEthernet 1/0/1 は VLAN2 のプロミスカスポートです。
- GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 はホストポートです。
- GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 はセカンダリ VLAN4 をレイヤ 2 で隔離します。

VLAN2 とプライマリ VLAN とし、セカンダリ VLAN4 と関連付けます。

<Switch> system-view

[Switch] vlan 4

[Switch-vlan4] quit

[Switch] vlan 2

[Switch-vlan2] private-vlan primary

[Switch-vlan2] private-vlan secondary 4

[Switch-vlan2] quit

GigabitEthernet 1/0/1 を VLAN2 のプロミスカスポートに設定します。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port private-vlan 2 promiscuous

[Switch-GigabitEthernet1/0/1] quit

GigabitEthernet 1/0/2 を VLAN4 に割り当てホストポートに設定します。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] port access vlan 4

[Switch-GigabitEthernet1/0/2] port private-vlan host

GigabitEthernet 1/0/3 を VLAN 4 に割り当てホストポートに設定します。

[Switch] interface gigabitethernet 1/0/3

[Switch-GigabitEthernet1/0/3] port access vlan 4

[Switch-GigabitEthernet1/0/3] port private-vlan host

セカンダリ VLAN4 のレイヤ 2 を隔離します。

[Switch] vlan 4

[Switch-vlan4] private-vlan isolated

関連コマンド

- **private-vlan (VLAN view)**
- **private-vlan primary**

11.1.9 private-vlan primary

Syntax

private-vlan primary

undo private-vlan primary

デフォルト

設定なし

View

VLAN view

定義済みユーザロール

network-admin

説明

private-vlan primary コマンドは VLAN をプライマリ VLAN に設定します。

undo private-vlan primary コマンドは設定をデフォルトに戻します。

設定コマンドの同期動作は以下の条件に従います。

- このコマンドはセカンダリ VLAN と関連付けられた VLAN に設定されます。
- ポートはプロミスカス、トランクプロミスカス、ホスト、トランクセカンダリポートです。

例

VLAN5 をプライマリ VLAN に設定します。

<Switch> system-view

[Switch] vlan 5

[Switch-vlan5] private-vlan primary

関連コマンド

- **port private-vlan host**
- **port private-vlan promiscuous**
- **port private-vlan trunk promiscuous**
- **port private-vlan trunk secondary**
- **private-vlan primary**

目次

このセクションのページは **3-x-x** です。

12 章 Voice VLAN 12-1
12.1 Voice VLAN 設定コマンド 12-1
12.1.1 display voice-vlan mac-address 12-1
12.1.2 display voice-vlan state 12-2
12.1.3 voice-vlan aging 12-3
12.1.4 voice-vlan enable 12-4
12.1.5 voice-vlan mac-address 12-5
12.1.6 voice-vlan mode auto 12-7
12.1.7 voice-vlan qos 12-7
12.1.8 voice-vlan qos trust 12-8
12.1.9 voice-vlan security enable 12-9

12章 Voice VLAN

12.1 Voice VLAN設定コマンド

12.1.1 display voice-vlan mac-address

Syntax

display voice-vlan mac-address

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display voice-vlan mac-address コマンドは OUI アドレス、OUI アドレスのマスク、説明を表示します。

例

OUI アドレス、OUI アドレスのマスク、説明を表示します。

<Switch> display voice-vlan mac-address

```
OUI Address    Mask          Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  Aolynk phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

表 12-1 コマンド出力

フィールド	説明
OUI address	装置で許可されるOUIアドレスです。
Mask	OUIアドレスのマスクです。

フィールド	説明
Description	OUIアドレスの説明です。

関連コマンド

voice-vlan mac-address

12.1.2 display voice-vlan state

Syntax

display voice-vlan state

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display voice-vlan state コマンドは voice VLAN の情報を表示します。

例

voice VLAN の情報を表示します。

<Switch> display voice-vlan state

```
Current voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                    VLAN       Mode       CoS        DSCP
 GE1/0/1                  111        Auto       6          46
```

表 12-2 コマンド出力

フィールド	説明
Current Voice VLANs	既存のvoice VLANの番号です。
Voice VLAN security mode	voice VLAN動作モードです。 • Security: 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 aging time	voice VLANエージングタイマです。**No aging**は、voice VLANがエージングアウトしないことを示します。
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。 • Manual: 手動です。 • Auto: 自動です。

関連コマンド

- **voice-vlan aging**
- **voice-vlan enable**
- **voice-vlan mode auto**
- **voice-vlan security enable**

12.1.3 voice-vlan aging

Syntax

voice-vlan aging *minutes*

undo voice-vlan aging

デフォルト

1440 分

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。

voice VLAN エージングタイマを 0 分に設定した場合、voice VLAN はエージングアウトしません。

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 割り当てモードでは、装置は voice VLAN にポートを割り当てるときに、voice VLAN のエージングタイマを開始します。voice VLAN エージングタイマが期限切れになる前に voice パケットがポートで受信されない場合、装置は voice VLAN からポートを削除します。

voice VLAN エージングタイマは、voice VLAN 割り当てモードが自動の場合にのみ設定してください。

例

エージングタイマを 100 分に設定します。

<Switch> system-view

[Switch] voice-vlan aging 100

関連コマンド

display voice-vlan state

12.1.4 voice-vlan enable

Syntax

voice-vlan *vlan-id* **enable**

undo voice-vlan [*vlan-id*] **enable**

デフォルト

無効

View

Layer 2 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、ポートに voice VLAN として VLAN を設定します。

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。

このコマンドを実行する前に、指定した VLAN がすでに存在していることを確認してください。

例

#voice VLAN 機能を有効にし、GigabitEthernet 1/0/1 に VLAN2 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] voice-vlan 2 enable

関連コマンド

- **display voice-vlan state**
- **voice-vlan mode auto**

12.1.5 voice-vlan mac-address

Syntax

voice-vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice-vlan mac-address *oui*

デフォルト

システムのデフォルト OUI アドレスを表 12-3 に示します。

表 12-3 デフォルト OUI アドレス

番号	OUI アドレス	ベンダ
1	0001-E300-0000	Siemens phone
2	0003-6B00-0000	Cisco phone
3	0004-0D00-0000	Avaya phone
4	000F-E200-0000	Aolynk phone
5	0060-B900-0000	Philips/NEC phone
6	00D0-1E00-0000	Pingtel phone
7	00E0-7500-0000	Polycom phone

番号	OUI アドレス	ベンダ
8	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

12.1.6 voice-vlan mode auto

Syntax

voice-vlan mode auto

undo voice-vlan mode auto

デフォルト

自動 voice VLAN 動作モードでポートは動作します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

voice-vlan mode auto コマンドは自動 voice VLAN 動作モードで動作するポートを設定します。

undo voice-vlan mode auto コマンドは手動 voice VLAN 動作モードで動作するポートを設定します。

voice VLAN 機能が有効で手動モードで動作するポートでは、voice VLAN を適用するために手動で voice VLAN にポートを割り当てる必要があります。

例

GigabitEthernet 1/0/1 を手動 voice VLAN 動作モードで動作するように設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo voice-vlan mode auto

関連コマンド

display voice-vlan state

12.1.7 voice-vlan qos

Syntax

voice-vlan qos *cos-value dscp-value*

undo voice-vlan qos

デフォルト

CoS は 6、DSCP は 46 です。

View

Layer 2 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。CoS 値が大きいほど、優先度が高くなります。

dscp-value: DSCP を指定します。設定範囲は 0～63 です。DSCP 値が大きいほど、優先度が高くなります。

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。

voice-vlan qos コマンドと **voice-vlan qos trust** コマンドの両方を設定した場合、最後に行った設定が適用されます。

例

GigabitEthernet 1/0/1 の voice VLAN の CoS を 5、DSCP を 45 に変更します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] voice-vlan qos 5 45

関連コマンド

voice-vlan qos trust

12.1.8 voice-vlan qos trust

Syntax

voice-vlan qos trust

undo voice-vlan qos

デフォルト

CoS は 6、DSCP は 46 です。

View

Layer 2 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。

デフォルトでは、ポートは受信パケットの 802.1p プライオリティを信頼しません。入力 voice VLAN パケットのプライオリティ設定を信頼するようにポートを設定するには、**qos trust dot 1 p** コマンドも使用して、ポートのプライオリティ信頼モードを 802.1p プライオリティに設定する必要があります。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* を参照してください。

voice-vlan qos コマンドと **voice-vlan qos trust** コマンドの両方を設定した場合、最後に行った設定が適用されます。

例

#入力 voice VLAN パケットのプライオリティの設定を信用し、GigabitEthernet 1/0/1 のプライオリティとして設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] voice-vlan qos trust

関連コマンド

voice-vlan qos

12.1.9 voice-vlan security enable

Syntax

voice-vlan security enable

undo voice-vlan security enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

voice-vlan security enable コマンドは voice VLAN のセキュリティモードを有効にします。

undo voice-vlan security enable コマンドは voice VLAN のセキュリティモードを無効にします。

セキュリティモードでは送信元 MAC アドレスが OUI アドレスに一致する音声パケットのみ voice VLAN に転送することができます。

通常モードでは、voice VLAN は音声パケットも非音声パケットも転送します。

例

voice VLAN のセキュリティモードを無効にします。

<Switch> system-view

[Switch] undo voice-vlan security enable

関連コマンド

display voice-vlan state

目次

このセクションのページは **3-x-x** です。

13 章 QinQ.....13-1
13.1 QinQ 設定コマンド.....13-1
13.1.1 display qinq.....13-1
13.1.2 qinq enable.....13-2
13.1.3 qinq ethernet-type (interface view).....13-3
13.1.4 qinq ethernet-type (system view).....13-5
13.1.5 qinq transparent-vlan.....13-6

13章 QinQ

13.1 QinQ設定コマンド

同じレイヤ 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に QinQ および Ethernet サービスインスタンスから VSI へのバインディングを設定しないでください。それ以外の場合、これらの機能は有効にならない可能性があります。

この章では以下の用語を使用します。

- **CVLAN**—カスタマネットワーク VLAN（CVLAN [内部 VLAN]）は、顧客のプライベートネットワーク上で使う VLAN を示します。
- **SVLAN**—サービスプロバイダネットワーク VLAN（SVLAN[外部 VLAN]）は、サービスプロバイダが顧客の VLAN タグ付けされたトラフィックを転送する VLAN を示します。

13.1.1 display qinq

Syntax

display qinq [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、QinQ が有効なすべてのインタフェースを表示します。

説明

display qinq コマンドは QinQ が有効なインタフェースを表示します。

インタフェースで QinQ が無効である場合、出力されません。

例

GigabitEthernet 1/0/1 で QinQ を有効にします。QinQ がインタフェースで有効であるかどうかを確認します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qinq enable

[Switch-GigabitEthernet1/0/1] display qinq interface gigabitethernet 1/0/1

```
Interface
 GigabitEthernet1/0/1
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/3 で QinQ を有効にします。QinQ がインタフェースで有効であるかどうかを確認します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qinq enable

[Switch-GigabitEthernet1/0/1] quit

[Switch] interface gigabitethernet 1/0/3

[Switch-GigabitEthernet1/0/3] qinq enable

[Switch-GigabitEthernet1/0/3] display qinq

```
Interface
 GigabitEthernet1/0/1
 GigabitEthernet1/0/3
```

関連コマンド

qinq enable

13.1.2 qinq enable

Syntax

qinq enable

undo qinq enable

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

qinq enable コマンドはインタフェースで QinQ を有効にします。

undo qinq enable コマンドはインタフェースで QinQ を無効にします。

例

GigabitEthernet 1/0/1 で QinQ を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qinq enable

関連コマンド

display qinq

13.1.3 qinq ethernet-type (interface view)

Syntax

qinq ethernet-type service-tag *hex-value*

undo qinq ethernet-type service-tag

デフォルト

0x8100

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

service-tag: SVLAN タグに TPID 値を設定します。

hex-value: 16 進数の TPID を設定します。設定範囲は 0x0001～0xffff です。表 13-1 に示す予約済み EtherType 値を除きます。

表 13-1 予約済み EtherType 値

プロトコルタイプ	値
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800

プロトコルタイプ	値
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888e
802.1ag	0x8902
LLDP	0x88cc
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

説明

qinq ethernet-type コマンドは SVLAN タグの TPID を設定します。

undo qinq ethernet-type コマンドはデフォルトの SVLAN タグの TPID に戻します。

QinQ が有効になっていないポートは、SVLAN TPID を使用して入力タグ付きフレームを照合します。ポートは、出力フレームの SVLAN タグ内の TPID を設定値として変更します。

例

GigabitEthernet 1/0/1 の SVLAN タグの TPID 値を 9100（16 進数）に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qinq ethernet-type service-tag 9100

関連コマンド

qinq ethernet-type (system view)

13.1.4 qinq ethernet-type (system view)

Syntax

qinq ethernet-type customer-tag *hex-value*

undo qinq ethernet-type customer-tag

デフォルト

0x8100

View

System view

定義済みユーザロール

network-admin

パラメータ

customer-tag： CVLAN タグの TPID 値を設定します。

hex-value: 16 進数の TPID を設定します。設定範囲は 0x0001～0xffff です。表 13-2 に示す予約済み EtherType 値を除きます。

表 13-2 予約済み EtherType 値

プロトコルタイプ	値
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888e

プロトコルタイプ	値
802.1ag	0x8902
LLDP	0x88cc
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

説明

qinq ethernet-type コマンドは CVLAN タグの TPID を設定します。

undo qinq ethernet-type コマンドはデフォルトの CVLAN タグの TPID に戻します。

例

CVLAN タグの TPID 値を 8200（16 進数）に設定します。

<Switch> system-view

[Switch] qinq ethernet-type customer-tag 8200

関連コマンド

qinq ethernet-type (interface view)

13.1.5 qinq transparent-vlan

Syntax

qinq transparent-vlan *vlan-id-list*

undo qinq transparent-vlan { *vlan-id-list* | **all** }

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての VLAN を指定します。

説明

qinq transparent-vlan コマンドはポートの VLAN のリストでトランスペアレントな転送を有効にします。

undo qinq transparent-vlan コマンドはポートの VLAN のリストでトランスペアレントな転送を無効にします。

デフォルトで、QinQ はポートの PVID のすべての入力フレームにタグをつけます。このコマンドは QinQ で VLAN リストからの入力トラフィックにタグをつけることを無効にします。この VLAN はトランスペアレント VLAN と呼ばれます。

このコマンドを繰り返して、VLAN をトランスペアレント VLAN のリストに追加できます。

トランスペアレント VLAN の転送を正常に行うため、以下の設定ガイドラインに従ってください。

- ポートのリンクタイプをトランクあるいはハイブリッドに設定し、PVID とトランスペアレント VLAN にポートを割り当ててください。
- ポートでトランスペアレント VLAN を行うため、他の VLAN を操作するアクションを設定しないでください。
- トラフィックパスのすべてのポートがトランスペアレント VLAN を通過させるため、トランスペアレント VLAN を許可していることを確認してください。
- インタフェースでトランスペアレント VLAN と VLAN マッピングの両方を使用する場合、トランスペアレント VLAN を次の VLAN にすることはできません。
  - one-to-one または one-to-two の VLAN マッピングのオリジナルまたは変換された VLAN です。
  - two-to-two の VLAN マッピングのオリジナルまたは変換された外部 VLAN です。

例

トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 2、VLAN 3、VLAN 50～VLAN 100 に割り当てます。GigabitEthernet 1/0/1 で QinQ を有効にし、VLAN 2 からのフレームをトランスペアレントに転送するようにポートを設定します。

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 2 3 50 to 100
[Switch-GigabitEthernet1/0/1] qinq enable
[Switch-GigabitEthernet1/0/1] qinq transparent-vlan 2
```

目次

このセクションのページは **3-x-x** です。

14 章 VLAN マッピング 14-1
14.1 VLAN マッピング設定コマンド 14-1
14.1.1 display vlan mapping 14-1
14.1.2 vlan mapping 14-2

14章 VLAN マッピング

14.1 VLANマッピング設定コマンド

14.1.1 display vlan mapping

Syntax

display vlan mapping [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの VLAN マッピングを表示します。

説明

display vlan mapping コマンドは VLAN マッピングを表示します。

例

すべてのインタフェースの VLAN マッピングを表示します。

<Switch> display vlan mapping

```
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10           N/A          120                   N/A
  Outer VLAN    Inner VLAN    Nested VLAN
  200          100          300


Interface GigabitEthernet1/0/3:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  12           N/A          110                    12

Interface GigabitEthernet1/0/4:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
```

```
11          30          130                 40
```

表 14-1 コマンド出力

フィールド	説明
Outer VLAN	もとの外部VLANです。 このフィールドは、one-to-oneのVLANマッピングおよびone-to-twoのVLANマッピングの元のVLANを示します。
Inner VLAN	もとの内部VLANです。 このフィールドには、one-to-oneのVLANマッピングおよびone-to-twoのVLANマッピングの**N/A**が表示されます。
Translated Outer VLAN	変換される外部VLANです。 このフィールドは、one-to-oneのVLANマッピング用に変換されたVLANを示します。
Translated Inner VLAN	変換される内部VLANです。 このフィールドには、one-to-oneのVLANマッピングの場合は**N/A**が表示されます。

関連コマンド

vlan mapping

14.1.2 vlan mapping

Syntax

vlan mapping { *vlan-id* **translated-vlan** *vlan-id* | **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id* | **tunnel** *outer-vlan-id inner-vlan-id* **translated-vlan** *outer-vlan-id inner-vlan-id* }

undo vlan mapping { *vlan-id* **translated-vlan** *vlan-id* | **all** | **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id* | **tunnel** *outer-vlan-id inner-vlan-id* **translated-vlan** *outer-vlan-id inner-vlan-id* }

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 **translated-vlan** *vlan-id*: one-to-one VLAN マッピングでもとの VLAN と変換される VLAN を指定します。*vlan-id* の設定範囲は 1～4094 です。もとの VLAN と変換される VLAN は同一にすることができません。

nest range *vlan-range-list* **nested-vlan** *vlan-id*: one-to-two VLAN マッピングでの CVLAN の範囲と SVLAN を指定します。*vlan-range-list* は半角スペースで区切り 10 まで設定します。CVLAN ID を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。異なる CVLAN 範囲は重複することはできません。*vlan-id* は、SVLAN ID の範囲を 1～4094 で指定します。

nest single *vlan-id-list* **nested-vlan** *vlan-id*: one-to-two VLAN マッピングでの CVLAN と SVLAN を指定します。*vlan-range-list* は半角スペースで区切り 10 まで設定します。設定範囲は 1～4094 です。*vlan-id* は SVLAN ID を指定し、設定範囲は 1～4094 です。

tunnel *outer-vlan-id inner-vlan-id* **translated-vlan** *outer-vlan-id inner-vlan-id*: two-to-two VLAN マッピングに対して、元の外部 VLAN ID、元の内部 VLAN ID、変換された外部 VLAN ID、および変換された内部 VLAN ID を指定します。*outer-vlan-id* と *inner-vlan-id* の設定範囲は、両方とも 1～4094 です。

all: インタフェースからのすべての VLAN マッピングの設定を削除します。

説明

vlan mapping コマンドはインタフェースの VLAN マッピングを設定します。

undo vlan mapping コマンドは VLAN マッピングを取り消します。

VLAN マッピングは、インタフェース上で受信された VLAN タグ付きパケットにのみ有効です。

インタフェース上の VLAN マッピング内の元のおよび変換された VLAN は、次の要件を満たす必要があります。

- 異なるタイプの VLAN マッピングエントリに、元の同じ VLAN または変換された VLAN を含めることはできません。
- 異なる one-to-one または two-to-two の VLAN マッピングエントリに、同じ変換済み VLAN を含めることはできません。同じ元の VLAN に複数の one-to-one または two-to-two の VLAN マッピングエントリを設定した場合は、最新の設定が有効になります。

QinQ と VLAN マッピング間の設定上の制限は次のとおりです。

- ポートで QinQ を有効または無効にする前に、そのポートのすべての VLAN マッピングを削除する必要があります。
- QinQ 対応ポートに two-to-two の VLAN マッピングを設定することはできません。

インタフェースでトランスペアレント VLAN と VLAN マッピングの両方を使用する場合、トランスペアレント VLAN を次の VLAN にすることはできません。

- one-to-one および one-to-two の VLAN マッピングのオリジナルまたは変換された VLAN です。
- two-to-two の VLAN マッピングの元のまたは変換された外部 VLAN です。

インタフェースの MTU はデフォルトで 1500 バイトです。パケットに VLAN タグを追加したのち、パケット長は 4 バイト追加されます。one-to-two VLAN マッピングを設定するとき、サービスプロバイダ側ネットワークのインタフェースの MTU を少なくとも 1504 バイトに設定することを推奨します。

VLAN マッピングを適用したインタフェースを経由し、かつ VLAN マッピング対象の VLAN インタフェースを経由する L3 通信は未サポートです。

VLAN マッピング対象の VLAN に VLAN インタフェースを作成および IP アドレスを設定する場合は、L3 通信の経路（送受信インタフェース）には VLAN マッピングを適用しないでください。

例

VLAN 1 に VLAN101 をマッピングするため GigabitEthernet1/0/1 で one-to-one VLAN マッピングを設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101

VLAN タグ 1～VLAN 10、VLAN 80 を送信するパケットに SVLAN タグ 101 を追加するため、GigabitEthernet1/0/4 の one-to-two VLAN マッピングを設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/4

[Switch-GigabitEthernet1/0/4] vlan mapping nest range 1 to 10 nested-vlan 101

[Switch-GigabitEthernet1/0/4] vlan mapping nest single 80 nested-vlan 101

SVLAN 101 に SVLAN201 をマッピングし、CVLAN 1 に CVLAN 10 をマッピングするため、GigabitEthernet1/0/5 の two-to-two VLAN マッピングを設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/5

[Switch-GigabitEthernet1/0/5] vlan mapping tunnel 101 1 translated-vlan 201 10

関連コマンド

display vlan mapping

目次

このセクションのページは **3-x-x** です。

15 章 LLDP 15-1
15.1 LLDP 設定コマンド 15-1
15.1.1 display lldp local-information 15-1
15.1.2 display lldp neighbor-information 15-7
15.1.3 display lldp statistics 15-14
15.1.4 display lldp status 15-16
15.1.5 display lldp tlv-config 15-19
15.1.6 lldp admin-status 15-23
15.1.7 lldp check-change-interval 15-25
15.1.8 lldp compliance admin-status cdp 15-26
15.1.9 lldp compliance cdp 15-27
15.1.10 lldp enable 15-28
15.1.11 lldp encapsulation snap 15-29
15.1.12 lldp fast-count 15-30
15.1.13 lldp global enable 15-30
15.1.14 lldp hold-multiplier 15-31
15.1.15 lldp management-address-format string 15-32
15.1.16 lldp notification remote-change enable 15-33
15.1.17 lldp timer notification-interval 15-34
15.1.18 lldp timer reinit-delay 15-35
15.1.19 lldp timer tx-interval 15-36
15.1.20 lldp tlv-enable 15-36

15章 LLDP

15.1 LLDP設定コマンド

15.1.1 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。

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         : 74ea-c834-8758
 System name        : QX-S5324GT-4X1C
 System description  :
   Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge

 MED information:
 Device class             : Connectivity device
```

```
 MED inventory information of master board:
 HardwareRev             : Ver.B
 FirmwareRev             : 111
 SoftwareRev             : 7.1.4
 SerialNum               : 210235A2BKH177000081
 Manufacturer name        : NEC
 Model name              : QX-S5324GT-4X1C
 Asset tracking identifier  : Unknown

LLDP local-information of port 1[GigabitEthernet1/0/1]:
 Port ID type       : Interface name
 Port ID           : GigabitEthernet1/0/1
 Port description    : GigabitEthernet1/0/1 Interface
 LLDP agent nearest-bridge management address:
 Management address type         : All802
 Management address              : 74ea-c834-8782
 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              : 74ea-c834-8782
 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              : 74ea-c834-8782
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID          : 0
 Port VLAN ID(PVID)  : 4000
 Port and protocol VLAN ID(PPVID)  : 0
 Port and protocol VLAN supported  : Yes
 Port and protocol VLAN enabled    : No
 VLAN name of VLAN 4000     : VLAN 4000
 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 15-1 コマンド出力

フィールド	説明
Chassis ID	装置のBridge MACアドレスです。
System capabilities supported	サポートされる機能です。 • **Bridge**—スイッチングがサポートされます。 • **Router**—ルーティングがサポートされます。 • **Repeater**—信号の繰り返しはサポートされています。 • **Telephone**—ローカル装置は電話として機能できます。 • **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**—信号の繰り返しが有効になっています。 ● **Telephone**—ローカル装置は電話として機能しています。 ● **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。
MED inventory information of master board	IRFスタック装置のマスタのMEDインベントリ情報です。
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。
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。

フィールド	説明
Management address interface type	管理アドレスで識別されるインタフェースの番号タイプです。
Management address interface ID	管理アドレスで識別されるインタフェースのインデックスです。
Management address OID	管理アドレスのオブジェクトIDです。
Port VLAN ID(PVID)	ポートVLAN IDです。
Port and protocol VLAN ID(PPVID)	ポートプロトコルのVLAN IDです。
Port and protocol VLAN supported	プロトコルVLANがポートでサポートされているかどうかを示します。
Port and protocol VLAN enabled	プロトコルVLANがポートで有効になっているかどうかを示します。
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、デュプレックスモードです。
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。

フィールド	説明
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。
PoE PSE power source	PSE電源タイプです。 ● **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電源タイプです。 ● **Unknown**—不明な電力供給です。 ● **PSE**—**PSE**電源です。 ● **Local**—ローカル電源です。 ● **PSE and local**—PSEとローカルの電源です。
Port PSE priority	PSEポートのPoE電源プライオリティです。 ● Unknown. ● Critical. ● High. ● Low.
Port PD priority	PDポートのPoE受電優先順位です。 ● Unknown. ● Critical. ● High. ● Low.
Port available power value	PSEポートで利用可能なPoE電力、またはPDポートで必要な電力（ワット単位）です。
Transmit Tw	ローカルクライアントのスリープ時間（μs）です。
Receive Tw	ローカルクライアントが予期しているピアクライアントのスリープ時間（μs単位）です。
Fallback Tw	ローカルクライアントが予想しているピアクライアントの候補スリープ時間（μs単位）です。
Echo Transmit Tw	ピアクライアントのスリープ時間（μs）です。 次のいずれかの場合に、このフィールドにはゼロが表示されます。 ● ローカルクライアントは、ピアクライアントのスリープ時間を受信していません。 ● ピアクライアントのスリープ時間は0 μsです。

フィールド	説明
Echo Receive Tw	ピアクライアントが予想しているローカルクライアントのスリープ時間（μs単位）です。次のいずれかの場合に、このフィールドにはゼロが表示されます。 • ローカルクライアントは、ピア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。 • ピアクライアントによって期待されるローカルクライアントのスリープ時間は0 μsです。

15.1.2 display lldp neighbor-information

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }] [**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。

agent: エージェントタイプを指定します。指定しない場合、すべての LLDP エージェントが隣接装置から受信する LLDP 情報を表示します。

nearest-bridge: 最も近いブリッジエージェントを指定します。

nearest-customer: 最も近いカスタマブリッジエージェントを指定します。

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。

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 33[FortyGigE1/0/33]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 Update time         : 3 days, 0 hours, 12 minutes, 21 seconds
 Chassis type        : MAC address
 Chassis ID          : 74ea-c834-8758
 Port ID type        : Interface name
 Port ID             : FortyGigE2/0/54
 Time to live        : 121
 Port description    : FortyGigE2/0/54 Interface
 System name         : QX-S5324GT-4X1C
 System description  :
   Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge
```

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 33[FortyGigE1/0/33]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : 74ea-c834-8758/MAC address
 PortID/subtype      : FortyGigE2/0/54/Interface name
 Capabilities        : Bridge, Router, Customer Bridge

LLDP neighbor-information of port 38[FortyGigE1/0/34]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : 74ea-c834-8758/MAC address
 PortID/subtype      : FortyGigE2/0/53/Interface name
 Capabilities        : Bridge, Router, Customer Bridge

LLDP neighbor-information of port 116[FortyGigE2/0/53]:
```

```
LLDP agent nearest-bridge:
 LLDP neighbor index  : 1
 ChassisID/subtype    : 74ea-c834-8758/MAC address
 PortID/subtype       : FortyGigE1/0/34/Interface name
 Capabilities         : Bridge, Router, Customer Bridge

LLDP neighbor-information of port 121[FortyGigE2/0/54]:
LLDP agent nearest-bridge:
 LLDP neighbor index  : 1
 ChassisID/subtype    : 74ea-c834-8758/MAC address
 PortID/subtype       : FortyGigE1/0/33/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
LocalIf        Nbr chassis ID  Nbr port ID                 Nbr system name
FGE1/0/33       74ea-c834-8758  FortyGigE2/0/54             QX-S5324GT-4X1C
FGE1/0/34       74ea-c834-8758  FortyGigE2/0/53             QX-S5324GT-4X1C
FGE2/0/53       74ea-c834-8758  FortyGigE1/0/34             QX-S5324GT-4X1C
FGE2/0/54       74ea-c834-8758  FortyGigE1/0/33             QX-S5324GT-4X1C
```

表 15-2 コマンド出力

フィールド	説明
LLDP neighbor-information of port 1	LLDP情報がポート1から受信されました。
Update time	隣接情報のLLDP情報が最後にアップデートされた時間です。
LLDP mac type	隣接MACアドレスのタイプです。 ● Nearest bridge. ● Nearest customer bridge. ● Nearest non-TPMR bridge.

フィールド	説明
Chassis type	装置IDタイプです。 ● **Chassis component**－装置設定です。 ● **Interface alias**－インタフェースの通称です。 ● **Port component**－ポート設定です。 ● **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。
Nbr 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**－ポート設定です。 ● **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。
Nbr port ID	ポートIDのタイプの値です。
Nbr 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)	ポートおよびプロトコルのVLANIDです。
Port and protocol VLAN supported	プロトコルVLANがポートでサポートされているかどうかを示します。
Port and protocol VLAN enabled	ポートでプロトコルVLANが有効かどうかを示します。
VLAN name of VLAN 12	VLAN12の名前です。
Link aggregation supported	リンクアグリゲーションがサポートされているかどうかを示します。

フィールド	説明
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の場合は0です。
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デュプレックス状態です。
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**－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。
PoE PSE power source	PSE電源タイプです。 ● **Unknown**—不明な電源です。 ● **Primary**—プライマリ電源です。 ● **Backup**—バックアップ電源です。
PoE PD power source	PD電源タイプです。 ● **Unknown**—不明な電源です。 ● **PSE**—PSE電源です。 ● **Local**—ローカル電源です。 ● **PSE and local**—PSEおよびローカル電源です。

フィールド	説明
Port PSE priority	PSEポートのPoE電源プライオリティです。 • Unknown • Critical • High • Low
Port PD priority	PDポートのPoE受電プライオリティです。 • Unknown • Critical • High • Low
Port available power value	PSEポートで使用可能なPoE電力、またはPDポートで必要な電力（ワット単位）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。
LocalIf	LLDPフレームを受信するローカルインタフェースです。
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。

15.1.3 display lldp statistics

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }]]

View

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。

agent: LLDP エージェントタイプを指定します。指定しない場合、すべての LLDP エージェントに対して統計情報を表示します。

nearest-bridge: 最も近いブリッジエージェントを指定します。

nearest-customer: 最も近いカスタマブリッジエージェントを指定します。

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。

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
```

GigabitEthernet 1/0/1 で最も近いカスタマブリッジエージェントの LLDP 統計情報を表示します。

<Switch> display lldp statistics interface GigabitEthernet1/0/1 agent nearest-customer

```
LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-customer:
```

```
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0
```

表 15-3 コマンド出力

フィールド	説明
LLDP statistics global information	グローバルのLLDPの統計情報です。
LLDP neighbor information last change time	隣接情報が最後にアップデートした時間です。
The number of LLDP neighbor information inserted	隣接情報が追加された回数です。
The number of LLDP neighbor information deleted	隣接情報が削除された回数です。
The number of LLDP neighbor information dropped	メモリ空き容量が足りないために隣接情報が廃棄された回数です。

15.1.4 display lldp status

Syntax

display lldp status [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }]

View

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。このオプションを指定しない場合、このコマンドはグローバル LLDP ステータスとすべてのポートの LLDP ステータスを表示します。

agent: LLDP エージェントタイプを指定します。指定しない場合、すべての LLDP エージェントのステータス情報を表示します。

nearest-bridge: 最も近いブリッジエージェントを指定します。

nearest-customer: 最も近いカスタマブリッジエージェントを指定します。

説明

display lldp status コマンドは LLDP の状態を表示します。

例

グローバルの LLDP の状態と各ポートの LLDP の状態を表示します。

<Switch> display lldp status

```
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 5
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval            : 30s
Fast transmit interval        : 1s
Transmit max credit           : 5
Hold multiplier              : 4
Reinit delay                 : 2s
Trap interval                : 5s
Fast start times             : 3

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP          : Enable
Admin status                 : TX_RX
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors      : 5
Number of MED neighbors       : 2
Number of CDP neighbors       : 0
Number of sent optional TLV   : 12
Number of received unknown TLV : 5
```

```
LLDP agent nearest-nontpmr:
Port status of LLDP          : Enable
Admin status                 : TX_RX
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 5
Number of MED neighbors      : 2
Number of CDP neighbors      : 0
Number of sent optional TLV  : 12
Number of received unknown TLV : 5

LLDP agent nearest-customer:
Port status of LLDP          : Enable
Admin status                 : TX_RX
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 5
Number of MED neighbors      : 2
Number of CDP neighbors      : 0
Number of sent optional TLV  : 12
Number of received unknown TLV : 5
```

表 15-4 コマンド出力

フィールド	説明
Bridge mode of LLDP	LLDPブリッジモードです。サービスブリッジあるいはカスタマブリッジがあります。
Global status of LLDP	LLDPがグローバルで有効かどうかを示します。
LLDP neighbor information last changed time	隣接情報が最後にアップデートされた時間です。
Transmit interval	LLDPフレームの転送間隔です。
Hold multiplier	TTL乗数です。
Reinit delay	LLDPを再初期化の遅延時間です。
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。

フィールド	説明
Fast start times	新しい隣接装置が検出された際、連続して送信されるLLDPフレームの回数です。
Port 1	ポート1のLLDPの状態です。
Port status of LLDP	ポートのLLDPが有効かどうかを示します。
Admin status	ポートのLLDP動作モードです。 • **TX_RX**—ポートはLLDPフレームの送受信ができます。 • **Rx_Only**—ポートはLLDPフレームの受信のみができます。 • **Tx_Only**—ポートはLLDPフレームの送信のみができます。 • **Disable**—ポートはLLDPフレームの送受信ができません。
Trap Flag	トラップが有効かどうかを示します。
Polling interval	LLDPのポーリング間隔です。0はLLDPのポーリングが無効であることを示します。
Number of neighbors	ポートに接続しているLLDPの隣接数です。
Number of MED neighbors	ポートに接続しているMEDの隣接数です。
Number of CDP neighbors	ポートに接続しているCDPの隣接数です。
Number of sent optional TLV	LLDPフレームに含まれるオプションTLVがポートに送信された数です。
Number of received unknown TLV	受信されたLLDPフレームに含まれる不明なTLVの数です。

15.1.5 display lldp tlv-config

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }]

View

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、すべてのポートの通知可能なオプションの TLV のタイプを表示します。

agent: LLDP エージェントタイプを指定します。指定しない場合、すべての LLDP エージェントの通知可能なオプションの LLDP TLV のタイプを表示します。

nearest-bridge: 最も近いブリッジエージェントを指定します。

nearest-customer: 最も近いカスタマブリッジエージェントを指定します。

説明

display lldp tlv-config コマンドはポートで通知可能なオプション LLDP TLV のタイプを表示します。

例

GigabitEthernet 1/0/1 で通知可能なオプションの LLDP TLV のタイプを表示します。

<Switch> display lldp tlv-config interface gigabitethernet 1/0/1

```
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
NAME                          STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV           YES       YES
 System Name TLV               YES       YES
 System Description TLV         YES       YES
 System Capabilities TLV        YES       YES
 Management Address TLV         YES       YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV              YES       YES
 Port And Protocol VLAN ID TLV    NO        NO
 VLAN Name TLV                 NO        NO
 DCBX TLV                      NO        NO
 EVB TLV                       NO        NO
 Link Aggregation TLV           YES       YES
 Management VID TLV            NO        NO
 Congestion notification TLV     NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                YES       YES
 Power via MDI TLV             YES       YES
 Maximum Frame Size TLV         YES       YES
LLDP-MED extend TLV:
 Capabilities TLV              YES       YES
 Network Policy TLV            YES       YES
 Location Identification TLV     NO        NO
```

```
 Extended Power via MDI TLV      YES      YES
 Inventory TLV                  YES      YES

LLDP agent nearest-nontpmr:
NAME                           STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV           NO       NO
 System Name TLV               NO       NO
 System Description TLV         NO       NO
 System Capabilities TLV        NO       NO
 Management Address TLV         NO       NO
IEEE 802.1 extend TLV:
 Port VLAN ID TLV              NO       NO
 Port And Protocol VLAN ID TLV   NO       NO
 VLAN Name TLV                 NO       NO
 DCBX TLV                      NO       NO
 EVB TLV                       YES      YES
 Link Aggregation TLV           NO       NO
 Management VID TLV            NO       NO
 Congestion notification TLV     NO       NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                NO       NO
 Power via MDI TLV             NO       NO
 Maximum Frame Size TLV         NO       NO
LLDP-MED extend TLV:
 Capabilities TLV              NO       NO
 Network Policy TLV            NO       NO
 Location Identification TLV     NO       NO
 Extended Power via MDI TLV      NO       NO
 Inventory TLV                 NO       NO

LLDP agent nearest-customer:
NAME                           STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV           YES      YES
 System Name TLV               YES      YES
 System Description TLV         YES      YES
 System Capabilities TLV        YES      YES
 Management Address TLV         YES      YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV              YES      YES
 Port And Protocol VLAN ID TLV   NO       NO
 VLAN Name TLV                 NO       NO
```

```
 DCBX TLV                      NO       NO
 EVB TLV                       NO       NO
 Link Aggregation TLV           YES      YES
 Management VID TLV            NO       NO
 Congestion notification TLV     NO       NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                NO       NO
 Power via MDI TLV             NO       NO
 Maximum Frame Size TLV         NO       NO
LLDP-MED extend TLV:
 Capabilities TLV              NO       NO
 Network Policy TLV            NO       NO
 Location Identification TLV     NO       NO
 Extended Power via MDI TLV      NO       NO
 Inventory TLV                 NO       NO
```

表 15-5 コマンド出力

フィールド	説明
LLDP tlv-config of port 1	ポート1の通知可能なオプションTLVです。
NAME	TLVのタイプです。
STATUS	TLVのタイプがポートに送信されたかどうかを示します。
DEFAULT	デフォルトでTLVのタイプがポートに送信されたかどうかを示します。
Basic optional TLV	basic TLVのオプションTLVです。 ● **Port Description TL**Vーポート説明TLVです。 ● **System Name TLV**ーシステム名TLVです。 ● **System Description TLV**ーシステム説明TLVです。 ● **System Capabilities TLV**ーシステム機能TLVです。 ● **Management Address TLV**ー管理アドレスTLVです。 ● **Congestion notification TLV**ー輻輳通知TLVです。輻輳通知TLVはサポートしていません。

フィールド	説明
IEEE 802.1 extended TLV	IEEE802.1組織指定TLVです。 ● **Port VLAN ID TLV**－ポートVLAN ID TLVです。 ● **Port and protocol VLAN ID TLV**－ポートのプロトコルVLAN TLVです。 ● **VLAN name TLV**－VLAN名TLVです。 ● **DCBX TLV**－DCBX TLVです。DCBX TLVはサポートしていません。 ● **EVB TLV**－EVB TLVです。EVB TLVはサポートしていません。 ● **Management VID TLV**－管理VID TLVです。
IEEE 802.3 extended TLV	IEEE802.3組織指定TLVです。 ● **MAC-Physic TLV**－MAC物理TLVです。 ● **Power via MDI TLV**－MDI経由の電力TLVです。 ● **Link aggregation TLV**－リンクアグリゲーションTLVです。 ● **Maximum frame size TLV**－最大フレームサイズTLVです。
LLDP-MED extend TLV	LLDP-MED TLVです。 ● **Capabilities TLV**－機能TLVです。 ● **Network Policy TLV**－ネットワークポリシーTLVです。 ● **Extended Power-via-MDI TLV**－拡張MDI経由TLVです。 ● **Location Identification TLV**－位置識別TLVです。 ● **Inventory TLV**－インベントリTLVです。
Inventory TLV	インベントリTLVです。 ● **Hardware Revision TLV**－ハードウェアレビジョンTLVです。 ● **Firmware Revision TLV**－ファームウェアレビジョンTLVです。 ● **Software Revision TLV**－ソフトウェアレビジョン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。

15.1.6 lldp admin-status

Syntax

Layer 2 Ethernet interface view または management 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

IRF physical interface view :

lldp admin-status { **disable** | **rx** | **tx** | **txrx** }
undo lldp 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** モードです。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの動作モードを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

disable: Disable モードを指定します。**Disable** モードのポートは LLDP フレームの送受信ができません。

rx: Rx モードを指定します。**Rx** モードのポートは LLDP フレームの受信のみができます。

ポートは LLDP フレームの送受信ができます。

tx: Tx モードを指定します。**Tx** モードのポートは LLDP フレームの送信のみができます。

ポートは LLDP フレームの送受信ができます。

txrx: TxRx モードを指定します。**TxRx** モードのポートは LLDP フレームの送受信ができます。

説明

lldp admin-status コマンドは LLDP の動作モードを指定します。

undo lldp admin-status コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP 動作モードを **Rx** に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx

15.1.7 lldp check-change-interval

Syntax

Layer 2 Ethernet interface view または management 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

IRF physical interface view：

lldp check-change-interval *interval*
undo lldp check-change-interval

デフォルト

無効

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical 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 LLDP ポーリングを無効にします。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP ポーリングを有効にし、ポーリング間隔を 30 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30

15.1.8 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

Management Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

disable: Disable モードを指定します。Disable モードは CDP パケットの送受信を行うことができません。

txrx: **TxRx** モードを指定します。**TxRx** モードは CDP パケットの送受信を行うことができます。

説明

lldp compliance admin-status cdp コマンドは CDP 互換 LLDP モードの動作モードを設定します。

undo lldp compliance admin-status cdp コマンドはデフォルトに戻します。

Cisco の IP 電話を動作させるため以下の作業を行ってください。

- グローバルで CDP 互換 LLDP を有効にします。
- 指定したポートを TxRx モードで動作するように CDP 互換 LLDP を設定します。

例

グローバルで CDP 互換 LLDP を有効にし、GigabitEthernet 1/0/1 を **TxRx** モードで動作するように CDP 互換 LLDP を設定します。

<Switch> system-view

[Switch] lldp compliance cdp

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx

関連コマンド

lldp compliance cdp

15.1.9 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 CDP 互換モードを無効にします。

CDP で許可される最大 TTL は 255 秒です。Cisco の IP 電話と一緒に運用するため、CDP 互換 LLDP の送信間隔の設定は TTL 値の 1/3 以内にする必要があります。

例

CDP 互換モードを有効にします。

<Switch> system-view

[Switch] lldp compliance cdp

関連コマンド

- **lldp hold-multiplier**
- **lldp timer tx-interval**

15.1.10 lldp enable

Syntax

lldp enable

undo lldp enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

定義済みユーザロール

network-admin

説明

lldp enable コマンドはポートで LLDP を有効にします。

undo lldp enable コマンドはポートで LLDP を無効にします。

LLDP はグローバルとポートの両方で有効にしたときのみ適用されます。

例

GigabitEthernet 1/0/1 で LLDP を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo lldp enable

関連コマンド

lldp global enable

15.1.11 lldp encapsulation snap

Syntax

Layer 2 Ethernet interface view または management 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

IRF physical interface view :

lldp encapsulation snap
undo lldp encapsulation

デフォルト

Ethernet II

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの LLDP フレームのカプセル化フォーマットを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

説明

lldp encapsulation snap コマンドは LLDP フレームのカプセル化フォーマットを SNAP に設定します。

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

LLDP-CDP パケットは SNAP のカプセル化フォーマットのみ使用します。

例

GigabitEthernet 1/0/1 の LLDP フレームのカプセル化フォーマットを SNAP に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp encapsulation snap

15.1.12 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

15.1.13 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

15.1.14 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

15.1.15 lldp management-address-format string

Syntax

Layer 2 Ethernet interface view または management 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

Management 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。

装置は、IPv6 管理アドレスの数値カプセル化フォーマットのみをサポートします。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントで管理アドレスの TLV のカプセル化フォーマットを string 形式に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format string

15.1.16 lldp notification remote-change enable

Syntax

Layer 2 Ethernet interface view/management 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

IRF physical interface view :

lldp notification remote-change enable
undo lldp notification remote-change enable

デフォルト

無効

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの LLDP トラップを有効にします。

nearest-customer: nearest customer bridge エージェントを指定します。

説明

lldp notification remote-change enable コマンドは LLDP トラップを有効にします。

undo lldp notification remote-change enable コマンドは LLDP トラップを無効にします。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP トラップを有効にします。

<Switch> system-view

[Switch] interface GigabitEthernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change enable

15.1.17 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

15.1.18 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

15.1.19 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 1～32768 秒です。

説明

lldp timer tx-interval コマンドは LLDP フレームの送信間隔を設定します。

undo lldp timer tx-interval コマンドはデフォルトに戻します。

例

LLDP フレームの送信間隔を 20 秒に設定します。

<Switch> system-view

[Switch] lldp timer tx-interval 20

15.1.20 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*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] |

power-over-ethernet | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<*1-10*> | **elin-address** *tel-number* } } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [**vlan-id**] | **power-over-ethernet** | **location-id** } }

- nearest customer bridge エージェント

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

In management Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<*1-10*> | **elin-address** *tel-number* } } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

Layer 2 aggregate interface view :

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

IRF physical interface view :

lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }
undo lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }

デフォルト

レイヤ 2 Ethernet インタフェースのデフォルトを以下に示します。

- nearest bridge エージェントは以下のタイプの LLDP TLV を除いたすべての LLDP TLV を送信します。
  - 位置識別 TLV
  - ポートのプロトコル VLAN ID TLV
  - VLAN 名 TLV
  - 管理 VLAN ID TLV
- nearest customer bridge エージェントは basic TLV と IEEE802.1 組織指定 TLV を送信します。

マネジメント 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、ネットワークポリシーTLV を除いたすべての LLDP TLV（IEEE802.1 組織指定の TLV 中のリンクアグリゲーション TLV のみ）を送信します。
- nearest customer bridge エージェントは basic TLV と IEEE802.1 組織指定 TLV（リンクアグリゲーション TLV のみ）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。

IRF スタック物理インタフェースは、使用可能なすべてのタイプの TLV をサポートします。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical 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。インタフェースは次の TLV を送信できます。

- **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*]: 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。

- **lldp tlv-enable** コマンドを実行すると、次のようになります。
  - レイヤ 2 Ethernet インタフェースまたはアグリゲートインタフェースでは、次のいずれかの条件が存在する場合、VLAN インタフェースの IPv4 アドレスが管理アドレスとして送信されます。
    - アップ状態です。
    - 対応する VLAN ID は、インタフェースで許可されている VLAN の中で最も小さいものです。

    許可された VLAN の VLAN インタフェースのいずれにも IPv4 アドレスが割り当てられていないか、すべての VLAN インタフェースがダウンしている場合、ポートの MAC アドレスが送信されます。
- **undo lldp tlv-enable** コマンドを実行したとき、レイヤ 2 Ethernet インタフェース、管理 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は次のようになります。
  - *ip-address* を指定しない場合、ポートは管理アドレス TLV を送信しません。
  - *ip-address* を指定すると、ポートはデフォルト管理アドレス TLV を送信します。

port-description: ポート説明 TLV を送信します。

system-capability: システム機能 TLV を送信します。

system-description: システム説明 TLV を送信します。

system-name: システム名 TLV を送信します。

dot1-tlv: IEEE 802.1 組織指定 LLDP TLV を送信します。

port-vlan-id: ポート VLAN ID TLV を送信します。

protocol-vlan-id [*vlan-id*]: ポートのプロトコル VLAN ID TLV を送信します。*vlan-id* は送信される TLV の VLAN ID を指定します。VLAN ID の設定範囲は 1～4094 です。デフォルトはポートでもっとも小さい VLAN ID です。

vlan-name [*vlan-id*]: VLAN 名 TLV を送信します。*vlan-id* は送信される TLV の VLAN ID を指定します。VLAN ID の設定範囲は 1～4094 です。デフォルトはポートでもっとも小さい VLAN ID です。VLAN ID を指定せず、ポートがどの VLAN にも割り当てられていない場合、ポートの PVID が送信されます。

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。

link-aggregation: リンクアグリゲーション TLV を送信します。

dot3-tlv: IEEE802.3 組織指定 LLDP 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 はネットワーク装置を指定します。
- 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: ネットワークポリシーTLV を送信します。

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 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-MED TLV が送信されない場合、通知可能であるにも関わらず、他の LLDP-MED TLV が送信されません。

IEEE802.1 組織指定 LLDP TLV のプロトコル VLAN ID、VLAN 名 TLV、管理 VLAN ID TLV は nearest bridge エージェントでのみ設定できます。

例

GigabitEthernet 1/0/1 の IEEE802.1 組織指定 TLV のリンクアグリゲーション TLV を送信するため、GigabitEthernet 1/0/1 の nearest customer bridge エージェントを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv link-aggregation

目次

このセクションのページは **3-x-x** です。

16 章 L2PT.....16-1
16.1 L2PT 設定コマンド.....16-1
16.1.1 display l2protocol statistics.....16-1
16.1.2 l2protocol tunnel dot1q.....16-3
16.1.3 l2protocol tunnel-dmac.....16-5
16.1.4 reset l2protocol statistics.....16-5

16章 L2PT

16.1 L2PT設定コマンド

16.1.1 display l2protocol statistics

Syntax

display l2protocol statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: レイヤ 2 Ethernet またはアグリゲートインタフェースをそのタイプと番号で指定します。このオプションを指定しない場合、このコマンドはすべてのレイヤ 2 Ethernet およびアグリゲートインタフェースの L2PT 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

すべてのレイヤ 2 Ethernet およびアグリゲートインタフェースの L2PT 統計情報を表示します。

<Switch> display l2protocol statistics

```
L2PT statistics information on interface Bridge-Aggregation1:
Protocol  Encapsulated     Decapsulated     Forwarded        Dropped
CDP       0                0                0                0
DLDP      0                3                0                0
EOAM      0                2                0                0
GVRP      8                4                9                2
LACP      0                0                0                0
LLDP      0                3                0                0
MVRP      0                0                0                0
PAGP      0                1                0                0
```

```
PVST      0               0               0               0
STP       5               5               5               0
Tunnel    N/A             N/A             100             10
VTP       0               6               0               0
UDLD      0               0               0               0

L2PT statistics information on interface GigabitEthernet1/0/1:
Protocol  Encapsulated    Decapsulated    Forwarded       Dropped
CDP       0               0               0               0
DLDP      2               3               3               0
EOAM      5               2               9               0
GVRP      8               4               9               2
LACP      0               0               0               0
LLDP      3               3               3               3
MVRP      0               0               0               0
PAGP      5               1               7               3
PVST      0               0               0               0
STP       5               5               5               0
Tunnel    N/A             N/A             100             10
VTP       0               6               0               0
UDLD      0               0               0               0
```

表 16-1 コマンド出力

フィールド	説明
Encapsulated	カプセル化したパケット数です。 インタフェースがカスタマネットワークからプロトコルパケットを受信し、カプセル化したとき、1つずつ数が増えます。 **Tunnel**プロトコルの場合、**N/A**と表示されます。**Tunnel**プロトコルはトンネルパケットを示します。
Decapsulated	復号化したパケット数です。 インタフェースがサービスプロバイダネットワークからプロトコルパケットを受信し、トンネルパケットを復号化したとき、1つずつ数が増えます。 **Tunnel**プロトコルの場合、**N/A**と表示されます。**Tunnel**プロトコルはトンネルパケットを示します。
Forwarded	転送されたパケット数です。 インタフェースがプロトコルパケットを受信し、転送したとき、1つずつ数が増えます。 **Tunnel**プロトコルの場合、インタフェースがプロトコルパケットを受信し、転送したとき、1つずつ数が増えます。PEのインタフェースがカスタマネットワークに接続されていない場合、値は増加しません。

フィールド	説明
Dropped	廃棄されたパケット数です。 インタフェースがプロトコルパケットを受信し、廃棄したとき、1つずつ数が増えます。ハードウェアによって廃棄されたプロトコルパケットはカウントされません。 Tunnelプロトコルの場合、インタフェースがプロトコルパケットを受信し、廃棄したとき、1つずつ数が増えます。

16.1.2 l2protocol tunnel dot1q

Syntax

Layer 2 Ethernet interface view:

l2protocol { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

undo l2protocol { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

Layer 2 aggregate interface view:

🕮 **メモ:**

cdp , **lacp** , **lldp** , **pagp** , **udld** オプションはVersion 7.2.23以降のソフトウェアからサポートされています。
Version 7.3.21 は上記オプションをサポートしていません。

l2protocol { **cdp** | **lacp** | **lldp** | **gvrp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

undo l2protocol { **cdp** | **lacp** | **lldp** | **gvrp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

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 コマンドはプロトコルの L2PT を無効にします。

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。
- 次の条件に当てはまる場合は、CE のアグリゲートインタフェースに接続している PE ポートでプロトコル（STP など）を無効にします。
  - プロトコルは CE のアグリゲートインタフェースで動作しています。
  - CE のアグリゲートインタフェースは、PE の L2PT 対応ポートに接続します。

レイヤ 2 アグリゲーショングループのメンバポートで L2PT を有効にできますが、設定は有効になりません。

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。Bridge-Aggregation 1 で STP の L2PT を有効にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] undo stp enable

[Switch-Bridge-Aggregation1] l2protocol stp tunnel dot1q

16.1.3 l2protocol tunnel-dmac

Syntax

l2protocol tunnel-dmac *mac-address*

undo l2protocol tunnel-dmac

デフォルト

010f-e200-0003

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address: 宛先マルチキャスト MAC アドレスを指定します。有効なアドレスは 0100-0ccd-cdd0、0100-0ccd-cdd1、0100-0ccd-cdd2、010f-e200-0003 です。

説明

l2protocol tunnel-dmac コマンドはトンネルパケットの宛先マルチキャスト MAC アドレスを設定します。

undo l2protocol tunnel-dmac コマンドはデフォルトに戻します。

例

トンネルパケットの宛先マルチキャスト MAC アドレスを 0100-0ccd-cdd0 に設定します。

<Switch> system-view

[Switch] l2protocol tunnel-dmac 0100-0ccd-cdd0

16.1.4 reset l2protocol statistics

Syntax

reset l2protocol statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 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を指定します。指定しない場合、すべてのレイヤ 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の L2PT の統計情報を削除します。

<Switch> reset l2protocol statistics

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

4. IP サービス

本マニュアルは以下に示す章で構成されています。

01-ARP

02-Gratuitous ARP

03-Proxy ARP

04-ARP スヌーピング

05-IP アドレス

06-DHCP

07-DNS

08-IP フォワーディングの基本

09-IP パフォーマンスの最適化

10-UDP ヘルパー

11-IPv6 の基本

12-HTTP リダイレクト

目次

このセクションのページは **4-x-x** です。

1 章 ARP.....1-1
1.1 ARP 設定コマンド.....1-1
1.1.1 arp check enable.....1-1
1.1.2 arp check log enable.....1-2
1.1.3 arp mac-interface-consistency check enable.....1-3
1.1.4 arp max-learning-num.....1-4
1.1.5 arp max-learning-number.....1-5
1.1.6 arp multiport.....1-6
1.1.7 arp static.....1-7
1.1.8 arp timer aging.....1-8
1.1.9 display arp.....1-9
1.1.10 display arp ip-address.....1-13
1.1.11 display arp timer aging.....1-14
1.1.12 reset arp.....1-14

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。

この機能は、ARP が IP アドレスを正しく解決できない場合に、装置が ARP イベントを記録できるようにします。ログ情報は、管理者が問題を見つけて解決するのに役立ちます。装置は次の ARP イベントを記録できます。

- 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、次の IP アドレスのいずれでもありません。
  - 受信側インタフェースの IP アドレス
  - VRRP グループの仮想 IP アドレス
- 受信した ARP エントリの送信元 IP アドレスが、次のいずれかの IP アドレスと重複しています。
  - 受信側インタフェースの IP アドレス
  - VRRP グループの仮想 IP アドレス

装置は ARP ログメッセージをインフォメーションセンタに送信します。**info-center source** コマンドを使用すると、情報センタのログ出力ルールを指定できます。インフォメーションセンタの詳細は、オペレーションマニュアルのセクション 10 *システム管理* を参照してください。

装置は、大量の ARP ログを生成する可能性があります。システムリソースを節約するには、ARP イベントを監査またはトラブルシューティングするときにだけ ARP ログを有効にします。

例

ARP ロギングを有効にします。

<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 ARP および MAC アドレスエントリのインタフェースの整合性チェックを有効にします。

undo arp mac-interface-consistency check enable コマンドはこの機能を無効にします。

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インタフェースが変更される場合があります。MAC アドレスエントリのインタフェースはすぐに更新されますが、ARP エントリのインタフェースは更新されません。この場合、ARP エントリに一致するパケットは、間違った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、ユーザの ARP および MAC アドレスエントリのインタフェースの整合性を定期的に確認します。インタフェースが同じでない場合、ARP は ARP エントリの VLAN で ARP 要求を送信し、ARP 応答受信インタフェースでエントリを更新します。

display mac-address コマンドは、MAC アドレスエントリを表示します。

例

ARP および MAC アドレスエントリのインタフェースの整合性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 (コマンドマニュアルのセクション 3 *アクセス*)

1.1.4 arp max-learning-num

Syntax

arp max-learning-num *max-number*

undo arp max-learning-num

デフォルト

1024

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

max-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 1～1024 です。

説明

arp max-learning-num コマンドはインタフェースのダイナミック ARP ラーニング制限を設定します。

undo arp max-learning-num コマンドはデフォルトに戻します。

インタフェースは ARP エントリをダイナミックに学習できます。多くの ARP エントリを保持することを防ぐため、インタフェースが学習できるダイナミック ARP エントリの最大数を設定することができます。設定した最大数に到達すると、インタフェースは ARP エントリの学習を停止します。

0 に設定した場合、ダイナミック ARP エントリの学習を無効にします。

例

VLAN インタフェース 40 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 40

[Switch-Vlan-interface40] arp max-learning-num 10

#GigabitEthernet 1/0/1 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] arp max-learning-num 10

bridge-aggregation 1 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] arp max-learning-num 10

1.1.5 arp max-learning-number

Syntax

arp max-learning-number *max-number* **slot** *slot-number*

undo arp max-learning-number slot *slot-number*

デフォルト

1024

View

System view

定義済みユーザロール

network-admin

パラメータ

max-number: 装置のダイナミック ARP エントリの最大数を指定します。設定範囲は 1～1024 です。

slot *slot-number:* メンバ ID によって IRF スタックメンバ装置を指定します。

説明

arp max-learning-number コマンドは装置のダイナミック ARP 学習制限を設定します。

undo arp max-learning-number コマンドはデフォルトに戻します。

装置は ARP エントリを動的に学習できます。装置が多くの ARP エントリを保持しすぎるのを防ぐために、装置が学習できるダイナミック ARP エントリの最大数を設定できます。最大数に達すると、装置は ARP エントリの学習を停止します。

number を 0 に設定すると、装置はダイナミック ARP エントリの学習を無効になります。

例

スロット 1 のダイナミック ARP 学習制限を 64 に設定します。

<Switch> system-view

[Switch] arp max-learning-number 64 slot 1

1.1.6 arp multiport

Syntax

arp multiport *ip-address mac-address vlan-id*

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: マルチポート ARP エントリの IP アドレスを指定します。

mac-address:マルチポート ARP エントリの MAC アドレスを指定します。形式は H-H-H です。

vlan-id: マルチポート ARP エントリの VLAN を指定します。設定範囲は 1～4094 です。指定した VLAN がすでに存在している必要があります。

説明

arp multiport コマンドはマルチポート ARP エントリを設定します。

undo arp コマンドは ARP エントリを無効にします。

VLAN あるいは対応する VLAN インタフェースが削除された場合、マルチポート ARP エントリも削除されます。

マルチポート ARP エントリをパケット転送に対して有効にするには、マルチキャストまたはマルチポートユニキャストのエントリアドレスを設定して、複数の出力インタフェースを指定する必要があります。MAC アドレスエントリは、マルチポート ARP エントリと同じ MAC アドレスおよび VLAN ID を持つ必要があります。また、マルチポート ARP エントリ内の IP アドレスは、指定された VLAN の VLAN インタフェースと同じサブネット上に存在する必要があります。

例

VLAN10 の IP アドレス 202.38.10.2 および MAC アドレス f474-8801-0000 を含むマルチポート ARP エントリを設定します。

<Switch> system-view

[Switch] arp multiport 202.38.10.2 f474-8801-0000 10

関連コマンド

- **display arp multiport**
- **reset arp multiport**

1.1.7 arp static

Syntax

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

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。

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、ショートとロングがあります。

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未解決になります。

ロングスタティック ARP エントリは、有効または無効です。効果的でないロングスタティック ARP エントリは、パケット転送には使用できません。ロングスタティック ARP エントリは、次のいずれかの状況では無効です。

- 対応する VLAN インタフェースまたは出力インタフェースがダウンしています。
- エントリの IP アドレスがローカル IP アドレスと競合しています。
- ARP エントリの IP アドレスと同じサブネット内に IP アドレスを持つローカルインタフェースはありません。

vlan-id interface-type interface-number を指定する場合は、次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 インタフェースでもアグリゲートインタフェースでもよい。
- VLAN および VLAN インタフェースがすでに存在している必要があります。指定した Ethernet インタフェースは、指定した 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* で指定した IP アドレスは、同じネットワーク上にある必要があります。
- VLAN または VLAN インタフェースが削除されると、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 に対応するロングスタティック ARP エントリを設定します。

<Switch> system-view

[Switch] arp static 202.38.10.2 f474-8801-0000 10 gigabitethernet 1/0/1

関連コマンド

- **display arp**
- **reset arp**

1.1.8 arp timer aging

Syntax

arp timer aging *aging-minutes*

undo arp timer aging

デフォルト

20 分

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-minutes:エージングするタイマを分単位で指定します。設定範囲は 1～1440 です。

説明

arp timer aging コマンドはダイナミック ARP エントリのエージングタイマを設定します。

undo arp timer aging コマンドはデフォルトに戻します。

ARP テーブル上の各ダイナミック ARP エントリは有効期限を持っています。有効期限はエージングタイマと呼ばれ、有効期限内にダイナミック ARP エントリがアップデートされるたびに、エージングタイマはリセットされます。有効期限切れになる前に更新されなかったダイナミック ARP エントリは、ARP テーブルから削除されます。

必要に応じてダイナミック ARP エントリのエージングタイマを設定してください。たとえば proxy ARP を設定するとき、不正なダイナミック ARP エントリが時間内に削除されるようにエージングタイマを短い値に設定してください。

例

ダイナミック ARP エントリのエージングタイマを 10 分に設定します。

<Switch> system-view

[Switch] arp timer aging 10

関連コマンド

display arp timer aging

1.1.9 display arp

Syntax

display arp [[**all** | **dynamic** | **multiport** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての ARP エントリを表示します。

dynamic: ダイナミック ARP エントリを表示します。

multiport: マルチポート ARP エントリを表示します。

static: スタティック ARP エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置の ARP エントリを表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。

vlan *vlan-id*: 指定した VLAN の ARP エントリを表示します。設定範囲は 1～4094 です。

interface *interface-type interface-number*: *interface-type interface-number* で指定されたインタフェースの ARP エントリを表示します。

count: ARP エントリ数を表示します。

verbose: ARP エントリの詳細情報を表示します。

説明

display arp コマンドは ARP エントリを表示します。

このコマンドは IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプ、エージングタイマを含む ARP エントリの情報を表示します。

例

すべての ARP エントリを表示します。

<Switch> display arp all

```
 Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address      MAC Address    VID    Interface/Link ID     Aging Type
1.1.1.1         02e0-f102-0023 1      GE1/0/1              N/A   S
1.1.1.2         f474-8800-0001 12     GE1/0/2               960   D
```

すべての ARP エントリの詳細情報を表示します。

<Switch> display arp all verbose

```
IP address         : 1.1.1.1           MAC address    : 02e0-f102-0023
Type              : Static            Aging         : --
Interface          : GE1/0/1           VLAN          : 1
VPN instance       : --
Link ID           : --
VXLAN ID          : --
VSI name          : --
VSI interface      : --
Nickname          : 0x0000

IP address         : 1.1.1.2           MAC address    : 0015-e944-adc5
Type              : Static           Aging         : 960 sec
```

```
Interface          : GE1/0/2           VLAN          : 12
VPN instance       : --
Link ID            : --
VXLAN ID           : --
VSI name           : --
VSI interface      : --
Nickname           : 0x0000
```

すべての ARP エントリの数を表示します。

<Switch> display arp all count

```
Total number of entries : 4
```

表 1-1 コマンド出力

フィールド	説明
IP address	ARPエントリのIPアドレスです。
MAC address	ARPエントリのMACアドレスです。
VID	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ARPエントリが所属するVLAN IDです。このフィールドには、次のいずれかの状況で**N/A**が表示されます。 ● 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。このフィールドには、次のいずれかの状況で**N/A**が表示されます。 ● 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エントリがマルチポートARPエントリで、出力インタフェースの情報がありません。 マルチポートARPエントリの出力インタフェースの情報を取得する場合、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てください。
Link ID	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ARPエントリのリンクIDです。ARPエントリがどのVSIにも属していない場合、このフィールドにはハイフン(**--**)が表示されます。

フィールド	説明
Aging	ダイナミックARPエントリのエージングタイマです。単位は秒です。 スタティックARPのエントリアドレスの場合、このフィールドには常に**N/A**が表示されます。手動で削除しない限り、スタティックARPエントリはエージングアウトしません。 ダイナミックARPエントリの場合、エージングタイムが不明な場合、このフィールドには**N/A**が表示されます。
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 ARPエントリです。OpenFlowはQX-S5300Gシリーズではサポートしていません。 • **R**—ルールARPエントリです。 • **M**—マルチポートARPエントリです。 • **I**—無効なARPエントリです。
Vpn Instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 VPNインスタンスの名前です。ARPエントリにVPNインスタンスが設定されていない場合、このフィールドには**[No Vrf]**が表示されます。
VXLAN ID	ARPエントリが属するVXLANのIDです。VXLAN IDはVNIとも呼ばれます。ARPエントリがどのVXLANにも属していない場合、このフィールドには**N/A**が表示されます。VXLANはQX-S5300Gシリーズではサポートしていません。
VSI name	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ARPエントリが属するVSIの名前です。ARPエントリがどのVSIにも属していない場合、このフィールドには**N/A**が表示されます。
VSI interface	このフィールドは、QX-S5300Gシリーズではサポートしていません。 VSIのゲートウェイインタフェースの名前です。VSIのゲートウェイインタフェースが指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。
Nickname	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ARPエントリのニックネームです。ニックネームは、4つの16進数の文字列(012aなど)です。
Total number of entries	ARPエントリ数です。

関連コマンド

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

1.1.10 display arp ip-address

Syntax

display arp *ip-address* [**slot** *slot-number*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: 指定した IP アドレスの ARP エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置の ARP エントリを表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の情報を表示します。

verbose: ARP エントリの詳細情報を表示します。

説明

display arp ip-address コマンドは IP アドレスの ARP エントリを表示します。

ARP エントリの情報は IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプ、エージングタイマを含みます。

例

IP アドレス 20.1.1.1 の ARP エントリを表示します。

<Switch> display arp 20.1.1.1

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address      MAC Address    VID    Interface/Link ID     Aging Type
20.1.1.1        f474-8800-0001 N/A    N/A                N/A   S
```

関連コマンド

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

1.1.11 display arp timer aging

Syntax

display arp timer aging

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display arp timer aging コマンドはダイナミック ARP エントリのエージングタイマを表示します。

このコマンドは、**arp timer aging** コマンドで設定した単位に関係なく、常にエージングタイムを秒単位で表示します。

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 1200 seconds
```

関連コマンド

arp timer aging

1.1.12 reset arp

Syntax

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **multiport** | **slot** *slot-number* | **static** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての ARP エントリを削除します。

dynamic: すべてのダイナミック ARP エントリを削除します。

multiport: マルチポート ARP エントリを削除します。

static: すべてのスタティック ARP エントリを削除します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の ARP エントリを削除します。

interface *interface-type interface-number*: インタフェースをタイプと番号で指定します。インタフェースを指定しない場合、このコマンドはすべてのインタフェースの ARP エントリを削除します。

説明

reset arp コマンドは ARP テーブルから ARP エントリを削除します。

例

すべてのスタティック ARP エントリを削除します。

<Switch> reset arp static

関連コマンド

- **arp static**
- **display arp**

目次

このセクションのページは **4-x-x** です。

2 章 Gratuitous ARP 2-1
2.1 Gratuitous ARP 設定コマンド 2-1
2.1.1 arp ip-conflict log prompt.....2-1
2.1.2 arp send-gratuitous-arp.....2-2
2.1.3 gratuitous-arp mac-change retransmit.....2-3
2.1.4 gratuitous-arp-learning enable 2-4
2.1.5 gratuitous-arp-sending enable.....2-5

2章 Gratuitous ARP

2.1 Gratuitous ARP設定コマンド

2.1.1 arp ip-conflict log prompt

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

デフォルト

無効

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。

デフォルトでは、受信 ARP パケットの送信側 IP アドレスを使用している場合、装置は次の操作を実行します。

- Gratuitous ARP 要求を送信します。
- 装置が重複に関する ARP 応答を受信した後にエラーメッセージを表示します。

このコマンドを使用して、Gratuitous ARP 応答または重複確認の要求を送信する前に装置がエラーメッセージを表示できるように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

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。デフォルトは 2000 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。

この機能がインタフェースで有効になるのは、インタフェースに IP アドレスがあり、インタフェースのデータリンク層の状態がアップしている場合だけです。

この機能は、VRRP 仮想 IP アドレス、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 mac-change retransmit

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

デフォルト

MAC アドレスが変更された時に gratuitous ARP パケットを 1 回送信します。

View

System view

定義済みユーザロール

network-admin

パラメータ

times: gratuitous ARP パケットを再送信する回数を設定します。設定範囲は 1 から 10 です。

interval *seconds*: gratuitous ARP パケットを再送信する送信間隔を設定します。設定範囲は 1 秒から 10 秒です。

説明

gratuitous-arp mac-change retransmit コマンドは MAC アドレス変更による gratuitous ARP パケットの複数送信を有効にし、送信間隔を設定します。

undo gratuitous-arp mac-change retransmit コマンドは MAC アドレス変更による gratuitous ARP パケットの送信を 1 回にします。

この機能は、装置の MAC アドレスが変更にされたときに送信する gratuitous ARP パケットを、指定された間隔で指定された時間再送信します。

装置は、MAC アドレスの変更を他のデバイスに通知するために、gratuitous ARP パケットを送信します。ただし、装置はデフォルトで 1 回だけ gratuitous ARP パケットを送信するため、他の装置はパケットの受信に失敗する可能性があります。この機能を使用して、他の装置がパケットを受信できるように、gratuitous ARP パケットを再送信するパラメータを設定します。

例

MAC アドレス変更による gratuitous ARP パケットの再送信を有効にし、送信数を 3 回、間隔を 5 秒に設定します。

<Switch> system-view

[Switch] gratuitous-arp mac-change retransmit 3 interval 5

2.1.4 gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-learning enable コマンドは gratuitous ARP パケットの学習機能を有効にします。

undo gratuitous-arp-learning enable コマンドは gratuitous ARP パケットの学習機能を無効にします。

gratuitous ARP パケットの学習機能は、装置が受信した gratuitous ARP パケットをもとに ARP エントリを作成あるいはアップデートすることで ARP テーブルを維持することができます。

学習機能が無効であるとき、装置は既存の ARP エントリのみをアップデートするため受信した gratuitous ARP パケットを使用します。ARP エントリは受信した gratuitous ARP パケットをもとに作成されません。これは ARP テーブルの空き容量を節約します。

例

gratuitous ARP パケットの学習機能を有効にします。

<Switch> system-view

[Switch] gratuitous-arp-learning enable

2.1.5 gratuitous-arp-sending enable

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-sending enable コマンドは異なるサブネットから ARP 要求を受信した際に、gratuitous ARP パケットの送信を有効にします。

undo gratuitous-arp-sending enable コマンドはデフォルトに戻します。

例

異なるサブネットから ARP 要求を受信した際に、gratuitous ARP パケットの送信を無効にします。

<Switch> system-view

[Switch] undo gratuitous-arp-sending enable

目次

このセクションのページは **4-x-x** です。

3 章 Proxy ARP 3-1
3.1 Proxy ARP 設定コマンド 3-1
3.1.1 display local-proxy-arp 3-1
3.1.2 display proxy-arp 3-2
3.1.3 local-proxy-arp enable 3-2
3.1.4 proxy-arp enable 3-4

3章 Proxy ARP

3.1 Proxy ARP設定コマンド

3.1.1 display local-proxy-arp

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースのローカル Proxy ARP の状態を表示します。

説明

display local-proxy-arp コマンドはローカル Proxy ARP の状態を表示します。

このコマンドを使用すると、ローカル Proxy ARP が有効か無効かを確認できます。

インタフェースを指定しない場合、このコマンドはすべてのインタフェースのローカル Proxy ARP ステータスを表示します。

例

VLAN インタフェース 2 のローカル Proxy ARP の状態を表示します。

<Switch> display local-proxy-arp interface vlan-interface 2

```
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

関連コマンド

local-proxy-arp enable

3.1.2 display proxy-arp

Syntax

display proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの Proxy ARP の状態を表示します。インタフェースを指定しない場合、このコマンドはすべてのインタフェースの 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。

このコマンドを使用すると、Proxy ARP が有効か無効かを確認できます。

例

VLAN インタフェース 2 の Proxy ARP の状態を表示します。

<Switch> display proxy-arp interface vlan-interface 2

```
Interface Vlan-interface2
 Proxy ARP status: disabled
```

関連コマンド

proxy-arp enable

3.1.3 local-proxy-arp enable

Syntax

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

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 *start-ip-address* **to** *end-ip-address*: ローカル Proxy ARP が有効になる IP アドレス範囲を指定します。*start-ip-address* は、*end-ip-address* 以下でなければなりません。

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。

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

VLAN インタフェース 2 でローカル Proxy ARP を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] local-proxy-arp enable

VLAN インタフェース 2 で IP アドレス範囲 1.1.1.1～1.1.1.20 のローカル Proxy ARP を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20

関連コマンド

display local-proxy-arp

3.1.4 proxy-arp enable

Syntax

proxy-arp enable

undo proxy-arp enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

説明

proxy-arp enable コマンドは Proxy ARP を有効にします。

undo proxy-arp enable コマンドは Proxy ARP を無効にします。

Proxy ARP は異なるネットワークの IP アドレスの ARP 要求に応答するため、ネットワークの装置で有効にします。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

一般的な Proxy ARP は異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ローカル Proxy ARP は同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

例

VLAN インタフェース 2 で Proxy ARP を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] proxy-arp enable

関連コマンド

display proxy-arp

目次

このセクションのページは **4-x-x** です。

4 章 ARP スヌーピング.....4-1
4.1 ARP スヌーピング設定コマンド.....4-1
4.1.1 arp snooping enable.....4-1
4.1.2 display arp snooping.....4-1
4.1.3 reset arp snooping.....4-3

4章 ARP スヌーピング

4.1 ARPスヌーピング設定コマンド

4.1.1 arp snooping enable

Syntax

arp snooping enable

undo arp snooping enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

arp snooping enable コマンドは ARP snooping を有効にします。

undo arp snooping enable コマンドは ARP snooping を無効にします。

例

VLAN 2 で ARP snooping を有効にします。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] arp snooping enable

4.1.2 display arp snooping

Syntax

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

display arp snooping ip *ip-address* [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN の ARP snooping エントリを表示します。設定範囲は 1～4094 です。

count: 現在の ARP snooping エントリの数を表示します。

ip *ip-address*: 指定された IP アドレスの ARP snooping エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックユニットのメンバ装置 ID です。メンバ装置を指定しない場合、このコマンドはマスタ装置の ARP snooping エントリを表示します。

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 ARP 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
```

ARP snooping エントリの数を表示します。

<Switch> display arp snooping count

```
Total entries: 2
```

表 4-1 コマンド出力

フィールド	説明
IP Address	ARP snoopingエントリのIPアドレスです。
MAC Address	ARP snoopingエントリのMACアドレスです。
VLAN ID	ARP snoopingエントリが所属するVLAN IDです。
Interface	ARP snoopingエントリの入力インタフェースです。
Aging	ARP snoopingエントリのエージングタイムです。単位は分です。 別の拡張インタフェースカードからARPエントリを学習した場合、拡張インタフェースカードはエントリのエージングタイムを学習することはできません。このフィールドは**N/A**と表示されます。

フィールド	説明
Status	ARP snoopingエントリの状態です。 ● **Valid**－正常なARP snoopingエントリです。 ● **Invalid**－不正なARP snoopingエントリです。 ● **Collision**－ARP snoopingエントリが重複しています。
Total entries	ARP snoopingエントリの数です。

関連コマンド

reset arp snooping

4.1.3 reset arp snooping

Syntax

reset arp snooping [**ip** *ip-address* | **vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 指定した IP アドレスの ARP snooping エントリを削除します。

vlan *vlan-id*: 指定した VLAN の ARP snooping エントリを削除します。設定範囲は 1～4094 です。

説明

reset arp snooping コマンドは ARP snooping エントリを削除します。

オプションを指定しないと、このコマンドはすべての ARP snooping エントリを削除します。

例

VLAN 2 の ARP snooping エントリを削除します。

<Switch> reset arp snooping vlan 2

関連コマンド

display arp snooping

目次

このセクションのページは **4-x-x** です。

5 章 IP アドレス.....5-1
5.1 IP アドレス設定コマンド.....5-1
5.1.1 display ip interface.....5-1
5.1.2 display ip interface brief.....5-4
5.1.3 ip address.....5-7

5章 IP アドレス

5.1 IPアドレス設定コマンド

5.1.1 display ip interface

Syntax

display ip interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、すべてのレイヤ 3 インタフェースの IP 設定と統計情報を表示します。

説明

display ip interface コマンドはレイヤ 3 インタフェースの IP 設定および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。

- インタフェースが送受信したユニキャストパケットの数、バイトの数、およびマルチキャストパケットの数が含まれます。
- インタフェースが受信した TTL 無効のパケットの数と ICMP パケットの数が含まれます。

パケットの統計情報はネットワークへの攻撃の可能性を探すのに役立ちます。

例

VLAN-interface 10 の IP 設定と統計情報を表示します。

<Switch> display ip interface vlan-interface 10

```
Vlan-interface10 current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
```

```
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:        0
ICMP packet input number:         0
  Echo reply:                    0
  Unreachable:                   0
  Source quench:                 0
  Routing redirect:              0
  Echo request:                  0
  Router advert:                 0
  Router solicit:                0
  Time exceed:                   0
  IP header bad:                 0
  Timestamp request:             0
  Timestamp reply:               0
  Information request:           0
  Information reply:             0
  Netmask request:               0
  Netmask reply:                 0
  Unknown type:                  0
```

表 5-1 コマンド出力

フィールド	説明
current state	インタフェースの現在の物理状態です。 • **Administrative DOWN**—インタフェースが**shutdown**コマンドでシャットダウンしています。 • **DOWN**—インタフェースが管理上upとなっていますが、物理的にdownしています。ケーブル接続あるいはリンク障害によって引き起こされる可能性があります。 • **UP**—インタフェースが管理上および物理的にupとなっています。
Line protocol current state	データ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。しかし、対応するリンクが存在しない、または永久に対応するリンクは存在しないが要求されれば確立できる状態です。

フィールド	説明
Internet Address	インタフェースのIPアドレスです。 ● **Primary**—プライマリIPアドレスです。 ● **Sub**—セカンダリIPアドレスです。 ● **DHCP-Allocated**—DHCPによって取得したIPアドレスです。 ● **BOOTP-Allocated**—BOOTPによって取得したIPアドレスです。 ● **Mad**—MADのIPアドレスです。 ● **IRF-Member**—IRFスタックメンバ装置の管理Ethernetポートの IPアドレスです。
Broadcast address	インタフェースに接続されたサブネットのブロードキャストアドレスです。
The Maximum Transmit Unit	インタフェースのMTU（最大転送ユニット）です。単位はバイトです。
input packets, bytes, multicasts output packets, bytes, multicasts	送受信されたすべてのパケットとバイト、およびインタフェース上で送受信されたマルチキャストパケットです。（装置起動時に統計情報の取得が開始されます。）
TTL invalid packet number	インタフェースで受信したTTL無効のパケット数です。（装置起動時に統計情報の取得が開始されます。）

フィールド	説明
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	インタフェースで受信したICMPパケットの総数です。（装置起動時に統計情報の取得が開始されます。） • **Echo reply packets**－エコー応答パケットです。 • **Unreachable packets**－到達不能パケットです。 • **Source quench packets**－送信元抑制パケットです。 • **Routing redirect packets**－ルーティングリダイレクトパケットです。 • **Echo request packets**－エコー要求パケットです。 • **Router advertisement packets**－ルータ通知パケットです。 • **Router solicitation packets**－ルータ選択要求パケットです。 • **Time exceeded packets**－時間超過パケットです。 • **IP header bad packets**－IPヘッダ不良パケットです。 • **Timestamp request packets**－タイムスタンプ要求パケットです。 • **Timestamp reply packets**－タイムスタンプ応答パケットです。 • **Information request packets**－情報要求パケットです。 • **Information reply packets**－情報応答パケットです。 • **Netmask request packets**－ネットマスク要求パケットです。 • **Netmask reply packets**－ネットマスク応答パケットです。 • **Unknown type packets**－不明なタイプのパケットです。

関連コマンド

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

5.1.2 display ip interface brief

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**description**]

View

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: インタフェースの種類を指定します。

interface-number: インタフェース番号を指定します。

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、コマンドは各インタフェース記述に最大 13 文字を表示します。説明が 13 文字を超える場合は、最初の 10 文字が表示され、その後に省略記号（...）が続きます。

説明

display ip interface brief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 設定の概要情報を表示します。

コマンドによって表示される情報には、物理層プロトコルとリンク層プロトコルの状態、IP アドレス、およびインタフェースの説明が含まれます。

例

VLAN インタフェースの IP 設定の概要情報を表示します。

<Switch> display ip interface vlan-interface brief

```
*down: administratively down
(s): spoofing  (l): loopback
Interface          Physical Protocol IP address     VPN instance Description
Vlan10             down     down     6.6.6.1        --          Link to Co...
```

<Switch> display ip interface vlan-interface brief description

```
*down: administratively down
(s): spoofing  (l): loopback
Interface          Physical Protocol IP address     VPN instance Description
Vlan10             down     down     6.6.6.1        --          Link to CoreR
                                                                 Outer
```

表 5-2 コマンド出力

フィールド	説明
*down: administratively down	インタフェースが**shutdown**コマンドでシャットダウンしています。
(s) : spoofing	インタフェースのスプーフィング属性です。リンクレイヤプロトコルがup表示されているインタフェースにリンクがない、あるいはリンクがオンデマンドでのみ設定されることを示します。

フィールド	説明
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。 ● **down(l)**—インタフェースのプロトコル状態はdownしています。（loopback） ● **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)**—インタフェースのプロトコル状態がup（loopback）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。IPアドレスが設定されていない場合、このフィールドにはハイフン(--)が表示されます。
VPN instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 インタフェースが属するVPNインスタンス名です。このフィールドには最大12文字が表示されます。VPNインスタンス名が12文字を超える場合、最初の9文字が表示され、その後に省略記号(...)が続きます。インタフェースがどのVPNインスタンスにも属していない場合、このフィールドにはハイフン(--)が表示されます。
Description	インタフェースの説明の情報です。 このフィールドには最大13文字が表示されます。説明が13文字を超える場合は、最初の10文字が表示され、その後に省略記号(...)が続きます。説明が設定されていない場合、このフィールドにはハイフン(--)が表示されます。

関連コマンド

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

5.1.3 ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address *ip-address* { *mask-length* | *mask* } [**sub**]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: インタフェースの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: サブネットマスクの長さを指定します。設定範囲は 1～31 です。ループバックインタフェースの設定範囲は 1～32 です。

mask: サブネットマスクを指定します。ドットで区切り、10 進数で指定します。

sub: インタフェースにセカンダリ IP アドレスを割り当てます。

説明

ip address コマンドはインタフェースに IP アドレスを割り当てます。

undo ip address コマンドはインタフェースから IP アドレスを削除します。

インタフェースのプライマリまたはセカンダリ IP アドレスを設定するために、このコマンドを使用します。

インタフェースは 1 つのプライマリ IP アドレスのみ設定することができます。新しく設定されたプライマリ IP アドレスは、古いアドレスを上書きします。インタフェースが複数のサブネットに接続されている場合、サブネットがインタフェースを通して通信できるように、プライマリ IP アドレスとサブネットを設定します。

BOOTP あるいは DHCP 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。

パラメータを指定しない場合、**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 **4-x-x** です。

6 章 DHCP 6-1
6.1 DHCP 設定コマンド 6-1
6.1.1 dhcp dscp 6-1
6.1.2 dhcp enable 6-2
6.1.3 dhcp select 6-2
6.2 DHCP サーバ設定コマンド 6-3
6.2.1 address range 6-3
6.2.2 bims-server 6-5
6.2.3 bootfile-name 6-6
6.2.4 dhcp server apply ip-pool 6-7
6.2.5 dhcp server forbidden-ip 6-8
6.2.6 dhcp server ip-pool 6-9
6.2.7 dhcp server ping packets 6-10
6.2.8 dhcp server ping timeout 6-11
6.2.9 dhcp server relay information enable 6-12
6.2.10 display dhcp server conflict 6-12
6.2.11 display dhcp server expired 6-14
6.2.12 display dhcp server free-ip 6-15
6.2.13 display dhcp server ip-in-use 6-16
6.2.14 display dhcp server pool 6-18
6.2.15 display dhcp server statistics 6-21
6.2.16 dns-list 6-23
6.2.17 domain-name 6-24
6.2.18 expired 6-25
6.2.19 forbidden-ip 6-26
6.2.20 gateway-list 6-27
6.2.21 nbns-list 6-28
6.2.22 netbios-type 6-29
6.2.23 network 6-30
6.2.24 next-server 6-31
6.2.25 option 6-32
6.2.26 reset dhcp server conflict 6-34
6.2.27 reset dhcp server expired 6-34
6.2.28 reset dhcp server ip-in-use 6-35
6.2.29 reset dhcp server statistics 6-36
6.2.30 static-bind 6-36

6.2.31 tftp-server domain-name 6-38
6.2.32 tftp-server ip-address 6-39
6.2.33 voice-config 6-40
6.3 DHCP リレーエージェント設定コマンド 6-41
6.3.1 dhcp relay client-information record 6-41
6.3.2 dhcp relay client-information refresh enable 6-42
6.3.3 dhcp relay information circuit-id 6-43
6.3.4 dhcp relay information enable 6-45
6.3.5 dhcp relay information remote-id 6-46
6.3.6 dhcp relay information strategy 6-48
6.3.7 dhcp relay release ip 6-49
6.3.8 dhcp relay server-address 6-50
6.3.9 display dhcp relay client-information 6-51
6.3.10 display dhcp relay information 6-53
6.3.11 display dhcp relay server-address 6-54
6.3.12 display dhcp relay statistics 6-56
6.3.13 reset dhcp relay client-information 6-57
6.3.14 reset dhcp relay statistics 6-58
6.4 DHCP クライアント設定コマンド 6-59
6.4.1 dhcp client dad enable 6-59
6.4.2 dhcp client dscp 6-59
6.4.3 display dhcp client 6-60
6.4.4 ip address dhcp-alloc 6-63
6.5 DHCP スヌーピング設定コマンド 6-64
6.5.1 dhcp snooping binding record 6-64
6.5.2 dhcp snooping enable 6-65
6.5.3 dhcp snooping information circuit-id 6-66
6.5.4 dhcp snooping information enable 6-68
6.5.5 dhcp snooping information remote-id 6-69
6.5.6 dhcp snooping information strategy 6-71
6.5.7 dhcp snooping trust 6-72
6.5.8 display dhcp snooping binding 6-73
6.5.9 display dhcp snooping information 6-75
6.5.10 display dhcp snooping packet statistics 6-76
6.5.11 display dhcp snooping trust 6-77
6.5.12 reset dhcp snooping binding 6-78
6.5.13 reset dhcp snooping packet statistics 6-79
6.6 BOOTP クライアント設定コマンド 6-80
6.6.1 display bootp client 6-80
6.6.2 ip address bootp-alloc 6-81

6章 DHCP

6.1 DHCP設定コマンド

6.1.1 dhcp dscp

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

デフォルト

56

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DHCP パケットの DSCP を設定します。設定範囲は 0～63 です。

説明

dhcp dscp コマンドは DHCP サーバあるいは DHCP リレーエージェントに送信される DHCP パケットの DSCP を設定します。

undo dhcp dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

DHCP パケットの DSCP を 30 に設定します。

<Switch> system-view

[Switch] dhcp dscp 30

6.1.2 dhcp enable

Syntax

dhcp enable

undo dhcp enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp enable コマンドは DHCP を有効にします。

undo dhcp enable コマンドは DHCP を無効にします。

DHCP 関連の設定は、DHCP を有効にした後にのみ有効になります。

DHCP サーバあるいは DHCP リレーエージェントの設定を実行する前に、DHCP を有効にしてください。

例

DHCP を有効にします。

<Switch> system-view

[Switch] dhcp enable

6.1.3 dhcp select

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

デフォルト

インタフェースは DHCP サーバモードで動作し、設定パラメータの DHCP 要求に応答します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

relay: インタフェースで DHCP リレーエージェントを有効にします。

server: インタフェースで DHCP サーバを有効にします。

説明

dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを有効にします。

undo dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを無効にします。インタフェースは着信 DHCP パケットを破棄します。

DHCP サーバが DHCP リレーエージェントとして動作できるようにする前に、**reset dhcp server ip-in-use** コマンドを使用してアドレスの割り当てと許可された ARP エントリを消去します。これらの許可 ARP エントリは、DHCP リレーエージェントが有効になった後に作成された ARP エントリと競合する可能性があります。

DHCP リレーエージェントで DHCP サーバ proxy が有効になっていると、proxy は DHCP クライアントと DHCP サーバの間でパケットを転送します。

- DHCP クライアントから DHCP 要求を受信すると、proxy はそれらを DHCP サーバに転送します。
- DHCP サーバから DHCP 応答を受信すると、proxy はこれらの応答内の DHCP サーバの IP アドレスを独自の IP アドレスとして変更します。

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**
- **reset dhcp server ip-in-use**

6.2 DHCPサーバ設定コマンド

6.2.1 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 アドレス範囲をデフォルトに戻します。

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**

6.2.2 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。セキュリティ保護のため、プレーンテキスト形式で指定されたキーは暗号化された形式で保存されます。

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、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 サーバ情報をデフォルトに戻します。

コマンドを複数回、使用した場合、最後の設定が有効になります。

セキュリティ目的のため、平文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

6.2.3 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。

TFTP サーバでコンフィグレーションファイルを指定するには、*bootfile-name* を使用します。

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**

6.2.4 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 コマンドは設定をデフォルトに戻します。

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

6.2.5 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。

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。

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、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。

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**

6.2.6 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: アドレスプールを一意に識別するため 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**

6.2.7 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**

6.2.8 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**

6.2.9 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 Option82 を有効にします。

undo dhcp server relay information enable コマンドは DHCP サーバの Option82 を無効にします。

DHCP サーバが Option82 を処理するように設定されている場合、Option82 のメッセージを受信すると、DHCP サーバは Option82 を DHCP 応答メッセージに追加します。DHCP サーバが Option82 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 Option82 を追加しません。

例

DHCP サーバの Option82 を無効にします。

<Switch> system-view

[Switch] undo dhcp server relay information enable

6.2.10 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 6-1 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

6.2.11 display dhcp server expired

Syntax

display dhcp server expired [**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 アドレスのリース期限の終了に関する情報を表示します。IP アドレスを指定しない場合、このコマンドはすべての IP アドレスに関するリースの有効期限情報を表示します。

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。

パラメータを指定しない場合、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。

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 6-2 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

6.2.12 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 6-3 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**

6.2.13 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。P アドレスを指定しない場合、このコマンドは割り当てられたすべての IP アドレスに関する割り当て情報を表示します。

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。アドレスプールを指定しない場合、このコマンドは、すべてのアドレスプールで割り当てられている IP アドレスに関するバインド情報を表示します。

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。

パラメータを指定しない場合、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。

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。

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。

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 6-4 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。

フィールド	説明
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

6.2.14 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
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired 1 2 3 0

Pool name: 1
  Network 20.1.2.0 mask 255.255.255.0
  secondary networks:
    20.1.3.0 mask 255.255.255.0
    20.1.4.0 mask 255.255.255.0
  bims-server ip 192.168.0.51 port 50 sharekey cipher
$c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
  forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
  gateway-list 20.1.1.1 20.1.1.2 20.1.1.4
  nbns-list 20.1.1.5 20.1.1.6 20.1.1.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired 1 0 0 0

Pool name: 2
  Network 20.1.3.0 mask 255.255.255.0
  address range 20.1.3.1 to 20.1.3.15

  next-server 20.1.3.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 20.1.3.2
  voice-config as-ip 20.1.3.5
  voice-config voice-vlan 3 enable
  voice-config fail-over 20.1.3.6 123*
  option 2 ip-address 20.1.3.10
  expired 1 0 0 0
```

```
Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
```

表 6-5 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。
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。
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。

フィールド	説明
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。

6.2.15 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 6-6 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。
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。

フィールド	説明
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

6.2.16 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

6.2.17 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。

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

6.2.18 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 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 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 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**

6.2.19 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にします。

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**

6.2.20 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 個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。

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 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。

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。

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

6.2.21 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**

6.2.22 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宛先名-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。

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**

6.2.23 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。指定されない場合、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**

6.2.24 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 アドレスをデフォルトに戻します。

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

6.2.25 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、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。

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。

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指定された DHCP オプションは、DHCP アドレスプールで指定された DHCP オプションよりも優先されます。

同じコードを指定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

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

6.2.26 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

6.2.27 reset dhcp server expired

Syntax

reset dhcp server expired [**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*: 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。

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。

パラメータを指定しない場合、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。

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

6.2.28 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。

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。

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。

パラメータを指定しない場合、すべての IP アドレスの割り当て情報を削除します。

割り当てられたスタティック割り当て情報、未割り当てになったスタティック割り当て情報を削除するために、**reset dhcp server ip-in-use** コマンドを使用します。

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

6.2.29 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

6.2.30 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

6.2.31 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**

6.2.32 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**

6.2.33 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

6.3 DHCPリレーエージェント設定コマンド

6.3.1 dhcp relay client-information record

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information record コマンドはリレーエントリのクライアント情報の記録を有効にします。リレーエントリはクライアントの IP アドレス、MAC アドレスのようなクライアントの情報が含まれます。

undo dhcp relay client-information コマンドはリレーエントリのクライアント情報の記録を無効にします。

リレーエントリのクライアント情報の記録を無効にすると、記録されたすべてのリレーエントリを削除します。

DHCP リレーエージェントが DHCP クライアントのゲートウェイで設定されたときのみクライアント情報が記録されます。

例

リレーエントリのクライアント情報の記録を有効にします。

<Switch> system-view

[Switch] dhcp relay client-information record

関連コマンド

dhcp relay client-information refresh enable

6.3.2 dhcp relay client-information refresh enable

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

デフォルト

リレーエントリを定期的に更新します。

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information refresh enable コマンドは DHCP リレーエージェントがダイナミックリレーエントリを定期的に更新できるようにします。

undo dhcp relay client-information refresh enable コマンドは DHCP リレーエージェントを無効にし、ダイナミックリレーエントリを定期的に更新します。

DHCP クライアントは、DHCP-RELEASE メッセージを DHCP サーバにユニキャストして、IP アドレスを解放します。DHCP リレーエージェントはメッセージを DHCP サーバに伝達し、クライアントの IP-to-MAC エントリを削除しません。

この機能により、DHCP リレーエージェントはクライアントの IP アドレスを使用して、DHCP-REQUEST メッセージを DHCP サーバに定期的に送信します。

- サーバが DHCP-ACK メッセージを返すか、間隔内にメッセージを返さない場合、DHCP リレーエージェントは次の操作を実行します。

- □ リレーエントリを削除します。
- □ DHCP-RELEASE メッセージを DHCP サーバに送信して、IP アドレスを解放します。

- サーバが DHCP-NAK メッセージを返した場合、リレーエージェントはエントリを保持します。

この機能を無効にすると、DHCP リレーエージェントはリレーエントリを自動的に削除しません。DHCP クライアントが IP アドレスを解放した後、対応するリレーエントリを削除するには、リレーエージェントで **reset dhcp relay client-information** を使用する必要があります。

例

リレーエントリの定期的な更新を無効にします。

<Switch> system-view

[Switch] undo dhcp relay client-information refresh enable

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

6.3.3 dhcp relay information circuit-id

Syntax

dhcp relay information circuit-id { **bas** | **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

デフォルト

コードモードは normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

bas: circuit ID サブオプションを埋め込むためにインタフェースと VLAN 情報を使用する bas モードを指定します。

string *circuit-id*: circuit ID サブオプションの内容を指定します。設定範囲は 3～63 です。大文字、小文字を区別します。

normal: コードモードを normal モードに指定します。このパディングの内容は VLAN ID とポート番号から設定されます。

verbose: verbose モードを指定します。パディングの内容には、ノード識別子、インタフェース情報、および VLAN ID が含まれています。デフォルトのノード識別子は、アクセスノードの MAC アドレスです。デフォルトのインタフェース情報は、Ethernet タイプ（eth で固定）、シャーシ番号、スロット番号、サブスロット番号、およびインタフェース番号で設定されています。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: アクセスノードの識別子を指定します。

- **mac**: アクセスノードの MAC アドレスをノード識別子として使用します。
- **sysname**: 装置名をノード識別子として使用します。system view で **sysname** コマンドを使用して装置名を設定できます。指定されたパディング形式に関係なく、装置名のパディング形式は常に ASCII です。

🕮 **メモ**:

ノード識別子として **sysname** を指定する場合は、装置名を設定するときにスペースを含めないでください。それ以外の場合、DHCP リレーエージェントは Option82 の追加または置換に失敗します。

- **user-defined** *node-identifier*: ノード識別子を使用します。設定範囲は 1～50 文字です。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、指定されたパディング形式に関係なく、常に ASCII です。

interface: インタフェース情報としてインタフェース名を使用します。指定したパディング形式に関係なく、インタフェース名のパディング形式は常に ASCII です。

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 relay information circuit-id コマンドは Option82 の circuit ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp relay information circuit-id コマンドはデフォルトに戻します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

string モード、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 6-7 に異なるモードのパディング形式を示します。

表 6-7 異なるモードのパディング形式

キーワード（モード）	パディング形式が指定されていない場合	パディング形式が ASCII	パディング形式が hex
string *circuit-id*	パディング形式を指定できません。常にASCIIになります。	ー	ー
normal	hexです。	ASCIIです。	hexです。
verbose	VLAN IDはhexです。 ノード識別子、Ethernetタイプ、シャーシ番号、スロット番号、サブスロット番号、およびインタフェース番号にはASCIIです。	ASCIIです。	ノード識別子およびEthernetタイプ用の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、およびVLAN IDのhexです。

例

circuit ID サブオプションのコードモードが verbose、ノード識別子が装置名、パディング形式が ASCII に指定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] dhcp relay information enable

[Switch-Vlan-interface10] dhcp relay information strategy replace

[Switch-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier sysname format ascii

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

6.3.4 dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

dhcp relay information enable コマンドはリレーエージェントで Option82 のサポートを有効にします。

undo dhcp relay information enable コマンドは Option82 のサポートを無効にします。

このコマンドによって DHCP リレーエージェントが DHCP サーバに要求を転送する前に、Option82 が含まれない DHCP 要求に Option82 を追加します。Option82 の内容は **dhcp relay information circuit-id** コマンド、**dhcp relay information remote-id** コマンドによって決まります。DHCP 要求に Option82 が含まれる場合、リレーエージェントは **dhcp relay information strategy** コマンドで設定された方法にしたがって DHCP 要求を処理します。

この機能が無効である場合、リレーエージェントは Option82 を含む DHCP 要求と Option82 を含まない DHCP 要求を DHCP サーバに転送します。

例

Option82 のサポートを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] dhcp relay information enable

関連コマンド

- **dhcp relay information circuit-id**
- **dhcp relay information remote-id**
- **dhcp relay information strategy**
- **display dhcp relay information**

6.3.5 dhcp relay information remote-id

Syntax

dhcp relay information remote-id { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

デフォルト

コードモードは **normal** で、パディング形式は **hex** です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

normal: コードモードを normal モードに指定します。このパディングの内容は受信インタフェースの MAC アドレスです。

format: remote ID サブオプションのパディング形式を指定します。デフォルトパディング形式は 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。

string *remote-id*: remote ID サブオプションの内容を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

sysname: リモート ID サブオプションの内容として装置名を指定します。装置名は **sysname** コマンドを使用して設定することができます。

説明

dhcp relay information remote-id コマンドは Option82 の remote ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp relay information remote-id コマンドはデフォルトに戻します。

指定した文字列（**string**）あるいは装置名（**sysname**）は常に ASCII です。**normal** モードのパディング形式はコマンドの設定によって変わります。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

Option82 の remote ID サブオプションのパディング内容を **device001** に指定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] dhcp relay information enable

[Switch-Vlan-interface10] dhcp relay information strategy replace

[Switch-Vlan-interface10] dhcp relay information remote-id string device001

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

6.3.6 dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

デフォルト

replace

View

Interface view

定義済みユーザロール

network-admin

パラメータ

drop: Option82 メッセージが含まれる DHCP メッセージを廃棄します。

keep: 元の Option82 をそのまま保持し、DHCP メッセージを転送します。

replace: DHCP メッセージを転送する前に、元の Option82 を設定済みの Option82 に置き換えます。

説明

dhcp relay information strategy コマンドは DHCP リレーエージェントで Option82 が含まれるメッセージの処理方法を設定します。

undo dhcp relay information strategy コマンドはデフォルトに戻します。

このコマンドは DHCP 要求に Option82 が含まれるときのみ適用します。

Option82 を含まない DHCP 要求の場合、DHCP リレーエージェントは、要求を DHCP サーバに転送する前に、常に Option82 を要求に追加します。

処理方法が **replace** の場合は、Option82 のパディングモードとパディングフォーマットを設定します。処理方法が **keep** または **drop** の場合は、パディングモードまたはパディングフォーマットを設定する必要はありません。設定しても設定は有効になりません。

例

DHCP リレーエージェントで Option82 が含まれるメッセージの処理方法を **keep** に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] dhcp relay information enable

[Switch-Vlan-interface10] dhcp relay information strategy keep

関連コマンド

- **dhcp relay information enable**
- **display dhcp relay information**

6.3.7 dhcp relay release ip

Syntax

dhcp relay release ip *ip-address*

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: リリースされる IP アドレスを指定します。

説明

dhcp relay release ip コマンドは指定したクライアントの IP アドレスをリリースします。

このコマンドを実行した後、リレーエージェントは DHCP サーバに DHCP-RELEASE パケットを送信し、IP アドレスのリレーエントリを削除します。パケットを受信するとサーバは、IP アドレスをリリースするため、指定された IP アドレスの割り当て情報を削除します。

例

IP アドレス 1.1.1.1 をリリースします。

<Switch> system-view

[Switch] dhcp relay release ip 1.1.1.1

6.3.8 dhcp relay server-address

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: DHCP サーバの IP アドレスを指定します。DHCP リレーエージェントは DHCP クライアントから受信した DHCP パケットを DHCP サーバに転送します。

説明

dhcp relay server-address コマンドは DHCP リレーエージェントの DHCP サーバを指定します。

undo dhcp relay server-address コマンドは DHCP サーバを削除します。

DHCP サーバを指定する IP アドレスは、DHCP リレーエージェントインタフェースの IP アドレスと同一のサブネット上にすることはできません。そうでなければ、DHCP クライアントは IP アドレスの取得に失敗します。

インタフェースで最大 8 つの DHCP サーバを指定することができます。DHCP リレーエージェントはクライアントからのパケットをすべての指定された DHCP サーバに転送します。

- 要求がユーザクラスルールと一致する場合、DHCP リレーエージェントはパケットをそのユーザクラスで設定されている DHCP サーバに転送します。
- 要求がどのユーザクラスルールとも一致しない場合、DHCP リレーエージェントは、ユーザクラスが設定されていない DHCP サーバに要求を転送します。

このコマンドを同じユーザクラスで実行し、*ip-address* に異なる値を指定した場合は、異なる DHCP サーバに対して同じユーザクラスを指定します。同じ IP アドレスに対して異なるユーザクラスでコマンドを実行した場合は、最新の設定が有効になります。

IP アドレスを指定しない場合、**undo dhcp relay server-address** コマンドはインタフェースのすべての DHCP サーバを削除します。

DHCP サーバ選択アルゴリズムが **master-backup** の場合は、マスタサーバとバックアップサーバの両方で同じユーザクラスが設定されているか、ユーザクラスが設定されてい

ないことを確認してください。そうでないと、DHCP クライアントは IP アドレスを正しく取得できません。

例

リレーエージェントの VLAN インタフェース 10 で DHCP サーバ 1.1.1.1 を指定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] dhcp relay server-address 1.1.1.1

関連コマンド

dhcp select relay

6.3.9 display dhcp relay client-information

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースのリレーエントリを表示します。インタフェースを指定しない場合、このコマンドはすべてのインタフェースのリレーエントリを表示します。

ip *ip-address*: 指定された IP アドレスのリレーエントリを表示します。IP アドレスを指定しないと、このコマンドはすべての IP アドレスのリレーエントリを表示します。

説明

display dhcp relay client-information コマンドはリレーエージェントのリレーエントリを表示します。

dhcp relay client-information record コマンドは設定されているときのみ、DHCP リレーエージェントはリレーエントリを記録します。

パラメータを指定しない場合、**display dhcp relay client-information** コマンドはリレーエージェントのすべてのリレーエントリを表示します。

例

リレーエージェントのすべてのリレーエントリを表示します。

<Switch> display dhcp relay client-information

```
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address      MAC address     Type       Interface          VPN name
10.1.1.5        00e0-0000-0000  Temporary  Vlan2              N/A
```

表 6-8 コマンド出力

フィールド	説明
Total number of client-information items	リレーエントリの総数です。
Total number of dynamic items	ダイナミックリレーエントリの総数です。
Total number of temporary items	一時的なリレーエントリの総数です。
IP address	DHCPクライアントのIPアドレスです。
MAC address	DHCPクライアントのMACアドレスです。
Type	リレーエントリタイプです。 • **Dynamic**—リレーエージェントはDHCPサーバからAck応答を受信した際にダイナミックリレーエントリを作成します。 • **Temporary**—リレーエージェントはDHCPクライアントからREQUESTパケットを受信した際に一時的なリレーエントリを作成します。
Interface	DHCPクライアントに接続されたレイヤ3インタフェースです。リレーエージェントにインタフェース情報がない場合、**N/A**と表示されます。
VPN name	このフィールドは、QX-S5300Gシリーズではサポートしていません。 DHCPクライアントが属するVPNインスタンス名です。DHCPクライアントがどのVPNにも属していない場合、このフィールドには**N/A**と表示されます。

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

6.3.10 display dhcp relay information

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの Option82 の設定情報を表示します。インタフェースを指定しない場合、すべてのインタフェースの Option82 の設定情報を表示します。

説明

display dhcp relay information コマンドは DHCP リレーエージェントの Option82 の設定情報を表示します。

例

すべてのインタフェースの Option82 の設定情報を表示します。

<Switch> display dhcp relay information

```
Interface: Vlan-interface100
  Status: Enable
  Strategy: Replace
  Circuit ID Pattern: Verbose
  Remote ID Pattern: Sysname
  Circuit ID format-type: Undefined
  Remote ID format-type: ASCII
  Node identifier: aabbcc
Interface: Vlan-interface200
  Status: Enable
  Strategy: Replace
  Circuit ID Pattern: User Defined
  Remote ID Pattern: User Defined
  Circuit ID format-type: ASCII
  Remote ID format-type: ASCII
  User defined:
```

```
Circuit ID: vlan100
Remote ID: device001
```

表 6-9 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	Option82の状態です。 • **Enable**—DHCPリレーエージェントはOption82のサポートが有効です。 • **Disable**—DHCPリレーエージェントはOption82のサポートが無効です。
Strategy	要求メッセージの処理方法です。 Option82、**Drop**、**Keep**、**Replace**が含まれます。
Circuit ID Pattern	circuit IDサブオプションのパディングモードです。**Verbose**、**Normal**、**User Defined.**があります。
Remote ID Pattern	remote IDサブオプションのパディングモードです。**Sysname**、**Normal**、**User Defined.**があります。
Circuit ID format-type	circuit IDサブオプションのパディング形式です。**ASCII**、**hex**、**Undefined**があります。
Remote ID format-type	remote IDサブオプションのパディング形式です。**ASCII**、**hex**、**Undefined**があります。
Node identifier	アクセスノード識別子です。
User defined	ユーザ定義サブオプションの内容です。
Circuit ID	circuit IDサブオプションのユーザ定義の内容です。
Remote ID	remote IDサブオプションのユーザ定義の内容です。

6.3.11 display dhcp relay server-address

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの DHCP サーバのアドレスを表示します。指定されない場合、DHCP リレーエージェントで動作するすべてのインタフェースの DHCP サーバのアドレスを表示します。

説明

display dhcp relay server-address コマンドはインタフェースに設定された DHCP サーバのアドレスを表示します。

例

すべてのインタフェースの DHCP サーバのアドレスを表示します。

<Switch> display dhcp relay server-address

```
Interface name     Server IP address   Public/VRF name     Class name
Vlan2              2.2.2.2             Y/--                --
Vlan2              2.2.2.3             Y/--                abc
```

表 6-10 コマンド出力

フィールド	説明
Interface name	インタフェース名です。
Server IP address	DHCPサーバのIPアドレスです。
Public/VRF name	DHCPサーバのロケーションです。**dhcp relay server-address**コマンドの設定によって決まります。 ● **public**が指定されていない場合、このフィールドには **--/--** が表示されます。 ● **public**が指定されている場合、このフィールドには**Y/--** が表示されます。
Class name	DHCP要求を照合するためのDHCPユーザクラスの名前です。**dhcp relay server-address**コマンドで**class** *class-name*オプションが指定されていない場合、このフィールドにはハイフン(**--**)が表示されます。

関連コマンド

dhcp relay server-address

6.3.12 display dhcp relay statistics

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの DHCP パケットの統計情報を表示します。指定されない場合、DHCP リレーエージェントのすべての DHCP パケットの統計情報を表示します。

説明

display dhcp relay statistics コマンドは DHCP リレーエージェントの DHCP パケットの統計情報を表示します。

例

DHCP リレーエージェントのすべての DHCP パケットの統計情報を表示します。
<Switch> display dhcp relay statistics

```
DHCP packets dropped:                0
DHCP packets received from clients:    0
   DHCPDISCOVER:                     0
   DHCPREQUEST:                      0
   DHCPINFORM:                       0
   DHCPRELEASE:                      0
   DHCPDECLINE:                      0
   BOOTPREQUEST:                     0
DHCP packets received from servers:    0
   DHCPOFFER:                        0
   DHCPACK:                          0
   DHCPNAK:                          0
   BOOTPREPLY:                       0
DHCP packets relayed to servers:       0
   DHCPDISCOVER:                     0
   DHCPREQUEST:                      0
   DHCPINFORM:                       0
   DHCPRELEASE:                      0
```

```
  DHCPDECLINE:                    0
  BOOTPREQUEST:                   0
DHCP packets relayed to clients:      0
  DHCPOFFER:                      0
  DHCPACK:                        0
  DHCPNAK:                        0
  BOOTPREPLY:                     0
DHCP packets sent to servers:         0
  DHCPDISCOVER:                   0
  DHCPREQUEST:                    0
  DHCPINFORM:                     0
  DHCPRELEASE:                    0
  DHCPDECLINE:                    0
  BOOTPREQUEST:                   0
DHCP packets sent to clients:         0
  DHCPOFFER:                      0
  DHCPACK:                        0
  DHCPNAK:                        0
  BOOTPREPLY:                     0
```

関連コマンド

reset dhcp relay statistics

6.3.13 reset dhcp relay client-information

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースのリレーエントリを削除します。インタフェースを指定しないと、このコマンドはすべてのインタフェースのリレーエントリを削除します。

ip *ip-address*: 指定された IP アドレスのリレーエントリを削除します。

IP アドレスを指定しない場合、このコマンドはすべての IP アドレスのリレーエントリを削除します。

説明

reset dhcp relay client-information コマンドは DHCP リレーエージェントのリレーエントリを削除します。

パラメータを指定しない場合、DHCP リレーエージェントのすべてのリレーエントリを削除します。

例

DHCP リレーエージェントのすべてのリレーエントリを削除します。

<Switch> reset dhcp relay client-information

関連コマンド

display dhcp relay client-information

6.3.14 reset dhcp relay statistics

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの DHCP リレーエージェントの統計情報を削除します。指定されない場合、すべての DHCP リレーエージェントの統計情報を削除します。

説明

reset dhcp relay statistics コマンドは DHCP リレーエージェントの統計情報を削除します。

例

すべての DHCP リレーエージェントの統計情報を削除します。

<Switch> reset dhcp relay statistics

関連コマンド

display dhcp relay statistics

6.4 DHCPクライアント設定コマンド

6.4.1 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有効にします。

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有効にします。

<Switch> system-view

[Switch] undo dhcp client dad enable

6.4.2 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

6.4.3 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、このコマンドは 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。インタフェースを指定しない場合、このコマンドはすべてのインタフェースの DHCP クライアント情報を表示します。

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 クライアントの概要情報を表示します。

<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 6-11 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に関するパラメータです。
URL	ACSのURLです。
Username	ACSにログインするためのユーザ名です。
Password	ACSにログインするためのパスワードです。パスワードが設定されている場合、このフィールドには******と表示されます。パスワードが設定されていない場合、このフィールドは表示されません。
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

6.4.4 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。サブインタフェースが DHCP 経由で IP アドレスを取得し、プライマリインタフェースで **shutdown** コマンドが実行された場合に発生する可能性があります。サブインタフェースは、DHCP-RELEASE メッセージの送信に失敗します。

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

6.5 DHCPスヌーピング設定コマンド

🕮 **メモ**:

DHCP スヌーピングは、DHCP クライアントと DHCP サーバ間、または DHCP クライアントとリレーエージェント間で機能します。DHCP スヌーピングは、DHCP サーバと DHCP リレーエージェントの間では機能しません。

6.5.1 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 view

Layer 2 aggregate interface view

VLAN 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 の DHCP snooping エントリに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

6.5.2 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。

装置でグローバルに DHCP snooping を有効にすると、信頼できるポートは DHCP サーバからの応答を転送し、信頼できないポートは応答を破棄します。このメカニズムにより、DHCP クライアントは承認された DHCP サーバから IP アドレスを取得できます。

DHCP snooping がグローバルに無効である場合、装置上のすべてのポートは、DHCP サーバからの応答を転送できます。

例

DHCP snooping をグローバルに有効にします。

<Switch> system-view

[Switch] dhcp snooping enable

6.5.3 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*: 指定された VLAN から受信したパケットの circuit ID サブオプションをパッドします。VLAN を指定しない場合、装置はデフォルト VLAN から受信したパケットに circuit ID サブオプションを埋め込みます。

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。パディングの内容には、ノード識別子、インタフェース情報、および VLAN ID が含まれます。デフォルトのノード識別子は、アクセスノードの MAC アドレスです。デフォルトのインタフェース情報は、Ethernet タイプ(**eth** に固定)、シャーシ番号、スロット番号、サブスロット番号、およびインタフェース番号で構成されています。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: アクセスノードの識別子を指定します。

このパディングの内容はノード識別子、Ethernet タイプ（eth で固定）、インタフェース番号、VLAN ID が含まれます。ノード識別子は **mac**、**sysname**、**user-defined** によって変更します。

- **mac**: アクセスノードの MAC アドレスをノード識別子として使用します。
- **sysname**: ノード名として装置名を使用します。system-view で **sysname** コマンドを使用して装置名を設定できます。装置名のパディング形式は、指定されたパディング形式に関係なく、常に ASCII です。

🕮 **メモ**:

ノード識別子として **sysname** を指定する場合は、装置名を設定するときにスペースを含めないでください。そうしないと、DHCP snooping 装置は Option82 の追加または置換に失敗します。

- **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らず、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。

Circuit ID サブオプションは、インタフェース分割またはサブインタフェースに関する情報を伝達できません。インタフェース分割とサブインタフェースの詳細については、オペレーションマニュアルのセクション 3 *アクセス “Ethernet インタフェース”*を参照してください。

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。

string モード、normal モード、verbose モードのパディング形式は、コマンド設定によって異なります。表 6-12 に異なるモードのパディング形式を示します。

表 6-12 異なるモードのパディング形式

キーワード（モード）	パディング形式が指定されていない場合	パディング形式が ASCII	パディング形式が hex
string *circuit-id*	パディング形式を指定できません。常にASCIIになります。	ー	ー
normal	hexです。	ASCIIです。	hexです。
verbose	VLAN IDはhexです。 ノード識別子、Ethernetタイプ、インタフェース番号はASCIIです。	ASCIIです。	ノード識別子とEthernetタイプはASCIIです。 インタフェース番号とVLAN IDはhexです。

例

circuit ID サブオプションの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**

6.5.4 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 Option82 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 Option82 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、Option82 が含まれない DHCP 要求に Option82 を追加します。Option82 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。DHCP 要求に Option82 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 Option82 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**

6.5.5 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*: 指定された VLAN から受信したパケットの Remote ID サブオプションを追加します。 VLAN を指定しないと、装置はデフォルト VLAN から受信したパケットの Remote ID サブオプションを埋め込みます。

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: リモート ID サブオプションの内容として装置名を指定します。装置名は 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: リモート 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**

6.5.6 dhcp snooping information strategy

Syntax

dhcp snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

デフォルト

replace

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

drop: Option82 メッセージが含まれる DHCP メッセージを廃棄します。

keep: Option82 を含むメッセージをそのまま転送するよう指定します。

replace: 元の Option82 のメッセージを設定された Option82 のメッセージに置き換えします。

説明

dhcp snooping information strategy コマンドは Option82 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 Option82 が含まれるときのみ適用します。

Option82 のサポートを有効にした場合、DHCP リレーエージェントが DHCP サーバに要求を転送する前、DHCP リレーエージェントは常に Option82 が含まれない DHCP 要求に Option82 を追加します。

処理方法が **append** または **replace** である場合、Option82 にパディングモードとパディングフォーマットを設定します。操作方法が **keep** または **drop** の場合、Option82 に対してパディングモードやパディングフォーマットを設定する必要はありません。

例

Option82 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**

6.5.7 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 view

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

6.5.8 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。

vlan *vlan-id*: IP アドレスが存在する VLAN ID を指定します。

説明

display dhcp snooping binding コマンドは DHCP snooping エントリを表示します。

パラメータを指定しない場合、すべての DHCP snooping エントリを表示します。

例

すべての DHCP snooping エントリに関する概要情報を表示します。

<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
```

#すべての DHCP snooping エントリに関する詳細情報を表示します。

<Switch> display dhcp snooping binding verbose

```
IP address: 1.1.1.7
MAC address: 0000-0101-0107
```

```
Lease: 16907553 seconds
VLAN: 2
SVLAN: 3
Interface: GigabitEthernet1/0/1
Parameter request list: 03 06 21

IP address: 1.1.1.104
MAC address: 0000-0101-010b
Lease: 16907537 seconds
VLAN: 2
SVLAN: 3
Interface: GigabitEthernet1/0/3
Parameter request list: 37 0B 01 0F 03 06 2C 2E 2F 1F 21 F9 2B
```

表 6-13 コマンド出力

フィールド	説明
DHCP snooping entries found	DHCP snoopingエントリの数です。
IP address	DHCPクライアントに割り当てられたIPアドレスです。
MAC address	DHCPクライアントのMACアドレスです。
Lease	残りリース期間です。単位は秒です。
VLAN	DHCP snoopingとQinQの両方が有効、あるいはDHCPパケットに2つのVLANタグが含まれる場合、このフィールドは外部VLANタグを示します。そうでない場合、DHCPクライアントが存在するポートに接続しているVLANを示します。
SVLAN	DHCP snoopingとQinQの両方が有効、あるいはDHCPパケットに2つのVLANタグが含まれる場合、このフィールドは内部VLANタグを示します。そうでない場合、**N/A**と表示されます。
Interface	DHCPクライアントに接続されたポートです。
Parameter request list	DHCPクライアントが要求するパラメータ (16進数表記)。

関連コマンド

- **dhcp snooping enable**
- **reset dhcp snooping binding**

6.5.9 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 Option82 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 Option82 の設定を表示します。

例

すべてのインタフェースの Option82 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
  VLAN 10:
    Circuit ID: abcd
    Remote ID: company
```

表 6-14 コマンド出力

フィールド	説明
Interface	インタフェース名です。

フィールド	説明
Status	Option82の状態です。EnableあるいはDisableです。
Strategy	DHCP要求の処理方法です。 Option82、**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	Option82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。
Node identifier	アクセスノード識別子です。
User defined	ユーザ定義サブオプションの内容です。
Format	Option82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。
VLAN	指定したVLANで受信したDHCPパケットのcircuit IDサブオプションとremote IDサブオプションを挿入します。

6.5.10 display dhcp snooping packet statistics

Syntax

display dhcp snooping packet statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックユニットのメンバ装置の DHCP パケット統計情報を表示します。

説明

display dhcp snooping packet statistics コマンドは DHCP snooping の DHCP パケットの統計情報を表示します。

パラメータを指定しない場合、コマンドが実行された装置の 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

6.5.11 display dhcp snooping trust

Syntax

display dhcp snooping trust

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display dhcp snooping trust コマンドはトラステッドポートの情報を表示します。

例

トラステッドポートの情報を表示します。

<Switch> display dhcp snooping trust

```
DHCP snooping is enabled.
Interface                                Trusted        VLAN
```

```
=========================                    ============    =======
GigabitEthernet1/0/1                    Trusted
GigabitEthernet1/0/2                    -               100
GigabitEthernet1/0/3                    -               100, 200
```

表 6-15 コマンド出力

フィールド	説明
Interface	インタフェース名です。
Trusted	system viewで設定されたDHCP snoopingトラステッドポートの場合、このフィールドは**Trusted**と表示されます。 VLAN viewで設定されたトラステッドポートの場合、このフィールドにはハイフン(-)が表示されます。
VLAN	ポートがTrustedとして設定されているVLANです。 信頼できるポートがDHCP snoopingをグローバルに有効にした後に設定される場合、このフィールドは空です。

関連コマンド

dhcp snooping trust

6.5.12 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。VLAN を指定しない場合、このコマンドはデフォルト 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

6.5.13 reset dhcp snooping packet statistics

Syntax

reset dhcp snooping packet statistics [**slot** *slot-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置をそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドはマスター装置の DHCP パケット統計情報を削除します。

説明

reset dhcp snooping packet statistics コマンドは DHCP snooping の DHCP パケットの統計情報を削除します。

パラメータを指定しない場合、実行される IRF スタックメンバ装置の DHCP パケットの統計情報を削除します。

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

6.6 BOOTPクライアント設定コマンド

6.6.1 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。インタフェースを指定しない場合、このコマンドはすべてのインタフェースの 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。

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 BOOTP クライアント情報を表示します。

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 6-16 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応答をドロップします。
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

6.6.2 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にインタフェースは BOOTP を使用しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ip address bootp-alloc コマンドは IP アドレスを取得するために BOOTP を使用するインタフェースを設定します。

undo ip address bootp-alloc コマンドはインタフェースで BOOTP を使用することを中止します。

例

IP アドレスを取得するために BOOTP を使用する VLAN インタフェース 10 を設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ip address bootp-alloc

関連コマンド

display bootp client

目次

このセクションのページは **4-x-x** です。

7 章 DNS.....7-1
7.1 DNS 設定コマンド.....7-1
7.1.1 display dns domain.....7-1
7.1.2 display dns host.....7-2
7.1.3 display dns server.....7-3
7.1.4 dns domain.....7-5
7.1.5 dns dscp.....7-6
7.1.6 dns proxy enable.....7-6
7.1.7 dns server.....7-7
7.1.8 ip host.....7-8
7.1.9 reset dns host.....7-9

7章 DNS

7.1 DNS設定コマンド

7.1.1 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され、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用にスタティックに作成され、ダイナミックに取得されたドメイン名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 7-1 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

7.1.2 display dns host

Syntax

display dns host [**ip**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip: タイプ A のクエリを指定します。タイプ A のクエリは IPv4 アドレスにドメイン名サフィックスをマッピングします。

説明

display dns host コマンドはドメイン名から IP アドレスのマッピングを表示します。

ip キーワードを指定しない場合、このコマンドはすべての検索タイプのドメイン名から IP アドレスへ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 7-2 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の場合、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**

7.1.3 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 7-3 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

7.1.4 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。デフォルト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作成されます。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。ドメイン名サフィックスには最大 253 文字を含めることができ、各区切り文字列は最大 63 文字です。

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。

ドメイン名解決のために、リゾルバは自動的にサフィックスリストを使用して、ユーザが入力した不完全な名前の欠けている部分を提供します。

ドメイン名サフィックスは、IPv4 DNS に適用されます。

例

パブリックネットワークのドメイン名サフィックス **com** を設定します。

<Switch> system-view

[Switch] dns domain com

関連コマンド

display dns domain

7.1.5 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 を設定します。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

7.1.6 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、IPv4 DNS に適用されます。

例

DNS Proxy を有効にします。

<Switch> system-view

[Switch] dns proxy enable

7.1.7 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。

システムはパブリックネットワークに対して最大 6 台の DNS サーバ IPv4 アドレスを許可します。パブリックネットワークの DNS サーバの IPv4 アドレスを指定できます。

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 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

7.1.8 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から 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。

システムは、パブリックネットワークに対して最大 1024 のホスト名から IPv4 アドレスへのマッピングを許可します。パブリックネットワークのホスト名から IPv4 アドレスへのマッピングを設定できます。

パブリックネットワークにおいて、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。

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**、あるいは**–v** をホスト名として使用しないでください。**ping** コマンドのパラメータの詳細は、コマンドマニュアルのセクション 10 *システム管理 "システムの保守とデバッグ"* を参照してください。

例

パブリックネットワークの IPv4 アドレス 10.110.0.1 をホスト名 **aaa** にマッピングします。

<Switch> system-view

[Switch] ip host aaa 10.110.0.1

関連コマンド

display dns host

7.1.9 reset dns host

Syntax

reset dns host [**ip**]

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。

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。

ip キーワードを指定しない場合、**reset dns host** コマンドはすべてのクエリタイプのダイナミック DNS キャッシュ情報を削除します。

例

パブリックネットワークのすべてのクエリタイプのダイナミック DNS キャッシュ情報を削除します。

<Switch> reset dns host

関連コマンド

display dns host

目次

このセクションのページは **4-x-x** です。

8 章 IP フォワーディングの基本 8-1
8.1 IP フォワーディングの基本設定コマンド.....8-1
8.1.1 display fib 8-1

8章 IP フォワーディングの基本

8.1 IPフォワーディングの基本設定コマンド

8.1.1 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。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  USGR     M-GE0/0/0               Null
127.0.0.0/8        127.0.0.1      U        InLoop0                 Null
127.0.0.0/32       127.0.0.1      UH       InLoop0                 Null
127.0.0.1/32       127.0.0.1      UH       InLoop0                 Null
```

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 8-1 コマンド出力

フィールド	説明
Destination count	宛先アドレスの総数です。
FIB entry count	FIBエントリの総数です。
Destination/Mask	宛先アドレス/マスク長です。
Nexthop	ネクストホップアドレスです。
Flag	ルートフラグです。 • **U**—使用可能なルートです。 • **G**—ゲートウェイルートです。 • **H**—ホストルートです。 • **B**—ブラックホールルートです。 • **D**—ダイナミックルートです。 • **S**—スタティックルートです。 • **R**—中継ルートです。 • **F**—fastルート変更です。
OutInterface/Token	出力インタフェース/LSPインデックス番号です。
Label	内部ラベルです。

目次

このセクションのページは **4-x-x** です。

9 章 IP パフォーマンスの最適化 9-1
9.1 IP パフォーマンスの最適化設定コマンド 9-1
9.1.1 display icmp statistics 9-1
9.1.2 display ip statistics 9-2
9.1.3 display rawip 9-4
9.1.4 display rawip verbose 9-5
9.1.5 display tcp 9-9
9.1.6 display tcp statistics 9-10
9.1.7 display tcp verbose 9-13
9.1.8 display udp 9-18
9.1.9 display udp statistics 9-19
9.1.10 display udp verbose 9-20
9.1.11 ip forward-broadcast 9-23
9.1.12 ip icmp error-interval 9-24
9.1.13 ip mtu 9-25
9.1.14 ip redirects enable 9-26
9.1.15 ip ttl-expires enable 9-27
9.1.16 ip unreachables enable 9-28
9.1.17 reset ip statistics 9-29
9.1.18 reset tcp statistics 9-30
9.1.19 reset udp statistics 9-30
9.1.20 tcp path-mtu-discovery 9-31
9.1.21 tcp timer fin-timeout 9-32
9.1.22 tcp timer syn-timeout 9-33
9.1.23 tcp window 9-33

9章 IP パフォーマンスの最適化

9.1 IPパフォーマンスの最適化設定コマンド

9.1.1 display icmp statistics

Syntax

display icmp statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置に対して ICMP 統計情報を表示します。

説明

display icmp statistics コマンドは ICMP パケットの送受信に関する統計情報を表示します。

例

ICMP の統計情報を表示します。

<Switch> display icmp statistics

```
  Input: bad formats   0               bad checksum          0
         echo         175             destination unreachable 0
         source quench 0               redirects             0
         echo replies  201             parameter problem      0
         timestamp     0               information requests    0
         mask requests 0               mask replies           0
         time exceeded 0               invalid type           0
         router advert 0               router solicit         0
         broadcast/multicast echo requests ignored          0
         broadcast/multicast timestamp requests ignored      0
 Output: echo         0               destination unreachable 0
         source quench 0               redirects             0
         echo replies  175             parameter problem      0
```

```
timestamp     0              information replies     0
mask requests 0               mask replies           0
time exceeded 0               bad address            0
packet error  1442            router advert          3
```

9.1.2 display ip statistics

Syntax

display ip statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IP パケット統計情報を表示します。

説明

display ip statistics コマンドは IP パケットの統計情報を表示します。

IP パケットの統計情報はパケットの送受信、フラグメント、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 9-1 コマンド出力

フィールド		説明
Input	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	forwarding	転送されて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	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	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**

9.1.3 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の RawIP 接続に関する概要情報を表示します。

説明

display rawip コマンドは RawIP 接続の概要情報を表示します。

RawIP 接続の概要情報はローカルアドレス、ピアのアドレス、プロトコル、PCB が含まれます。

例

RawIP 接続の概要情報を表示します。

<Switch> display rawip

```
Local Addr      Foreign Addr    Protocol   Slot   PCB
0.0.0.0         0.0.0.0         1          1      0x0000000000000009
0.0.0.0         0.0.0.0         1          1      0x0000000000000008
```

表 9-2 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。

9.1.4 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*: PCB のインデックスを指定します。指定した PCB の詳細な RawIP 接続情報を表示します。インデックスは、1～ffffffffffffff の範囲の 16 進文字列です。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合､このコマンドはすべてのメンバ装置の RawIP 接続に関する詳細情報を表示します。

説明

display rawip verbose コマンドは RawIP 接続の詳細情報を表示します。

RawIP 接続の詳細情報はソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、RawIP 接続の送信元 IP アドレス、RawIP 接続の宛先 IP アドレスが含まれます。

例

RawIP 接続の詳細情報を表示します。

<Switch> display rawip verbose

```
Total RawIP socket number: 1

 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 9-3 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アドレスおよび宛先IPアドレスを含む接続情報です。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。
Options	ソケットのオプションです。
Error	エラーコードです。
Receiving buffer (cc/hiwat/lowat/drop/state)	以下の順番で受信バッファ情報を表示します。 • **cc**—使用されているバッファ空間です。 • **hiwat**—最大バッファ空間です。 • **lowat**—最小バッファ空間です。 • **drop**—ドロップされたパケットの数です。 • **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。

フィールド	説明
Inpcb flags	インタネットPCBのフラグです。 ● **INP_RECVOPTS**—IPオプションを受信します。 ● **INP_RECVRETOPTS**—応答したIPオプションを受信します。 ● **INP_RECVDSTADDR**—宛先IPアドレスを受信します。 ● **INP_HDRINCL**—全体のIPヘッダを提供します。 ● **INP_REUSEADDR**—IPアドレスを再利用します。 ● **INP_REUSEPORT**—ポート番号を再利用します。 ● **INP_ANONPORT**—ポート番号が指定されていません。 ● **INP_RECVIF**—パケットの入力インタフェースを記録します。 ● **INP_RECVTTL**—パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 ● **INP_DONTFRAG**—DF(**Don't Fragment**)フラグを設定します。 ● **INP_ROUTER_ALERT**—ルータ警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 ● **INP_PROTOCOL_PACKET**—プロトコルパケットを識別します。 ● **INP_RCVVLANID**—パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 ● **INP_RCVMACADDR**—フレームのMACアドレスを受信します。 ● **INP_SNDBYLSPV**—MPLSを経由して送信します。 ● **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: ● **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_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リングします。 ● **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	パケットの送信元のVRFです。
Receive VRF	パケットの受信元のVRFです。

9.1.5 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の TCP 接続に関する簡単な情報を表示します。

説明

display tcp コマンドは TCP 接続の概要情報を表示します。

TCP 接続の概要情報はローカル IP アドレス、ローカルポート番号、ピアの IP アドレス、ピアのポート番号、TCP 接続情報が含まれます。

例

TCP 接続の概要情報を表示します。

<Switch> display tcp

```
*: TCP connection with authentication
 Local Addr:port      Foreign Addr:port    State      Slot  PCB
*0.0.0.0:21          0.0.0.0:0           LISTEN     1     0x000000000000c387
 192.168.20.200:23  192.168.20.14:1284    ESTABLISHED 1   0x0000000000000009
 192.168.20.200:23    192.168.20.14:1283   ESTABLISHED 1     0x000000000000
```

表 9-4 コマンド出力

フィールド	説明
*	TCP接続がMD5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。

9.1.6 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置に対して TCP トラフィック統計情報を表示します。

説明

display tcp statistics コマンドは TCP トラフィックの統計情報を表示します。

TCP トラフィックの統計情報は受信 TCP パケット、送信 TCP パケット、Syncache/syncookie が含まれます。

例

TCP トラフィックの統計情報を表示します。

<Switch> display tcp statistics

```
Received packets:
    Total: 4150
    packets in sequence: 1366 (134675 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0
    packets dropped for lack of memory: 0
    packets dropped due to PAWS: 0
    duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0
    ACK packets: 3531 (795048 bytes)
    duplicate ACK packets: 33, ACK packets for unsent data: 0

Sent packets:
    Total: 4058
    urgent packets: 0
    control packets: 50
    window probe packets: 3, window update packets: 11
    data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 150 (52 delayed)
    unnecessary packet retransmissions: 0

Syncache/syncookie related statistics:
    entries added to syncache: 12
    syncache entries retransmitted: 0
    duplicate SYN packets: 0
```

```
    reply failures: 0
    successfully build new socket: 12
    bucket overflows: 0
    zone failures: 0
    syncache entries removed due to RST: 0
    syncache entries removed due to timed out: 0
    ACK checked by syncache or syncookie failures: 0
    syncache entries aborted: 0
    syncache entries removed due to bad ACK: 0
    syncache entries removed due to ICMP unreachable: 0
    SYN cookies sent: 0
    SYN cookies received: 0

SACK related statistics:
    SACK recoveries: 1
    SACK retransmitted segments: 0 (0 bytes)
    SACK blocks (options) received: 0
    SACK blocks (options) sent: 0
    SACK scoreboard overflows: 0

Other statistics:
    retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
    persist timeout: 0
    keepalive timeout: 21, keepalive probe: 0
    keepalive timeout, so connections disconnected: 0
    fin_wait_2 timeout, so connections disconnected: 0
    initiated connections: 29, accepted connections: 12, established connections:
23
    closed connections: 50051 (dropped: 0, initiated dropped: 0)
    bad connection attempt: 0
    ignored RSTs in the window: 0
    listen queue overflows: 0
    RTT updates: 3518(attempt segment: 3537)
    correct ACK header predictions: 0
    correct data packet header predictions: 568
    resends due to MTU discovery: 0
    packets dropped due to MD5 authentication failure: 0
    packets that passed MD5 authentication: 0
    sent Keychain-encrypted packets: 0
    packets that passed Keychain authentication: 0
    packets dropped due to Keychain authentication failure: 0
```

関連コマンド

reset tcp statistics

9.1.7 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 の詳細な TCP 接続情報を表示します。インデックスは、1 ～ffffffffffffff の範囲の 16 進文字列です。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。

説明

display tcp verbose コマンドは TCP 接続の詳細情報を表示します。

TCP 接続の詳細情報はソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号、接続状態が含まれます。

例

TCP 接続の詳細情報を表示します。

<Switch> display tcp verbose

```
TCP inpcb number: 1(tcpcb number: 1)

 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 9-5 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。
tcpcb number	TCP PCBの数です。TCP接続の状態が**TIME_WAIT**の場合、このフィールドは表示されません。
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**—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_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破棄しません。 ● **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オプションなし。 ● **TF_NOPUSH**—フルサイズのセグメントがTCPバッファにバッファされるまで、TCPによるTCPデータの送信を強制的に遅延させます。 ● **TF_BINDFOREIGNADDR**—ピアのIPアドレスをバインドします。 ● **TF_NSR**—TCP NSRを有効にします。 ● **TF_REQ_SCALE**—TCPウィンドウスケールオプションを使用可能にします。 ● **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選択的受信確認オプションを使用可能にします。 ● **TF_ENHANCED_AUTH**—拡張認証オプションを使用可能にします。
NSR state	TCP接続の状態です。 括弧の間は、接続の役割です。 ● **M**—メイン接続です。 ● **S**—スタンバイ接続です。
Send VRF	パケットの送信元のVRFです。
Receive VRF	パケットの受信元のVRFです。

9.1.8 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の UDP 接続に関する概要情報を表示します。

説明

display udp コマンドは UDP 接続の概要情報を表示します。

UDP 接続の概要情報はローカル IP アドレス、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 PCB
0.0.0.0:69            0.0.0.0:0             1    0x0000000000000003
```

表 9-6 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。

9.1.9 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置に対して UDP トラフィック統計情報を表示します。

説明

display udp statistics コマンドは UDP トラフィックの統計情報を表示します。

UDP トラフィックの統計情報は受信 UDP パケット、送信 UDP パケットが含まれます。

例

UDP トラフィックの統計情報を表示します。

<Switch> display udp statistics

```
Received packets:
    Total: 240
    checksum error: 0, no checksum: 0
    shorter than header: 0, data length larger than packet: 0
    no socket on port(unicast): 0
    no socket on port(broadcast/multicast): 240
    not delivered, input socket full: 0
Sent packets:
    Total: 0
```

関連コマンド

reset udp statistics

9.1.10 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 の詳細な UDP 接続情報を表示します。インデックスは、1～ffffffffffff の範囲の 16 進文字列です。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の UDP 接続に関する詳細情報を表示します。

説明

display udp verbose コマンドは UDP 接続の詳細情報を表示します。

UDP 接続の詳細情報は UDP 接続のソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号が含まれます。

例

UDP 接続の詳細情報を表示します。

<Switch> display udp verbose

```
Total UDP socket number: 1


 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 9-7 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。
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**—ドロップされたパケットの数です。 • **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_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	パケットの送信元のVRFです。
Receive VRF	パケットの受信元のVRFです。

9.1.11 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特定のネットワークにだけ送ら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 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
```

9.1.12 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 ミリ秒です。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 エラーメッセージのバケットサイズとトークンがバケットに到着する間隔を設定します。

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

9.1.13 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 128～9216 バイトです。

説明

ip mtu コマンドはインタフェースを介して送信される 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。

インタフェースが **mtu** と **ip mtu** の両方のコマンドをサポートしている場合、装置は **ip mtu** コマンドで設定された MTU に基づいてパケットをフラグメント化します。

例

VLAN インタフェース 100 の MTU を 1280 バイトに設定します。

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip mtu 1280
```

9.1.14 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、デフォルトゲートウェイ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

9.1.15 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。

- 次の条件が満たされると、装置は送信元に ICMP TTL exceeded in transit メッセージを送信します。
  - □ 受信したパケットの宛先は装置ではありません。
  - □ パケットの TTL フィールドは 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

9.1.16 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。

- 次の条件が満たされると、装置は ICMP ネットワーク到達不能メッセージを送信元に送信します。

- □ 受信したパケットはどのルートとも一致しません。
- □ ルーティングテーブルにデフォルトルートが存在しません。

- 次の条件が満たされると、装置は ICMP プロトコル到達不能メッセージを送信元に送信します。
  - □ 受信したパケットの宛先は装置です。
  - □ パケットのトランスポートレイヤプロトコルが装置でサポートされていません。
- 次の条件が満たされると、装置は ICMP ポート到達不能メッセージを送信元に送信します。
  - □ 受信した UDP パケットの宛先は装置です。
  - □ パケットのポート番号が実行中のプロセスと一致しません。
- 次の条件が満たされた場合、装置は ICMP 送信元経路失敗メッセージを送信元に送信します。
  - □ 送信元は、Strict Source Routing を使用してパケットを送信します。
  - □ 中継装置は、ソースによって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す。
- 次の条件が満たされると、装置はソースに必要な ICMP フラグメンテーションと DF set メッセージを送信します。
  - □ 送信側インタフェースの MTU はパケットよりも小さいです。
  - □ パケットには Don't Fragment が設定されています。

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

9.1.17 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IP トラフィック統計情報を削除します。

説明

reset ip statistics コマンドは IP トラフィックの統計情報を削除します。

新しく一定期間内の IP トラフィックの統計情報を取得する場合、このコマンドを使用し、最初に既存の IP トラフィックの統計情報を削除します。

例

IP トラフィックの統計情報を削除します。

<Switch> reset ip statistics

関連コマンド

- **display ip interface**
- **display ip statistics**

9.1.18 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

9.1.19 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

9.1.20 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

9.1.21 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

9.1.22 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

9.1.23 tcp window

Syntax

tcp window *window-size*

undo tcp window

デフォルト

63KB

View

System view

定義済みユーザロール

network-admin

パラメータ

window-size: TCP 受信/送信バッファのサイズを指定します。設定範囲は 1～64KB です。

説明

tcp window コマンドは TCP 受信/送信バッファのサイズを設定します。

undo tcp window コマンドはデフォルトに戻します。

例

TCP 受信/送信バッファのサイズを 3KB に設定します。

<Switch> system-view

[Switch] tcp window 3

目次

このセクションのページは **4-x-x** です。

10 章 UDP ヘルパー.....10-1
10.1 UDP ヘルパー設定コマンド.....10-1
10.1.1 display udp-helper interface.....10-1
10.1.2 reset udp-helper statistics.....10-2
10.1.3 udp-helper enable.....10-3
10.1.4 udp-helper port.....10-3
10.1.5 udp-helper server.....10-5

10章 UDP ヘルパー

10.1 UDPヘルパー設定コマンド

10.1.1 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への変換についての情報を表示します。

このコマンドは宛先サーバと UDP ヘルパーによって UDP ブロードキャストパケットから変換されたユニキャストパケットの総数の情報を示します。

例

VLAN インタフェース 100 で UDP ヘルパーによってブロードキャストからユニキャストへの変換について情報を表示します。

<Switch> display udp-helper interface vlan-interface 100

```
Interface            Server VPN instance         Server address Packets sent
Vlan-interface100        N/A                      192.1.1.2      0
Vlan-interface100        N/A                      192.1.1.2      0
```

表 10-1 コマンド出力

フィールド	説明
Interface	インタフェース名です。

フィールド	説明
Server VPN instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 宛先サーバが所属するVPNインスタンスです。
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**

10.1.2 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 ヘルパーによるブロードキャストからユニキャストへの変換に関する統計を削除します。

<Switch> reset udp-helper statistics

関連コマンド

display udp-helper interface

10.1.3 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。

udp-helper port コマンドをインタフェースで有効にするには、次の条件が満たされていることを確認します。

- **UDP** ヘルパーは有効です。
- **udp-helper port** コマンドを使用して UDP ポート番号を指定します。
- **UDP** ヘルパーのパケット変換はインタフェースに設定されています。

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**

10.1.4 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 ヘルパーに UDP ポート 100 を指定します。

<Switch> system-view

[Switch] udp-helper port 100

10.1.5 udp-helper server

Syntax

udp-helper server *ip-address* [**global**]

undo udp-helper server [*ip-address* [**global**]]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 宛先サーバの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

global: 変換されたユニキャストパケットを公衆ネットワークのサーバに転送します。

説明

udp-helper server コマンドはブロードキャストからユニキャストに変換するために UDP ヘルパーの宛先サーバを指定します。

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 ヘルパーポートと一致する場合、UDP ヘルパーはブロードキャストを指定されたサーバに転送します。

インタフェースでブロードキャストパケットに変換されるように、UDP ヘルパーに最大 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 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 のブロードキャストをユニキャストに変換するための UDP ヘルパー用の送信先サーバ 192.1.1.2 を指定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] udp-helper server 192.1.1.2

UDP ヘルパー用にパブリックネットワーク上の宛先サーバ 192.1.1.2 を指定して、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します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] udp-helper server 192.1.1.2 global

関連コマンド

display udp-helper interface

目次

このセクションのページは **4-x-x** です。

11 章 IPv6 の基本.....11-1
11.1 IPv6 の基本設定コマンド.....11-1
11.1.1 display ipv6 fib.....11-1
11.1.2 display ipv6 interface.....11-2
11.1.3 display ipv6 neighbors.....11-8
11.1.4 display ipv6 neighbors count.....11-11
11.1.5 display ipv6 pathmtu.....11-12
11.1.6 display ipv6 rawip.....11-13
11.1.7 display ipv6 rawip verbose.....11-14
11.1.8 display ipv6 statistics.....11-18
11.1.9 display ipv6 tcp.....11-20
11.1.10 display ipv6 tcp verbose.....11-21
11.1.11 display ipv6 udp.....11-27
11.1.12 display ipv6 udp verbose.....11-28
11.1.13 ipv6 address.....11-32
11.1.14 ipv6 address anycast.....11-33
11.1.15 ipv6 address auto.....11-34
11.1.16 ipv6 address auto link-local.....11-35
11.1.17 ipv6 address eui-64.....11-37
11.1.18 ipv6 address link-local.....11-38
11.1.19 ipv6 hop-limit.....11-39
11.1.20 ipv6 hoplimit-expires enable.....11-40
11.1.21 ipv6 icmpv6 error-interval.....11-40
11.1.22 ipv6 icmpv6 multicast-echo-reply enable.....11-42
11.1.23 ipv6 mtu.....11-42
11.1.24 ipv6 nd autoconfig managed-address-flag.....11-43
11.1.25 ipv6 nd autoconfig other-flag.....11-44
11.1.26 ipv6 nd dad attempts.....11-45
11.1.27 ipv6 nd ns retrans-timer.....11-46
11.1.28 ipv6 nd nud reachable-time.....11-47
11.1.29 ipv6 nd ra halt.....11-48
11.1.30 ipv6 nd ra interval.....11-49
11.1.31 ipv6 nd ra prefix.....11-50
11.1.32 ipv6 nd ra router-lifetime.....11-51
11.1.33 ipv6 neighbor.....11-52
11.1.34 ipv6 neighbor stale-aging.....11-54

11.1.35 ipv6 neighbors max-learning-num 11-55
11.1.36 ipv6 pathmtu.....11-56
11.1.37 ipv6 pathmtu age 11-57
11.1.38 ipv6 unreachables enable 11-58
11.1.39 reset ipv6 neighbors.....11-59
11.1.40 reset ipv6 pathmtu 11-60
11.1.41 reset ipv6 statistics.....11-60

11章 IPv6 の基本

11.1 IPv6の基本設定コマンド

11.1.1 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: 宛先 IPv6 アドレスの IPv6 FIB エントリを表示します。IPv6 アドレスを指定しない場合、このコマンドはすべての 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。プレフィックスの長さを指定しない場合、このコマンドは IPv6 アドレスに一致する IPv6 FIB エントリ最長を表示します。

説明

display ipv6 fib コマンドは IPv6 FIB エントリを表示します。

例

パブリックネットワークのすべての IPv6 FIB エントリを表示します。

<Switch> display ipv6 fib

```
Destination count: 1 FIB entry count: 1

Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay    F:FRR

Destination: ::1                                  Prefix length: 128
Nexthop    : ::1                                   Flags: UH
Time stamp : 0x1                                   Label: Null
```

```
Interface  : InLoop0                                Token: Invalid
```

表 11-1 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	ネクストホップアドレスです。
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	このフィールドは、QX-S5300Gシリーズではサポートしていません。 内部MPLSラベルです。パブリックネットワークのIPv6 FIBエントリの場合、このフィールドには**Null**が表示されます。
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。

11.1.2 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: インタフェースタイプです。

interface-number: インタフェース番号です。

brief: 物理ステータス、リンクレイヤプロトコル、IPv6 アドレスなど、IPv6 インタフェース概要情報を表示します。キーワードを指定しない場合、このコマンドは IPv6 設定と操作情報、および IPv6 パケット統計情報を含む詳細な IPv6 インタフェース情報を表示します。

説明

display ipv6 interface コマンドは IPv6 インタフェース情報を表示します。

インタフェースを指定しない場合、すべてのインタフェースの IPv6 情報を表示します。

interface-type のみを指定した場合、指定したタイプのインタフェースの IPv6 情報を表示します。

interface-type と *interface-number* の両方を指定した場合、指定したインタフェースの IPv6 情報を表示します。

例

VLAN インタフェース 2 の IPv6 情報を表示します。

<Switch> display ipv6 interface vlan-interface 2

```
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322 [TENTATIVE]
  Global unicast address(es):
    10::1234:56FF:FE65:4322, subnet is 10::/64 [TENTATIVE] [AUTOCFG]
      [valid lifetime 4641s/preferred lifetime 4637s]
    20::1234:56ff:fe65:4322, subnet is 20::/64 [TENTATIVE] [EUI-64]
    30::1, subnet is 30::/64 [TENTATIVE] [ANYCAST]
    40::2, subnet is 40::/64 [TENTATIVE] [DHCP]
    50::3, subnet is 50::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF65:4322
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

```
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                0
  InTooShorts:               0
  InTruncatedPkts:           0
  InHopLimitExceeds:         0
  InBadHeaders:              0
  InBadOptions:              0
  ReasmReqds:                0
  ReasmOKs:                  0
  InFragDrops:               0
  InFragTimeouts:            0
  OutFragFails:              0
  InUnknownProtos:           0
  InDelivers:                0
  OutRequests:               0
  OutForwDatagrams:          0
  InNoRoutes:                0
  InTooBigErrors:            0
  OutFragOKs:                0
  OutFragCreates:            0
  InMcastPkts:               0
  InMcastNotMembers:         0
  OutMcastPkts:              0
  InAddrErrors:              0
  InDiscards:                0
  OutDiscards:               0
```

表 11-2 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**–VLANインタフェースはupですが、VLAN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**–VLAN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。

フィールド	説明
Line protocol current state	インタフェースのリンクレイヤ状態です。 ● **DOWN**–VLAN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**– VLANインタフェースのリンクレイヤ状態がupです。
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一意ではありません。 ● **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。

フィールド	説明
MTU	インタフェースのMTU（Maximum transmission unit）です
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	パケットで指定されたパケット長よりも短いパケット長を受信したIPv6パケットです。
InHopLimitExceeds	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。

フィールド	説明
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。
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 11-3 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。

フィールド	説明
Interface	インタフェースの名前です。
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。

11.1.3 display ipv6 neighbors

Syntax

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-address: 情報が表示されているネイバの IPv6 アドレスを指定します。

all: パブリックネットワークとすべてのプライベートネットワークでダイナミックおよびスタティックに設定されたネイバを含むすべてのネイバの情報を表示します。

dynamic: ダイナミックに取得したすべてのネイバの情報を表示します。

static: スタティックに設定されたすべてのネイバの情報を表示します。

slot *slot-number*: メンバ ID で IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IPv6 ネイバ情報を表示します。

interface *interface-type interface-number*:インタフェースのタイプと番号を指定します。

vlan *vlan-id*: 指定した VLAN 内のネイバに関する情報を表示します。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。

IPv6 ネイバ情報を削除する場合、**reset ipv6 neighbors** コマンドを使用します。

例

すべての IPv6 ネイバ情報を表示します。

<Switch> display ipv6 neighbors all

```
Type: S-Static    D-Dynamic    O-Openflow    R-Rule    I-Invalid
IPv6 address       Link layer    VID      Interface          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
```

すべての IPv6 ネイバの詳細情報を表示します。

<Switch> display ipv6 neighbors all verbose

```
Type: S-Static    D-Dynamic    O-Openflow    R-Rule    I-Invalid
IPv6 Address: 1::2
Link Layer  : 6864-6839-0202     VID : 1    Interface: GE1/0/1
State       : STALE              Type: D    Aging     : 290
Vpn-instance: [No Vrf]
Nickname    : 0x0
IPv6 Address: FE80::6A64:68FF:FE39:202
Link Layer  : 6864-6839-0202     VID : 1    Interface: GE1/0/1
State       : STALE              Type: D    Aging     : 280
Vpn-instance: [No Vrf]
Nickname    : 0x0
```

表 11-4 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。

フィールド	説明
Link Layer	ネイバのリンクレイヤアドレス（MACアドレス）です。
VID	ネイバに接続されたインタフェースが属するVLANまたは仮想スイッチインスタンス（VSI）です。VLAN IDまたはVSIインデックスが無効な場合、このフィールドには**N/A**が表示されます。
Interface	ネイバに接続されたインタフェースです。
State	ネイバの状態です。 • **INCMP**–アドレスが解決されています。ネイバのリンクレイヤアドレスは不明です。 • **REACH**–ネイバは到達可能です。 • **STALE**–ネイバの到達可能性が不明です。装置は、ネイバに送信するデータがない限り、到達可能性を検証しません。 • **DELAY**–ネイバの到達可能性が不明です。装置は遅延後にNSメッセージを送信します。 • **PROBE**–ネイバの到達可能性が不明です。装置は、ネイバへの到達可能性を調査するためのNSメッセージです。
Type	ネイバノード情報の種類です。 • **S**–スタティックに設定されます。 • **D**–ダイナミックに取得されます。 • **O**–OpenFlowモジュールから学習します。OpenFlowはQX-S5300Gシリーズではサポートしていません。 • **R**–ポータルモジュールから学習します。 • **I**–無効です。
Aging	ハイフン(-)は、スタティックエントリを示します。 • ダイナミックエントリの場合、このフィールドには経過時間が秒単位で表示されます。ダイナミックエントリでネイバに到達できない場合、このフィールドには(#)が表示されます。
Vpn-instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 VPNの名前です。VPNが設定されていない場合**[No Vrf]**と表示されます。
Nickname	ネイバエントリの愛称です。名前は、4つの16進数の文字列です。

関連コマンド

- **ipv6 neighbor**
- **reset ipv6 neighbors**

11.1.4 display ipv6 neighbors count

Syntax

display ipv6 neighbors { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: ダイナミックに作成およびスタティックに設定されたネイバエントリを含む、すべてのネイバエントリの総数を表示します。

dynamic: ダイナミックに作成されたネイバエントリの総数を表示します。

static: スタティックに設定されたネイバエントリの総数を表示します。

slot *slot-number*: メンバ ID で IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドは、すべてのメンバ装置のネイバエントリの数を表示します。

interface *interface-type interface-number*:インタフェースのタイプと番号を指定します。

vlan *vlan-id*: 指定した VLAN 内のネイバエントリの合計数を表示します。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
```

11.1.5 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: パブリックネットワークのすべての PMTU の情報を表示します。

dynamic: すべてのダイナミック PMTU の情報を表示します。

static: すべてのスタティック PMTU の情報を表示します。

count: PMTU エントリの総数を表示します。

説明

display ipv6 pathmtu コマンドは IPv6 PMTU（Path MTU）情報を表示します。

ダイナミック PMTU とスタティック PMTU を含む IPv6 PMTU 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   Aging   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 11-5 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PMTUの値です。
Aging	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。

フィールド	説明
Type	PMTUタイプです。 • **Dynamic**–ダイナミックにネゴシエートされます。 • **Static**–スタティックに設定されます。
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**

11.1.6 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*: メンバ ID で IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IPv6 RawIP 接続に関する概要情報を表示します。

説明

display ipv6 rawip コマンドは IPv6 RawIP 接続の概要情報を表示します。

IPv6 RawIP 接続の概要情報はローカル IPv6 アドレス、ピアの IPv6 アドレス、プロトコル、PCB が含まれます。

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 11-6 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。

11.1.7 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 接続に関する詳細情報を表示します。設定範囲は 1～16 です。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IPv6 RawIP 接続に関する詳細情報を表示します。

説明

display ipv6 rawip verbose コマンドは IPv6 RawIP 接続の詳細情報を表示します。

例

IPv6 RawIP 接続の詳細情報を表示します。

<Switch> display ipv6 rawip verbose

```
Total RawIP socket number: 1
```

```
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
Receive VRF: 0xffff
```

表 11-7 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。
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**–ドロップされたパケットの数です。 • **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。

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	インターネット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_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リングします。 • **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。
Send VRF	送信されたインスタンスです。
Receive VRF	受信されたインスタンスです。

11.1.8 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IPv6 および ICMPv6 パケット統計情報を表示します。

説明

display ipv6 statistics コマンドは IPv6、ICMPv6 パケットの統計情報を表示します。

reset ipv6 statistics コマンドはすべての IPv6、ICMPv6 パケットの統計情報を削除します。

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

11.1.9 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IPv6 TCP 接続に関する概要情報を表示します。

説明

display ipv6 tcp コマンドは IPv6 TCP 接続の概要情報を表示します。

IPv6 TCP 接続の概要情報は、ローカル IPv6 アドレス、ポート番号、ピアの IPv6 アドレス、ピアのポート番号、TCP 接続状態が含まれます。

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 11-8 コマンド出力

フィールド	説明
*	TCP接続がMD5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	TCP接続状態です。
PCB	PCBインデックスです。

11.1.10 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 接続に関する詳細情報を表示します。設定範囲は 1～16 です。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IPv6 TCP 接続に関する詳細情報を表示します。

説明

display ipv6 tcp verbose コマンドは IPv6 TCP 接続の詳細情報を表示します。

例

IPv6 TCP 接続の詳細情報を表示します。

<Switch> display ipv6 tcp verbose

```
TCP inpcb number: 1(tcpcb number: 1)
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 11-9 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。
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。
Options	ソケットのオプションです。
Error	エラーコードです。
Receiving buffer(cc/hiwat/lowat/state)	以下の順番で受信バッファ情報を表示します。 • **cc**–使用されているバッファ空間です。 • **hiwat**–最大バッファ空間です。 • **lowat**–最小バッファ空間です。 • **state**–バッファ状態です。 ■ **CANTSENDMORE**–ピアにデータを送信できません。 ■ **CANTRCVMORE**–ピアからデータを受信できません。 ■ **RCVATMARK**–タグを受信しています。 ■ **N/A**–上記以外の状態です。
Sending buffer(cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。 • **cc**–使用されているバッファ空間です。 • **hiwat**–最大バッファ空間です。 • **lowat**–最小バッファ空間です。 • **state**–バッファ状態です。 ■ **CANTSENDMORE**–ピアにデータを送信できません。 ■ **CANTRCVMORE**–ピアからデータを受信できません。 ■ **RCVATMARK**–タグを受信しています。 ■ **N/A**–上記以外の状態です。
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破棄しません。 • **INP_EXLISTEN**–ソケットを待機中です。 • **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	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オプションなし。 • **TF_NOPUSH**–フルサイズのセグメントがTCPバッファにバッファされるまで、TCPによるTCPデータの送信を強制的に遅延させます。 • **TF_BINDFOREIGNADDR**–ピアのIPアドレスをバインドします。 • **TF_NSR**–TCP NSRを有効にします。 • **TF_REQ_SCALE**–TCPウィンドウスケールオプションを使用可能にします。 • **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選択的受信確認オプションを使用可能にします。 • **TF_ENHANCED_AUTH**–拡張認証オプションを使用可能にします。
NSR state	TCP接続の状態です。 括弧の間は、接続の役割です。 • **M**–メイン接続。 • **S**–スタンバイ接続。
Send VRF	送信されたインスタンスです。
Receive VRF	受信されたインスタンスです。

11.1.11 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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IPv6 UDP 接続についての概要情報を表示します。

説明

display ipv6 udp コマンドは IPv6 UDP 接続の概要情報を表示します。

例

IPv6 UDP 接続の概要情報を表示します。

<Switch> display ipv6 udp

```
LAddr->port        FAddr->port        Slot   PCB
 2001:2002:2003:2   3001:3002:3003:3   1      0x000000000000c387
 004:2005:2006:20   004:3005:3006:30
 07:2008->1200     07:3008->1200
 2001::1->23        2001::5->1284      2      0x0000000000000008
 2003::1->25        2001::2->1283      3      0x0000000000000009
```

表 11-10 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。

11.1.12 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 接続に関する詳細情報を表示します。設定範囲は 1～16 です。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置の IPv6 UDP 接続に関する詳細情報を表示します。

説明

display ipv6 udp verbose コマンドは IPv6 UDP 接続の詳細情報を表示します。

例

IPv6 UDP 接続の詳細情報を表示します。

<Switch> display ipv6 udp verbose

```
Total UDP socket number: 1
Connection info: src = ::->69, dst = ::->0
 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 11-11 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。
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。

フィールド	説明
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**–ドロップされたパケットの数です。 • **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_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。
Send VRF	送信されたインスタンスです。
Receive VRF	受信されたインスタンスです。

11.1.13 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

11.1.14 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

11.1.15 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オートコンフィギュレーション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オートコンフィギュレーション機能を無効にします。

ステートレスオートコンフィギュレーション機能によって、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 **undo ipv6 address auto** コマンドあるいは **undo ipv6 address** コマンドで削除することができます。

例

VLAN インタフェース 100 でステートレスアドレスオートコンフィギュレーション機能を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address auto

11.1.16 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ローバル 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オートコンフィギュレーションに使用されます。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ているインタフェースで **undo** コマンドを実行した場合、インタフェースにはまだリンクローカルアドレスがあります。

ipv6 address link-local コマンドを使用して、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もできます。IPv6 リンクローカルアドレスの自動生成よりも手動割り当てが優先されます。

- 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

11.1.17 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。

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

11.1.18 ipv6 address link-local

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: IPv6 リンクローカルアドレスを指定します。アドレスの最初の 10 ビットは、1111111010（バイナリ表示）である必要があります。つまり、アドレス内の 16 進数の最初のグループの範囲は FE80 から FEBF になります。

説明

ipv6 address link-local コマンドはインタフェースにリンクローカルアドレスを設定します。

undo ipv6 address link-local コマンドはインタフェースにリンクローカルアドレスをデフォルトに戻します。

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。IPvv6 リンクローカルアドレスの自動作成の詳細は、**ipv6 address auto link-local** コマンドを参照してください。

例

VLAN インタフェース 100 でリンクローカルアドレスを設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

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

関連コマンド

ipv6 address auto link-local

11.1.19 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 フィールドを通知すると、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

11.1.20 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

11.1.21 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

11.1.22 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 コマンドはマルチキャストエコー要求への応答を無効にします。

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、攻撃者は、ホスト A を送信元とするマルチキャストアドレスにエコー要求を送信できます。マルチキャストグループ内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

11.1.23 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: MTU サイズをバイト単位で指定します。次に、さまざまなインタフェースタイプの値の範囲を示します。

- VLAN インタフェースの場合は 1280～9216 です。
- 管理 Ethernet インタフェースの場合は 1280～1500 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化をサポートしていません。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

11.1.24 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、ステートレスオートコンフィギュレーションを使用します。

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、ステートフルオートコンフィギュレーション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オートコンフィギュレーション（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オートコンフィギュレーションを使用します。
- ステートレスオートコンフィギュレーション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。ステートレスオートコンフィギュレーションは、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って IPv6 アドレスを生成します。

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

11.1.25 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、ステートレスオートコンフィギュレーションを使用します。

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、ステートフルオートコンフィギュレーション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オートコンフィギュレーション（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オートコンフィギュレーションを使用します。

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

11.1.26 ipv6 nd dad attempts

Syntax

ipv6 nd dad attempts *interval*

undo ipv6 nd dad attempts

デフォルト

1

View

Interface view

定義済みユーザロール

network-admin

パラメータ

interval: DAD の NS メッセージを送信する試行回数を指定します。設定範囲は 0～600 です。0 に設定すると DAD は無効になります。

説明

ipv6 nd dad attempts コマンドは DAD の NS メッセージを送信する試行回数を設定します。

undo ipv6 nd dad attempts コマンドはデフォルトに戻します。

IPv6 アドレスを取得したのち、インタフェースは DAD の NS メッセージを送信します。

インタフェースが **ipv6 nd ns retrans-timer** コマンドで指定された時間以内に応答を受信しない場合、インタフェースは NS メッセージを再送します。

インタフェースが試行回数（**ipv6 nd dad attempts** コマンドで設定します）を超過しても応答を受信しない場合、取得したアドレスが使用できないと認識します。

例

DAD の NS メッセージを送信する試行回数を 20 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd dad attempts 20

関連コマンド

- **display ipv6 interface**
- **ipv6 nd ns retrans-timer**

11.1.27 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: 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

11.1.28 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 30000 ミリ秒です。RA メッセージの Reachable Time フィールドの値は 0 です。到達可能時間は受信装置によって決まります。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

time: インタフェースのネイバ到達可能時間を指定します。設定範囲は 1～3600000 ミリ秒です。

説明

ipv6 nd nud reachable-time コマンドはインタフェースのネイバ到達可能時間を設定します。

undo ipv6 nd nud reachable-time コマンドはデフォルトに戻します。

ネイバの到達可能性の検出を行い到達可能であった場合、装置は指定した到達可能時間内にネイバに到達できると認識します。指定した到達可能時間が終了した後、ネイバにパケットを送信する必要がある場合、装置はネイバが到達可能かどうか再確認を行います。

装置はローカルインタフェースのネイバ到達可能時間を設定し、送信する RA メッセージの Reachable Time フィールドに指定した値を設定します。

例

VLAN インタフェース 100 のネイバ到達可能時間を 10000 ミリ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd nud reachable-time 10000

関連コマンド

display ipv6 interface

11.1.29 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

11.1.30 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秒単位で指定します。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有効期限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

11.1.31 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**] *]

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期限 2592000 秒（30 日）と preferred（推奨）期限 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 アドレスの有効期限と preferred（推奨）期限を使用します。

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期限を指定します。設定範囲は 0～4294967295 秒です。

preferred-lifetime: ステートレスオートコンフィギュレーションに使用するプレフィックスの preferred（推奨）期限を指定します。設定範囲は 0～4294967295 秒です。preferred（推奨）期限は有効期限よりも大きい時間にすることはできません。デフォルトは 604800 秒(7 日)です。

no-autoconfig: ステートレスオートコンフィギュレーションを使用しないようにプレフィックスを指定します。**no-autoconfig** を指定しない場合、プレフィックスはステートレスオートコンフィギュレーションを使用します。

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。このキーワードがない場合、プレフィックス付きアドレスはリンク上で直接到達可能になります。

説明

ipv6 nd ra prefix コマンドは RA メッセージのプレフィックス情報を設定します。

undo ipv6 nd ra prefix コマンドは RA メッセージからプレフィックス情報を削除します。

同一リンクのホストが RA メッセージを受信したのち、ステートレスオートコンフィギュレーションのため、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。

プレフィックスは次の設定を使用します。

- 有効な存続時間は 2592000 秒(30 日分)です。
- 604800 秒(7 日)の推奨存続時間。
- プレフィックスはステートレス自動設定に使用されます。
- プレフィックスを持つアドレスは、リンク上で直接到達可能です。
- RA メッセージを送信するインタフェースの IPv6 アドレスをプレフィクス情報として使用します。RA メッセージにプレフィクス情報は設定されません。

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

11.1.32 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: ルータの有効期限を指定します。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有効期限を設定します。

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有効期限は、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、ルータの有効期限をチェックし、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。ルータの有効期限間が 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有効期限は 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有効期限を 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

11.1.33 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 コマンドはスタティックネイバエントリを削除します。

ネイバエントリはリンクローカルノードに関する情報を保存します。エントリは、NS および NA メッセージを介してダイナミックに作成することも、スタティックに構成することもできます。

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一意に識別します。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**

11.1.34 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。

ND エントリは、エージングタイマを持っています。エージングタイマが終了する前に、STALE 状態の ND エントリがリフレッシュされない場合、NG エントリは DELAY 状態に遷移します。5 秒以内にリフレッシュされない場合、PROBE 状態に遷移し、装置は 3 回、NS メッセージを送信します。もし応答がない場合、ND エントリを削除します。

例

STALE 状態の ND エントリのエージングタイマを 120 分に設定します。

<Switch> system-view

[Switch] ipv6 neighbor stale-aging 120

11.1.35 ipv6 neighbors max-learning-num

Syntax

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

undo ipv6 neighbors max-learning-num

デフォルト

1024

View

Layer 2 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 1～1024 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

11.1.36 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**

11.1.37 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

11.1.38 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。

宛先到達不能エラーのために、装置が受信した IPv6 パケットを転送できない場合、装置は次の操作を実行します。

- パケットを廃棄します。
- ICMPv6 宛先到達不能メッセージを送信元に送ります。

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

11.1.39 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*: タイプと番号で指定された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*: IRF スタックメンバ装置の ID を指定します。メンバ装置を指定しない場合、このコマンドはすべてのメンバ装置のダイナミックネイバ情報を削除します。

static: すべてのインタフェースのスタティックネイバ情報を削除します。

説明

reset ipv6 neighbors コマンドは IPv6 ネイバ情報を削除します。

例

すべてのインタフェースのネイバ情報を削除します。

<Switch> reset ipv6 neighbors all

```
This will delete all the entries. Continue? [Y/N]:Y
```

すべてのインタフェースのダイナミックネイバ情報を削除します。

<Switch> reset ipv6 neighbors dynamic

```
This will delete all the dynamic entries. Continue? [Y/N]:Y
```

すべての GigabitEthernet 1/0/1 インタフェース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**

11.1.40 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

11.1.41 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*: IRF スタックメンバ装置の ID を指定します。**slot** *slot-number* のオプションを指定しない場合、このコマンドは IRF スタックメンバ装置の IPv6 パケットと ICMPv6 パケットの統計情報を削除します。

説明

reset ipv6 statistics コマンドは IPv6 パケットと ICMPv6 パケットの統計情報を削除します。

例

IPv6 パケットと ICMPv6 パケットの統計情報を削除します。

<Switch> reset ipv6 statistics

関連コマンド

display ipv6 statistics

目次

このセクションのページは **4-x-x** です。

12 章 HTTP リダイレクト 12-1
12.1 HTTP リダイレクト設定コマンド 12-1
12.1.1 http-redirect https-port 12-1
12.1.2 http-redirect ssl-server-policy 12-2

12章 HTTP リダイレクト

12.1 HTTPリダイレクト設定コマンド

12.1.1 http-redirect https-port

Syntax

http-redirect https-port *port-number*

undo http-redirect https-port

デフォルト

8443

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: HTTPS リダイレクトサービスが HTTPS 要求を listen する TCP ポート番号を指定します。ポート番号の値の範囲は 1～65535 です。

説明

http-redirect https-port コマンドは HTTPS リダイレクトの待機ポート番号を指定します。

undo http-redirect https-port コマンドは 6654 ポートにリダイレクトします。

ポートの競合が原因でサービスが使用できなくなるのを防ぐために、ウェルノウンプロトコルまたは他のサービスで使用されている TCP ポート番号を指定しないでください。サービスによって使用されている TCP ポート番号を表示するには、**display tcp** コマンドを使用します。

このコマンドを複数回実行すると最新の設定が有効になります。

undo http-redirect https-port コマンドを実行した場合、デフォルトには戻りません。

デフォルトに戻す場合は、**http-redirect https-port 8443** コマンドを実行してください。

undo http-redirect https-port コマンドを設定すると、QX はユーザの HTTPS 要求を Web 認証にリダイレクトしません。Web 認証を使用する場合は、この設定を無効に変更しないことを推奨します。

例

HTTPS リダイレクトリスニングポート番号として 8888 を指定します。

<Switch> system-view

[Switch] http-redirect https-port 8888

12.1.2 http-redirect ssl-server-policy

Syntax

http-redirect ssl-server-policy *policy-name*

undo http-redirect ssl-server-policy

デフォルト

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: SSL サーバポリシーを名前で指定します。（1 文字～31 文字の大/小文字を区別しない文字列）

説明

http-redirect ssl-server-policy コマンドは SSL サーバポリシーを HTTPS リダイレクトサービスに関連付けします。

undo http-redirect ssl-server-policy コマンドは設定をデフォルトに戻します。

関連付けられている SSL サーバポリシーが存在しない場合、HTTPS リダイレクトは利用できません。最初に存在しない SSL サーバポリシーを HTTPS リダイレクトサービスに関連付けてから、SSL サーバポリシーを設定できます。

HTTPS リダイレクトサービスに関連付けられている SSL サーバポリシーを変更した場合、新しいポリシーはただちに有効になります。

この作業を複数回実行すると最新の設定が有効になります。

例

SSL サーバポリシーpolicy1 を HTTPS リダイレクトサービスに関連付けます。

<Switch> system-view

[Switch] http-redirect ssl-server-policy policy1

関連コマンド

ssl server-policy

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

5. ルーティングプロトコル

本マニュアルは以下に示す章で構成されています。

01-IP ルーティングの概要
02-スタティックルーティング
03-IPv6 スタティックルーティング

目次

このセクションのページは **5-x-x** です。

1 章 IP ルーティングの概要 1-1
1.1 IP ルーティングの概要設定コマンド.....1-1
1.1.1 address-family ipv4.....1-1
1.1.2 address-family ipv6.....1-1
1.1.3 display ip routing-table.....1-2
1.1.4 display ip routing-table acl.....1-7
1.1.5 display ip routing-table ip-address.....1-10
1.1.6 display ip routing-table prefix-list.....1-13
1.1.7 display ip routing-table protocol.....1-14
1.1.8 display ip routing-table statistics.....1-16
1.1.9 display ipv6 rib graceful-restart.....1-17
1.1.10 display ipv6 routing-table.....1-18
1.1.11 display ipv6 routing-table acl.....1-23
1.1.12 display ipv6 routing-table ipv6-address.....1-27
1.1.13 display ipv6 routing-table prefix-list.....1-30
1.1.14 display ipv6 routing-table protocol.....1-31
1.1.15 display ipv6 routing-table statistics.....1-33
1.1.16 display rib graceful-restart.....1-34
1.1.17 ip route fast-switchover enable.....1-37
1.1.18 ipv6 route fast-switchover enable.....1-37
1.1.19 protocol lifetime.....1-38
1.1.20 reset ip routing-table statistics protocol.....1-39
1.1.21 reset ipv6 routing-table statistics protocol.....1-40
1.1.22 rib.....1-40
1.1.23 routing-table limit.....1-41

1章 IP ルーティングの概要

1.1 IPルーティングの概要設定コマンド

1.1.1 address-family ipv4

Syntax

address-family ipv4

undo address-family ipv4

デフォルト

設定なし

View

RIB view

定義済みユーザロール

network-admin

説明

address-family ipv4 コマンドは RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行します。

undo address-family ipv4 コマンドは RIB IPv4 アドレスファミリーを削除し、RIB IPv4 address family view のすべての設定を削除します。

例

RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4]

1.1.2 address-family ipv6

Syntax

address-family ipv6

undo address-family ipv6

デフォルト

設定なし

View

RIB view

定義済みユーザロール

network-admin

説明

address-family ipv6 コマンドは RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行します。

undo address-family ipv6 コマンドは RIB IPv6 アドレスファミリーを削除し、RIB IPv6 address family view のすべての設定を削除します。

例

RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv6

[Switch-rib-ipv6]

1.1.3 display ip routing-table

Syntax

display ip routing-table [**verbose**]

display ip routing-table [**all-routes**]

View

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-routes: パブリックネットワークのルーティングテーブル情報を表示します。

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ip routing-table コマンドはルーティングテーブルの情報を表示します。

パラメータを指定しないと、パブリックネットワークのルーティングテーブル情報が表示されます。

例

ルーティングテーブルのアクティブルートの概要情報を表示します。

<Switch> display ip routing-table

```
Destinations : 12       Routes : 12

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
192.168.1.0/24      Direct 0    0           192.168.1.40    Vlan11
192.168.1.0/32      Direct 0    0           192.168.1.40    Vlan11
192.168.1.40/32     Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.40    Vlan11
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

表 1-1 コマンド出力

フィールド	説明
VPN instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ルーティングテーブルが属するパブリックネットワークです。パブリックネットワークの場合、このフィールドには**public instance**が表示されます。
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。

フィールド	説明
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 : 2       Routes : 2

Destination: 0.0.0.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 08h34m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1000c       OrigNextHop: 127.0.0.1
      Label: NULL         RealNextHop: 127.0.0.1
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A               PathID: 0x0

Destination: 1.1.1.0/24
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 60
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
```

```
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.47.4
      Label: NULL         RealNextHop: 192.168.47.4
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A
```

表 1-2 コマンド出力

フィールド	説明
VPN instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ルーティングテーブルが属するパブリックネットワークです。パブリックネットワークの場合、このフィールドには**public instance**が表示されます。
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	インストールしたプロトコルルートです。
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優先順位です。
QosLocalID	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ローカルQoS IDです。
Tag	ルートタグです。

フィールド	説明
State	ルート状態です。 • **Active**—アクティブなユニキャストルートです。 • **Adv**—配信できるルートです。 • **Inactive**—非アクティブルートです。 • **NoAdv**—ルータが配信できないルートです。 • **Vrrp**—VRRPによって作成されたルートです。 • **Nat**—NATによって作成されたルートです。 • **TunE**—トンネルです。
OrigTblID	もとのルーティングテーブルIDです。
OrigVrf	ルートが属するもとのVPNインスタンスです。ルートがIPv4パブリックネットワーク上にある場合、このフィールドには**default-vrf**が表示されます。
TableID	ルーティングテーブルのIDです。
OrigAs	もとのAS番号です。
NibID	ネクストホップのIDです。
LastAs	最新のAS番号です。
AttrID	属性IDです。
Neighbor	ルーティングプロトコルによって決定された隣接アドレスです。
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。
Tunnel ID	トンネルIDです。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
BkTunnel ID	バックアップトンネルIDです。
BkInterface	バックアップ出力インタフェースです。

フィールド	説明
FtnIndex	FTNエントリのインデックスです。
TrafficIndex	1～64の範囲のトラフィックインデックスです。値が無効な場合、このフィールドには「**N/A**」と表示されます。
Connector	このフィールドは、QX-S5300Gシリーズではサポートしていません。 VPN IPv4ルートとともにBGPピア間で交換されるBGPコネクタ属性です。この属性の値は、リモートPE装置のIPアドレスです。BGPコネクタ属性は、MD VPNに使用されます。BGPコネクタ属性がサポートされていない場合、このフィールドには「**N/A**」と表示されます。
Summary count	ルート数です。
PathID	BGPルートのAdd-Path IDです。 BGPはQX-S5300Gシリーズではサポートしていません。

1.1.4 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-ipv4-basic-2000] display ip routing-table acl 2000

```
Summary count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
192.168.1.0/24      Direct 0    0           192.168.1.111   Vlan11
192.168.1.0/32      Direct 0    0           192.168.1.111   Vlan11
192.168.1.111/32    Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.111   Vlan11
```

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

```
Destination: 192.168.1.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.1.111
      Label: NULL          RealNextHop: 192.168.1.111
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A               PathID: 0x0

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

Destination: 192.168.1.255/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
```

```
     Cost: 0            Preference: 0
    IpPre: N/A          QosLocalID: N/A
      Tag: 0               State: Active NoAdv
 OrigTblID: 0x0           OrigVrf: default-vrf
  TableID: 0x2             OrigAs: 0
    NibID: 0x10000003       LastAs: 0
   AttrID: 0xffffffff      Neighbor: 0.0.0.0
    Flags: 0x1008c      OrigNextHop: 192.168.1.111
    Label: NULL        RealNextHop: 192.168.1.111
  BkLabel: NULL          BkNextHop: N/A
 Tunnel ID: Invalid       Interface: Vlan-interface11
BkTunnel ID: Invalid     BkInterface: N/A
  FtnIndex: 0x0        TrafficIndex: N/A
 Connector: N/A             PathID: 0x0
```

コマンド出力は表 1-2 を参照してください。

1.1.5 display ip routing-table ip-address

Syntax

display ip routing-table *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 11.0.0.1.のルートエントリの概要情報を表示します。

<Switch> display ip routing-table 11.0.0.1

```
Summary count : 3

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/8          Static 60   0           0.0.0.0         NULL0
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
11.0.0.0/24         Static 60   0           0.0.0.0         NULL0
```

宛先 IP アドレス 11.0.0.1 およびマスク長 20 のルートの概要情報を表示します。

<Switch> display ip routing-table 11.0.0.1 20

```
Summary count : 2

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/8          Static 60   0           0.0.0.0         NULL0
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス 11.0.0.1 のマスク長が最長のルートの概要情報を表示します。

<Switch> display ip routing-table 11.0.0.1 longer-match

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/24         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス 11.0.0.1、マスク長 20、マスク長が最長のルートの概要情報を表示します。

<Switch> display ip routing-table 11.0.0.1 20 longer-match

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス範囲 1.1.1.0～5.5.5.0 の宛先アドレスのルートの概要情報を表示します。

<Switch> display ip routing-table 1.1.1.0 to 5.5.5.0

```
Summary count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.1.1.1/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0           2.2.2.1         Vlan2
3.3.3.1/32          Direct 0    0           127.0.0.1       InLoop0
```

```
4.4.4.1/32        Direct 0    0          127.0.0.1      InLoop0
```

コマンド出力は表 1-1 を参照してください。

1.1.6 display ip routing-table prefix-list

Syntax

display ip routing-table 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
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
  FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A               PathID: 0x0
```

コマンド出力は表 1-2 を参照してください。

1.1.7 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 : 0

Static Routing Table Status : <Inactive>
Summary count : 1
```

```
Destination/Mask    Proto  Pre  Cost        NextHop       Interface
1.2.3.0/24          Static 60   0           1.2.4.5       Vlan10
```

コマンド出力は表 1-1 を参照してください。

1.1.8 display ip routing-table statistics

Syntax

display ip routing-table [**all-routes**] **statistics**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all-routes: パブリックネットワークの IPv4 ルート統計情報を表示します。

説明

display ip routing-table statistics コマンドは総ルート数、プロトコルによってインストールされたルート、削除とマークされたルート、およびアクティブルートを含む IPv4 ルート統計を表示します。

パラメータを指定しない場合、コマンドはパブリックネットワークの IPv4 ルート統計情報を表示します。

例

パブリックネットワークの IPv4 ルートの統計情報を表示します。

<Switch> display ip routing-table statistics

```
Total prefixes: 15       Active prefixes: 15

Proto      Routes      Active      Added       Deleted
DIRECT     12          12          30          18
STATIC     3           3           5           2
Total      15          15          35          20
```

表 1-3 コマンド出力

フィールド	説明
VPN instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ルーティングテーブルが属するパブリックネットワークです。パブリックネットワークの場合、このフィールドには**public instance**が表示されます。
Proto	ルートを指定したプロトコルです。
Routes	プロトコルによって指定されたルート数です。
Active	アクティブルート数です。
Added	ルータが起動あるいはルーティングテーブルが最後に削除した後にルーティングテーブルに追加されたルート数です。
Deleted	deletedと記載されたルート数です。一定期間後に削除されます。
Total	ルートの総数です。

1.1.9 display ipv6 rib graceful-restart

Syntax

display ipv6 rib graceful-restart

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ipv6 rib graceful-restart コマンドは IPv6 RIB GR の状態情報を表示します。

例

IPv6 RIB GR の状態情報を表示します。

<Switch> display ipv6 rib graceful-restart

```
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
```

```
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT6    480      29   End      No/No
 2    STATIC6    480      32   End      No/No
```

コマンド出力は address-family ipv4 を参照してください。

1.1.10 display ipv6 routing-table

Syntax

display ipv6 routing-table [**verbose**]

display ipv6 routing-table [**all-routes**]

View

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-routes: パブリックネットワークの IPv6 ルーティングテーブル情報を表示します。

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ipv6 routing-table コマンドは IPv6 ルーティングテーブルの情報を表示します。

パラメータを指定しない場合、コマンドはパブリックネットワークの IPv6 ルーティングテーブル情報を表示します。

例

IPv6 ルーティングテーブルのアクティブルートの概要情報を表示します。

<Switch> display ipv6 routing-table

```
Destinations : 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
```

パブリックネットワークの IPv6 ルーティングテーブルに、アクティブルートに関する簡単な情報を表示します。

<Switch> display ipv6 routing-table all-routes

```
VPN instance: public instance
Destinations : 2 Routes : 2

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

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

表 1-4 コマンド出力

フィールド	説明
VPN instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 IPv6ルーティングテーブルが属するパブリックネットワークです。パブリックネットワークの場合、このフィールドには**public instance**が表示されます。
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。

IPv6 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 : 2 Routes : 2

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 19h23m02s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
      NibID: 0x20000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A               PathID: 0x0

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

表 1-5 コマンド出力

フィールド	説明
VPN instance	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ルーティングテーブルが属するパブリックネットワークです。パブリックネットワークの場合、このフィールドにはパブリックインスタンスが表示されます。
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。
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	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ローカルQoS IDです。
Tag	ルートのタグです。
State	ルートの状態です。 ● **Active**—アクティブなユニキャストルートです。 ● **Adv**—配信できるルートです。 ● **Inactive**—非アクティブルートです。 ● **NoAdv**—ルータが配信できないルートです。 ● **Vrrp**—VRRPによって作成されたルートです。 ● **Nat**—NATによって作成されたルートです。 ● **TunE**—トンネルです。
OrigTblID	もとのルーティングテーブルIDです。
OrigVrf	ルートが属するもとのVPNインスタンスです。ルートがIPv6ネットワーク上にある場合、このフィールドには**default-vrf**が表示されます。
TableID	ルーティングテーブルのIDです。
OrigAs	もとのAS番号です。

フィールド	説明
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。
Tunnel ID	トンネルIDです。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
BkTunnel ID	バックアップトンネルIDです。
BkInterface	バックアップ出力インタフェースです。
FtnIndex	FTNエントリの指標です。
TrafficIndex	1～64の範囲のトラフィックインデックスです。値が無効な場合、このフィールドには「N/A」と表示されます。
Connector	このフィールドは、QX-S5300Gシリーズではサポートしていません。 VPN IPv4ルートとともにBGPピア間で交換されるBGPコネクタ属性です。この属性の値は、リモートPE装置のIPアドレスです。BGPコネクタ属性は、MD VPNに使用されます。BGPコネクタ属性がサポートされていない場合、このフィールドには「**N/A**」と表示されます。
Summary count	ルート数です。
PathID	BGPルートのAdd-Path IDです。 BGPはQX-S5300Gシリーズではサポートしていません。

1.1.11 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: 11::1/128                          Protocol  : O_INTER
NextHop    : FE80::A1F:3FFF:FE45:206              Preference: 10
Interface  : Vlan11                             Cost      : 2

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

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

コマンド出力は表 1-4 を参照してください。

IPv6 ACL 2000 によって許可されたすべてのルートに関する詳細情報を表示します。

<Switch> display ipv6 routing-table acl 2000 verbose

```
Summary count : 6

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

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 00h07m57s
      Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
```

```
      Tag: 0                State: Active Adv
 OrigTblID: 0x0             OrigVrf: default-vrf
   TableID: 0xa             OrigAs: 0
     NibID: 0x20000003       LastAs: 0
    AttrID: 0xffffffff      Neighbor: ::
     Flags: 0x10080      OrigNextHop: ::
     Label: NULL         RealNextHop: ::
   BkLabel: NULL           BkNextHop: N/A
 Tunnel ID: Invalid        Interface: Vlan-interface11
BkTunnel ID: Invalid      BkInterface: N/A
  FtnIndex: 0x0          TrafficIndex: N/A
 Connector: N/A              PathID: 0x0

Destination: 12::1/128
  Protocol: Direct
 Process ID: 0
 SubProtID: 0x0                Age: 00h07m55s
     Cost: 0            Preference: 0
     IpPre: N/A          QosLocalID: N/A
      Tag: 0               State: Active NoAdv
 OrigTblID: 0x0            OrigVrf: default-vrf
   TableID: 0xa             OrigAs: 0
     NibID: 0x20000000       LastAs: 0
    AttrID: 0xffffffff      Neighbor: ::
     Flags: 0x10004      OrigNextHop: ::1
     Label: NULL         RealNextHop: ::1
   BkLabel: NULL           BkNextHop: N/A
 Tunnel ID: Invalid        Interface: InLoopBack0
BkTunnel ID: Invalid      BkInterface: N/A
  FtnIndex: 0x0          TrafficIndex: N/A
 Connector: N/A              PathID: 0x0

Destination: 11::1/128
  Protocol: O_INTER
 Process ID: 1
 SubProtID: 0x2                Age: 00h06m43s
     Cost: 2            Preference: 10
     IpPre: N/A          QosLocalID: N/A
      Tag: 0               State: Active Adv
 OrigTblID: 0x0            OrigVrf: default-vrf
   TableID: 0xa             OrigAs: 0
     NibID: 0x23000003       LastAs: 0
    AttrID: 0x ffffffff     Neighbor: ::
```

```
     Flags: 0x10041       OrigNextHop: FE80::A1F:3FFF:FE45:206
     Label: NULL          RealNextHop: FE80::A1F:3FFF:FE45:206
   BkLabel: NULL            BkNextHop: N/A
 Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
  FtnIndex: 0x0           TrafficIndex: N/A
 Connector: N/A               PathID: 0x0

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

Destination: FF00::/8
  Protocol: Direct
Process ID: 0
 SubProtID: 0x0                 Age: 19h29m12s
     Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
      Tag: 0                 State: Active NoAdv
 OrigTblID: 0x0             OrigVrf: default-vrf
   TableID: 0xa              OrigAs: 0
     NibID: 0x20000001        LastAs: 0
    AttrID: 0xffffffff       Neighbor: ::
     Flags: 0x10014       OrigNextHop: ::
     Label: NULL          RealNextHop: ::
   BkLabel: NULL            BkNextHop: N/A
 Tunnel ID: Invalid          Interface: NULL0
BkTunnel ID: Invalid       BkInterface: N/A
```

```
  FtnIndex: 0x0          TrafficIndex: N/A
Connector: N/A               PathID: 0x0
```

コマンド出力は表 1-5 を参照してください。

1.1.12 display ipv6 routing-table ipv6-address

Syntax

display ipv6 routing-table *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 10::1 127 のルートエントリの概要情報を表示します。

<Switch> display ipv6 routing-table 10::1 127

```
Summary count: 3

Destination: 10::/64                              Protocol  : Static
NextHop    : ::                                  Preference: 60
Interface  : NULL0                                Cost      : 0

Destination: 10::/68                              Protocol  : Static
NextHop    : ::                                  Preference: 60
Interface  : NULL0                                Cost      : 0

Destination: 10::/120                             Protocol  : Static
NextHop    : ::                                  Preference: 60
Interface  : NULL0                                Cost      : 0
```

宛先 IPv6 アドレス 10::1 およびプレフィックス長 127 のプレフィックス長が最長のルートの概要情報を表示します。

<Switch> display ipv6 routing-table 10::1 127 longer-match

```
Summary count : 1

Destination: 10::/120                          Protocol  : Static
NextHop    : ::                               Preference: 60
Interface  : NULL0                             Cost      : 0
```

宛先アドレス範囲 100::～300::の宛先アドレスのルートの概要情報を表示します。

<Switch> display ipv6 routing-table 100:: to 300::

```
Summary count : 3

Destination: 100::/64                          Protocol  : Static
NextHop    : ::                               Preference: 60
Interface  : NULL0                             Cost      : 0

Destination: 200::/64                          Protocol  : Static
NextHop    : ::                               Preference: 60
Interface  : NULL0                             Cost      : 0

Destination: 300::/64                          Protocol  : Static
NextHop    : ::                               Preference: 60
Interface  : NULL0                             Cost      : 0
```

宛先 IPv6 アドレス範囲 1：2 :: 3：4/128 の宛先アドレスのルートの詳細情報を表示します。

<Switch> display ipv6 routing-table 1:2::3:4 128 verbose

```
Summary count : 1

Destination: 1:2::3:4/128
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 00h01m14s
      Cost: 1             Preference: 10
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                 State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
     NibID: 0x23000002         LastAs: 0
```

```
    AttrID: 0xffffffff       Neighbor: ::
     Flags: 0x10041       OrigNextHop: FE80::A1F:3FFF:FE45:206
     Label: NULL          RealNextHop: FE80::A1F:3FFF:FE45:206
   BkLabel: NULL            BkNextHop: N/A
 Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
  FtnIndex: 0x0          TrafficIndex: N/A
 Connector: N/A               PathID: 0x0
```

コマンド出力は表 1-4 を参照してください。

1.1.13 display ipv6 routing-table prefix-list

Syntax

display ipv6 routing-table 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
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A               PathID: 0x0
```

コマンド出力は表 1-5 を参照してください。

1.1.14 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 : 3

Static Routing table Status : <Active>
Summary count : 3
Destination: 2::2/128                          Protocol  : Static
NextHop    : fe80::2                          Preference: 60
Interface  : Vlan12                           Cost      : 0

Destination: 2::2/128                          Protocol  : Static
NextHop    : fe80::3                          Preference: 60
Interface  : Vlan12                           Cost      : 0

Destination: 3::3/128                          Protocol  : Static
NextHop    : 2::2                             Preference: 60
Interface  : Vlan12                           Cost      : 0

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

コマンド出力は表 1-4 を参照してください。

1.1.15 display ipv6 routing-table statistics

Syntax

display ipv6 routing-table [**all-routes**] **statistics**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all-routes: パブリックネットワークの IPv6 ルート統計情報を表示します。

説明

display ipv6 routing-table statistics コマンドは IPv6 ルートの統計情報を表示します。

パラメータを指定しない場合、コマンドはパブリックネットワークの IPv6 ルート統計情報を表示します。

例

パブリックネットワークの IPv6 ルートの統計情報を表示します。

<Switch> display ipv6 routing-table statistics

```
Total prefixes: 8       Active prefixes: 8

Proto      Routes      Active      Added       Deleted
DIRECT     5           5           5           0
STATIC     3           3           3           0
Total      8           8           8           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。
Routes	プロトコルによって指定されたルート数です。
Active	アクティブルート数です。
Added	ルータが起動あるいはルーティングテーブルが最後に削除した後にルーティングテーブルに追加されたルート数です。
Deleted	deletedと記載されたルート数です。一定期間後に削除されます。
Total	ルートの総数です。

1.1.16

1.1.16 display rib graceful-restart

Syntax

display rib graceful-restart

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display rib graceful-restart コマンドは RIB GR の状態情報を表示します。

例

RIB GR の状態情報を表示します。

<Switch> display rib graceful-restart

```
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT     100      30   End      No/No
 2    STATIC     480      34   End      No/No
```

表 1-7 コマンド出力

フィールド	説明
RIB GR state	RIB GRの状態です。 ● **Start**—GRが起動します。 ● **IGP end**—すべてのIGPプロトコルがGRを完了します。 ● **VPN-triggering end**—VPNルートによって開始した最適ルートの選定が完了します。 ● **VPN-calculation end**—最適VPNルートの選定が完了します。 ● **Routing protocol end**—すべてのルーティングプロトコルがGRを完了します。 ● NSR-calculation unfinished—NSRが最適ルートの選定を完了していません。 ● **Triggering start**—開始したすべてのルートの選定が行われます。 ● **Triggering end**—開始したすべてのルートの選定が完了します。 ● **Phase1-calculation end**—最適ルートの選定のフェーズ1が完了します。 ● **All end**—すべてのプロトコルがGRを完了します。 ● **Phase2-calculation end**—最適ルートの選定のフェーズ2が完了します。

フィールド	説明
RCOM GR state	RCOM GRの状態です。 ● **Start**—GRが開始します。 ● **VPN-calculation end**—最適VPNルートの選定が完了します。 ● **VPN-notification end**—VPNルートがルート管理モジュールに配送されています。 ● **Routing protocol end**—すべてのルーティングプロトコルがGRを完了します。 ● NSR-calculation unfinished—NSRが最適ルートの選定を完了していません。 ● **Phase1-calculation end**—最適ルートの選定のフェーズ1が完了します。 ● **Notification end**—すべてのルートがルート管理モジュールに配送されています。 ● **Phase2-calculation end**—最適ルートの選定のフェーズ2が完了します。 ● **Flush start**—ルートをFIBに配信し始めます。 ● **Flush end**—FIBへのルートの配信が完了します。
No.	プロトコル番号です。
Lifetime	GRの間でのRIBのルート/ラベルの生存時間です。単位は秒です。
FD	プロトコルとRIB間で処理を行います。
State	プロトコルのGRの状態です。 ● **Init**—初期状態です。 ● **Listen**—リスニング状態です。 ● **Idle**－アイドル状態です。 ● **Active**－アクティブ状態です。 ● **Start**—GRが開始します。 ● **End**—GRが完了します。
Start/End	メッセージ送信状態です。 ● **No**—メッセージが送信されていません。 ● **Yes**—メッセージが送信されています。

1.1.17 ip route fast-switchover enable

Syntax

ip route fast-switchover enable

undo ip route fast-switchover 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 route fast-switchover enable コマンドは IPv4 ルートファーストスイッチオーバーを有効にします。

undo ip route fast-switchover enable コマンドは IPv4 ルートファーストスイッチオーバーを無効にします。

このコマンドは、ECMP ルートやプライマリ/セカンダリルートなど、多数のルートに対して同じ物理出力インタフェースを提供する装置に適用されます。インタフェースでリンク障害が発生した場合、トラフィックを別のルートに切り替える前に、装置は次の操作を実行する必要があります。

1. リンクのすべての ARP エントリを削除します。
2. 関連する FIB エントリを削除するよう FIB に指示します。

この手順には時間がかかり、トラフィックの動作が長時間中断されます。この問題を解決するには、ルートファーストスイッチオーバーを有効にします。この機能により、装置は､最初にルート切り替えの無効な FIB エントリを削除するよう FIB に指示できます。

例

#IPv4 ルートファーストスイッチオーバーを有効にします。

<Switch> system-view

[Switch] ip route fast-switchover enable

1.1.18 ipv6 route fast-switchover enable

Syntax

ipv6 route fast-switchover enable

undo ipv6 route fast-switchover 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 route fast-switchover enable コマンドは IPv6 ルートファーストスイッチオーバーを有効にします。

undo ipv6 route fast-switchover enable コマンドは IPv6 ルートファーストスイッチオーバーを無効にします。

このコマンドは、ECMP ルートやプライマリ/セカンダリルートなど、多数のルートに対して同じ物理出力インタフェースを提供する装置に適用されます。インタフェースでリンク障害が発生した場合、トラフィックを別のルートに切り替える前に、装置は次の操作を実行する必要があります。

1. リンクのすべての ND エントリを削除します。
2. 関連する FIB エントリを削除するよう FIB に指示します。

この手順には時間がかかり、トラフィックの動作が長時間中断されます。この問題を解決するには、ルートファーストスイッチオーバーを有効にします。この機能により、装置は、最初にルート切り替えの無効な FIB エントリを削除するよう FIB に指示できます。

例

#IPv6 ルートファーストスイッチオーバーを有効にします。

<Switch> system-view

[Switch] ipv6 route fast-switchover enable

1.1.19 protocol lifetime

Syntax

protocol *protocol* **lifetime** *seconds*

undo protocol *protocol* **lifetime**

デフォルト

480 秒

View

RIB IPv4 address family view

RIB IPv6 address family view

定義済みユーザロール

network-admin

パラメータ

protocol: ルーティングプロトコルを指定します。

seconds: RIB のルートと、ラベルの生存時間を指定します。設定範囲は 1～6000 秒です。0 を指定した場合、プロトコルの切り替わりが発生した場合、RIB はすぐにエージアウトします。

説明

protocol lifetime コマンドは RIB の IPv4 ルートあるいは IPv6 ルートと、ラベルの最大生存時間を設定します。

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

GR が有効である場合、プロトコルは設定された生存時間内に GR が完了し、RIB にすべてのルートエントリをインストールすることができます。

例

RIB のスタティックルートとラベルの最大生存時間を 60 秒に設定します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4] protocol static lifetime 60

1.1.20 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

パブリックネットワークのすべての IPv4 ルートの統計情報を削除します。

<Switch> reset ip routing-table statistics protocol all

1.1.21 reset ipv6 routing-table statistics protocol

Syntax

reset ipv6 routing-table statistics protocol { *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

パブリックネットワークのすべての IPv6 ルートの統計情報を削除します。

<Switch> reset ipv6 routing-table statistics protocol all

1.1.22 rib

Syntax

rib

undo rib

View

System view

定義済みユーザロール

network-admin

説明

rib コマンドは RIB view に移行します。

undo rib コマンドは RIB view ですべての設定を削除します。

例

RIB view に移行します。

<Switch> system-view

[Switch] rib

[Switch-rib]

1.1.23 routing-table limit

Syntax

routing-table limit *number* **simply-alert**

undo routing-table limit

デフォルト

設定なし

View

RIB IPv4 address family view

RIB IPv6 address family view

定義済みユーザロール

network-admin

パラメータ

number: 装置がサポートするアクティブ IPv4/IPv6 ルートの最大数を指定します。設定範囲は 1～4294967295 です。

simply-alert: 装置がアクティブなルートを受け入れながら、アクティブな IPv4/IPv6 ルートの数が最大数を超えたときにログメッセージを作成できるようにします。

🕮 **メモ：**

QX-S5300G シリーズのルーティングテーブルは IPv4 が 256、IPv6 が 128 です。そのため、simply-alert を設定する場合は、これらの値よりも小さい値を設定してください。

説明

routing-table limit コマンドは装置がサポートするアクティブな IPv4/IPv6 ルートの最大数を設定します。

undo routing-table limit コマンドはデフォルトに戻します。

RIB IPv4 アドレスファミリーview での設定は、パブリックネットワークのアクティブ IPv4 ルートの数を制限します。

RIB IPv6 アドレスファミリーview での設定は、パブリックネットワークのアクティブ IPv6 ルートの数を制限します。

例

RIB IPv4 アドレスファミリーview で、パブリックネットワークのアクティブな IPv4 ルートの最大数を 1000 に設定します。装置はまだ新しいアクティブルートを受け入れますが、アクティブルートの最大数を超えるとシステムログメッセージを作成します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4] routing-table limit 1000 simply-alert

目次

このセクションのページは **5-x-x** です。

2 章 スタティックルーティング 2-1
2.1 スタティックルーティング設定コマンド.....2-1
2.1.1 delete static-routes all.....2-1
2.1.2 ip route-static.....2-2
2.1.3 ip route-static default-preference.....2-4

2章 スタティックルーティング

2.1 スタティックルーティング設定コマンド

2.1.1 delete static-routes all

Syntax

delete 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 *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] } [**preference** *preference*] [**description** *text*]

undo ip route-static *dest-address* { *mask-length* | *mask* } [*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

dest-address: スタティックルートの宛先アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 の整数です。

mask: ドット区切りの 10 進表記でサブネットマスクを指定します。

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。詳細はオペレーションマニュアルのセクション 5 *ルーティングプロトコル* 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。詳細はオペレーションマニュアルのセクション 5 *ルーティングプロトコル* を参照してください。

bfd: スタティックルートのネクストホップの到達可能性を検出する BFD を有効にします。ネクストホップが到達不可能である場合、システムはすぐにバックアップルートに切り替えます。

control-packet: BFD コントロールモードを指定します。

bfd-source *ip-address*: BFD パケットの送信元 IP アドレスを指定します。ループバックインタフェースのアドレスを指定することを推奨します。

permanent: 固定のスタティックルートを指定します。出力インタフェースがダウンしても、固定のスタティックルートはアクティブのままです。

track *track-entry-number*: track エントリの番号とスタティックルートを関連づけます。設定範囲は 1～1024 です。Track の詳細は、オペレーションマニュアルのセクション 9 *高可用性* “*Track*”を参照してください。

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 *text:* スタティックルートの説明を設定します。設定範囲は 1～60 文字です。半角スペースのような記号を含むことができますがクエスチョンマーク（?）は含むことができません。

説明

ip route-static コマンドはスタティックルートを設定します。

undo ip route-static コマンドはスタティックルートを削除します。

宛先アドレスとマスクの両方が 0.0.0.0（あるいは 0）である場合、設定されたルートはデフォルトルートです。デフォルトルートはルーティングテーブルに一致するエントリがないパケットを転送するのに使用されます。

異なるルートの優先順位を設定するため、異なる preference を設定してください。たとえば、同一宛先の複数のルートのロードバランスを有効にする場合、ルートに同一の優先順位を割り当ててください。一方をバックアップルートとする場合、ルートに異なる優先順位を割り当ててください。

スタティックルートの出力インタフェースあるいはネクストホップアドレスを指定するとき、以下のガイドラインに従ってください。

- 出力インタフェースが Null 0 インタフェースである場合、ネクストホップアドレスは必要ありません。
- 出力インタフェースがポイントツーポイントインタフェースの場合は、出力インタフェースだけを指定できます。ピアアドレスが変更された場合でも、ルートの設定を変更する必要はありません。
- NBMA または P2MP インタフェースは、パケット配信を成功させるために IP アドレスからリンクへのレイヤアドレスマッピングを必要とします。最善の方法として、出力インタフェースがネクストホップである場合、同時にそのルートのネクストホップアドレスを指定します。NBMA または P2MP インタフェースです。

スタティックルートを設定するとき、以下のガイドラインに従ってください。

- ルートが頻繁に切り替わる状態で BFD を有効にした場合、ルートのフラッピングを悪化させます。使用する場合、注意してください。BFD の詳細は、オペレーションマニュアルのセクション 9 *高可用性* “*BFD*”を参照してください。
- **permanent** を **bfd** あるいは **track** と一緒に使用しないでください。

例

宛先アドレスが 1.1.1.1/24、ネクストホップが 2.2.2.2、説明が for internet のスタティックルートを設定します。

<Switch> system-view

[Switch] ip route-static 1.1.1.1 24 2.2.2.2 description for internet

関連コマンド

display ip routing-table protocol

2.1.3 ip route-static default-preference

Syntax

ip route-static default-preference *default-preference*

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が再設定された場合、新しく追加されたスタティックルートが適用されます。

例

スタティックルートのデフォルトの優先順位を 120 に設定します。

<Switch> system-view

[Switch] ip route-static default-preference 120

関連コマンド

display ip routing-table protocol

目次

このセクションのページは **5-x-x** です。

3 章 IPv6 スタティックルーティング 3-1
3.1 IPv6 スタティックルーティング設定コマンド.....3-1
3.1.1 delete ipv6 static-routes all.....3-1
3.1.2 ipv6 route-static 3-1
3.1.3 ipv6 route-static default-preference 3-3

3章 IPv6 スタティックルーティング

3.1 IPv6 スタティックルーティング設定コマンド

3.1.1 delete ipv6 static-routes all

Syntax

delete ipv6 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

3.1.2 ipv6 route-static

Syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] [**bfd** { **control-packet** | **echo-packet** } | **permanent**] | *next-hop-address* [**bfd control-packet bfd-source** *ipv6-address* | **permanent**] } [**preference** *preference*] [**description** *text*]

undo ipv6 route-static *ipv6-address prefix-length* [*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。出力インタフェースが NBMA インタフェースあるいはブロードキャストインタフェースである場合、またはポイントツーポイント（P2P）インタフェースでない場合、ネクストホップアドレスを指定する必要があります。

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

bfd: スタティックルートのネクストホップの到達可能性を検出する BFD を有効にします。

control-packet: BFD コントロールモードを指定します。

bfd-source *ipv6-address*: BFD パケットの送信元 IPv6 アドレスを指定します。

echo-packet: BFD エコーモードを指定します。

permanent: 固定の IPv6 スタティックルートを指定します。出力インタフェースがダウンしても、固定の IPv6 スタティックルートはアクティブのままです。

preference *preference:* 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。

宛先アドレスが**::/0**（あるいはプレフィックス長が 0）である場合、設定されたルートは IPv6 デフォルトルートです。IPv6 デフォルトルートはルーティングテーブルに一致するエントリがないパケットを転送するのに使用されます。

スタティックルート用に出力インタフェース、ネクストホップアドレス、またはその両方を設定するには、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ブロードキャストインタフェースまたは NBMA インタフェースの場合は、ネクストホップアドレスを指定する必要があります。
- 出力インタフェースが P2P インタフェースの場合は、出力インタフェースのみを指定できます。ピアアドレスが変更されても、ルートの設定を変更する必要はありません。

IPv6 スタティックルート用に BFD を設定するときは、以下のガイドラインに従ってください。

- BFD パケットの送信元 IPv6 アドレスを指定する場合は、ピア装置のネクストホップ IPv6 アドレスとして IPv6 アドレスを指定する必要があります。

スタティックルートを設定するとき、以下のガイドラインに従ってください。

- フラッピングルートに対して BFD を有効にすると、ルートフラッピングの状況が悪化する可能性があります。 したがって、慎重に使用してください。BFD の詳細は、オペレーションマニュアルのセクション 9 *高可用性*“*BFD*”を参照してください。
- エコーパケットのネクストホップ IPv6 アドレスはグローバルユニキャストアドレスにしてください。
- **permanent** と、**bfd** を同時に指定しないでください。

例

宛先アドレスが 1:1:2::/64、ネクストホップが 1:1:3::1 の IPv6 スタティックルートを設定します。

<Switch> system-view

[Switch] ipv6 route-static 1:1:2:: 64 1:1:3::1

関連コマンド

display ipv6 routing-table protocol

3.1.3 ipv6 route-static default-preference

Syntax

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

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-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

6. マルチキャスト

本マニュアルは以下に示す章で構成されています。

01-IGMP スヌーピング
02-マルチキャスト VLAN
03-MLD スヌーピング
04-IPv6 マルチキャスト VLAN

目次

このセクションのページは **6-x-x** です。

1 章 IGMP スヌーピング 1-1
1.1 IGMP スヌーピング設定コマンド 1-1
1.1.1 display igmp-snooping 1-1
1.1.2 display igmp-snooping group 1-4
1.1.3 display igmp-snooping router-port 1-6
1.1.4 display igmp-snooping static-group 1-8
1.1.5 display igmp-snooping static-router-port 1-10
1.1.6 display igmp-snooping statistics 1-11
1.1.7 display l2-multicast ip 1-12
1.1.8 display l2-multicast ip forwarding 1-14
1.1.9 display l2-multicast mac 1-16
1.1.10 display l2-multicast mac forwarding 1-17
1.1.11 display mac-address [multicast] 1-19
1.1.12 dot1p-priority (IGMP-snooping view) 1-20
1.1.13 dscp 1-21
1.1.14 entry-limit (IGMP-snooping view) 1-22
1.1.15 fast-leave (IGMP-snooping view) 1-23
1.1.16 group-policy (IGMP-snooping view) 1-24
1.1.17 host-aging-time (IGMP-snooping view) 1-25
1.1.18 igmp-snooping 1-26
1.1.19 igmp-snooping dot1p-priority 1-27
1.1.20 igmp-snooping drop-unknown 1-28
1.1.21 igmp-snooping enable 1-29
1.1.22 igmp-snooping fast-leave 1-30
1.1.23 igmp-snooping general-query source-ip 1-31
1.1.24 igmp-snooping group-limit 1-32
1.1.25 igmp-snooping group-policy 1-33
1.1.26 igmp-snooping host-aging-time 1-35
1.1.27 igmp-snooping host-join 1-36
1.1.28 igmp-snooping last-member-query-interval 1-38
1.1.29 igmp-snooping leave source-ip 1-39
1.1.30 igmp-snooping max-response-time 1-40
1.1.31 igmp-snooping overflow-replace 1-41
1.1.32 igmp-snooping proxy enable 1-42
1.1.33 igmp-snooping querier 1-43
1.1.34 igmp-snooping query-interval 1-44

1.1.35 igmp-snooping report source-ip 1-45
1.1.36 igmp-snooping router-aging-time 1-46
1.1.37 igmp-snooping source-deny 1-47
1.1.38 igmp-snooping special-query source-ip 1-48
1.1.39 igmp-snooping static-group 1-49
1.1.40 igmp-snooping static-router-port 1-50
1.1.41 igmp-snooping version 1-51
1.1.42 last-member-query-interval (IGMP-snooping view) 1-52
1.1.43 mac-address multicast 1-53
1.1.44 max-response-time (IGMP-snooping view) 1-54
1.1.45 overflow-replace (IGMP-snooping view) 1-55
1.1.46 report-aggregation (IGMP-snooping view) 1-56
1.1.47 reset igmp-snooping group 1-57
1.1.48 reset igmp-snooping router-port 1-58
1.1.49 reset igmp-snooping statistics 1-58
1.1.50 router-aging-time (IGMP-snooping view) 1-59
1.1.51 source-deny (IGMP-snooping view) 1-60

1章 IGMP スヌーピング

1.1 IGMPスヌーピング設定コマンド

1.1.1 display igmp-snooping

Syntax

display igmp-snooping [**global** | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルの IGMP snooping の状態を表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

display igmp-snooping コマンドは IGMP snooping の状態を表示します。

パラメータを指定しない場合、グローバルとすべての VLAN の IGMP snooping の状態を表示します。

例

🕮 **メモ：**

Global-enable の表示は未サポートです。Global-enable の表示が Disabled であっても、IGMP snooping はグローバルで有効の状態です。なお、グローバルで無効の場合は、IGMP snooping is not configured.と表示されます。

グローバルとすべての VLAN の IGMP snooping の状態を表示します。

<Switch> display igmp-snooping

```
IGMP snooping information: Global
 Global-enable: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
```

```
 Report-aggregation: Enabled
 Host-tracking: Disabled
 Dot1p-priority: --

IGMP snooping information: VLAN 1
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Version: 2
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

IGMP snooping information: VLAN 10
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 3
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: --
 Proxy: Disabled
```

表 1-1 コマンド出力

フィールド	説明
Global-enable	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。
IGMP snooping	VLANの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 queryの最大応答時間です。
Last-member-query-interval	IGMP group-specific queryの間隔です。
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802.1 p優先度です。優先順位が設定されていない場合、このフィールドにはハイフンが2つ表示されます(--)。
Querier	IGMP snoopingクエリアの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
(IP: 1.1.1.1, Expires: 00:02:05)	IGMP snoopingクエリア情報: ● **IP**－IGMP snoopingクエリアのIPアドレスです。 ● **Expire**－IGMP snoopingクエリアの残りエージングタイムです。 IGMP snoopingクエリア選択が無効になっている場合、このフィールドは表示されません。
Querier-election	IGMP snoopingクエリア選択のステータスです。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Query-interval	IGMP general queryの間隔です。

フィールド	説明
General-query source IP	IGMP general queryの送信元IPアドレスです。
Special-query source IP	IGMP group-specific query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	ホスト追跡のステータス: ● **Enabled**－有効です。 ● **Disabled**－無効です。
Proxy	IGMP snoopingプロキシのステータス: ● **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 グループ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 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 のダイナミック IGMP snooping グループエントリを表示します。

verbose: ダイナミック IGMP snooping グループエントリの詳細情報を表示します。指定しない場合、このコマンドはダイナミック IGMP snooping グループエントリに関する概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。指定しない場合、マスタ装置のダイナミック IGMP snooping グループエントリを表示します。

説明

display igmp-snooping group コマンドはダイナミック IGMP snooping グループエントリに関する情報を表示します。

例

VLAN2 のダイナミック IGMP snooping グループエントリの詳細情報を表示します。

<Switch> display igmp-snooping group vlan 2 verbose

```
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2                         (00:03:23)
```

表 1-2 コマンド出力

フィールド	説明
Total 1 entries	ダイナミックIGMP snoopingグループ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グループエントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Attribute	エントリ属性です。 • **global port**—エントリにグローバルポートがあります。 • **local port**—エントリに指定された装置上のポートがあります。 • **slot**—エントリに指定された装置以外の装置上のポートがあります。

フィールド	説明
FSM information	エントリの有限状態装置（Finite state machine）情報です。 ● **delete**—エントリの属性が削除されています。 ● **dummy**—エントリが新規で一時的なエントリです。 ● **no info**—エントリが存在しません。
Host slots (0 in total)	メンバポートとマスタ装置のメンバポートの総数です。 メンバポートがあるメンバ装置のメンバIDとメンバ装置の総数です（指定メンバ装置またはマスタ装置を除きます）。
Host ports (1 in total)	メンバポートとメンバポートの総数です。
(00:03:23)	ダイナミックメンバポートの残りのエージング時間です。 グローバルポート(レイヤ2アグリゲートインタフェース、AC、N-PW、U-PWなど)の場合、このフィールドは常に表示されます。 非グローバル・ポートの場合、このフィールドは次のいずれかの条件が存在する場合に表示されます。 ● ポートは指定されたメンバ装置上にあります ● ポートはマスタ装置上にあり、メンバ装置が指定されていません。
GE1/0/3 (Link ID 0)	ACとそのリンクIDです。
NPW (Link ID 8)	N-PWとそのリンクIDです。
UPW (Link ID 9)	U-PWとそのリンクIDです。
Tun0 (VXLAN ID 0)	VXLANトンネルとそのVXLAN IDです。VXLANはQX-S5300Gシリーズではサポートしていません。
VLAN pairs (1 in total)	VLANペアとVLANペアの総数です。
Outer VLAN 5 Inner VLAN 2	外部VLAN IDと内部VLAN ID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。

slot *slot-number*: IRF スタックメンバ装置を指定します。指定しない場合、マスタ装置のダイナミックルータポートを表示します。

説明

display igmp-snooping router-port コマンドはダイナミックルータポートの情報を表示します。

例

VLAN 2 のダイナミックルータポートの概要情報を表示します。

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

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

表 1-3 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	ルータポートがあるメンバ装置のメンバIDとメンバ装置の総数です（指定メンバ装置またはマスタ装置を除きます）。
Router ports (2 in total)	ダイナミックルータポートと、ダイナミックルータポートの総数です。
(00:01:30)	ダイナミックルータポートの残りのエージング時間です。 グローバルポートでは常に表示されます。 非グローバルポートの場合、このフィールドは次のいずれかの条件が存在する場合に表示されます。 • ポートは指定されたメンバ装置上にあります。 • ポートはマスタ装置上にあり、メンバ装置は指定されていません。
GE1/0/3 (Link ID 1)	ACとそのリンクIDです。

フィールド	説明
NPW (Link ID 8)	N-PWとそのリンクIDです。
UPW (Link ID 9)	U-PWとそのリンクIDです。
Tun0 (VXLAN ID 0)	VXLANトンネルとそのVXLAN IDです。VXLANはQX-S5300Gシリーズではサポートしていません。
VLAN pairs (1 in total)	VLANペアとVLANペアの総数です。
Outer VLAN 5 Inner VLAN 2	外部VLAN IDと内部VLAN ID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 グループ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 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 のスタティック IGMP snooping グループエントリを表示します。

verbose: スタティック IGMP snooping グループエントリの詳細情報を表示します。指定しない場合、概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。指定しない場合、マスタ装置のスタティック IGMP snooping グループエントリを表示します。

説明

display igmp-snooping static-group コマンドはスタティック IGMP snooping グループエントリを表示します。

例

VLAN 2 のスタティック IGMP snooping グループ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グループ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グループエントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Attribute	エントリ属性です。 • **global port**—エントリにグローバルポートがあります。 • **local port**—エントリに指定された装置上のポートがあります。 • **slot**—エントリに指定された装置以外の装置上のポートがあります。
FSM information	エントリの有限状態装置（Finite state machine）情報です。 • **delete**—エントリの属性が削除されています。 • **dummy**—エントリが新規で一時的なエントリです。 • **no info**—エントリが存在しません。
Host slots (0 in total)	メンバポートがあるメンバ装置のメンバIDとメンバ装置の総数です（指定メンバ装置またはマスタ装置を除きます）。

フィールド	説明
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*] [**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

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

verbose: スタティックルータポートに関する詳細情報を表示します。このキーワードを指定しない場合、このコマンドはスタティックルータポートに関する簡単な情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。指定しない場合、マスタ装置のスタティックルータポートの情報を表示します。

説明

display igmp-snooping static-router-port コマンドはスタティックルータポートの情報を表示します。

例

VLAN 2 のスタティックルータポートの概要情報を表示します。

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

```
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

VLAN2 のスタティックルータポートの詳細情報を表示します。

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

```
VLAN 2:
```

```
Router slots (0 in total):
Router ports (2 in total):
  GE1/0/1
  GE1/0/2
```

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)	ルータポートがあるメンバ装置のメンバIDとメンバ装置の総数です（指定メンバ装置またはマスタ装置を除きます）。
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 queryの数です。
specific queries	IGMP group-specific query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 queryの数です。
PIMv2 hello	PIMv2 helloメッセージの数です。
error IGMP messages	エラーがあるIGMPメッセージの数です。

関連コマンド

reset igmp-snooping statistics

1.1.7 display l2-multicast ip

Syntax

display l2-multicast ip [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *group-address*: マルチキャストグループを IP アドレスで指定します。マルチキャストグループを指定しない場合、このコマンドはすべてのレイヤ 2 IP マルチキャストグループの情報を表示します。

source *source-address*: マルチキャスト送信元を IP アドレスで指定します。マルチキャスト送信元アドレスを指定しない場合、このコマンドは、すべてのマルチキャスト送信元のレイヤ 2 IP マルチキャストグループの情報を表示します。

vlan *vlan-id*: VLAN ID で VLAN を 1～4094 の範囲で指定します。VLAN を指定しない場合、このコマンドは、すべての VLAN のレイヤ 2 IP マルチキャストグループの情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置のレイヤ 2 IP マルチキャストグループの情報を表示します。

説明

display l2-multicast ip コマンドはレイヤ 2IP マルチキャストグループの情報を表示します。

例

VLAN2 のレイヤ 2 IP マルチキャストグループの情報を表示します。

<Switch> display l2-multicast ip vlan 2

```
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: static, success
    Host ports (1 in total):
      GE1/0/1                          (S, SUC)
```

表 1-7 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPマルチキャストグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2 IPマルチキャストグループエントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。

フィールド	説明
Attribute	エントリ属性です。 • **dynamic**—エントリはダイナミックプロトコルによって作成されます。 • **static**—エントリはスタティックプロトコルによって作成されます。 • **pim**—エントリはPIMによって作成されます。PIMはQX-S5300Gシリーズではサポートしていません。 • **kernel**—エントリはカーネルから取得されます。 • **success**—処理に成功しました。 • **fail**—処理に失敗しました。
Host ports (1 in total)	メンバポートおよびメンバポートの総数です。
(S, SUC)	ポート属性です。 • **D**—ダイナミックポートです。 • **S**—スタティックポートです。 • **P**—PIMポートです。PIMはQX-S5300Gシリーズではサポートしていません。 • **K**—カーネルから取得されたポートです。 • **R**—(*, *)エントリから学習したポートです。 • **W**—(*, G)エントリから学習したポートです。 • **SUC**—処理に成功しました。 • **F**—処理に失敗しました。
GE1/0/1 (Link ID 1)	ACとそのリンクIDです。
NPW (Link ID 8)	N-PWとそのリンクIDです。
UPW (Link ID 9)	U-PWとそのリンクIDです。
Tun0 (VXLAN ID 0)	VXLANトンネルとそのVXLAN IDです。VXLANはQX-S5300Gシリーズではサポートしていません。

1.1.8 display l2-multicast ip forwarding

Syntax

display l2-multicast ip forwarding [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *group-address*: マルチキャストグループの IP アドレスを指定します。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのレイヤ 2 マルチキャスト IP 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 マルチキャスト IP 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 マルチキャスト IP 転送エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。指定しない場合、マスタ装置のレイヤ 2 マルチキャスト IP 転送エントリを表示します。

説明

display l2-multicast ip forwarding コマンドはレイヤ 2 マルチキャスト IP 転送エントリを表示します。

例

VLAN 2 のレイヤ 2 マルチキャスト IP 転送エントリを表示します。

<Switch> display l2-multicast ip forwarding vlan 2

```
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

表 1-8 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2マルチキャストIP転送エントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2マルチキャストIP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。

フィールド	説明
Host ports (3 in total)	メンバポートとメンバポートの総数です。
GigabitEthernet1/0/3 (Link ID 0)	ACとそのリンクIDです。
NPW (Link ID 8)	N-PWとそのリンクIDです。
UPW (Link ID 9)	U-PWとそのリンクIDです。
Tunnel0 (VXLAN ID 0)	VXLANトンネルとそのVXLAN IDです。VXLANはQX-S5300Gシリーズではサポートしていません。

1.1.9 display l2-multicast mac

Syntax

display l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: マルチキャスト MAC アドレスで MAC マルチキャストグループを指定します。MAC マルチキャストグループを指定しない場合、このコマンドはすべてのレイヤ 2 MAC マルチキャストグループの情報を表示します。

vlan *vlan-id*: VLAN ID で VLAN を 1～4094 の範囲で指定します。VLAN を指定しない場合、このコマンドは、すべての VLAN のレイヤ 2 MAC マルチキャストグループの情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置のレイヤ 2 MAC マルチキャストグループの情報を表示します。

説明

display l2-multicast mac コマンドはレイヤ 2 MAC マルチキャストグループの情報を表示します。

例

VLAN2 のレイヤ 2 MAC マルチキャストグループの情報を表示します。

<Switch> display l2-multicast mac vlan 2

```
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host ports (1 in total):
      GE1/0/1
```

表 1-9 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 MACマルチキャストグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2 MACマルチキャストグループエントリの総数です。
MAC group address	MACマルチキャストグループのアドレスです。
Attribute	エントリ属性です。 ● **success**—処理に成功しました。 ● **fail**—処理に失敗しました。
Host ports (1 in total)	メンバポートとメンバポートの総数です。
GE1/0/3 (Link ID 0)	ACとそのリンクIDです。
NPW (Link ID 8)	N-PWとそのリンクIDです。
UPW (Link ID 9)	U-PWとそのリンクIDです。
Tun0 (VXLAN ID 0)	VXLANトンネルとそのVXLAN IDです。VXLANはQX-S5300Gシリーズではサポートしていません。

1.1.10 display l2-multicast mac forwarding

Syntax

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: MAC アドレスで MAC マルチキャストグループを指定します。指定しない場合、すべての MAC マルチキャストグループのレイヤ 2 マルチキャスト MAC 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 マルチキャスト MAC 転送エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。指定しない場合、マスタ装置のレイヤ 2 マルチキャスト MAC グループエントリを表示します。

説明

display l2-multicast mac forwarding コマンドはレイヤ 2 マルチキャスト MAC 転送エントリを表示します。

例

VLAN 2 のレイヤ 2 マルチキャスト MAC 転送エントリを表示します。

<Switch> display l2-multicast mac forwarding vlan 2

```
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

表 1-10 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2マルチキャストMAC転送エントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2マルチキャストMAC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。
GigabitEthernet1/0/3 (Link ID 0)	ACとそのリンクIDです。
NPW (Link ID 8)	N-PWとそのリンクIDです。
UPW (Link ID 9)	U-PWとそのリンクIDです。

フィールド	説明
Tunnel0 (VXLAN ID 0)	VXLANトンネルとそのVXLAN IDです。VXLANはQX-S5300Gシリーズではサポートしていません。

1.1.11 display mac-address [multicast]

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: マルチキャスト MAC アドレスを指定します。MAC アドレスには、0100-5Exx-xxxx および 3333xxxx-xxxx を除く、有効なマルチキャスト MAC アドレスを使用できます。「x」の設定範囲は、0～F の 16 進数です。

vlan *vlan-id*: VLAN ID で VLAN の設定範囲は、1～4094 です。VLAN を指定しない場合、このコマンドはすべての VLAN の 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: MAC アドレスエントリの数を指定します。このキーワードを指定すると、コマンドは一致する MAC アドレスエントリの数を表示します。このキーワードを指定しない場合、コマンドはエントリカウント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、このコマンドはユニキャスト 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

VLAN2 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
```

スタティックマルチキャスト MAC アドレスエントリ数を表示します。

<Switch> display mac-address multicast count

```
1 mac address(es) found.
```

表 1-11 コマンド出力

フィールド	説明
MAC address	マルチキャストグループのMACアドレスです。
VLAN ID	MACアドレスで識別されるネットワーク装置が属するVLANのIDです。
State	MACアドレスのステータスです。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、このフィールドには**Multicast**と表示されます。
Port/NickName	出力ポートまたはこのアドレスエントリ内のMACアドレスに送信されるパケットに対する、TRILLネットワーク内のEgress RBのニックネームです。 TRILLはQX-S5300Gシリーズではサポートしていません。
Aging	エージングタイマの状態です。このエントリが無期限の場合、このフィールドには**N**と表示されます。
1 mac address(es) found	スタティックマルチキャストエントリアドレスが1つ見つかりました。

関連コマンド

mac-address multicast

1.1.12 dot1p-priority (IGMP-snooping view)

Syntax

dot1p-priority *priority*

undo dot1p-priority

デフォルト

IGMP メッセージの 802.1p 優先度は設定されていません。装置によって作成された IGMP メッセージの場合、802.1p 優先度は 0 です。転送される IGMP メッセージの場合、装置は 802.1p 優先度を変更しません。

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 802.1 p 優先度の設定範囲は、0～7 です。値が大きいほど、優先順位が高くなります。

説明

dot1p-priority コマンドは IGMP メッセージの 802.1 p 優先度をグローバルに設定します。

undo dot1p-priority コマンドはデフォルトに戻します。

IGMP snooping view のすべての VLAN、または VLAN view の VLAN に対して、グローバルに 802.1 p 優先度を設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

IGMP メッセージの 802.1 p 優先度をグローバルに 3 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] dot1p-priority 3

関連コマンド

igmp-snooping dot1p-priority

1.1.13 dscp

Syntax

dscp *dscp-value*

undo dscp

デフォルト

48

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 0～63 の範囲で DSCP 値を指定します。

説明

dscp コマンドは出力 IGMP snooping プロトコルパケットの DSCP 値を設定します。

undo dscp コマンドはデフォルトに戻します。

DSCP 値は、パケットの送信優先順位を決定するために、IP パケットの ToS フィールドで伝送されます。DSCP 値が大きいほど、優先順位が高くなります。

例

出力 IGMP snooping プロトコルパケットの DSCP 値を 63 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] dscp 63

1.1.14 entry-limit (IGMP-snooping view)

Syntax

entry-limit *limit*

undo entry-limit

デフォルト

4294967295

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

limit: IGMP snooping 転送エントリの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 IGMP 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

IGMP snooping 転送エントリのグローバルの最大数を 512 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] entry-limit 512

1.1.15 fast-leave (IGMP-snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

デフォルト

無効

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、1 行のコマンドで 10 個まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

fast-leave コマンドはグローバルに fast-leave 処理機能を有効にします。

undo fast-leave コマンドはグローバルに fast-leave 処理機能を無効にします。

ポートが leave メッセージを受信したとき、装置はマルチキャストグループの転送エントリから迅速にポートを削除します。

IGMP-snooping view のすべてのポートまたは interface view のポートに対してグローバルに fast-leave 処理を有効にできます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

例

VLAN 2 でグローバルに fast-leave 処理機能を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] fast-leave vlan 2

関連コマンド

igmp-snooping fast-leave

1.1.16 group-policy (IGMP-snooping view)

Syntax

group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

デフォルト

マルチキャストグループポリシーは設定されていません。受信ホストは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、ホストが参加できるマルチキャストグループを制御するために IGMP レポートをフィルタします。

スタティックメンバポートは IGMP レポートを送信しないため、このコマンドはスタティックメンバポートには影響しません。

IGMP snooping view のすべてのポート、または interface view のポートに対して、グローバルにマルチキャストグループポリシーを設定できます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

IPv4 ACL でルールを設定する場合は、次の制限とガイドラインに従ってください。

- 標準 ACL では、**source** *source-address source-wildcard* オプションはマルチキャストグループアドレスを指定します。
- 拡張 ACL では、**source** *source-address source-wildcard* オプションは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 オプションは、マルチキャストグループアドレスを指定します。

次の IGMP レポートに一致させるには、**source** *source-address source-wildcard* オプションを 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

- その他のオプションパラメータのうち、**fragment** キーワードと **time-range** *time-range-range-name* オプションだけが有効になります。

異なる VLAN のすべてのポートに異なる ACL を設定できます。同じ VLAN 内のすべてのポートに複数の ACL を設定する場合、最新の設定が有効になります。

例

VLAN 2 のホストがマルチキャストグループ 225.1.1.1 のみ加入できるように VLAN 2 のマルチキャストグループポリシーをグローバルに設定します。

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Switch-acl-ipv4-basic-2000] quit
[Switch] igmp-snooping
[Switch-igmp-snooping] group-policy 2000 vlan 2
```

関連コマンド

igmp-snooping group-policy

1.1.17 host-aging-time (IGMP-snooping view)

Syntax

host-aging-time *seconds*

undo host-aging-time

デフォルト

260 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds:ダイナミックメンバポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

host-aging-time コマンドはグローバルでダイナミックメンバポートのエージングタイマを設定します。

undo host-aging-time コマンドはデフォルトに戻します。

IGMP snooping view ですべての VLAN に対してグローバルに、VLAN view で VLAN に対してタイマを設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

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 query の間隔]＋[IGMP general query の最大応答時間]

例

グローバルでダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] host-aging-time 300

関連コマンド

igmp-snooping host-aging-time

1.1.18 igmp-snooping

Syntax

igmp-snooping

undo igmp-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

igmp-snooping コマンドはグローバルで IGMP snooping を有効にし、IGMP-snooping view に移行します。グローバルで IGMP snooping を有効にした後、使用する VLAN で IGMP snooping を有効にしてください。IGMP snooping の設定については、セクション 6 *マルチキャスト オペレーションマニュアル*の“*IGMP スヌーピング*”を参照してください。

undo igmp-snooping コマンドはグローバルで IGMP snooping を無効にします。

IGMP snooping 機能を無効にすると、すべての VLAN で IGMP snooping が無効になります。

例

グローバルで IGMP snooping を有効にし、IGMP-snooping view に移行します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping]

関連コマンド

- **igmp-snooping enable**

1.1.19 igmp-snooping dot1p-priority

Syntax

igmp-snooping dot1p-priority *priority*

undo igmp-snooping dot1p-priority

デフォルト

IGMP メッセージの 802.1p 優先度は設定されていません。装置によって作成された IGMP メッセージの場合、802.1p 優先度は 0 です。転送される IGMP メッセージの場合、装置は 802.1p 優先度を変更しません。

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 802.1 p 優先度の設定範囲は 0～7 です。値が大きいほど、優先順位が高くなります。

説明

igmp-snooping dot1p-priority コマンドは VLAN 内の IGMP メッセージの 802.1 p 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 の IGMP snooping を有効にする必要があります。

VLAN view で VLAN の 802.1 p 優先度を設定するか、IGMP snooping view ですべての VLAN に対してグローバルに設定できます。VLAN 固有の設定は、グローバル設定よりも優先されます。

例

VLAN2 で IGMP snooping を有効にし、IGMP メッセージの 802.1 p 優先度を 3 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping dot1p-priority 3

関連コマンド

- **dot1p-priority (IGMP-snooping view)**
- **igmp-snooping enable**

1.1.20 igmp-snooping drop-unknown

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

デフォルト

VLAN の未知のマルチキャストデータの廃棄機能は無効です。未知のマルチキャストデータは VLAN にフラッディングされます。

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping drop-unknown コマンドは VLAN の未知のマルチキャストデータの廃棄機能を有効にします。

undo igmp-snooping drop-unknown コマンドは VLAN の未知のマルチキャストデータの廃棄機能を無効にします。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

例

IGMP snooping を有効にし、VLAN 2 の未知のマルチキャストデータの廃棄機能を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping drop-unknown

関連コマンド

igmp-snooping enable

1.1.21 igmp-snooping enable

Syntax

igmp-snooping enable

undo igmp-snooping

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 コマンドは VLAN の IGMP snooping を無効にします。

VLAN の IGMP snooping を有効にする前に、**igmp-snooping** コマンドを使用して IGMP snooping 機能を有効にする必要があります。

VLAN view でこのコマンドを使用して VLAN の IGMP snooping を有効にできます。VLAN view の設定は IGMP snooping view の設定と同じ優先度を持ち、最新の設定が有効になります。

IGMP snooping の設定については、セクション 6 *マルチキャスト オペレーションマニュアルの“IGMP スヌーピング”*を参照してください。

例

IGMP snooping 機能を有効にし、次に VLAN2 の IGMP snooping を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

関連コマンド

igmp-snooping

1.1.22 igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping fast-leave コマンドはポートで fast-leave 処理機能を有効にします。

undo igmp-snooping fast-leave コマンドはポートで fast-leave 処理機能を無効にします。

この機能は、ポートが leave メッセージを受信したとき、装置がマルチキャストグループの転送エントリから迅速にポートを削除します。

IGMP snooping view では、interface view のポートまたはグローバルにすべてのポートに対して fast-leave 処理機能を有効にできます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

例

GigabitEthernet 1/0/1 の VLAN 2 で fast-leave 処理機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2

関連コマンド

fast-leave (IGMP-snooping view)

1.1.23 igmp-snooping general-query source-ip

Syntax

igmp-snooping general-query source-ip *ip-address*

undo igmp-snooping general-query source-ip

デフォルト

VLAN では、IGMP general query 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 の general query 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 query 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 query の送信元 IP アドレス 10.1.1.1 を設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping general-query source-ip 10.1.1.1

関連コマンド

igmp-snooping enable

1.1.24 igmp-snooping group-limit

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

デフォルト

制限なし

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

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 コマンドはポートが加入できるマルチキャストグループの最大数の制限を解除します。

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/が加入できるマルチキャストグループの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2

1.1.25 igmp-snooping group-policy

Syntax

igmp-snooping group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

デフォルト

ポートでマルチキャストグループポリシーは設定されていません。ポートに接続されたホストは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、ホストが参加できるマルチキャストグループを制御するために IGMP レポートをフィルタします。

スタティックメンバポートは IGMP レポートを送信しないため、このコマンドはスタティックメンバポートには影響しません。

IGMP snooping view では、interface view 内のポートに対して、またはグローバルに、マルチキャストグループポリシーを設定できます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

IPv4 ACL でルールを設定する場合は、次の制限とガイドラインに従ってください。

- 標準 ACL では、**source** *source-address source-wildcard* オプションはマルチキャストグループアドレスを指定します。
- 拡張 ACL では、**source** *source-address source-wildcard* オプションは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* オプションは、マルチキャストグループアドレスを指定します。

次の IGMP レポートに一致させるには、**source** *source-address source-wildcard* オプションを 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

- その他のオプションパラメータのうち、**fragment** キーワードと **time-range** *time-range-name* オプションだけが有効になります。

VLAN ごとに異なる ACL をポートに設定できます。同じ VLAN のポートに複数の ACL を設定する場合、最新の設定が有効になります。

例

ポートに接続されたホストがマルチキャストグループ 225.1.1.1 のみ加入できるように VLAN 2 の GigabitEthernet 1/0/1 でマルチキャストグループポリシーを設定します。

<Switch> system-view

[Switch] acl basic 2000

[Switch-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0

[Switch-acl-ipv4-basic-2000] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2

関連コマンド

group-policy (IGMP-snooping view)

1.1.26 igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

デフォルト

260 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: VLAN のダイナミックメンバポートのエージングタイマを設定します。設定範囲は 1~8097894 秒です。

説明

igmp-snooping host-aging-time コマンドは VLAN のダイナミックメンバポートのエージングタイマを設定します。

undo igmp-snooping host-aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

VLAN view で VLAN 用に、または IGMP snooping view ですべての VLAN 用にグローバルに、タイマを設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

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 query の間隔]＋[IGMP general query 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 query の間隔]×2＋[IGMP general query の最大応答時間]

例

VLAN 2 の IGMP snooping を有効にし、VLAN のダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping host-aging-time 300

関連コマンド

- **host-aging-time (IGMP-snooping view)**
- **igmp-snooping enable**

1.1.27 igmp-snooping host-join

Syntax

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-ip *source-address*: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定した場合、ポートをマルチキャストソースとグループのシミュレーティッドメンバホストとして設定します。マルチキャストソースを指定しない場合、マルチキャストグループのポートをシミュレーティッドメンバホストとして設定します。このパラメータは IGMPv3 snooping が動作する装置で有効です。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべてのマルチキャストグループを指定します。

説明

igmp-snooping host-join コマンドはポートをマルチキャストグループのシミュレーティッドメンバホストとして設定します。

undo igmp-snooping host-join コマンドはシミュレーティッドメンバホストの設定を削除します。

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。

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。

例

VLAN2 のマルチキャストソースとマルチキャストグループの(1.1.1.1, 232.1.1.1)のシミュレーティッドメンバポートを GigabitEthernet 1/0/1 に設定します。

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping version 3
[Switch-vlan2] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan 2
```

1.1.28 igmp-snooping last-member-query-interval

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

デフォルト

1 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP last member query の間隔を設定します。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 query の間隔を設定します。

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。

VLAN view で VLAN の間隔を設定するか、IGMP snooping view ですべての VLAN の間隔をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

VLAN 2 の IGMP snooping を有効にし、VLAN 2 の IGMP last member query の間隔を 3 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping last-member-query-interval 3

関連コマンド

- **igmp-snooping enable**
- **last-member-query-interval (IGMP-snooping view)**

1.1.29 igmp-snooping leave source-ip

Syntax

igmp-snooping leave source-ip *ip-address*

undo igmp-snooping leave source-ip

デフォルト

VLAN では、IGMP leave メッセージの送信元 IP アドレスは現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスがない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP leave メッセージの送信元 IP アドレスを指定します。

説明

igmp-snooping leave source-ip コマンドは IGMP leave メッセージの送信元 IP アドレスを設定します。

undo igmp-snooping leave source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

例

VLAN 2 で IGMP snooping を有効にし、IGMP leave メッセージの送信元 IP アドレスを 10.1.1.1 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping leave source-ip 10.1.1.1

関連コマンド

igmp-snooping enable

1.1.30 igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

デフォルト

10 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: IGMP general query の最大応答時間を設定します。設定範囲は 1～25 秒です。

説明

igmp-snooping max-response-time コマンドは VLAN の IGMP general query 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。

VLAN view で VLAN の時間を設定するか、IGMP snooping view ですべての VLAN の時間をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

誤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 の general query の最大応答時間を IGMP の一般的な検索インターバルよりも短く設定します。

例

VLAN 2 の IGMP snooping を有効にし、VLAN 2 の IGMP general query の最大応答時間を 5 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping max-response-time 5

関連コマンド

- **igmp-snooping enable**
- **igmp-snooping query-interval**
- **max-response-time (IGMP-snooping view)**

1.1.31 igmp-snooping overflow-replace

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping overflow-replace コマンドはポートでマルチキャストグループ置き換え機能を有効にします。

undo igmp-snooping overflow-replace コマンドはポートでマルチキャストグループ置き換え機能を無効にします。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。

IGMP snooping view で、interface view のポートまたはグローバルにすべてのポートに対して、マルチキャストグループ置き換え機能を有効にできます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます

例

GigabitEthernet 1/0/1 の VLAN2 でマルチキャストグループ置き換え機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2

関連コマンド

overflow-replace (IGMP-snooping view)

1.1.32 igmp-snooping proxy enable

Syntax

igmp-snooping proxy enable

undo igmp-snooping proxy enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping proxy enable コマンドは VLAN の IGMP snooping proxy を有効にします。

undo igmp-snooping proxy enable コマンドは VLAN の IGMP snooping proxy を無効にします。

このコマンドを実行する前に、VLAN の IGMP snooping を有効にする必要があります。

このコマンドは、マルチキャスト VLAN のサブ VLAN である VLAN には適用されません。

例

VLAN2 で、IGMP snooping を有効にし、IGMP snooping proxy を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping proxy enable

関連コマンド

- **igmp-snooping enable**
- **subvlan (multicast-VLAN view)**

1.1.33 igmp-snooping querier

Syntax

igmp-snooping querier

undo igmp-snooping querier

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping querier コマンドは IGMP snooping クエリアを有効にします。

undo igmp-snooping querier コマンドは IGMP snooping クエリアを無効にします。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

このコマンドは、マルチキャスト VLAN からサブ VLAN を削除した後、サブ VLAN に適用されます。

例

VLAN 2 の IGMP snooping を有効にし、IGMP snooping クエリアを有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping querier

関連コマンド

- **igmp-snooping enable**
- **subvlan (multicast VLAN view)**

1.1.34 igmp-snooping query-interval

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

デフォルト

125 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP general query の間隔を設定します。設定範囲は 2～300 秒です。

説明

igmp-snooping query-interval コマンドは VLAN の IGMP general query の間隔を設定します。

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 query の最大応答時間より IGMP general query の間隔を大きい値に設定してください。

例

VLAN 2 の IGMP snooping を有効にし、IGMP general query の間隔を 20 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping query-interval 20

関連コマンド

- **igmp-snooping enable**

- **igmp-snooping max-response-time**
- **igmp-snooping querier**
- **max-response-time**

1.1.35 igmp-snooping report source-ip

Syntax

igmp-snooping report source-ip *ip-address*

undo igmp-snooping report source-ip

デフォルト

VLAN では、IGMP report の送信元 IP アドレスは、現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスが設定されていない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP report の送信元 IP アドレスを指定します。

説明

igmp-snooping report source-ip コマンドは IGMP report の送信元 IP アドレスを設定します。

undo igmp-snooping report source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

例

VLAN 2 で IGMP snooping を有効にし、IGMP report の送信元 IP アドレスを 10.1.1.1 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping report source-ip 10.1.1.1

関連コマンド

igmp-snooping enable

1.1.36 igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

デフォルト

260 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: VLAN のダイナミックルータポートのエージングタイマを設定します。設定範囲は 1~8097894 秒です。

説明

igmp-snooping router-aging-time コマンドは VLAN のダイナミックルータポートのエージングタイマを設定します。

undo igmp-snooping router-aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

VLAN view で VLAN 用に、または IGMP snooping view ですべての VLAN 用にグローバルに、タイマを設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

VLAN 2 の IGMP snooping を有効にし、ダイナミックルータポートのエージングタイマを 100 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping router-aging-time 100

関連コマンド

- **igmp-snooping enable**
- **router-aging-time (IGMP-snooping view)**

1.1.37 igmp-snooping source-deny

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

デフォルト

マルチキャストソースポートフィルタリングは無効です。ポートはマルチキャストソースとマルチキャストレシーバの両方に接続することができます。

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リングを有効にします。

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リングを無効にします。

この機能は、interface view のポートまたは IGMP snooping view の指定されたポートで有効にできます。ポートについては、interface view の設定は IGMP snooping view の設定と同じプライオリティを持っており、最新の設定が有効になります。

例

GigabitEthernet 1/0/1 でマルチキャストソースポートフィルタリングを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping source-deny

関連コマンド

source-deny (IGMP-snooping view)

1.1.38 igmp-snooping special-query source-ip

Syntax

igmp-snooping special-query source-ip *ip-address*

undo igmp-snooping special-query source-ip

デフォルト

VLAN での IGMP グループ固有の query の送信元 IP アドレスは次のいずれかです。

- VLAN の IGMP snooping クエリアが IGMP general query を受信した場合、IGMP グループ固有の query の送信元アドレスです。
- IGMP snooping クエリアが IGMP general query を受信しない場合、現在の VLAN インタフェースの IP アドレスです。
- 0.0.0.0-IGMP snooping クエリアが IGMP general query を受信せず、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 query の 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 query 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 query の送信元 IP アドレス 10.1.1.1 を設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping special-query source-ip 10.1.1.1

関連コマンド

igmp-snooping enable

1.1.39 igmp-snooping static-group

Syntax

igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping static-group { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-ip *source-address*: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定した場合、ポートをマルチキャストソースとグループのスタティックグループメンバとして設定します。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グループメンバとして設定します。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グループメンバを設定します。

undo igmp-snooping static-group コマンドはスタティックグループメンバを削除します。

例

VLAN2 のマルチキャストソースとマルチキャストグループの(1.1.1.1, 225.0.0.1)のスタティックメンバポートを GigabitEthernet 1/0/1 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping version 3

[Switch-vlan2] quit

[Switch] interface GigabitEthernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping static-group 225.0.0.1 source-ip 1.1.1.1 vlan 2

1.1.40 igmp-snooping static-router-port

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port { **all** | **vlan** *vlan-id* }

デフォルト

設定なし

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

all: すべての VLAN を指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

igmp-snooping static-router-port コマンドはスタティックルータポートを設定します。

undo igmp-snooping static-router-port コマンドはスタティックルータポートを削除します。

例

VLAN 2 の GigabitEthernet 1/0/1 をスタティックルータポートに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2

1.1.41 igmp-snooping version

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

デフォルト

2

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

version-number: IGMP snooping のバージョンを指定します。2 あるいは 3 です。

説明

igmp-snooping version コマンドは VLAN の 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。

VLAN view で VLAN のバージョンを指定するか、IGMP snooping view で指定した VLAN のバージョンを指定できます。VLAN 固有の設定は、IGMP snooping view での設定と同じ優先度を持ち、最新の設定が有効になります。

例

VLAN 2 の IGMP snooping を有効にし、IGMP snooping のバージョンを 3 に指定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping version 3

関連コマンド

igmp-snooping enable

1.1.42 last-member-query-interval (IGMP-snooping view)

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

デフォルト

1 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP last member query の間隔を設定します。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 query の間隔を設定します。

undo last-member-query-interval コマンドはデフォルトに戻します。

VLAN view で VLAN の間隔を設定するか、IGMP snooping view ですべての VLAN をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

IGMP last member query の間隔を 3 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] last-member-query-interval 3

関連コマンド

igmp-snooping last-member-query-interval

1.1.43 mac-address multicast

Syntax

system view:

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [**multicast**] [[*mac-address* [**interface** *interface-list*]] **vlan** *vlan-id*]

Layer 2 aggregate interface view あるいは 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: H-H-H の形式で、スタティックマルチキャスト MAC アドレスを指定します。未使用のマルチキャスト MAC アドレスを指定する必要があります。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が 1 である MAC アドレスです。

interface interface-list: 最大 4 つのインタフェース項目をスペースで区切ってリストを指定します。各項目は、*start-interface-type interface-number* **to** *end-interface-type interface-number.*の形式でインタフェースまたはインタフェースリストを指定します。*interface-type interface-number* パラメータには、インタフェースをタイプと番号で指定します。使用可能なインタフェースタイプには、レイヤ 2 Ethernet インタフェースとレイヤ 2 アグリゲートインタフェースがあります。

vlan *vlan-id*: 既存の VLAN を VLAN ID で指定します。設定範囲は 1～4094 です。指定したインタフェースが VLAN に属していない場合は、プロンプトが表示されます。

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 の指定されたインタフェースまたは interface view の現在のインタフェースに対して、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できます。

undo mac-address コマンドに **multicast** キーワードを指定しない場合、すべてのスタティックユニキャスト MAC アドレスエントリとスタティックマルチキャスト MAC エントリが削除されます。

例

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。エントリでは、マルチキャスト MAC アドレスは 0100-0001-0001 で、発信ポートは VLAN 2 の GigabitEthernet 1/0/1 から GigabitEthernet 1/0/5 です。

<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 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します。エントリでは、マルチキャスト MAC アドレスは 0100-0001-0001 であり、発信ポートは VLAN 2 に属する GigabitEthernet 1/0/1 です。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address multicast 0100-0001-0001 vlan 2

関連コマンド

display mac-address multicast

1.1.44 max-response-time (IGMP-snooping view)

Syntax

max-response-time *seconds*

undo max-response-time

デフォルト

10 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds: IGMP general query 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 query 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。

VLAN view で VLAN の時間を設定するか、IGMP snooping view ですべての VLAN の時間をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

誤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 query の最大応答時間を IGMP の一般的な検索インターバルよりも小さい値を設定します。

例

グローバルで IGMP general query の最大応答時間を 5 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] max-response-time 5

関連コマンド

- **igmp-snooping max-response-time**
- **igmp-snooping query-interval**

1.1.45 overflow-replace (IGMP-snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

デフォルト

無効

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

overflow-replace コマンドはグローバルでマルチキャストグループ置き換え機能を有効にします。

undo overflow-replace コマンドはグローバルでマルチキャストグループ置き換え機能を無効にします。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。IGMP snooping view のすべてのポートまたは interface view のポートに対して、グローバルにマルチキャストグループ置き換え機能を有効にできます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

例

VLAN2 でマルチキャストグループ置き換え機能を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] overflow-replace vlan 2

関連コマンド

igmp-snooping overflow-replace

1.1.46 report-aggregation (IGMP-snooping view)

Syntax

report-aggregation

undo report-aggregation

デフォルト

有効

View

IGMP-snooping view

定義済みユーザロール

network-admin

説明

report-aggregation コマンドは IGMP report 抑制機能を有効にします。

undo report-aggregation コマンドは IGMP report 抑制機能を無効にします。

例

IGMP report 抑制機能を無効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] undo report-aggregation

1.1.47 reset igmp-snooping group

Syntax

reset igmp-snooping group { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-address: マルチキャストソースの IP アドレスを指定します。指定しない場合、すべてのマルチキャストソースのダイナミック IGMP snooping グループエントリに関する情報を削除します。

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 グループエントリに関する情報を削除します。

説明

reset igmp-snooping group コマンドはダイナミック IGMP snooping グループエントリに関する情報を削除します。

例

すべてのダイナミック IGMP snooping グループエントリに関する情報を削除します。

<Switch> reset igmp-snooping group all

関連コマンド

display igmp-snooping group

1.1.48 reset igmp-snooping router-port

Syntax

reset igmp-snooping router-port { **all** | **vlan** *vlan-id* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべてのダイナミックルータポートを指定します。

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を削除します。

例

すべてのダイナミックルータポートを削除します。

<Switch> reset igmp-snooping router-port all

関連コマンド

display igmp-snooping router-port

1.1.49 reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

定義済みユーザロール

network-admin

説明

reset igmp-snooping statistics コマンドは IGMP snooping によって学習した IGMP メッセージと PIMv2 hello メッセージの統計情報を削除します。

例

IGMP snooping によって学習した IGMP メッセージと PIMv2 hello メッセージの統計情報を削除します。

<Switch> reset igmp-snooping statistics

関連コマンド

display igmp-snooping statistics

1.1.50 router-aging-time (IGMP-snooping view)

Syntax

router-aging-time *seconds*

undo router-aging-time

デフォルト

260 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds: ダイナミックルータポートのエージングタイマを設定します。設定範囲は 1~8097894 秒です。

説明

router-aging-time コマンドはグローバルでダイナミックルータポートのエージングタイマを設定します。

undo router-aging-time コマンドはデフォルトに戻します。

IGMP snooping view ですべての VLAN に対してグローバルに、または VLAN view で VLAN に対してタイマを設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

グローバルでダイナミックルータポートのエージングタイマを 100 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] router-aging-time 100

関連コマンド

igmp-snooping router-aging-time

1.1.51 source-deny (IGMP-snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

デフォルト

無効

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

port *interface-list*: ポートリストを指定します。ポートのアイテムを半角スペースで区切り、ポートのタイプと番号を指定するか、ポートの範囲で指定します。ポートを範囲で指定する形式は *start-interface-type interface-number* **to** *end-interface-type interface-number* です。

説明

source-deny コマンドはすべての受信したマルチキャストデータパケットを廃棄するため、ポートでマルチキャストソースポートのフィルタリングを有効にします。

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リングを無効にします。

この機能は、IGMP snooping view で指定されたポート、または interface view のポートで有効にできます。ポートについては、IGMP snooping view の設定は interface view の設定と同じ優先度を持ち、最新の設定が有効になります。

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リングを有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

関連コマンド

igmp-snooping source-deny

目次

このセクションのページは **6-x-x** です。

2 章 マルチキャスト VLAN 2-1
2.1 マルチキャスト VLAN 設定コマンド 2-1
2.1.1 display multicast-vlan 2-1
2.1.2 display multicast-vlan forwarding-table 2-2
2.1.3 display multicast-vlan group 2-4
2.1.4 multicast-vlan 2-6
2.1.5 multicast-vlan entry-limit 2-8
2.1.6 port (multicast-VLAN view) 2-9
2.1.7 port multicast-vlan 2-10
2.1.8 reset multicast-vlan group 2-10
2.1.9 subvlan (multicast-VLAN view) 2-11

2章 マルチキャスト VLAN

2.1 マルチキャストVLAN設定コマンド

2.1.1 display multicast-vlan

Syntax

display multicast-vlan [*vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのマルチキャスト VLAN の情報を表示します。

説明

display multicast-vlan コマンドはマルチキャスト VLAN の情報を表示します。

例

すべてのマルチキャスト VLAN の情報を表示します。

<Switch> display multicast-vlan

```
Total 2 multicast VLANs.

Multicast VLAN 100:
  Sub-VLAN list(3 in total):
    2-3, 6
  Port list(3 in total):
    GE1/0/1
    GE1/0/2
    GE1/0/3

Multicast VLAN 200:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
```

表 2-1 コマンド出力

フィールド	説明
Total 2 multicast VLANs	マルチキャストVLANの総数です。
Sub-VLAN list(3 in total)	マルチキャストVLANのサブVLANと、サブVLANの総数です。
Port list(3 in total)	マルチキャストVLANのポートリストとポートの総数です。

2.1.2 display multicast-vlan forwarding-table

Syntax

display multicast-vlan forwarding-table [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.0.0～239.255.255.255 です。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのマルチキャスト VLAN 転送エントリを表示します。

mask { *mask-length* | *mask* }: マルチキャストグループアドレスのマスク長あるいはサブネットマスクを指定します。マスク長の設定範囲は 4～32 です。デフォルトは 32 です。マスクのデフォルトは 255.255.255.255 です。

source-address: マルチキャスト送信元の IP アドレスを指定します。マルチキャスト送信元を指定しない場合、すべてのマルチキャスト送信元のマルチキャスト VLAN 転送エントリを表示します。

mask { *mask-length* | *mask* }: マルチキャスト送信元アドレスのマスク長あるいはサブネットマスクを指定します。マスク長の設定範囲は 0～32 です。デフォルトは 32 です。マスクのデフォルトは 255.255.255.255 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のマルチキャスト VLAN 転送エントリを表示します。

subvlan *vlan-id*: サブ VLAN の ID を指定します。指定しない場合、すべてのサブ VLAN のマルチキャスト VLAN 転送エントリを表示します。

vlan *vlan-id*: マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのマルチキャスト VLAN のマルチキャスト VLAN 転送エントリを表示します。

説明

display multicast-vlan forwarding-table コマンドはマルチキャスト VLAN 転送エントリを表示します。

例

すべてのマルチキャスト VLAN 転送エントリを表示します。

<Switch> display multicast-vlan forwarding-table

```
Multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1.1.1.1, 225.0.0.1)
    Flags: 0x10000
    Multicast VLAN: 100
    List of sub-VLANs (3 in total):
      1: VLAN 10
      2: VLAN 20
      3: VLAN 30
```

表 2-2 コマンド出力

フィールド	説明
Multicast VLAN 100 Forwarding Table	マルチキャストVLAN 100の転送テーブルです。
Total 1 entries, 1 matched	転送エントリ（S,G）の数と一致するエントリの数です。
00001	（S,G）エントリのシーケンス番号です。
(1.1.1.1, 255.0.0.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャスト送信元を示します。

フィールド	説明
Flags	エントリの現在の状態です。このフィールドは、1つのフラグあるいは複数のフラグの合計を表示します。たとえば、0x10000の場合、エントリは0x10000のフラグのみであることを意味します。 エントリでは次のフラグを使用できます。 • **0x1**–エントリが非アクティブ状態です。 • **0x4**–エントリがアップデートに失敗しています。 • **0x8**–エントリがサブVLAN情報のアップデートに失敗しています。 • **0x200**–エントリが円滑な状態です。 • **0x10000**–エントリがマルチキャストVLAN転送エントリです。
List of sub-VLANs (3 in total)	マルチキャストVLANのサブVLANとサブVLANの総数です。

2.1.3 display multicast-vlan group

Syntax

display multicast-vlan group [*source-address* | *group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

source-address: マルチキャスト送信元の IP アドレスを指定します。マルチキャスト送信元を指定しない場合、マルチキャスト VLAN のすべてのマルチキャスト送信元のマルチキャストグループの情報を表示します。

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。マルチキャストグループを指定しない場合、マルチキャスト VLAN のすべてのマルチキャストグループの情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のマルチキャスト VLAN のマルチキャストグループの情報を表示します。

verbose: 詳細情報を表示します。

vlan *vlan-id*: マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのマルチキャスト VLAN のマルチキャストグループの情報を表示します。

説明

display multicast-vlan group コマンドはマルチキャスト VLAN のマルチキャストグループの情報を表示します。

例

すべてのマルチキャスト VLAN のすべてのマルチキャストグループの詳細情報を表示します。

<Switch> display multicast-vlan group verbose

```
Total 6 entries.

Multicast VLAN 10: Total 3 entries.
  (2.2.2.2, 225.1.1.2)
    Flags: 0x70000020
    Sub-VLANs (1 in total):
      VLAN 40
  (111.112.113.115, 225.1.1.4)
    Flags: 0x70000030
    Sub-VLANs (1 in total):
      VLAN 40
  (0.0.0.0, 226.1.1.6)
    Flags: 0x60000020
    Sub-VLANs (1 in total):
      VLAN 40

Multicast VLAN 20: Total 3 entries.
  (2.2.2.2, 225.1.1.2)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (111.112.113.115, 225.1.1.4)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (0.0.0.0, 226.1.1.6)
    Flags: 0x50000010
    Sub-VLANs (0 in total):
```

表 2-3 コマンド出力

フィールド	説明
Total 6 entries	（S,G）エントリの総数です。
Multicast VLAN 10: Total 3 entries	マルチキャストVLAN 10の（S,G）エントリの総数です。
(0.0.0.0, 226.1.1.6)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャスト送信元を示します。
Flags	エントリの現在の状態です。このフィールドは、1つのフラグあるいは複数のフラグの合計を表示します。たとえば、0x70000020の場合、エントリは0x20、0x10000000、0x20000000、0x40000000のフラグがあることを意味します。 エントリでは次のフラグを使用できます。 ● **0x10**—エントリがマルチキャストVLANによって作成されました。 ● **0x20**—エントリがマルチキャストVLANのサブVLANによって作成されました。 ● **0x40**—エントリが削除されました。 ● **0x10000000**—この値は以下の状態の1つを示します。 　■ エントリが新規に作成されました。 　■ 装置は（S,G）エントリに一致するIGMP queryを受信しましたが、IGMP general query送信間隔内に一致するIGMPv1 reportを受信していません。 ● **0x20000000**—装置はIGMP general query送信間隔内に（S,G）エントリに一致するIGMPv2あるいはIGMPv3 reportを受信していません。 ● **0x40000000**—装置はIGMP general query送信間隔内に（S,G）エントリに一致するIGMPv3 IS_EX (NULL) reportを受信していません。
Sub-VLANs (1 in total)	マルチキャストVLANのサブVLANとサブVLANの総数です。

関連コマンド

reset multicast-vlan group

2.1.4 multicast-vlan

Syntax

multicast-vlan *vlan-id*

undo multicast-vlan { **all** | *vlan-id* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべてのマルチキャスト VLAN を指定します。

説明

multicast-vlan コマンドはマルチキャスト VLAN を設定し、その view に移行するか、またはデフォルトの multicast VLAN view に移行します。

undo multicast-vlan コマンドはマルチキャスト VLAN を削除します。

IP マルチキャストルーティングが有効な装置で、マルチキャスト VLAN の設定を行わないことを推奨します。

装置のマルチキャスト VLAN の総数はシステムがサポートする最大数を超過することができません。

VLAN をマルチキャスト VLAN として設定するには、IGMP snooping を有効にする必要があります。

例

VLAN 100 で IGMP snooping を有効にします。マルチキャスト VLAN として VLAN 100 を設定し、multicast VLAN view に移行します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 100

[Switch-vlan100] igmp-snooping enable

[Switch-vlan100] quit

[Switch] multicast-vlan 100

[Switch-mvlan-100]

関連コマンド

igmp-snooping enable

2.1.5 multicast-vlan entry-limit

Syntax

multicast-vlan entry-limit *limit*

undo multicast-vlan entry-limit

デフォルト

4000

View

System view

定義済みユーザロール

network-admin

パラメータ

limit: マルチキャスト VLAN 転送エントリの最大数を設定します。設定範囲は 0～4000 です。

説明

multicast-vlan entry-limit コマンドはマルチキャスト VLAN 転送エントリの最大数を設定します。

undo multicast-vlan entry-limit コマンドはデフォルトに戻します。

設定された値がマルチキャスト VLAN 転送エントリの現在の数より小さい場合、いくつかのエントリがエイジアウトするか、手動で削除されるまで、装置は新しいエントリを作成できません。新しいエントリをすぐに作成できるようにするには、**reset multicast-vlan group** コマンドを使用して、マルチキャスト VLAN 転送エントリを削除します。

例

マルチキャスト VLAN 転送エントリの最大数を 128 に設定します。

<Switch> system-view

[Switch] multicast-vlan entry-limit 128

関連コマンド

entry-limit (IGMP-snooping view)

2.1.6 port (multicast-VLAN view)

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

デフォルト

設定なし

View

Multicast VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list: ポートあるいはポート範囲を指定します。形式は *interface-type interface-number* です。ポート範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。

all: 現在のマルチキャスト VLAN のすべてのユーザポートを指定します。

説明

port コマンドはマルチキャスト VLAN にユーザポートを割り当てます。

undo port コマンドはマルチキャスト VLAN からユーザポートを取り外します。

マルチキャスト VLAN に割り当てることができるのは、レイヤ 2 Ethernet ポートまたはレイヤ 2 アグリゲートインタフェースだけです。さらに、ポートを 1 つのマルチキャスト VLAN だけに割り当てることができます。

ポートがマルチキャスト VLAN に割り当てられるためには、ポートが属する VLAN の IGMP snooping を有効にする必要があります。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 をマルチキャスト VLAN 100 に割り当てます。

<Switch> system-view

[Switch] multicast-vlan 100

[Switch-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3

2.1.7 port multicast-vlan

Syntax

port multicast-vlan *vlan-id*

undo port multicast-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

port multicast-vlan コマンドはマルチキャスト VLAN にポートを割り当てます。

undo port multicast-vlan コマンドはデフォルトに戻します。

ポートは 1 つのマルチキャスト VLAN にのみ所属することができます。

ポートをマルチキャスト VLAN に割り当てるためには、ポートが所属する VLAN の IGMP snooping を有効にする必要があります。

例

GigabitEthernet 1/0/1 をマルチキャスト VLAN 100 に割り当てます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

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

2.1.8 reset multicast-vlan group

Syntax

reset multicast-vlan group [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **vlan** *vlan-id*] *

View

User view

定義済みユーザロール

network-admin

パラメータ

source-address: マルチキャスト送信元の IP アドレスを指定します。マルチキャスト送信元を指定しない場合、マルチキャスト VLAN のすべてのマルチキャスト送信元へのマルチキャストグループを削除します。

mask { *mask-length* | *mask* }: マルチキャスト送信元アドレスのマスク長あるいはサブネットマスクを指定します。マスク長の設定範囲は 0～32 です。デフォルトは 32 です。マスクのデフォルトは 255.255.255.255 です。

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。マルチキャストグループを指定しない場合、マルチキャスト VLAN のすべてのマルチキャストグループを削除します。

mask { *mask-length* | *mask* }: マルチキャストグループアドレスのマスク長あるいはサブネットマスクを指定します。マスク長の設定範囲は 4～32 です。デフォルトは 32 です。マスクのデフォルトは 255.255.255.255 です。

vlan *vlan-id*: マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのマルチキャスト VLAN のマルチキャストグループを削除します。

説明

reset multicast-vlan group コマンドはマルチキャスト VLAN のマルチキャストグループを削除します。

例

すべてのマルチキャスト VLAN のマルチキャストグループを削除します。

<Switch> reset multicast-vlan group

関連コマンド

display multicast-vlan group

2.1.9 subvlan (multicast-VLAN view)

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

デフォルト

設定なし

View

Multicast VLAN view

定義済みユーザロール

network-admin

パラメータ

vlan-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定された VLAN は存在する必要があり、マルチキャスト VLAN または他のマルチキャスト VLAN のサブ VLAN にすることはできません。

all: 現在のマルチキャスト VLAN のすべてのサブ VLAN を指定します。

説明

subvlan コマンドはマルチキャスト VLAN にサブ VLAN を割り当てます。

undo subvlan コマンドはマルチキャスト VLAN からサブ VLAN を削除します。

VLAN をサブ VLAN として設定するには、IGMP snooping を有効にする必要があります。

例

マルチキャスト VLAN 100 のサブ VLAN として VLAN 10～VLAN 15 を設定します。

<Switch> system-view

[Switch] multicast-vlan 100

[Switch-mvlan-100] subvlan 10 to 15

目次

このセクションのページは **6-x-x** です。

3 章 MLD スヌーピング 3-1
3.1 MLD スヌーピング設定コマンド 3-1
3.1.1 display ipv6 l2-multicast ip 3-1
3.1.2 display ipv6 l2-multicast ip forwarding 3-3
3.1.3 display ipv6 l2-multicast mac 3-4
3.1.4 display ipv6 l2-multicast mac forwarding 3-5
3.1.5 display mld-snooping 3-6
3.1.6 display mld-snooping group 3-10
3.1.7 display mld-snooping router-port 3-11
3.1.8 display mld-snooping static-group 3-13
3.1.9 display mld-snooping static-router-port 3-15
3.1.10 display mld-snooping statistics 3-16
3.1.11 dot1p-priority (MLD-snooping view) 3-17
3.1.12 enable (MLD-snooping view) 3-18
3.1.13 entry-limit (MLD-snooping view) 3-19
3.1.14 fast-leave (MLD-snooping view) 3-20
3.1.15 group-policy (MLD-snooping view) 3-21
3.1.16 host-aging-time (MLD-snooping view) 3-23
3.1.17 last-listener-query-interval (MLD-snooping view) 3-24
3.1.18 max-response-time (MLD-snooping view) 3-25
3.1.19 mld-snooping 3-26
3.1.20 mld-snooping done source-ip 3-26
3.1.21 mld-snooping dot1p-priority 3-27
3.1.22 mld-snooping drop-unknown 3-28
3.1.23 mld-snooping enable 3-29
3.1.24 mld-snooping fast-leave 3-30
3.1.25 mld-snooping general-query source-ip 3-31
3.1.26 mld-snooping group-limit 3-32
3.1.27 mld-snooping group-policy 3-33
3.1.28 mld-snooping host-aging-time 3-35
3.1.29 mld-snooping host-join 3-37
3.1.30 mld-snooping last-listener-query-interval 3-38
3.1.31 mld-snooping max-response-time 3-39
3.1.32 mld-snooping overflow-replace 3-40
3.1.33 mld-snooping querier 3-41
3.1.34 mld-snooping query-interval 3-42

3.1.35 mld-snooping report source-ip 3-43
3.1.36 mld-snooping router-aging-time 3-44
3.1.37 mld-snooping source-deny 3-45
3.1.38 mld-snooping special-query source-ip 3-46
3.1.39 mld-snooping static-group 3-47
3.1.40 mld-snooping static-router-port 3-49
3.1.41 mld-snooping version 3-49
3.1.42 overflow-replace (MLD-snooping view) 3-50
3.1.43 report-aggregation (MLD-snooping view) 3-51
3.1.44 reset mld-snooping group 3-52
3.1.45 reset mld-snooping router-port 3-53
3.1.46 reset mld-snooping statistics 3-54
3.1.47 router-aging-time (MLD-snooping view) 3-54
3.1.48 source-deny (MLD-snooping view) 3-55
3.1.49 version (MLD-snooping view) 3-56

3章 MLD スヌーピング

3.1 MLDスヌーピング設定コマンド

3.1.1 display ipv6 l2-multicast ip

Syntax

display ipv6 l2-multicast ip [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *ipv6-group-address*: IPv6 マルチキャストグループを IPv6 アドレスで指定します。IPv6 マルチキャストグループを指定しない場合、このコマンドはすべてのレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

source *ipv6-source-address*: IPv6 アドレスで IPv6 マルチキャスト送信元を指定します。IPv6 マルチキャスト送信元を指定しない場合、このコマンドはすべての IPv6 マルチキャストソースのレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

vlan *vlan-id*: VLAN ID で VLAN を指定します。設定範囲は 1～4094 です。VLAN を指定しない場合、このコマンドは、すべての VLAN のレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置のレイヤ 2 IP マルチキャストグループの情報を表示します。

説明

display ipv6l2-multicast ip コマンドはレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

例

VLAN2 のレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

<Switch> display ipv6 l2-multicast ip vlan 2

```
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
   (::, FF1E::101)
    Attribute: static, success
    Host ports (1 in total):
      GE1/0/1                          (S, SUC)
```

表 3-1 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPv6マルチキャストグループの総数です。
VLAN 2: Total 1 entries	VLAN2のレイヤ2 IPv6マルチキャストグループの総数です。
(::, FF1E::101)	(S, G)エントリ。S位置の二重コロン(:)は、すべてのIPv6マルチキャストソースを意味します。
Attribute	エントリ属性です。 • **dynamic**ーエントリはダイナミックプロトコルによって作成されます。 • **static**ーエントリはスタティックプロトコルによって作成されます。 • **pim**ーエントリは IPv6 PIM によって作成されます。PIM および IPv6 PIM は QX-S5300G シリーズではサポートしていません。 • **kernel**ーエントリはカーネルから取得されます。 • **success**ー処理に成功しました。 • **fail**ー処理に失敗しました。
Host ports (1 in total)	メンバポートおよびメンバポートの総数です。
(S, SUC)	ポート属性です。 • **D**ーダイナミックポートです。 • **S**ースタティックポートです。 • **P**ーIPv6PIM ポートです。PIM および IPv6 PIM は QX-S5300G シリーズではサポートしていません。 • **K**ーカーネルから取得されたポートです。 • **R**ー(*、*)エントリから学習したポートです。 • **W**ー(*,G 様)エントリから学習したポートです。 • **SUC**ー処理に成功しました。 • **F**ー処理に失敗しました。

3.1.2 display ipv6 l2-multicast ip forwarding

Syntax

display ipv6 l2-multicast ip forwarding [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *ipv6-group-address*: IPv6 マルチキャストグループの IPv6 アドレスを指定します。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループのレイヤ 2 IPv6 マルチキャスト IP フォワーディング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 IP フォワーディングエントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のレイヤ 2 IPv6 マルチキャスト IP フォワーディングエントリを表示します。

説明

display ipv6 l2-multicast ip forwarding コマンドはレイヤ 2 IPv6 マルチキャストグループエントリを表示します。

例

VLAN2 のレイヤ 2IPv6 マルチキャスト IP フォワーディングエントリを表示します。

<Switch> display ipv6 l2-multicast ip forwarding vlan 2

```
Total 1 entries.

VLAN 2: Total 1 entries.
   (::, FF1E::101)
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
```

```
GigabitEthernet1/0/3
```

表 3-2 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPv6マルチキャストグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2 IPv6マルチキャストグループエントリの総数です。
(::, FF1E::101)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャストソースを示します。
Host ports (3 in total)	メンバポートとメンバポートの総数です。

3.1.3 display ipv6 l2-multicast mac

Syntax

display ipv6 l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: IPv6 MAC アドレスで IPv6 MAC マルチキャストグループを指定します。指定しない場合、すべての IPv6 MAC マルチキャストグループの IPv6 MAC マルチキャストグループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN の IPv6 MAC マルチキャストグループエントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の IPv6 MAC マルチキャストグループエントリを表示します。

説明

display ipv6 l2-multicast mac コマンドはレイヤ 2IPv6 マルチキャスト MAC マルチキャストグループの情報を表示します。

例

VLAN2 のレイヤ 2 IPv6 マルチキャスト MAC マルチキャストグループの情報を表示します。

<Switch> display ipv6 l2-multicast mac vlan 2

```
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 3333-0000-0101
    Attribute: success
    Host ports (1 in total):
      GE1/0/1
```

表 3-3 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPv6MACマルチキャストグループの総数です。
VLAN 2: Total 1 entries	VLAN2内のレイヤ2 IPv6MACマルチキャストグループの総数です。
MAC group address	レイヤ2 IPv6MACマルチキャストグループのIPv6アドレスです。
Attribute	エントリ属性です。 • **success**–処理に成功しました。 • **fail**–処理に失敗しました。
Host ports (1 in total)	メンバポートおよびメンバポートの総数です。

3.1.4 display ipv6 l2-multicast mac forwarding

Syntax

display ipv6 l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: IPv6 MAC アドレスで IPv6 MAC マルチキャストグループを指定します。指定しない場合、すべての IPv6 MAC マルチキャストグループの IPv6 MAC マルチキャストグループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN の IPv6 MAC マルチキャストグループエントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の IPv6 MAC マルチキャストグループエントリを表示します。

説明

display ipv6 l2-multicast mac forwarding コマンドは IPv6 MAC マルチキャストグループエントリを表示します。

例

VLAN2 のレイヤ 2 IPv6 マルチキャスト MAC 転送エントリを表示します。

<Switch> display ipv6 l2-multicast mac forwarding vlan 2

```
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 3333-0000-0101
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

表 3-4 コマンド出力

フィールド	説明
Total 1 MAC entries	IPv6 MACマルチキャストグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のIPv6 MACマルチキャストグループエントリの総数です。
MAC group address	IPv6 MACマルチキャストグループのアドレスです。
Host ports (3 in total)	メンバポートとメンバポートの総数です。

3.1.5 display mld-snooping

Syntax

display mld-snooping [**global** | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルの MLD snooping の状態を表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

display mld-snooping コマンドは MLD snooping の状態を表示します。

パラメータを指定しない場合、グローバルとすべての VLAN の MLD snooping の状態を表示します。

例

すべての VLAN のグローバル MLD snooping の状態および MLD snooping の状態を表示します。

<Switch> display mld-snooping

```
MLD snooping information: Global
  Global-enable: Enabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Report-aggregation: Enabled
 Host-tracking: Disabled
 Dot1p-priority: --

MLD snooping information: VLAN 1
 MLD snooping: Enabled
 Drop-unknown: Disabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Querier: Enabled (IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
```

```
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
 Report source IP: FE80::2FF:FFFF:FE00:2
 Done source IP: FE80::2FF:FFFF:FE00:3
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

MLD snooping information: VLAN 10
 MLD snooping: Enabled
 Drop-unknown: Enabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Querier: Enabled (IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
 Report source IP: FE80::2FF:FFFF:FE00:2
 Done source IP: FE80::2FF:FFFF:FE00:3
 Host-tracking: Disabled
 Dot1p-priority: --
 Proxy: Disabled
```

表 3-5 コマンド出力

フィールド	説明
MLD snooping	MLD snoopingの状態です。 • **Enabled**－有効です。 • **Disabled**－無効です。
Drop-unknown	未知のIPv6マルチキャストデータの廃棄機能の状態です。 • **Enabled**－有効です。 • **Disabled**－無効です。
Version	MLD snoopingのバージョンです。
Host-aging-time	ダイナミックメンバポートのエージングタイマです。
Router-aging-time	ダイナミックルータポートのエージングタイマです。
Max-response-time	MLD general queryの最大応答時間です。

フィールド	説明
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802.1 pの優先度です。802.1 pの優先度が設定されていない場合、このフィールドには二つのハイフン(--)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。
(IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)	MLD snoopingクエリア情報です。 ● **IP**－MLD snoopingクエリアのIPアドレスです。 ● **Expire**－MLD snoopingクエリアの残りエージングタイムです。 このフィールドは、MLD snoopingクエリア選択が無効になっている場合は表示されません。
Querier-election	MLD snoopingクエリア選択の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Query-interval	MLD general queryの送信間隔です。
General-query source IP	MLD general queryの送信元IPアドレスです。
Special-query source IP	MLD multicast-address-specific queryの送信元IPアドレスです。
Report source IP	MLD reportの送信元IPアドレスです。
Done source IP	MLD done messageの送信元IPアドレスです。
Host-tracking	ホスト追跡の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Proxy	MLD snoopingプロキシの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。

3.1.6 display mld-snooping group

Syntax

display mld-snooping group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループのダイナミック MLD snooping グループエントリを表示します。

ipv6-source-address: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定しない場合、すべての IPv6 マルチキャストソースのダイナミック MLD snooping 転送エントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミック MLD snooping 転送エントリを表示します。

verbose: 詳細な情報を表示します。指定しない場合、概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のダイナミック MLD snooping 転送エントリを表示します。

説明

display mld-snooping group コマンドはダイナミック MLD snooping 転送エントリを表示します。

例

VLAN2 のダイナミック MLD snooping グループエントリの詳細情報を表示します。

<Switch> display mld-snooping group vlan 2 verbose

```
Total 1 entries.

VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
```

```
Host slots (0 in total):
Host ports (1 in total):
  GE1/0/2                          (00:03:23)
```

表 3-6 コマンド出力

フィールド	説明
Total 1 entries	ダイナミックMLD snoopingグループ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。
Attribute	エントリ属性です。 • **global port**—エントリにグローバルポートがあります。 • **local port**—エントリに指定された装置上のポートがあります。 • **slot**—エントリに指定された装置以外の装置上のポートがあります。
FSM information	エントリの有限状態装置（Finite state machine）情報です。 • **delete**—エントリの属性が削除されています。 • **dummy**—エントリが新規で一時的なエントリです。 • **no info**—エントリが存在しません。
Host slots (0 in total)	メンバポートを持つメンバ装置のメンバIDと、(指定のメンバ装置を除く)メンバ装置の総数です。
Host ports (1 in total)	メンバポートとメンバポートの総数です。
(00:03:23)	ダイナミックメンバポートの残りのエージング時間です。IRFスタック装置では以下のように表示されます。 • ポートは指定されたメンバ装置上にあります。 • ポートはマスタ装置上にあり、メンバ装置が指定されていません。

関連コマンド

reset mld-snooping group

3.1.7 display mld-snooping router-port

Syntax

display mld-snooping router-port [**vlan** *vlan-id*] [**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

verbose: ダイナミックルータポートの詳細情報を表示します。指定しない場合、ダイナミックルータポートの概要情報が表示されます。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。VLAN を指定しないと、このコマンドはすべての VLAN のスタティックルータポート情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のダイナミックルータポートの情報を表示します。

説明

display 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概要情報を表示します。

<Switch> display mld-snooping router-port vlan 2

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

表 3-7 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	メンバポートを持つメンバ装置のメンバIDと、(指定のメンバ装置を除く)メンバ装置の総数です。
Router ports (2 in total)	ダイナミックルータポートと、ダイナミックルータポートの総数です。

フィールド	説明
(00:01:30)	ダイナミックルータポートの残りのエージング時間です。 IRFスタック装置では以下のように表示されます。 • グローバルポート（レイヤ2アグリゲートインタフェースを含む）では常に表示されます。 • グローバルポートでない場合、マスタ装置のときに表示されます。マスタ装置でない場合は**slot** *slot-number*パラメータを指定することで表示します。

関連コマンド

reset mld-snooping router-port

3.1.8 display mld-snooping static-group

Syntax

display mld-snooping static-group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループのスタティック MLD snooping 転送エントリを表示します。

ipv6-source-address: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定しない場合、すべての IPv6 マルチキャストソースのスタティック MLD snooping 転送エントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のスタティック MLD snooping 転送エントリを表示します。

verbose: 詳細な情報を表示します。指定しない場合、概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のスタティック MLD snooping 転送エントリを表示します。

説明

display mld-snooping static-group コマンドはスタティック MLD snooping 転送エントリを表示します。

例

VLAN 2 のスタティック MLD snooping 転送エントリの詳細情報を表示します。

<Switch> display mld-snooping static-group vlan 2 verbose

```
Total 1 entries.

VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

表 3-8 コマンド出力

フィールド	説明
Total 1 entries	スタティックMLD snooping転送エントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のスタティックMLD snooping転送エントリの総数です。
(::, FF1E::101)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャストソースを示します。
Attribute	エントリ属性です。 ● **global port**—エントリにグローバルポートがあります。 ● **local port**—エントリに指定された装置上のポートがあります。 ● **slot**—エントリに指定された装置以外の装置上のポートがあります。
FSM information	エントリの有限状態装置（Finite state machine）情報です。 ● **delete**—エントリの属性が削除されています。 ● **dummy**—エントリが新規で一時的なエントリです。 ● **no info**—エントリが存在しません。
Host slots (0 in total)	メンバポートを持つメンバ装置のメンバIDと、(指定のメンバ装置を除く)メンバ装置の総数です。

フィールド	説明
Host ports (1 in total)	メンバポートとメンバポートの総数です。

3.1.9 display mld-snooping static-router-port

Syntax

display mld-snooping static-router-port [**vlan** *vlan-id*] [**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

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

verbose: スタティックルータポートの詳細情報を表示します。指定しない場合、このコマンドはスタティックルータポートの概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のスタティックルータポートの情報を表示します。

説明

display mld-snooping static-router-port コマンドはスタティックルータポートの情報を表示します。

例

VLAN 2 のスタティックルータポートの概要情報を表示します。

<Switch> display mld-snooping static-router-port vlan 2

```
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

VLAN2 のスタティックルータポートの詳細情報を表示します。

<Switch> display mld-snooping static-router-port vlan 2 verbose

```
VLAN 2:
  Router slots (0 in total):
```

```
Router ports (2 in total):
  GE1/0/1
  GE1/0/2
```

表 3-9 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	メンバポートを持つメンバ装置のメンバIDと、(指定のメンバ装置を除く)メンバ装置の総数です。
Router ports (2 in total)	スタティックルータポートとスタティックルータポートの総数です。

3.1.10 display mld-snooping statistics

Syntax

display mld-snooping statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mld-snooping statistics コマンドは MLD snooping によって学習した MLD メッセージの統計情報を表示します。

例

MLD snooping によって学習した MLD メッセージと IPv6 PIM hello メッセージの統計情報を表示します。

<Switch> display mld-snooping statistics

```
Received MLD general queries:  0
Received MLDv1 specific queries:  0
Received MLDv1 reports:  0
Received MLD dones:  0
Sent     MLDv1 specific queries:  0
Received MLDv2 reports:  0
Received MLDv2 reports with right and wrong records:  0
Received MLDv2 specific queries:  0
```

```
Received MLDv2 specific sg queries:  0
Sent     MLDv2 specific queries:  0
Sent     MLDv2 specific sg queries:  0
Received IPv6 PIM hello:  0
Received error MLD messages:  0
```

表 3-10 コマンド出力

フィールド	説明
general queries	MLD general queryの数です。
specific queries	MLD multicast-address-specific query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 queryの数です。
IPv6 PIM hello	IPv6 PIM helloメッセージの数です。
error MLD messages	エラーがあるMLDメッセージの数です。

関連コマンド

reset mld-snooping statistics

3.1.11 dot1p-priority (MLD-snooping view)

Syntax

dot1p-priority *priority*

undo dot1p-priority

デフォルト

MLD メッセージの 802.1p 優先度は設定されていません。装置によって作成された MLD メッセージの場合、802.1p 優先度は 0 です。転送される MLD メッセージの場合、装置は 802.1p 優先度を変更しません。

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

priority: MLD メッセージの 802.1 p の優先度を指定します。設定範囲は 0～7 です。値が大きいほど、優先順位が高くなります。

説明

dot1p-priority コマンドは MLD メッセージの 802.1 p の優先度をグローバルに設定します。

undo dot1p-priority コマンドは設定をデフォルトに戻します。

MLD snooping view のすべての VLAN または VLAN view の VLAN に対して、802.1p 優先度をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

MLD メッセージの 802.1 p の優先度をグローバルに 3 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] dot1p-priority 3

関連コマンド

mld-snooping dot1p-priority

3.1.12 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。

VLAN の MLD snooping を有効にする前に、**mld-snooping** コマンドを使用して MLD snooping 機能を有効にする必要があります。

MLD-snooping view でこのコマンドを使用すると、複数の VLAN に対して MLD snooping を有効にできます。VLAN view で **mld-snooping enable** コマンドを使用すると、VLAN に対して MLD snooping を有効にできます。VLAN view の設定は MLD-snooping view の設定と同じ優先度を持ち、最新の設定が有効になります。

例

MLD snooping 機能を有効にし、次に VLAN10 を介して VLAN2 の MLD snooping を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] enable vlan 2 to 10

関連コマンド

- **mld-snooping**
- **mld-snooping enable**

3.1.13 entry-limit (MLD-snooping view)

Syntax

entry-limit *limit*

undo entry-limit

デフォルト

4294967295

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

limit: MLD snooping 転送エントリのグローバルの最大数を指定します。設定範囲は 0～4294967295 です。

説明

entry-limit コマンドはダイナミックエントリとスタティックエントリを含む MLD snooping 転送エントリのグローバルの最大数を設定します。

undo entry-limit コマンドはデフォルトに戻します。

例

MLD snooping 転送エントリのグローバルの最大数を 512 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] entry-limit 512

3.1.14 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。

fast-leave は、ポートが完了メッセージを受信した時、装置がすぐに IPv6 マルチキャストグループの転送エントリからポートを削除することを可能にします。

fast-leave 処理は、MLD snooping view のすべてのポートまたは interface view のポートに対してグローバルに有効にできます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

例

VLAN2 の MLD Snooping の fast-leave 処理をグローバルに有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] fast-leave vlan 2

関連コマンド

mld-snooping fast-leave

3.1.15 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 に対して適用します。

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、ホストが参加できる IPv6 マルチキャストグループを制御するために、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、このコマンドはスタティックメンバポートには影響しません。

IPv6 マルチキャストグループポリシーは、MLD-snooping view 内のすべてのポート、または interface view のポートに対してグローバルに設定できます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

IPv6 ACL でルールを設定する場合は、次の制限とガイドラインに従ってください。

- 標準 ACL では、*source source-address source-prefix* オプションは、IPv6 マルチキャストグループアドレスを指定します。
- 詳細 ACL では、**source** *source-address source-prefix* オプションは 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* オプションは、IPv6 マルチキャストグループアドレスを指定します。

  IPv6 マルチキャスト送信元アドレスを持たない MLDv1 レポート、MLDv2IS_EX および MLDv2TO_EX レポートに一致させるには、**source** *source-address source-prefix* オプションを 0 :: 0 に設定します。
- その他のオプションパラメータのうち、**fragment** と time-range *time-range-name* オプションだけが有効になります。

異なる VLAN のすべてのポートに異なる ACL を設定できます。同じ VLAN 内のすべてのポートに複数の ACL を設定する場合、最新の設定が有効になります。

例

VLAN 2 のホストがマルチキャストグループ FF03::101 のみ加入できるように VLAN 2 の IPv6 マルチキャストグループポリシーをグローバルに設定します。

<Switch> system-view

[Switch] acl ipv6 basic 2000

[Switch-acl-ipv6-basic-2000] rule permit source ff03::101 128

[Switch-acl-ipv6-basic-2000] quit

[Switch] mld-snooping

[Switch-mld-snooping] group-policy 2000 vlan 2

関連コマンド

mld-snooping group-policy

3.1.16 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 200 ～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。

MLD-snooping view のすべての VLAN、または VLAN view の VLAN に対してグローバルにタイマを設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

IPv6 マルチキャストグループメンバを誤って削除しないように、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形式で計算されるよりも大きい値に設定してください。

[MLD general query 間隔]+[MLD general query 最大応答時間]

以下の形式で計算される値をダイナミックメンバポートのエージングタイマに設定することを推奨します。

[MLD general query 間隔]×2+[MLD general query 最大応答時間]

例

グローバルでダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] host-aging-time 300

関連コマンド

mld-snooping host-aging-time

3.1.17 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 query 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 query 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。

VLAN view で VLAN の間隔を設定するか、MLD-snooping view ですべての VLAN の間隔をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

MLD last listener query 間隔を 3 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] last-listener-query-interval 3

関連コマンド

mld-snooping last-listener-query-interval

3.1.18 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 query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 query 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。

MLD-snooping view のすべての VLAN、または VLAN view の VLAN に対してグローバルに時間を設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

誤って 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 query の最大応答時間を MLD general query 間隔よりも短く設定してください。

例

グローバルで MLD general query の最大応答時間を 5 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] max-response-time 5

関連コマンド

- **mld-snooping max-response-time**
- **mld-snooping query-interval**

3.1.19 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。

MLD snooping 機能を無効にすると、すべての VLAN で MLD snooping が無効になります。

例

グローバルで MLD snooping を有効にし、MLD-snooping view に移行します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping]

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.20 mld-snooping done source-ip

Syntax

mld-snooping done source-ip *ipv6-address*

undo mld-snooping done source-ip

デフォルト

MLD done メッセージの送信元 IPv6 アドレスは現在の VLAN インタフェースの IPv6 リンクローカルアドレスです。現在の VLAN インタフェースに IPv6 リンクローカルアドレスがない場合、送信元 IPv6 アドレスは FE80::02FF:FFFF:FE00:0001 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: MLD done メッセージの送信元 IPv6 アドレスを指定します。

説明

mld-snooping done source-ip コマンドは MLD done メッセージの送信元 IPv6 アドレスを設定します。

undo mld-snooping done source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で MLD snooping を有効にしてください。

例

VLAN 2 で MLD snooping を有効にし、MLD done メッセージの送信元 IPv6 アドレスを FE80:0:0:1::1 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping done source-ip fe80:0:0:1::1

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.21 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 優先度は設定されていません。装置によって作成された MLD メッセージの場合、802.1p 優先度は 0 です。転送される MLD メッセージの場合、装置は 802.1p 優先度を変更しません。

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 802.1 p の優先度を指定します。設定範囲は 0〜7 です。値が大きいほど、優先順位が高くなります。

説明

mld-snooping dot1p-priority コマンドは VLAN 内の MLD メッセージの 802.1 p の優先度を設定します。

undo mld-snooping dot1p-priority コマンドは設定をデフォルトに戻します。

例

VLAN2 で MLD snooping を有効にし、MLD メッセージの 802.1 p の優先度を 3 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping dot1p-priority 3

関連コマンド

- **dot1p-priority (MLD-snooping view)**
- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.22 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パケットの廃棄機能を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping drop-unknown

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.23 mld-snooping enable

Syntax

mld-snooping enable

undo mld-snooping

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 コマンドは VLAN の MLD snooping を無効にします。

VLAN の MLD snooping を有効にする前に、**mld-snooping** コマンドを使用して、MLD snooping 機能を有効にする必要があります。

VLAN view でこのコマンドを使用して VLAN の MLD snooping を有効にしたり、**enable** コマンドを使用して複数の VLAN の MLD snooping を有効にしたりできます。VLAN view の設定は MLD-snooping view の設定と同じの優先度を持ち、最新の設定が有効になります。

例

MLD snooping 機能を有効にし、次に VLAN2 の MLD snooping を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping**

3.1.24 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、このコマンドはすべての 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、interface view のポートに対して有効にすることも、MLD snooping view のすべてのポートに対してグローバルに有効にすることもできます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

例

GigabitEthernet 1/0/1 の VLAN 2 で fast-leave 処理機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2

関連コマンド

fast-leave (MLD-snooping view)

3.1.25 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

VLAN では、MLD general query 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: 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 query 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 の 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 query の送信元 IPv6 アドレス FE80:0:0:1::1 を設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.26 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

ポートが参加できる IPv6 マルチキャストグループの最大数に制限はありません。

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

limit: ポートが加入できるマルチキャストグループの最大数を設定します。設定範囲は 0～4294967295 です。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

mld-snooping group-limit コマンドはポートが加入できる IPv6 マルチキャストグループの最大数を設定します。

undo mld-snooping group-limit コマンドはデフォルトに戻します。

このコマンドはポートがダイナミックに加入する IPv6 マルチキャストグループでのみ適用します。

例

VLAN 2 の GigabitEthernet 1/0/1 が加入できる IPv6 マルチキャストグループの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping group-limit 10 vlan 2

3.1.27 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、ホストが参加できる IPv6 マルチキャストグループを制御するために、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、このコマンドはスタティックメンバポートには影響しません。

MLD-snooping view で、IPv6 マルチキャストグループポリシーを interface view のポート、またはグローバルに全てのポートに設定できます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

IPv6 ACL でルールを設定する場合は、次の制限とガイドラインに従ってください。

- 標準 ACL では、**source** *source-address source-prefix* オプションは、IPv6 マルチキャストグループアドレスを指定します。
- 詳細な ACL では、**source** *source-address source-prefix* オプションは 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* オプションは、IPv6 マルチキャストグループアドレスを指定します。

IPv6 マルチキャスト送信元アドレスを持たない MLDv1 レポート、MLD IS_EX および MLDv2TO_EX レポートに一致させるには、**source** *source-address source-prefix* オプションを 0 :: 0 に設定します。

- その他のオプションパラメータのうち、**fragment** と time-range time-range-name オプションだけが有効になります。

ポート上の異なる VLAN に対して異なる ACL を設定できます。ポート上の同じ VLAN に複数の ACL を設定する場合、最新の設定が有効になります。

例

ポートに接続されたホストがマルチキャストグループ FF03::101 のみ加入できるように VLAN 2 の GigabitEthernet 1/0/1 で IPv6 マルチキャストグループポリシーを設定します。

<Switch> system-view

[Switch] acl ipv6 basic 2000

[Switch-acl-ipv6-basic-2000] rule permit source ff03::101 128

[Switch-acl-ipv6-basic-2000] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2

関連コマンド

group-policy (MLD-snooping view)

3.1.28 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: 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。

VLAN view で VLAN のタイマを設定するか、またはMLD-snooping view ですべての VLAN をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

IPv6 マルチキャストグループメンバの誤った削除を避けるために、ダイナミックメンバポートのエージングタイマを次の式を使用して計算された値より大きい値に設定します。

[MLD general query 間隔] + [MLD general query 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次の式を使用して計算された値に設定します。

[MLD general query 間隔] × 2 + [MLD general query 最大応答時間]

例

VLAN 2 の MLD snooping を有効にし、VLAN のダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping host-aging-time 300

関連コマンド

- **enable (MLD-snooping view)**
- **host-aging-time (MLD-snooping view)**
- **mld-snooping enable**

3.1.29 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

ポートは IPv6 マルチキャストグループや IPv6 マルチキャストソースとグループのシミュレートされたメンバホストではありません。

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

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。

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。

シミュレートされたメンバホストで動作している 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。ポートは、ダイナミックメンバポートと同様にエージアウトします。

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(2002::22, FF3E::101)のシミュレーティッドメンバホストを GigabitEthernet 1/0/1 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 vlan 2

3.1.30 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 query 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 query 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 の MLD snooping を有効にする必要があります。

VLAN view で VLAN の間隔を設定するか、MLD-snooping view ですべての VLAN の間隔をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

VLAN 2 の MLD snooping を有効にし、VLAN 2 の MLD last listener query 間隔を 3 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping last-listener-query-interval 3

関連コマンド

- **enable (MLD-snooping view)**
- **last-listener-query-interval (MLD-snooping view)**
- **mld-snooping enable**

3.1.31 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 query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 query 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 の MLD snooping を有効にする必要があります。

VLAN view で VLAN の時間を設定するか、MLD-snooping view ですべての VLAN の時間をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

誤って 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 query の最大応答時間を MLD general query 間隔よりも短く設定してください。

例

VLAN 2 の MLD snooping を有効にし、VLAN 2 の MLD general query の最大応答時間を 5 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping max-response-time 5

関連コマンド

- **enable (MLD-snooping view)**
- **max-response-time (MLD-snooping view)**
- **mld-snooping enable**
- **mld-snooping query-interval**

3.1.32 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。

IPv6 マルチキャストグループ置換機能は、interface view 内のポートで有効にすることも、MLD-snooping view 内のすべてのポートでグローバルに有効にすることもできます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

例

GigabitEthernet 1/0/1 の VLAN2 で IPv6 マルチキャストグループ置き換え機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2

関連コマンド

overflow-replace (MLD-snooping view)

3.1.33 mld-snooping querier

Syntax

mld-snooping querier

undo mld-snooping querier

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

mld-snooping querier コマンドは MLD snooping クエリアを有効にします。

undo mld-snooping querier コマンドは MLD snooping クエリアを無効にします。

このコマンドを実行する前に、VLAN の MLD snooping 機能を有効にしてください。

このコマンドは、IPv6 マルチキャスト VLAN からサブ VLAN を削除した後、サブ VLAN に適用されます。

例

VLAN 2 の MLD snooping を有効にし、MLD snooping クエリアを有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping querier

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**
- **subvlan (IPv6 multicast VLAN view)**

3.1.34 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 query 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 query 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 query の最大応答時間より MLD general query 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 query 送信間隔を 20 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping query-interval 20

関連コマンド

- **enable (MLD-snooping view)**
- **max-response-time**
- **mld-snooping enable**
- **mld-snooping max-response-time**
- **mld-snooping querier**

3.1.35 mld-snooping report source-ip

Syntax

mld-snooping report source-ip *ipv6-address*

undo mld-snooping report source-ip

デフォルト

VLAN では、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 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 コマンドは設定を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 機能を有効にしておいてください。

例

VLAN2 で MLD snooping 機能を有効にし、MLD report の送信元 IPv6 アドレスを FE80:0:0:1::1 と設定します。

<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

例

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.36 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。

VLAN view で VLAN のタイマを設定するか、または MLD-snooping view ですべての VLAN をグローバルに設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

VLAN 2 の MLD snooping を有効にし、ダイナミックルータポートのエージングタイマを 100 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping router-aging-time 100

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**
- **router-aging-time (MLD-snooping view)**

3.1.37 mld-snooping source-deny

Syntax

mld-snooping source-deny

undo mld-snooping source-deny

デフォルト

IPv6 マルチキャストソースポートフィルタは無効です。

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。

この機能は、interface view のポートまたは MLD-snooping view 内の指定されたポートに対して有効にできます。ポートについては、interface view の設定は MLD-snooping view の設定と同じ優先度を持ち、最後に行われた設定が適用されます。

例

GigabitEthernet 1/0/1 で IPv6 マルチキャストソースポートフィルタを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping source-deny

関連コマンド

source-deny (MLD-snooping view)

3.1.38 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 では、MLD マルチキャストアドレス固有のクエリの送信元 IPv6 アドレスは、次のいずれかです。

- VLAN の MLD snooping クエリアが MLD general query を受信した場合、MLD general query の送信元アドレスです。

- MLD snooping クエリアが MLD 一般検索を受信しない場合の、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。
- FE80 :: 02FF:FFFF:FE00:0001:MLD snooping クエリアが MLD 汎用検索を受信せず、現在の VLAN インタフェースが IPv6 リンクローカルアドレスを持っていません。

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 query 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 query 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 query の送信元 IPv6 アドレス FE80:0:0:1::1 を設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.39 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 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(2002::22, FF3E::101)のスタティックメンバポートを GigabitEthernet 1/0/1 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 vlan 2

3.1.40 mld-snooping static-router-port

Syntax

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port { **all** | **vlan** *vlan-id* }

デフォルト

設定なし

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

all: すべての VLAN を指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

mld-snooping static-router-port コマンドはスタティックルータポートを設定します。

undo mld-snooping static-router-port コマンドはスタティックルータポートを削除します。

例

VLAN 2 の GigabitEthernet 1/0/1 をスタティックルータポートに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping static-router-port vlan 2

3.1.41 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。

VLAN view で VLAN のバージョンを指定するか、MLD-snooping view で指定した VLAN のバージョンを指定できます。VLAN 固有の設定は、MLD-snooping view では設定と同一の優先度を持ち、最後に行われた設定が適用されます。

例

VLAN 2 の MLD snooping を有効にし､MLD snooping のバージョンを 2 に指定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping version 2

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**
- **version (MLD-snooping view)**

3.1.42 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。

MLD-snooping view 内のすべてのポート、または interface view のポートで、グローバルに IPv6 マルチキャストグループ置き換え機能を有効にできます。ポートの場合、ポート固有の設定がグローバル設定よりも優先されます。

例

VLAN2 で IPv6 マルチキャストグループ置き換え機能を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] overflow-replace vlan 2

関連コマンド

mld-snooping overflow-replace

3.1.43 report-aggregation (MLD-snooping view)

Syntax

report-aggregation

undo report-aggregation

デフォルト

有効

View

MLD-snooping view

定義済みユーザロール

network-admin

説明

report-aggregation コマンドは MLD report 抑制機能を有効にします。

undo report-aggregation コマンドは MLD report 抑制機能を無効にします。

例

MLD report 抑制機能を無効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] undo report-aggregation

3.1.44 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 グループ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 グループ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

すべてのダイナミック MLD snooping グループエントリを削除します。

<Switch> reset mld-snooping group all

関連コマンド

display mld-snooping group

3.1.45 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: すべてのダイナミックルータポートを指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。VLAN を指定しない場合、このコマンドはすべての VLAN のダイナミックルータポート情報を削除します。

説明

reset mld-snooping router-port コマンドはダイナミックルータポートを削除します。

例

すべての VLAN のダイナミックルータポートを削除します。

<Switch> reset mld-snooping router-port all

関連コマンド

display mld-snooping router-port

3.1.46 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 と IPv6 PIM hello メッセージによって学習した MLD メッセージの統計情報を削除します。

例

MLD snooping によって学習したすべての MLD メッセージと IPv6 PIM hello メッセージの統計情報を削除します。

<Switch> reset mld-snooping statistics

関連コマンド

display mld-snooping statistics

3.1.47 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。

MLD-snooping view のすべての VLAN、または VLAN view の VLAN に対してグローバルにタイマを設定できます。VLAN の場合、VLAN 固有の設定がグローバル設定よりも優先されます。

例

グローバルでダイナミックルータポートのエージングタイマを 100 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] router-aging-time 100

関連コマンド

mld-snooping router-aging-time

3.1.48 source-deny (MLD-snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

デフォルト

IPv6 マルチキャストソースポートフィルタは無効です。

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。

この機能は、MLD snooping view 内の指定されたポート、または interface view のポートに対して有効にできます。ポートについては、MLDsnooping view の設定は、interface view の設定と同一の優先度を持ち、最後に行われた設定が適用されます。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 で IPv6 マルチキャストデータのソースポートのフィルタを有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

関連コマンド

mld-snooping source-deny

3.1.49 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。

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、指定された VLAN の MLD snooping を有効にする必要があります。

MLD snooping view では指定された VLAN のバージョンを、VLAN view では VLAN のバージョンを指定できます。VLAN 固有の設定は、MLD snooping view では設定と同一の優先度を持ち、最後に行われた設定が適用されます。

例

VLAN 2～VLAN 10 の MLD snooping を有効にし、MLD snooping のバージョンを 2 に指定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] enable vlan 2 to 10

[Switch-mld-snooping] version 2 vlan 2 to 10

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**
- **mld-snooping version**

目次

このセクションのページは **6-x-x** です。

4 章 IPv6 マルチキャスト VLAN 4-1
4.1 IPv6 マルチキャスト VLAN 設定コマンド 4-1
4.1.1 display ipv6 multicast-vlan 4-1
4.1.2 display ipv6 multicast-vlan forwarding-table 4-2
4.1.3 display ipv6 multicast-vlan group 4-4
4.1.4 ipv6 multicast-vlan 4-6
4.1.5 ipv6 multicast-vlan entry-limit 4-8
4.1.6 ipv6 port multicast-vlan 4-9
4.1.7 port (IPv6 multicast VLAN view) 4-9
4.1.8 reset ipv6 multicast-vlan group 4-10
4.1.9 subvlan (IPv6 multicast VLAN view) 4-11

4章 IPv6 マルチキャスト VLAN

4.1 IPv6マルチキャストVLAN設定コマンド

4.1.1 display ipv6 multicast-vlan

Syntax

display ipv6 multicast-vlan [*vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id: IPv6 マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての IPv6 マルチキャスト VLAN の情報を表示します。

説明

display ipv6 multicast-vlan コマンドは IPv6 マルチキャスト VLAN の情報を表示します。

例

すべての IPv6 マルチキャスト VLAN の情報を表示します。

<Switch> display ipv6 multicast-vlan

```
Total 2 IPv6 multicast VLANs.

IPv6 multicast VLAN 100:
  Sub-VLAN list(3 in total):
    2-3, 6
  Port list(3 in total):
    GE1/0/1
    GE1/0/2
    GE1/0/3

IPv6 multicast VLAN 200:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
```

表 4-1 コマンド出力

フィールド	説明
Total 2 IPv6 multicast VLANs	IPv6マルチキャストVLANの総数です。
Sub-VLAN list(3 in total)	IPv6マルチキャストVLANのサブVLANのリストと、サブVLANの総数です。
Port list(3 in total)	IPv6マルチキャストVLANのポートリストとポートの総数です。

4.1.2 display ipv6 multicast-vlan forwarding-table

Syntax

display ipv6 multicast-vlan forwarding-table [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-source-address: IPv6 マルチキャスト送信元の IPv6 アドレスを指定します。IPv6 マルチキャスト送信元を指定しない場合、すべての IPv6 マルチキャスト送信元の IPv6 マルチキャスト VLAN 転送エントリを表示します。

prefix-length: IPv6 マルチキャスト送信元の IPv6 アドレスのプレフィックス長を指定します。設定範囲は 0～128 です。デフォルトは 128 です。

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16 です。“x”と“y”は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループの IPv6 マルチキャスト VLAN 転送エントリを表示します。

prefix-length: IPv6 マルチキャストグループの IPv6 アドレスのプレフィックス長を指定します。設定範囲は 8～128 です。デフォルトは 128 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の IPv6 マルチキャスト VLAN 転送エントリを表示します。

subvlan *vlan-id*: サブ VLAN の ID を指定します。指定しない場合、すべてのサブ VLAN の IPv6 マルチキャスト VLAN 転送エントリを表示します。

vlan *vlan-id*: IPv6 マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての IPv6 マルチキャスト VLAN の IPv6 マルチキャスト VLAN 転送エントリを表示します。

説明

display ipv6 multicast-vlan forwarding-table コマンドは IPv6 マルチキャスト VLAN 転送エントリを表示します。

例

すべての IPv6 マルチキャスト VLAN 転送エントリを表示します。

<Switch> display ipv6 multicast-vlan forwarding-table

```
IPv6 multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1::1, FF0E::1)
    Flags: 0x10000
    IPv6 multicast VLAN: 100
    List of sub-VLANs (3 in total):
      1: VLAN 10
      2: VLAN 20
      3: VLAN 30
```

表 4-2 コマンド出力

フィールド	説明
IPv6 multicast VLAN 100 Forwarding Table	IPv6マルチキャストVLAN 100の転送テーブルです。
Total 1 entries, 1 matched	（S,G）エントリの総数と一致するエントリの数です。
00001	（S,G）エントリのシーケンス番号です。
(1::1, FF0E::1)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャスト送信元を示します。

フィールド	説明
Flags	エントリフラグです。 このフィールドは1つのフラグあるいは複数のフラグの合計を表示します。たとえば、0x10000は、エントリに1つのフラグ0x10000があることを示します。 エントリは以下のフラグがあります。 • **0x1**—エントリは非アクティブ状態です。 • **0x4**—エントリがアップデートに失敗しました。 • **0x8**—エントリのサブVLANの情報がアップデートに失敗しました。 • **0x200**—エントリはGR状態です。 • **0x10000**—エントリはIPv6マルチキャスト転送エントリです。
List of sub-VLANs (3 in total)	IPv6マルチキャストVLANのサブVLANリストと、サブVLANの総数です。

4.1.3 display ipv6 multicast-vlan group

Syntax

display ipv6 multicast-vlan group [*ipv6-source-address* | *ipv6-group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-source-address: IPv6 マルチキャスト送信元の IPv6 アドレスを指定します。IPv6 マルチキャスト送信元を指定しない場合、IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャスト送信元の IPv6 マルチキャストグループの情報を表示します。

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy ::/ 16（FFx1 ::/ 16 および FFx2 ::/ 16 を除きます）です。“x”と“y”は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャストグループの情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループの情報を表示します。

verbose: 詳細情報を表示します。指定しない場合、概要情報を表示します。

vlan *vlan-id*: IPv6 マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループの情報を表示します。

説明

display ipv6 multicast-vlan group コマンドは IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループの情報を表示します。

例

すべての IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャストグループの詳細情報を表示します。

<Switch> display ipv6 multicast-vlan group verbose

```
Total 6 entries.

IPv6 multicast VLAN 10: Total 3 entries.
  (2::2, FF0E::2)
    Flags: 0x70000020
    Sub-VLANs (1 in total):
      VLAN 40
  (22::22, FF0E::4)
    Flags: 0x70000030
    Sub-VLANs (1 in total):
      VLAN 40
  (::, FF0E::10)
    Flags: 0x10000030
    Sub-VLANs (1 in total):
      VLAN 40

IPv6 multicast VLAN 20: Total 3 entries.
  (2::2, FF0E::2)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (22::22, FF0E::4)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (::, FF0E::10)
    Flags: 0x50000010
    Sub-VLANs (0 in total):
```

表 4-3 コマンド出力

フィールド	説明
Total 6 entries	（S,G）エントリの総数です。
IPv6 multicast VLAN 10: Total 3 entries	IPv6マルチキャストVLAN 10の（S,G）エントリの総数です。
(::, FF0E::10)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャスト送信元を示します。
Flags	エントリフラグです。 このフィールドは1つのフラグあるいは複数のフラグの合計を表示します。たとえば、0x70000020は、エントリにフラグ0x20、0x10000000、0x20000000、0x40000000があることを示します。 エントリは以下のフラグがあります。 • **0x10**—エントリがIPv6マルチキャストVLANによって作成されました。 • **0x20**—エントリがIPv6マルチキャストVLANのサブVLANによって作成されました。 • **0x40**—エントリが削除されました。 • **0x10000000**—この値は以下の状態の1つを示します。 　• エントリが新規に作成されました。 　• 装置はMLD general query送信間隔内にMLD queryを受信しました。 • **0x20000000**—装置はMLD general query送信間隔内にMLDv1あるいはMLDv2 reportを受信していません。 • **0x40000000**—装置はMLD general query送信間隔内にMLDv2 IS_EX (NULL) reportを受信していません。 MLDはQX-S5300Gシリーズではサポートしていません。
Sub-VLANs (1 in total)	IPv6マルチキャストVLANのサブVLANとサブVLANの総数です。

関連コマンド

reset ipv6 multicast-vlan group

4.1.4 ipv6 multicast-vlan

Syntax

ipv6 multicast-vlan *vlan-id*

undo ipv6 multicast-vlan { **all** | *vlan-id* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id: 既存の VLAN ID を指定します。設定範囲は 1～4094 です。

all: すべての IPv6 マルチキャスト VLAN を指定します。

説明

ipv6 multicast-vlan コマンドは IPv6 マルチキャスト VLAN を設定し、IPv6 multicast VLAN view に移行するか、既存の IPv6 マルチキャスト VLAN view に移行します。

undo ipv6 multicast-vlan コマンドは IPv6 マルチキャスト VLAN を削除します。

IPv6 マルチキャストルーティングが有効な装置で、IPv6 マルチキャスト VLAN の設定を行わないことを推奨します。

装置の IPv6 マルチキャスト VLAN の総数はシステムがサポートする最大数を超過することができません。

VLAN を IPv6 マルチキャスト VLAN として設定するには、MLD snooping を有効にする必要があります。

例

VLAN 100 で MLD snooping を有効にします。IPv6 マルチキャスト VLAN として VLAN 100 を設定し、IPv6 multicast VLAN view に移行します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 100

[Switch-vlan100] mld-snooping enable

[Switch-vlan100] quit

[Switch] ipv6 multicast-vlan 100

[Switch-ipv6-mvlan-100]

関連コマンド

mld-snooping enable

4.1.5 ipv6 multicast-vlan entry-limit

Syntax

ipv6 multicast-vlan entry-limit *limit*

undo ipv6 multicast-vlan entry-limit

デフォルト

4000

View

System view

定義済みユーザロール

network-admin

パラメータ

limit: IPv6 マルチキャスト VLAN 転送エントリの最大数を設定します。設定範囲は 0～4000 です。

説明

ipv6 multicast-vlan entry-limit コマンドは IPv6 マルチキャスト VLAN 転送エントリの最大数を設定します。

undo ipv6 multicast-vlan entry-limit コマンドはデフォルトに戻します。

設定された値が IPv6 マルチキャスト VLAN 転送エントリの現在の数より小さい場合、いくつかのエントリがエイジアウトするか、手動で削除されるまで、装置は新しいエントリを作成できません。新しいエントリをすぐに作成できるようにするには、**reset ipv6multicast-vlan group** コマンドを使用して、IPv6 マルチキャスト VLAN 転送エントリを削除します。

例

IPv6 マルチキャスト VLAN 転送エントリの最大数を 120 に設定します。

<Switch> system-view

[Switch] ipv6 multicast-vlan entry-limit 120

関連コマンド

entry-limit (MLD-snooping view)

4.1.6 ipv6 port multicast-vlan

Syntax

ipv6 port multicast-vlan *vlan-id*

undo ipv6 port multicast-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: IPv6 マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

ipv6 port multicast-vlan コマンドは IPv6 マルチキャスト VLAN にポートを割り当てます。

undo ipv6 port multicast-vlan コマンドはデフォルトに戻します。

ポートは 1 つの IPv6 マルチキャスト VLAN にのみ所属することができます。

ポートを IPv6 マルチキャスト VLAN に割り当てるためには、ポートが属する VLAN の MLD snooping を有効にする必要があります。

例

GigabitEthernet 1/0/1 を IPv6 マルチキャスト VLAN 100 に割り当てます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] ipv6 port multicast-vlan 100

4.1.7 port (IPv6 multicast VLAN view)

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

デフォルト

設定なし

View

IPv6 multicast VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list: ポートあるいはポート範囲を指定します。形式は *interface-type interface-number* です。ポート範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。

all: 現在の IPv6 マルチキャスト VLAN のすべてのユーザポートを指定します。

説明

port コマンドは IPv6 マルチキャスト VLAN にユーザポートを割り当てます。

undo port コマンドは IPv6 マルチキャスト VLAN からユーザポートを削除します。

IPv6 マルチキャスト VLAN にユーザポートとして割り当てることができるのは、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だけです。さらに、1 つのポートを 1 つの IPv6 マルチキャスト VLAN だけに割り当てることができます。

ポートを IPv6 マルチキャスト VLAN に割り当てるためには、ポートが属する VLAN の MLD snooping を有効にする必要があります。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 を IPv6 マルチキャスト VLAN 100 にユーザポートを割り当てます。

<Switch> system-view

[Switch] ipv6 multicast-vlan 100

[Switch-ipv6-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5

4.1.8 reset ipv6 multicast-vlan group

Syntax

reset ipv6 multicast-vlan group [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **vlan** *vlan-id*] *

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy ::/ 16 です。FFx1 ::/ 16 および FFx2 ::/ 16 を除きます。“x”と“y”の設定範囲は 16 進数で 0～F です。IPv6 マルチキャストグループを指定しない場合、IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャストグループを削除します。

prefix-length: IPv6 マルチキャストグループアドレスのプレフィックス長を指定します。設定範囲は 8～128 です。デフォルトは 128 です。

ipv6-source-address: IPv6 マルチキャスト送信元の IPv6 アドレスを指定します。IPv6 マルチキャスト送信元を指定しない場合、IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャスト送信元への IPv6 マルチキャストグループを削除します。

prefix-length: IPv6 マルチキャスト送信元アドレスのプレフィックス長を指定します。設定範囲は 0～128 です。デフォルトは 128 です。

vlan *vlan-id*: IPv6 マルチキャスト VLAN を指定します。設定範囲は 1～4094 です。指定しない場合、すべての IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループを削除します。

説明

reset ipv6 multicast-vlan group コマンドは IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループを削除します。

例

すべての IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャストグループを削除します。

<Switch> reset ipv6 multicast-vlan group

関連コマンド

display ipv6 multicast-vlan group

4.1.9 subvlan (IPv6 multicast VLAN view)

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

デフォルト

設定なし

View

IPv6 multicast VLAN view

定義済みユーザロール

network-admin

パラメータ

vlan-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定された VLAN は存在する必要があり、マルチキャスト VLAN または他の IPv6 マルチキャスト VLAN のサブ VLAN にすることはできません。

all: 現在の IPv6 マルチキャスト VLAN のすべてのサブ VLAN を指定します。

説明

subvlan コマンドは IPv6 マルチキャスト VLAN にサブ VLAN を割り当てます。

undo subvlan コマンドは IPv6 マルチキャスト VLAN からサブ VLAN を削除します。

VLAN を IPv6 マルチキャスト VLAN のサブ VLAN として設定するには、MLD snooping を有効にする必要があります。

例

IPv6 マルチキャスト VLAN 100 のサブ VLAN として VLAN 10～VLAN 15 を設定します。

<Switch> system-view

[Switch] ipv6 multicast-vlan 100

[Switch-ipv6-mvlan-100] subvlan 10 to 15

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

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

目次

このセクションのページは **7-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 1-4
1.1.3 acl logging interval 1-5
1.1.4 description 1-6
1.1.5 display acl 1-7
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 1-19
1.1.12 packet-filter filter 1-21
1.1.13 reset acl counter 1-22
1.1.14 reset packet-filter statistics 1-23
1.1.15 rule (IPv4 advanced ACL view) 1-24
1.1.16 rule (IPv4 basic ACL view) 1-30
1.1.17 rule (IPv6 advanced ACL view) 1-32
1.1.18 rule (IPv6 basic ACL view) 1-38
1.1.19 rule (Layer2 ACL view) 1-40
1.1.20 rule comment 1-43
1.1.21 step 1-44

1章 ACL

1.1 ACL設定コマンド

1.1.1 acl

Syntax

コマンドセット 1：

acl [**ipv6**] { **name** *acl-name* | **number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }] }

undo acl [**ipv6**] { **all** | **name** *acl-name* | **number** *acl-number* }

コマンドセット 2：

acl [**ipv6**] { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

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。IPv4 ACL タイプを指定する場合は使用しないでください。

basic: 標準 ACL を指定します。

advanced: 拡張 ACL を指定します。

mac: Layer ACL を指定します。

number *acl-number*: ACL の番号を指定します。

acl-number: ACL の番号を指定します。使用可能な設定範囲は以下のとおりです。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：Layer 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。マッチの順番を指定しない場合、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。

acl-number を作成する場合、次のコマンドを使用して ACL の view に移行できます。

- **acl** [**ipv6**] **number** *acl-number*
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number*

acl [**ipv6**] **number** *acl-number* **name** *acl-name* コマンドを使用して ACL を作成する場合、次のコマンドを使用して ACL の view に移行できます。

- **acl** [**ipv6**] **name** *acl-name* (標準 ACL と拡張 ACL の場合のみ)
- **acl** [**ipv6**] **number** *acl-number* [**name** *acl-name*]
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*

acl { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* コマンドを使用して *acl-name* を作成する場合、次のコマンドを使用して ACL の view に移行できます。

- **acl** [**ipv6**] **name** *acl-name* (標準 ACL と拡張 ACL の場合のみ)
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*

ルールが含まれない ACL のみパケットを比較する ACL ルールの順番を変更することができます。

ACL が ACL ルールの順番を含んでいる場合、あるいは以下のマッチ条件と機能に加えて有効な機能がある場合、マッチするパケットはソフトウェアベースによるスロー転送が行われます。

- 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
- TransportLayer プロトコル
- ICMP/ICMPv6 メッセージタイプ、ICMP/ICMPv6 メッセージコード、ICMP/ICMPv6 メッセージ名
- ロギング
- タイムレンジ

スロー転送は、スロー転送エントリの計算を行うため、コントロールプレーンにパケットを送信する必要があります。この処理は装置の転送性能に影響を与えます。

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]

標準 IPv4 ACL **flow** 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]

標準 IPv6 ACL **flow** 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]

拡張 IPv6 ACL **abc** 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]

Layer2ACL 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]

Layer2ACL **flow** 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: Layer ACL を指定します。

source-acl-number: デフォルトの ACL の番号を指定します。使用可能な値の範囲は次のとおりです。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：Layer ACL 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: 作成される ACL に一意の番号を割り当てます。使用可能な値の範囲は次のとおりです。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：Layer ACL です。

name *dest-acl-name*: 作成される ACL に一意の名前を割り当てます。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 コマンドはデフォルトの ACL をコピーします。

新しい ACL とデフォルトの ACL は同じタイプでなければなりません。

新しい ACL はデフォルトの ACL と同一カテゴリ、同一内容ですが、ACL 名と ACL 番号が異なります。

IPv4 ACL を指定する際、**ipv6** または **mac** を指定しないでください。

例

標準 IPv4 ACL 2001 をコピーし、標準 IPv4 ACL 2002 を作成します。

<Switch> system-view

[Switch] acl copy 2001 to 2002

標準 IPv4 ACL **test** をコピーし、標準 IPv4 ACL **paste** 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。

ロギング機能は、**logging** を持つ IPv4 または IPv6 ACL ルールで使用できます。

パケットフィルタリング用のログエントリを生成し、出力間隔でインフォメーションセンターに出力するように ACL モジュールを設定できます。フローの最初のパケットが ACL ルールとマッチすると、出力インターバルが開始します。インターバルの終わりに、装置はインターバルの間のマッチしたパケットの数とマッチした ACL ルールを記録する

ためにログエントリを出力します。インフォメーションセンターの詳細は、オペレーションマニュアルのセクション 10 *システム管理* を参照してください。

例

IPv4 パケットフィルタリングのログを作成し、出力することを有効にし、出力間隔を 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: Layer 2 ACL を指定します。

acl-number: ACL の番号を指定します。使用可能な値の範囲は次のとおりです。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：Layer 2 ACL 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。

説明

display acl コマンドは ACL の設定とマッチ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 を指定するには、**ipv6** または **mac** を指定しないでください。

例

標準 IPv4 ACL 2001 の設定とマッチする統計情報を表示します。

<Switch> display acl 2001

```
Basic IPv4 ACL 2001, 1 rule, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5, start ID is 0
 rule 5 permit source 1.1.1.1 0
 rule 5 comment This rule is used on GigabitEthernet1/0/1.
```

表 1-1 コマンド出力

フィールド	説明
Basic IPv4 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1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	開始ルールIDは0です。
rule 5 permit source 1.1.1.1 0	ルール5の内容です。ルールはIPアドレス1.1.1.1からの送信元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。

1.1.6 display packet-filter

Syntax

display packet-filter interface [*interface-type 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。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。Ethernet インタフェースを指定する場合は、**slot** *slot-number* オプションを指定する必要はありません。

inbound: インタフェースで受信されたパケットを指定します。

outbound: インタフェースで送信されたパケットを指定します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタのパケットフィルタリングの ACL 情報を表示します。

説明

display packet-filter コマンドはパケットフィルタリングの ACL の情報を表示します。

Inbound と **outbound** 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の ACL の情報を表示します。

例

GigabitEthernet 1/0/1 で受信されたパケットフィルタリングの ACL の情報を示します。

<Switch> display packet-filter interface gigabitethernet 1/0/1 inbound

```
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003
```

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ルールにマッチした回数をカウントするようにします。
Hardware-count(Failed)	ACLルールにマッチした回数のカウントに失敗しました。

フィールド	説明
IPv4 default action	どのIPv4 ACLにもマッチしないパケットに対するパケットフィルタのデフォルトの動作です。 • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。この動作は、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が正常に適用されました。
IPv6 default action	どのIPv6 ACLともマッチしないパケットに対するパケットフィルタの既定の動作です。 • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。この動作は、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が正常に適用されました。
MAC default action	どのLayer2 ACLともマッチしないパケットに対するパケットフィルタの既定の動作です。 • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。この動作は、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が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: Layer ACL を指定します。

acl-number: ACL の番号を指定します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：Layer ACL 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 にマッチする統計情報を表示します。

acl-number、**name** *acl-name*、**ipv6** または **mac** 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 にマッチする統計情報を表示します。

IPv4 ACL を指定するには、**ipv6** または **mac** を指定しないでください。

例

GigabitEthernet 1/0/1 で受信されたパケットフィルタリングのすべての ACL（標準 IPv4 ACL、拡張 IPv4 ACL、Layer2 ACL）にマッチする統計情報を表示します。

<Switch> display packet-filter statistics interface gigabitethernet 1/0/1 inbound

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

  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ルールにマッチした回数をカウントするようにします。
Hardware-count(Failed)	ACLルールにマッチした回数のカウントに失敗しました。
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パケットがルールにマッチしました。 このフィールドはパケットがルールにマッチしない場合、表示されません。
No resource	ルールにマッチした回数をカウントするためのリソースが十分ではありません。 このフィールドはリソースが十分ではない場合、ルールに表示されます。
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、拒否されているパケット数です。
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	どのIPv4 ACLにもマッチしないパケットに対するパケットフィルタのデフォルトの動作です。 • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。この動作は、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が正常に適用されました。

フィールド	説明
IPv6 default action	どのIPv6 ACLともマッチしないパケットに対するパケットフィルタのデフォルトの動作です。 • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。この動作は、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が正常に適用されました。
MAC default action	どのLayer2 ACLともマッチしないパケットに対するパケットフィルタのデフォルトの動作です。 • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。この動作は、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が正常に適用されました。

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: Layer2 ACL を指定します。

acl-number: ACL の番号を指定します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：Layer 2 ACL 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: 累積統計情報の概要を表示します。

説明

display packet-filter statistics sum コマンドはパケットフィルタリングの ACL にマッチする統計情報の累積を表示します。

IPv4 ACL タイプを指定するには、**ipv6** または **mac** 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 にマッチ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 にマッチする統計情報の累積を概要表示します。

<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にマッチする累積統計情報です。

フィールド	説明
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マッチしました。 このフィールドはルールにマッチしない場合、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。**slot** *slot-number*オプションは、Ethernetインタフェースでは使用できません。

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。I

mac: Layer2 ACL を指定します。

acl-number: ACL の番号を指定します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：Layer2 ACL 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。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタのパケットフィルタリングの ACL の詳細情報を表示します。

説明

display packet-filter verbose コマンドはパケットフィルタリングの ACL の詳細情報を表示します。

acl-number、**name** *acl-name*、**ipv6**、**mac** が指定されていないとき、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。

IPv4 ACL タイプを指定するには、**ipv6** または **mac** を指定しないでください。

例

GigabitEthernet 1/0/1 で受信されたパケットフィルタリングのすべての ACL（標準 IPv4 ACL、拡張 IPv4 ACL、Layer2 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

  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。

フィールド	説明
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ルールにマッチした回数をカウントするようにします。
Hardware-count(Failed)	ACLルールにマッチした回数のカウントに失敗しました。
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	どのIPv4 ACLにもマッチしないパケットに対するパケットフィルタデフォルトの動作です。 • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。このアクションは、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が正常に適用されました。
IPv6 default action	どのIPv6 ACLともマッチしないパケットに対するパケットフィルタの既定の動作です。 • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。このアクションは、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が正常に適用されました。
MAC default action	どのLayer2 ACLともマッチしないパケットに対するパケットフィルターデフォルトアクション: • **Deny**–パケットフィルタリングにデフォルトの動作拒否が正常に適用されました。 • **Deny(Failed)**–装置は、パケットフィルタリングにデフォルトの動作拒否を適用できませんでした。このアクションは、still関数を許可します。 • **Permit**–パケットフィルタリングにデフォルトの動作許可が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*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置の QoS と ACL のリソースの使用状況を表示します。

説明

display qos-acl resource コマンドは QoS と ACL のリソースの使用状況を表示します。

例

QoS と ACL のリソースの使用状況を表示します。

<Switch> display qos-acl resource

```
Interfaces: GE1/0/1 to GE1/0/24, XGE1/0/25 to XGE1/0/28
          GE1/1/1 to GE1/1/8 (slot 1)
-----------------------------------------------------------------------
 Type           Total     Reserved   Configured Remaining  Usage
-----------------------------------------------------------------------
 TTI ACL         3072      0         2         3070      0%
 IPCL0+IPCL2 ACL  1024      32        5         987       3%
 IPCL Counter     2048      28        2         2018      1%
 EPCL+IPCL1 ACL   512       0         0         512       0%
 EPCL Counter     1024      0         0         1024      0%
 IPCL Meter       4888      30        0         4858      0%
 EPCL Meter       4096      0         0         4096      0%
```

表 1-6 コマンド出力

フィールド	説明
Interfaces	ACLが適用されるインタフェースです。

フィールド	説明
Type	リソースタイプです。 • **TTI ACL**–トンネルの終端およびインタフェースに使用されるACLリソースです。 • **IPCL0+IPCL2 ACL**–受信ポリシーに使用されるACLリソースです。 • **IPCL Counter**–受信ポリシーに使用されるアカウンティングリソースです。 • **EPCL+IPCL1 ACL**–受信および送信ポリシーに使用されるACLリソースです。 • **EPCL Counter**–送信ポリシーに使用されるアカウンティングリソースです。 • **IPCL Meter**–受信QoSポリシーで使用されるトラフィックポリシングリソースです • **EPCL Meter**–送信QoSポリシーで使用されるトラフィックポリシングリソースです。
Total	リソースの総数です。
Reserved	予約されたリソース数です。
Configured	適用されたリソース数です。
Remaining	適用可能なリソース数です。
Usage	リソースの総数に対する設定されたリソースと予約済みリソース数の割合です。 割合が整数でない場合、整数部分のみ表示します。たとえば、正確な割合が50.8%である場合、50%と表示されます。

1.1.11 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: Layer2 ACL を指定します。

acl-number: ACL の番号を指定します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：Layer 2 ACL 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。

inbound: インタフェースで受信されるパケットをフィルタリングします。

outbound: インタフェースで送信されるパケットをフィルタリングします。

hardware-count: ハードウェアで実行される ACL ルールにマッチした回数をカウントするようにします。ACL のすべてのルールをカウントします。**rule** コマンドの **counting** はルールにマッチする回数をカウントするようにします。**hardware-count** が指定されない場合、ACL ルールにマッチする回数はカウントしません。

説明

packet-filter コマンドはパケットをフィルタするため、インタフェースに ACL を適用します。

undo packet-filter コマンドはインタフェースから ACL を削除します。

IPv4 ACL タイプを指定するには、**ipv6** または **mac** を指定しないでください。

このコマンドの **hardware-count** は、ACL 内のすべてのルールのハードウェアでのマッチカウントを有効にします。**rule** コマンドの **counting** は、ルール固有のマッチカウントを有効にします。

リソースが不十分な場合にハードウェアで ACL ルールマッチカウントを無効にするには、**undo packet-filter** コマンドを実行してから、**hardware-count** を指定せずに **packet-filter** コマンドを再設定する必要があります。

リソースが十分な場合にハードウェアで ACL ルールマッチカウントを無効にするには、**hardware-count** を指定せずに直接 **packet-filter** コマンドを再設定します。

インタフェースの同じ方向に、最大 3 つの（1 つの IPv4 ACL、1 つの IPv6 ACL、および 1 つの Layer2 ACL）ACL を適用できます。

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 ルールにマッチ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**

🕮 **メモ**:

同じ vlan-interface で同じ **packet-filter** コマンドを設定すると、vlan-interface で packet-filter が競合します。失敗したコマンドは、**display packet-filter verbose interface Vlan-interface** コマンドで確認できます。

1.1.12 packet-filter filter

🕮 **メモ**:

packet-filter filter コマンドは、Ver7.2.17 以降でサポートされています。

Syntax

packet-filter filter [**route** | **all**]

undo packet-filter filter

デフォルト

VLAN インタフェースが転送する L3 パケット(**route**)

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

route: レイヤ 3 で VLAN インタフェースが転送したパケットをフィルタします。

all: レイヤ 3 で VLAN インタフェースが転送したパケットとレイヤ 2 で VLAN インタフェースに関連付けられた物理ポートが転送したパケットを含む、すべてのパケットをフィルタします。

説明

packet-filter filter コマンドは VLAN インタフェース上でパケットフィルタリングの適用範囲を指定します

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

例

VLAN インタフェース 2 でパケットフィルタリングを設定して、レイヤ 3 で転送されるパケットをフィルタします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] packet-filter filter route

1.1.13 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。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

all: すべての ACL の統計情報を削除します。

name *acl-name*: 指定された ACL 名の統計情報を削除します。設定範囲は 1～63 です。大文字、小文字は区別しません。

説明

reset acl counter コマンドは ACL の統計情報を削除します。

IPv4 ACL タイプを指定するには、**ipv6** または **mac** を指定しないでください。

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

1.1.14 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。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 ACL 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: Layer2 ACL を指定します。

acl-number: ACL の番号を指定します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

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 packet-filter statistics コマンドはパケットフィルタリングの ACL にマッチする統計情報を削除します。

acl-number と **name** *acl-name* 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 にマッチする統計情報を削除します。

IPv4ACL タイプを指定するには、ipv6 または mac 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**

1.1.15 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。開始ルール ID 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: マッチするパケットを拒否します。

permit: マッチするパケットを許可します。

protocol: 次のいずれかの値を指定します。

- 0～255 の範囲のプロトコル番号です。
- 名前によるプロトコル：**icmp**(1)、**igmp**(2)、**ip**、**ipinip**(4)、**tcp**(6)、または **udp**(17) です。**ip** はすべてのプロトコルを指定します。

表 1-7 に、*protocol* 引数の値に関係なく指定できるパラメータを示します。

表 1-7 拡張 IPv4 ACL ルールのマッチ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ルールがマッチした回数をカウントします。	**counting**は指定したルールにマッチ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	パケットにマッチするログを指定します。	この機能はACLがloggingをサポートするモジュール（たとえばパケットフィルタリング）が必要です。
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション*7 ACL and QoS “タイムレンジ”*を参照してください。

protocol が **tcp** (6)あるいは **udp** (17)である場合、設定するパラメータを表 1-8 に示します。

表 1-8 拡張 IPv4 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port*	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	*operator*は**lt** (lower than)、**gt** (greater than)、**eq** (equal to)、**neq** (not equal to)、**range** (inclusive range)が指定できます。*port1*、*port2*はTCPあるいはUDPポート番号です。設定範囲は0～65535です。*port2*

パラメータ	機能	説明
destination-port *operator port*	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	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)
{ **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マッチします。
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接続パケットにマッチします。

🕮 **メモ：**

lt (lower than)、gt (greater than)、range オプションは、Versio 7.4.30 を含む以降のソフトウェアでサポートされています。
Versio 7.3.24 を含むそれ以前のソフトウェアは、eq (equal) のみをサポートします。

protocol が **icmp** (1)である場合、設定するパラメータを表 1-9 に示します。

表 1-9 拡張 IPv4 ACL ルールの ICMP 指定パラメータ

パラメータ	機能	説明
icmp-type { **icmp-type** *icmp-code* | *icmp-message* }	ICMPメッセージタイプとコードを指定します。	*icmp-type*の設定範囲は0～255です。*icmp-code*の設定範囲は0～255です。*icmp-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 1-10に示します。

表 1-10 拡張 IPv4 ACL ルールでサポートされる ICMP メッセージ名

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

説明

rule コマンドは拡張 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは拡張 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は一意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。

マッチの順番が **config** であるときのみ ACL ルールを修正することができます。

デフォルトの標準 IPv4 ACL ルールと拡張 ACL ルールを表示するには、**display acl all** コマンドを使用します。

オプションのパラメータを指定しないで **undo rule** *rule-id* コマンドを実行すると、ルール全体が削除されます。オプションのパラメータを指定した場合、**undo rule** *rule-id* コマンドはルールに指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドは、ルール全体の削除にのみ使用できます。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**

1.1.16 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。開始ルール ID 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: マッチするパケットを拒否します。

permit: マッチするパケットを許可します。

counting: 標準 IPv4 ACL ルールがマッチした回数をカウントします。**counting** は指定したルールにマッチ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。

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: パケットにマッチするログを指定します。この機能は ACL が logging をサポートするモジュール（たとえばパケットフィルタリング）が必要です。

source { *source-address source-wildcard* | **any** }: 送信元アドレスを定義します。*source-address* と *source-wildcard* はドットで区切られた 10 進数表記の送信元 IP アドレスとワイルドカードマスクを示します。すべてが 0 のワイルドカードはホストアドレスを示します。**any** は、任意の送信元 IP アドレスを示します。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション *7 ACL and QoS* “*タイムレンジ*”を参照してください。

説明

rule コマンドは標準 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は一意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。

マッチの順番が **config** であるときのみ ACL ルールを修正することができます。

このコマンドの **counting** は、ルールに固有のマッチカウントを有効にします。また、**packet-filter** コマンドの **hardware-count** は、ACL 内のすべてのルールについて、ハードウェアでのマッチカウントを有効にします。

デフォルトの標準 IPv4 ACL ルールと拡張 ACL ルールを表示するには、**display acl all** コマンドを使用します。

オプションのパラメータを指定しないで **undo rule** *rule-id* コマンドを実行すると、ルール全体が削除されます。オプションのパラメータを指定した場合、**undo rule** *rule-id* コマンドはルールに指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドは、ルール全体の削除にのみ使用できます。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**

1.1.17 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* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmp6-type** | **logging** | **routing** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type*

icmp6-code | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

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。開始ルール ID 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: マッチするパケットを拒否します。

permit: マッチするパケットを許可します。

protocol: 次のいずれかの値を指定します。

- 0 から 255 の範囲のプロトコル番号です。
- プロトコル番号あるいはプロトコル名を指定します。プロトコル番号の設定範囲は 0～255 です。プロトコル名は **icmpv6**(58)、**ipv6**、**ipv6-ah**(51)、**ipv6-esp**(50)、**tcp**(6)、**udp**(17)があります。**ipv6** はすべてのプロトコルを指定します。

表 1-11 にプロトコルの値に関わらず指定できるパラメータを示します。

表 1-11 拡張 IPv6 ACL ルールのマッチ基準と他のルールの情報

パラメータ	機能	説明
source { *source-address source-prefix* | *source-address*/*source-prefix* | **any** }	送信元IPv6アドレスを指定します。	*dest-address*と*dest-prefix*は送信元IPv6アドレスとプレフィックス長を示します。プレフィックス長の範囲は1～128です。 **any**は、任意の送信元IPv6アドレスを示します。
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。 **any**は、任意の宛先IPv6アドレスを示します。

パラメータ	機能	説明
counting	拡張IPv6 ACLルールがマッチした回数をカウントします。	**counting**は指定したルールにマッチ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	パケットにマッチするログを指定します。	この機能はACLがloggingをサポートするモジュール（たとえばパケットフィルタリング）が必要です。
routing [**type** *routing-type*]	IPv6ルーティングヘッダタイプを指定します。	*routing-type*: IPv6ルーティングヘッダタイプの値です。設定範囲は0～255です。*routing-type*を指定する場合、ルールはIPv6ルーティングヘッダの指定されたタイプを適用します。そうでなければ、IPv6ルーティングヘッダのすべてのタイプを適用します。
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション*7 ACL and QoS* “*タイムレンジ*”を参照してください。

protocol が **tcp**(6)あるいは **udp**(17)である場合、設定するパラメータを表 1-12 に示します。

表 1-12 拡張 IPv6 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port*	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	operatorパラメータには**eq**が指定できます。*port* はTCPあるいはUDPポート番号です。設定範囲は0～65535です。 TCPポート番号は以下の名前で指定できます。**chargen**(19)、**cmd**(514)、**daytime**(13)、**discard**(9)、**dns**(53)、**domain**(53)、**echo**(7)、**exec**(512)、**finger**(79)、**ftp**(21)、**ftp-data**(20)、**gopher**(70)、**hostname**(101)、**irc**(194)、**klogin**(543)、**kshell**(544)、**login**(513)、**lpd**(515)、**nntp**(119)、**pop2**(109)、**pop3**(110)、**smtp**(25)、**sunrpc**(111)、**tacacs**(49)、**talk**(517)、**telnet**(23)、**time**(37)、**uucp**(540)、**whois**(43)、**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)、**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*	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	ACK、FIN、PSH、RST、SYN、URGを含む1つまたは複数のTCPフラグを指定します。	TCP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マッチします。
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接続パケットにマッチします。

protocol が **icmpv6**(58)である場合、設定するパラメータを表 1-13 に示します。

表 1-13 拡張 IPv6 ACL ルールの ICMPv6 指定パラメータ

パラメータ	機能	説明
icmp6-type { *icmp6-type* *icmp6-code* | *icmp6-message* }	ICMPv6メッセージタイプとコードを指定します。	*icmp6-type*の設定範囲は0～255です。 *icmp6-code*の設定範囲は0～255です。 *icmp6-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 1-14 に示します。

表 1-14 拡張 IPv6 ACL ルールでサポートされる ICMPv6 メッセージ名

ICMPv6 メッセージ名	ICMPv6 メッセージタイプ	ICMPv6 メッセージコード
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
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、以下のパラメータを指定できません。

- **fragment** を指定できません。
- ACL が送信アプリケーション用の場合、**routing** または **flow-label** を指定することはできません。
- *protocol* に **ipv6-ah** を指定しないでください。また、ACL が送信アプリケーション用の場合は、その値を 0、43、44、51、または 60 に設定してください。

ACL 内では、各ルールの **permit** または **deny** ステートメントは固有でなければなりません。作成または修正しているルールに、ACL 内の別のルールと同じ **deny** または **permit** ステートメントがある場合、ルールは作成または変更されません。

マッチの順番が **config** であるときのみ ACL ルールを修正することができます。

デフォルトの標準 IPv6 および拡張 ACL ルールを表示するには、**display acl ipv6 all** コマンドを使用します。

オプションのパラメータを指定しないで **undo rule** *rule-id* コマンドを実行すると、ルール全体が削除されます。オプションのパラメータを指定した場合、**undo rule** *rule-id* コマンドはルールに指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドは、ルール全体の削除にのみ使用できます。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 2030:5060::/64～FE80:5060::/96 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。

<Switch> system-view

[Switch] acl ipv6 advanced 3000

[Switch-acl-ipv6-adv-3000] rule permit tcp source 2030:5060::/64 destination fe80:5060::/96 destination-port eq 80

FE80:5060:1001::/48 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。

<Switch> system-view

[Switch] acl ipv6 advanced 3001

[Switch-acl-ipv6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48

[Switch-acl-ipv6-adv-3001] rule permit ipv6

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**

1.1.18 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。開始ルール ID 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: マッチするパケットを拒否します。

permit: マッチするパケットを許可します。

counting: 標準 IPv6 ACL ルールがマッチした回数をカウントします。**counting** は指定したルールにマッチ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。

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: パケットにマッチ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。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 7 *ACL and QoS* ”*タイムレンジ*”を参照してください。

説明

rule コマンドは標準 IPv6 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv6 ACL ルールを削除あるいはルールから属性を削除します。

fragment は、QoS ポリシーまたはパケットフィルタではサポートされていません。

routing は、発信 QoS ポリシーまたはパケットフィルタではサポートされていません。

ACL 内では、各ルールの **permit** または **deny** ステートメントは固有でなければなりません。作成または修正しているルールに、ACL 内の別のルールと同じ **deny** または **permit** ステートメントがある場合、ルールは作成または変更されません。

ACL ルールを修正できるのは、マッチの順番が **config** の場合のみです。

このコマンドの counting は、ルールに固有のマッチカウントを有効にします。また、**packet-filter ipv6** コマンドの **hardware-count** は、ACL 内のすべてのルールのハードウェアでのマッチカウントを有効にします。

デフォルトの標準 IPv6 および拡張 ACL ルールを表示するには、**display acl ipv6 all** コマンドを使用します。

オプションのパラメータを指定しないで **undo rule** *rule-id* コマンドを実行すると、ルール全体が削除されます。オプションのパラメータを指定した場合、**undo rule** *rule-id* コマンドはルールに指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドは、ルール全体の削除にのみ使用できます。コマンドの規則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**

1.1.19 rule (Layer2 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

Layer2 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。開始ルール ID 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: マッチするパケットを拒否します。

permit: マッチ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。802.1 p プライオリティは、次のいずれかの値で指定できます。

- 0~7 の設定範囲です。
- **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 ルールがマッチした回数をカウントします。**counting** は指定したルールにマッチ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。

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。値の設定範囲は 0~ffff です。*lsap-type-mask* は 16 進数表記で LSAP マスクを示します。値の設定範囲は 0 から ffff です。

type *protocol-type protocol-type-mask*: Layer2 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。値の設定範囲は 0~ffff です。*lprotocol-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。値の設定範囲は 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。*source-mask* はマスクを示します。マスクの形式は H-H-H です。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 7 *ACL and QoS* “*タイムレンジ*”を参照してください。

説明

rule コマンドは L2 ACL のルールを作成あるいは修正します。

undo rule コマンドは L2 ACL ルールを削除あるいはルールから属性を削除します。

ACL 内では、各ルールの **permit** または **deny** ステートメントは固有でなければなりません。作成または編集しているルールに、ACL 内の別のルールと同じ **deny** または **permit** ステートメントがある場合、ルールは作成または変更されません。

ACL ルールを編集できるのは、マッチの順番が **config** の場合のみです。

マッチの順番が **config** であるときのみ ACL ルールを修正することができます。

また、packet-filter コマンドの hardware-count キーワードは、ACL 内のすべてのルールについて、ハードウェアでのマッチカウントを有効にします。

デフォルトの Layer2 ACL ルールを表示するには、**display acl mac all** コマンドを使用します。

オプションのパラメータを指定しないで **undo rule** *rule-id* コマンドを実行すると、ルール全体が削除されます。オプションのパラメータを指定した場合、**undo rule** *rule-id* コマンドはルールに指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドは、ルール全体の削除にのみ使用できます。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**

1.1.20 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 のルールのコメントを指定します。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 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。

このコマンドは、ルールに説明がない場合に、ルールに説明を追加します。ルールに既に説明がある場合は、ルールの説明を変更します。

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

1.1.21 step

Syntax

step *step-value*

undo step

デフォルト

ルール番号のステップは 5 で、開始ルール ID は 0 です。

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。ACL ルールの作成時にルール ID を指定しない場合、ルール ID が自動的に割り当てられます。このルール ID は、開始ルール ID から開始して、現在の最大ルール ID までの番号ステップのもっとも近い倍数です。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 0、5、9、10、15 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 **7-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 2-6
2.2 トラフィック動作設定コマンド 2-7
2.2.1 accounting 2-7
2.2.2 car 2-8
2.2.3 display traffic behavior 2-10
2.2.4 filter 2-12
2.2.5 nest top-most 2-13
2.2.6 redirect 2-14
2.2.7 remark dot1p 2-15
2.2.8 remark dscp 2-16
2.2.9 remark local-precedence 2-18
2.2.10 remark service-vlan-id 2-19
2.2.11 traffic behavior 2-20
2.3 QoS ポリシー設定コマンド 2-21
2.3.1 classifier behavior 2-21
2.3.2 display qos policy 2-22
2.3.3 display qos policy global 2-24
2.3.4 display qos policy interface 2-25
2.3.5 display qos vlan-policy 2-29
2.3.6 qos apply policy (interface view) 2-31
2.3.7 qos apply policy global 2-32
2.3.8 qos policy 2-33
2.3.9 qos vlan-policy 2-34
2.3.10 reset qos policy global 2-35
2.3.11 reset qos vlan-policy 2-35

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指定します。

classifier-name: トラフィッククラスを指定します。設定範囲は 1～31 文字です。指定しない場合、すべてのトラフィッククラスを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、マスタ装置のトラフィッククラスを表示します。

説明

display traffic classifier コマンドはトラフィッククラスを表示します。

例

ユーザ定義のすべてのトラフィッククラスを表示します。

<Switch> display traffic classifier user-defined

```
User-defined classifier information:

 Classifier: 1 (ID 100)
   Operator: AND
   Rule(s) :
    If-match acl 2000

 Classifier: 2 (ID 101)
```

```
  Operator: AND
  Rule(s) :
   If-match protocol ipv6

Classifier: 3 (ID 102)
  Operator: AND
  Rule(s) :
   -none-
```

表 2-1 コマンド出力

フィールド	説明
Classifier	トラフィッククラス名と一致条件です。
Operator	トラフィッククラスが一致したときの動作です。動作がANDであるとき、トラフィッククラスはすべての一致条件に一致するパケットにマッチします。動作がORであるとき、トラフィッククラスはいずれかの一致条件に一致するパケットにマッチします。
Rule(s)	一致条件です。

2.1.2 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** | **mac**] { *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。 ● レイヤ2 MAC 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。混乱を避けるため、パラメータがすべてではないことを確認してください。
any	すべてのパケットにマッチするように指定します。
customer-dot1p *dot1p-value*&<1-8>	2重にタグが付いたパケットの内部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* &<1-8>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。
customer-vlan-id *vlan-id-list*	2重にタグが付いたパケットの内部VLANタグのVLAN ID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>のフォーマットで、VALN IDの設定範囲が1～4094の最大10個までのVLAN IDのリストです。*vlan-id1* **to** *vlan-id2*は、VALN IDの範囲を指定します。*vlan-id2*は*vlan-id1*以上で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。
destination-mac *mac-address*	指定した宛先MACアドレスのパケットにマッチするよう指定します。 このオプションは、Ethernetインタフェースでのみ有効です。
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 2-4に示します。
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。

オプション	説明
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-id2*は、*vlan-id1*以上で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。 このオプションを使用すると、単一タグのパケットにマッチさせることができます。
source-mac *mac-address*	指定した送信元MACアドレスのパケットにマッチするよう指定します。 このオプションは、Ethernetインタフェースでのみ有効です。

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。

論理 OR 演算子を持つトラフィッククラスでは、使用可能ないずれかの一致条件に対して複数の **if match** コマンドを設定できます。

1 つの **if-match** コマンドで複数の値を指定できる一致条件を設定する場合は、次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、次のいずれかの一致条件に最大 8 つの値を指定できます。
  - DSCP
  - 802.1p プライオリティ
  - VLAN ID
- パケットが指定された値の 1 つに一致する場合、**if-match** コマンドに一致します。
- 複数の値を持つ条件を削除するには、**undo if-match** コマンドで指定する値は、**if-match** コマンドで指定する値と同じである必要があります。値の順序は異なる場合があります。

ACL ベースの一致条件を設定する場合は、次の制限およびガイドラインに従います。

- ACL はすでに存在している必要があります。
- ACL は分類にのみ使用され、ACL ルールの permit/deny アクションは無視されます。一致するパケットに対して実行されるアクションは、トラフィックの動作で定義されます。

AND とおよび OR 演算子を使用して、クラスの条件の一致関係を定義します。たとえば、トラフィック区分 **classA** の 3 つの一致条件の関連を次のように定義できます。

```
traffic classifier classB operator and
if-match criterion 1
```

```
if-match criterion 2
traffic classifier classA operator or
if-match criterion 3
```

例

トラフィッククラス **class1** の一致条件を定義して、宛先 MAC アドレス 0050-ba27-bed3 のパケットと照合します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match destination-mac 0050-ba27-bed3

トラフィッククラス **class2** の一致条件を定義して、送信元 MAC アドレス 0050-ba27-bed2 のパケットと照合します。

<Switch> system-view

[Switch] traffic classifier class2

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

トラフィッククラス **class1** の一致条件を定義して、外部 VLAN タグの 802.1p プライオリティ 5 パケットと照合します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match service-dot1p 5

トラフィッククラス **class1** の一致条件を定義して、拡張 ACL 3101 のパケットと照合します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match acl 3101

トラフィッククラス **class1** の一致条件を定義して、**flow** という名前の ACL と照合します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match acl name flow

トラフィッククラス **class1** の一致条件を定義して、拡張 IPv6 ACL 3101 と照合します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match acl ipv6 3101

トラフィッククラス **class1** の一致条件を定義して、ACL 名が **flow** の拡張 IPv6 ACL と照合します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match acl ipv6 name flow

トラフィッククラス **class1** の一致条件を定義して、すべてのパケットを照合します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match any

トラフィッククラス **class1** の一致条件を定義して、DSCP が 1、6、9 のパケットと照合します。

<Switch> system-view

[Switch] traffic classifier class1 operator or

[Switch-classifier-class1] if-match dscp 1 6 9

トラフィッククラス **class1** の一致条件を定義して、IP パケットと照合します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match protocol ip

トラフィッククラス **class1** の一致条件を定義して、外部 VLAN タグの VLAN ID が 2、7、10 のパケットと照合します。

<Switch> system-view

[Switch] traffic classifier class1 operator or

[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の名前を指定します。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 コマンドはデフォルトに戻します。

例

トラフィックをバイトでカウントするトラフィック動作 **database** のトラフィックのアカウンティングアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] accounting byte

2.2.2 car

Syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo car

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

cir *committed-information-rate*: CIR（認定情報レート）を kbps 単位で指定します。設定範囲は 1～160000000 です

cbs *committed-burst-size*: CBS（認定バーストサイズ）を byte 単位で指定します。設定範囲は 512～256000000 です。512 の整数倍で設定します。デフォルトは 62.5 と CIR の

積で、512 の整数倍である必要があります。積が 512 の整数倍でないときは、積より大きい 512 の最も近い整数倍に切り上げられます。256000000 バイトを超えることはできません。超えた場合、256000000 バイトとなります。

ebs *excess-burst-size*: EBS（最大許容バーストサイズ）をバイト単位で指定します。設定範囲は 0～256000000 です。512 の整数倍で設定します。デフォルトは 62.5 と PIR の積であり、512 の整数倍である必要があります。積が 512 の整数倍でないときは、最も近い 512 の整数倍に切り上げられます。256000000 バイトを超えることはできません。超えた場合、256000000 バイトとなります。

pir *peak-information-rate*: PIR（最大情報速度）を kbps 単位で指定します。設定範囲は 1～160000000 です。

green *action*: CIR に対応するパケットに対して実施されるアクションを指定します。デフォルトは **pass** です。

red *action*: CIR および PIR のどちらにも対応しないパケットに対して実施されるアクションを指定します。デフォルトは **discard** です。

yellow *action*: PIR に対応し、CIR に対応しないパケットに対して実施されるアクションを指定します。デフォルトは **pass** です。

action: パケットに対して実施されるアクションを指定します。

- **discard**: パケットを廃棄します。
- **pass**: パケットを転送します。
- **remark-dot1p-pass** *new-cos*: 802.1p のパケットに *new-cos* を設定し、パケット転送を許可します。設定範囲は 0～7 です。
- **remark-dscp-pass** *new-dscp*: DSCP のパケットに *new-dscp* を設定し、パケット転送を許可します。設定範囲は 0～63 です。
- **remark-lp-pass** *new-local-precedence*: ローカル優先順位のパケットに *new-local-precedence* を設定し、パケット転送を許可します。設定範囲は 0～7 です。

説明

car コマンドはトラフィック動作に CAR アクションを絶対値で設定します。

undo car コマンドはデフォルトに戻します。

トラフィックポリシーで 2 つのレートを使用するには、**pir** *peak-information-rate* オプションで **car** コマンドを設定してください。トラフィックポリシーで 1 つのレートを使用するには、**pir** *peak-information-rate* オプションなしで **car** コマンドを設定してください。

同一トラフィック動作に **car** コマンドを複数設定した場合、最後に行った設定が適用されます。

⚠ **重要:**

TCP 通信 (例：FTP,CIFS,SMTP,HTTP 等)では、CBS 値が小さいと、再送処理が発生しやすくなり、速度が低下する可能性があります。

CBS 値を十分な大きさに設定することで、再送処理を減らし、速度の低下を防ぎます。下表及び補足に合わせ、CIR と CBS の値を設定してください。

タイプ	CIR		CBS		
	粒度(Kbps)	最大(Kbps)	粒度(Kbps)	最小(B)	最大(B)
3	1,000	102,300,000	512	4,194,304	33,553,920
4	10,000	1,023,000,000	4,096	33,554,432	256,000,000

- CIR を 102,300,000Kbps までの範囲で設定する場合、CIR を 1000Kbps（1Mbps）単位で設定してください。CBS は 4,194,304～33,553,920B の範囲で、かつ 512 の整数倍で設定してください。
- CIR を 102,300,000Kbps を超えて設定する場合（最大 1,023,000,000Kbps まで）、CBS は 33,554,432～256,000,000B の範囲で、かつ 4,096 の整数倍で設定してください。

例

トラフィック動作 **database** に CAR アクションを以下のように設定します。

- CIR を 200kbps、CBS を 51200 バイト、EBS を 0 に設定します。
- 一致するパケットの通過を許可し、DSCP プレシーデンス 0 で超過パケットをマーキングし、転送します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] car cir 200 cbs 51200 ebs 0 green pass red remark-dscp-pass 0

2.2.3 display traffic behavior

Syntax

display traffic behavior user-defined [*behavior-name*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-defined: ユーザ定義のトラフィック動作を指定します。

behavior-name: トラフィック動作を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのトラフィック動作を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置のトラフィック動作を表示します。

説明

display traffic behavior コマンドはトラフィック動作を表示します。

例

すべてのユーザ定義のトラフィック動作を表示します。

<Switch> display traffic behavior user-defined

```
User-defined behavior information:

  Behavior: 1 (ID 100)
    Marking:
      Remark dscp 3
    Committed Access Rate:
      CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
      Green action  : pass
      Yellow action : pass
      Red action    : discard

  Behavior: 2 (ID 101)
    Accounting enable: Packet
    Filter enable: Permit
    Redirecting:
      Redirect to the CPU

  Behavior: 3 (ID 102)
    -none-
```

表 2-3 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。

フィールド	説明
Remark dscp	DSCP値をパケットに設定するアクションです。
Committed Access Rate	CARアクションの情報です。
Green action	greenパケットを適用するアクションです。
Yellow action	yellowパケットを適用するアクションです。
Red action	redパケットを適用するアクションです。
Accounting enable	トラフィックアカウンティングアクションです。
Filter enable	トラフィックフィルタリングアクションです。
Redirecting	トラフィックのリダイレクトに関する情報です。
Mirroring	トラフィックミラーリングに関する情報です。
none	トラフィック動作が設定されていません。

2.2.4 filter

Syntax

filter { **deny** | **permit** }

undo filter

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

deny: パケットを廃棄します。

permit: パケットを転送します。

説明

filter コマンドはトラフィック動作にトラフィックフィルタリングアクションを設定します。

undo filter コマンドはデフォルトに戻します。

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アクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] filter deny

2.2.5 nest top-most

Syntax

nest top-most vlan *vlan-id*

undo nest top-most

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: 追加される VLAN タグの ID を指定します。設定範囲は 1～4094 です。

説明

nest top-most コマンドはトラフィック動作に VLAN タグを追加するアクションを設定します。

undo nest top-most コマンドはデフォルトに戻します。

Qos ポリシーに 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。

nest top-most コマンドを同じトラフィック動作で複数回実行すると、最新の設定が有効になります。

例

トラフィック動作 **b1** に VLAN タグ 123 を追加するアクションを設定します。

<Switch> system-view

[Switch] traffic behavior b1

[Switch-behavior-b1] nest top-most vlan 123

2.2.6 redirect

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* }

undo redirect { **cpu** | **interface** *interface-type interface-number* }

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

cpu: CPU にトラフィックをリダイレクトします。

interface *interface-type interface-number:* タイプと番号を指定されたインタフェースにトラフィックをリダイレクトします。

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 コマンドはデフォルトに戻します。

同じトラフィック動作で **redirect** 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。

トラフィックリダイレクト操作が有効になるのは、QoS ポリシーが入力方向に適用されている場合だけです。

アクセスポートへのトラフィックリダイレクトについては、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 と同じであることを確認します。それ以外の場合、アクセスポートはリダイレクトされたパケットを廃棄します。

トランクポートへのトラフィックリダイレクトについては、QoS ポリシーが適用されるインタフェースの PVID がトランクポートの許可 VLAN リストにあることを確認します。それ以外の場合、トランクポートはリダイレクトされたパケットを廃棄します。

例

トラフィック動作 **database** で GigabitEthernet 1/0/1 にトラフィックをリダイレクトするように設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] redirect interface gigabitethernet 1/0/1

関連コマンド

- **classifier behavior**
- **qos policy**
- **traffic behavior**

2.2.7 remark dot1p

Syntax

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

undo remark [**green** | **red** | **yellow**] **dot1p**

remark dot1p customer-dot1p-trust

undo remark dot1p

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

green: green パケットを指定します。

red: red パケットを指定します。

yellow: yellow パケットを指定します。

dot1p-value: パケットに設定する 802.1p プライオリティを指定します。設定範囲は 0～7 です。

customer-dot1p-trust: 内部 VLAN タグの 802.1p プライオリティを外部 VLAN タグにコピーします。

説明

remark dot1p コマンドは 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 コマンドはデフォルトに戻します。

remark dot1p 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。

同じカラーに対して **remark dot1p** コ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。

802.1 p プライオリティマーキングアクションは、QoS ポリシーが入力方向に適用されている場合にのみ有効になります。

例

トラフィック動作 **database** に 802.1p 2 を設定するアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] remark dot1p 2

トラフィック動作 **database** に内部 VLAN タグから外部 VLAN タグにコピーするアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] remark dot1p customer-dot1p-trust

2.2.8 remark dscp

Syntax

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

undo remark [**green** | **red** | **yellow**] **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 2-4 に示します。

表 2-4 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

キーワード	DSCP 値（バイナリ）	DSCP 値（10 進数）
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 コマンドはデフォルトに戻します。

例

トラフィック動作 **database** の DSCP を 6 にするアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] remark dscp 6

2.2.9 remark local-precedence

Syntax

remark local-precedence *local-precedence-value*

undo remark local-precedence

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

local-precedence-value: パケットに設定するローカルプレシーデンスを指定します。設定範囲は 0～7 です。

説明

remark local-precedence コマンドはトラフィック動作にローカルプレシーデンスアクションを設定します。

undo remark local-precedence コマンドはデフォルトに戻します。

ローカルプレシーデンスアクションは、QoS ポリシーが入力方向に適用されている場合にのみ有効になります。

例

トラフィック動作 **database** 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

2.2.10 remark service-vlan-id

Syntax

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

vlan-id: SVLAN 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 SVLAN マーキングアクションを指定します。

undo remark service-vlan-id コマンドはデフォルトに戻します。

例

トラフィック動作 **b1** に SVLAN222 をマーキングするアクションを設定します。

<Switch> system-view

[Switch] traffic behavior b1

[Switch-behavior-b1] remark service-vlan-id 222

2.2.11 traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

behavior-name: 作成するトラフィック動作の名前を指定します。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 に移行しまするか、デフォルトのトラフィック動作の 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 ポリシーの既存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。*before-classifier-name* には、既存のトラフィッククラスを名前で指定します。設定範囲は 1～31 文字です。大文字と小文字が区別されます。**insert-before** *before-classifier-name* オプションを指定しない場合、新しいトラフィッククラスは QoS ポリシーの最後に配置されます。

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

#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** に関連づけて、**class-a** という名前のデフォルトのトラフィッククラスの前にトラフィッククラス **database** を挿入します。

<Switch> system-view

[Switch] qos policy user1

[Switch-qospolicy-user1] classifier database behavior test insert-before class-a

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 ポリシーを指定します。

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのユーザ定義の QoS ポリシーを表示します。

classifier *classifier-name*: トラフィッククラス名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのトラフィッククラスを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置の QoS ポリシーを表示します。

説明

display qos policy コマンドは QoS ポリシーを表示します。

例

すべてのユーザ定義の QoS ポリシーを表示します。

<Switch> display qos policy user-defined

```
User-defined QoS policy information:

Policy: 1 (ID 100)
 Classifier: 1 (ID 100)
   Behavior: 1
    Marking:
      Remark dscp 3
    Committed Access Rate:
      CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
      Green action  : pass
      Yellow action : pass
      Red action    : discard
 Classifier: 2 (ID 101)
   Behavior: 2
    Accounting enable: Packet
    Filter enable: Permit
    Marking:
      Remark dot1p 4
 Classifier: 3 (ID 102)
   Behavior: 3
    -none-
```

表 2-5 コマンド出力

フィールド	説明
User-defined QoS policy information	ユーザ定義のQoSポリシーに関する情報です。
System-defined QoS policy information	システム定義のQoSポリシーに関する情報です。
Policy	QoSポリシー名です。

他のフィールドの説明は表 2-1、表 2-3 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 ポリシーを指定します。

outbound: 送信方向にグローバルで適用された QoS ポリシーを指定します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のグローバルに適用された QoS ポリシーを表示します。

説明

display qos policy global コマンドはグローバルで適用された QoS ポリシーを表示します。

方向を指定しない場合、受信と送信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

グローバルに適用される汎用 QoS ポリシーを表示します。

<Switch> display qos policy global

```
Direction: Inbound
Policy: 1
 Classifier: 1
   Operator: AND
   Rule(s) :
    If-match acl 2000
   Behavior: 1
    Marking:
      Remark dscp 3
    Committed Access Rate:
      CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
      Green action  : pass
      Yellow action : pass
```

```
    Red action    : discard
    Green packets : 0 (Packets) 0 (Bytes)
    Yellow packets: 0 (Packets) 0 (Bytes)
    Red packets   : 0 (Packets) 0 (Bytes)
Classifier: 2
  Operator: AND
  Rule(s) :
   If-match protocol ipv6
  Behavior: 2
   Accounting enable:
     0 (Packets)
   Filter enable: Permit
   Marking:
     Remark dscp 3
Classifier: 3
  Operator: AND
  Rule(s) :
   -none-
  Behavior: 3
   -none-
```

表 2-6 コマンド出力

フィールド	説明
Direction	QoSポリシーが適用された方向です。
Green packets	greenパケットの統計情報です。
Yellow packets	Yellowパケットの統計情報です。
Red packets	redパケットの統計情報です。

他のフィールドの説明は表 2-1、表 2-3 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 ポリシーを指定します。

outbound: 送信トラフィックに適用された QoS ポリシーを指定します。

説明

display qos policy 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、受信と送信の両方のトラフィックの QoS ポリシーを表示します。

例

GigabitEthernet 1/0/1 の受信方向のトラフィックに適用された QoS ポリシーを表示します。

<Switch> display qos policy interface gigabitethernet 1/0/1 inbound

```
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
```

```
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match protocol ipv6
    Behavior: 2
     Accounting enable:
       0 (Packets)
     Filter enable: Permit
     Marking:
       Remark dscp 3
  Classifier: 3
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     -none-
    Behavior: 3
     -none-
```

すべてのインタフェースに適用される QoS ポリシーを表示します。

<Switch> display qos policy interface

```
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/2
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

```
Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: b
   Classifier: b
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: b
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets)
        Red packets   : 0 (Packets)

Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/4
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

表 2-7 コマンド出力

フィールド	説明
Direction	QoSポリシーが適用される方向です。
Policy	QoSポリシー名です。
Matched	一致したパケットの数です。

フィールド	説明
Forwarded	統計情報収集期間中に正常に転送された一致パケットの平均回数です。
Dropped	統計情報収集期間中に廃棄された一致パケットの平均率です。
Green packets	greenパケットのトラフィックの統計情報です。
Yellow packets	Yellowパケットのトラフィックの統計情報です。
Red packets	redパケットのトラフィックの統計情報です。

他のフィールドの説明は表 2-1、表 2-3 を参照してください。

2.3.5

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 ポリシーを指定します。

outbound: 送信トラフィックに適用された QoS ポリシーを指定します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の VLAN に適用された QoS ポリシーを表示します。

説明

display qos vlan-policy コマンドは VLAN に適用された QoS ポリシーを表示します。

方向を指定しない場合、inbound に適用された QoS ポリシーと outbound 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	QoSポリシーが適用される方向です。
Green packets	greenパケットの統計情報です。
Yellow packets	Yellowパケットの統計情報です。
Red packets	redパケットの統計情報です。

他のフィールドの説明は表 2-1、表 2-3 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: 受信トラフィックに QoS ポリシーを適用します。

outbound: 送信トラフィックに QoS ポリシーを適用します。

説明

qos apply policy コマンドは QoS ポリシーをインタフェースに適用します。

undo qos apply policy コマンドは QoS ポリシーを削除します。

例

GigabitEthernet 1/0/1 の送信トラフィックに適用された QoS ポリシー**USER1** を適用します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos apply policy USER1 outbound

2.3.7 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 コマンドはグローバルに適用された QoS ポリシーを削除します。

グローバルに適用された 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。

最大 2 つの QoS ポリシー(1 つの汎用ポリシーと 1 つのミラーリングタイプ)を、グローバルに一方向に適用できます。

例

グローバルの受信トラフィックに適用された汎用 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 に移行するか、またはデフォルトの QoS policy 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。

オブジェクトに適用されているポリシーを削除するには、最初にオブジェクトからポリシーを削除してください。

例

QoS ポリシー**user1** を作成します。

<Switch> system-view

[Switch] qos policy user1

[Switch-qospolicy-user1]

関連コマンド

- **classifier behavior**

- **qos apply policy**
- **qos apply policy global**
- **qos vlan-policy**

🕮 **メモ：**

- このコマンドと **packet-filter** コマンドを同じポートで使用することはできません。
- **mirror-to** コマンドは、送信ポートでは使用できません。

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 *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* 以上の値にしてください。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: 受信トラフィックにグローバルに適用されるグローバル 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グローバルに適用されるグローバル 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 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、受信と送信の両方のグローバル QoS ポリシーの統計情報を削除します。

例

受信トラフィックにグローバルで適用されたグローバル 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 ポリシーを指定します。

outbound: 送信トラフィックに適用された QoS ポリシーを指定します。

説明

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、受信と送信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 **7-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 “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、ローカルプライオリティ 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

キーワードの説明は表 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。

フィールド	説明
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**—受信したパケットの802.1pプライオリティをマッピングに使用します。 ● **dscp**—受信したIPパケットのDSCPプライオリティをマッピングに使用します。 ● **none**—パケットプライオリティを信頼しません。

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プライオリティを信頼せず、ポートプライオリティをマッピングの 802.1p プライオリティとして使用します。

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設定に戻します。

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 **7-x-x** です。

4 章 GTS、ラインレート 4-1
4.1 GTS 設定コマンド.....4-1
4.1.1 display qos gts interface 4-1
4.1.2 qos gts 4-2
4.2 レートリミットコマンド.....4-3
4.2.1 display qos lr interface 4-3
4.2.2 qos lr 4-4

4章 GTS、ラインレート

4.1 GTS設定コマンド

4.1.1 display qos gts interface

Syntax

display qos gts interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの GTS の設定と統計を表示します。

説明

display qos gts interface コマンドはインタフェースの GTS 設定と統計を表示します。

例

すべてのインタフェースの GTS 設定と統計を表示します。

<Switch> display qos gts interface

```
Interface: GigabitEthernet1/0/1
 Rule: If-match queue 1
  CIR 512 (kbps), CBS 51200 (Bytes)
```

表 4-1 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Rule	一致条件です。
CIR	CIR です。単位は kbps です。
CBS	CBSです。単位はバイトです。

4.1.2 qos gts

Syntax

qos gts queue *queue-id* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts queue *queue-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

queue *queue-id*: ID で指定されたキュー内のパケットを形成します。設定範囲は 0〜7 です。

cir *committed-information-rate*: 平均トラフィックレートを指定する CIR を kbps 単位で指定します。GE インタフェースの設定範囲は 1000〜1048576 です。10GE インタフェースの設定範囲は 1000〜10485760 です。

cbs *committed-burst-size*: CBS をバイト単位で指定します。設定範囲は 512〜16777216 です。512 の整数倍にする必要があります。デフォルトは 62.5 と CIR の積で、512 の整数倍にする必要があります。512 と CIR の積が 512 の整数倍でない場合、512 にもっとも近い値になります。デフォルトが 16777216 より大きい場合は、16777216 に変換されます。

説明

qos gts コマンドはインタフェースのキューに GTS のパラメータを設定します。

undo qos gts コマンドはインタフェースのキューの GTS パラメータを削除します。

例

GigabitEthernet 1/0/1 のキュー1 のパケットに GTS のパラメータを設定します。GTS パラメータは次のとおりです。

- CIR は 6400kbps です。
- CBS は 51200 バイトです。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos gts queue 1 cir 6400 cbs 51200

4.2 レートリミットコマンド

4.2.1 display qos lr interface

Syntax

display qos lr interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのレートリミッ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レートリミットの設定を表示します。

<Switch> display qos lr interface

```
Interface: GigabitEthernet1/0/1
 Direction: Outbound
  CIR 2000 (kbps), CBS 20480 (Bytes)
```

表 4-2 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Direction	レートリミットの設定が適用される方向です。
CIR	CIRです。単位はkbpsです。
CBS	CBSです。単位はバイトです。

4.2.2 qos lr

Syntax

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr { **inbound** | **outbound** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

inbound: 受信パケットのレートを制限します。

outbound: 送信パケットのレートを制限します。

cir *committed-information-rate*: 平均トラフィックレートを指定する CIR を kbps 単位で指定します。GE インタフェースの設定範囲は 1000～1048576 です。10GE インタフェースの設定範囲は 1000～10485760 です。

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、512 にもっとも近い値になります。デフォルトが 134217728 より大きい場合は、134217728 に変換されます。

説明

qos lr コマンドはインタフェースのレート制限を設定します。

undo qos lr コマンドはインタフェースに設定しているレート制限を削除します。

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 **7-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 5-4
5.2.3 qos wrr weight 5-4
5.2.4 qos wrr group sp 5-6
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

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 キューイングを有効にします。

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 キューイングを有効します。

<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IDです。 グループIDは1のみです。
Weight	Packet-count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

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 コマンドはインタフェースで 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 でパケットカウント 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 対応インタフェース上のすべてのキューは WRR グループ 1 にあり、キュー0~7 の重み付けはそれぞれ 1、2、3、4、5、9、13、および 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。

表 5-3 コマンド出力

番号	キーワード
0	be
1	af1
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

group 1: WRR group1 を指定します。QX-S5300G シリーズでは、WRR グループ 1 だけがサポートされています。

weight: パケット内のキューに帯域幅を割り当てます。

schedule-value: スケジューリングの重みを指定します。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の 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 キューイングパラメータを設定する前に、**qos wrr** コマンドを使用して WRR キューイングを有効にする必要があります。

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、WRR グループ 1 にキュー0 を割り当て、キュー0 にスケジューリング重み 10 を指定します。

<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

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。

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。

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。

SP グループのキューは SP で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。

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 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送信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のキューベースの送信トラフィックの統計情報を表示します。

例

GigabitEthernet 1/0/1 でキューベースの送信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	キューに入っている現在のパケットの数です。

関連コマンド

reset counters interface (コマンドマニュアルのセクション 3 *アクセス“Ethernet インタフェース”*)

目次

このセクションのページは **7-x-x** です。

6 章 データバッファ.....6-1
6.1 データバッファ設定コマンド.....6-1
6.1.1 buffer apply.....6-1
6.1.2 buffer shared.....6-1
6.1.3 burst-mode enable.....6-3
6.1.4 display buffer.....6-4

6章 データバッファ

6.1 データバッファ設定コマンド

6.1.1 buffer apply

Syntax

buffer apply

undo buffer apply

View

System view

定義済みユーザロール

network-admin

説明

データバッファの手動設定を適用するには、データバッファの設定後にこのコマンドを実行する必要があります。

手動で設定したデータバッファ設定を適用した後で、適用した設定を直接変更することはできません。設定を変更するには、**undo buffer apply** コマンドで適用された設定を解除してから、新しい値を再設定して **buffer apply** コマンドで再適用する必要があります。

例

buffer shared コマンドによって設定した値を適用します。

<Switch> system-view

[Switch] buffer apply

🕮 **メモ**:

buffer apply コマンドは、Version 7.3.24 以降のソフトウェアからサポートされています。

6.1.2 buffer shared

Syntax

buffer egress [**slot** *slot-number*] **cell** [**queue** *queue-id*] **shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell** [**queue** *queue-id*] **shared**

デフォルト

ポート単位の最大セルリソースは合計セルリソースの 33%

キュー単位の最大セルリソースは合計セルリソースの 33%

View

System view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置をメンバ ID (スロット番号) で指定します。IRF スタックメンバ装置を指定しない場合、このコマンドはすべての IRF スタックメンバ装置に適用されます。

queue *queue-id*: キューID を指定します。設定範囲は 0～7 です。

ratio *ratio*: 共有エリアの最大値を指定します。設定範囲は 0～100%です。

説明

デフォルトでは、すべてのポートまたはキューが共有エリアを均等に共有します。

ポートまたはキューごとに共有エリアの比率を設定できます。各キューの実際の最大共有エリアサイズは、設定値と送受信されるパケット数に基づいて決定されます。未設定のキューはデフォルト設定を使用します。

例

キュー0 の共有エリアの最大セルリソースを 4%に設定します。

<Switch> system-view

[Switch] buffer egress cell queue 0 shared ratio 4

🕮 **メモ：**

- **buffer shared** コマンドは、Version 7.3.24 以降のソフトウェアからサポートされています。
- **buffer shared** コマンドは、SP キューイングなどの輻輳制御を使用する場合のみ設定することを推奨します。また、輻輳制御で使用する場合にはキュー0 から 7 まで以下の設定をしてください。他のパラメータを使用する場合は、使用する前にお使いの環境での事前検証を推奨します。
  buffer egress cell queue 7 shared ratio 4
  buffer egress cell queue 6 shared ratio 4
  buffer egress cell queue 5 shared ratio 4
  buffer egress cell queue 4 shared ratio 4
  buffer egress cell queue 3 shared ratio 4
  buffer egress cell queue 2 shared ratio 4
  buffer egress cell queue 1 shared ratio 4
  buffer egress cell queue 0 shared ratio 4
- データバッファ機能の変更が不適切であると、システムに問題が発生する可能性があります。データバッファ設定を手動で変更する前に、装置への影響を理解しておく必要があります。データバッファ設定を変更する場合は、装置の動作について事前に検証することを推奨します。

6.1.3 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、以下のように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。

例

バースト機能を有効にします。

<Switch> system-view

[Switch] burst-mode enable

6.1.4 display buffer

Syntax

display buffer [**slot** *slot-number*] [**queue** [*queue-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置をメンバ ID (スロット番号) で指定します。IRF スタックメンバ装置を指定しない場合、このコマンドはすべての IRF スタックメンバ装置の情報を表示します。

queue *queue-id*: キューID を指定します。設定範囲は 0～7 です。キューID を指定した場合、指定したキューの固定エリア比率と共有エリア比率を表示します。queue パラメータを指定してキューID を指定しない場合、このコマンドは各キューの固定エリア比率と共有エリア比率を表示します。queue パラメータを指定しない場合、このコマンドはポートの共有エリア比率を表示します。

例

バッファサイズの設定を表示します。

<Switch> display buffer

```
Slot  Type    Eg(Total-shared , Shared)
1     cell    77 , 33


        Eg: Size of the sending buffer
Total-shared: Size of the shared buffer for all ports
     Shared: Size of the maximum shared buffer per port
```

```
       Unit: Ratio
```

キューの専用エリアと共有エリアの設定を表示します。

<Switch> display buffer queue

```
Slot  Queue       Type    Eg(Guaranteed , Shared)
1     0-7         cell    12 , 10


        Eg: Size of the sending buffer
  Guaranteed: Size of the minimum guaranteed buffer per queue
     Shared: Size of the maximum shared buffer per queue
       Unit: Ratio
```

表 6-1 コマンド出力

フィールド	説明
Type	リソースタイプ
Queue	キューID（0～7の範囲）
Eg	出力（Egress）バッファ
(Total-shared , Shared)	● Total-shared：全ポートの共有エリア合計比率 ● Shared：ポートの共有エリア比率
(Guaranteed , Shared)	● Guaranteed：キューの専用エリア比率 ● Shared：キューの共有エリア比率

🕮 **メモ：**

display buffer コマンドは、Version 7.3.24 以降のソフトウェアからサポートされています。

目次

このセクションのページは **7-x-x** です。

7 章 タイムレンジ.....7-1
7.1 タイムレンジ設定コマンド 7-1
7.1.1 display time-range 7-1
7.1.2 time-range 7-2

7章 タイムレンジ

7.1 タイムレンジ設定コマンド

7.1.1 display time-range

Syntax

display time-range { *time-range-name* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

time-range-name: タイムレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。文字列の最初は英字を指定します。

all: 既存のすべてのタイムレンジの設定と状態を表示します。

説明

display time-range コマンドはタイムレンジの設定と状態を表示します。

例

タイムレンジ **t4** の設定と状態を表示します。

<Switch> display time-range t4

```
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2011 to 00:00 1/1/2012
 from 00:00 6/1/2011 to 00:00 7/1/2011
```

表 7-1 コマンド出力

フィールド	説明
Current time	現在のシステム時間です。

フィールド	説明
Time-range	タイムレンジの設定と状態です。タイムレンジ名、状態（activeあるいはinactive）、開始時間、終了時間が含まれます。

7.1.2 time-range

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

time-range-name: タイムレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。文字列の最初は英字を指定します。混乱をさけるため **all** を使用してはいけません。

start-time **to** *end-time*: 周期的なタイムレンジを指定します。*start-time* と *end-time* の形式は hh:mm です。24 時間時計です。*start-time* の設定範囲は 00:00～23:59 です。*end-time* の設定範囲は 00:00～24:00 です。*end-time* は *start-time* よりも大きい値にする必要があります。

days: 周期的なタイムレンジの日時あるいは曜日を指定します。複数の値を指定する場合、スペースで区切ります。値は重複することができません。値は以下のいずれかを指定することができます。

- **0～6**：それぞれ日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日の設定範囲を指定します。
- **Sun**、**Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**：曜日を指定します。
- **working-day**：月曜日～金曜日の営業日を指定します。
- **off-day**：土曜日、日曜日の非営業日を指定します。
- **daily**：一週間の日付を指定します。

from *time1 date1*: 絶対的なタイムレンジの開始時間と開始日を指定します。*time1* は時間を指定します。形式は hh:mm です。24 時間時計です。設定範囲は 00:00～23:59 です。*date1* は日付を指定します。形式は MM/DD/YYYY あるいは YYYY/MM/DD です。MM は 1～12 の月、*DD* は各月の日付、*YYYY* は 1970～2100 の年です。このパラメータを指定しない場合、開始時間と開始日はシステムで有効なもっとも早い時間の 01/01/1970 00:00 AM となります。

to *time2 date2*: 絶対的なタイムレンジの終了時間と終了日を指定します。*time2* は時間を指定します。形式は hh:mm です。24 時間時計です。設定範囲は 00:00～24:00 です。*date2* は日付を指定します。形式は MM/DD/YYYY あるいは YYYY/MM/DD です。MM は 1～12 の月、*DD* は各月の日付、*YYYY* は 1970～2100 の年です。このパラメータを指定しない場合、終了時間と終了日はシステムで有効なもっとも遅い時間の 12/31/2100 24:00 PM となります。

説明

time-range コマンドはタイムレンジを作成あるいは修正します。

undo time-range コマンドはタイムレンジあるいはタイムレンジのパラメータを削除します。

タイムレンジ名が既に存在する場合、タイムレンジのパラメータを追加します。

タイムレンジの複数のパラメータを作成することができます。各時間のパラメータは以下の形式の 1 つを指定することができます。

- *start-time* **to** *end-time days* の形式の周期的なパラメータを指定します。周期的なパラメータは日付あるいは曜日を周期的に繰り返します。
- *from time1 date1* **to** *time2 date2* の形式の絶対的なパラメータを指定します。一度限りで繰り返しません。
- *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* の形式の組み合わせを指定します。指定した期間内で日付あるいは曜日を周期的に繰り返します。たとえば、2015 年 1 月 1 日 00:00～12 月 31 日 23:59 までの月曜日の 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 月と 6 月の月曜日の 10:00～12:00 と水曜日の 14:00～16:00 をアクティブな期間に設定します。

<Switch> system-view

[Switch] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011

[Switch] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011

関連コマンド

display time-range

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

8. セキュリティ

本マニュアルは以下に示す章で構成されています。

01-AAA
02-802.1X
03-MAC アドレス認証
04-Web 認証
05-ポートセキュリティ
06-パスワード管理
07-公開鍵
08-PKI
09-SSH
10-SSL
11-TCP フラグメントアタックプロテクション
12-IP ソースガード
13-ARP アタックプロテクション

目次

このセクションのページは **8-x-x** です。

1 章 AAA 1-1
1.1 AAA 設定コマンド 1-1
1.1.1 aaa session-limit 1-1
1.1.2 accounting default 1-2
1.1.3 accounting lan-access 1-3
1.1.4 accounting login 1-4
1.1.5 accounting start-fail 1-6
1.1.6 accounting update-fail 1-7
1.1.7 authentication default 1-8
1.1.8 authentication lan-access 1-9
1.1.9 authentication login 1-10
1.1.10 authorization command 1-11
1.1.11 authorization default 1-13
1.1.12 authorization lan-access 1-14
1.1.13 authorization login 1-15
1.1.14 display domain 1-17
1.1.15 domain 1-21
1.1.16 domain default enable 1-23
1.1.17 state (ISP domain view) 1-24
1.2 ローカルユーザ設定コマンド 1-25
1.2.1 access-limit 1-25
1.2.2 authorization-attribute (local user view/user group view) 1-26
1.2.3 bind-attribute 1-28
1.2.4 display local-user 1-29
1.2.5 display user-group 1-33
1.2.6 group 1-35
1.2.7 local-user 1-36
1.2.8 password (device management user view) 1-37
1.2.9 password (network access user view) 1-39
1.2.10 service-type 1-40
1.2.11 state (local user view) 1-41
1.2.12 user-group 1-42
1.3 RADIUS 設定コマンド 1-43
1.3.1 accounting-on enable 1-43
1.3.2 data-flow-format (RADIUS scheme view) 1-44
1.3.3 display radius scheme 1-45

1.3.4 display radius statistics 1-50
1.3.5 display stop-accounting-buffer (for RADIUS) 1-51
1.3.6 key (RADIUS scheme view) 1-53
1.3.7 nas-ip (RADIUS scheme view) 1-54
1.3.8 primary accounting (RADIUS scheme view) 1-55
1.3.9 primary authentication (RADIUS scheme view) 1-57
1.3.10 radius dscp 1-59
1.3.11 radius nas-ip 1-60
1.3.12 radius scheme 1-61
1.3.13 reauthentication server-select 1-62
1.3.14 reset radius statistics 1-63
1.3.15 reset stop-accounting-buffer (for RADIUS) 1-64
1.3.16 retry 1-65
1.3.17 retry realtime-accounting 1-66
1.3.18 retry stop-accounting (RADIUS scheme view) 1-67
1.3.19 secondary accounting (RADIUS scheme view) 1-69
1.3.20 secondary authentication (RADIUS scheme view) 1-71
1.3.21 snmp-agent trap enable radius 1-73
1.3.22 state primary 1-74
1.3.23 state secondary 1-75
1.3.24 stop-accounting-buffer enable (RADIUS scheme view) 1-77
1.3.25 timer quiet (RADIUS scheme view) 1-78
1.3.26 timer realtime-accounting (RADIUS scheme view) 1-79
1.3.27 timer response-timeout (RADIUS scheme view) 1-80
1.3.28 user-name-format (RADIUS scheme view) 1-81

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、および Telnet サービスの設定範囲は 1～32 です。HTTP および HTTPS サービスの設定範囲は 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 コマンドは指定したログイン方法のデフォルトの最大同時ユーザ数に戻します。

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、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** では、プライマリデフォルトアカウンティング方式として RADIUS スキーム **rd** を使用し、バックアップとしてローカルアカウンティングを使用します。

<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** では、LAN ユーザに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

ISP ドメイン **test** では、スキーム **rd** をもとにした LAN ユーザには RADIUS アカウンティング方式を使用し、バックアップとしてローカルアカウンティングを使用します。

<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** では、ログインユーザには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

ISP ドメイン **test** では、スキーム **rd** をもとにしたログインユーザには RADIUS アカウンティング方式を設定し、バックアップとしてローカルアカウンティングを使用します。

<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

アカウンティング開始に失敗したユーザがオンライン状態を維持できるようにします。

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に失敗したユーザをログオフします。

online: アカウントの開始に失敗したユーザがオンライン状態を維持できるようにします。

説明

accounting start-fail コマンドはアカウンティングの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を復元します。

例

ISP ドメイン **test** では、アカウンティングの開始に失敗したユーザがオンライン状態を維持できるように装置を設定します。

<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

アカウンティングアップデートに失敗したユーザがオンライン状態を維持できるようにします。

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*: 各ユーザに対して、装置が許容する連続したアカウンティングアップデート失敗の最大数を指定します。**times** の設定範囲は 1～255 です。デフォルトは 1 です。

offline: すべてのアカウンティングアップデートに失敗したユーザをログオフします。

online: すべてのアカウントアップデートに失敗したユーザがオンライン状態を維持できるようにします。

説明

accounting update-fail コマンドはアカウンティングのアップデート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 コマンドはデフォルトを復元します。

例

ISP ドメイン **test** では、すべてのアカウンティングアップデートに失敗したユーザがオンライン状態を維持できるように装置を設定します。

<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** では、プライマリデフォルト認証方式として RADIUS スキーム **rd** を使用し、バックアップとしてローカル認証を使用します。

<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** では、LAN ユーザには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

ISP ドメイン **test** では、スキーム **rd** をもとにした LAN ユーザに RADIUS 認証方式を設定し、バックアップとしてローカル認証を使用します。

<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 { **local** [**none**] | **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** では、ログインユーザにローカル認証を設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authentication login local

ISP ドメイン **test** では、スキーム **rd** にもとづくログインユーザに RADIUS 認証方式を設定し、バックアップとしてローカル認証を使用します。

<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。

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。

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。

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** では、装置に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

関連コマンド

local-user

1.1.11 authorization default

Syntax

authorization default { l**ocal** [**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。

- ログインユーザがレベル 0 のユーザロールを取得します。Telnet、FTP、SFTP、SCP、および端末ユーザが含まれます。端末ユーザは、コンソールポートを介して装置にアクセスできます。レベル 0 ユーザロールについての詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*RBAC*”を参照してください。
- FTP、SFTP ユーザは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。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。
- ログインユーザがネットワークにアクセスできません。

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。

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** では、プライマリデフォルト許可方式として RADIUS スキーム **rd** を使用し、バックアップとしてローカル許可を使用します。

<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** では、LAN ユーザに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

ISP ドメイン **test** では、スキーム **rd** をもとにした LAN ユーザに RADIUS 許可方式を設定し、バックアップとしてローカル許可を使用します。

<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。

- ログインユーザがレベル 0 のユーザロールに割り当てられています。ログインユーザには、Telnet、FTP、SFTP、SCP、および端末ユーザが含まれます。端末ユーザは、コンソールポートを介して装置にアクセスできます。レベル 0 のユーザロールについての詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*RBAC*” を参照してください。
- FTP、SFTP および SCP ユーザは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。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。

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** では、ログインユーザにローカル許可を設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization login local

ISP ドメイン **test** では、スキーム **rd** をもとにしたログインユーザに RADIUS 許可方式を設定し、バックアップとしてローカル許可を使用します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization login radius-scheme rd local

関連コマンド

- **authorization default**
- **local-user**
- **radius scheme**

1.1.14 display domain

Syntax

display domain [*isp-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。ISP ドメインを指定しない場合、すべての ISP ドメインの設定を表示します。

説明

display domain コマンドは ISP ドメインの設定を表示します。

例

すべての ISP ドメインの設定を表示します。

<Switch> display domain

```
Total 2 domains

Domain: system
  State: Active
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
```

```
  Default accounting    scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out policy: Offline
  Service type: HSI
  Session time: Exclude idle time
  Dual-stack accounting method: Merge
  Authorization attributes:
    Idle cut: Disabled
    IGMP access number: 4
    MLD access number:  4

Domain: dm
  State: Active
  Login   authentication scheme:  RADIUS=rad
  Super   authentication scheme:  RADIUS=rad
  LAN access authentication scheme:  RADIUS=r4
  Portal  authentication scheme:  LDAP=ldp
  Default authentication scheme:  RADIUS=rad, Local, None
  Default authorization  scheme:  Local
  Default accounting    scheme:  None
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out policy: Offline
  Service type: HSI
  Session time: Include idle time
  Dual-stack accounting method: Merge
  Authorization attributes:
    Idle cut : Disabled
    IP pool: appy
    User profile: test
    Inbound CAR: CIR 64000 bps PIR 640000 bps
    Outbound CAR: CIR 64000 bps PIR 640000 bps
    ACL number: 3000
    User group: ugg
    IPv6 pool: ipv6pool
    URL: http://test
    IGMP access number: 4
    MLD access number: 4

Default domain name: system
```

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。
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	装置に再接続せずに別のユーザロールを取得するための認証方式です。
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。
Portal authentication scheme	ポータルユーザの認証方式です。
Portal authorization scheme	ポータルユーザの許可メソッドです。
Portal accounting scheme	ポータルユーザのアカウンティング方式です。
RADIUS	RADIUSスキームです。
LDAP	LDAPスキームです。
Local	ローカルスキームです。
None	認証なし、承認なし、またはアカウンティングなしです。

フィールド	説明
Accounting start failure action	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です。 ● **Online**—ユーザはオンライン状態を維持できます。 ● **Offline**—ユーザをログオフします。
Accounting update failure max-times	装置が許可する、ドメイン内の各ユーザの連続したアカウンティングアップデート失敗の最大数です。
Accounting update failure action	すべてのアカウンティングアップデートに失敗したユーザのアクセス制御です。 ● **Online**—ユーザはオンライン状態を維持できます。 ● **Offline**—ユーザをログオフします。
Accounting quota out policy	データ割り当てを使い切ったユーザのアクセス制御です。 ● **Online**—ユーザはオンライン状態を維持できます。 ● **Offline**—ユーザをログオフします。
Service type	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ISPドメインのサービスタイプです。(HSI、STB、VoIPなど)。
Session time	接続障害または誤動作によってオフラインになったユーザのためにサーバに送信されたオンライン期間です。 ● **Include idle time**—オンライン期間には、アイドルタイムアウト期間が含まれます。 ● **Exclude idle time**—オンライン期間にはアイドルタイムアウト期間は含まれません。
Dual-stack accounting method	このフィールドは、QX-S5300Gシリーズではサポートしていません。 デュアルスタックユーザのアカウンティング方法です。 ● **Merge**—IPv4データをアカウンティング用のIPv6データとマージします。 ● **Separate**—アカウンティング用にIPv4データとIPv6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	このフィールドは、QX-S5300Gシリーズではサポートしていません。 アイドルカットフィーチャー状態です。 ● **Enabled**—この機能は有効です。この装置は、トラフィックの最小要件を満たさないユーザをアイドルタイムアウト期間中にログオフします。 ● **Disabled**—この機能は無効です。デフォルトのアイドルカット状態です。

フィールド	説明
IP pool	認証IPv4アドレスプール名です。
User profile	許可ユーザプロファイル名です。
Inbound CAR	許可インバウンドCARです。 ● **CIR**—認定情報レート(bps)です。 ● **PIR**—ピーク情報レート(bps)です。 着信CARが許可されていない場合、このフィールドには「**N/A**」と表示されます。
Outbound CAR	許可発信CARです。 ● **CIR**—認定情報レート(bps)です。 ● **PIR**—ピーク情報レート(bps)です。 アウトバウンドCARが許可されていない場合、このフィールドには「**N/A**」と表示されます。
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。
IPv6 pool	ユーザの認可IPv6アドレスプール名です。
URL	ユーザの許可リダイレクトURLです。
IGMP max access number	IPv4ユーザが同時に参加することを認可されるIGMPグループの最大数です。 このフィールドは、QX-S5300Gシリーズではサポートしていません。
MLD max access number	IPv6ユーザが同時に参加することを認可されるMLDグループの最大数です。 このフィールドは、QX-S5300Gシリーズでは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。名前は、次の要件を満たしている必要があります。

- 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(@)を含めることはできません。
- d、de、def、defa、defau、defaul、default、i、if、if-、if-u、if-un、if-unk、if-unkn、if-unkno、if-unknow、あるいは if-unknown は使用できません。

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。

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が、異なるタイプのユーザを必要とする最大長を超えないようにするには、短いドメイン名を使用します。

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。ISP ドメインがすでに存在している必要があります。

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 ISP ドメインを削除することはできません。

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 ユーザまたは SCP ユーザには適用されません。これらのユーザはアカウンティングをサポートしていません。

このコマンドをネットワークアクセスユーザに有効にするには、ISP ドメイン view で **accounting start-fail offline** コマンドも実行する必要があります。

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

- **accounting start-fail offline**
- **display local-user**

1.2.2 authorization-attribute (local user view/user group view)

Syntax

authorization-attribute { **acl** *acl-number* | **idle-cut** *minutes* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **idle-cut** | **user-role** *role-name* | **vlan** | **work-directory** } *

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 またはレベル 15 ユーザによって作成されたローカルユーザには、ネットワークオペレーターユーザロールが割り当てられます。

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 2000～4999 です。装置は、ルールの **permit** または **deny** ステートメントに基づいて、許可 ACL のルールに一致するトラフィックを処理します。

idle-cut *minutes*: アイドルタイムアウト時間を分単位で設定します。設定範囲は 1～120 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-role *role-name*: 許可されたユーザロールを指定します。設定範囲は 1～63 です。ユーザに 64 のユーザロールを指定することができます。ユーザロールに関するコマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに* “*RBAC*” を参照してください。このオプションは local user view でのみ有効で、user group view では無効です。

vlan *vlan-id*: 許可 VLAN を指定します。設定範囲は 1～4094 です。認証にパスし、VLAN が許可されたのち、ローカルユーザは VLAN のリソースのみアクセスすることができます。

work-directory *directory-name*: FTP、SFTP または SCP 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。

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**、**VLAN** のみが適用できます。

SSH、Telnet、および端末ユーザの場合、許可属性 **idle-cut** および **user-role** のみが有効になります。

HTTP および HTTPS ユーザの場合、許可属性 **user-role** のみが有効になります。

FTP ユーザの場合、許可属性 **user-role** および **work-directory** のみが有効になります。

ローカルユーザの他のタイプは、許可属性は適用されません。

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。

FTP、SFTP、および SCP ユーザが IRF スタックマスタ/下位スイッチオーバー後にディレクトリにアクセスできるようにするには、作業ディレクトリのスロット情報を指定しないでください。

ユーザが許可されたユーザロールのみ適用させるため、あらかじめ定義されたユーザロールを削除するために **undo authorization-attribute user-role** コマンドを使用してください。

例

ネットワークアクセスユーザ **abc** の許可される VLAN を VLAN 2 として設定します。

<Switch> system-view

[Switch] local-user abc class network

[Switch-luser-network-abc] authorization-attribute vlan 2

ユーザグループ **abc** の許可される VLAN を VLAN3 として設定します。

<Switch> system-view

[Switch] user-group abc

[Switch-ugroup-abc] authorization-attribute vlan 3

関連コマンド

- **display local-user**
- **display user-group**

1.2.3 bind-attribute

Syntax

bind-attribute { **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **ip** | **location** | **mac** | **vlan** } *

デフォルト

設定なし

View

Local user view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: ユーザの IP アドレスを指定します。このオプションは 802.1X ユーザのみ適用可能です。

location interface *interface-type interface-number*: ユーザのインタフェースを指定します。*interface-type* はインタフェースタイプ、*interface-number* はインタフェース番号を示します。認証にパスするため、ユーザはインタフェースを通してネットワークにアクセスする必要があります。このオプションは LAN ユーザのみ適用可能です。

mac *mac-address*: ユーザの MAC アドレスを指定します。形式は H-H-H です。このオプションは LAN ユーザのみ適用可能です。

vlan *vlan-id*: ユーザが所属する VLAN を指定します。設定範囲は 1～4094 です。このオプションは LAN ユーザのみ適用可能です。

説明

bind-attribute コマンドはローカルユーザのバインディング属性を設定します。

undo bind-attribute コマンドはローカルユーザのバインディング属性を削除します。

バインディング属性は、ローカルユーザの認証時に確認されます。

ローカルユーザのバインディング属性が設定と一致しない場合、あるいは必要な属性が不足している場合、ユーザの認証は失敗します。

バインド属性チェックは、すべてのアクセスサービスで有効になります。アクセスサービスに基づいてユーザのバインド属性を設定検索し、装置がユーザのパケットからチェックされるすべての属性を取得できることを確認します。たとえば、802.1X 認証ではパケットにユーザの IP アドレスを含めることができるため、802.1X ユーザの IP アドレスバインディングを設定できます。ただし、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 アドレスバインディングを設定することはできません。

バインディングインタフェースタイプは、ローカルユーザの要件を満たす必要があります。ユーザのサービスタイプに基づいてインタフェース設定をバインドします。

- 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 認証が有効なレイヤ 2 Ethernet インタフェースを指定します。
- ユーザが Web 認証ユーザの場合、Web 認証が有効なレイヤ 2 Ethernet インタフェースを指定します。

例

MAC アドレス 11-11-11 をネットワークアクセスユーザ **abc** にバインドします。

<Switch> system-view

[Switch] local-user abc class network

[Switch-luser-network-abc] bind-attribute mac 11-11-11

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** | **https** | **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。

https: HTTPS ユーザを指定します。

lan-access: 802.1X ユーザなど、通常はイーサネット経由でネットワークにアクセスする LAN 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が、使用中のアカウンティングサービスを停止するように要求することができます。

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。名前は、次の要件を満たしている必要があります。

- 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(\)、縦棒(|)、コロン(:)、アスタリスク(*)、疑問符(?)、小なり記号(<)、大なり記号(>)、アットマーク(@)を含めることはできません。
- **a**、**al**、または **all** にすることはできません。

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。

フィールド	説明
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。
IP pool	ローカルユーザに認可されたIPv4アドレスプールです。
IPv6 pool	ローカルユーザに認可されたIPv6アドレスプールです。
Password control configurations	ローカルユーザ用に設定されたパスワード制御属性です。
Password aging	パスワードの有効期限です。
Password length	パスワードに必要な最小文字数です。
Password composition	このフィールドはパスワードの構成のポリシーチェック機能が有効であるときのみ表示されます。フィールドは括弧で以下のように表示されます。 • 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	このフィールドはパスワードの複雑性のポリシーチェック機能が有効であるときのみ表示されます。フィールドは括弧で以下のように表示されます。 • 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。

フィールド	説明
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削除された最新時刻です。
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有効になり始める日付と時刻です。
Expiration date and time	ネットワークアクセスユーザの有効期限が切れる日時です。

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名を指定します。

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	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	セッションタイムアウトタイマです。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あるいはSCPユーザのディレクトリです。
ACL number	許可ACLです。
VLAN ID	許可VLANです。
User profile	許可ユーザプロファイルです。
IP pool	ユーザグループに許可されたIPv4アドレスプールです。
IPv6 pool	ユーザグループに許可されたIPv6アドレスプールです。
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	パスワードの有効期限です。
Password length	パスワードの最小パスワード長です。

フィールド	説明
Password composition	このフィールドはパスワードの構成のポリシーチェック機能が有効であるときのみ表示されます。フィールドは括弧で以下のように表示されます。 • 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	このフィールドはパスワードの複雑性のポリシーチェック機能が有効であるときのみ表示されます。フィールドは括弧で以下のように表示されます。 • 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: 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。名前は、次の要件を満たしている必要があります。

- 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(|)、コロン(:)、アスタリスク(*)、疑問符(?)、小なり記号(<)、大なり記号(>)、アットマーク(@)は使えません。
- **a**、**al**、または **all** にすることはできません。

class: ローカルユーザタイプを指定します。指定しない場合、コマンドは装置管理ユーザを追加します。

manage: ログイン後に装置の設定、モニタを行うユーザです。装置管理ユーザは、FTP、HTTP、HTTPS、Telnet、SSH、端末サービスを使用することができます。

network: 装置を介してネットワークリソースにアクセスするネットワークアクセスユーザです。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: 802.1X ユーザなど、通常はイーサネット経由でネットワークにアクセスする LAN 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、その view に移行するか、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、localuser 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、localuser 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 (device management user view)

Syntax

password [{ **hash** | **simple** } *string*]

undo password

デフォルト

装置管理ユーザにはパスワードがなく、正しいユーザ名を入力し、属性チェックにパスした後で認証にパスできます。

View

Device management user view

定義済みユーザロール

network-admin

パラメータ

hash: ハッシュアルゴリズムによって暗号化されたパスワードを指定します。

simple: パスワードをプレーンテキスト形式で指定します。セキュリティ保護のため、プレーンテキスト形式で指定されたパスワードは暗号化された形式で保存されます。

string: パスワード文字列を指定します。大文字、小文字を区別します。パスワードのハッシュ形式は 1～110 文字です。パスワードのプレーンテキスト形式は、1～63 文字の文字列です。

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 コマンドはデフォルトに戻します。

パラメータを指定しない場合は、インタラクティブモードに入り、プレーンテキストのパスワードを設定します。

パスワードが指定されていない装置管理ユーザは、正しいユーザ名を入力し、属性チェックにパスした後、認証にパスできます。セキュリティを強化するには、装置管理ユーザごとにパスワードを設定します。

例

装置管理ユーザ **user1** のパスワード **123456TESTplat&!**をプレーンテキストで設定します。

<Switch> system-view

[Switch] local-user user1 class manage

[Switch-luser-manage-user1] password simple 123456TESTplat&!

装置管理ユーザ **test** のパスワードをインタラクティブモードで設定します。

<Switch> system-view

[Switch] local-user test class manage

[Switch-luser-manage-test] password

```
Password:
confirm :
```

関連コマンド

display local-user

🕮 **メモ**：

Ver7.2.23 を含む以降のソフトウェアでは、パスワード管理機能によってデフォルト値は以下の条件に制限されています。

- プレーンテキストの最小文字数は 10 文字以上です。
- プレーンテキストの最小文字タイプ数は 2 種類以上です。
- ローカルユーザ名に使用した文字列（逆の文字列も含む）は使用できません。
- 上記の制限を解除する場合は、パスワード管理機能の **undo password-control length enable** コマンド、**undo password-control composition enable** コマンド、**undo password-control complexity user-name check** コマンドを設定します。

1.2.9 password (network access user view)

Syntax

password { **cipher** | **simple** } *string*

undo password

デフォルト

ネットワークアクセスユーザにはパスワードがなく、正しいユーザ名を入力して属性チェックに合格すると、認証をパスできます。

View

Network access user view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号化形式でパスワードを指定します。

simple: パスワードをプレーンテキスト形式で指定します。セキュリティ保護のため、プレーンテキスト形式で指定されたパスワードは暗号化された形式で保存されます。

string: パスワード文字列を指定します。プレーンテキスト形式は、大文字、小文字を区別します。設定範囲は 1～63 文字です。暗号化形式は、大文字、小文字を区別します。設定範囲は 1～117 文字です。

説明

password コマンドはネットワークアクセスユーザのパスワードを設定します。

undo password コマンドはデフォルトに戻します。

セキュリティを強化するため、ネットワークアクセスユーザごとにパスワードを設定します。

例

装置管理ユーザ **user1** 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 user1 class network

[Switch-luser-network-user1] password simple 123456TESTuser&!

関連コマンド

display local-user

1.2.10 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: ユーザが HTTP サービスを使用することを許可します。

https: ユーザが HTTPS サービスを使用することを許可します。

lan-access: LAN アクセスサービスの使用をユーザに許可します。ユーザは通常、イーサネットユーザ(802.1X ユーザなど)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

1.2.11 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:ローカルユーザがネットワークサービスを要求しないように、現在のローカルユーザをブロック状態にします。

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

1.2.12 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、その view に移行するか、デフォルトの user group 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。

1 つまたは複数の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*: アカウンティングパケットを再送信する間隔を秒単位で指定します。interval の設定範囲は 1～15 です。デフォルトは 3 です。

send *send-times*: アカウンティングパケット送信の最大試行回数を指定します。send-times の設定範囲は 1～255 です。デフォルトは 50 です。

説明

accounting-on enable コマンドはアカウンティング機能を設定します。

undo accounting-on enable コマンドはアカウンティング機能を無効にします。

アカウンティング機能は装置がリブート後に自動的にアカウンティングパケットを RADIUS サーバに送ることを可能にします。アカウンティングパケットを受信すると、RADIUS サーバはすべてのオンラインユーザをログアウトし、装置を介して再度ログインできるようにします。

save コマンドを実行して、次回の装置再起動時に **accounting-on enable** コマンドが有効になることを確認します。**save** コマンドの詳細については、オペレーションマニュアルのセクション 1 *はじめに* を参照してください。

accounting-on enable コマンドを使用して設定されたパラメータは、すぐに有効になります。

例

RADIUS スキーム **radius1** のアカウンティング機能を有効にし、再送間隔を 5 秒、送信試行回数を 15 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: 単位を byte として指定します。

giga-byte: 単位を giga-byte で指定します。

kilo-byte: 単位を kilo-byte で指定します。

mega-byte: 単位を mega-byte で指定します。

packet: データパケットの単位を指定します。

giga-packet: 単位を giga-packet として指定します。

kilo-packet: 単位を kilo-packet として指定します。

mega-packet: 単位を mega-packet に指定します。

one-packet: ユニットを one-packet として指定します。

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:
    Host name: Not configured
    IP   : 2.2.2.2                          Port: 1812
    VPN  : vpn1
    State: Active
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
    Weight: 40
  Primary accounting server:
    Host name: Not configured
    IP   : 1.1.1.1                          Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 40
  Second authentication server:
    Host name: Not configured
    IP   : 3.3.3.3                          Port: 1812
    VPN  : Not configured
    State: Block
    Test profile: Not configured
    Weight: 40
  Second accounting server:
    Host name: Not configured
    IP   : 3.3.3.3                          Port: 1813
    VPN  : Not configured
    State: Block (Mandatory)
    Weight: 0
  Accounting-On function                  : Enabled
    extended function                     : Disabled
    retransmission times                  : 5
    retransmission interval(seconds)      : 2
  Timeout Interval(seconds)               : 3
  Retransmission Times                    : 3
```

```
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)             : 5
  Realtime Accounting Interval(seconds)     : 22
  Stop-accounting packets buffering         : Enabled
    Retransmission times                   : 500
  NAS IP Address                           : 1.1.1.1
  VPN                                      : Not configured
  User Name Format                          : with-domain
  Data flow unit                           : Megabyte
  Packet unit                              : One
  Attribute 15 check-mode                   : Strict
  Attribute 25                             : CAR
  Attribute Remanent-Volume unit            : Mega
  server-load-sharing                       : Enabled
  Attribute 31 MAC format                   : hh:hh:hh:hh:hh:hh
  Stop-accounting-packet send-force         : Disabled
------------------------------------------------------------------
```

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。
Host name	サーバのホスト名です。 このフィールドは以下の状況では**Not configured**と表示されます。 ● サーバが設定されていません。 ● サーバのIPアドレスが設定されていません。
IP	サーバのIPアドレスです。 このフィールドは以下の状況では**Not configured**と表示されます。 ● サーバが設定されていません。 ● ホスト名でサーバが指定されており、ホスト名解決ができません。

フィールド	説明
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、デフォルトのポート番号を表示します。
VPN	サーバまたはRADIUSスキームが属するVPNインスタンスです。サーバにVPNインスタンスが指定されていない場合、このフィールドには**Not configured**と表示されます。 このフィールドは、QX-S5300Gシリーズでは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な状態です。 ● **Block**－サーバは自動的にブロックされた状態に変更されます。 ● **Block(Mandatory)**－サーバは手動でブロック状態に設定されます。
Test profile	RADIUSサーバの状態検出に使用されるテストプロファイルです。
Probe username	RADIUSサーバの状態検出に使用されるユーザ名です。
Probe interval	サーバ状態検出間隔です。単位は分です。
Weight	RADIUSサーバのウェイト値です。
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	最大アカウンティング試行回数です。
Server Quiet Period(minutes)	サーバの停止時間です。単位は分です。
Realtime Accounting Interval(seconds)	リアルタイムアカウンティングアップデートの送信間隔です。単位は秒です。
Stop-accounting packets buffering	応答のないRADIUS Stop-Accounting要求のバッファリングが有効かどうかを示します。

フィールド	説明
Retransmission times	個々のRADIUS Stop-Accounting要求に対する送信試行の最大回数です。
NAS IP Address	送信RADIUSパケットの送信元IPアドレスです。送信RADIUSパケットの送信元IPアドレスが指定されていない場合、このフィールドには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	データフローの測定単位です。
Packet unit	パケットの測定単位です。
Attribute 15 check-mode	RADIUSがSSH、FTP、端末ユーザのログインサービスの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アトリビュート25の解釈状態です。 ● **Standard**—この属性はCARパラメータとして解釈されません。 ● **CAR**—この属性はCARパラメータとして解釈されます。
Attribute Remanent-Volume unit	RADIUS Remanent_Volume属性のデータ測定単位です。
server-load-sharing	RADIUSサーバロードシェアリング機能の状態です。 ● **Disabled**—この機能は無効です。装置は、プライマリおよびセカンダリサーバの役割に基づいて選択されたサーバにトラフィックを転送します。 ● **Enabled**—この機能は有効です。この装置は,負荷分散のために複数のサーバ間にトラフィックを分配します。
Attribute 31 MAC format	RADIUSアトリビュート31のMACアドレスフォーマットです。
Stop-accounting-packet send-force	開始アカウンティングパケットが送信されないユーザがオフラインになったときに、装置が強制的に停止アカウンティングパケットを送信できるかどうかです。

1.3.4 display radius statistics

Syntax

display radius statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display radius statistics コマンドは RADIUS パケットの統計情報を表示します。

例

RADIUS パケットの統計情報を表示します。

<Switch> display radius statistics

```
                        Auth.        Acct.      SessCtrl.
      Request Packet:       0            0            0
       Retry Packet:        0            0            -
     Timeout Packet:        0            0            -
  Access Challenge:         0            -            -
     Account Start:         -            0            -
    Account Update:         -            0            -
      Account Stop:         -            0            -
 Terminate Request:         -            -            0
         Set Policy:        -            -            0
Packet With Response:       0            0            0
Packet Without Response:    0            0            -
    Access Rejects:         0            -            -
    Dropped Packet:         0            0            0
    Check Failures:         0            0            0
```

表 1-5 コマンド出力

フィールド	説明
Auth.	認証パケットです。
Acct.	アカウンティングパケットです。

フィールド	説明
SessCtrl.	セッションコントロールパケットです。
Request Packet	パケット要求数です。
Retry Packet	パケット要求が再送された数です。
Timeout Packet	パケット要求がタイムアウトした数です。
Access Challenge	アクセスチャレンジを行ったパケット数です。
Account Start	スタートアカウンティング要求のパケット数です。
Account Update	アップデートアカウンティング要求のパケット数です。
Account Stop	ストップアカウンティング要求のパケット数です。
Terminate Request	強制的にユーザをログオフするためのパケット数です。
Set Policy	ユーザ許可情報をアップデートするパケット数です。
Packet With Response	応答が受信されたパケット数です。
Packet Without Response	応答が受信されていないパケット数です。
Access Rejects	アクセス拒否のパケット数です。
Dropped Packet	廃棄されたパケット数です。
Check Failures	チェックサムエラーのパケット数です。

関連コマンド

reset radius statistics

1.3.5 display stop-accounting-buffer (for RADIUS)

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。

session-id *session-id*: セッションを ID で指定します。設定範囲は 1～64 文字です。文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一意に識別します。

time-range *start-time end-time*: 時間範囲を指定します。開始時刻と終了時刻は、hh:mm:ss-mm/dd/yyyy または hh:mm:ss-yyyy/mm/dd の形式で指定してください。

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。大文字、小文字を区別します。**user-name** にドメイン名を含めるかどうかは、RADIUS スキームの **user-name-format** コマンドを使用して設定した設定によって異なります。

説明

display stop-accounting-buffer コマンドは応答を受信していないバッファリングされた RADIUS stop-accounting 要求の情報を表示します。

例

ユーザ **abc** 用にバッファされた応答のない RADIUS stop-accounting 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
```

フィールド	説明
Session ID	セッションIDです。Acct-Session-Idの属性値です。
First sending time	アカウンティング停止要求が最初に送信された時刻です。
Attempts	アカウンティング停止要求を送信しようとした回数です。

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鍵を設定します。

authentication: セキュアな RADIUS 認証の通信を行うために共有鍵を設定します。

cipher: 暗号テキストの共有鍵を設定します。

simple: プレーンテキストの共有鍵を設定します。セキュリティ保護のため、プレーンテキスト形式で指定された鍵は暗号化された形式で保存されます。

string: 共有鍵を指定します。大文字、小文字を区別します。暗号化された形式の設定範囲は 1～117 文字です。プレーンテキスト形式の設定範囲は 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 通信を行うために共有鍵を設定します。

undo key コマンドはセキュリティの高いセキュアな RADIUS 通信を行うために共有鍵を削除します。

このコマンドを使用して設定された共有鍵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鍵と一致していることを確認してください。

指定した RADIUS サーバの共有鍵は **key** コマンドで指定された共有鍵よりも優先されます。

例

RADIUS スキーム **radius1** の共有鍵 **ok** をプレーンテキストで設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] key accounting simple ok

関連コマンド

display radius scheme

1.3.7 nas-ip (RADIUS scheme view)

Syntax

nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo nas-ip [**ipv6**]

デフォルト

サーバへ送信されるパケットの送信元 IP アドレスは、system view の **radius nas-ip** コマンドを使用して指定されます。

radius nas-ip コマンドが設定されていない場合、送信元インタフェースの IP アドレスがパケットの送信元 IP アドレスとなります。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: 装置の IPv4 アドレスを指定します。0.0.0.0、255.255.255.255、クラス D アドレス、クラス E アドレス、ループバックアドレスを指定することはできません。

ipv6 *ipv6-address*: 装置の IPv6 アドレスを指定します。装置のユニキャストアドレスを指定します。ループバックアドレス、リンクローカルアドレスを指定することはできません。

説明

nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを設定します。

undo nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを削除します。

NAS が送信した RADIUS パケットの送信元 IP アドレスは RADIUS サーバに設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバは IP アドレスで NAS を識別します。RADIUS パケットを受信すると、RADIUS サーバは、パケットの送信元 IP アドレスが管理 NAS の IP アドレスであるかどうかチェックします。

- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致する場合、サーバはパケットを処理します。
- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致しない場合、サーバはパケットを廃棄します。

物理ポートエラーによって引き起こされる RADIUS パケット損失を避けるために、送信 RADIUS パケットの送信元 IP アドレスとしてループバックインタフェースアドレスを指定します。

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 の設定は、system view の設定よりも優先されます。

RADIUS スキームは、送信 RADIUS パケット用に 1 つの送信元 IPv4 アドレスと 1 つの送信元 IPv6 アドレスのみを持つことができます。

undo nas-ip コマンドに ipv6 を指定しない場合、コマンドは送信 RADIUS パケット用に設定された送信元 IPv4 アドレスを削除します。

例

サーバへ送信される RADIUS パケットの送信元アドレス 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 { *host-name* | *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

host-name: プライマリ RADIUS アカウンティングサーバの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。

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: プライマリ RADIUS アカウンティングサーバとの安全な通信のために共有鍵を指定します。

cipher: 暗号化形式で鍵を指定します。

simple: プレーンテキスト形式の鍵を指定します。セキュリティ保護のため、プレーンテキスト形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵を指定します。大文字、小文字を区別します。鍵の暗号化形式の設定範囲は、1～117 文字です。鍵の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 コマンドはデフォルトを復元します。

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鍵の設定は、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鍵は **key accounting** コマンドで設定された共有鍵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。

- RADIUS サーバのロードシェアリング機能が無効になっている場合、装置はアカウンティングの優先順位が最も高いアクティブサーバとの通信を試みます。
- RADIUS サーバのロードシェアリング機能を有効にすると、装置は別のアクティブなアカウンティングサーバを検索するのではなく、アカウンティング失敗メッセージを返します。

もしアクティブな使用されているアカウンティングサーバを削除する場合、装置はユーザのリアルタイムアカウンティング要求とストップアカウンティング要求を送信しません。ストップアカウンティング要求を保持することはできません。装置は不正確なアカウンティングの結果を生成する可能性があります。

例

RADIUS スキーム **radius1** に IP アドレス 10.110.1.2、UDP ポート番号 1813、プレーンテキスト共有鍵 **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 { *host-name* | *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

host-name: プライマリRADIUS認証サーバの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。

ipv4-address: プライマリ RADIUS 認証サーバの IPv4 アドレスを指定します。

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

port-number: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: プライマリ RADIUS 認証サーバとのセキュア通信のための共有鍵を指定します。

cipher: 暗号化形式で鍵を指定します。

simple: プレーンテキスト形式の鍵を指定します。セキュリティ保護のため、プレーンテキスト形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵を指定します。大文字、小文字が区別されます。設定範囲は 1～117 文字です。鍵のプレーンテキストの設定範囲は、1～64 文字です。

説明

primary authentication コマンドはプライマリ RADIUS 認証サーバを指定します。

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

プライマリ RADIUS 認証サーバのポート番号と共有鍵の設定は、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鍵は **key authentication** コマンドで設定された共有鍵よりも優先されます。

認証プロセス中に 1 次認証コマンドを使用して 1 次認証サーバを変更または削除すると、1 次サーバとの通信がタイムアウトになります。

- RADIUS サーバのロードシェアリング機能が無効になっている場合、装置は認証に最も高い優先順位を持つアクティブサーバとの通信を試みます。
- RADIUS サーバのロードシェアリング機能が有効になっている場合、装置は次の操作を実行します。
  - 各アクティブサーバの現在サービスを受けているユーザの数を確認します。
  - AAA 要求を受信するためにパフォーマンスが最も適切なサーバを決定します。

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鍵 **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、このコマンドは IPv4 RADIUS パケットの DSCP 優先順位を設定します。

dscp-value: RADIUS パケットの DSCP 優先順位の設定範囲は 0～63 です。値が大きいほど、優先順位が高くなります。

説明

radius dscp コマンドは RADIUS パケットの DSCP 優先順位を変更します。

undo radius dscp コマンドはデフォルトに戻します。

伝送の優先順位を変更するために RADIUS パケットの ToS フィールドに DSCP の優先順位を設定するために使用します。

例

IPv4 RADIUS パケットの DSCP 優先順位を 10 に設定します。

<Switch> system-view

[Switch] radius dscp 10

1.3.11 radius nas-ip

Syntax

radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

デフォルト

送信 RADIUS 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 IPv4 アドレスまたは IPv6 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

ipv4-address: 装置の IPv4 アドレスを指定します。0.0.0.0、255.255.255.255、クラス D アドレス、クラス E アドレス、ループバックアドレスを指定することはできません。

ipv6 *ipv6-address*: 装置の IPv6 アドレスを指定します。装置のユニキャストアドレスを指定します。ループバックアドレス、リンクローカルアドレスを指定することはできません。

説明

radius nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを設定します。

undo radius nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを削除します。

NAS が送信した RADIUS パケットの送信元 IP アドレスは RADIUS サーバに設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバは IP アドレスで NAS を識別します。RADIUS パケットを受信すると、RADIUS サーバは、パケットの送信元 IP アドレスが管理 NAS の IP アドレスであるかどうかチェックします。

- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致する場合、サーバはパケットを処理します。
- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致しない場合、サーバはパケットを廃棄します。

物理ポートエラーによる RADIUS パケットの損失を防ぐために、送信 RADIUS パケットの送信元 IP アドレスとしてループバックインタフェースアドレスを指定します。

nas-ip コマンドと **radius nas-ip** コマンドの両方を使用する場合は、次のガイドラインが適用されます。

- RADIUS scheme view で **nas-ip** コマンドを使用して設定した設定は、RADIUS スキームにのみ適用されます。
- system view で **radius nas-ip** コマンドを使用して設定した設定は、すべての RADIUS 方式に適用されます。
- RADIUS scheme view の設定は、system view の設定よりも優先されます。

以下の IP アドレスを含む最大 16 の送信元 IP アドレスを指定できます。

- 0 または 1 つのパブリックネットワーク送信元 IPv4 アドレス
- 0 または 1 つのパブリックネットワーク送信元 IPv6 アドレス
- プライベートネットワーク送信元 IP アドレス

例

サーバへ送信される RADIUS パケットの送信元アドレス 129.10.10.1 を設定します。

<Switch> system-view

[Switch] radius nas-ip 129.10.10.1

関連コマンド

nas-ip (RADIUS scheme view)

1.3.12 radius scheme

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

radius-scheme-name: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

radius scheme コマンドは RADIUS スキームを作成し、RADIUS scheme view に移行します。

undo radius scheme コマンドは RADIUS スキームを削除します。

RADIUS スキームは、同時に 2 つ以上の ISP ドメインから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

🕮 **メモ：**

reauthentication server-select コマンドは、Version 7.1.8 以降のソフトウェアからサポートされています。

Syntax

reauthentication server-select { **inherit** | **reselect** }

undo reauthentication server-select

デフォルト

inherit モード

View

RADIUS scheme view

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指定します。

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。ネットワーク状況により、以下のどちらかのモードを使用します。

- **Inherit**—装置は、ユーザの認証を実行した RADIUS サーバを使用して、そのユーザを再認証します。このモードで再認証に要する時間を短縮できます。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**—装置は到達可能な RADIUS サーバを検索してユーザを再認証します。このモードは、inherit モードよりも時間がかかりますが、装置は確実に再認証に最適な到達可能な RADIUS サーバを使用します。RADIUS サーバの選択には、次の要因が影響します。
  - 設定順序を含む、RADIUS スキームでのサーバ設定。
  - RADIUS サーバの負荷共有機能の有効化状態。
  - RADIUS スキームでの RADIUS サーバの状態。

例

RADIUS スキーム **radius1** で、RADIUS サーバ選択モードを再認証用に再選択するように設定します

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] reauthentication server-select reselect

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 統計情報を消去します。

例

RADIUS 統計情報を消去します。

<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 文字です。大文字、小文字を区別しません。

session-id *session-id*: セッションを ID で指定します。*session-id* の設定範囲は、1～64 文字です。文字を含めることはできません。セッション ID は、RADIUS scheme のオンラインユーザを一意に識別します。

time-range *start-time end-time*: 時間範囲を指定します。開始時刻と終了時刻は、hh:mm:ss-mm/dd/yyyy または hh:mm:ss-yyyy/mm/dd の形式で指定してください。

user-name *user-name*: ユーザ名を指定します。大文字、小文字を区別します。設定範囲は 1～255 文字です。*user-name* にドメイン名を含めるかどうかは、RADIUS スキームの **user-name-format** コマンドを使用して設定した設定によって異なります。

説明

reset stop-accounting-buffer コマンドは応答を受信していないバッファ RADIUS の stop-accounting 要求を削除します。

例

ユーザ **user0001@test** にバッファリングされた応答のない RADIUS 停止アカウンティング要求を削除します。

<Switch> reset stop-accounting-buffer user-name user0001@test

2015 年 8 月 31 日に 0:0:0 から 23:59:59 にバッファリングされた応答のない RADIUS 停止アカウンティング要求を削除します。

<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。

応答タイムアウト時間内に RADIUS サーバからの要求に対する応答を装置が受信しない場合、装置は RADIUS 要求を再送信します。応答のタイムアウト時間を設定するには、タイマの **response-timeout** コマンドを使用します。

最大送信試行回数に達しても RADIUS サーバからの応答を受信しない場合、装置は要求が失敗したと見なします。

認証プロセス中にクライアントがタイムアウトになると、ユーザはただちにログオフされます。ユーザのログオフを回避するため、次のアイテムを乗算した値は、アクセスモジュールで定義されたクライアントのタイムアウト時間より長くすることはできません。

- RADIUS パケット送信の最大試行回数
- RADIUS サーバの応答タイムアウト時間
- RADIUS スキーム内の RADIUS 認証サーバの数

装置が新しい RADIUS サーバに RADIUS 要求を送信すると、RADIUS パケットの送信にかかった合計時間がチェックされます。この時間が 300 秒に達すると、装置は次の RADIUS サーバへの RADIUS 要求の送信を停止します。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期間を設定するときは、RADIUS サーバの数を検討します。

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 NAS からユーザへのリアルタイムアカウンティングパケットを受け取らなければ、回線または装置に不具合があるとみなします。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、次の条件が存在します。

- RADIUS サーバの応答タイムアウト時間は 3 秒(**timer response-timeout** コマンドを使用して設定)です。
- RADIUS パケットの送信試行の最大数は 3(**retry** コマンドを使用して設定)です。
- リアルタイムアカウンティングの間隔は 12 分(**timer realtime-accounting** コマンドを使用して設定)です。
- アカウンティングの最大試行回数は 5 回(**retry realtime-accounting** コマンドを使用して設定する)です。

上記の場合、装置は 12 分ごとにアカウンティング要求を生成し、要求を送信して 3 秒以内に応答を受信しない場合は要求を再送信します。要求を 3 回送信しても応答がない場合、装置はアカウンティングの試行が失敗したと見なし、再度アカウンティングを試行します。アカウンティングに 5 回連続して失敗すると、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

最大数は 500 です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries: 送信試行の最大回数を指定します。設定範囲は 10～65535 です。

説明

retry stop-accounting コマンドは個々の RADIUS 停止アカウンティング要求に対する送信試行の最大回数を設定します。

undo retry stop-accounting コマンドはデフォルトに戻します。

stop accounting 要求の送信試行の最大数は、次のパラメータとともに stop accounting 要求の送信を制御します。

- RADIUS サーバの応答タイムアウトのタイマ(**timer response-timeout** コマンドを使用して設定)です。
- ラウンドごとに RADIUS パケットを送信する最大回数(**retry** コマンドを使用して設定)です。

たとえば、次の設定があります。

- RADIUS サーバの応答タイムアウトタイマは 3 秒です。
- ラウンドごとに RADIUS パケットを送信する最大回数は 5 です。
- アカウンティング停止要求の送信試行の最大数は 20 です。

装置が 3 秒以内に応答を受信しない場合、アカウンティング停止要求が再送信されます。このラウンドの 5 回の送信試行すべてが使用されると、装置は要求をバッファし、再送信の別のラウンドを開始します。20 回連続して失敗すると、装置は要求を破棄します。

例

RADIUS スキーム **radius1** について、アカウンティング要求送信の最大試行回数を 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 { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *

undo secondary accounting [{ *host-name* | *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

host-name: セカンダリ RADIUS アカウンティングサーバの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。

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: secondary RADIUS アカウンティングサーバと安全に通信するための共有鍵を指定します。

cipher: 暗号化形式で鍵を指定します。

simple:プレーンテキスト形式の鍵を指定します。セキュリティ保護のため、プレーンテキスト形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵を指定します。大文字、小文字を区別します。鍵の暗号化形式の設定範囲は、1～117 文字です。鍵のプレーンテキストは、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鍵の設定は、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。

このコマンドで設定された共有鍵は、**key accounting** コマンドで設定された共有鍵よりも優先されます。

secondary accounting コマンドを使用して、装置がアカウンティング開始要求を送信しているセカンダリアカウンティングサーバを変更または削除すると、セカンダリサーバとの通信がタイムアウトします。

- RADIUS サーバのロードシェアリング機能が無効になっている場合、装置はアカウンティングの優先順位が最も高いアクティブサーバとの通信を試みます。
- RADIUS サーバのロードシェアリング機能を有効にすると、装置は別のアクティブなアカウンティングサーバを検索するのではなく、アカウンティング失敗メッセージを返します。

アクティブに使用されているアカウンティングサーバを削除すると、装置はユーザのリアルタイムアカウンティング要求とアカウンティング停止要求を送信しなくなります。装置は、停止アカウンティング要求もバッファリングしません。

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 { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *

undo secondary authentication [{ *host-name* | *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

host-name: セカンダリRADIUS認証サーバの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。

ipv4-address: セカンダリ RADIUS 認証サーバの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: セカンダリ RADIUS 認証サーバの IPv6 アドレスを指定します。

port-number: セカンダリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: 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: 暗号化形式で鍵を指定します。

simple: プレーンテキスト形式の鍵を指定します。セキュリティ保護のため、プレーンテキスト形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵を指定します。大文字、小文字を区別します。鍵の暗号化形式の設定範囲は、1～117 文字です。鍵のプレーンテキストの設定範囲は、1～64 文字です。

説明

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

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

セカンダリ RADIUS 認証サーバのポート番号と共有鍵の設定は、サーバで設定された値と同一にしてください。

RADIUS スキームに最大 16 のセカンダリ RADIUS 認証サーバを設定することができます。プライマリサーバが故障したとき、装置はアクティブ状態のセカンダリサーバと通信しようとします。装置は設定された順番でセカンダリサーバと接続します。

スキームのプライマリとセカンダリの 2 つの認証サーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

このコマンドで設定された共有鍵は、**key authentication** コマンドで設定された共有鍵よりも優先されます。

認証プロセス中に **secondary authentication** コマンドを使用して 2 次認証サーバを変更または削除すると、2 次サーバとの通信がタイムアウトになります。

- RADIUS サーバのロードシェアリング機能が無効になっている場合、装置は認証に最も高い優先順位を持つアクティブサーバとの通信を試みます。
- RADIUS サーバのロードシェアリング機能が有効になっている場合、装置は次の操作を実行します。
  - □ 各アクティブサーバの現在サービスを受けているユーザの数を確認します。
  - □ AAA 要求を受信するためにパフォーマンスが最も適切なサーバを決定します。

例

RADIUS スキーム **radius1** に IP アドレス 10.110.1.2、UDP ポート番号 1812 のセカンダリ認証サーバを指定します。

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] secondary authentication 10.110.1.2 1812
```

RADIUS スキーム **radius2** の 2 つのセカンダリ認証サーバの IP アドレスを 10.110.1.1 と 10.110.1.2、UDP ポートを 1812 に指定します。

```
<Switch> system-view
[Switch] radius scheme radius2
[Switch-radius-radius2] secondary authentication 10.110.1.1 1812
[Switch-radius-radius2] secondary authentication 10.110.1.2 1812
```

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **primary authentication (RADIUS scheme view)**

1.3.21 snmp-agent trap enable radius

Syntax

snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

undo snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

accounting-server-down: RADIUS アカウンティングサーバに到達不能になったとき、notification を送信します。

accounting-server-up: RADIUS アカウンティングサーバに到達可能になったとき、notification を送信します。

authentication-error-threshold: 認証の失敗がしきい値を超過したとき、notification を送信します。しきい値は認証を試行する総数に対する認証失敗の割合を示します。設定範囲は 1～100%です。デフォルトは 30%です。しきい値は MIB を通してのみ設定できます。

authentication-server-down: RADIUS 認証サーバに到達不能になったとき、notification を送信します。

authentication-server-up: RADIUS 認証サーバに到達可能になったとき、notification を送信します。

説明

snmp-agent trap enable radius コマンドは RADIUS の SNMP notification 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 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 を有効または無効にします。

RADIUS の SNMP notification が有効であるとき、SNMP エージェントは RADIUS によって作成された以下の notification をサポートします。

- **RADIUS server unreachable notification**－RADIUS サーバに通信できません。指定した RADIUS 要求の再送信の最大試行回数以内にアカウンティング要求あるいは認証要求に対する応答を受信できない場合、RADIUS は notification を作成します。
- **RADIUS server reachable notification**－RADIUS サーバと通信できます。RADIUS サーバが停止タイマの満了後、以前にブロックされた RADIUS サーバに対して notification を作成します。
- **Excessive authentication failures notification**－認証を行った際、失敗した総数が指定したしきい値を超過しています。

例

SNMP エージェントが RADIUS アカウンティングサーバに到達不能になったとき、notification を送信します。

<Switch> system-view

[Switch] snmp-agent trap enable radius accounting-server-down

1.3.22 state primary

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

デフォルト

active

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: プライマリ RADIUS アカウンティングサーバの状態を設定します。

authentication: プライマリ RADIUS 認証サーバの状態を設定します。

active: RADIUS サーバの状態を **active**（正常稼動の状態）に設定します。

block: RADIUS サーバの状態を **block** 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。

RADIUS サーバのロードシェアリング機能を無効にすると、プライマリサーバがアクティブ状態である場合、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。

RADIUS サーバのロードシェアリング機能が有効になっている場合、装置はアクティブ状態のサーバについてのみ現在サービスされているユーザの数をチェックします。最も適切なアクティブサーバが通信用に選択されます。

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になると、装置はプライマリサーバとの通信を試みます。

例

RADIUS スキーム **radius1** のプライマリ認証サーバの状態を blocked 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** } [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *] { **active** | **block** }

デフォルト

active

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: セカンダリ RADIUS アカウンティングサーバの状態を設定します。

authentication: セカンダリ RADIUS 認証サーバの状態を設定します。

host-name: セカンダリ RADIUS サーバの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。

ipv4-address: セカンダリ RADIUS サーバの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: セカンダリ RADIUS サーバの IPv6 アドレスを指定します。

port-number: セカンダリ RADIUS サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。セカンダリ RADIUS 認証サーバのデフォルトは 1812 です。セカンダリ RADIUS アカウンティングサーバのデフォルトは 1813 です。

active: RADIUS サーバの状態を **active**（正常稼動の状態）に設定します。

block: RADIUS サーバの状態を **block** 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。設定されているすべてのセカンダリサーバにアクセスできない場合、装置は認証またはアカウンティングの試みが失敗したと見なします。

RADIUS サーバのロードシェアリング機能が有効になっている場合、装置はアクティブ状態のサーバについてのみ現在サービスされているユーザ数をチェックします。最も適切なアクティブサーバが通信用に選択されます。

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 blocked 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

装置は、応答を受信していない RADIUS stop-accounting 要求をバッファリングします。

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信していない RADIUS stop-accounting 要求のバッファを有効にします。

undo stop-accounting-buffer enable コマンドはバッファ機能を無効にします。

このコマンドは、最大の送信試行(retry コマンドを使用して設定する)が行われた後、応答のない RADIUS stop-accounting 要求を装置がバッファリングできるようにします。装置は、サーバ応答を受信するか、アカウンティングストップ要求の送信試行回数が上限に達するまで、バッファリングされた要求を再送信します。これ以上、試行できない場合、装置は要求を破棄します。ただし、アカウンティングサーバを削除した場合、そのサーバ宛ての停止アカウンティング要求はバッファに格納されません。

例

応答を受信していない RADIUS Stop-Accounting 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分単位で指定します。設定範囲は 1～255 です。

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** の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: リアルタイムアカウンティングの間隔を指定します。設定範囲は 0～71582 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 1-6 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

ユーザ数	リアルタイムのアカウンティング間隔
1000以上	15分以上

例

RADIUS スキーム **radius1** のリアルタイムのアカウンティング間隔を 51 分に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] timer realtime-accounting 51

関連コマンド

retry realtime-accounting

1.3.27 timer response-timeout (RADIUS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

デフォルト

3 秒

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

seconds: RADIUS サーバの応答タイムアウト時間を指定します。設定範囲は 1～10 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。

認証プロセス中にクライアントがタイムアウトになると、ユーザはただちにログオフされます。ユーザのログオフを回避するため、次のアイテムを乗算した値は、アクセスモジュールで定義されたクライアントのタイムアウト時間より長くすることはできません。

- RADIUS パケット送信の最大試行回数です。
- RADIUS サーバの応答タイムアウト時間です。
- RADIUS スキーム内の RADIUS サーバの数です。

装置が新しい RADIUS サーバに RADIUS 要求を送信すると、RADIUS パケットの送信にかかった合計時間がチェックされます。この時間が 300 秒に達すると、装置は次の RADIUS サーバへの RADIUS 要求の送信を停止します。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期間を設定するときは、RADIUS サーバの数を検討します。

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

ISP ドメイン名は、RADIUS サーバに送信されるユーザ名に含まれます。

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。

EAP 認証を使用する 802.1X ユーザの場合、RADIUS スキームに設定された **user-name-format** コマンドは有効になりません。装置は、RADIUS サーバに転送する前にクライアントのユーザ名を変更しません。

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 **8-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 2-6
2.1.3 dot1x 2-9
2.1.4 dot1x access-user log enable 2-10
2.1.5 dot1x authentication-method 2-11
2.1.6 dot1x auth-fail vlan 2-13
2.1.7 dot1x guest-vlan 2-14
2.1.8 dot1x handshake 2-15
2.1.9 dot1x handshake reply enable 2-16
2.1.10 dot1x mandatory-domain 2-17
2.1.11 dot1x max-user 2-18
2.1.12 dot1x multicast-trigger 2-18
2.1.13 dot1x port-control 2-19
2.1.14 dot1x port-method 2-20
2.1.15 dot1x quiet-period 2-21
2.1.16 dot1x re-authenticate 2-22
2.1.17 dot1x retry 2-23
2.1.18 dot1x timer 2-24
2.1.19 dot1x timer reauth-period 2-26
2.1.20 dot1x unicast-trigger 2-27
2.1.21 reset dot1x guest-vlan 2-28
2.1.22 reset dot1x statistics 2-29

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 キーワードあるいは **statistics** キーワード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* オプションを指定しない場合、すべてのグローバルおよびポート固有の 802.1X 情報を表示します。

例

802.1X のすべての情報を表示します。

<Switch> display dot1x

```
Global 802.1X parameters:
  802.1X authentication  : Enabled
  CHAP authentication    : Enabled
  Max-tx period         : 30 s
  Handshake period      : 15 s
  Quiet timer           : Disabled
       Quiet period     : 60 s
  Supp timeout          : 30 s
```

```
  Server timeout        : 100 s
  Reauth period         : 3600 s
  Max auth requests     : 2
  EAD assistant function : Disabled
     URL              : http://www.dwsoft.com
     Free IP          : 6.6.6.0       255.255.255.0
     EAD timeout      : 30 min
  Domain delimiter      : @
Online 802.1X wired users    : 1

GigabitEthernet1/0/1  is link-up
  802.1X authentication     : Enabled
  Handshake                 : Enabled
  Handshake reply           : Disabled
  Handshake security        : Disabled
  Unicast trigger           : Disabled
  Periodic reauth           : Disabled
  Port role                 : Authenticator
  Authorization mode        : Auto
  Port access control       : Port-based
  Multicast trigger         : Enabled
  Mandatory auth domain     : Not configured
  Guest VLAN                : 3
  Auth-Fail VLAN            : Not configured
  Critical VLAN             : Not configured
  Critical voice VLAN       : Disabled
  Add Guest VLAN delay      : Disabled
  Re-auth server-unreachable : Logoff
  Max online users          : 4294967295
  User IP freezing          : Disabled
  Reauth period             : 0 s
  Send Packets Without Tag   : Disabled
  Max Attempts Fail Number   : 0
  Guest VSI                 : Not configured
  Auth-Fail VSI             : Not configured
  Critical VSI              : Not configured
  Add Guest VSI delay       : Disabled

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
      EAP Request/Challenge packets: 1
      EAP Success packets: 1
      EAP Failure packets: 0
```

```
Received EAPOL Start packets : 1
        EAPOL LogOff packets: 1
        EAP Response/Identity packets : 1
        EAP Response/Challenge packets: 1
        Error packets: 0
Online 802.1X users: 1
      MAC address        Auth state
      0001-0000-0000     Authenticated
```

表 2-1 コマンド出力

フィールド	説明
Global 802.1X parameters	グローバル802.1Xの設定です。
802.1X authentication	802.1Xがグローバルで有効かどうかを示します。
CHAP authentication	RADIUSサーバと通信する際にEAPを終端しCHAPを実行しています。
EAP authentication	RADIUSサーバと通信する際にEAPパケットの中継とEAP認証のいずれかを実行しています。
PAP authentication	RADIUSサーバと通信する際にEAPを終端しPAPを実行しています。
Max-tx period	ユーザ名の要求タイムアウトタイマです。単位は秒です。
Handshake period	ハンドシェイクタイマです。単位は秒です。
Quiet timer	停止タイマの状態をenabledあるいはdisabledで示します。
Quiet period	停止タイマです。単位は秒です。
Supp timeout	クライアントタイムアウトタイマです。単位は秒です。
Server timeout	サーバタイムアウトタイマです。単位は秒です。
Reauth period	定期再認証タイマです。単位は秒です。
Max auth requests	認証要求をクライアントに送信する最大試行回数です。
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。

フィールド	説明
Domain delimiter	装置がサポートするドメインデリミタです。
Online 802.1X wired users	有線のオンライン802.1Xユーザ数です。802.1X認証にパスしたユーザおよび802.1X認証を実行しているユーザを含みます。
GigabitEthernet1/0/1 is link-up	ポートの状態です。たとえば、GigabitEthernet 1/0/1がupです。
802.1X authentication	802.1Xがポートで有効かを示します。
Handshake	オンラインユーザハンドシェイク機能がポートで有効かを示します。
Handshake reply	オンラインユーザハンドシェイク応答機能がポートで有効かを示します。
Handshake security	オンラインユーザハンドシェイクセキュリティ機能がポートで有効かを示します。
Unicast trigger	802.1Xユニキャストトリガがポートで有効かを示します。
Periodic reauth	802.1Xの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のいずれかです。
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。 802.1X critical VLANが設定されていない場合、**Not configured**と表示されます。
Critical voice VLAN	802.1X critical voice VLAN機能がポートで有効かを示します。

フィールド	説明
Add Guest VLAN delay	ポートの802.1X guest VLAN割り当て遅延機能の状態とモードです。 ● **EAPOL**— EAPOLトリガの802.1 X guest VLAN割り当て遅延が有効になります。 ● **NewMac**— MACがトリガする新しい802.1 X guest VLAN割り当て遅延を有効にします。 ● **ALL**— EAPOLでトリガされた802.1 X guest VLAN割り当て遅延と、MACでトリガされた新しい802.1 X guest VLAN割り当て遅延の両方が有効になります。 ● **Disabled**—802.1 X guest VLAN割り当て遅延は 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。
User IP freezing	ポートでユーザIPフリージングが有効かを示します。
Reauth period	ポートでのタイマの定期的な再認証です。単位は秒です。
Send Packets Without Tag	ポートから802. 1Xクライアントに送信されるすべての802. 1Xプロトコルパケットの VLANタグを削除するかどうかを示します。
Max Attempts Fail Number	MAC認証ユーザに対する802. 1X認証の最大試行回数です。
Guest VSI	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ポートに802.1X guest VSIが設定されています。
Auth-Fail VSI	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ポートに802.1X Auth-Fail VSIが設定されています。
Critical VSI	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ポートに802.1X Critical VSIが設定されています。
Add Guest VSI delay	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ポートの802.1X guest VSI割り当て遅延機能の状態とモードです。
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。

フィールド	説明
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および802.1X認証を実行しているユーザを含みます。
MAC address	オンライン802.1XユーザのMACアドレスです。
Auth state	オンライン802.1Xユーザの認証状態です。

2.1.2 display dot1x connection

Syntax

display dot1x connection [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *name-string*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。ポートが指定されない場合、すべてのポートのオンライン 802.1X ユーザの情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのオプションが指定されない場合、すべての IRF スタックのメンバ装置のオンライン 802.1X ユーザの情報を表示します。

user-mac *mac-address*: 802.1X ユーザの MAC アドレスを指定します。形式は H-H-H です。802.1X ユーザを指定しない場合、すべてのオンライン 802.1X ユーザ情報を表示します。

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。802.1X ユーザを指定しない場合、すべてのオンライン 802.1 X ユーザ情報を表示します。

説明

display dot1x connection コマンドはオンライン 802.1X ユーザの情報を表示します。

例

すべてのオンライン 802.1X ユーザの情報を表示します。

<Switch> display dot1x connection

```
Total connections: 1

Slot ID: 1
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: nec
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
Initial VLAN: 1
Authorization untagged VLAN: 6
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33
29 31 33
                          35 37 40 to 100
Authorization VSI: N/A
Authorization ACL ID: 3001
Authorization user profile: N/A
Authorization CAR:
  Average input rate: 102400
  Peak input rate: 204800
  Average output rate: 102400
  Peak output rate: 204800
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

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**—ユーザは802.1X認証にパスし、オンラインになります。 • **Open**—ユーザは、存在しないユーザ名または不正なパスワードを使用して、open認証モードでオンラインになります。
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アドレスを取得しない場合、このフィールドは使用できません。
IPv6 address	ユーザのIPv6アドレスです。 装置がユーザのIPv6アドレスを取得しない場合、このフィールドは利用できません。
Authentication method	EAPメッセージ操作方式です。 • **CHAP**–RADIUSサーバと通信するEAPを終端しCHAPを実行しています。 • **EAP**–RADIUSサーバと通信する際にEAPパケットの中継とEAP認証のいずれかを実行しています。 • **PAP**–RADIUSサーバと通信する際にEAPを終端しPAPを実行しています。
Initial VLAN	802.1X認証を行う前にユーザが所属するVLANです。
Authorization untagged VLAN	ユーザに許可されたタグなしVLANです。
Authorization tagged VLAN list	ユーザに許可されたタグづけVLANです。
Authorization VSI	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ユーザに認定されたVSIです。
Authorization ACL ID	ユーザに許可されたACLです。 ACL許可が失敗した場合、このフィールドは、ACL IDの後に(**Not effective**)と表示します。
Authorization user profile	ユーザに許可されたユーザプロファイルです。

フィールド	説明
Authorization CAR	サーバによって割り当てられた承認CAR属性です。 • **Average input rate**—bps単位のインバウンドトラフィックの平均速度です。 • **Peak input rate**—bps単位のインバウンドトラフィックのピークレートです。 • **Average output rate**—bps単位のアウトバウンドトラフィックの平均レートです。 • **Peak output rate**—bps単位のアウトバウンドトラフィックのピークレートです。 サーバがピークレートを割り当てない場合、デフォルトのピークレートは割り当てられた平均レートと同じになります。QX-S5300Gシリーズでは、装置はサーバからのピークレートの排他的割り当てをサポートしていません。 Authorization CAR属性が割り当てられていない場合、このフィールドには**N/A**と表示されます。
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 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。

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

🕮 **メモ：**

QX-S5300G シリーズは最大 100PPS まで認証できます。

2.1.4 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: リアルタイムアカウンティングの失敗や再認証の失敗によって発生するログオフなど、802.1X ユーザの例外的なログオフに対して生成されるログを指定します。

failed-login: 802.1X ユーザのログインに失敗した場合に生成されるログを指定します。

normal-logoff: 802.1X ユーザが要求したログオフに対して生成されるログを指定します。

successful-login: 802.1X ユーザの正常なログインに対して生成されるログを指定します。

説明

dot1x access-user log enable コマンドは 802.1X ユーザのロギングを有効にします。

undo dot1x access-user log enable コマンドは 802.1X ユーザのロギングを無効にします。

802.1X ユーザが過度にログを出力しないようにするには、この機能を無効にすることを推奨します。

パラメータを指定しない場合、802.1X ユーザのすべてのログ機能を有効にします。

例

802.1X ユーザのログイン失敗のロギングを有効にします。

<Switch> system-view

[Switch] dot1x access-user log enable failed-login

関連コマンド

info-center source dot1x logfile deny (コマンドマニュアルのセクション 10 *システム管理*)

2.1.5 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、コマンドマニュアルのセクション 8 *セキュリティ* “*AAA*”を参照してください。

RADIUS 認証が使用されると、RADIUS サーバとして同じ認証方式（PAP、CHAP、EAP）を使用するようにアクセス装置を設定する必要があります。

例

EAP パケットを終端するアクセス装置を有効にし、RADIUS サーバで PAP 認証を実行します。

<Switch> system-view

[Switch] dot1x authentication-method pap

関連コマンド

display dot1x

2.1.6 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。制限 VLAN のユーザは、限られたネットワークリソースにアクセスできます。

802.1X 制限 VLAN として設定された VLAN を削除するためには、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 VLAN100 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

2.1.7 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 を削除するためには、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

2.1.8 dot1x handshake

Syntax

dot1x handshake

undo dot1x handshake

デフォルト

RJ-45 ポート: 無効

他のポート: 有効

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を使用すると、装置は EAP-Request/Identity パケットをクライアントに定期的に送信して、オンライン 802.1X ユーザの接続状態を確認できます。ユーザ期間内に最大試行回数を超えてもユーザから EAP-Response/Identity パケットを受信しない場合、装置はハンドシェイク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には、**dot1x timer handshake-period** コマンドを使用します。最大ハンドシェイク試行回数を設定するには、**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**

2.1.9 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。

このコマンドは、装置がオンラインハンドシェイクプロセス中に EAP-Success パケットで 802.1X クライアントの EAP-Response/Identity パケットに応答できるようにします。

802.1X クライアントが装置から EAP-Success パケットを受信せずにオフラインになる場合にのみ、このコマンドを使用します。

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

2.1.10 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 コマンドはデフォルトに戻します。

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

2.1.11 dot1x max-user

Syntax

dot1x max-user *max-number*

undo dot1x max-user

デフォルト

ポートは、最大 4294967295 の同時 802.1X ユーザを許可します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

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。

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

2.1.12 dot1x multicast-trigger

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

デフォルト

RJ-45 ポート: 無効

他のポート: 有効

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**

2.1.13 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、拒否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

2.1.14 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

2.1.15 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**

2.1.16 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、サーバに割り当てられた許可属性をアップデートします。

再認証を行う期間を設定する場合、**dot1x timer reauth-period** コマンドを使用します。

例

GigabitEthernet 1/0/1 で 802.1X オンラインユーザの再認証機能を有効にし、再認証を行う期間を 1800 秒に設定します。

<Switch> system-view

[Switch] dot1x timer reauth-period 1800

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x re-authenticate

関連コマンド

- **display dot1x**
- **dot1x timer**

2.1.17 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**

2.1.18 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* }

undo dot1x timer { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

デフォルト

- ハンドシェイクタイマ：15 秒
- 停止タイマ：60 秒
- 定期再認証タイマ：3600 秒
- サーバタイムアウトタイマ：100 秒
- クライアントタイムアウトタイマ：30 秒
- ユーザ名要求タイムアウトタイマ：30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

handshake-period *handshake-period-value*: ハンドシェイクタイマを設定します。設定範囲は 5～1024 秒です。

quiet-period *quiet-period-value*: 停止タイマを設定します。設定範囲は 10～120 秒です。

reauth-period *reauth-period-value*: 定期再認証タイマを設定します。設定範囲は 60～7200 秒です。

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 10～120 秒です。

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っても応答がない場合、802.1X 認証は失敗します。

- **クライアントタイムアウトタイマ（supp-timeout）**–アクセス装置がクライアントに EAP-Request/MD5 Challenge パケットを送信するときに開始します。このタイマが時間切れになるまで応答がなかった場合、アクセス装置は、クライアントに要求を再送します。
- **ユーザ名要求タイムアウトタイマ（tx-period）**–装置が EAP-Request/Identity パケットをクライアントに認証要求の応答として送信するときに開始します。タイマが終了する前に装置が応答を受信しない場合、要求を再送します。認証をアクティブに要求できないクライアントを検出するため、EAP-Request/Identity パケットをネットワーク装置に、設定されたタイマの間隔でマルチキャストします。

定期再認証タイマに対する変更は、旧タイマの有効期限が切れた後にのみオンラインになっていたユーザに適用されます。その他のタイマの変更は直ちに装置に反映されます。

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

2.1.19 dot1x timer reauth-period

Syntax

dot1x timer reauth-period *reauth-period-value*

undo dot1x timer reauth-period

デフォルト

802.1X 定期再認証タイマがポートに設定されていません。ポートは、グローバル 802.1X 定期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: 802.1X 定期再認証タイマを秒単位で指定します。設定範囲は 60～7200 です。

説明

dot1x timer reauth-period コマンドは 802.1X 定期再認証タイマをポートに設定します。

undo dot1x timer reauth-period コマンドはデフォルトに戻します。

定期的な再認証でポートが有効になっている場合、装置は指定された定期的な再認証間隔でポートのオンライン 802.1X ユーザを再認証します。ポートで定期的な再認証を有効にするには、**dot1x re-authenticate** コマンドを使用します。

定期再認証タイマへの変更は、旧タイマの有効期限が切れた後にのみオンラインユーザに適用されます。

機器は 802.1X 再認証のために定期的な再認証タイマを以下の順序で選択します。

1) サーバが割り当てた再認証タイマ
2) ポート固有の再認証タイマ
3) グローバル再認証タイマ
4) デフォルトの再認証タイマ

例

GigabitEthernet 1/0/1 で 802.1X 定期再認証タイマを 60 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x timer reauth-period 60

関連コマンド

dot1x timer

2.1.20 dot1x unicast-trigger

Syntax

dot1x unicast-trigger

undo dot1x unicast-trigger

デフォルト

RJ-45 ポート: 有効

他のポート: 無効

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。このプロセスは設定された最大試行回数(**dot1x retry** コマンドで指定されます)で実施します。

例

GigabitEthernet 1/0/1 のユニキャストトリガ機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x unicast-trigger

関連コマンド

- **display dot1x**
- **dot1x multicast-trigger**
- **dot1x retry**
- **dot1x timer**

2.1.21 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*: 802.1X 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 802.1X ゲスト VLAN からすべての 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

2.1.22 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。指定しない場合、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

目次

このセクションのページは **8-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 3-13
3.1.7 mac-authentication guest-vlan auth-period 3-14
3.1.8 mac-authentication max-user 3-15
3.1.9 mac-authentication parallel-with-dot1x 3-16
3.1.10 mac-authentication timer 3-17
3.1.11 mac-authentication timer auth-delay 3-18
3.1.12 mac-authentication user-name-format 3-19
3.1.13 reset mac-authentication guest-vlan 3-21
3.1.14 reset mac-authentication statistics 3-22

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。指定されたポートが MAC アドレス認証で有効になっていない場合、グローバル MAC アドレス認証情報のみを表示します。

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。

パラメータを指定しない場合、グローバル設定、ポート固有の設定、MAC アドレス認証統計情報、およびオンラインのユーザ統計情報を含むすべての MAC アドレス認証情報を表示します。

例

すべての MAC アドレス認証の設定と統計情報を表示します。

<Switch> display mac-authentication

```
Global MAC authentication parameters:
  MAC authentication     : Enabled
  Username format        : MAC address in lowercase(xxxxxxxxxxxx)
         Username       : mac
         Password       : Not configured
  Offline detect period  : 300 s
  Quiet period           : 60 s
  Server timeout         : 100 s
```

```
  Reauth period         : 3600 s
  Authentication domain  : Not configured, use default domain
Online MAC-auth wired users    : 1

Silent MAC users:
       MAC address      VLAN ID  From port             Port index
       0001-0000-0001    100     GE1/0/2              21

GigabitEthernet1/0/1  is link-up
  MAC authentication        : Enabled
  Carry User-IP            : Disabled
  Authentication domain     : Not configured
  Auth-delay timer          : Enabled
  Auth-delay period         : 60 s
  Periodic reauth           : Enabled
     Reauth period         : 120 s
  Re-auth server-unreachable : Logoff
  Guest VLAN               : 100
  Guest VLAN auth-period    : 150 s
  Critical VLAN            : Not configured
  Critical voice VLAN       : Disabled
  Host mode                : Multiple VLAN
  Offline detection         : Enabled
  Authentication order      : Parallel
  Guest VSI                : Not configured
  Guest VSI auth-period     : 30 s
  Critical VSI             : Not configured
  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。

フィールド	説明
Username format	ユーザアカウントタイプです。MACベースあるいは共有があります。 ● MACベースアカウントが使用される場合、ユーザ名のフォーマットで表示されます。たとえば、**MAC address in lowercase(xxxxxxxxxxxx)**はMACアドレスがハイフンなし、16進数表示、小文字であることを示します。 ● 共有アカウントが使用される場合、**Fixed account**と表示されます。
Username	MACアドレス認証のユーザ名です。 ● MACベースアカウントが使用される場合、**mac**と表示されます。装置はMAC認証のユーザ名とパスワードとして各ユーザのMACアドレスを使用します。 ● 共有アカウントが使用される場合、MACアドレス認証ユーザの共有アカウントのユーザ名が表示されます。デフォルトのユーザ名は**mac**です。
Password	MACアドレス認証のパスワードです。 ● MACベースアカウントが使用されている場合、あるいは共有アカウントでパスワードが設定されていない場合、**Not configured**と表示されます。 ● 共有アカウントでパスワードが設定されている場合、とアスタリスク（******）の文字列が表示されます。
Offline detect period	オフライン検出タイマです。
Quiet period	Quietタイマです。
Server timeout	サーバタイムアウトタイマです。
Reauth period	タイマの定期的な再認証を秒単位で実行します。
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アドレス認証を通過したユーザおよびMACアドレス認証を使用しているユーザを含む、有線オンラインMACアドレス認証ユーザの数です。
Silent MAC users	RADIUSサーバからblackholeMACアドレス認証アトリビュートに割り当てられたMACアドレスや、MACアドレスに障害が発生したMACアドレスなど、サイレントMACアドレスに関する情報です。
MAC address	サイレントMACアドレスです。

フィールド	説明
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	ポートでMAC認証が有効になっているかどうかを示します。
Carry User-IP	ユーザIPアドレスがMACアドレス認証要求に含まれるかどうかを示します。
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になっている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	ポートでMAC再認証が定期的に有効になっているかどうかを示します。
Reauth period	ポートでの定期的なタイマ再認証です。
Re-auth server-unreachable	MACアドレス認証の再認証を行う際、到達可能なサーバがない場合に取られるアクションです。 • **Logoff**—オンラインのMACアドレス認証ユーザをログオフします。 • **Online**—MAC認証済みユーザをオンラインのままにします。
Guest VLAN	ポートでゲストVLANが設定されています。 MAC認証ゲストVLANが設定されていない場合、**Not configured**と表示されます。
Guest VLAN auth-period	ポートのMACアドレス認証ゲストVLAN内のユーザの認証間隔です。
Critical VLAN	ポートでcritical VLANが設定されています。 装置はcritical VLANをサポートしていないため、**Not configured**と表示されます。
Critical voice VLAN	ポートでMACアドレス認証Critical Voice VLAN機能が有効になっているかどうかを示します。

フィールド	説明
Host mode	• multi-VLANモードが無効の場合、**Single VLAN**と表示されます。 • multi-VLANモードが有効の場合、**Multiple VLAN**と表示されます。
Offline detection	MACアドレス認証オフライン検出の状態です。 • **Enabled** • **Disabled**
Authentication order	MACアドレス認証と802.1X認証の並列処理が無効になっている場合、このフィールドには**Default**と表示されます。 MACアドレス認証と802.1X認証の並列処理が有効になっている場合、このフィールドには**Parallel**と表示されます。
Guest VSI	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ポートに設定されているMACアドレス認証ゲストVSIです。
Guest VSI auth-period	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ポートのMACアドレス認証ゲストVSI内のユーザの認証間隔です。
Critical VSI	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ポートに設定されているMACアドレス認証Critical VSIです。
Auto-tag feature	このフィールドは、QX-S5300Gシリーズではサポートしていません。 許可VLAN auto-tag featureの状態です。 • **Enabled** • **Disabled**
VLAN tag configuration ignoring	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ignore-configモードの状態です。 • **Enabled** • **Disabled**
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。

フィールド	説明
Auth state	ユーザの状態です。 • **Authenticated**—ユーザがMACアドレス認証に成功しています。 • **Unauthenticated**—ユーザがMACアドレス認証に失敗しています。

3.1.2 display mac-authentication connection

Syntax

display mac-authentication connection [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *user-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートのオンライン MAC アドレス認証ユーザの情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置のオンライン MAC アドレス認証ユーザの情報を表示します。

user-mac *mac-address:* オンライン MAC アドレス認証ユーザの MAC アドレスです。*mac-address* はユーザの MAC アドレスを示します。形式は H-H-H です。オンライン MAC アドレス認証ユーザを指定しない場合、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。オンライン MAC アドレス認証ユーザを指定しない場合、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: macusers
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization ACL ID: 3001
Authorization user profile: N/A
Authorization CAR: N/A
Termination action: Radius-request
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

表 3-2 コマンド出力

フィールド	説明
Total connections	MACアドレス認証のオンラインユーザの総数です。
User MAC address	ユーザのMACアドレスです。
Access interface	ユーザが装置にアクセスするインタフェースです。
User access state	ユーザのアクセス状況です。 • **Successful**—ユーザがMACアドレス認証をパスし、オンラインになります。 • **Open**—ユーザは、存在しないユーザ名または不正なパスワードを使用して、オープン認証モードでオンラインにします。
Authentication domain	ユーザが所属するMACアドレス認証のドメインです。

フィールド	説明
IPv4 address	ユーザのIPv4アドレスです。 使用可能なユーザIPv4アドレスがない場合、このフィールドは表示されません。
IPv6 address	ユーザのIPv6アドレスです。 使用可能なユーザIPv6アドレスがない場合、このフィールドは表示されません。
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なしVLANです。
Authorization tagged VLAN	ユーザに許可されたタグつきVLANです。
Authorization VSI	このフィールドは、QX-S5300Gシリーズではサポートしていません。 ユーザが許可されたVSIです。
Authorization ACL ID	ユーザに許可されたACLです。 ACL許可が失敗した場合、このフィールドは、ACL IDの後に(**Not effective**)と表示します。
Authorization user profile	ユーザに許可されたユーザプロファイルです。
Authorization CAR	サーバによって割り当てられた承認CAR属性です。 ● **Average input rate**—bps単位のインバウンドトラフィックの平均速度です。 ● **Peak input rate**—bps単位のインバウンドトラフィックのピークレートです。 ● **Average output rate**—bps単位のアウトバウンドトラフィックの平均レートです。 ● **Peak output rate**—bps単位のアウトバウンドトラフィックのピークレートです。 サーバがピークレートを割り当てない場合、デフォルトのピークレートは割り当てられた平均レートと同じになります。QX-S5300Gシリーズでは、装置はサーバからのピークレートの排他的割り当てをサポートしていません。 Authorization CAR属性が割り当てられていない場合、このフィールドには **N/A** と表示されます。

フィールド	説明
Termination action	セッションタイムアウトタイマが終了したとき、サーバに割り当てられたアクションの属性です。 • **Default**—セッションタイムアウトタイマが終了したときオンライン認証ユーザをログオフします。この属性は、定期的な再認証が有効で、定期的な再認証のタイマがサーバ割り当てのセッションタイムアウトタイマよりも短い場合には有効になりません。 • **Radius-request**—定期的なMAC再認証機能が有効になっているかどうかに関係なく、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、**N/A**と表示されます。
Session timeout period	サーバによって割り当てられたセッションタイムアウトタイマです。
Online from	MACアドレス認証ユーザがオンラインになった時間です。
Online duration	MACアドレス認証ユーザがオンラインになってからの経過時間です。

3.1.3 mac-authentication

Syntax

mac-authentication

undo mac-authentication

デフォルト

無効

View

System view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-authentication コマンドはグローバルあるいはポートで MAC アドレス認証を有効にします。

undo mac-authentication コマンドはグローバルあるいはポートで MAC アドレス認証を無効にします。

ポートで MAC アドレス認証を使用する場合、グローバルとポートの両方で MAC アドレス認証を有効にする必要があります。

例

グローバルで MAC アドレス認証を有効にします。

<Switch> system-view

[Switch] mac-authentication

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication

関連コマンド

display mac-authentication

🕮 **メモ：**

QX-S5300G シリーズは最大 100PPS まで認証できます。

3.1.4 mac-authentication access-user log enable

Syntax

mac-authentication access-user log enable [**failed-login | ip-change** | **logoff** | **successful-login**] *

undo mac-authentication access-user log enable [**failed-login | ip-change** | **logoff** | **successful-login**] *

デフォルト

有効

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

failed-login: MAC アドレス認証ユーザのログイン失敗に対して生成されるログを指定します。

ip-change: ユーザの IP アドレスの変更に対して生成されるログを指定します。

logoff: MAC アドレス認証ユーザのログオフのために生成されるログを指定します。

successful-login: MAC アドレス認証ユーザの正常なログインのために生成されたログを指定します。

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ギングを有効にします。

undo mac-authentication access-user log enable コマンドは MAC アドレス認証ユーザのロギングを無効にします。

MAC アドレス認証ユーザが過度にログを出力しないようにするには、この機能を無効にすることを推奨します。

パラメータを指定しない場合、MAC アドレス認証ユーザのすべてのログ機能を有効にします。

この機能は、グローバルと該当のインタフェースの両方で有効にした場合のみ、そのインタフェース上で有効になります。

例

GigabitEthernet 1/0/1 ですべてのタイプの MAC 認証ユーザログを無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo mac-authentication access-user log enable

関連コマンド

info-center source maca logfile deny (コマンドマニュアルのセクション 10 *システム管理*)

3.1.5 mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

デフォルト

システムはデフォルト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、コマンドマニュアルのセクション 8 *セキュリティ* “*AAA*”の **domain default enable** コマンドを参照してください。

View

System view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメインの名前を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別しません。

説明

mac-authentication domain コマンドはグローバルあるいは指定ポートで認証ドメインを指定します。

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

グローバルの認証ドメインは MAC アドレス認証が有効なすべてのポートに適用します。レイヤ 2 Ethernet interface view で指定された認証ドメインは、ポートにのみ適用されます。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 ISP 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 ISP 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 が作成されていることを確認します。

説明

mac-authentication guest-vlan コマンドはポートで MAC 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。

MAC アドレス認証ゲスト VLAN は、サーバ到達不能以外の理由で MAC アドレス認証に障害が発生したユーザに対応します。たとえば、指定した VLAN は無効なパスワードが入力されたユーザに対応します。MAC アドレス認証ゲスト VLAN には、限定されたネットワークリソースを展開できます。たとえば、ソフトウェアとシステムパッチをダウンロードするためのソフトウェアサーバなどです。

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 認証ゲスト VLAN として VLAN100 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

装置は 30 秒毎に MAC アドレス認証ゲスト VLAN 内のユーザを認証します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

period-value: MAC アドレス認証ゲスト VLAN 内のユーザの認証間隔を指定します。設定範囲は 1～3600 秒です。

説明

mac-authentication guest-vlan auth-period コマンドは装置が MAC アドレス認証ゲスト VLAN 内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 認証ゲスト VLAN 内のユーザの認証間隔を 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

設定可能な最大数は 4294967295 ですが、実際に使用できる数は 2048 になります。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

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指定します。設定範囲は 1～4294967295 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過剰に使用されないように、ポートで同時に使用できる MAC アドレス認証ユーザの最大数を設定します。最大数に達すると、ポートはそれ以降の MAC アドレス認証ユーザを拒否します。

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 parallel-with-dot1x

Syntax

mac-authentication parallel-with-dot1x

undo mac-authentication parallel-with-dot1x

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-authentication 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 コマンドはデフォルトに戻します。

ポートで設定する場合は、次の制限およびガイドラインに従ってください。

- ポートが次の要件を満たしていることを確認します。
  - ポートは 802.1X 認証と MAC アドレス認証の両方で設定され、802.1X 認証のための MAC ベースのアクセス制御を実行します。
  - ポートは **dot1x unicast-trigger** コマンドが有効になっています。
- ポートで MAC アドレス認証遅延を有効にしないでください。この操作は、802.1X 認証がトリガされた後に MAC アドレス認証を遅延させます。
- ポートに 802.1X 認証と MAC アドレス認証の両方を設定するには、次のいずれかの方法を使用します。
  - ポートで 802.1X 機能と MAC アドレス認証機能を別々に有効にします。
  - ポートのポートセキュリティを有効にします。ポートセキュリティモードは、**userlogin-secure-or-mac** または **userlogin-secure-or-mac-ext** である必要があります。

ポートセキュリティモード設定の詳細は、オペレーションマニュアルのセクション 8 *セキュリティ “ポートセキュリティ”*を参照してください。

例

GigabitEthernet 1/0/1 で MAC 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

3.1.10 mac-authentication timer

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **reauth-period** | **server-timeout** }

デフォルト

以下の MAC アドレス認証タイマが適用されます。

- オフライン検出タイマは 300 秒です。
- quiet タイマは 60 秒です。
- グローバルな periodic タイマ再認証 MAC は 3600 秒です。
- サーバタイムアウトタイマは 100 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

offline-detect *offline-detect-value*: オフライン検出タイマを秒単位で指定します。設定範囲は 60~2147483647 です。

quiet *quiet-value*: quiet タイマを指定します。設定範囲は 1～3600 秒です。

reauth-period *reauth-period-value*: グローバルな定期タイマ再認証 MAC を指定します。設定範囲は 60~7200 秒です。

server-timeout *server-timeout-value*: サーバのタイムアウトタイマを指定します。設定範囲は 100～300 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 アドレス認証オフライン検出機能が有効になっている場合にのみ有効です。

- **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。
- **Periodic MAC reauthentication time**r–ポートで定期的な MAC アドレス再認証が有効になっている場合に、ポートで装置がオンライン MAC ユーザを再認証する間隔を設定します。グローバル定期再認証タイマへの変更は、旧タイマの有効期限が切れた後にのみオンラインユーザに適用されます。
- **Server timeout timer**–RADIUS サーバが使用不能であることを検出する前に、装置が RADIUS サーバからの応答を待つ時間をタイマに設定します。MAC アドレス認証中にタイムアウトした場合、ユーザはネットワークにアクセスすることはできません。

例

サーバタイムアウトのタイマを 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

3.1.11 mac-authentication timer auth-delay

Syntax

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

undo mac-authentication timer auth-delay

デフォルト

ポートに MAC 認証遅延タイマが設定されていません。MAC 認証の遅延は無効になっています。MAC 認証は、ユーザパケットによってトリガされた直後に開始されます。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auth-delay *auth-delay-time*: MAC 認証の遅延時間を秒単位で指定します。設定範囲は 1 ～180 です。

説明

mac-authentication timer auth-delay コマンドはポートに MAC 認証タイマを設定します。

undo mac-authentication timer auth-delay コマンドは MAC 認証タイマをデフォルトに戻します。

ポートで 802.1X 認証と MAC 認証の両方が有効になっている場合は、MAC 認証を遅らせて、802.1X 認証が優先的にトリガされるようにすることができます。802.1X 認証がトリガされない場合、または遅延期間内に 802.1X 認証が失敗した場合、ポートは引き続き MAC 認証を処理します。

MAC 認証遅延を使用する場合は、ポートセキュリティモードを **mac-else-userlogin-secure** または **mac-else-userlogin-secure-ext** に設定しないでください。遅延は、2 つのモードのいずれのポートでも有効になりません。ポートセキュリティモードの詳細については、コマンドマニュアルのセクション 8 *セキュリティ“ポートセキュリティ”*を参照してください。

例

GigabitEthernet 1/0/1 で MAC 認証遅延を有効にし、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 user-name-format

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] }

undo mac-authentication user-name-format

デフォルト

MAC アドレス認証のユーザ名とパスワードの両方として各ユーザの 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。ユーザ名を指定しない場合、デフォルトのユーザ名 **mac** が適用されます。

password: 共有ユーザアカウントのパスワードを指定します。

cipher: 暗号化形式でパスワードを指定します。

simple: プレーンテキスト形式でパスワードを設定します。セキュリティ保護のため、プレーンテキストで指定されたパスワードは暗号化されて保存されます。

string: パスワードを指定します。プレーンテキスト形式の設定範囲は 1～63 文字です。大文字、小文字を区別します。暗号化形式の設定範囲は 1～117 文字です。大文字と小文字を区別します。

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した場合、装置は 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。このユーザアカウントタイプは、高い認証セキュリティが保証されます。ただし、ユーザの MAC アドレスをユーザ名とパスワードの両方として使用して、認証サーバ上に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指定した場合、装置はすべてのユーザの MAC アドレス認証に対して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 アドレス認証ユーザが認証に 1 つのアカウントを使用するため、認証サーバに作成する必要があるのは 1 つのアカウントだけです。このユーザアカウントの種類は、信頼されたネットワークに適しています。

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 認証ユーザには MAC ベースのユーザアカウントを使用します。各 MAC アドレスは、ハイフンを含む 16 進表記で、文字は大文字です。

<Switch> system-view

[Switch] mac-authentication user-name-format mac-address with-hyphen uppercase

関連コマンド

display mac-authentication

3.1.13 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。

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**

3.1.14 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 **8-x-x** です。

4 章 Web 認証.....4-1
4.1 Web 認証設定コマンド.....4-1
4.1.1 display web-auth.....4-1
4.1.2 display web-auth free-ip.....4-2
4.1.3 display web-auth server.....4-3
4.1.4 display web-auth user.....4-4
4.1.5 ip.....4-5
4.1.6 url.....4-7
4.1.7 web-auth auth-fail vlan.....4-8
4.1.8 web-auth domain.....4-9
4.1.9 web-auth enable.....4-10
4.1.10 web-auth free-ip.....4-11
4.1.11 web-auth max-user.....4-12
4.1.12 web-auth offline-detect.....4-13
4.1.13 web-auth proxy port.....4-13
4.1.14 web-auth server.....4-15

4章 Web 認証

4.1 Web認証設定コマンド

4.1.1 display web-auth

Syntax

display web-auth [*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 Web 認証の設定を表示します。

説明

display web-auth コマンドはインタフェースの Web 認証設定と実行ステータスを表示します。

例

GigabitEthernet 1/0/1 の Web 認証の設定を表示します。

<Switch> display web-auth interface gigabitethernet 1/0/1

```
Global Web-auth parameters  :
 Proxy Port Numbers        : Not configured
 Total online web-auth users: 1
GigabitEthernet1/0/1  is link-up
  Port role               : Authenticator
  Web-auth domain          : my-domain
  Auth-Fail VLAN           : Not configured
  Offline-detect           : Not configured
  Max online users         : 1024
  Web-auth enable          : Enabled

 Total online web-auth users: 1
```

表 4-1 コマンド出力

フィールド	説明
Global Web-auth parameters	グローバルWeb認証設定です。
Proxy Port Numbers	Webプロキシサーバのポート番号です。
Total online web-auth users	装置のオンラインWeb認証ユーザの総数です。
GigabitEthernet1/0/1 is link-up	インタフェースの状態： ● **link-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。 ● **link-down**：インタフェースがdownしています。
Port role	ポートの役割です。ポートは**Authenticator**としてのみ機能します。
Web-auth domain	Web認証で使用されるISPドメインです。
Auth-fail VLAN	Web認証用のVLAN制限です。Auth-Fail VLANが設定されていない場合、**Not configured**と表示されます。
Offline-detect	Web認証ユーザの検出間隔です。Web認証ユーザのオンライン検出が無効になっている場合、**Not configured**と表示されます。
Max online users	インタフェースで許可されるWeb認証ユーザの最大数です。
Web-auth enable	Web認証の状態： ● 有効 ● 無効
Total online web-auth users	インタフェース上のオンラインWeb認証ユーザの総数です。

4.1.2 display web-auth free-ip

Syntax

display web-auth free-ip

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display web-auth free-ip コマンドは Web 認証のないサブネットを表示します。

例

Web 認証のないサブネットを表示します。

<Switch> display web-auth free-ip

```
Free IP
                : 1.1.0.0       255.255.0.0
                : 1.2.0.0       255.255.0.0
```

関連コマンド

web-auth free-ip

4.1.3 display web-auth server

Syntax

display web-auth server [*server-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

server-name: Web 認証サーバ名を指定します。大文字と小文字が区別されます。設定範囲は 1~32 文字です。Web 認証サーバを指定しない場合は、すべての Web 認証サーバの情報を表示します。

説明

display web-auth server コマンドは Web 認証サーバの情報を表示します。

例

Web 認証サーバ **aaa** の情報を表示します。

<Switch> display web-auth server aaa

```
Web-auth server: aaa
  IP                    : 8.8.8.8
  Port                  : 80
  URL                   : http://8.8.8.8/portal/
```

```
Redirect-wait-time    : 5
URL parameters        : Not configured
```

表 4-2 コマンド出力

フィールド	説明
Web-auth server	Web認証サーバの名前です。
IP	Web認証サーバのIPアドレスです。
Port	Web認証サーバのポート番号です。
URL	Web認証サーバのリダイレクトURLです。
Redirect-wait-time	認証されたユーザをユーザによって要求されたWebページにリダイレクトするまでの時間です。
URL parameters	リダイレクトURLのパラメータです。

4.1.4 display web-auth user

Syntax

display web-auth user [**interface** *interface-type interface-number* | **slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: タイプと番号によって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インタフェースのオンライン Web 認証ユーザに関する情報を表示します。

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、このコマンドはすべてのメンバ装置のオンライン Web 認証ユーザ情報を表示します。

説明

display web-auth user コマンドはインタフェースのオンライン Web 認証ユーザに関する情報を表示します。

例

GigabitEthernet 1/0/1 のオンライン Web 認証ユーザに関する情報を表示します。

<Switch> display web-auth user interface gigabitethernet 1/0/1

```
  Total online web-auth users: 1

User name: user1
  MAC address: 0000-2700-b076
  Access interface: GigabitEthernet 1/0/1
  Initial VLAN: 1
  Authorization VLAN: N/A
  Authorization ACL ID: N/A
  Authorization user profile: N/A
```

表 4-3 コマンド出力

フィールド	説明
Total online web-auth users	オンラインWeb認証ユーザの総数です。
User Name	オンラインWeb認証ユーザの名前です。
MAC address	オンラインWeb認証ユーザのMACアドレスです。
Access interface	オンラインWeb認証ユーザのアクセスインターフェイスです。
Initial VLAN	ユーザがWeb認証を通過する前のユーザの初期VLANです。
Authorization VLAN	オンラインWeb認証ユーザの認証VLAN IDです。
Authorization ACL ID	オンラインWeb認証ユーザの認証ACL番号です。
Authorization user profile	オンラインWeb認証ユーザのユーザプロファイルの状態： • **N/A**–ユーザプロファイルは許可されません。 • **Active**–許可されたユーザプロファイルが、ユーザアクセスインタフェースに正常に適用されます。 • **Inactive**–許可されたユーザプロファイルがユーザアクセスインタフェースに適用されていないか、ユーザプロファイルが装置上に存在しません。

4.1.5 ip

Syntax

ip *ipv4-address* **port** *port-number*

undo ip

デフォルト

Web 認証サーバの IP アドレスまたはポート番号が指定されていません。

View

Web 認証サーバ view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: Web 認証サーバの IPv4 アドレスを指定します。この IP アドレスは、アクセス装置のレイヤ 3 インタフェースの IP アドレスであり、Web 認証ユーザとの間でルーティング可能である必要があります。

port *port-number*: Web 認証サーバのポート番号を指定します。設定範囲は 1~65535 です。

説明

ip コマンドは Web 認証サーバの IP アドレスとポート番号を設定します。

undo ip コマンドはデフォルトに戻します。

Web 認証サーバの IP アドレスとして、ループバックインタフェースの IP アドレスを使用することを推奨します。ループバックインタフェースには次の利点があります。

- ループバックインタフェースのステータスは安定しています。これにより、インタフェース障害による認証ページへのアクセス障害を回避できます。
- ループバックインタフェースは受信パケットを転送しません。これにより、ネットワークアクセス要求が多い場合に、システムパフォーマンスへの影響を回避できます。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

Web 認証サーバ **wbs** の view を設定します。

<Switch> system-view

[Switch] web-auth server wbs

Web 認証サーバ **wbs** の IP アドレスとして 192.168.1.1 を指定し、ポート番号として 8080 を設定します。

[Switch-web-auth-server-wbs] ip 192.168.1.1 port 8080

関連コマンド

url

4.1.6 url

Syntax

url *url-string*

undo url

デフォルト

設定なし

View

Web 認証サーバ view

定義済みユーザロール

network-admin

パラメータ

url-string: Web 認証サーバのリダイレクション URL を指定します。設定範囲は 1〜256 文字です。大文字と小文字を区別します。

説明

url コマンドは Web 認証サーバのリダイレクト URL を指定します。

undo url コマンドはデフォルトに戻します。

リダイレクション URL は、標準の HTTP または HTTPS を介してアクセスできる URL です。リダイレクト URL は http ://または https ://.で始まる必要があります。リダイレクト URL が http ://または https://、で始まっていない場合、システムは URL が http ://.で始まると判断します。

URL の IP アドレスとポート番号は、Web 認証サーバの IP アドレスおよびポート番号と同じである必要があります。

例

Web 認証サーバ **wbs** のリダイレクト URL として http://192.168.1.1:80/portal/を指定します。

<Switch> system-view

[Switch] web-auth server wbs

[Switch-web-auth-server-wbs] url http://192.168.1.1:80/portal/

関連コマンド

ip

4.1.7 web-auth auth-fail vlan

Syntax

web-auth auth-fail vlan *authfail-vlan-id*

undo web-auth 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: Auth-Fail VLAN ID を指定します。設定範囲は 1～4094 です。指定した VLAN はすでに存在している必要があります。

説明

web-auth auth-fail vlan コマンドは Web 認証の Auth-FailVLAN を指定します。

undo web-auth auth-fail vlan コマンドはデフォルトに戻します。

インタフェースでこのコマンドを設定すると、インタフェースで Web 認証に失敗したユーザは、Auth-FailVLAN のリソースにアクセスできるようになります。リソースを提供するサーバの IP アドレスも、認証なしの IP アドレスとして設定する必要があります。

Auth-Fail VLAN を有効にするには、インタフェースで MAC ベース VLAN を有効にし、Auth-FailVLAN のサブネットを Web 認証なしのサブネットとして設定する必要があります。

MAC ベースの VLAN はハイブリッドポートでのみ有効になるため、Auth-FailVLAN もハイブリッドポートでのみ有効になります。

ユーザが Web 認証に失敗した場合、装置はユーザの MAC アドレスを Auth-FailVLAN にマッピングします。

Auth-Fail VLAN として設定されている VLAN は削除できません。この VLAN を削除するには、まず **undo web-auth auth-fail vlan** コマンドを使用して Auth-Fail VLAN 設定をキャンセルします。

VLAN がスーパーVLAN として指定されている場合は、この VLAN をインタフェースの Auth-Fail VLAN として設定しないでください。VLAN がインタフェースの Auth-Fail VLAN として指定されている場合、この VLAN をスーパーVLAN として設定しないでください。

例

GigabitEthernet 1/0/1 で VLAN 5 を Web 認証 Auth-Fail VLAN として指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch–GigabitEthernet1/0/1] port link-type hybrid

[Switch–GigabitEthernet1/0/1] mac-vlan enable

[Switch–GigabitEthernet1/0/1] web-auth auth-fail vlan 5

関連コマンド

display web-auth

4.1.8 web-auth domain

Syntax

web-auth domain *domain-name*

undo web-auth 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: ISP 認証ドメイン名を指定します。設定範囲は 1~255 文字です。大文字と小文字は区別されません。

説明

web-auth domain コマンドはインタフェースの Web 認証ユーザの認証ドメインを指定します。

undo web-auth domain コマンドはデフォルトに戻します。

このコマンドを設定すると、装置はインタフェースの Web 認証ユーザの認証、許可、およびアカウンティング（AAA）に認証ドメインを使用します。

例

GigabitEthernet 1/0/1 で Web 認証ユーザの認証ドメインとして domain **my-domain** を指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch–GigabitEthernet1/0/1] web-auth domain my-domain

4.1.9 web-auth enable

Syntax

web-auth enable apply server *server-name*

undo web-auth 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

パラメータ

server-name: Web 認証サーバ名を指定します。設定範囲は 1~32 文字です。大文字と小文字が区別されます。

説明

web-auth enable コマンドは Web 認証を有効にします。

undo web-auth enable コマンドは Web 認証を無効にします。

このコマンドを使用して、インタフェースで Web 認証を有効にし、Web 認証サーバを指定します。

Web 認証が正しく機能するためには、ポートセキュリティを有効にしたり、Web 認証が有効になっているレイヤ 2Ethernet インタフェースでポートセキュリティモードを設定したりしないでください。

例

Web 認証を有効にし、GigabitEthernet 1/0/1 で Web 認証サーバ **wbs** を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] web-auth enable apply server wbs

関連コマンド

web-auth server

4.1.10 web-auth free-ip

Syntax

web-auth free-ip *ip-address* { *mask-length* | *mask* }

undo web-auth free-ip { *ip-address* { *mask-length* | *mask* } | **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

ip-address: Web 認証のないサブネットアドレスを指定します。

mask-length: Web 認証のないサブネットアドレスのマスク長を指定します。設定範囲は 1~32 です。

mask: Web 認証のないサブネットの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。

all: すべての Web 認証なしサブネットを指定します。

説明

web-auth free-ip コマンドは Web 認証のないサブネットを指定します。

undo web-auth free-ip コマンドはデフォルトに戻します。

Web 認証ユーザは、認証されていなくても、Web 認証のないサブネット内のリソースにアクセスできます。

このコマンドを繰り返して、複数の Web 認証なしのサブネットを設定できます。

例

サブネット 192.168.0.0/24 を Web 認証なしのサブネットとして設定します。

<Switch> system-view

[Switch] web-auth free-ip 192.168.0.0 24

4.1.11 web-auth max-user

Syntax

web-auth max-user *max-number*

undo web-auth max number

デフォルト

1024

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: インタフェースで許可される Web 認証ユーザの最大数を指定します。設定範囲は 1~2048 です。

説明

web-auth max-user コマンドはインタフェースで許可される Web 認証ユーザの最大数を設定します。

undo web-auth max-user コマンドはデフォルトに戻します。

指定された最大数がインタフェースの現在のオンラインWeb認証ユーザの数よりも少ない場合、制限を正常に設定できます。この制限は、オンラインWeb認証ユーザには影響しません。ただし、新しいWeb認証ユーザがインタフェースからログインするには、装置のその数が制限を下回る必要があります。

このコマンドは、IPv4Web 認証ユーザのみの最大数を指定します。

例

GigabitEthernet 1/0/1 で、Web 認証ユーザの最大数を 32 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] web-auth max-user 32

関連コマンド

display web-auth

4.1.12 web-auth offline-detect

Syntax

web-auth offline-detect interval *interval*

undo web-auth offline-detect interval

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: Web 認証ユーザの検出間隔を指定します。設定範囲は 60~65535 秒です。

説明

web-auth offline-detect コマンドは Web 認証ユーザのオンライン検出を有効にします。

undo web-auth max-user コマンドは Web 認証ユーザのオンライン検出を無効にします。

この機能により、装置は指定された検出間隔でオンラインユーザのパケットを検出できます。インターバル内にユーザからのパケットが受信されない場合、装置はユーザをログアウトし、RADIUS サーバにユーザのアカウンティングを停止するよう通知します。

装置が誤ってユーザをログアウトするのを防ぐためには、検出間隔を MAC アドレスエントリのエージングタイムと同じに設定します。

例

GigabitEthernet 1/0/1 で、Web 認証ユーザのオンライン検出を有効にし、検出間隔を 3600 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] web-auth offline-detect interval 3600

4.1.13 web-auth proxy port

Syntax

web-auth proxy port *port number*

undo web-auth proxy port { *port-number* | **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

port number: Web プロキシサーバの TCP ポート番号を指定します。設定範囲は 1~65535 です。

all: すべての Web プロキシサーバの TCP ポート番号を指定します。

説明

web-auth proxy port コマンドは Web プロキシサーバのポート番号を追加し、Web プロキシサーバによって転送される HTTP 要求によって Web 認証が実行されるようにします。

undo web-auth proxy port コマンドは 1 つまたはすべての Web プロキシサーバのポート番号を削除します。

デフォルトでは、プロキシされた HTTP 要求は Web 認証を実行できませんが、サイレントにドロップされます。このような HTTP 要求が Web 認証を実行できるようにするには、装置の Web プロキシサーバのポート番号を指定します。

このコマンドを繰り返すと、複数の Web プロキシサーバのポート番号を追加できます。

ユーザのブラウザが Web Proxy Auto-Discovery (WPAD) プロトコルを使用して Web プロキシサーバを検出している場合、以下のタスクを実行する必要があります。

- 装置の Web プロキシサーバのポート番号を追加します。
- 認証なしのルールに設定して、WPAD サーバの IP アドレス宛てのユーザパケットが認証なしで通過できるようにします。
- Web プロキシをサポートする Web 認証の場合：
- 装置の Web プロキシサーバのポート番号を追加する必要があります。
- ユーザは、Web プロキシサーバを使用するブラウザが、ローカルポータル Web サービスのリスニング IP アドレスにプロキシサーバを使用しないようにする必要があります。その場合、Web 認証ユーザがローカルポータル Web サービスに送信する HTTP パケットは、Web プロキシサーバに送信されません。

例

Web 認証用の Web プロキシサーバの TCP ポート番号 7777 を追加します。

<Switch> system-view

[Switch] web-auth proxy port 7777

4.1.14 web-auth server

Syntax

web-auth server *server-name*

undo web-auth server *server-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

server-name: Web 認証サーバ名を指定します。設定範囲は 1~32 文字です。大文字と小文字が区別されます。

説明

web-auth server コマンドは Web 認証サーバを作成し、その view を入力するか、既存の Web 認証サーバの view を入力します。

undo web-auth server コマンドは Web 認証サーバを削除します。

Web 認証サーバ view では、Web 認証サーバの次のパラメータと機能を設定できます。

- サーバの IP アドレス
- リダイレクト URL
- リダイレクト URL で伝送されるパラメータ

例

wbs という名前の Web 認証サーバを作成し、その view を設定します。

<Switch> system-view

[Switch] web-auth server wbs

[Switch-web-auth-server-wbs]

関連コマンド

web-auth enable apply server

目次

このセクションのページは **8-x-x** です。

5 章 ポートセキュリティ 5-1
5.1 ポートセキュリティ設定コマンド 5-1
5.1.1 display port-security 5-1
5.1.2 display port-security mac-address block 5-5
5.1.3 display port-security mac-address security 5-6
5.1.4 port-security access-user log enable 5-8
5.1.5 port-security authorization ignore 5-9
5.1.6 port-security enable 5-10
5.1.7 port-security intrusion-mode 5-11
5.1.8 port-security mac-address security 5-12
5.1.9 port-security mac-move permit 5-14
5.1.10 port-security max-mac-count 5-15
5.1.11 port-security ntk-mode 5-16
5.1.12 port-security oui 5-17
5.1.13 port-security port-mode 5-18
5.1.14 port-security timer autolearn aging 5-23
5.1.15 port-security timer disableport 5-24
5.1.16 snmp-agent trap enable port-security 5-25

5章 ポートセキュリティ

5.1 ポートセキュリティ設定コマンド

5.1.1 display port-security

Syntax

display port-security [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートセキュリティの情報を表示します。

説明

display port-security コマンドはポートのポートセキュリティの設定、稼働状況、統計情報を表示します。

例

すべてのポートのポートセキュリティの情報を表示します。

<Switch> display port-security

```
Global port security parameters:
   Port security         : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 20 s
   MAC move              : Denied
   Authorization fail     : Online
   NAS-ID profile        : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap      : Disabled
   Dot1x-logoff trap      : Enabled
   Intrusion trap        : Disabled
   Address-learned trap   : Enabled
   Mac-auth-failure trap  : Disabled
```

```
  Mac-auth-logon trap    : Enabled
  Mac-auth-logoff trap   : Disabled
  Open authentication    : Disabled
  OUI value list         :
   Index :  1          Value : 123401

GigabitEthernet1/0/1 is link-up
  Port mode                    : userLogin
  NeedToKnow mode              : Disabled
  Intrusion protection mode     : NoAction
  Security MAC address attribute
     Learning mode             : Sticky
     Aging type                : Periodical
  Max secure MAC addresses      : 32
  Current secure MAC addresses   : 0
  Authorization                : Permitted
  NAS-ID profile               : Not configured
  Free VLANs                   : Not configured
  Open authentication           : Disabled
```

表 5-1 コマンド出力

フィールド	説明
Port security	ポートセキュリティ機能が有効かどうかを示します。
AutoLearn aging time	Sticky MACアドレスエージングタイマです。単位は分または秒です。
Disableport timeout	不正なパケットを受信するポートの無効状態を解除するタイムアウト時間です。単位は秒です。
MAC move	MAC移動機能の状態です。 ● MAC移動機能が有効である場合、**Permitted**と表示されます。 ● MAC移動機能が無効である場合、**Denied**と表示されます。
Authorization fail	ACLに失敗あるいはユーザプロファイルの許可に失敗したユーザのアクションです。 ● **Online**–ユーザがオンライン接続することを許可します。 ● **Offline**–ユーザをログオフします。
NAS-ID profile	グローバルに適用されたNAS IDのプロファイルです。
Dot1x-failure trap	SNMP通知が802.1X 認証の失敗が有効になります。
Dot1x-logon trap	SNMP通知が802.1X 認証成功が有効になります。

フィールド	説明
Dot1x-logoff trap	SNMP通知が802.1X 認証済みユーザログオフが有効になります。
Intrusion trap	侵入防止のSNMP通知を有効にするかどうかを示します。有効になっている場合、装置は不正なパケットが検出された後にSNMP通知を送信します。
Address-learned trap	MACアドレス学習のSNMP通知を有効にするかどうかを示します。有効になっている場合、装置は新しいMACアドレスを学習した後にSNMP通知を送信します。
Mac-auth-failure trap	MACアドレス認証障害のSNMP通知を有効にするかどうかを示します。
Mac-auth-logon trap	MACアドレス認証成功のSNMP通知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ログオフのSNMP通知を有効にするかどうかを示します。
Open authentication	グローバルオープン認証モードが使用可能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** ポートセキュリティモードの詳細は、オペレーションマニュアルのセクション8 *セキュリティ* を参照してください。

フィールド	説明
NeedToKnow mode	NTK（Need to know）モードです。 • **NeedToKnowOnly**–認証された宛先MACアドレスのユニキャストパケットのみ許可します。 • **NeedToKnowWithBroadcast**–認証された宛先MACアドレスのユニキャストパケット、ブロードキャストパケットのみ許可します。 • **NeedToKnowWithMulticast**–認証された宛先MACアドレスのユニキャストパケット、マルチキャストパケット、ブロードキャストパケットのみ許可します。 • **Disabled**–NTKが無効です。
Intrusion protection mode	侵入防止アクションです。 • **BlockMacAddress**–不正なパケットの送信元MACアドレスをブロックMACアドレスリストに追加します。 • **DisablePort**–不正なパケットを受信したポートを手動でアップするまでシャットダウンします。 • **DisablePortTemporarily**–不正なパケットを受信したポートを指定した期間、シャットダウンします。 • **NoAction**–侵入防止アクションを実行しません。
Learning mode	セキュアMACアドレス学習モードです。 • **Dynamic** • **Sticky**
Aging type	セキュアMACアドレスエージングのタイプです。 • **Periodical**–エージングタイマのみです。 • **Inactivity**–インアクティビティエージング機能とエージングタイマです。QX-S5300Gシリーズは、インアクティビティエージングをサポートしていません。
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。
Free VLANs	VLAN パケットは認証をトリガしません。 free VLANを設定しない場合、このフィールドには**Not configured**と表示されます。

フィールド	説明
Open authentication	ポートでオープン認証モードが有効になっているかどうかを示します。

5.1.2 display port-security mac-address block

Syntax

display port-security mac-address block [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

count: ブロックされた MAC アドレスの数のみを表示します。

説明

display port-security mac-address block コマンドはブロックされた MAC アドレスの情報を表示します。

パラメータを指定しない場合、ブロックされたすべての MAC アドレスの情報を表示します。

例

#ブロックされたすべての MAC アドレスの情報を表示します。

<Switch> display port-security mac-address block

```
MAC ADDR           Port                    VLAN ID
 000f-3d80-0d2d     GE1/0/1                 30

 --- On slot 1, 1 MAC address(es) found ---

 --- 1 mac address(es) found ---
```

ブロックされたすべての MAC アドレスの数を表示します。

<Switch> display port-security mac-address block count

```
--- On slot 1, 1 MAC address(es) found ---

--- 1 mac address(es) found ---
```

表 5-2 コマンド出力

フィールド	説明
MAC ADDR	ブロックされたMACアドレスです。
Port	ブロックされたMACアドレスが送信元アドレスのフレームを受信したポートです。
VLAN ID	ポートが所属するVLANのIDです。
number mac address(es) found	ブロックされたMACアドレスの数です。

関連コマンド

port-security intrusion-mode

5.1.3 display port-security mac-address security

Syntax

display port-security mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

count: セキュア MAC アドレスの数のみを表示します。

説明

display port-security mac-address security コマンドはセキュア MAC アドレスの情報を表示します。

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。

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。

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        Security      GE1/0/1                    Not aged

 --- Number of secure MAC addresses: 1 ---
```

セキュア MAC アドレスの数のみを表示します。

<Switch> display port-security mac-address security count

```
--- Number of secure MAC addresses: 1 ---
```

表 5-3 コマンド出力

フィールド	説明
MAC ADDR	セキュアMACアドレスです。
VLAN ID	ポートが所属するVLANのIDです。
STATE	MACアドレスのタイプです。セキュアMACアドレスは**Security**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。
AGING TIME	セキュアMACアドレスがエージアウトするまでの時間です。 • セキュアMACアドレスがスタティックアドレスである場合、**Not aged**と表示されます。 • セキュアMACアドレスがsticky MACアドレスである場合、エージアウトするまでの時間を表示します。エージアウトするまでの時間が60秒未満の場合、ライフタイムは秒単位でカウントされます。エージアウトするまでの時間が60秒以上の場合、ライフタイムは分単位でカウントされます。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	保存されているセキュアMACアドレスの数です。

関連コマンド

port-security mac-address security

5.1.4 port-security access-user log enable

Syntax

port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation**] *

undo port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation**] *

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

failed-authorization: 802.1X または MAC アドレス認証ユーザの認証失敗に対して生成されるログを指定します。

mac-learning: 新しい MAC アドレス学習用に生成されるログを指定します。

violation: 侵入保護が実行されたときに生成されるログを指定します。

説明

port-security access-user log enable コマンドはポートセキュリティユーザのロギングを有効にします。

undo port-security access-user log enable コマンドはポートセキュリティユーザのロギングを無効にします。

ポートセキュリティユーザのログが過剰に出力されないようにするには、この機能を無効にすることをお勧めします。

パラメータを指定しない場合、このコマンドはポートセキュリティユーザのすべてのログ機能を有効にします。

例

侵入防止のログを有効にします。

<Switch> system-view

[Switch] port-security access-user log enable violation

関連コマンド

info-center source portsec logfile deny (コマンドマニュアルのセクション 10 *システム管理*)

5.1.5 port-security authorization ignore

Syntax

port-security authorization ignore

undo port-security authorization ignore

デフォルト

ポートはサーバから受信した許可情報を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

port-security authorization ignore コマンドは認証サーバ（RADIUS サーバあるいはローカル装置）から受信した許可情報を無視するようポートを設定します。

undo port-security authorization ignore コマンドはデフォルトに戻します。

ユーザが RADIUS あるいはローカル認証を通過後、サーバはユーザのアカウント用に設定された許可属性にもとづいて許可を実行します。たとえば、VLAN が付与されることもあります。ポートがユーザの許可属性を使用しない場合、サーバから許可情報を無視します。

例

認証サーバから受信した許可情報を無視するように GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security authorization ignore

関連コマンド

display port-security

5.1.6 port-security enable

Syntax

port-security enable

undo port-security enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

port-security enable コマンドはポートセキュリティを有効にします。

undo port-security enable コマンドはポートセキュリティを無効にします。

ポートでポートセキュリティを有効にする前にグローバルで 802.1X 認証と MAC アドレス認証を無効にする必要があります。

ポートセキュリティを有効あるいは無効にすると、以下のセキュリティの設定がデフォルトに戻ります。

- 802.1X アクセス制御モードが MAC ベースになります。
- 802.1X ポート許可状態が auto になります。

ポートにオンラインユーザが存在する場合、ポートセキュリティを無効にするとオンラインユーザもログオフします。

例

ポートセキュリティを有効にします。

<Switch> system-view

[Switch] port-security enable

関連コマンド

- **display port-security**
- **dot1x**
- **dot1x port-control**
- **dot1x port-method**
- **mac-authentication**

5.1.7 port-security 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、正常状態に戻ります。ブロックする時間は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後、不正なフレームの送信元 MAC アドレスをブロックするように GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security intrusion-mode blockmac

関連コマンド

- **display port-security**
- **display port-security mac-address block**
- **port-security timer disableport**

5.1.8 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

Layer 2 Ethernet interface view

system view

定義済みユーザロール

network-admin

パラメータ

sticky: sticky MAC アドレスを指定します。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。

mac-address: MAC アドレスを H-H-H 形式で指定します。

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。

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** モードで設定または学習された MAC アドレスです。一度保存されると、装置のリブートが行われても変更されません。VLAN に 1 ポートのみに MAC アドレスを割り当てることができます。

ポートが **autoLearn** モードのとき、認証失敗によってセキュア送信元 MAC アドレスが制限となることを防ぐため、sticky またはスタティックセキュア MAC アドレスとして、重要な MAC アドレスやよく使われる MAC アドレスを追加することができます。ポートにセキュア MAC アドレスを追加するため、最初に以下の作業を完了してください。

- ポートでポートセキュリティを有効にします。
- ポートのセキュリティモードを **autoLearn** に設定します。
- ポートで指定した VLAN のパケットが通過できるように許可する、あるいは VLAN にポートを追加するように設定を行ってください。VLAN が既に存在することを確認してください。

sticky MAC アドレスは **autoLearn** モードで設定または学習されます。sticky MAC アドレスはデフォルトではエージアウトしません。**port-security timer autolearn aging** コマンドで sticky MAC アドレスのエージアウト時間を設定できます。タイマがエージアウトしたとき、sticky MAC アドレスは削除されます。

スタティックセキュア MAC アドレスは、以下の作業を行わない限り、エージアウトしません。

- **undo port-security mac-address security** コマンドで MAC アドレスを削除します。
- ポートセキュリティモードを変更します。
- ポートセキュリティ機能を無効にします。

追加されたセキュア MAC アドレスのタイプを変更することはできません。あるいは追加されたエントリタイプを除いた同一の 2 つのエントリを追加することができません。

たとえば、**port-security mac-address security** 1-1-1 **vlan** 10 コマンドが設定されているとき、**port-security mac-address security sticky** 1-1-1 **vlan** 10 を設定することはできません。新しく設定する場合、古い設定を削除する必要があります。

例

ポートセキュリティを有効にし、GigabitEthernet 1/0/1 のポートセキュリティモードを **autoLearn** に設定します。ポートで許可されるセキュア MAC アドレスの最大数を 100 に設定します。

<Switch> system-view

[Switch] port-security enable

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security max-mac-count 100

[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn

sticky MAC アドレスとして VLAN 4 の MAC アドレス 0001-0002-0003 を指定します。

[Switch-GigabitEthernet1/0/1] port-security mac-address security sticky 0001-0002-0003 vlan 4

[Switch-GigabitEthernet1/0/1] quit

system view で GigabitEthernet 1/0/1 に VLAN 10 に属するセキュア MAC アドレス 0001-0001-0002 を追加します。

[Switch] port-security mac-address security 0001-0001-0002 interface gigabitethernet 1/0/1 vlan 10

関連コマンド

- **display port-security**
- **port-security timer autolearn aging**

5.1.9 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 コマンドは装置で MAC アドレス移動機能を無効にします。

このコマンドは、802.1X 認証ユーザと MAC 認証ユーザの両方で有効になります。

MAC 移動により、802.1X または MAC 認証済みユーザが装置のポート間を移動できます。たとえば、802.1X 認証されたユーザが装置の別の 802.1X 対応ポートに移動すると、認証セッションは最初のポートから削除されます。ユーザは新しいポートで再認証されます。

MAC 移動が無効になっている場合、あるポートで認証された 802.1X または MAC ユーザは、別のポートに移動した後、認証にパスできません。

認証サーバ（ローカルまたはリモート）のオンラインユーザの数が上限に達した場合、802.1X または MAC 認証済みユーザは装置のポート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

5.1.10 port-security max-mac-count

Syntax

port-security max-mac-count *max-count* [**vlan** [*vlan-id-list*]]

undo port-security max-mac-count [**vlan** [*vlan-id-list*]]

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: ポートに許可するセキュア MAC アドレスの最大数を指定します。設定範囲は 1～2147483647 です。設定可能な設定の最大数は 2147483647 ですが、実際に使用できる数は 2048 になります。

vlan [*vlan-id-list*]: 最大 10 までの空白区切りリストを指定します。各 VLAN 項目は、*start-vlan-id* **to** *end-vlan-id* の形式で VLAN ID または VLAN ID の範囲を指定します。終了 VLAN ID を開始 VLAN ID より小さくすることはできません。VLAN ID の設定範囲は 1～4094 です。**vlan** を指定しない場合、このコマンドはポートセキュリティがポートで許可するセキュア MAC アドレスの最大数を設定します。*vlan-id-list* を指定しない場合、このコマンドはそれぞれのセキュア MAC アドレスの最大数を設定します。このオプションは、autoLearn モードで動作しているポートでのみ有効です。

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許可するセキュア 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た値
- 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。

このコマンドを設定する場合は、次のガイドラインと制限に従ってください。

- セキュリティで保護された MAC アドレスの最大数を確認します。VLAN は、現在保存されている MAC アドレスの数以上です。
- このコマンドを複数回実行して、同じ MAC アドレスに対してセキュア MAC アドレスの最大数を設定した場合 VLAN 最新の設定が有効になります。
- ポートが autoLearn モードで動作しているときは、ポートセキュリティの MAC アドレス数の制限を変更できません。

例

ポートセキュリティで GigabitEthernet 1/0/1 に許可するセキュア MAC アドレスの最大数を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security max-mac-count 100

関連コマンド

display port-security

5.1.11 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 はポートに設定されておらず、すべてのフレームは送信されます。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ntk-withbroadcasts: 認証された宛先 MAC アドレスのブロードキャストフレーム、ユニキャストフレームのみを送信します。

ntk-withmulticasts: 認証された宛先 MAC アドレスのブロードキャストフレーム、マルチキャストフレーム、ユニキャストフレームのみを送信します。

ntkonly: 認証された宛先 MAC アドレスのユニキャストフレームのみを送信します。

説明

port-security ntk-mode コマンドは NTK 機能を設定します。

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

NTK（need to know）機能は、送信フレームの宛先 MAC アドレスを確認します。この機能は、不正な装置がネットワークトラフィックを遮断することを防止し、認証にパスした装置のみフレームを送信できるようにします。

例

認証にパスした装置に受信パケットを転送するため、GigabitEthernet 1/0/1 の NTK モードを **ntkonly** に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly

関連コマンド

display port-security

5.1.12 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。このコマンドを使用して、特定のベンダの装置が認証されずにネットワークにアクセスできるようにします。たとえば、IP 電話とプリンタの OUI を指定できます。

このコマンドで設定された OUI 値は **userLoginWithOUI** モードで動作するポートにのみ適用します。**userLoginWithOUI** モードのポートは 802.1X ユーザと設定された OUI 値に一致する MAC アドレスのユーザのみ許可します。

例

OUI 値 000d2a を設定し、OUI インデックスを 4 に設定します。

<Switch> system-view

[Switch] port-security oui index 4 mac-address 000d-2a10-0033

関連コマンド

display port-security

5.1.13 port-security port-mode

Syntax

port-security port-mode { **autolearn** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }

undo port-security port-mode

デフォルト

ポートは **noRestrictions** モードで動作します。ポートセキュリティは適用しません。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

キーワード	セキュリティモード	説明
autolearn	autoLearn	このポートはMACアドレスを記憶できます。自動で学習されたMACアドレスは、ダイナミックMACアドレスとしてMACアドレステーブルに追加されません。セキュアMACアドレスとしてセキュアMACアドレステーブルに追加されます。**port-security mac-address security**コマンドでセキュアMACアドレスを設定することができます。**autoLearn**モードのポートは、以下の送信元MACアドレスのフレームを許可します。 ● セキュアMACアドレス ● **mac-address dynamic**コマンドと**mac-address static**コマンドで設定されたMACアドレス **port-security max-mac-count**コマンドで設定されたセキュアMACアドレス数が上限に到達したとき、ポートは**secure**モードに変更します。
mac-authentication	macAddressWithRadius	このモードのポートは、ユーザのMACアドレス認証を実行します。複数のユーザを処理します。

キーワード	セキュリティモード	説明
mac-else-userlogin-secure	macAddressElseUserLoginSecure	このモードは高いプライオリティを持つMACアドレス認証を行う**macAddressWithRadius**モードと**userLoginSecure**モードの組み合わせです。このモードのポートは、1つの802.1X認証ユーザと複数のMACアドレス認証を許可します。 ● non-802.1Xフレームを受信しているとき、MACアドレス認証のみを実行します。 ● 802.1Xフレームを受信しているとき、MACアドレス認証を行います。MACアドレス認証に失敗した場合は、802.1X認証を行います。
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	このモードは、ポート上の複数の802.1X認証およびMACアドレス認証を受けたユーザをサポートすること以外は、**macAddressElseUserLoginSecure**モードと同じです。
secure	secure	このモードでは、ポート上のMACアドレスの学習が無効です。**mac-address static**コマンドと**mac-address dynamic**コマンドを使ってMACアドレスの設定ができます。 以下の送信元MACアドレスのフレームを許可します。 ● セキュアMACアドレス ● **mac-address dynamic**コマンドと**mac-address static**コマンドで設定されたMACアドレス
userlogin	userLogin	このモードのポートは、802.1X認証を実行し、ポートベースのアクセス制御を行います。1つの802.1Xユーザが認証をパスした場合、他のすべての802.1Xユーザは、認証を受けることなく、ネットワークにアクセスできます。
userlogin-secure	userLoginSecure	このモードのポートは、802.1X認証を実行し、MACベースのアクセス制御を行います。802.1X認証をパスした1ユーザのみに対し、サービスを提供します。

キーワード	セキュリティモード	説明
userlogin-secure-ext	userLoginSecureExt	ポート上の複数のオンライン802.1X認証を受けたユーザをサポートすることを除き、**userLoginSecure**モードと同じです。
userlogin-secure-or-mac	macAddressOrUserLoginSecure	このモードは、**userLoginSecure**モードと**macAddressWithRadius**モードを組み合わせたものです。ポートは1つの802.1X認証ユーザと複数のMACアドレス認証を許可します。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。 ただし、次の条件に当てはまる場合、このモードのポートは認証を異なる方法で処理します。 ● ポートはMAC認証と802.1X認証の並列処理で有効になっています。 ● ポートが802.1Xユニキャストトリガで有効になっています。 ● ポートは不明なMACアドレスからパケットを受信します。 このような条件下では、ポートはユニキャストEAP-Request / Identityパケットを MACアドレスに送信して、802.1X認証を開始します。その後、ポートは802.1X認証結果を待たずにただちにMAC認証を処理します。
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	このモードは、複数の802.1X認証およびMACアドレス認証を受けたポート上のユーザをサポートすること以外は、**macAddressOrUserLoginSecure**モードと同じです。
userlogin-withoui	userLoginWithOUI	**userLoginSecure**モードと同じです。加えて、このモードのポートは、指定されたOUIを含むMACアドレスを持つユーザからのフレームを許可します。このモードのポートは、OUIの確認を最初に実行します。OUIの確認が失敗した場合、802.1X認証を実行します。ポートはOUIの確認あるいは802.1X認証にパスしたフレームを許可します。

説明

port-security port-mode コマンドはポートのセキュリティモードを設定します。

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

ポートセキュリティが有効なポートのセキュリティモードを変更する場合、最初に **noRestrictions** モードに設定します。ポートにオンラインユーザがいる場合、セキュリティモードを変更することができません。

⚠ **注意:**

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ます。ポートが **autoLearn** モードで動作しているとき、設定を変更することはできません。

ポートセキュリティが有効なとき、802.1X や MAC アドレス認証を手動で有効にすることはできません。また、アクセスコントロールモードやポート許可状態を変更することはできません。ポートセキュリティは、異なるセキュリティモードの設定を自動で修正します。

MAC アドレス認証の開始を遅らせる機能が有効なポートで **mac-else-userlogin-secure** モードあるいは **mac-else-userlogin-secure-ext** モードを有効にしないことを推奨します。2 つのモードは MAC アドレス認証の開始を遅らせる機能と同時に設定することができません。MAC アドレス認証の開始を遅らせる機能の詳細は、コマンドマニュアルのセクション 8 *セキュリティ “MAC アドレス認証”* を参照してください。

例

ポートセキュリティを有効にし、GigabitEthernet 1/0/1 が secure モードで動作するように設定します。

<Switch> system-view

[Switch] port-security enable

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security port-mode secure

GigabitEthernet 1/0/1 のポートセキュリティモードを userLogin に変更します。

[Switch-GigabitEthernet1/0/1] undo port-security port-mode

[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin

関連コマンド

- **display port-security**
- **port-security max-mac-count**

5.1.14 port-security timer autolearn aging

Syntax

port-security timer autolearn aging second *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

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

second *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。time-value 引数の設定範囲は 10～7776000 です。

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。

タイマのエージングの効果は、タイマのエージングの設定によって異なります。

- エージングタイマを秒単位で設定する場合、有効なエージングタイマは次のいずれかの値になります。
  - 設定されたタイマが 60 秒以上である場合、設定されたエージングタイマに最も近い 30 秒の倍数です。有効エージングタイマは、設定エージングタイマ以上です。
    たとえば、エージングタイマを 80 秒に設定した場合、実際に有効になるエージングタイマは 90 秒です。
  - 設定されているタイマが 60 秒未満の場合は、設定されているエージングタイマです。

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。

インアクティビティエージングで短時間のエージングタイム(60 秒未満)を使用する場合は、ポートのセキュア MAC アドレスの最大数に大きな値を割り当てないでください。この場合、大きな値を設定すると、装置のパフォーマンスに影響することがあります。QX-S5300G シリーズは、インアクティビティエージングをサポートしていません。

インタフェースビューとシステムビューの両方でタイマを設定する場合、インタフェースビューの設定が優先されます。実際に有効になるエージングタイマは、インタフェースビューで設定された値を使用します。

例

GigabitEthernet 1/0/1 のセキュア MAC アドレスのエージング タイマを 50 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security timer autolearn aging second 50

関連コマンド

- **display port-security**
- **port-security mac-address security**

5.1.15 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指定します。

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することができます。

例

GigabitEthernet 1/0/1 で一時的にポートを無効にするように侵入防止アクションを設定し、タイムアウト時間を 30 秒に設定します。

<Switch> system-view

[Switch] port-security timer disableport 30

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily

関連コマンド

- **display port-security**
- **port-security intrusion-mode**

5.1.16 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

パラメータ

address-learned: 新しい MAC アドレスが学習されたとき、SNMP notification の送信を有効にします。

dot1x-failure: ユーザが 802.1X 認証に失敗したとき、SNMP notification の送信を有効にします。

dot1x-logoff: 802.1X 認証にパスしたユーザがログオフしたとき、SNMP notification の送信を有効にします。

dot1x-logon: ユーザが 802.1X 認証にパスしたとき、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とき、SNMP notification の送信を有効にします。

mac-auth-failure: ユーザが MAC アドレス認証に失敗したとき、SNMP notification の送信を有効にします。

mac-auth-logoff: MAC アドレス認証にパスしたユーザがログオフしたとき、SNMP notification の送信を有効にします。

mac-auth-logon: ユーザが MAC アドレス認証にパスしたとき、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 SNMP notification の通知を有効にします。

undo snmp-agent trap enable port-security コマンドは SNMP notification の通知を無効にします。

パラメータを指定しない場合、すべての SNMP notification を有効にします。

ポートセキュリティモジュールで重要なイベントを通知するため、SNMP notification を作成します。作成された notification は SNMP モジュールに送信されます。SNMP モジュールは SNMP 通知の設定にもとづいて通知します。SNMP notification の詳細は、オペレーションマニュアルのセクション 10 *システム管理* “*SNMP*”を参照してください。

このコマンドを有効にするには、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

新しい MAC アドレスが学習されたとき、装置で 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 **8-x-x** です。

6 章 パスワード管理.....6-1
6.1 パスワード管理設定コマンド.....6-1
6.1.1 display password-control.....6-1
6.1.2 display password-control blacklist.....6-3
6.1.3 password-control { aging | composition | history | length } enable.....6-4
6.1.4 password-control aging.....6-6
6.1.5 password-control alert-before-expire.....6-7
6.1.6 password-control complexity.....6-8
6.1.7 password-control composition.....6-10
6.1.8 password-control enable.....6-12
6.1.9 password-control expired-user-login.....6-13
6.1.10 password-control history.....6-14
6.1.11 password-control length.....6-15
6.1.12 password-control login idle-time.....6-16
6.1.13 password-control login-attempt.....6-17
6.1.14 password-control super aging.....6-20
6.1.15 password-control super composition.....6-21
6.1.16 password-control super length.....6-22
6.1.17 password-control update-interval.....6-23
6.1.18 reset password-control blacklist.....6-24
6.1.19 reset password-control history-record.....6-25

6章 パスワード管理

6.1 パスワード管理設定コマンド

6.1.1 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。

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
 Password history was last reset:     0 days ago (device management users)
                                  0 days ago (network access users)
 Minimum interval between two updates: 24 hours
```

```
User account idle time:              90 days
Logins with aged password:           3 times in 30 days
Password complexity:                 Disabled (username checking)
                                     Disabled (repeated characters checking)
Password change:                     Enabled (first login)
                                     Enabled (mandatory weak password change)
```

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 6-1 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。
User authentication timeout	ユーザ認証タイムアウト時間です。
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。
Password history was last reset	装置管理またはネットワークアクセスユーザのパスワード履歴レコードが最後に削除された時刻です。
Minimum interval between two updates	パスワードアップデートの最小間隔です。
Logins 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。
Password change	初回ログイン時のパスワード変更機能が有効かどうか示します。 ● Enabled (first login) ● Disabled (first login) 脆弱なログインパスワードの変更必須機能が有効かどうか示します。 ● Enabled (mandatory weak password change) ● Disabled (mandatory weak password change)

6.1.2 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。

ユーザが認証に失敗すると、ユーザの IP アドレスとユーザアカウントがパスワード管理ブラックリストに追加されます。このコマンドを使用して、ブラックリストに登録された FTP および VTY ユーザに関する情報を表示できます。

コンソールインタフェースを経由してシステムにアクセスするユーザは、次の理由でブラックリストに登録されません。

- システムはこれらのユーザの IP アドレスを取得できません。
- これらのユーザには特権があり、したがって、システムに対して比較的安全です。

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 6-2 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。 ● **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無効になります。

6.1.3 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。

特定のパスワード制御機能を有効にするには、グローバルパスワード制御と特定のパスワード制御機能の両方が有効になっていることを確認してください。たとえば、グローバルパスワード制御と最小パスワード長制限機能が有効になっていない場合、**password-control length** コマンドは有効になりません。

undo password-control history enable コマンドを実行すると、システムは履歴パスワードの記録を停止しますが、以前の記録は削除されません。

グローバルパスワード制御機能が有効になっているが、最小パスワード長制限機能が無効になっている場合、パスワードには 4 文字以上が含まれている必要があり、4 文字以上が異なっている必要があります。

Ver7.2.23 を含む以降のソフトウェアでは、グローバルパスワード制御機能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。

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機能を有効にします。

[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**

6.1.4 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**

6.1.5 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

6.1.6 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

グローバルのパスワードの複雑性のポリシーは、**user-name check** と **same-character check** の両方が無効です。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。

Version 7.2.23 以降：

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。Version 7.2.23 以降は、**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。

user-name check コマンドと、**same-character check** コマンドの両方を有効にすることができます。

例

ユーザ名を含むパスワード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**

6.1.7 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 1 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。

Version 7.2.23 以降：

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。

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。

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**

6.1.8 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 complexity**
- **password-control** { **aging** | **composition** | **history** | **length** } **enable**
- **password-control update-interval**

6.1.9 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。

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、ユーザがログインできないようにするには、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。

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

6.1.10 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。

undo password-control history enable コマンドを実行すると、システムはパスワードの記録を停止しますが、以前の記録は削除されません。

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**

6.1.11 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。

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**

6.1.12 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

6.1.13 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**: ユーザアカウントを永久に無効にします。
  Version 7.2.23 以降では、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*: ユーザアカウントを一定の期間、無効にします。ユーザは一定の期間が終了した後、ユーザアカウントを使用することができます。設定範囲は 1～360 分です。
  Version 7.2.23 以降では、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。Version 7.2.23 以降では、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。Version 7.2.23 以降では、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。

🕮 **メモ：**

このアカウントは、このユーザに対してのみロックされています。他のユーザは引き続きこのアカウントを使用でき、ブラックリストに登録されたユーザは他のユーザアカウントを使用できます。

---

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**

6.1.14 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**

6.1.15 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 1 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。

Version 7.2.23 以降：

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。

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**

6.1.16 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。

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**

6.1.17 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

6.1.18 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。次に、ブラックリストに記録されたユーザは、このユーザアカウントを使用してログインできます。

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**

6.1.19 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 です。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 **8-x-x** です。

7 章 公開鍵 7-1
7.1 公開鍵設定コマンド.....7-1
7.1.1 display public-key local public.....7-1
7.1.2 display public-key peer 7-5
7.1.3 peer-public-key end 7-7
7.1.4 public-key local create 7-8
7.1.5 public-key local destroy.....7-12
7.1.6 public-key local export dsa.....7-14
7.1.7 public-key local export rsa.....7-17
7.1.8 public-key peer 7-19
7.1.9 public-key peer import sshkey.....7-20

7章 公開鍵

7.1 公開鍵設定コマンド

7.1.1 display public-key local public

Syntax

display public-key local { **dsa** | **ecdsa** | **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。

ecdsa: ECDSA 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*: 鍵ペアの名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しません。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。

ローカル非対称鍵ペアの公開鍵を、装置のピアにコピー、転送することができます。

name key-name オプションを指定しても、デフォルトの鍵ペア名を持つホスト公開鍵を表示することはできません。デフォルトの鍵ペア名を持つホスト公開鍵を表示するには、鍵ペア名を指定せずにこのコマンドを使用してすべてのローカル公開鍵を表示します。

例

すべてのローカル RSA 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 公開鍵を表示します。

<Switch> display public-key local dsa public

```
==========================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
  308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
  96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
  DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
  DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
  7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
  4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
  35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
  91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
```

```
  585DA7F42519718CC9B09EEF038184000281804191 2CE34D12BCD2157E7AB1C2F03B3EF395
  100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
  52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
  887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
=============================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
  308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
  96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
  DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
  DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
  7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
  4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
  35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
  91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
  585DA7F42519718CC9B09EEF038185000281810 0A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
  3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
  0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
  15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

すべてのローカル ECDSA 公開鍵を表示します。

<Switch> display public-key local ecdsa public

```
=============================================
Key name: ecdsakey (default)
Key type: ECDSA
Time when key pair created: 15:42:04 2011/05/12
Key code:
  3049301306072A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
  68F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
  1D
=============================================
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
  3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
  AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
  4D
```

ローカルの RSA 鍵ペア rsa1 の公開鍵を表示します。

<Switch> display public-key local rsa public name rsa1

```
=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
  30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
  426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
  1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
  9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
  92D8C6D940890BF4290203010001
```

ローカルの 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
```

ローカルの ECDSA 鍵ペア ecdsa1 の公開鍵を表示します。

<Switch> display public-key local ecdsa public name ecdsa1

```
=============================================
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
  3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
  AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
  4D
```

表 7-1 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。 ● **ecdsakey**–デフォルトECDSAホスト鍵ペア名です。
Key type	オプションです。 ● RSA ● DSA ● ECDSA
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

7.1.2 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 7-2 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あるいはECDSA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 7-3 コマンド出力

フィールド	説明
Type	鍵タイプです。RSA、DSA あるいはECDSAがあります。
Modulus	鍵モジュール長です。単位はビットです。
Name	ピアのホスト公開鍵の名前です。

関連コマンド

- **public-key peer**
- **public-key peer import sshkey**

7.1.3 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、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**

7.1.4 public-key local create

Syntax

public-key local create { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] | **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。

ecdsa: ECDSA 鍵ペアタイプを指定します。

- secp192r1: secp192r1 曲線を使用して、192 ビット ECDSA 鍵ペアを作成します。
- secp256r1: secp256r1 曲線を使用して、256 ビット ECDSA 鍵ペアを作成します。
- secp384r1: secp384r1 曲線を使用して、384 ビットの ECDSA 鍵ペアを作成します。
- secp521r1: secp521r1 曲線を使用して、521 ビットの ECDSA 鍵ペアを作成します。

デフォルトでは、secp192r1 カーブが使用されます。

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。大文字、小文字を区別しません。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 7-4 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
ECDSA	ecdsakey

説明

public-key local create コマンドはローカル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。

RSA または DSA 鍵ペアを作成するときは、プロンプトで適切な鍵モジュールの長さを入力します。

ECDSA 鍵ペアを作成するときは、適切な楕円曲線を選択します。楕円曲線は ECDSA 鍵長を決定します。鍵の長さは表 7-5 に示すように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 7-5 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
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。 📖 **メモ**: SSH1.5のみがRSAサーバ鍵ペアを使用します。	RSA鍵係数の長さ: ● 512～4096ビットです。デフォルトは1024ビットです。セキュリティを確保するには、768ビット以上を使用してください。
DSA	1つのホスト鍵ペアを作成します。	DSA鍵係数の長さ: ● 512～2048ビットです。デフォルトは1024ビットです。セキュリティを確保するには、768ビット以上を使用してください。
ECDSA	ホスト鍵ペアを作成します。	ECDSA鍵長: ● 192,256,384ビットまたは521ビットです。

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.
```

デフォルト名のローカル ECDSA 鍵ペアを作成します。

<Switch> system-view

[Switch] public-key local create ecdsa

```
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.
```

名前が ecdsa1 のローカル ECDSA 鍵ペアを作成します。

<Switch> system-view

[Switch] public-key local create ecdsa name ecdsa1

```
Generating Keys...
Create the key pair successfully.
```

関連コマンド

- **display public-key local public**
- **public-key local destroy**

7.1.5 public-key local destroy

Syntax

public-key local destroy { **dsa** | **ecdsa** | **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。

ecdsa: ECDSA 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。大文字、小文字を区別しません。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、デフォルト名のローカル鍵ペアの指定されたタイプを削除します。

説明

public-key local destroy コマンドはローカル鍵ペアを削除します。

以下の状況が発生した場合、鍵を正常に保つため、ローカル非対称鍵ペアを削除し、新しいペアを生成する必要があります。

- 不正侵入が発生した場合。
- 装置の記憶媒体を交換した場合。
- ローカル証明書が期限切れとなった場合。ローカル証明書の詳細は、オペレーションマニュアルのセクション 8 *セキュリティ* を参照してください。

例

デフォルト名のローカル RSA 鍵ペアを削除します。

<Switch> system-view

[Switch] public-key local destroy rsa

```
Confirm to destroy the key pair? [Y/N]:y
```

デフォルト名のローカル DSA 鍵ペアを削除します。

<Switch> system-view

[Switch] public-key local destroy dsa

```
Confirm to destroy the key pair? [Y/N] :y
```

デフォルト名のローカルの ECDSA 鍵ペアを削除します。

<Switch> system-view

[Switch] public-key local destroy ecdsa

```
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
```

名前が ecdsa1 のローカル ECDSA 鍵ペアを削除します。

<Switch> system-view

[Switch] public-key local destroy ecdsa name ecdsa1

```
Confirm to destroy the key pair? [Y/N]:y
```

関連コマンド

public-key local create

7.1.6 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。大文字、小文字を区別しません。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 DSA 鍵ペアのホスト公開鍵をエクスポートします。

openssh: OpenSSH の形式のホスト公開鍵をエクスポートします。

ssh2: SSH2.0 の形式のホスト公開鍵をエクスポートします。

filename: 保存するローカルホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。”./”、”../”を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュにすることができません。ファイル名の詳細は、オペレーションマニュアルのセクション 1 *はじめに “ファイルシステム管理”* を参照してください。名前を指定しない場合、鍵はエクスポートせず、モニタスクリーン上の鍵を表示します。

説明

public-key local export dsa コマンドはローカル DSA ホスト公開鍵をエクスポートします。

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エクスポートすることができます。

ローカル DSA ホスト公開鍵をピアの装置に分配するには、以下の手順に従ってください。

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、ローカルホスト公開鍵をエクスポートします。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、指定したファイルに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 あるいは TFTP の詳細については、オペレーションマニュアルのセクション 1 *はじめに* 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**

7.1.7 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。大文字、小文字を区別しません。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エクスポートします。

openssh: OpenSSH の形式のホスト公開鍵をエクスポートします。

ssh1: SSH1.5 の形式のホスト公開鍵をエクスポートします。

ssh2: SSH2.0 の形式のホスト公開鍵をエクスポートします。

filename: 保存するローカルホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。“./”、“../” を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュにすることができません。ファイル名の詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*ファイルシステム管理*” を参照してください。名前を指定しない場合、鍵はエクスポートせず、モニタスクリーン上の鍵を表示します。

説明

public-key local export rsa コマンドはローカル RSA ホスト公開鍵をエクスポートします。

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、ローカルホスト公開鍵をエクスポートします。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、指定したファイルに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。詳細はオペレーションマニュアルのセクション 1 *はじめに* 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。

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を使用して、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

SSH 2.0 形式で、ローカル RSA 鍵ペアのホスト公開鍵をデフォルト名で表示します。

<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 形式で、ローカル RSA 鍵ペアのホスト公開鍵をデフォルト名で表示します。

<Switch> system-view

[Switch] public-key local export rsa openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

ローカル RSA 鍵ペア rsa1 のホスト公開鍵を OpenSSH 形式でファイル 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

SSH 2.0 形式で、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 形式で、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**

7.1.8 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

public-key peer コマンドはピアのホスト公開鍵の名前を指定し、public key view に移行するか、drive デフォルトのピアのホスト公開鍵の view に移行します。

undo public-key peer コマンドはピアのホスト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ホスト公開鍵を手動で指定するため、あらかじめ 16 進数のピアのホスト公開鍵を取得し、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

ピアのホスト公開鍵 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**

7.1.9 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。

filename: 保存するピアのホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。”./”、”../” を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭

をスラッシュにすることができません。ファイル名の詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*ファイルシステム管理*”を参照してください。

説明

public-key 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ため、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が必要となります。

装置は SSH 1.5、SSH 2.0、OpenSSH の形式の公開鍵のインポートをサポートします。

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 **8-x-x** です。

8 章 PKI 8-1
8.1 PKI 設定コマンド 8-1
8.1.1 attribute 8-1
8.1.2 ca identifier 8-3
8.1.3 certificate request entity 8-4
8.1.4 certificate request from 8-5
8.1.5 certificate request mode 8-6
8.1.6 certificate request polling 8-7
8.1.7 certificate request url 8-8
8.1.8 common-name 8-9
8.1.9 country 8-10
8.1.10 crl check enable 8-10
8.1.11 crl url 8-11
8.1.12 display pki certificate access-control-policy 8-12
8.1.13 display pki certificate attribute-group 8-14
8.1.14 display pki certificate domain 8-15
8.1.15 display pki certificate request-status 8-19
8.1.16 display pki crl domain 8-20
8.1.17 fqdn 8-23
8.1.18 ip 8-23
8.1.19 locality 8-24
8.1.20 organization 8-25
8.1.21 organization-unit 8-26
8.1.22 pki abort-certificate-request 8-27
8.1.23 pki certificate access-control-policy 8-28
8.1.24 pki certificate attribute-group 8-29
8.1.25 pki delete-certificate 8-30
8.1.26 pki domain 8-31
8.1.27 pki entity 8-32
8.1.28 pki import 8-33
8.1.29 pki request-certificate 8-38
8.1.30 pki retrieve-certificate 8-40
8.1.31 pki retrieve-crl 8-42
8.1.32 pki storage 8-43
8.1.33 pki validate-certificate 8-44
8.1.34 public-key dsa 8-47

8.1.35 public-key ecdsa 8-48
8.1.36 public-key rsa 8-49
8.1.37 root-certificate fingerprint 8-51
8.1.38 state 8-53

8章 PKI

8.1 PKI設定コマンド

8.1.1 attribute

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

undo attribute *id*

デフォルト

設定なし

View

Certificate attribute group view

定義済みユーザロール

network-admin

パラメータ

id: ルール ID を指定します。設定範囲は 1～16 です。

alt-subject-name: 代替サブジェクト名フィールドを指定します。

fqdn: FQDN 属性を指定します。

ip: IP アドレス属性を指定します。

dn: DN 属性を指定します。

issuer-name: 発行者名フィールドを指定する。

subject-name: サブジェクト名のフィールドを指定します。

ctn: コンテインオペレーションを指定します。

equ: イコールオペレーションを指定します。

nctn: 非コンテインオペレーションを指定します。

nequ: 非イコールオペレーションを指定します。

attribute-value: 属性値を設定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。

説明

attribute コマンドは証明書の発行者名、サブジェクト名、または代替サブジェクト名フィールドの属性に基づいて証明書をフィルタリングするルールを設定します。

undo attribute コマンドは属性ルールを削除します。

証明書のフィールドによってサポートされる属性が異なります。

- サブジェクト名フィールドおよび発行者名フィールドには、単一の DN、複数の FQDN、および複数の IP アドレスを含めることができます。
- 代替のサブジェクト名フィールドには、複数の FQDN と IP アドレスを含めることができますが、DN は 0 です。

属性ルールは、表 8-1 に示すように、属性-値のペアと操作キーワードの組み合わせたものです。

表 8-1 属性-値のペアと操作キーワードの組み合わせ

オプション	DN	FQDN/IP
ctn	DNには指定された属性値が含まれています。	FQDNまたはIPアドレスには、指定された属性値が含まれています。
nctn	DNには指定された属性値が含まれていません。	指定された属性値を含むFQDNまたはIPアドレスがありません。
equ	DNは指定された属性値と同じです。	FQDNまたはIPアドレスは、指定された属性値と同じです。
nequ	DNは指定された属性値と同じではありません。	指定された属性値と同じFQDNまたはIPアドレスはありません。

証明書が属性ルールに一致するのは、ルールで定義された基準に一致する属性を含む場合です。例えば、証明書が以下の条件を満たす場合、証明書は **attribute 1 subject-name dn ctn abc** ルールに一致します。

- 証明書のサブジェクト名フィールドに DN 属性が含まれています。
- DN 属性値に **abc** の文字列が含まれています。

証明書が属性グループに一致するのは、そのグループ内のすべての属性ルールに一致する場合です。

例

証明書属性グループを作成し、その view に移行します。

<Switch> system-view

[Switch] pki certificate attribute-group mygroup

サブジェクト DN に **abc** 文字列を含む証明書と一致する属性ルールを設定します。

[Switch-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc

発行者名フィールドに FQDN **abc** を含まない証明書に一致する属性ルールを設定します。

[Switch-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc

代替サブジェクト名フィールドに IP アドレス **10.0.0.1** が含まない証明書と一致するように属性ルールを設定します。

[Switch-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1

関連コマンド

display pki certificate attribute-group

8.1.2 ca identifier

Syntax

ca identifier *name*

undo ca identifier

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name: 信頼できる CA 名で指定します。設定範囲は 1～63 文字です。大文字小文字を区別する文字列です。

説明

ca identifier コマンドは信頼できる CA を指定します。

undo ca identifier コマンドはデフォルトに戻します。

PKI ドメインで CA 証明書を取得するには、信頼できる CA 名を指定する必要があります。信頼できる CA 名は、PKI ドメインに指定された CA サーバに複数の CA が存在する場合に使用される CA を一意に識別します。

指定された CA 名が、取得する CA 証明書を所有する CA 名と一致していることを確認してください。

例

信頼できる CA 名を **new-ca** に設定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] ca identifier new-ca

8.1.3 certificate request entity

Syntax

certificate request entity *entity-name*

undo certificate request entity

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

entity-name: PKI エンティティ名を指定します。設定範囲は 1～31 文字です。大文字と小文字を区別しません。

説明

certificate request entity コマンドは証明書要求の PKI エンティティを指定します。

undo certificate request entity コマンドはデフォルトに戻します。

PKI エンティティは、次の情報を含む、証明書要求のエンティティの ID 属性を記述します。

- コモンネーム
- 組織
- 組織内のユニット
- 地域
- エンティティが存在する州と国
- FQDN
- IP アドレス

PKI ドメインに指定できる PKI エンティティは 1 つだけです。このコマンドを複数回実行すると、最新の設定が有効になります。

例

PKI ドメイン **aaa** の証明書要求に PKI エンティティ **en1** を指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] certificate request entity en1

関連コマンド

pki entity

8.1.4 certificate request from

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

ca: CA に証明書要求を送信します。

ra: RA に証明書要求を送信します。

説明

certificate request from コマンドは証明書要求の受信機関の種類を指定します。

undo certificate request from コマンドはデフォルトに戻します。

CA サーバは、CA または RA が証明書要求を受け入れるかどうかを決定します。この権限設定は、CA サーバの設定と一致している必要があります。

例

RA に証明書要求を送信します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] certificate request from ra

8.1.5 certificate request mode

Syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string*] | **manual** }

undo certificate request mode

デフォルト

manual

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

auto: 自動証明書要求モードを指定します。

password: 証明書失効時のパスワードを指定します。

cipher: 暗号化形式でパスワードを指定します。

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設定されたパスワードは暗号化された形式で保存されます。

string: パスワードを指定します。プレーンテキスト形式は、設定範囲が 1～31 文字です。大文字小文字を区別する文字列です。暗号化形式は、設定範囲が 1～73 文字です。大文字小文字を区別する文字列です。

manual: 手動証明書要求モードを指定します。

説明

certificate request mode コマンドは証明書要求モードを設定します。

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

証明書要求は、オフラインモードまたはオンラインモードで CA に送信できます。オンラインモードでは、証明書要求を自動または手動で送信できます。

- **Auto request mode**—次の両方の条件が存在する場合、PKI エンティティは自動的に CA 証明書を取得し、CA に証明書要求を送信します。
  - 関連するアプリケーション（IKE など）が ID 認証を実行します。
  - 装置のアプリケーションで使用できる証明書がありません。

  自動要求モードでは、CA ポリシーで要求される証明書失効のためのパスワードを指定します。
- **Manual request mode**— CA 証明書を手動で取得し、証明書要求を送信する必要があります。

例

証明書要求モードを **auto** に設定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] certificate request mode auto

証明書要求モードを **auto** に設定し、証明書失効パスワードをプレーンテキストで **123456** に設定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] certificate request mode auto password simple 123456

関連コマンド

pki request-certificate

8.1.6 certificate request polling

Syntax

certificate request polling { **count** *count* | **interval** *interval* }

undo certificate request polling { **count** | **interval** }

デフォルト

ポーリング間隔は 20 分で、最大試行回数は 50 回です。

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

count *count*: クエリの最大試行回数を指定します。設定範囲は 1～100 です。

interval *interval*: ポーリング間隔を分単位で指定します。設定範囲は 5～168 です。

説明

certificate request polling コマンドはポーリング間隔と証明書要求ステータスを照会する最大試行回数を設定します。

undo certificate request polling コマンドはデフォルトに戻します。

PKI エンティティが証明書要求を送信した後、CA 管理者が証明書要求を手動で承認する必要がある場合、CA サーバが証明書を発行するまでにしばらく時間がかかることがあります。この期間中、PKI エンティティは定期的に CA サーバに証明書要求ステータスを問い合せます。定期的なクエリ動作は、PKI エンティティが証明書を取得するか、クエリの最大試行回数に達するまで停止します。クエリの最大試行回数に達すると、証明書要求は失敗します。

CA サーバが証明書要求を自動的に承認する場合、PKI エンティティは、証明書要求を送信した直後に証明書を取得できます。この場合、PKI エンティティは CA サーバにクエリを送信しません。

例

ポーリング間隔を 15 分、クエリの最大試行回数を 40 回に設定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] certificate request polling interval 15

[Switch-pki-domain-aaa] certificate request polling count 40

関連コマンド

display pki certificate request-status

8.1.7 certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

url-string: 証明書要求受信機関の URL を指定します。設定範囲は 1～511 文字です。大文字と小文字を区別します。URL の長さは、CLI 文字列の制限または *url-string* パラメータのいずれか小さい方によって制限されます。

説明

certificate request url コマンドは装置が SCEP 証明書要求を送信する証明書要求受信機関（CA または RA）の URL を指定します。

undo certificate request url コマンドはデフォルトに戻します。

証明書要求 URL には、証明書要求受信機関サーバの場所と、サーバ上のアプリケーションスクリプトのパスが http://*server_location/cgi_script_location* の形式で含まれています。

例

証明書要求 URL を **http://169.254.0.1/certsrv/mscep/mscep.dll** に設定します。

<Switch> system-view

[Switch] pki domain a

[Switch-pki-domain-a] certificate request url http://169.254.0.1/certsrv/mscep/mscep.dll

8.1.8 common-name

Syntax

common-name *common-name-sting*

undo common-name

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

common-name-sting: コモンネームを指定します。設定範囲は 1～63 文字です。大文字と小文字を区別します。カンマを含めることはできません。PKI エンティティのユーザ名をコモンネームとして設定できます。

説明

common-name コマンドは PKI エンティティのコモンネームを設定します。

undo common-name コマンドはデフォルトに戻します。

例

PKI エンティティ **en** を **test** するためのコモンネームを設定します。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en] common-name test

8.1.9 country

Syntax

country *country-code-string*

undo country

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

country-code-string: 国コードを指定します。大文字と小文字を区別する 2 文字の文字列です。例えば、JP は日本の国コードです。

説明

country コマンドは PKI エンティティの国コードを設定します。

undo country コマンドはデフォルトに戻します。

例

PKI エンティティ 1 の国コードを JP に設定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] country JP

8.1.10 crl check enable

Syntax

crl check enable

undo crl check enable

デフォルト

有効

View

PKI domain view

定義済みユーザロール

network-admin

説明

crl check enable コマンドは CRL チェックを有効にします。

undo crl check enable コマンドは CRL チェックを無効にします。

CRL は、CA によって署名し公開された失効した証明書のリストです。失効した証明書は信頼できなくなります。

CRL チェックを有効にして、装置が発行元の CA によって取り消されていない証明書のみを受け入れるようにします。

例

CRL チェックを無効にします。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] undo crl check enable

関連コマンド

pki import

pki retrieve-certificate

pki validate-certificate

8.1.11 crl url

Syntax

crl url *url-string*

undo crl url

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

url-string: CRL リポジトリの URL を指定します。設定範囲は 1～511 文字です。大文字と小文字を区別します。URL の形式は ldap://*server_location* または http://*server_location* です。URL の長さは、CLI 文字列の制限または *url-string* パラメータのいずれか小さい方によって制限されます。

説明

crl url コマンドは CRL リポジトリの URL を設定します。

undo crl url コマンドはデフォルトに戻します。

CRL チェックを使用するには、CRL リポジトリから CRL を取得する必要があります。

装置は、次の順序で CRL リポジトリを選択します。

1) このコマンドを使用して PKI ドメインに指定された CRL リポジトリ
2) 検証中の証明書の CRL リポジトリ
3) CA 証明書の CRL リポジトリ、または CA 証明書が検証対象の証明書の場合は上位レベルの CA 証明書の CRL リポジトリ

前の選択プロセスの後、CRL リポジトリが見つからない場合、装置は SCEP を通じて CRL を取得します。このシナリオでは、CA 証明書とローカル証明書が取得されている必要があります。

例

CRL リポジトリの URL を **http://169.254.0.30** に設定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] crl url http://169.254.0.30

関連コマンド

pki retrieve-crl

8.1.12 display pki certificate access-control-policy

Syntax

display pki certificate access-control-policy [*policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name: 証明書ベースのアクセスコントロール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、小文字を区別しません。

説明

display pki certificate access-control-policy コマンドは証明書ベースのアクセスコントロールポリシーに関する情報を表示します。

ポリシー名を指定しない場合、このコマンドはすべての証明書ベースのアクセスコントロールポリシーに関する情報を表示します。

例

証明書ベースのアクセスコントロールポリシー**mypolicy** に関する情報を表示します。

<Switch> display pki certificate access-control-policy mypolicy

```
Access control policy name: mypolicy
    Rule 1  deny    mygroup1
    Rule 2  permit  mygroup2
```

すべての証明書ベースのアクセスコントロールポリシーに関する情報を表示します。

<Switch> display pki certificate access-control-policy

```
Total PKI certificate access control policies: 2
 Access control policy name: mypolicy1
    Rule 1  deny    mygroup1
    Rule 2  permit  mygroup2
 Access control policy name: mypolicy2
    Rule 1  deny    mygroup3
    Rule 2  permit  mygroup4
```

表 8-2 コマンド出力

フィールド	説明
Total PKI certificate access control policies	証明書ベースのアクセスコントロールポリシーの合計数です。
permit	アクセスコントロールルールの属性グループと一致する証明書を許可します。
deny	アクセスコントロールルールの属性グループに一致する証明書を拒否します。

関連コマンド

pki certificate access-control-policy

8.1.13 display pki certificate attribute-group

Syntax

display pki certificate attribute-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: 証明書属性グループ名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。

説明

display pki certificate attribute-group コマンドは証明書属性グループに関する情報を表示します。

証明書属性グループを指定しない場合、このコマンドはすべての証明書属性グループに関する情報を表示します。

例

証明書属性グループ **mygroup** に関する情報を表示します。

<Switch> display pki certificate attribute-group mygroup

```
Attribute group name: mygroup
     Attribute  1 subject-name    dn    ctn   abc
     Attribute  2 issuer-name     fqdn  nctn  app
```

すべての証明書属性グループに関する情報を表示します。

<Switch> display pki certificate attribute-group

```
Total PKI certificate attribute groups: 2.
 Attribute group name: mygroup1
     Attribute  1 subject-name    dn    ctn   abc
     Attribute  2 issuer-name     fqdn  nctn  app
Attribute group name: mygroup2
     Attribute  1 subject-name    dn    ctn   def
     Attribute  2 issuer-name     fqdn  nctn  fqd
```

表 8-3 コマンド出力

フィールド	説明
Total PKI certificate attribute groups	証明書属性グループの合計数です。
ctn	操作が含まれています。
nctn	操作は含まれていません。
equ	同等の操作です。
nequ	等しくない操作です。
Attribute 1 subject-name dn ctn abc	属性ルールの内容： • **alt-subject-name**—代替のサブジェクト名です。 • **issuer-name**—証明書の発行者名です。 • **subject-name**—証明書のサブジェクト名です。 • **fqdn**— PKIエンティティのFQDNです。 • **ip**— PKI エンティティの IP アドレスです。 • **dn**— PKIエンティティのDNです。 • **ctn**—含有操作を示します。 • **equ**—等しい操作を示します。 • **nctn**—含まれていない操作を示します。 • **nequ**—等しくない操作を示します。

関連コマンド

attribute

pki certificate attribute-group

8.1.14 display pki certificate domain

Syntax

display pki certificate domain *domain-name* { **ca** | **local** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-4 に示す特殊文字を含めることはできません。

表 8-4 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: CA 証明書を指定します。

local: ローカル証明書を指定します。

説明

display pki certificate domain コマンドは証明書に関する情報を表示します。

CA キーワードを指定した場合、このコマンドはドメイン内のすべての CA 証明書に関する情報を表示します。ドメインに RA 証明書がある場合は、RA 証明書も表示されます。

local キーワードを指定すると、このコマンドはドメイン内のすべてのローカル証明書に関する情報を表示します。

例

PKI ドメイン **aaa** の CA 証明書に関する情報を表示します。

<Switch> display pki certificate domain aaa ca

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=docm, OU=rnd, CN=rootca
        Validity
            Not Before: Jan  6 02:51:41 2011 GMT
            Not After : Dec  7 03:12:05 2013 GMT
        Subject: C=cn, O=ccc, OU=ppp, CN=rootca
        Subject Public Key Info:
```

```
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
                    28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
                    4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
                    57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
                    7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
                    6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
                    c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
                    84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
                    52:db:7b:cd:5d:2b:66:5a:fb
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
        3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
        09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
        4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
        e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
        07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
        fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
        88:a6
```

PKI ドメイン **aaa** のローカル証明書に関する情報を表示します。

<Switch> display pki certificate domain aaa local

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, O=sec, OU=software, CN=abdfdc
        Validity
            Not Before: Jan  7 20:05:44 2011 GMT
            Not After : Jan  7 20:05:44 2012 GMT
        Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
                    52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
                    d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
```

```
                    4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
                    12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
                    46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
                    a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
                    bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
                    8a:f0:ea:02:fd:2d:44:7a:67
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
            Netscape Comment:
                User Certificate of OpenCA Labs
            X509v3 Subject Key Identifier:
                91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
            X509v3 Authority Key Identifier:

keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

            X509v3 Subject Alternative Name:
                email:fips@ccc.com
            X509v3 Issuer Alternative Name:
                email:pki@openca.org
            Authority Information Access:
                CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
                OCSP - URI:http://titan:2560/
                1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://titan/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
        ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
        f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
```

```
95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
de:18:9d:c1
```

関連コマンド

pki domain

pki retrieve-certificate

8.1.15 display pki certificate request-status

Syntax

display pki certificate request-status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display pki certificate request-status コマンドは証明書要求ステータスを表示します。

PKI ドメインを指定しない場合、このコマンドはすべての PKI ドメインの証明書要求ステータスを表示します。

例

すべての PKI ドメインの証明書要求ステータスを表示します。

<Switch> display pki certificate request-status

```
Certificate Request Transaction 1
   Domain name: domain1
   Status: Pending
   Key usage: General
```

```
   Remain polling attempts: 10
   Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
   Domain name: domain2
   Status: Pending
   Key usage: Signature
   Remain polling attempts: 10
   Next polling attempt after : 188 seconds
```

表 8-5 コマンド出力

フィールド	説明
Certificate Request Transaction number	1から始まる証明書要求トランザクション番号です。
Status	保留中のステータスのみを含む、証明書要求ステータスです。
Key usage	証明書の目的: • **General**—署名と暗号化 • **Signature**—署名のみ • **Encryption**—暗号化のみ
Remain polling attempts	証明書要求ステータスのクエリの残りの試行回数です。
Next polling attempt after	次の要求ステータスポーリングまでの残り秒数です。

関連コマンド

certificate request polling

pki domain

pki retrieve-certificate

8.1.16 display pki crl domain

Syntax

display pki crl domain *domain-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

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-6 に示す特殊文字を含めることはできません。

表 8-6 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

説明

display pki crl domain コマンドは PKI ドメインのローカルに保存されている CRL に関する情報を表示します。

このコマンドを使用して、証明書が失効しているかどうかを判別します。

例

PKI ドメイン **aaa** のローカルに保存されている CRL に関する情報を表示します。

<Switch> display pki crl domain aaa

```
Certificate Revocation List (CRL):
       Version 2 (0x1)
       Signature Algorithm: sha1WithRSAEncryption
       Issuer: /C=cn/O=docm/OU=sec/CN=therootca
       Last Update: Apr 28 01:42:13 2011 GMT
       Next Update: NONE
       CRL extensions:
          X509v3 CRL Number:
              6
          X509v3 Authority Key Identifier:

keyid:49:25:DB:07:3A:C4:8A:C2:B5:A0:64:A5:F1:54:93:69:14:51:11:EF

Revoked Certificates:
    Serial Number: CDE626BF7A44A727B25F9CD81475C004
```

```
    Revocation Date: Apr 28 01:37:52 2011 GMT
    CRL entry extensions:
        Invalidity Date:
            Apr 28 01:37:49 2011 GMT
Serial Number: FCADFA81E1F56F43D3F2D3EF7EB56DE5
    Revocation Date: Apr 28 01:33:28 2011 GMT
    CRL entry extensions:
        Invalidity Date:
            Apr 28 01:33:09 2011 GMT
Signature Algorithm: sha1WithRSAEncryption
    57:ac:00:3e:1e:e2:5f:59:62:04:05:9b:c7:61:58:2a:df:a4:
    5c:e5:c0:14:af:c8:e7:de:cf:2a:0a:31:7d:32:da:be:cd:6a:
    36:b5:83:e8:95:06:bd:b4:c0:36:fe:91:7c:77:d9:00:0f:9e:
    99:03:65:9e:0c:9c:16:22:ef:4a:40:ec:59:40:60:53:4a:fc:
    8e:47:57:23:e0:75:0a:a4:1c:0e:2f:3d:e0:b2:87:4d:61:8a:
    4a:cb:cb:37:af:51:bd:53:78:76:a1:16:3d:0b:89:01:91:61:
    52:d0:6f:5c:09:59:15:be:b8:68:65:0c:5d:1b:a1:f8:42:04:
    ba:aa
```

表 8-7 コマンド出力

フィールド	説明
Version	CRLのバージョン番号です。
Signature Algorithm	CAがCRLに署名するために使用する署名アルゴリズムです。
Issuer	CRLを発行したCA名です。
Last Update	最新のCRL更新時刻です。
Next Update	次のCRL更新時刻です。
X509v3 Authority Key Identifier	CRLを発行するCAのX509v3IDです。
keyid	鍵ID このフィールドは、CRLに署名するために使用される鍵ペアを識別します。
Signature Algorithm:	署名アルゴリズムと署名データです。

関連コマンド

pki retrieve-crl

8.1.17 fqdn

Syntax

fqdn *fqdn-name-string*

undo fqdn

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

fqdn-name-string: *hostname@domainname* の形式で FQDN を指定します。設定範囲は 1～255 文字です。大文字と小文字を区別します。

説明

fqdn コマンドはエンティティの FQDN を設定します。

undo fqdn コマンドはデフォルトに戻します。

FQDN は、ネットワーク上の PKI エンティティを一意に識別します。

例

PKI エンティティ **en** の FQDN を **pki.domain-name.com** に設定します。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en] fqdn abc@pki.domain.com

8.1.18 ip

Syntax

ip { *ip-address* | **interface** *interface-type interface-number* }

undo ip

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

ip-address: IPv4 アドレスを指定します。

interface *interface-type interface-number*: タイプと番号によって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、PKI エンティティの IP アドレスとして使用されます。

説明

ip コマンドは PKI エンティティに IP アドレスを割り当てます。

undo ip 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、PKI エンティティに IP アドレスを割り当てるか、エンティティの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、PKI エンティティの IP アドレスとして使用されます。インタフェースを指定する場合は、PKI エンティティが証明書を要求する前に、インタフェースに 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。

例

IP アドレス **192.168.0.2** を PKI エンティティ **en** に割り当てます。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en] ip 192.168.0.2

8.1.19 locality

Syntax

locality *locality-name*

undo locality

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

locality-name: locality を指定します。設定範囲は 1～63 文字です。大文字と小文字を区別します。カンマを含めることはできません。市町村名を地域として設定できます。

説明

locality コマンドは PKI エンティティの locality を設定します。

undo locality コマンドはデフォルトに戻します。

例

PKI エンティティ **en** の locality を **pukras** に設定します。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en] locality pukras

8.1.20 organization

Syntax

organization *org-name*

undo organization

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

org-name: 組織名を指定します。設定範囲は 1～63 文字です。大文字と小文字を区別します。カンマを含めることはできません。

説明

organization コマンドは PKI エンティティの組織名を設定します。

undo organization コマンドはデフォルトに戻します。

例

PKI エンティティ **en** の組織名を **abc** に設定します。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en] organization abc

8.1.21 organization-unit

Syntax

organization-unit *org-unit-name*

undo organization-unit

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

org-unit-name: 組織単位名を指定します。設定範囲は 1～63 文字です。大文字と小文字を区別します。カンマを含めることはできません。

説明

organization-unit コマンドは PKI エンティティの組織単位名を設定します。

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

例

PKI エンティティ **en** の組織ユニット名を **rdtest** に設定します。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en] organization-unit rdtest

8.1.22 pki abort-certificate-request

Syntax

pki abort-certificate-request domain *domain-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-8 に示す特殊文字を含めることはできません。

表 8-8 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

説明

pki abort-certificate-request コマンドは PKI ドメインの証明書要求を中止します。

CA が証明書を発行する前に、証明書要求を中止し、証明書要求のコモンネーム、国コード、FQDN などの一部のパラメータを変更できます。証明書要求ステータスを表示するには、**display pki certificate request-status** コマンドを使用します。

例

PKI ドメイン **1** の証明書要求を中止します。

<Switch> system-view

[Switch] pki abort-certificate-request domain 1

```
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

関連コマンド

display pki certificate request-status

pki request-certificate domain

8.1.23 pki certificate access-control-policy

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-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: ポリシー名を指定します。設定範囲は 1～31 文字です。大文字と小文字を区別しません。

説明

pki certificate access-control-policy コマンドは証明書ベースのアクセスコントロールポリシーを作成してその view に移行するか、既存の証明書ベースのアクセスコントロールポリシーの view に移行します。

undo pki certificate access-control-policy コマンドは証明書ベースのアクセスコントロールポリシーを削除します。

証明書ベースのアクセスコントロールポリシーには、要求元クライアントの証明書の属性に基づいて装置へのアクセスを許可または拒否するアクセスコントロールルールが含まれています。

例

mypolicy という名前の証明書ベースのアクセスコントロールポリシーを作成し、その view に移行します。

<Switch> system-view

[Switch] pki certificate access-control-policy mypolicy

[Switch-pki-cert-acp-mypolicy]

関連コマンド

display pki certificate access-control-policy

8.1.24 pki certificate attribute-group

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group *group-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

group-name: グループ名を指定します。設定範囲は 1～31 文字です。大文字と小文字を区別しません。

説明

pki certificate attribute-group コマンドは証明書属性グループを作成し、その view に移行するか、または既存の証明書属性グループの view に移行します。

undo pki certificate attribute-group コマンドは証明書属性グループを削除します。

証明書属性グループは、**attribute** コマンドを使用して設定される属性ルールのセットです。各属性ルールは、証明書の発行者名、サブジェクト名、または代替サブジェクト名フィールドの属性の一致基準を定義します。

証明書属性グループは、アクセスコントロールルールに関連付ける必要があります。証明書属性グループに属性ルールがない場合、システムはすべての証明書が関連するアクセスコントロールルールに一致すると判断します。

例

mygroup という名前の証明書属性グループを作成し、その view に移行します。

<Switch> system-view

[Switch] pki certificate attribute-group mygroup

[Switch-pki-cert-attribute-group-mygroup]

関連コマンド

attribute

display pki certificate attribute-group

8.1.25 pki delete-certificate

Syntax

pki delete-certificate domain *domain-name* { **ca** | **local** }

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-9 に示す特殊文字を含めることはできません。

表 8-9 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: CA 証明書を指定します。

local: ローカル証明書を指定します。

説明

pki delete-certificate コマンドは PKI ドメインから証明書を削除します。

PKI ドメインの CA 証明書を削除すると、システムは PKI ドメインのローカル証明書、ピア証明書、および CRL も削除します。

PKI ドメイン内の特定のピア証明書を削除するには、次の手順を実行します。

1) **display pki certificate** コマンドを実行して、ピア証明書のシリアル番号を確認します。

例

PKI ドメイン **aaa** の CA 証明書を削除します。

<Switch> system-view

[Switch] pki delete-certificate domain aaa ca

```
Local certificates, peer certificates and CRL will also be deleted while deleting
the CA certificate.
Confirm to delete the CA certificate? [Y/N]:y
```

[Switch]

PKI ドメイン **aaa** のローカル証明書を削除します。

<Switch> system-view

[Switch] pki delete-certificate domain aaa local

[Switch]

関連コマンド

display pki certificate

8.1.26 pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-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

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-10 に示す特殊文字を含めることはできません。

表 8-10 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

説明

pki domain コマンドは PKI ドメインを作成し、その view に移行するか、または既存の PKI ドメインの view に移行します。

undo pki domain コマンドは PKI ドメインを削除します。

PKI ドメインを削除すると、ドメイン内の証明書と CRL も削除されます。

例

aaa という名前の PKI ドメインを作成し、その view に移行します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa]

8.1.27 pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-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

entity-name: PKI エンティティ名を指定します。設定範囲は 1～31 文字です。大文字と小文字を区別しません。

説明

pki entity コマンドは PKI エンティティを作成し、その view に移行するか、または既存の PKI エンティティの view に移行します。

undo pki entity コマンドは PKI エンティティを削除します。

PKI エンティティには、CA が証明書の申請者を識別するために使用できる ID 情報が含まれています。PKI エンティティには、コモンネーム、組織、組織単位、地域、州、国、FQDN、IP アドレスなど、複数の属性を設定できます。この情報は、CA によって発行される証明書のサブジェクトコンテンツとして含まれます。

例

en という名前の PKI エンティティを作成し、その view に移行します。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en]

関連コマンド

pki domain

8.1.28 pki import

Syntax

pki import domain *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-11 に示す特殊文字を含めることはできません。

表 8-11 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

der: PKCS#7 を含む DER 証明書ファイル形式を指定します。

p12: PKCS#12 証明書ファイル形式を指定します。

pem: PEM 証明書ファイル形式を指定します。

ca: CA 証明書を指定します。

local: ローカル証明書を指定します。

peer: ピア証明書を指定します。

filename *filename*: 証明書ファイル名を指定します。大文字、小文字を区別しません。PEM 形式の証明書の場合は、ファイルからインポートする代わりに、証明書の内容を端末にコピーして貼り付けることもできます。

説明

pki import コマンドは PKI ドメインの CA 証明書、ローカル証明書、またはピア証明書をインポートします。

次の状況で証明書をインポートするには、このコマンドを使用します。

- CRL リポジトリが指定されていないか、CA サーバが SCEP をサポートしていません。
- 証明書は、サーバによって生成された鍵ペアとともに 1 つのファイルにパックされます。鍵ペアを含めることができるのは、PKCS12 形式または PEM 形式の証明書ファイルだけです。

証明書をインポートする前に、次の作業を実行します。

- FTP または TFTP を使用して、証明書ファイルを装置のストレージメディアにアップロードします。FTP または TFTP が使用できない場合は、証明書の内容を表示し、装置のファイルにコピーします。この方法でインポートできるのは PEM 形式の証明書だけなので、証明書が PEM 形式であることを確認します。
- ローカル証明書またはピア証明書をインポートするには、正しい CA 証明書チェーンが存在している必要があります。CA 証明書チェーンは、装置に保存することも、ローカル証明書またはピア証明書で伝送することもできます。PKI ドメイン、ローカル証明書、またはピア証明書に CA 証明書チェーンがない場合は、最初に CA 証

明書をインポートする必要があります。ローカル証明書またはピア証明書をインポートするには、CA 証明書チェーンが PKI ドメインに存在するか、ローカル証明書またはピア証明書で伝送されている必要があります。そうでない場合は、最初に取得します。

ローカル証明書またはピア証明書をインポートする場合は、次の手順を実行します。

- ローカル証明書またはピア証明書に CA 証明書チェーンが含まれている場合は、CA 証明書とローカル証明書またはピア証明書を同時にインポートできます。CA 証明書が PKI ドメインにすでに存在する場合は、既存の CA 証明書を上書きするかどうかを確認するプロンプトが表示されます。
- ローカル証明書またはピア証明書に CA 証明書チェーンが含まれていないが、CA 証明書が PKI ドメインにすでに存在する場合は、証明書を直接インポートできます。

次のいずれかの条件が満たされると、CA 証明書を PKI ドメインにインポートできます。

- インポートする CA 証明書がルート CA 証明書であるか、ルート証明書を持つ証明書チェーンが含まれています。
- CA 証明書にはルート証明書のない証明書チェーンが含まれていますが、装置の既存の CA 証明書で完全な証明書チェーンを形成できます。

次のシナリオのプロンプトに従って、CA 管理者に連絡して情報を取得します。

- 次の状況では、証明書のフィンガープリントを確認するプロンプトが表示されます。
  - □ インポートする証明書ファイルにルート証明書が含まれていますが、ルート証明書は装置のどの PKI ドメインにも存在しません。
  - □ **root-certificate fingerprint** コマンドが、証明書ファイルのインポート先となる PKI ドメインで設定されていません。
- インポートするローカル証明書に鍵ペアが含まれている場合は、プライベート鍵の暗号化に使用するチャレンジパスワードを入力するよう求められます。

鍵ペアを含むローカル証明書ファイルをインポートするときに、ドメインを鍵ペアで更新することを選択できます。鍵ペアの目的に応じて、次の条件が適用されます。

- 鍵ペアの目的が一般的な場合、装置は鍵ペアを使用して、次の順序で見つかったローカル鍵ペアを置き換えます。

a. 汎用鍵ペア。

b. 鍵ペアのサイン入り。

c. 暗号化鍵ペア。

- 鍵ペアの目的がシグニチャである場合、装置は鍵ペアを使用して、次の順序で見つかったローカル鍵ペアを置き換えます。

a. 汎用鍵ペア。

b. 鍵ペアのサイン入り。

- 鍵ペアの目的が暗号化である場合、装置はドメイン内で暗号化鍵ペアを検索します。

一致する鍵ペアが見つかった場合は、装置の既存の鍵ペアを上書きするかどうかを確認するメッセージが表示されます。一致するものが見つからない場合、装置は鍵ペア名 (デ

フォルトは PKI ドメイン名) の入力を要求します。次に、鍵アルゴリズムと証明書ファイルに定義された目的に従って鍵ペアを生成します。

インポート操作によって、正しい鍵ペアが自動的に更新または生成されます。インポート操作を実行するときは、データが失われないように、必ず設定ファイルを保存してください。

例

CA 証明書ファイル **rootca_pem.cer** を PEM 形式で PKI ドメイン **aaa** にインポートします。証明書ファイルにはルート証明書が含まれています。

<Switch> system-view

[Switch] pki import domain aaa pem ca filename rootca_pem.cer

```
The trusted CA's finger print is:
   MD5  fingerprint:FFFF 3EFF FFFF 37FF FFFF 137B FFFF 7535
   SHA1 fingerprint:FFFF FF7F FF2B FFFF 7618 FF4C FFFF 0A7D FFFF FF69
Is the finger print correct?(Y/N):y
```

[Switch]

CA 証明書ファイル **aca_pem.cer** を PEM 形式で PKI ドメイン bbb にインポートします。証明書ファイルにルート証明書が含まれていません。

<Switch> system-view

[Switch] pki import domain bbb pem ca filename aca_pem.cer

[Switch]

PKCS12 形式のローカル証明書ファイル **local-ca.p12** を PKI ドメイン **bbb** にインポートします。証明書ファイルに鍵ペアが含まれています。

<Switch> system-view

[Switch] pki import domain bbb p12 local filename local-ca.p12

```
Please input challenge password:
******
```

[Switch]

証明書の内容をコピーして貼り付け、PEM 形式のローカル証明書を PKI ドメイン **bbb** にインポートします。証明書には、鍵ペアと CA 証明書チェーンが含まれています。

<Switch> system-view

[Switch] pki import domain bbb pem local

```
Enter PEM-formatted certificate.
End with a Ctrl+c on a line by itself.
Bag Attributes
localKeyID: 01 00 00 00
friendlyName: {F7619D96-3AC2-40D4-B6F3-4EAB73DEED73}
Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
Key Attributes
```

```
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,8DCE37F0A61A4B8C

k9C3KHY5S3EtnF5iQymvHYYrVFy5ZdjSasU5y4XFubjdcvmpFHQteMjD0GKX6+xO
kuKbvpyCnWsPVg56sL/PDRyrRmqLmtUV3bpyQsFXgnc7p+Snj3CG2Ciow9XApybW
Ec1TDCD75yuQckpVQdhguTvoPQXf9zHmiGu5jLkySp2k7ec/Mc97Ef+qqpfnHpQp
GDmMqnFpp59ZzB21OGlbGzlPcsjoT+EGpZg6B1KrPiCyFim95L9dWVwX9sk+U1s2
+8wqac8jETwwM0UZ1NGJ50JJz1QYIzMbcrw+S5WlPxACTIz1cldlBlb1kpc+7mcX
4W+MxFzsL88IJ99T72eu4iUNsy26g0BZMAcc1sJA3A4w9RNhfs9hSG43S3hAh5li
JPp720LfYBlkQHn/MgMCZASWDJ5G0eSXQt9QymHAth4BiT9v7zetnQqf4q8plfd/
Xqd9zEFlBPpoJFtJqXwxHUCKgw6kJeC4CxHvi9ZCJU/upg9IpiguFPoaDOPia+Pm
GbRqSyy55clVde5GOccGN1DZ94DW7AypazgLpBbrkIYAdjFPRmq+zMOdyqsGMTNj
jnheI5l784pNOAKuGi0i/uXmRRcfoMh6qAnK6YZGS7rOLC9CfPmy8fgY+/Sl9d9x
Q00ruO1psxzh9c2YfuaiXFIx0auKl6o5+ZZYn7Rg/xy2Y0awVP+dO925GoAcHO40
cCl6jA/HsGAU9HkpwKHL35lmBDRLEzQeBFcaGwSm1JvRfE4tkJM7+Uz2QHJOfP10
0VLqMgxMlpk3TvBWgzHGJDe7TdzFCDPMPhod8pi4P8gGXmQd01PbyQ==
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/CN=sldsslserver
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIICjzCCAfigAwIBAgIRAJoDN+shVrofVHbk11SlqfcwDQYJKoZIhvcNAQEFBQAw
NzELMAkGA1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYD
VQQDEwNzc2wwHhcNMTAxMDE1MDEyMzA2WhcNMTIwNzI2MDYzMDU0WjAXMRUwEwYD
VQQDEwxzbGRzc2xzZXJ2ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMLP
N3aTKV7NDndIOk0PpiikYPgxVih/geMXR3iYaANbcvRX07/FMDINWHJnBAZhCDvp
rFO552loGiPyl0wmFMK12TSL7sHvrxr0OdrFrqtWlbW+DsNGNcFSKZy3RvIngC2k
ZZqBeFPUytP185JUhbOrVaUDlisZi6NNshcIjd2BAgMBAAGjgbowgbcwHwYDVR0j
BBgwFoAUmoMpEynZYoPLQdR1LlKhZjg8kBEwDgYDVR0PAQH/BAQDAgP4MBEGCWCG
SAGG+EIBAQQEAwIGQDASBgNVHREECzAJggdoM2MuY29tMB0GA1UdDgQWBBQ8dpWb
3cJ/X5iDt8eg+JkeS9cvJjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vczAzMTMw
LmgzYy5odWF3ZWktM2NvbS5jb206NDQ3L3NzbC5jcmwwDQYJKoZIhvcNAQEFBQAD
gYEAYS15x0kW474lu4twNzEy5dPjMSwtwfm/UK01S8GQjGV5tl9ZNiTHFGNEFx7k
zxBp/JPpcFM8hapAfrVHdQ/wstq0pVDdBkrVF6XKIBks6XgCvRl32gcaQt9yrQd9
5RbWdetuBljudjFj25airYO2u7pLeVmdWWx3WVvZBzOo8KU=
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/C=cn/O=ccc/OU=sec/CN=ssl
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
```

```
MIIB7DCCAVUCEG+jJTPxxiE67pl2ff0SnOMwDQYJKoZIhvcNAQEFBQAwNzELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYDVQQDEwNz
c2wwHhcNMDkwNzMxMDY0ODQ2WhcNMTIwNzI5MDYyODU4WjA3MQswCQYDVQQGEwJj
bjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNzZWMxDDAKBgNVBAMTA3NzbDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8QSMetQ70GONiFh7iJkvGQ8nC15zCF1
cqC/RcJhE/88LkKyQcu9j+Tz8Bk9Qj2UPaZdrk8fOrgtBsa7lZ+UO3j3l30q84l+
HjWq8yxVLRQahU3gqJze6pGR2l0s76u6GRyCX/zizGrHKqYlNnxK44NyRZx2klQ2
tKQAfpXCPIkCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBWsaMgRbBMtYNrrYCMjY6g
c7PBjvajVOKNUMxaDalePmXfKCxl91+PKM7+i8I/zLcoQO+sHbva26a2/C4sNvoJ
2QZs6GtAOahP6CDqXC5VuNBU6eTKNKjL+mf6uuDeMxrlDNha0iymdrXXVIp5cuIu
fl7xgArs8Ks6aXDXM1o4DQ==
-----END CERTIFICATE-----


Please input the password:********
Local certificate already exist, confirm to overwrite it? [Y/N]:y
The PKI domain already has a CA certificate. If it is overwritten, local
certificates, peer certificates and CRL of this domain will also be deleted.
Overwrite it? [Y/N]:y
The system is going to save the key pair. You must specify a key pair name, which
is a case-insensitive string of 1 to 64 characters. Valid characters include a
to z, A to Z, 0 to 9, and hyphens (-).
Please enter the key pair name [default name: bbb]:

The key pair already exists.
Please enter the key pair name:
import-key
```

関連コマンド

display pki certificate

public-key dsa

public-key ecdsa

public-key rsa

8.1.29 pki request-certificate

Syntax

pki request-certificate domain *domain-name* [**password** *password*] [**pkcs10** [**filename** *filename*]]

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-12 に示す特殊文字を含めることはできません。

表 8-12 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

password *password*: 証明書失効のパスワードを設定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。パスワードは証明書要求に含まれており、証明書が失効している場合は入力する必要があります。

pkcs10: BASE64 でエンコードされた PKCS#10 証明書要求情報を表示します。この情報は、電話、ディスク、電子メールなどの帯域外の手段で証明書を要求するために使用できます。

filename *filename*: 証明書要求を PKCS#10 形式で保存するためのローカルファイルを指定します。*filename* は、大文字、小文字を区別しません。

説明

pki request-certificate コマンドはローカル証明書要求を送信するか、PKCS#10 形式の証明書要求を生成します。

SCEP が失敗した場合は、次のいずれかのタスクを実行できます。

- **pkcs10** キーワードを使用して、BASE64 でエンコードされた要求情報を出力します。
- **pkcs10 filename** *filename* オプションを使用して、要求情報をローカルファイルに保存し、そのファイルを帯域外の手段で CA に転送します。ファイル名には絶対パスを含めることができます。指定したパスが存在する場合、要求情報は保存できません。

このコマンドは設定ファイルには保存されません。

例

証明書要求に関する情報を PKCS#10 形式で表示します。

<Switch> system-view

[Switch] pki request-certificate domain aaa pkcs10

```
*** Request for general certificate ***
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nmdcu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END NEW CERTIFICATE REQUEST-----
```

ローカル証明書を要求します。

[Switch] pki request-certificate domain openca

```
Start to request general certificate ...
...
Request certificate of domain openca successfully
```

関連コマンド

display pki certificate

8.1.30 pki retrieve-certificate

Syntax

pki retrieve-certificate domain *domain-name* { **ca** | **local** }

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-13 に示す特殊文字を含めることはできません。

表 8-13 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: CA 証明書を指定します。

local: ローカル証明書を指定します。

説明

pki retrieve-certificate コマンドは証明書配布サーバから証明書を取得します。

オンラインモードの場合:

- CA 証明書は SCEP プロトコルを介して取得できます。CA 証明書がすでにローカルに存在する場合は、CA 証明書を再度取得しないでください。新しい CA 証明書を取得するには、**pki delete-certificate** コマンドを使用して CA 証明書とローカル証明書を削除してから、CA 証明書を再度取得します。
- PKI ドメインにすでにローカル証明書がある場合でも、取得操作を実行でき、取得したローカル証明書またはピア証明書が既存の証明書を上書きします。RSA を使用する場合、PKI ドメインは、署名用と暗号化用の 2 つのローカル証明書を持つことができます。異なる目的の証明書は互いに上書きされません。

取得した CA 証明書、ローカル証明書、およびピア証明書は、ローカルに保存される前に自動的に検証されます。検証に失敗した場合は、保存されません。

このコマンドは設定ファイルには保存されません。

例

証明書配布サーバから CA 証明書を取得します。(この操作では、ユーザがルート CA 証明書のフィンガープリントを確認する必要があります)

<Switch> system-view

[Switch] pki retrieve-certificate domain aaa ca

```
The trusted CA's finger print is:
   MD5  fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
   SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
```

証明書配布サーバからローカル証明書を取得します。

<Switch> system-view
[Switch] pki retrieve-certificate domain aaa local

証明書配布サーバからピアエンティティ **en1** の証明書を取得します。

<Switch> system-view

[Switch] pki retrieve-certificate domain aaa peer en1

関連コマンド

display pki certificate

pki delete-certificate

8.1.31 pki retrieve-crl

Syntax

pki retrieve-crl domain *domain-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-14 に示す特殊文字を含めることはできません。

表 8-14 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

説明

pki retrieve-crl コマンドは CRL を取得し、ローカルに保存します。

CRL は、PKI ドメイン内のローカル証明書およびピア証明書の有効性を確認するために使用されます。CRL を取得するには、PKI ドメインに正しい CA 証明書が必要です。

CRL リポジトリの URL は、**crl url** コマンドを使用して指定します。

装置は、HTTP または SCEP プロトコルを介して CRL リポジトリから CRL を取得できます。どのプロトコルが使用されるかは、PKI ドメインの CRL リポジトリの設定によって異なります。

- CRL リポジトリの指定された URL が HTTP 形式の場合、装置は HTTP プロトコルを介して CRL を取得します。
- PKI ドメインが CRL リポジトリで設定されていない場合、装置はローカル証明書を検索し、次に CRL リポジトリの CA 証明書を検索します。CRL リポジトリが見つかった場合、装置は CRL リポジトリから CRL を取得します。CRL リポジトリが見つからない場合、装置は SCEP プロトコルを介して CRL を取得します。

例

CRL リポジトリから CRL を取得します。

<Switch> system-view

[Switch] pki retrieve-crl domain aaa

関連コマンド

crl url

8.1.32 pki storage

Syntax

pki storage { **certificates** | **crls** } *dir-path*

undo pki storage { **certificates** | **crls** }

デフォルト

証明書と CRL は、装置のストレージメディアの **PKI** ディレクトリに保存されます。**PKI** ディレクトリは、証明書が初めて正常に要求、取得、またはインポートされたときに自動的に作成されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

certificates: 証明書のストレージパスを指定します。

crls: CRL のストレージパスを指定します。

dir-path: ストレージパスを指定します。大文字と小文字を区別します。スラッシュ（/）で開始したり、2 つのドットとスラッシュ（../）を含めたりすることはできません。*dir-path* は絶対パスまたは相対パスを指定し、そのパスが存在している必要があります。

説明

pki storage コマンドは証明書または CRL のストレージパスを指定します。

undo pki storage コマンドはデフォルトに戻します。

指定されたストレージパスは、マスタ装置にある必要があります。

指定するパスが存在しない場合は、まず **mkdir** コマンドでパスを作成します。

証明書ファイルには、ファイル拡張子.cer または.p12 が使用されます。CRL ファイルには.crl ファイル拡張子が使用されます。証明書または CRL のストレージパスを変更すると、元のパスにある証明書ファイルと CRL ファイルが新しいパスに移動されます。

例

証明書のストレージパスとして **flash:/pki-new** を指定します。

<Switch> system-view

[Switch] pki storage certificates flash:/pki-new

CRL のストレージパスとして **pki-new** を指定します。

<Switch> system-view

[Switch] pki storage crls pki-new

8.1.33 pki validate-certificate

Syntax

pki validate-certificate domain *domain-name* { **ca** | **local** }

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名には、表 8-15 に示す特殊文字を含めることはできません。

表 8-15 特殊文字

文字名	記号	文字名	記号
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: CA 証明書を指定します。

local: ローカル証明書を指定します。

説明

pki validate-certificate コマンドは証明書の有効性を確認します。

通常、証明書を要求、取得、インポートするとき、またはアプリケーションが PKI を使用するときに、証明書は自動的に検証されます。

また、このコマンドを使用して、次の側面で証明書を手動で確認することもできます。

- 証明書が信頼できる CA によって発行されているかどうか。
- 証明書の有効期限が切れているかどうか。
- 証明書が失効しているかどうか。このチェックは、CRL チェックが有効な場合にのみ実行されます。

CRL チェックが有効な場合:

- ローカル証明書を確認するために、PKI ドメインに CRL がない場合、装置はローカルに保存された CRL を検索します。正しい CRL が見つかった場合、装置は CRL を PKI ドメインにロードします。正しい CRL がローカルに見つからない場合、装置は CA サーバから正しい CRL を取得し、それをローカルに保存します。
- CA 証明書を確認するために、現在の CA からルート CA までの CA 証明書チェーンに対して CRL チェックが実行されます。

例

PKI ドメイン **aaa** の CA 証明書の有効性を確認します。

<Switch> system-view

[Switch] pki validate-certificate domain aaa ca

```
Verifying certificate......
       Serial Number:
          f6:3c:15:31:fe:bb:ec:94:dc:3d:b9:3a:d9:07:70:e5
       Issuer:
```

```
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=abc
            OU=test
            CN=aca

Verify result: OK
Verifying certificate......
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca

Verify result: OK
```

PKI ドメイン **aaa** のローカル証明書を確認します。

<Switch> system-view

[Switch] pki validate-certificate domain aaa local

```
Verifying certificate......
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Issuer:
            C=CN
            O=sec
            OU=software
            CN=bca
        Subject:
            O=OpenCA Labs
            OU=Users
            CN=fips fips-sec
```

```
Verify result: OK
```

関連コマンド

crl check enable

pki domain

8.1.34 public-key dsa

Syntax

public-key dsa name *key-name* [**length** *key-length*]

undo public-key

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: 鍵ペア名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しません。鍵ペア名には、文字、数字、およびハイフン（-）のみを含めることができます。

length *key-length*: 鍵長をビット単位で指定します。設定範囲は 512～2048 で、デフォルトは 1024 です。鍵が長いほどセキュリティは高くなりますが、公開鍵の計算時間が長くなります。

説明

public-key dsa コマンドは証明書要求の DSA 鍵ペアを指定します。

undo public-key コマンドはデフォルトに戻します。

このコマンドでは、存在しない鍵ペアを指定できます。鍵ペアは、次のいずれかの方法で取得できます。

- **public-key local create** コマンドを使用して、鍵ペアを生成します。
- デジタル署名認証を使用する IKE のようなアプリケーションは、装置をトリガにして鍵ペアを生成します。
- 鍵ペアを含む証明書をインポートするには、**pki import** コマンドを使用します。

PKI ドメインは、1 つのタイプの暗号アルゴリズム(DSA、ECDSA、または RSA)のみを使用する鍵ペアを持つことができます。

PKI ドメインの DSA 鍵ペアを複数回設定すると、最新の設定が有効になります。

length *key-length* オプションは、存在しない鍵ペアを指定した場合にのみ有効です。装置は、証明書要求を送信する前に、指定された名前と長さを使用して鍵ペアを自動的に作成します。指定された鍵ペアがすでに存在するか、インポートされた証明書にすでに含まれている場合、**length** *key-length* オプションは無視されます。

例

証明書要求に 2048 ビット DSA 鍵ペア **abc** を指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] public-key dsa name abc length 2048

関連コマンド

pki import

public-key local create

8.1.35 public-key ecdsa

Syntax

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: 鍵ペア名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しません。鍵ペア名には、文字、数字、およびハイフン（-）のみを含めることができます。

secp192r1: secp192r1 カーブを使用して鍵ペアを生成します。デフォルトでは secp192r1 カーブを使用します。

secp256r1: secp256r1 カーブを使用して鍵ペアを生成します。

secp384r1: secp384r1 カーブを使用して鍵ペアを生成します。

secp521r1: secp521r1 カーブを使用して鍵ペアを生成します。

説明

public-key ecdsa コマンドは証明書要求のための ECDSA 鍵ペアを指定します。

undo public-key コマンドはデフォルトに戻します。

このコマンドでは、存在しない鍵ペアを指定できます。

鍵ペアは、次のいずれかの方法で取得できます。

- **public-key local create** コマンドを使用して、鍵ペアを生成します。
- デジタル署名認証を使用する IKE のようなアプリケーションは、装置をトリガにして鍵ペアを生成します。
- 鍵ペアを含む証明書をインポートするには、**pki import** コマンドを使用します。

PKI ドメインは、1 つのタイプの暗号アルゴリズム(DSA、ECDSA、または RSA)のみを使用する鍵ペアを持つことができます。

PKI ドメインの ECDSA 鍵ペアを複数回設定すると、最新の設定が有効になります。

指定した楕円曲線は、存在しない鍵ペアを指定した場合にのみ有効になります。装置は、証明書要求を送信する前に、指定された名前と曲線を使用して鍵ペアを自動的に作成します。指定された鍵ペアがすでに存在するか、インポートされた証明書にすでに含まれている場合、curve パラメータは無視されます。

例

証明書の要求には、384 ビット ECDSA 鍵ペア **abc** を指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] public-key ecdsa name abc secp384r1

関連コマンド

pki import

public-key local create

8.1.36 public-key rsa

Syntax

public-key rsa { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }

undo public-key

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

encryption: 暗号化の鍵ペアを指定します。

name *encryption-key-name*: 鍵ペア名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しません。鍵ペア名には、文字、数字、およびハイフン（-）のみを含めることができます。

signature: 署名用の鍵ペアを指定します。

name *signature-key-name*: 鍵ペア名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しません。鍵ペア名には、文字、数字、およびハイフン（-）のみを含めることができます。

general: 署名と暗号化の両方に鍵ペアを指定します。

name *key-name*: 鍵ペア名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しません。鍵ペア名には、文字、数字、およびハイフン（-）のみを含めることができます。

length *key-length*: 鍵長をビット単位で指定します。設定範囲は 512～2048 で、デフォルトは 1024 です。鍵が長いほどセキュリティは高くなりますが、公開鍵の計算時間が長くなります。

説明

public-key rsa コマンドは証明書要求のための RSA 鍵ペアを指定します。

undo public-key コマンドはデフォルトに戻します。

このコマンドでは、存在しない鍵ペアを指定できます。鍵ペアは、次のいずれかの方法で取得できます。

- **public-key local create** コマンドを使用して、鍵ペアを生成します。
- デジタル署名認証を使用する IKE のようなアプリケーションは、装置をトリガにして鍵ペアを生成します。
- 鍵ペアを含む証明書をインポートするには、**pki import** コマンドを使用します。

PKI ドメインは、1 つのタイプの暗号アルゴリズム(DSA、ECDSA、または RSA)のみを使用する鍵ペアを持つことができます。

PKI ドメインは、目的の異なる 2 つの RSA 鍵ペアを持つことができます。1 つは署名鍵ペアで、もう 1 つは暗号化鍵ペアです。RSA 署名鍵ペアまたは RSA 暗号化鍵ペアを複数回設定すると、最新の設定が有効になります。RSA 署名鍵ペアと暗号化鍵ペアは互いに上書きしません。

署名鍵ペアと暗号化鍵ペアを別々に指定する場合、鍵長が異なる場合があります。

length *key-length* オプションは、存在しない鍵ペアを指定した場合にのみ有効です。装置は、証明書要求を送信する前に、指定された名前と長さを使用して鍵ペアを自動的に作成します。指定された鍵ペアがすでに存在するか、インポートされた証明書にすでに含まれている場合、**length** *key-length* オプションは無視されます。

例

証明書要求には、2048 ビットの汎用 RSA 鍵ペア **abc** を指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] public-key rsa general name abc length 2048

証明書要求には、次の RSA 鍵ペアを指定します。

- 2048 ビット RSA 暗号化鍵ペア **rsa1**
- 2048 ビット RSA 署名鍵ペア **sig1**

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048

[Switch-pki-domain-aaa] public-key rsa signature name sig1 length 2048

関連コマンド

pki import

public-key local create

8.1.37 root-certificate fingerprint

Syntax

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

デフォルト

設定なし

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

md5: MD5 フィンガープリントを設定します。

sha1: SHA1 フィンガープリントを設定します。

string: 16 進表記でフィンガープリントを設定します。**MD5** キーワードを指定した場合、フィンガープリントは 32 文字の文字列になります。**SHA1** キーワードを指定すると、フィンガープリントは 40 文字の文字列になります。

説明

root-certificate fingerprint コマンドはルート CA 証明書を確認するためのフィンガープリントを設定します。

undo root-certificate fingerprint コマンドはデフォルトに戻します。

CA 証明書を持たない PKI ドメインの証明書要求モードを auto に設定する場合は、ルート CA 証明書検証用のフィンガープリントを設定する必要があります。アプリケーション（IKE など）が装置をトリガしてローカル証明書を要求すると、装置は自動的に次の操作を実行します。

1) CA サーバから CA 証明書を取得します。
2) 次のいずれかの条件が存在する場合、ルート CA 証明書に含まれるフィンガープリントを PKI ドメインに設定されたフィンガープリントと比較します。
   - 取得した CA 証明書はルート証明書です。
   - 取得した CA 証明書は証明書チェーンであり、装置に存在しないルート証明書が含まれています。

   2 つのフィンガープリントが一致しない場合、または PKI ドメインにフィンガープリントが設定されていない場合、装置は CA 証明書を拒否し、ローカル証明書要求は失敗します。

このコマンドで設定されたフィンガープリントは、装置が次の操作を実行するときに、ルート CA 証明書の検証にも使用されます。

- **pki import** コマンドで要求された CA 証明書をインポートします。
- **pki retrieve-certificate** コマンドで要求された CA 証明書を取得します。

次のいずれかの条件が存在する場合、装置はルート CA 証明書に含まれるフィンガープリントを PKI ドメインに設定されたフィンガープリントと比較します。

- インポートまたは取得する CA 証明書は、装置に存在しないルート証明書です。
- インポートまたは取得する CA 証明書が証明書チェーンであり、装置に存在しないルート証明書が含まれています。

2 つのフィンガープリントが一致しない場合、装置は CA 証明書を拒否します。PKI ドメインにフィンガープリントが設定されていない場合、装置はルート CA 証明書のフィンガープリントを手動で確認するよう求めます。

例

ルート CA 証明書を検証するための MD5 フィンガープリントを指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E

ルート CA 証明書を検証する SHA1 フィンガープリントを指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] root-certificate fingerprint sha1 D1526110AAD7527FB093ED7FC037B0B3CDDDAD93

関連コマンド

certificate request mode

pki import

pki retrieve-certificate

8.1.38 state

Syntax

state *state-name*

undo state

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

state-name: 州または県を名前で指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。カンマを含めることはできません。

説明

state コマンドは PKI エンティティの州または県名を設定します。

undo state コマンドはデフォルトに戻します。

例

PKI エンティティ **en** の状態名を **countryA** に設定します。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en] state countryA

目次

このセクションのページは **8-x-x** です。

9 章 SSH.....9-1
9.1 SSH サーバ設定コマンド.....9-1
9.1.1 display ssh server.....9-1
9.1.2 display ssh user-information.....9-3
9.1.3 free ssh.....9-4
9.1.4 scp server enable.....9-6
9.1.5 sftp server enable.....9-6
9.1.6 sftp server idle-timeout.....9-7
9.1.7 ssh server acl.....9-8
9.1.8 ssh server authentication-retries.....9-9
9.1.9 ssh server authentication-timeout.....9-10
9.1.10 ssh server compatible-ssh1x enable.....9-11
9.1.11 ssh server dscp.....9-12
9.1.12 ssh server enable.....9-12
9.1.13 ssh server ipv6 acl.....9-13
9.1.14 ssh server ipv6 dscp.....9-14
9.1.15 ssh server rekey-interval.....9-15
9.1.16 ssh user.....9-16
9.2 SSH クライアント設定コマンド.....9-19
9.2.1 bye.....9-19
9.2.2 cd.....9-20
9.2.3 cdup.....9-20
9.2.4 delete.....9-21
9.2.5 dir.....9-22
9.2.6 display sftp client source.....9-23
9.2.7 display ssh client source.....9-23
9.2.8 exit.....9-24
9.2.9 get.....9-25
9.2.10 help.....9-25
9.2.11 ls.....9-26
9.2.12 mkdir.....9-27
9.2.13 put.....9-28
9.2.14 pwd.....9-29
9.2.15 quit.....9-29
9.2.16 remove.....9-30
9.2.17 rename.....9-30

9.2.18 rmdir....9-31
9.2.19 scp....9-31
9.2.20 scp ipv6....9-34
9.2.21 sftp....9-37
9.2.22 sftp client ipv6 source....9-39
9.2.23 sftp client source....9-40
9.2.24 sftp ipv6....9-41
9.2.25 ssh client ipv6 source....9-43
9.2.26 ssh client source....9-44
9.2.27 ssh2....9-45
9.2.28 ssh2 ipv6....9-48
9.3 SSH2 設定コマンド....9-50
9.3.1 display ssh2 algorithm....9-50
9.3.2 ssh2 algorithm cipher....9-52
9.3.3 ssh2 algorithm key-exchange....9-53
9.3.4 ssh2 algorithm mac....9-54
9.3.5 ssh2 algorithm public-key....9-55

9章 SSH

9.1 SSHサーバ設定コマンド

9.1.1 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指定します。

status: SSH サーバの状態を指定します。

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 9-1 コマンド出力

フィールド	説明
Stelnet server	Stelnetサーバ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	RSAサーバ鍵ペアの最小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。
SCP server	SCPサーバが有効かどうかを示します。
SSH Server PKI domain name	SSHサーバに指定された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 9-2 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。

9.1.2 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 9-3 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、**null**と表示されます。
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利用できる場合、それらは(|) で区切られます。

関連コマンド

ssh user

9.1.3 free ssh

Syntax

free ssh { **user-ip** { *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

View

User view

定義済みユーザロール

network-admin

パラメータ

user-ip: 接続を解除する SSH セッションのユーザ IP アドレスを指定します。

ip-address: 接続を解除する SSH セッションのユーザ IPv4 アドレスを指定します。

ipv6 *ipv6-address:* 接続を解除する SSH セッションのユーザ IPv6 アドレスを指定します。

port *port-number*: 接続を解除する SSH セッションの送信元ポートを指定します。設定範囲は 1～65535 です。送信元ポートを指定しない場合、指定された IP アドレスを使用してすべての SSH セッションを切断します。

user-pid *pid-number*: 接続を解除する SSH セッションのユーザプロセス ID を指定します。設定範囲は 1~2147483647 です。SSH セッションのユーザプロセス ID を表示するには、**display ssh server session** コマンドを使用します。

username *username*: 接続を解除する SSH セッションのユーザ名を指定します。SSH セッションのユーザ名を表示するには、**display ssh server session** コマンドを使用します。

説明

free ssh コマンドは SSH セッションを切断します。

例

ユーザ IPv4 アドレス 192.168.15.45 の SSH セッションを切断します。

<Switch> free ssh user-ip 192.168.15.45

```
Releasing SSH connection. Continue? [Y/N]:y
```

ユーザ IPv6 アドレス 2000 :: 11 を持つ SSH セッションを切断します。

<Switch> free ssh user-ip ipv6 2000::11

```
Releasing SSH connection. Continue? [Y/N]:y
```

ユーザプロセス ID417 の SSH セッションを切断します。

<Switch> free ssh user-pid 417

```
Releasing SSH connection. Continue? [Y/N]:y
```

ユーザ名 **sshuser** で SSH セッションを切断します。

<Switch> free ssh username sshuser

```
Releasing SSH connection. Continue? [Y/N]:y
```

関連コマンド

display ssh server session

9.1.4 scp server enable

Syntax

scp server enable

undo scp server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

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

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

例

SCP サーバを有効にします。

<Switch> system-view

[Switch] scp server enable

関連コマンド

display ssh server

9.1.5 sftp server enable

Syntax

sftp server enable

undo sftp server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

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

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

例

SFTP サーバを有効にします。

<Switch> system-view

[Switch] sftp server enable

関連コマンド

display ssh server

9.1.6 sftp server idle-timeout

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

デフォルト

10 分

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value: タイムアウトタイマを指定します。設定範囲は 1～35791 分です。

説明

sftp server idle-timeout コマンドは SFTP サーバの SFTP 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

9.1.7 ssh server acl

Syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced-acl-number: 拡張 ACL 番号を指定します。設定範囲は 3000～3999 です。

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

mac *mac-acl-number*: レイヤ 2ACL を指定します。設定範囲は 4000～4999 です。

説明

ssh server acl コマンドはサーバへの IPv4 SSH 接続を制御するための ACL を指定します。

undo ssh server acl コマンドはデフォルトに戻します。

ACL を指定して IPv4 SSH ユーザ接続の要求パケットをフィルタします。ACL が許可した IPv4 SSH ユーザのみがサーバへの SSH 接続を開始できます。指定した ACL が存在しないか、ルールが含まれていない場合は、すべての IPv4SSH クライアントが装置にアクセスできます。

ACL 設定後に開始される SSH 接続においてのみ、ALC が有効です。

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

ACL 2001 を設定し、ユーザ 1.1.1.1 のみサーバにアクセスできるようにします。

<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

9.1.8 ssh server authentication-retries

Syntax

ssh server authentication-retries *retries*

undo ssh server authentication-retries

デフォルト

3

View

System view

定義済みユーザロール

network-admin

パラメータ

retries: SSH ユーザの認証を試行する最大数を指定します。設定範囲は 1～5 です。

説明

ssh server authentication-retries コマンドは SSH ユーザの認証を試行する最大数を指定します。

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

偽のユーザ名とパスワードの攻撃を防ぐため、最大数を設定することができます。

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。

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。

- どの認証でも、認証の試行は公開鍵またはパスワード認証プロセスです。
- 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。

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

9.1.9 ssh server authentication-timeout

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value: 認証タイムアウトタイマを指定します。設定範囲は 1～120 秒です。

説明

ssh server authentication-timeout コマンドは SSH サーバで SSH ユーザ認証のタイムアウトタイマを設定します。

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

タイムアウトタイマが終了したとき、ユーザが認証を終了しない場合、接続は確立することができません。

TCP 接続でいたずらに占有しないように、タイムアウトタイマの値を小さくしてください。

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

9.1.10 ssh server compatible-ssh1x enable

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [**enable**]

デフォルト

SSH サーバは、SSH1 クライアントをサポートしません。

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 [**enable**]コマンドはデフォルトに戻します。

このコマンドの undo 形式は、**enable** キーワードを指定したかどうかにかかわらず、デフォルト設定を復元します。

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

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

9.1.11 ssh server dscp

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 送信 IPv4 パケットの DSCP 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 DSCP 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。

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

9.1.12 ssh server enable

Syntax

ssh server enable

undo ssh server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

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

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

例

SSH 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

9.1.13 ssh server ipv6 acl

Syntax

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }

undo ssh server ipv6 acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。

advanced-acl-number: 拡張 ACL を指定します。設定範囲は 3000～3999 です。

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

mac *mac-acl-number*: レイヤ 2 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 ユーザ接続を制御するために ACL を指定します。

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

ACL を指定して IPv6 SSH ユーザ接続の要求パケットをフィルタします。ACL が許可した IPv6 SSH ユーザのみがサーバへの SSH 接続を開始できます。指定された ACL が存在しないか、ルールを含まない場合、すべての IPv6 SSH クライアントが装置にアクセスできます。

ACL 設定後に開始される SSH 接続においてのみ、ALC は有効です。

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

ACL 2001 を設定し、サブネット 1::1/64 のユーザのみサーバにアクセスできるよう許可します。

<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

9.1.14 ssh server ipv6 dscp

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 送信 IPv6 パケットの DSCP 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 DSCP 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。

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 DSCP を 30 に設定します。

<Switch> system-view

[Switch] ssh server ipv6 dscp 30

9.1.15 ssh server rekey-interval

Syntax

ssh server rekey-interval *interval*

undo ssh server rekey-interval

デフォルト

アップデート間隔の値は 0 時間です。RSA サーバ鍵ペアのアップデートを行いません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: サーバ鍵ペアのアップデート最小間隔を指定します。設定範囲は 1～24 時間です。

説明

ssh server rekey-interval コマンドはサーバ鍵ペアのアップデート最小間隔を設定します。

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 クライアントにのみ適用されます。

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

9.1.16 ssh user

Syntax

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign publickey** *keyname*&<1-6>] }

undo ssh user *username*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

username: SSH ユーザ名を指定します。設定範囲は 1～80 文字です。大文字、小文字を区別します。ユーザ名には、**a**、**al**、または **all** は使用できません。また、ユーザ名に縦棒(|)、コロン(:)、アスタリスク(*)、疑問符(?)または山かっこ(<>)を使用できます。アットマーク(@)、スラッシュ(/)、バックスラッシュ(\)は、*pureusername*@*domain*、*pureusername/domain*、pureusername *domain* の形式でユーザ名に ISP ドメイン名を付加する場合にのみ使用できます。SCP ユーザのユーザ名にハイフン(-)を含めない。そうしないと、そのユーザ名を使用した SCP ログインは失敗します。

service-type: SSH ユーザのサービスタイプを指定します。

- **all**: Stelnet、SFTP、SCP、および NETCONF を指定します。
- **scp**: scp のサービスタイプを指定します。
- **sftp**: SFTP のサービスタイプを指定します。
- **stelnet**: Stelnet のサービスタイプを指定します。
- **netconf**: NETCONF のサービスタイプを指定します。

authentication-type: SSH ユーザの認証方法を指定します。

- **password**: パスワード認証を指定します。認証方式は容易で暗号時間が早くなりますが、セキュリティ強度は脆弱です。ユーザ認証、許可、アカウンティングを実行する AAA と同時に使用することができます。
- **any**: パスワード認証あるいは公開鍵認証のどちらかを指定します。
- **password-publickey**: SSH2 クライアントのパスワード認証と公開鍵認証の両方を指定します。SSH2 クライアントでは、**password-publickey** 認証方式は高いセキュリティを提供します。SSH1 クライアントではパスワード認証あるいは公開鍵認証のどちらかを指定します。
- **publickey**: 公開鍵認証を指定します。認証方式は複雑で暗号時間が遅いですが、セキュリティ強度は強くなり、brute-force 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>:* スペースで区切られた最大 6 つの SSH クライアントの公開鍵を指定します。*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公開鍵を指定した場合、装置は公開鍵を指定順に使用してユーザ ID を検証します。ユーザは、ユーザが鍵の公開小切手を一枚通過すれば有効です。

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。

このコマンドを使用して、認証方式により SSH ユーザに設定してください。

- 認証方式が **publickey** の場合、SSH ユーザと SSH サーバ上のローカルユーザを作成しなければなりません。SSH ユーザが正しい作業エリアとユーザロールを割り当てられるように、２つのユーザ名は同じでなければなりません。
- 認証方式が **password** の場合、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、SSH サーバ上に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上に SSH ユーザを設定します。

  ssh user コマンドを使って SSH ユーザを作成する必要はありません。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。そのような SSH ユーザが作成された場合、サービスタイプと認証方式を適切に指定してい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、SSH サーバ上にローカルユーザを設定します。
  - リモート認証用に、RADIUS サーバのようなリモート認証サーバの SSH ユーザを設定します。

  どちらの場合でも、ローカルユーザあるいはリモート認証サーバで設定される SSH ユーザは SSH ユーザと同じユーザ名を使用する必要があります。

SFTP または SCP ユーザの場合、作業ディレクトリは認証方式に依存します。

- 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。
- 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。

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 **password** である場合、ユーザロールは AAA によって許可されます。
- 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。

このコマンドを使用して、ユーザのホスト公開鍵を複数回指定すると、最新の設定が有効になります。ホストの公開鍵がユーザに指定されていない場合、ユーザはログインに証明書認証を使用します。

コマンド設定は、ログインユーザには影響しません。影響を受けるのは、設定の後にログインしようとするユーザだけです。

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**

9.2 SSHクライアント設定コマンド

9.2.1 bye

Syntax

bye

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

説明

bye コマンドは SFTP サーバとの通信を終了し、user view に戻します。

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>

9.2.2 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 サーバの作業ディレクトリを変更します。

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

作業ディレクトリを **new1** に変更します。

sftp> cd new1

```
Current Directory is:/new1
```

sftp> pwd

```
Remote working directory: /new1
sftp>
```

9.2.3 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>
```

9.2.4 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: 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
```

9.2.5 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。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。

sftp> dir -l

```
-rwxrwxrwx    1 1       1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 012.pub
```

9.2.6 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 クライアントに設定された送信元 IP アドレスを表示します。

例

SFTP クライアントに設定された送信元 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**

9.2.7 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 クライアントに設定された送信元 IP アドレスを表示します。

例

Stelnet クライアントに設定された送信元 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**

9.2.8 exit

Syntax

exit

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

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>

9.2.9 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 SFTP 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 SFTP 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
```

9.2.10 help

Syntax

help

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

説明

help コマンドは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

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
```

9.2.11 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。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。

sftp> ls -l

```
-rwxrwxrwx    1 1        1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1             301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1             301 Dec 18 14:12 012.pub
```

9.2.12 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: 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 **test** を作成します。

sftp> mkdir test

9.2.13 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
```

9.2.14 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: /
```

出力は、現在の作業ディレクトリがルートディレクトリであることを示しています。

9.2.15 quit

Syntax

quit

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

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>

9.2.16 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
```

9.2.17 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** に指定します。

sftp> dir

```
aa.pub  temp1.c
```

sftp> rename temp1.c temp2.c

sftp> dir

```
aa.pub  temp2.c
```

9.2.18 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

9.2.19 scp

Syntax

scp *server* [*port-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } |

prefer-kex { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **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 アドレスまたはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

get: ファイルをダウンロードします。

put: ファイルをアップロードします。

source-file-name: ソースファイル名を指定します。大文字、小文字を区別し、設定範囲は 1～255 文字です。

destination-file-name: ターゲットファイル名を指定します。大文字、小文字を区別し、設定範囲は 1～255 文字です。指定しない場合、ターゲットファイルはソースファイルと同じファイル名を使用します。

identity-key: クライアントの公開鍵認証用の公開鍵アルゴリズムを指定します。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。指定されたアルゴリズムに関連付けられているローカルプライベート鍵を使用してクライアントはデジタル署名または証明書を作成します。

- **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のデータ圧縮に推奨される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先暗号化アルゴリズムを指定します。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC、です。

- **3des-cbc**: 暗号化アルゴリズム 3DES-CBC を指定します。
- **aes128-cbc**: 暗号化アルゴリズム AES128-CBC を指定します。
- **des-cbc**: 暗号化アルゴリズム DES-CBC を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先 HMAC アルゴリズムを指定します。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96 です。

- **md5**: HMAC アルゴリズム HMAC-MD5 を指定します。
- **md5-96**: HMAC アルゴリズム HMAC-MD5-96 を指定します。
- **sha1**: HMAC アルゴリズム HMAC-SHA1 を指定します。
- **sha1-96**: HMAC アルゴリズム HMAC-SHA1-96 を指定します。

prefer-kex: 優先鍵交換アルゴリズムを指定します。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、difie-hellman-group-exchange-sha1、difie-hellman-group1-sha1、difie-hellman-group14-sha1 です。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム difi-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム difie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム difie-hellman-group14-sha1 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先暗号化アルゴリズムを指定します。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズム(**prefer-ctos-cipher** キーワードを参照)と同じです。

prefer-stoc-hmac: サーバからクライアントへの優先 HMAC アルゴリズムを指定します。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズム(**prefer-ctos-hmac** キーワードを参照)と同じです。

public-key *keyname*: クライアントがサーバの認証に使用するサーバのホスト公開鍵を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しないストリングを指定します。

source: SCP パケットの送信元 IPv4 アドレスまたは送信元インタフェースを指定します。デフォルトでは、装置は SCP パケットの送信元アドレスとしてルーティングエントリの出力インタフェースのプライマリ IPv4 アドレスを使用します。SCP 接続を成功させるための最善の方法として、送信元インタフェースとしてループバックインタフェースを指定するか、送信元アドレスとして IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: ソースインタフェースをタイプと番号で指定します。このインタフェースの IPv4 アドレスは SCP パケットの送信元 IPv4 アドレスです。
- **ip** *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

scp コマンドは IPv4 SCP サーバへの接続を確立し、サーバとの間でファイルを転送します。

コマンドでユーザ名とパスワードを指定しない場合は、対話形式でユーザ名とパスワードを指定する必要があります。

SCP サーバが公開鍵認証を使用する場合、このコマンドによって指定されたパスワードは無視されます。

例

SCP クライアントを SCP サーバ **200.1.1.1** に接続します。サーバの公開鍵を **svkey** として指定し、ファイル **abc** をダウンロードします。.txt ファイルを作成します。SCP クライアントは、公開鍵認証を使用します。次のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは **dh-group14-sha1** です。
- サーバからクライアントへの優先される暗号化アルゴリズムは **aes128-cbc** です。
- クライアントからサーバへの優先される HMAC アルゴリズムは **sha1** です。
- サーバからクライアントへの優先される HMAC アルゴリズムは **sha1-96** です。
- サーバとクライアント間で優先される圧縮アルゴリズムは **zlib** です。

<Switch> scp 200.1.1.1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey

```
Username:
```

9.2.20 scp ipv6

Syntax

scp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv6 アドレスまたはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

-i *interface-type interface-number*: SCP パケットのタイプと数によって出力インタフェースを指定します。このオプションは、サーバがリンクローカルアドレスを使用してクライアントに SCP サービスを提供する場合にのみ使用されます。SCP クライアント上の指定された出力インタフェースはリンクローカルアドレスを持たなければなりません。

get: ファイルをダウンロードします。

put: ファイルをアップロードします。

source-file-name: ソースファイル名を指定します。大文字、小文字を区別し、設定範囲は 1～255 文字です。

destination-file-name: ターゲットファイル名を指定します。大文字、小文字を区別し、設定範囲は 1～255 文字です。指定しない場合、ターゲットファイルはソースファイルと同じファイル名を使用します。

identity-key: クライアントの公開鍵認証用の公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。ローカルプライベート鍵を使用してクライアントはデジタル署名または証明書を作成します。

- **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のデータ圧縮に推奨される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム **zlib** を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先暗号化アルゴリズムを指定します。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC です。

- **3des-cbc**: 暗号化アルゴリズム 3DES-CBC を指定します。
- **aes128-cbc**: 暗号化アルゴリズム AES128-CBC を指定します。
- **des-cbc**: 暗号化アルゴリズム DES-CBC を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先 HMAC アルゴリズムを指定します。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96 です。

- **md5**: HMAC アルゴリズム HMAC-MD5 を指定します。
- **md5-96**: HMAC アルゴリズム HMAC-MD5-96 を指定します。
- **sha1**: HMAC アルゴリズム HMAC-SHA1 を指定します。
- **sha1-96**: HMAC アルゴリズム HMAC-SHA1-96 を指定します。

prefer-kex: 優先鍵交換アルゴリズムを指定します。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、difie-hellman-group-exchange-sha1、difie-hellman-group1-sha1、difie-hellman-group14-sha1 です。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム difi-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム difie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム difie-hellman-group14-sha1 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先暗号化アルゴリズムを指定します。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズム(**prefer-ctos-cipher** キーワードを参照)と同じです。

prefer-stoc-hmac: サーバからクライアントへの優先 HMAC アルゴリズムを指定します。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズム(**prefer-ctos-hmac** キーワードを参照)と同じです。

public-key *keyname*: クライアントがサーバの認証に使用するサーバのホスト公開鍵を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しないストリングを指定します。

source: IPv6 SCP パケットの送信元 IPv6 アドレスまたは送信元インタフェースを指定します。デフォルトで、装置は RFC3484 に従って IPv6 SCP パケットの送信元アドレスを自動的に選択します。SCP 接続を成功させるための最善の方法として、ループバックインタフェースを送信元インタフェースとして指定するか、ループバックインタフェースの IPv6 アドレスを送信元アドレスとして指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースをタイプと番号で指定します。このインタフェース IPv6 アドレスは IPv6SCP パケットの送信元 IPv6 アドレスです。
- **ipv6** *ipv6-address*: 送信元 IPv6 アドレスを指定します。

説明

scp ipv6 コマンドは IPv6 SCP サーバへの接続を確立し、サーバとの間でファイルを転送します。

コマンドでユーザ名とパスワードを指定しない場合は、対話形式でユーザ名とパスワードを指定する必要があります。

SCP サーバが公開鍵認証を使用する場合、このコマンドによって指定されたパスワードは無視されます。

例

SCP クライアントを SCP サーバ **2000::1.**に接続します。サーバの公開鍵を **svkey** として指定し、ファイル **abc** をダウンロードします。.txt ファイルを作成します。SCP クライアントは、公開鍵認証を使用します。次のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは **dh-group14-sha1** です。
- サーバからクライアントへの優先される暗号化アルゴリズムは **aes128-cbc** です。
- クライアントからサーバへの優先される HMAC アルゴリズムは **sha1** です。
- サーバからクライアントへの優先される HMAC アルゴリズムは **sha1-96** です。
- サーバとクライアント間で優先される圧縮アルゴリズムは **zlib** です。

<Switch> scp ipv6 2000::1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey

```
Username:
```

9.2.21 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。ローカルプライベート鍵を使用してクライアントはデジタル署名または証明書を作成します。

- **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。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC です。

- **3des-cbc**: 暗号化アルゴリズム 3DES-CBC を指定します。
- **aes128-cbc**: 暗号化アルゴリズム AES128-CBC を指定します。
- **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。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96 です。

- **md5**: HMAC アルゴリズム HMAC-MD5 を指定します。
- **md5-96**: HMAC アルゴリズム HMAC-MD5-96 を指定します。

- **sha1**: HMAC アルゴリズム HMAC-SHA1 を指定します。
- **sha1-96**: HMAC アルゴリズム HMAC-SHA1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、difie-hellman-group-exchange-sha1、difie-hellman-group1-sha1、difie-hellman-group14-sha1 です。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム difi-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム difie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム difie-hellman-group14-sha1 を指定します。

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。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズム(**prefer-ctos-cipher** キーワードを参照)と同じです。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズム(**prefer-ctos-hmac** キーワードを参照)と同じです。

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: 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か、送信元アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: 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 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

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。

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

9.2.22 sftp client ipv6 source

Syntax

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

undo sftp client ipv6 source

デフォルト

SFTP パケットの送信元 IPv6 アドレスは設定されていません。SFTP パケットは RFC3484 で定義された送信元アドレスとして、自動で選択された IPv6 アドレスを選択します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。SFTP パケットは送信元アドレスとして指定されたインタフェースで、ロンゲストマッチの IPv6 アドレスを使用します。

ipv6 *ipv6-address*: 送信元 IPv6 アドレスを指定します。

説明

sftp client ipv6 source コマンドは SFTP パケットの送信元 IPv6 アドレスを指定します。

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

このコマンド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。

このコマンドで指定された IPv6 アドレスは、SFTP クライアントの送信元 IPv6 アドレスとして機能します。

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

9.2.23 sftp client source

Syntax

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

undo sftp client source

デフォルト

SFTP パケットの送信元 IPv4 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 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*: 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 IPv4 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。

このコマンドで指定された IPv4 アドレスは、SFTP クライアントの送信元 IPv4 アドレスとして機能します。

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 IPv4 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 IPv4 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 IPv4 アドレスが適用されます。

例

SFTP 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] sftp client source ip 192.168.0.1

関連コマンド

display sftp client source

9.2.24 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。ローカルプライベート鍵を使用してクライアントはデジタル署名または証明書を作成します。

- **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。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC です。

- **3des-cbc**: 暗号化アルゴリズム 3DES-CBC を指定します。
- **aes128-cbc**: 暗号化アルゴリズム AES128-CBC を指定します。
- **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。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96 です。

- **md5**: HMAC アルゴリズム HMAC-MD5 を指定します。
- **md5-96**: HMAC アルゴリズム HMAC-MD5-96 を指定します。
- **sha1**: HMAC アルゴリズム HMAC-SHA1 を指定します。
- **sha1-96**: HMAC アルゴリズム HMAC-SHA1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、difie-hellman-group-exchange-sha1、difie-hellman-group1-sha1、difie-hellman-group14-sha1 です。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム difi-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム difie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム difie-hellman-group14-sha1 を指定します。

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。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズム(**prefer-ctos-cipher** キーワードを参照)と同じです。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズム(**prefer-ctos-hmac** キーワードを参照)と同じです。

dscp *dscp-value*: SFTP クライアントによって送信される IPv6 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: 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か、送信元アドレスとしてループバックインタフェースの 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。

例

IPv6 SFTP サーバ **2000::1** 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 ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey

```
Username:
```

9.2.25 ssh client ipv6 source

Syntax

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

undo ssh client ipv6 source

デフォルト

SSH パケットの送信元 IPv6 アドレスは設定されていません。SSH パケットは RFC3484 で定義された送信元アドレスとして、自動で選択された IPv6 アドレスを選択します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。SSH パケットは送信元アドレスとして指定されたインタフェースで、ロンゲストマッチの IPv6 アドレスを使用します。

ipv6 *ipv6-address*: 送信元 IPv6 アドレスを指定します。

説明

ssh client ipv6 source コマンドは 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。

このコマンドで指定された IPv6 アドレスは、Stelnet クライアントの送信元 IPv6 アドレスとして機能します。

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。

例

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

9.2.26 ssh client source

Syntax

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

undo ssh client source

デフォルト

SSH パケットの送信元 IPv4 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 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*: 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 IPv4 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 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。

このコマンドで指定された IPv4 アドレスは、Stelnet クライアントの送信元 IPv4 アドレスとして機能します。

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 IPv4 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 IPv4 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 IPv4 アドレスが適用されます。

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

9.2.27 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。ローカルプライベート鍵を使用してクライアントはデジタル署名または証明書を作成します。

- **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。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC です。

- **3des-cbc**: 暗号化アルゴリズム 3DES-CBC を指定します。
- **aes128-cbc**: 暗号化アルゴリズム AES128-CBC を指定します。
- **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。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96 です。

- **md5**: HMAC アルゴリズム HMAC-MD5 を指定します。
- **md5-96**: HMAC アルゴリズム HMAC-MD5-96 を指定します。
- **sha1**: HMAC アルゴリズム HMAC-SHA1 を指定します。
- **sha1-96**: HMAC アルゴリズム HMAC-SHA1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、difie-hellman-group-exchange-sha1、difie-hellman-group1-sha1、difie-hellman-group14-sha1 です。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム difi-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム difie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム difie-hellman-group14-sha1 を指定します。

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。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズム(**prefer-ctos-cipher** キーワードを参照)と同じです。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズム(**prefer-ctos-hmac** キーワードを参照)と同じです。

dscp *dscp-value*: SFTP クライアントによって送信される 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*: 大文字、小文字を区別するエスケープ文字を指定します。デフォルトでは、エスケープ文字はチルダ(~)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か、送信元アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: 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 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

ssh2 コマンドは IPv4 Stelnet サーバとの接続を確立します。

escape *character* 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時に 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* 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 $

9.2.28 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。ローカルプライベート鍵を使用してクライアントはデジタル署名または証明書を作成します。

- **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。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC です。

- **3des-cbc**: 暗号化アルゴリズム 3DES-CBC を指定します。
- **aes128-cbc**: 暗号化アルゴリズム AES128-CBC を指定します。
- **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。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96 です。

- **md5**: HMAC アルゴリズム HMAC-MD5 を指定します。
- **md5-96**: HMAC アルゴリズム HMAC-MD5-96 を指定します。
- **sha1**: HMAC アルゴリズム HMAC-SHA1 を指定します。
- **sha1-96**: HMAC アルゴリズム HMAC-SHA1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、difie-hellman-group-exchange-sha1、difie-hellman-group1-sha1、difie-hellman-group14-sha1 です。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム difi-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム difie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム difie-hellman-group14-sha1 を指定します。

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。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズム(**prefer-ctos-cipher** キーワードを参照)と同じです。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズム(**prefer-ctos-hmac** キーワードを参照)と同じです。

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*: 大文字と小文字を区別するエスケープ文字を指定します。デフォルトでは、エスケープ文字はチルダ(~)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: 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 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か、送信元アドレスとしてループバックインタフェースの 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* 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時に 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* 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。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 ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey escape $

9.3 SSH2設定コマンド

9.3.1 display ssh2 algorithm

🕮 **メモ**:

display ssh 2 algorithm コマンドは、Version 7.2.17 以降のソフトウェアからサポートされています。

Syntax

display ssh2 algorithm

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ssh2 algorithm コマンドはアルゴリズムネゴシエーション段階で SSH2 によって使用されるアルゴリズムを表示します。

例

アルゴリズムネゴシエーション段階で SSH2 によって使用されるアルゴリズムを表示します。

<Switch> display ssh2 algorithm

```
Key exchange algorithms: ecdh-sha2-nistp256
ecdh-sha2-nistp384dh-group-exchange-sha1 dh-group14-sha1 dh-group1-sha1
Public key algorithms: x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 rsa dsa
Encryption algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-gcm
aes256-gcmaes128-cbc 3des-cbc aes256-cbc des-cbc
MAC algorithms: sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

表 9-4 コマンド出力

フィールド	説明
Key exchange algorithms	アルゴリズムネゴシエーションの優先度の高い順での鍵交換アルゴリズムです。
Public key algorithms	アルゴリズムネゴシエーションの優先度の高い順での公開鍵アルゴリズムです。
Encryption algorithms	アルゴリズムネゴシエーションの優先度の高い順での暗号化アルゴリズムです。
MAC algorithms	アルゴリズムネゴシエーションの優先度の高い順でのHMACアルゴリズムです。

関連コマンド

- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**

- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

9.3.2 ssh2 algorithm cipher

🕮 **メモ**:

ssh2 algorithm cipher コマンドは、Version 7.2.17 以降のソフトウェアからサポートされています。

Syntax

ssh2 algorithm cipher { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } *

undo ssh2 algorithm cipher

デフォルト

SSH2 は、アルゴリズムネゴシエーションの優先度の高い順に、暗号化アルゴリズム AES128-CTR 、 AES192-CTR 、 AES256-CTR 、 AES128-GCM 、 AES256-GCM 、 AES128-CBC、3DES-CBC、AES256-CBC、および DES-CBC 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

3des-cbc: 暗号化アルゴリズム 3DES-CBC を指定します。

aes128-cbc: 暗号化アルゴリズム AES128-CBC を指定します。

aes128-ctr: 暗号化アルゴリズム AES128-CTR を指定します。

aes128-gcm: 暗号化アルゴリズム AES128-GCM を指定します。

aes192-ctr: 暗号化アルゴリズム AES192-CTR を指定します。

aes256-cbc: 暗号化アルゴリズム AES256-CBC を指定します。

aes256-ctr: 暗号化アルゴリズム AES256-CTR を指定します。

aes256-gcm: 暗号化アルゴリズム AES256-GCM を指定します。

des-cbc: 暗号化アルゴリズム DES-CBC を指定します。

説明

ssh2 algorithm cipher コマンドは SSH2 の暗号化アルゴリズムを指定します。

undo ssh2 algorithm cipher コマンドはデフォルトに戻します。

暗号化アルゴリズムを指定すると、SSH2 は指定されたアルゴリズムのみをアルゴリズムネゴシエーションに使用します。前に指定したアルゴリズムの方が、ネゴシエーション期間中は優先度が高くなります。

例

SSH2 の暗号化アルゴリズムとしてアルゴリズム **aes256-cbc** を指定します。

<Switch> system-view

[Switch] ssh2 algorithm cipher aes256-cbc

関連コマンド

- **display ssh2 algorithm**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

9.3.3 ssh2 algorithm key-exchange

Syntax

ssh2 algorithm key-exchange { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

デフォルト

SSH2 は、アルゴリズムネゴシエーションの優先度の高い順に、鍵交換アルゴリズム ecdh-sha2-nistp256 、 ecdh-sha2-nistp384 、 diffie-hellman-group-exchange-sha1 、diffie-hellman-group14-sha1、および diffie-hellman-group1-sha1 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

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。
ecdh-sha2-nistp256: 鍵交換アルゴリズム ecdh-sha2-nistp256 を指定します。
ecdh-sha2-nistp384: 鍵交換アルゴリズム ecdh-sha2-nistp384 を指定します。

説明

ssh2 algorithm key-exchange コマンドは SSH2 の鍵交換アルゴリズムを指定します。

undo ssh2 algorithm key-exchange コマンドはデフォルトに戻します。

鍵交換アルゴリズムを指定すると、SSH2 は指定されたアルゴリズムのみをアルゴリズムネゴシエーションに使用します。前に指定したアルゴリズムの方が、ネゴシエーション期間中は優先度が高くなります。

例

アルゴリズム **dh-group1-sha1** を SSH2 の鍵交換アルゴリズムとして指定します。

<Switch> system-view

[Switch] ssh2 algorithm key-exchange dh-group1-sha1

関連コマンド

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

9.3.4 ssh2 algorithm mac

Syntax

ssh2 algorithm mac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

デフォルト

SSH2 は、アルゴリズムネゴシエーションの優先度の高い順に、HMAC アルゴリズム SHA2-256、SHA2-512、SHA1、MD5、SHA1-96、および MD5-96 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

md5: HMAC アルゴリズム HMAC-MD5 を指定します。

md5-96: HMAC アルゴリズム HMAC-MD5-96 を指定します。

sha1: HMAC アルゴリズム HMAC-SHA1 を指定します。

sha1-96: HMAC アルゴリズム HMAC-SHA1-96 を指定します。**sha2-256**: HMAC アルゴリズム HMAC-SHA2-256 を指定します。**sha2-512**: HMAC アルゴリズム HMAC-SHA2-512 を指定します。

説明

ssh2 algorithm mac コマンドは SSH2 の HMAC アルゴリズムを指定します。

undo ssh2 algorithm mac コマンドはデフォルトに戻します。

HMAC アルゴリズムを指定すると、SSH2 は指定されたアルゴリズムのみをアルゴリズムネゴシエーションに使用します。前に指定したアルゴリズムの方が、ネゴシエーション期間中は優先度が高くなります。

例

アルゴリズム **md5** を SSH2 の HMAC アルゴリズムとして指定します。

<Switch> system-view

[Switch] ssh2 algorithm mac md5

関連コマンド

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm public-key**

9.3.5 ssh2 algorithm public-key

Syntax

ssh2 algorithm public-key { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } *

undo ssh2 algorithm public-key

デフォルト

SSH2 は、アルゴリズムネゴシエーションの優先度の高い順に、公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp256 、 x509v3-ecdsa-sha2-nistp384 、 ecdsa-sha2-nistp256 、ecdsa-sha2-nistp384、RSA、および DSA 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

dsa: 公開鍵アルゴリズム DSA を指定します。**ecdsa-sha2-nistp256**: 公開鍵アルゴリズム ecdsa-sha2-nistp256 を指定します。**ecdsa-sha2-nistp384**: 公開鍵アルゴリズム ecdsa-sha2-nistp384 を指定します。

rsa: 公開鍵アルゴリズム RSA を指定します。**x509v3-ecdsa-sha2-nistp256**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp256 を指定します。**x509v3-ecdsa-sha2-nistp384**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp384 を指定します。

説明

ssh2 algorithm public-key コマンドは SSH2 の公開鍵アルゴリズムを指定します。

undo ssh2 algorithm public-key コマンドはデフォルトに戻します。

公開鍵アルゴリズムを指定すると、SSH2 は指定されたアルゴリズムのみをアルゴリズムネゴシエーションに使用します。前に指定したアルゴリズムの方が、ネゴシエーション期間中は優先度が高くなります。

例

アルゴリズム **dsa** を SSH2 の公開鍵アルゴリズムとして指定します。

<Switch> system-view

[Switch] ssh2 algorithm public-key dsa

関連コマンド

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**

目次

このセクションのページは **8-x-x** です。

10 章 SSL 10-1
10.1 SSL 設定コマンド 10-1
10.1.1 display ssl server-policy 10-1
10.1.2 pki-domain (SSL client policy view) 10-2
10.1.3 pki-domain (SSL server policy view) 10-3
10.1.4 security-enhanced level 10-4
10.1.5 ssl server-policy 10-5
10.1.6 ssl version disable 10-5

10章 SSL

10.1 SSL設定コマンド

10.1.1 display ssl server-policy

Syntax

display ssl server-policy [*policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name: SSL サーバポリシーの名前を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。指定しない場合、すべての SSL サーバポリシーの情報を表示します。

説明

display ssl server-policy コマンドは SSL サーバポリシーの情報を表示します。

例

SSL サーバポリシー**policy1** の情報を表示します。

<Switch> display ssl server-policy policy1

```
SSL server policy: policy1
    PKI domain: server-domain
    Ciphersuites:
        DHE_RSA_AES_128_CBC_SHA
        RSA_AES_128_CBC_SHA
    Session cache size: 600
    Caching timeout: 3600 seconds
    Client-verify: Enabled
```

表 10-1 コマンド出力

フィールド	説明
Caching timeout	セッションキャッシュのタイムアウト時間を指定します。 単位は秒です。
Client-verify	SSLクライアント認証モードは、以下を含みます。 ● **Disabled**－SSLクライアント認証を無効にします。 ● **Enabled**－SSLクライアント認証は必須です。 ● **Optional**－SSLクライアント認証はオプションです。

10.1.2 pki-domain (SSL client policy view)

Syntax

pki-domain *domain-name*

undo pki-domain

デフォルト

設定なし

View

SSL client policy view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメインをその名前で指定します。設定範囲は 1～31 です。大文字小文字を区別しない文字列です。

説明

pki-domain コマンドは SSL クライアントポリシーの PKI ドメインを指定します。

undo pki-domain コマンドはデフォルトに戻します。

SSL クライアントポリシーに PKI ドメインを指定した場合、SSL クライアントポリシーを使用する SSL クライアントは、指定された PKI ドメインを通じてデジタル証明書を取得します。

例

SSL クライアントポリシー**policy1** に PKI ドメイン **client-domain** を指定します。

<Switch> system-view

[Switch] ssl client-policy policy1

[Switch-ssl-client-policy-policy1] pki-domain client-domain

関連コマンド

pki domain

10.1.3 pki-domain (SSL server policy view)

Syntax

pki-domain *domain-name*

undo pki-domain

デフォルト

設定なし

View

SSL server policy view

定義済みユーザロール

network-admin

パラメータ

domain-name: 名前で PKI ドメインを指定します。設定範囲は 1～31 です。大文字と小文字を区別しません。

説明

pki-domain コマンドは SSL サーバポリシーの PKI ドメインを指定します。

undo pki-domain コマンドはデフォルトに戻します。

SSL サーバポリシーに PKI ドメインを指定すると、SSL サーバポリシーを使用する SSL サーバは、指定された PKI ドメインを通じてデジタル証明書を取得します。

例

SSL サーバポリシー**policy1** の PKI ドメイン **server-domain** を指定します。

<Switch> system-view

[Switch] ssl server-policy policy1

[Switch-ssl-server-policy-policy1] pki-domain server-domain

関連コマンド

- **display ssl server-policy**
- **pki domain**

10.1.4 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-S5300G 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

🕮 **メモ**:

security-enhanced level コマンドは、Version 7.4.30 を含む以降のソフトウェアでサポートされています。セキュリティレベルの仕様は Version 7.4.27 以前と同じです。

10.1.5 ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-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: SSL サーバポリシーの名前を指定します。設定範囲は 1～31 です。大文字と小文字を区別しません。

説明

ssl server-policy コマンドは SSL サーバポリシーを作成してその view を入力するか、既存の SSL サーバポリシーの view を入力します。

undo ssl server-policy コマンドは SSL サーバポリシーを削除します。

このコマンドは、PKI ドメインやサポートされている暗号スーツなどの SSL パラメータを設定できる SSL サーバポリシーを作成します。SSL サーバポリシーは、HTTPS などのアプリケーションに関連付けられて初めて有効になります。

例

policy1 という名前の SSL サーバポリシーを作成し、その view に入ります。

<Switch> system-view

[Switch] ssl server-policy policy1

[Switch-ssl-server-policy-policy1]

関連コマンド

display ssl server-policy

10.1.6 ssl version disable

Syntax

ssl version {ssl3.0 | tls1.0 | tls1.1 | tls1.2 | tls1.3 } disable

undo ssl version {ssl3.0 | tls1.0 | tls1.1 | tls1.2 | tls1.3 } disable

デフォルト

SSL サーバは、SSL3.0、TLS1.0、TLS1.1、TLS1.2、TLS1.3 をサポートします。

View

System view

定義済みユーザロール

network-admin

パラメータ

ssl3.0: SSL3.0 を指定します。

tls1.0: TLS1.0 を指定します。

tls1.1: TLS1.1 を指定します。

tls1.2: TLS1.2 を指定します。

tls1.3: TLS1.3 を指定します。

説明

ssl version disable コマンドは SSL サーバがセッションネゴシエーションに特定の SSL プロトコルバージョンを使用しないようにします。

undo ssl version disable コマンドはデフォルトに戻します。

システムセキュリティを強化するために、SSL サーバがセッションネゴシエーションに特定の SSL プロトコルバージョン(SSL3.0、TLS1.0、TLS1.1、TLS1.2、および TLS1.3)を使用しないようにすることができます。

例

SSL サーバの SSL3.0 を無効にします。

<Switch> system-view

[Switch] ssl version ssl3.0 disable

目次

このセクションのページは **8-x-x** です。

11 章 TCP フラグメントアタックプロテクション.....11-1
11.1 TCP フラグメントアタックプロテクション設定コマンド 11-1
11.1.1 attack-defense tcp fragment enable 11-1

11章 TCP フラグメントアタックプロテクション

11.1 TCPフラグメントアタックプロテクション設定コマンド

11.1.1 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 フラグメントアタックを防ぐために装置が TCP フラグメント攻撃のパケットを廃棄することを有効にします。RFC1858 で定義されているように、TCP フラグメントアタックは次の TCP フラグメントを参照します。

- TCP ヘッダが 20 バイトより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を持つ先頭以外のフラグメント(FO=1)

装置は、CPU を介して転送された TCP フラグメントのみの検証をサポートします。

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 **8-x-x** です。

12 章 IP ソースガード.....12-1
12.1 IP ソースガード設定コマンド.....12-1
12.1.1 display ip source binding.....12-1
12.1.2 display ipv6 source binding.....12-3
12.1.3 ip source binding (interface view).....12-5
12.1.4 ip verify source.....12-6
12.1.5 ipv6 source binding (interface view).....12-8
12.1.6 ipv6 verify source.....12-9

12章 IP ソースガード

12.1 IPソースガード設定コマンド

12.1.1 display ip source binding

Syntax

display ip source binding [**static** | [**arp-snooping-vlan** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

static: スタティック IPv4 ソースガードバインディングエントリを表示します。

arp-snooping-vlan: VLAN の ARP スヌーピングに基づいて生成される IPv4 ソースガードバインディングを指定します。

dhcp-relay: DHCP リレーエージェントに基づいて生成される IPv4 ソースガードバインディングを指定します。

dhcp-server: DHCP サーバに基づいて生成される IPv4 ソースガードバインディングを指定します。

dhcp-snooping: DHCP スヌーピングに基づいて生成される IPv4 ソースガードバインディングを指定します。

ip-address *ip-address*: IPv4 アドレスを指定します。

mac-address *mac-address*: 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。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

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。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。このオプションを指定しない場合、マスタ装置の IPv4 ソースガードバインディングエントリを表示します。

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 IP ソースガードバインディングエントリを表示します。

<Switch> display ip source binding

```
Total entries found: 5
IP Address      MAC Address    Interface             VLAN Type
10.1.0.5        040a-0000-4000 GE1/0/1               1    DHCP snooping
10.1.0.6        040a-0000-3000 GE1/0/1               1    DHCP snooping
10.1.0.7        040a-0000-2000 GE1/0/1               1    DHCP snooping
10.1.0.8        040a-0000-1000 GE1/0/2               N/A  DHCP relay
10.1.0.9        040a-0000-2000 GE1/0/2               N/A  Static
```

表 12-1 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—ip source binding**コマンドを使用して手動で設定されました。スタティックバインディングは、IPソースガードバインディングエントリのパケットフィルタリングや、セキュリティサービスを提供する他のモジュールで使用されます。 • **ARP snooping vlan**—VLANのARPスヌーピングに基づいて動的に生成されます。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用です。 • **DHCP relay**—DHCPリレーエントリをもとにダイナミックに作成されました。バインディングはIPソースガードバインディングエントリのパケットフィルタリング用です。 • **DHCP server**—DHCPサーバエントリをもとにダイナミックに作成されました。バインドは、セキュリティサービスを提供するためにほかのモジュールによって使用されます。 • **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ソースガードバインディングエントリのパケットフィルタリング用です。

関連コマンド

- **ip source binding**
- **ip verify source**

12.1.2 display ipv6 source binding

Syntax

display ipv6 source binding [**static** | [**dhcpv6-snooping**]] [**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 ソースガードアドレスバインディングエントリを表示します。

dhcpv6-snooping: DHCPv6 スヌーピングに基づいて生成された IPv6 ソースガードバインディングを指定します。

ip-address *ipv6-address*: IPv6 アドレスを指定します。

mac-address *mac-address*: 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。

vlan *vlan-id*: VLAN ID を指定し、設定範囲は 1～4094 です。

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。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。このオプションを指定しない場合、マスタ装置の IPv6 ソースガードアドレスバインディングエントリを表示します。

説明

display ipv6 source binding コマンドは IPv6 ソースガードバインディングエントリを表示します。

例

パブリックネットワークのすべての IPv6 ソースガードアドレス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 12-2 コマンド出力

フィールド	説明
Total entries found	IPv6ソースガードアドレスバインディングエントリの総数です。
IPv6 Address	IPv6ソースガードアドレス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ソースガードアドレス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ソースガードアドレス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ソースガードアドレス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ソースガードアドレスバインディングエントリのタイプです。 • **Static**—**ipv6source binding**コマンドを使用して手動で設定します。スタティックバインディングは、IPv6ソースガードバインディングエントリのパケットフィルタリング、またはセキュリティサービスを提供するためにほかのモジュールによって使用されます。 • **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、IPv6ソースガードでのパケットフィルタリング用です。

関連コマンド

- **ipv6 source binding**
- **ipv6 verify source**

12.1.3 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（ブロードキャストアドレス）、マルチキャスト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

GigabitEthernet1/0/1 の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。

<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

12.1.4 ip verify source

Syntax

ip verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip verify source

デフォルト

無効

View

Layer 2 Ethernet interface view, VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 送信元 IPv4 アドレスによって受信パケットをフィルタします。

ip-address mac-address: 送信元 IPv4 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

mac-address: 送信元 MAC アドレスによって受信パケットをフィルタします。

説明

ip verify source コマンドは IPv4 ソースガード機能を有効にします。

undo ip verify source コマンドは IPv4 ソースガード機能を無効にします。

インタフェースで IPv4 ソースガードバインディングエントリを有効にすると、この機能はスタティックおよびダイナミック IPv4 ソースガードバインディングエントリを使用して、インタフェースの受信パケットを照合します。IPv4 ソースガードバインディングエントリに一致するパケットは転送され、IPv4 ソースガードバインディングエントリに一致しないパケットは破棄されます。

このコマンドで指定された一致条件は、ダイナミック IP ソースガードバインディングエントリにのみ適用されます。スタティック IPv4 ソースガードバインディングエントリは、**ip source binding** コマンドを使用して設定されたスタティックバインディングを使用します。

例

レイヤ 2 Ethernet インタフェース GigabitEthernet 1/0/1 で IPv4 ソースガード機能を有効にします。ダイナミック IP ソースガード機能で送信元 IPv4 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] ip verify source ip-address mac-address

VLAN インタフェース 100 で IPv4 ソースガードを有効にします。ダイナミック IP ソースガード機能で送信元 IPv4 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ip verify source ip-address mac-address

関連コマンド

display ip source binding

12.1.5 ipv6 source binding (interface view)

Syntax

ipv6 source binding { **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ipv6 source binding { **all** | **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

デフォルト

設定なし

View

Layer 2 Ethernet interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

all: インタフェースのすべてのスタティック IPv6 ソースガードバインディングエントリを削除します。

ip-address *ipv6-address*: スタティックバインディングエントリの IPv6 アドレスを指定します。すべてが 0 のアドレス、マルチキャストアドレス、ループバックアドレスは指定することができません。

mac-address *mac-address*: スタティックバインディングエントリの MAC アドレスを指定します。MAC アドレスの形式は H-H-H です。すべてが 0 のアドレス、すべてが F のアドレス（ブロードキャストアドレス）、マルチキャスト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。

インタフェースの受信 IPv6 パケットをフィルタするため、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します。

例

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

12.1.6 ipv6 verify source

Syntax

ipv6 verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ipv6 verify source

デフォルト

無効

View

Layer 2 Ethernet interface view, VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 送信元 IPv6 アドレスによって受信パケットをフィルタします。

ip-address mac-address: 送信元 IPv6 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

mac-address: 送信元 MAC アドレスによって受信パケットをフィルタします。

説明

ipv6 verify source コマンドは IPv6 ソースガード機能を有効にします。

undo ipv6 verify source コマンドは IPv6 ソースガード機能を無効にします。

インタフェースで IPv6 ソースガードバインディングエントリを有効にすると、この機能はスタティックおよびダイナミック IPv6 ソースガードバインディングエントリを使用して、インタフェースの受信パケットを照合します。IPv6 ソースガードバインディングエントリに一致するパケットは転送され、IPv6 ソースガードバインディングエントリに一致しないパケットは破棄されます。

このコマンドで指定される照合基準は、ダイナミック IPv6 ソースガードバインディングエントリにのみ適用されます。スタティック IPv6 ソースガードバインディングエントリは、**ipv6 source binding** コマンドを使用して設定されたスタティックバインディングを使用します。

例

レイヤ 2 Ethernet インタフェース GigabitEthernet 1/0/1 で IPv6 ソースガード機能を有効にします。ダイナミック IPv6 ソースガード機能で送信元 IPv6 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address

関連コマンド

display ipv6 source binding

目次

このセクションのページは **8-x-x** です。

13 章 ARP アタックプロテクション 13-1
13.1 宛先不明の IP アタックプロテクション設定コマンド 13-1
13.1.1 arp resolving-route enable 13-1
13.1.2 arp resolving-route probe-count 13-2
13.1.3 arp resolving-route probe-interval 13-2
13.1.4 arp source-suppression enable 13-3
13.1.5 arp source-suppression limit 13-4
13.1.6 display arp source-suppression 13-5
13.2 ARP パケットレートリミット設定コマンド 13-6
13.2.1 arp rate-limit 13-6
13.2.2 arp rate-limit log enable 13-7
13.2.3 arp rate-limit log interval 13-8
13.2.4 snmp-agent trap enable arp 13-9
13.3 送信元 MAC ベース ARP アタック detection 設定コマンド 13-10
13.3.1 arp source-mac 13-10
13.3.2 arp source-mac aging-time 13-11
13.3.3 arp source-mac exclude-mac 13-12
13.3.4 arp source-mac threshold 13-12
13.3.5 display arp source-mac 13-13
13.4 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 13-14
13.4.1 arp valid-check enable 13-14
13.5 ARP 確認応答設定コマンド 13-15
13.5.1 arp active-ack enable 13-15
13.6 ARP アタック detection 設定コマンド 13-16
13.6.1 arp detection enable 13-16
13.6.2 arp detection trust 13-17
13.6.3 arp detection validate 13-17
13.6.4 arp restricted-forwarding enable 13-18
13.6.5 display arp detection 13-19
13.6.6 display arp detection statistics attack-source 13-20
13.6.7 display arp detection statistics packet-drop 13-21
13.6.8 reset arp detection statistics attack-source 13-22
13.6.9 reset arp detection statistics packet-drop 13-23
13.7 ARP ゲートウェイプロテクション設定コマンド 13-24
13.7.1 arp filter source 13-24
13.8 ARP フィルタリング設定コマンド 13-25

13.8.1 arp filter binding 13-25

13章 ARP アタックプロテクション

13.1 宛先不明のIPアタックプロテクション設定コマンド

13.1.1 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**

13.1.2 arp resolving-route probe-count

Syntax

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

デフォルト

それぞれの宛先不明 IP アドレスに 3 回の ARP ブラックホールのルートを調べます。

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**

13.1.3 arp resolving-route probe-interval

Syntax

arp resolving-route probe-interval *interval*

undo arp resolving-route probe-interval

デフォルト

ARP ブラックホールのルートを 1 秒周期で調査します。

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 1～5 秒で設定します。

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**

13.1.4 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 ARP 送信元抑制機能を無効にします。

このコマンドはゲートウェイで設定します。

例

ARP 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

13.1.5 arp source-suppression limit

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

デフォルト

送信元 IP アドレスあたり最大 10 個の宛先不明のパケットを 5 秒以内に処理できます。

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。

IP アドレスから 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 IP アドレス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

13.1.6 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 13-1 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。

13.2 ARPパケットレートリミット設定コマンド

13.2.1 arp rate-limit

Syntax

arp rate-limit [*pps*]

undo arp rate-limit

デフォルト

有効

v7.1.8 を含むそれ以前　100pps

v7.2.16 を含むそれ以降　600pps

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

v7.1.8 を含むそれ以前

pps: ARP パケットレートの上限を指定します。単位は pps です。設定範囲は 5～200 です。

v7.2.16 を含むそれ以降

pps: ARP パケットレートの上限を指定します。単位は pps です。設定範囲は 5～600 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ます。

undo arp rate-limit コマンドは ARP パケットのレートリミット設定を無効にします。

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。レートリミットを超えるパケットは破棄されます。

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

🕮 **メモ:**

QX-S5300G シリーズは最大 100PPS まで指定できます。

13.2.2 arp rate-limit log enable

Syntax

arp rate-limit log enable

undo arp rate-limit log enable

デフォルト

ARP パケットレートリミットのロギングは無効です。

View

System view

定義済みユーザロール

network-admin

説明

arp rate-limit log enable コマンドは ARP パケットレートリミットのロギングを有効にします。

undo arp rate-limit log enable コマンドは ARP パケットレートリミットのロギングを無効にします。

ARP パケットレートリミットのロギングが有効になっている場合、装置はログセンターメッセージに送信間隔内で最も高いしきい値を超えた ARP パケットレートをインフォメーションセンターに送信します。ログ出力ルールを設定するようにインフォメーションセンターモジュールを設定できます。詳細はオペレーションマニュアルのセクション 10 *システム管理* を参照してください。

例

ARP パケットレートリミットのロギングを有効にします。

<Switch> system-view

[Switch] arp rate-limit log enable

13.2.3 arp rate-limit log interval

Syntax

arp rate-limit log interval *interval*

undo arp rate-limit log interval

デフォルト

インタフェースで受信された ARP パケットのレートが制限を超えた場合、装置は 60 秒ごとに通知またはログメッセージを送信します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: 設定範囲は 1～86400 秒です。

説明

arp rate-limit log interval コマンドは ARP パケットレートリミットの通知およびログメッセージ送信間隔を設定します。

undo arp rate-limit log interval コマンドはデフォルトに戻します。

デフォルトの間隔を変更して有効にするには、ARP パケットレートリミットを有効にし、ARP パケットレートリミットの通知またはログメッセージの送信を有効にする必要があります。

例

インタフェースで受信する ARP パケットのレートが制限を超えた場合に 120 秒ごとに通知とログメッセージを送信するように装置を設定します。

<Switch> system-view

[Switch] arp rate-limit log interval 120

関連コマンド

- **arp rate-limit**
- **arp rate-limit log enable**
- **snmp-agent trap enable arp**

13.2.4 snmp-agent trap enable arp

Syntax

snmp-agent trap enable arp [**rate-limit**]

undo snmp-agent trap enable arp [**rate-limit**]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

rate-limit: ARP パケットのレートリミット機能を指定します。

説明

snmp-agent trap enable arp コマンドは ARP パケットの SNMP notification の送信を有効にします。

undo snmp-agent trap enable arp コマンドは ARP パケットの SNMP notification の送信を無効にします。

ARP の SNMP notification の送信が有効である場合、装置は SNMP notification の送信間隔以内に、もっとも高いしきい値と交差した ARP パケットのレートを、SNMP モジュールへ送信します。

ARP イベント通知を正しく送信するには、装置で SNMP も設定する必要があります。

SNMP 設定についての詳細は、オペレーションマニュアルのセクション 10 *システム管理* “*SNMP*”を参照してください。

例

ARP パケットの SNMP notification の送信を有効にします。

<Switch> system-view

[Switch] snmp-agent trap enable arp rate-limit

13.3 送信元MACベースARPアタックdetection設定コマンド

13.3.1 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: フィルタ処理方法を指定します。

monitor: モニタ処理方法を指定します。

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 アタック detection を有効にし、処理方法を指定します。

undo arp source-mac コマンドは送信元 MAC アドレスにもとづいた ARP アタック detection 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。

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、装置は、設定されたパラメータに従い、アタックに対する処理を実行します。

- **Monitor**—ログメッセージのみを生成します。
- **Filter**—ログメッセージを生成し、MAC アドレスからの後続の ARP パケットをフィルタします。

送信元の MAC ベースの ARP アタック detection 機能を有効にする前に、ARP ロギング機能を有効にしていることを確認してください。ARP ロギング機能についての詳細は、オペレーションマニュアルのセクション 4 *IP サービス* を参照してください。

undo arp source-mac コマンドで処理方法を指定しない場合、コマンドはこの機能を無効にします。

例

送信元 MAC アドレスにもとづいた ARP アタック 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

13.3.2 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（5 分）

View

System view

定義済みユーザロール

network-admin

パラメータ

time: ARP アタック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 アタック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 アタック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

13.3.3 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 source-mac exclude-mac コマンドは送信元 MAC アドレスにもとづいた ARP アタック detection から指定された MAC アドレスを除外します。

undo arp source-mac exclude-mac コマンドは送信元 MAC アドレスにもとづいた ARP アタック detection から除外された MAC アドレスを削除します。

MAC アドレスを指定しない場合、**undo arp source-mac exclude-mac** コマンドは除外されたすべての MAC アドレスを削除します。

例

送信元 MAC にもとづいた ARP アタック 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

13.3.4 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 アタック detection のしきい値を指定します。設定範囲は 1～5000 秒です。

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 アタック 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 アタック detection のしきい値を 30 に指定します。

<Switch> system-view

[Switch] arp source-mac threshold 30

13.3.5 display arp source-mac

Syntax

display arp source-mac { **interface** *interface-type interface-number* | **slot** *slot-number* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の ARP アタックエントリを表示します。

説明

display arp source-mac コマンドは送信元 MAC アドレスにもとづいた ARP アタック detection によって検出された ARP アタックエントリを表示します。

例

GigabitEthernet 1/0/1 の送信元 MAC アドレスにもとづいた ARP アタック detection によって検出された ARP アタックエントリを表示します。

<Switch> display arp source-mac interface gigabitethernet 1/0/1

```
Source-MAC         VLAN ID  Interface             Aging-time
23f3-1122-3344      4094    GE1/0/1               10
```

表 13-2 コマンド出力

フィールド	説明
Source-MAC	アタックの送信元MACアドレスです。
VLAN ID	アタックが検出されたVLANのIDです。
Interface	アタックが検出されたインタフェースです。
Aging-time	ARPアタックエントリのエージングタイムです(秒単位)。

13.4 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

13.4.1 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、ARP パケットをフィルタします。

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

13.5 ARP確認応答設定コマンド

13.5.1 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 ARP 確認応答機能を無効にします。

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 確認応答機能有効にします。

<Switch> system-view

[Switch] arp active-ack enable

13.6 ARPアタックdetection設定コマンド

13.6.1 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 detection を有効にします。

undo arp detection enable コマンドは ARP アタック detection を無効にします。

例

VLAN 2 で ARP アタック detection を有効にします。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] arp detection enable

関連コマンド

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

13.6.2 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するか、AC を ARP トラステッドポート AC 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

13.6.3 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、および ARP 要求の送信元 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 1、またはマルチキャスト 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 つのコマンドラインで複数のオブジェクトをチェック対象として指定できます。

キーワードが指定されていない場合、**undo arp detection validate** コマンドは、すべてのオブジェクトの ARP パケットの正当性の確認を無効にします。

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

13.6.4 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

13.6.5 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 detection が有効な VLAN を表示します。

例

ARP アタック detection が有効な VLAN を表示します。

<Switch> display arp detection

```
ARP detection is enabled in the following VLANs:
1-2, 4-5
```

関連コマンド

arp detection enable

13.6.6 display arp detection statistics attack-source

Syntax

display arp detection statistics attack-source slot *slot-number*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の ARP アタックの送信元統計情報を表示します。

説明

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

例

ARP アタックの送信元について統計情報を表示します。

<Switch> display arp detection statistics attack-source

```
Interface            VLAN  MAC address    IP address      Number     Time
GE1/0/1              1     0005-0001-0001 10.1.1.14       24         17:09:56
03-27-2017
```

表 13-3 コマンド出力

フィールド	説明
Interface	ARPアタックパケットのインタフェースを受信します。
VLAN	ARPアタックパケットが属するVLANです。
MAC address	ARPアタックパケットの送信元MACアドレスです。
IP address	ARPアタックパケットの送信元IPアドレスです。
Number	ARPアタック検出によってドロップされたARPアタックパケットの数です。
Time	ARPアタック検出がARPアタックパケットを破棄した最新の時刻です。

関連コマンド

arp detection enable

13.6.7 display arp detection statistics packet-drop

Syntax

display arp detection statistics packet-drop [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースをタイプと番号で指定します。インタフェースを指定しない場合、このコマンドは、すべてのインタフェースおよびインタフェース上のすべての Ethernet サービスインスタンスについて、ドロップされたパケット統計情報を表示します。

説明

display arp detection statistics packet-drop コマンドは ARP アタック detection で破棄されたパケットの統計情報を表示します。

このコマンドは、インタフェース上のユーザ妥当性チェックおよび ARP パケット妥当性チェックよって破棄されたパケットの数を表示します。

例

ARP アタック detection によって破棄されたパケットの統計情報を表示します。

<Switch> display arp detection statistics packet-drop

```
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)          IP       Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)               40       0         0         78
GE1/0/2(U)               0        0         0         0
GE1/0/3(T)               0        0         0         0
GE1/0/4(U)               0        0         30        0
```

表 13-4 コマンド出力

フィールド	説明
State	インタフェースの状態です。 • **U**–ARP の untrusted インタフェースです。 • **T**–ARP トラステッドインタフェースです。
Interface(State)	ARPパケットの着信インタフェースです。Stateは、ポートの状態 (trustedまたはuntrusted) を指定します。
IP	無効な送信元およびターゲットIPアドレスが原因で破棄されたARPパケットの数です。
Src-MAC	無効な送信元MACアドレスが原因で破棄されたARPパケットの数です。
Dst-MAC	無効な宛先MACアドレスが原因で破棄されたARPパケットの数です。
Inspect	ユーザの妥当性チェックに合格しなかったARPパケットの数です。

関連コマンド

reset arp detection statistics packet-drop

13.6.8 reset arp detection statistics attack-source

Syntax

reset arp detection statistics attack-source [**slot** *slot-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の ARP アタックの送信元統計情報を削除します。

説明

reset arp detection statistics attack-source コマンドは ARP アタックの送信元の統計情報を削除します。

例

ARP アタックの送信元の統計情報を削除します。

<Switch> reset arp detection statistics attack-source

関連コマンド

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

13.6.9 reset arp detection statistics packet-drop

Syntax

reset arp detection statistics packet-drop [interface *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースをタイプと番号で指定します。インタフェースを指定しない場合、このコマンドは、インタフェース上のすべてのインタフェースおよびすべての Ethernet サービスインスタンスについて、ドロップされたパケット統計情報を削除します。

説明

reset arp detection statistics packet-drop コマンドは ARP アタック detection によって破棄されたパケットの統計情報を削除します。

例

ARP アタック detection によって破棄されたパケットの統計情報を削除します。

<Switch> reset arp detection statistics packet-drop

関連コマンド

display arp detection statistics packet-drop

13.7 ARPゲートウェイプロテクション設定コマンド

13.7.1 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: 保護されたゲートウェイの IP アドレスを指定します。

説明

arp filter source コマンドはゲートウェイに対して ARP ゲートウェイ保護を有効にします。

undo arp filter source コマンドはゲートウェイの ARP ゲートウェイ保護を無効にします。

インタフェース上の最大 8 つのゲートウェイに対して ARP ゲートウェイ保護を有効にできます。同じインタフェースで **arp filter source** コマンドと **arp filter binding** コマンドの両方を設定することはできません。

例

IP アドレス 1.1.1.1 のゲートウェイに対して ARP ゲートウェイ保護を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] arp filter source 1.1.1.1

13.8 ARPフィルタリング設定コマンド

13.8.1 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: 許可された送信者 IP アドレスを指定します。

mac-address: 許可された送信者 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、ARP 許可エントリを設定します。

undo arp filter binding コマンドは ARP が許可されたエントリを削除します。

ARP パケットの送信元 IP アドレスおよび MAC アドレスが、ARP が許可するエントリアドレスと一致する場合、ARP パケットは許可されます。ARP パケットの送信元 IP アドレスおよび MAC アドレスが、ARP が許可したエントリアドレスと一致しない場合、ARP パケットは破棄されます。

インタフェースでは、最大 8 つの ARP 許可エントリを設定できます。

同じインタフェースで **arp filter source** コマンドと **arp filter binding** コマンドの両方を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、ARP 許可の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

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

9. 高可用性

本マニュアルは以下に示す章で構成されています。

01-Ethernet OAM

02-CFD

03-DLDP

04-RRPP

05-Smart Link

06-Monitor Link

07-BFD

08-Track

目次

このセクションのページは **9-x-x** です。

1 章 Ethernet OAM 1-1
1.1 Ethernet OAM 設定コマンド 1-1
1.1.1 display oam 1-1
1.1.2 display oam configuration 1-6
1.1.3 display oam critical-event 1-8
1.1.4 display oam link-event 1-9
1.1.5 oam enable 1-13
1.1.6 oam errored-frame threshold 1-14
1.1.7 oam errored-frame window 1-15
1.1.8 oam errored-frame-period threshold 1-16
1.1.9 oam errored-frame-period window 1-17
1.1.10 oam errored-frame-seconds threshold 1-18
1.1.11 oam errored-frame-seconds window 1-19
1.1.12 oam errored-symbol-period threshold 1-20
1.1.13 oam errored-symbol-period window 1-21
1.1.14 oam global errored-frame threshold 1-22
1.1.15 oam global errored-frame window 1-23
1.1.16 oam global errored-frame-period threshold 1-24
1.1.17 oam global errored-frame-period window 1-25
1.1.18 oam global errored-frame-seconds threshold 1-26
1.1.19 oam global errored-frame-seconds window 1-27
1.1.20 oam global errored-symbol-period threshold 1-28
1.1.21 oam global errored-symbol-period window 1-29
1.1.22 oam global timer hello 1-30
1.1.23 oam global timer keepalive 1-31
1.1.24 oam mode 1-32
1.1.25 oam remote-failure action 1-33
1.1.26 oam remote-loopback 1-34
1.1.27 oam remote-loopback interface 1-35
1.1.28 oam remote-loopback reject-request 1-36
1.1.29 oam timer hello 1-37
1.1.30 oam timer keepalive 1-38
1.1.31 reset oam 1-39

1章 Ethernet OAM

1.1 Ethernet OAM設定コマンド

1.1.1 display oam

Syntax

display oam { **local** | **remote** } [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

local: ローカル装置を指定します。

remote: リモートエンドを指定します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのインタフェースの Ethernet OAM 接続情報を表示します。

説明

display oam コマンドは Ethernet OAM の接続情報を表示します。

例

すべてのローカル装置の Ethernet OAM の接続情報を表示します。

<Switch> display oam local

```
----------- [GigabitEthernet1/0/1] -----------
 Enable status    : Enable
 Loopback status   : No loopback
 Link status      : UP
 OAM mode         : Active
 PDU             : ANY
 Mux action       : FWD
 Par action       : FWD
```

ローカル装置の GigabitEthernet 1/0/1 の Ethernet OAM の接続情報を表示します。

<Switch> display oam local interface gigabitethernet 1/0/1

```
Enable status     : Enable
Loopback status   : No loopback
Link status       : UP
OAM mode          : Active
PDU             : ANY
Mux action        : FWD
Par action        : FWD
Flags
  Link fault       : Not occurred
  Dying gasp       : Not occurred
  Critical event    : Not occurred
  Local evaluating  : COMPLETE
  Remote evaluating : COMPLETE
Packets statistics
  Packet type                    Sent               Received
  ------------------------------------------------------------------
  OAMPDU                         100                80
  OAMInformation                 64                 60
  OAMEventNotification           36                 20
  OAMUniqueEventNotification     36                 10
  OAMDuplicateEventNotification  0                  10
```

表 1-1 コマンド出力

フィールド	説明
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
Enable status	Ethernet OAMの状態です。有効あるいは無効があります。
Loopback status	Ethernet OAMループバックの状態です。 ● **No loopback**－ループバックがありません。 ● **Remote loopback**－リモートループバックです。 ● **Local loopback**－ローカルループバックです。
Link status	リンク状態です。UPあるいはDOWNがあります。
OAM mode	ローカルEthernet OAMモードです。 ● **Active**—ポートがアクティブEthernet OAMモードで動作することを示します。 ● **Passive**—ポートがパッシブEthernet OAMモードで動作することを示します。

フィールド	説明
PDU	ローカル装置でのEthernet OAMPDUの処理方法です。 • **RX_INFO**—ポートはEthernet OAMPDU情報を受信のみ行い、送信を行わないことを示します。 • **LF_INFO**—ポートは、TLVトリプレットの情報と設定したリンクエラーフラグを除いたOAMPDU情報の送信を行うことを示します。 • **INFO**—ポートは、OAMPDU情報のみを送受信することを示します。 • **ANY**—ポートは、どのタイプのEthernet OAMPDUも送受信することを示します。
Mux action	ローカル送信装置の動作モードです。 • **FWD**—ポートはどのようなパケットも送信できることを示します。 • **DISCARD**—ポートは、Ethernet OAMPDUの送信のみ行うことを示します。
Par action	ローカル受信装置の動作モードです。 • **FWD**—ポートはどのようなパケットも受信できることを示します。 • **DISCARD**—ポートは、Ethernet OAMPDUの受信のみ行うことを示します。 • **LB**—ローカル受信装置はEthernet OAMループバック試験が有効であることを示します。この場合、Ethernet OAMPDU以外のすべてのパケットは、送信された経路に沿って送信元に返されます。
Flags	送信されたEthernet OAMPDUのローカルフラグフィールドに挿入されたローカルフラグを示します。
Link fault	Ethernet OAMリンクエラーがあるかどうかを示します。
Dying gasp	致命的なエラーがあるかどうかを示します。
Critical event	クリティカルエラーがあるかどうかを示します。
Local evaluating	ローカル装置からリモート装置への設定のネゴシエーションが完了したかどうかを示します。 • **COMPLETE**—ネゴシエーションが完了しました。 • **NOTCOMPLETE**—ネゴシエーションが完了していません。

フィールド	説明
Remote evaluating	リモート装置からローカル装置への設定のネゴシエーションが完了したかどうかを示します。 • **COMPLETE**—ネゴシエーションが完了しました。 • **NOTCOMPLETE**—ネゴシエーションが完了していません。 • **RESERVED**—このフィールドは予約されており、ネゴシエーションは完了していません。 • **UNSATISFIED**—リモート装置がローカル装置の設定に満足しておらず、ネゴシエーションが完了していません。
Packets statistics	送受信したEthernet OAMPDUの統計情報です。
OAMPDU	送受信したEthernet OAMPDUの総数です。
OAMInformation	送受信したEthernet OAMPDU情報の数です。
OAMEventNotification	送受信したOAMPDUイベント通知の数です。
OAMUniqueEventNotification	１回だけ送信あるいは受信した重複していないOAMPDUイベント通知の数です。
OAMDuplicateEventNotification	送信あるいは受信した重複したOAMPDUイベント通知の数です。

すべてのリモートポートの Ethernet OAM の情報を表示します。

<Switch> display oam remote

```
---------- [GigabitEthernet1/0/1] ----------
 OAM mode         : Active
 MAC address      : 3822-d6a2-a800
 MTU size         : 1500
 Mux action       : FWD
 Par action       : FWD
```

リモートポート GigabitEthernet 1/0/1 の Ethernet OAM の情報を表示します。

<Switch> display oam remote interface gigabitethernet 1/0/1

```
 OAM mode         : Active
 MAC address      : 3822-d6a2-a800
 MTU size         : 1500
 Mux action       : FWD
 Par action       : FWD
 Configuration
   Unidirectional    : Not supported
   Remote loopback   : Supported
   Link events       : Supported
```

```
  MIB retrieval     : Not supported
Flags
  Link fault        : Not occurred
  Dying gasp        : Not occurred
  Critical event    : Not occurred
  Local evaluating  : COMPLETE
  Remote evaluating : COMPLETE
```

表 1-2 コマンド出力

フィールド	説明
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
OAM mode	ローカルEthernet OAMモードです。 • **Active**—ポートがアクティブEthernet OAMモードで動作することを示します。 • **Passive**—ポートがパッシブEthernet OAMモードで動作することを示します。
MAC address	リモート装置のMACアドレスです。
MTU size	MTUサイズです。単位はバイトです。
Mux action	リモート送信装置の動作モードです。 • **FWD**—ポートはどのようなパケットも送信できることを示します。 • **DISCARD**—ポートは、Ethernet OAMPDUの送信のみ行うことを示します。
Par action	リモート受信装置の動作モードです。 • **FWD**—ポートはどのようなパケットも受信できることを示します。 • **DISCARD**—ポートは、Ethernet OAMPDUの受信のみ行うことを示します。 • **LB**—ローカル受信装置はEthernet OAMループバック試験が有効であることを示します。この場合、Ethernet OAMPDU以外のすべてのパケットは、送信された経路に沿って送信元に返されます。
Configuration	リモートEthernet OAMエンティティの設定です。
Unidirectional	単方向通信がサポートされるかどうかを示します。
Remote loopback	Ethernet OAMリモートループバックがサポートされているかどうかを示します。
Link events	Ethernet OAMリンクエラーイベントがサポートされているかどうかを示します。

フィールド	説明
MIB retrieval	MIB変数検索がサポートされているかどうかを示します。
Flags	OAMパケットのピアのEthernet OAMPDUのフラグフィールドの値です。
Link fault	Ethernet OAMリンクエラーがあるかどうかを示します。
Dying gasp	致命的なエラーがあるかどうかを示します。
Critical event	クリティカルエラーがあるかどうかを示します。
Local evaluating	ローカル装置からリモート装置への設定のネゴシエーションが完了したかどうかを示します。 • **COMPLETE**—ネゴシエーションが完了しました。 • **NOTCOMPLETE**—ネゴシエーションが完了していません。 • **RESERVED**—このフィールドは予約されており、ネゴシエーションは完了していません。 • **UNSATISFIED**—リモート装置がローカル装置の設定に満足しておらず、ネゴシエーションが完了していません。
Remote evaluating	リモート装置からローカル装置への設定のネゴシエーションが完了したかどうかを示します。 • **COMPLETE**—ネゴシエーションが完了しました。 • **NOTCOMPLETE**—ネゴシエーションが完了していません。 • **UNSATISFIED**—リモート装置がローカル装置の設定に満足しておらず、ネゴシエーションが完了していません。

関連コマンド

reset oam

1.1.2 display oam configuration

Syntax

display oam configuration [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、デフォルトの設定で使用しないポートでのグローバルの Ethernet OAM の設定を表示します。

説明

display oam configuration コマンドは Ethernet OAM の設定を表示します。

例

デフォルトの設定で使用しないポートでのグローバルの Ethernet OAM の設定を表示します。

<Switch> display oam configuration

```
---------------- [Global] ----------------
 OAM timers
   Hello timer       : 1000 milliseconds
   Keepalive timer    : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window          : 100 x 1000000 symbols
     Threshold       : 1 error symbols
   Errored frame
     Window          : 10 x 100 milliseconds
     Threshold       : 1 error frames
   Errored frame period
     Window          : 1000 x 10000 frames
     Threshold       : 1 error frames
   Errored frame seconds
     Window          : 600 x 100 milliseconds
     Threshold       : 1 error seconds


----------- [GigabitEthernet1/0/1] -----------
 OAM timers
   Hello timer       : 500 milliseconds
   Keepalive timer    : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window          : 100 x 1000000 symbols
     Threshold       : 1 error symbols
   Errored frame
     Window          : 10 x 100 milliseconds
     Threshold       : 1 error frames
   Errored frame period
```

```
  Window          : 1000 x 10000 frames
  Threshold       : 1 error frames
Errored frame seconds
  Window          : 600 x 100 milliseconds
  Threshold       : 1 error seconds
```

表 1-3 コマンド出力

フィールド	説明
Global	グローバルの情報です。
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
OAM timers	Ethernet OAM接続検出タイマです。
Hello timer	Ethernet OAMハンドシェークパケットの転送間隔です。
Keepalive timer	Ethernet OAM接続タイムアウトタイマです。
Link monitoring	リンクイベント検出数としきい値です。
Errored symbol period	エラーシンボルイベントです。
Errored frame	エラーフレームイベントです。
Errored frame period	エラーフレーム期間イベントです。
Errored frame seconds	エラーフレーム秒イベントです。
Window	リンクイベントで設定された検出数です。
Threshold	リンクイベントで設定されたトリガとなるしきい値です。

1.1.3 display oam critical-event

Syntax

display oam critical-event [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、装置のすべてのポートで発生したクリティカルな Ethernet OAM リンクイベントの統計情報を表示します。

説明

display oam critical-event コマンドはポートでのクリティカルな Ethernet OAM リンクイベントの統計情報を表示します。

例

すべてのポートで発生したクリティカルな Ethernet OAM リンクイベントの統計情報を表示します。

<Switch> display oam critical-event

```
----------- [GigabitEthernet1/0/1] -----------
 Local link status   : UP
 Event statistics
   Link fault       : Not occurred
   Dying gasp       : Not occurred
   Critical event    : Not occurred
```

表 1-4 コマンド出力

フィールド	説明
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
Local link status	ローカルリンクの状態です。UPあるいはDOWNがあります。
Event statistics	クリティカルなEthernet OAMリンクイベントの統計情報です。
Link fault	リンクエラーがあるかどうかを示します。
Dying Gasp	致命的なエラーがあるかどうかを示します。
Critical Event	クリティカルエラーがあるかどうかを示します。

1.1.4 display oam link-event

Syntax

display oam link-event { **local** | **remote** } [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

local: ローカル装置を指定します。

remote: ピアの終端を指定します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのローカルポートおよびリモートポートの Ethernet OAM リンクエラーイベントの統計情報を表示します。

説明

display oam link-event コマンドはローカルポートあるいはリモートポートで発生した Ethernet OAM リンクエラーイベントの統計情報を表示します。

Ethernet OAM リンクエラーイベントは、エラーシンボルイベント、エラーフレームイベント、エラーフレーム期間イベント、エラーフレーム秒イベントを含みます。

例

すべてのローカルポートの Ethernet OAM リンクエラーイベントの統計情報を表示します。

<Switch> display oam link-event local

```
----------- [GigabitEthernet1/0/1] -----------
 Link status: UP
 OAM local errored symbol event
   Event time stamp        : 35498 x 100 milliseconds
   Errored symbol window    : 100000000 symbols
   Errored symbol threshold : 1 error symbols
   Errored symbol          : 1 error symbols
   Error running total     : 4 error symbols
   Event running total     : 4 events
 OAM local errored frame event
   Event time stamp       : 49582 x 100 milliseconds
   Errored frame window    : 10 x 100 milliseconds
   Errored frame threshold : 1 error frames
   Errored frame          : 1 error frames
   Error running total     : 6 error frames
   Event running total     : 6 events
 OAM local errored frame period event
   Event time stamp              : 16382 x 100 milliseconds
   Errored frame period window    : 10000000 frames
   Errored frame period threshold  : 1 error frames
```

```
  Errored frame period          : 1 error frames
  Error running total           : 5 error frames
  Event running total           : 5 events
 OAM local errored frame seconds summary event
  Event time stamp             : 50022 x 100 milliseconds
  Errored frame seconds window    : 600 x 100 milliseconds
  Errored frame seconds threshold : 1 error seconds
  Errored frame seconds         : 1 error seconds
  Error running total           : 1 error seconds
  Event running total           : 1 events
```

すべてのリモートポートの Ethernet OAM リンクエラーイベントの統計情報を表示します。

<Switch> display oam link-event remote

```
----------- [GigabitEthernet1/0/1] -----------
 Link status: UP
 OAM remote errored symbol event
  Event time stamp        : 35498 x 100 milliseconds
  Errored symbol window    : 100000000  symbols
  Errored symbol threshold : 1 error symbols
  Errored symbol          : 1 error symbols
  Error running total     : 4 error symbols
  Event running total     : 4 events
 OAM remote errored frame event
  Event time stamp       : 49582 x 100 milliseconds
  Errored frame window    : 10 x 100 milliseconds
  Errored frame threshold : 1 error frames
  Errored frame          : 1 error frames
  Error running total     : 6 error frames
  Event running total     : 6 events
 OAM remote errored frame period event
  Event time stamp             : 16382 x 100 milliseconds
  Errored frame period window    : 10000000 frames
  Errored frame period threshold  : 1 error frames
  Errored frame period          : 1 error frames
  Error running total           : 5 error frames
  Event running total           : 5 events
 OAM remote errored frame seconds summary event
  Event time stamp             : 50022 x 100 milliseconds
  Errored frame seconds window    : 600 x 100 milliseconds
  Errored frame seconds threshold : 1 error seconds
  Errored frame seconds         : 1 error seconds
  Error running total           : 1 error seconds
```

```
Event running total          : 1 events
```

表 1-5 コマンド出力

フィールド	説明
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
Link status	ローカルリンクの状態です。UPあるいはDOWNがあります。
OAM local/remote errored symbol event	リモートポートのエラーシンボルイベントの情報です。（エラーシンボルイベントが発生したときのみ有効です。） ● **Event time stamp**—エラーシンボルイベントが発生した時間です。 ● **Errored symbol window**—エラーシンボルの検出間隔です。 ● **Errored symbol threshold**—エラーシンボルイベントのトリガが発生したエラーのしきい値です。 ● **Errored symbol**—最新のエラーシンボルイベントが検出されたシンボル数です。 ● **Error running total**—エラーシンボルの総数です。 ● **Event running total**—発生したエラーシンボルイベントの総数です。
OAM local/remote errored frame event	ローカルポート、リモートポートのエラーフレームイベントの情報です。（エラーフレームイベントが発生したときのみ有効です。） ● **Event time stamp**—エラーフレームイベントが発生した時間です。 ● **Errored frame window**—エラーフレームの検出間隔です。 ● **Errored frame threshold**—エラーフレームイベントのトリガが発生したエラーのしきい値です。 ● **Errored frame**—最新のエラーフレームイベントが検出されたエラーフレーム数です。 ● **Error running total**—エラーフレームの総数です。 ● **Event running total**—発生したエラーフレームイベントの総数です。

フィールド	説明
OAM local/remote errored frame period event	ローカルポート、リモートポートのエラーフレーム期間イベントの情報です。（エラーフレーム期間イベントが発生したときのみ有効です。） • **Event time stamp**—エラーフレーム期間イベントが発生した時間です。 • **Errored frame period window**—エラーフレーム期間の検出間隔です。 • **Errored frame period threshold**—エラーフレーム期間イベントのトリガが発生したエラーのしきい値です。 • **Errored frame period**—最新のエラーフレーム期間イベントが検出されたエラーフレーム数です。 • **Error running total**—エラーフレーム期間の総数です。 • **Event running total**—発生したエラーフレーム期間イベントの総数です。
OAM local/remote errored frame seconds summary event	ローカルポート、リモートポートのエラーフレーム秒イベントの情報です。（エラーフレーム秒イベントが発生したときのみ有効です。） • **Event time stamp**—エラーフレーム秒イベントが発生した時間です。 • **Errored frame second window**—エラーフレーム秒の検出間隔です。 • **Errored Frame seconds threshold**—エラーフレーム秒イベントのトリガが発生したエラーのしきい値です。 • **Errored frame seconds**—最新のエラーフレーム秒イベントが検出されたエラーフレーム秒数です。 • **Error running total**—エラーフレーム秒の総数です。 • **Event running total**—発生したエラーフレーム秒イベントの総数です。

関連コマンド

reset oam

1.1.5 oam enable

Syntax

oam enable

undo oam enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

oam enable コマンドは Ethernet OAM を有効にします。

undo oam enable コマンドは Ethernet OAM を無効にします。

例

GigabitEthernet 1/0/1 で Ethernet OAM を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam enable

1.1.6 oam errored-frame threshold

Syntax

oam errored-frame threshold *threshold-value*

undo oam errored-frame threshold

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレームイベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam errored-frame threshold コマンドはポートでエラーフレームイベントのトリガが発生するしきい値を設定します。

undo oam errored-frame threshold コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレームイベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame threshold**

1.1.7 oam errored-frame window

Syntax

oam errored-frame window *window-value*

undo oam errored-frame window

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレームイベントの検出間隔を指定します。設定範囲は 10～600 です。単位は 1/10 秒（100 ミリ秒）です。

説明

oam errored-frame window コマンドはエラーフレームイベントの検出間隔を設定します。

undo oam errored-frame window コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレームイベントの検出間隔を 20（2000 ミリ秒）に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame window 20

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame window**

1.1.8 oam errored-frame-period threshold

Syntax

oam errored-frame-period threshold *threshold-value*

undo oam errored-frame-period threshold

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレーム期間イベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam errored-frame-period threshold コマンドはポートでエラーフレーム期間イベントのトリガが発生するしきい値を設定します。

undo oam errored-frame-period threshold コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレーム期間イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame-period threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame-period threshold**

1.1.9 oam errored-frame-period window

Syntax

oam errored-frame-period window *window-value*

undo oam errored-frame-period window

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレーム期間イベントの検出数を指定します。設定範囲は 1～65535 です。検出数は *window-value* の 10000 倍の値です。

説明

oam errored-frame-period window コマンドはエラーフレーム期間イベントの検出数を設定します。

undo oam errored-frame-period window コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレーム期間イベントの検出数を 20000000 に指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame-period window 2000

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame-period window**

1.1.10 oam errored-frame-seconds threshold

Syntax

oam errored-frame-seconds threshold *threshold-value*

undo oam errored-frame-seconds threshold

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレーム秒イベントのトリガが発生するしきい値を指定します。設定範囲は 0～900 です。

説明

oam errored-frame-seconds threshold コマンドはポートでエラーフレーム秒イベントのトリガが発生するしきい値を設定します。

undo oam errored-frame-seconds threshold コマンドはデフォルトに戻します。

エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間（秒）より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレーム秒イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame-seconds threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds window**
- **oam global errored-frame-seconds threshold**

1.1.11 oam errored-frame-seconds window

Syntax

oam errored-frame-seconds window *window-value*

undo oam errored-frame-seconds window

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレームイベントの検出間隔を指定します。設定範囲は 100～9000 です。単位は 1/10 秒（100 ミリ秒）です。

説明

oam errored-frame-seconds window コマンドはエラーフレーム秒イベントの検出間隔を設定します。

undo oam errored-frame-seconds window コマンドはデフォルトに戻します。

エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間（秒）より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレーム秒イベントの検出間隔を 100（10000 ミリ秒）に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame-seconds window 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds threshold**

1.1.12 oam errored-symbol-period threshold

Syntax

oam errored-symbol-period threshold *threshold-value*

undo oam errored-symbol-period threshold

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーシンボル期間イベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam errored-symbol-period threshold コマンドはエラーシンボル期間イベントのトリガが発生するしきい値を設定します。

undo oam errored-symbol-period threshold コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーシンボル期間イベントのトリガが発生するしきい値を 100 に指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-symbol-period threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-symbol-period threshold**

1.1.13 oam errored-symbol-period window

Syntax

oam errored-symbol-period window *window-value*

undo oam errored-symbol-period window

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーシンボル期間イベントの検出数を指定します。設定範囲は 1～65535 です。検出数は *window-value* の 1,000,000 倍の値です。

説明

oam errored-symbol-period window コマンドはエラーシンボル期間イベントの検出数を設定します。

undo oam errored-symbol-period window コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーシンボル期間イベントの検出数を 200,000,000 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-symbol-period window 200

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-symbol-period window**

1.1.14 oam global errored-frame threshold

Syntax

oam global errored-frame threshold *threshold-value*

undo oam global errored-frame threshold

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレームイベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam global errored-frame threshold コマンドはグローバルでエラーフレームイベントのトリガが発生するしきい値を設定します。

undo oam global errored-frame threshold コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレームイベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] oam global errored-frame threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame threshold**

1.1.15 oam global errored-frame window

Syntax

oam global errored-frame window *window-value*

undo oam global errored-frame window

デフォルト

10（1000 ミリ秒）

View

System view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレームイベントの検出間隔を指定します。設定範囲は 10～600 です。単位は 1/10 秒（100 ミリ秒）です。

説明

oam global errored-frame window コマンドはグローバルでエラーフレームイベントの検出間隔を設定します。

undo oam global errored-frame window コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレームイベントの検出間隔を 20（2000 ミリ秒）に設定します。

<Switch> system-view

[Switch] oam global errored-frame window 20

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame window**

1.1.16 oam global errored-frame-period threshold

Syntax

oam global errored-frame-period threshold *threshold-value*

undo oam global errored-frame-period threshold

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレーム期間イベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam global errored-frame-period threshold コマンドはグローバルでエラーフレーム期間イベントのトリガが発生するしきい値を設定します。

undo oam global errored-frame-period threshold コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム期間イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] oam global errored-frame-period threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-period threshold**

1.1.17 oam global errored-frame-period window

Syntax

oam global errored-frame-period window *window-value*

undo oam global errored-frame-period window

デフォルト

10000000

View

System view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレーム期間イベントの検出数を指定します。設定範囲は 1～65535 です。検出数は *window-value* の 10000 倍の値です。

説明

oam global errored-frame-period window コマンドはグローバルでエラーフレーム期間イベントの検出数を設定します。

undo oam global errored-frame-period window コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム期間イベントの検出数を 20000000 に指定します。

<Switch> system-view

[Switch] oam global errored-frame-period window 2000

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-period window**

1.1.18 oam global errored-frame-seconds threshold

Syntax

oam global errored-frame-seconds threshold *threshold-value*

undo oam global errored-frame-seconds threshold

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレーム秒イベントのトリガが発生するしきい値を指定します。設定範囲は 0～900 です。

説明

oam global errored-frame-seconds threshold コマンドはグローバルでエラーフレーム秒イベントのトリガが発生するしきい値を設定します。

undo oam global errored-frame-seconds threshold コマンドはデフォルトに戻します。

エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間（秒）より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム秒イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] oam global errored-frame-seconds threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds threshold**
- **oam global errored-frame-seconds window**

1.1.19 oam global errored-frame-seconds window

Syntax

oam global errored-frame-seconds window *window-value*

undo oam global errored-frame-seconds window

デフォルト

600（60000 ミリ秒）

View

System view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレーム秒イベントの検出間隔を指定します。設定範囲は 100～9000 です。単位は 1/10 秒（100 ミリ秒）です。

説明

oam global errored-frame-seconds window コマンドはグローバルでエラーフレーム秒イベントの検出間隔を設定します。

undo oam global errored-frame-seconds window コマンドはデフォルトに戻します。

エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間（秒）より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム秒イベントの検出間隔を 100（10000 ミリ秒）に設定します。

<Switch> system-view

[Switch] oam global errored-frame-seconds window 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame-seconds threshold**

1.1.20 oam global errored-symbol-period threshold

Syntax

oam global errored-symbol-period threshold *threshold-value*

undo oam global errored-symbol-period threshold

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーシンボル期間イベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam global errored-symbol-period threshold コマンドはエラーシンボル期間イベントのトリガが発生するしきい値を設定します。

undo oam global errored-symbol-period threshold コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーシンボル期間イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] oam global errored-symbol-period threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-symbol-period threshold**

1.1.21 oam global errored-symbol-period window

Syntax

oam global errored-symbol-period window *window-value*

undo oam global errored-symbol-period window

デフォルト

100,000,000

View

System view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーシンボル期間イベントの検出数を指定します。設定範囲は 1～65535 です。検出数は *window-value* の 1,000,000 倍の値です。

説明

oam global errored-symbol-period window コマンドはグローバルでエラーシンボル期間イベントの検出数を設定します。

undo oam global errored-symbol-period window コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーシンボル期間イベントの検出数を 200,000,000 に設定します。

<Switch> system-view

[Switch] oam global errored-symbol-period window 200

関連コマンド

- **display oam configuration**

- **display oam link-event**
- **oam global errored-symbol-period window**

1.1.22 oam global timer hello

Syntax

oam global timer hello *interval*

undo oam global timer hello

デフォルト

1000 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: Ethernet OAM ハンドシェークパケットを転送する間隔を指定します。設定範囲は 500～5000 ミリ秒です。100 ミリ秒単位で指定します。

説明

oam global timer hello コマンドはグローバルの Ethernet OAM ハンドシェークパケットを転送する間隔を設定します。

undo oam global timer hello コマンドはデフォルトに戻します。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

Ethernet OAM ハンドシェークパケットを転送する間隔を 600 ミリ秒に設定します。

<Switch> system-view

[Switch] oam global timer hello 600

関連コマンド

- **display oam configuration**

- **oam timer hello**

1.1.23 oam global timer keepalive

Syntax

oam global timer keepalive *interval*

undo oam global timer keepalive

デフォルト

5000 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: Ethernet OAM 接続のタイムアウトタイマを指定します。設定範囲は 1000～25000 ミリ秒です。100 ミリ秒単位で指定します。

説明

oam global timer keepalive コマンドは Ethernet OAM 接続のタイムアウトタイマを設定します。

undo oam global timer keepalive コマンドはデフォルトに戻します。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

Ethernet OAM 接続のタイムアウトタイマを 6000 ミリ秒に設定します。

<Switch> system-view

[Switch] oam global timer keepalive 6000

関連コマンド

- **display oam configuration**
- **oam timer keepalive**

1.1.24 oam mode

Syntax

oam mode { **active** | **passive** }

undo oam mode

デフォルト

アクティブ

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

active: アクティブ Ethernet OAM モードを指定します。

passive: パッシブ Ethernet OAM モードを指定します。

説明

oam mode コマンドは Ethernet OAM モードを設定します。

undo oam mode コマンドはデフォルトに戻します。

Ethernet OAM が有効なポートで Ethernet OAM モードを変更する場合、最初にポートで Ethernet OAM を無効にする必要があります。

例

GigabitEthernet 1/0/1 で Ethernet OAM を無効にし、Ethernet OAM モードをパッシブで動作するように設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo oam enable

[Switch-GigabitEthernet1/0/1] oam mode passive

関連コマンド

oam enable

1.1.25 oam remote-failure action

Syntax

oam remote-failure { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**

undo oam remote-failure { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**

デフォルト

ポートはリモートエンドからの Ethernet OAM イベントのみログを行います。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

connection-expired: 接続タイムアウト障害を指定します。

critical-event: 重大な障害を指定します。

dying-gasp: 致命的な障害を指定します。

link-fault: リンク障害を指定します。

error-link-down: OAM 接続を終了し、ポートのリンク状態をダウンに設定します。

説明

oam remote-failure action コマンドはリモートエンドから Ethernet OAM イベントを受信後にポートがとる行動を設定します。

undo oam remote-failure action コマンドはデフォルトに設定を戻します。

例

リモートエンドか致命的な障害を受信後に、OAM 接続を終わらせるよう GigabitEthernet 1/0/1 に設定し、ポートのリンクをダウンにします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam remote-failure critical-event action error-link-down

1.1.26 oam remote-loopback

Syntax

oam remote-loopback start

oam remote-loopback stop

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

oam remote-loopback start コマンドは指定されたポートで Ethernet OAM リモートループバックを有効にします。

oam remote-loopback stop コマンドはポートの Ethernet OAM リモートループバックを無効にします。

Ethernet OAM リモートループバックは、Ethernet OAM 接続が確立され、Ethernet OAM エンティティがアクティブ Ethernet OAM モードであるときのみ実行可能です。

user view あるいは system view で指定されたポート、あるいは port view で指定された現在のポート上で Ethernet OAM リモートループバックを有効にすることができます。これらのポートで行われた設定は同一の効果が適用されます。

例

アクティブ Ethernet OAM モードを設定し、GigabitEthernet 1/0/1 で Ethernet OAM を有効にします。GigabitEthernet 1/0/1 で Ethernet OAM リモートループバックを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam mode active

[Switch-GigabitEthernet1/0/1] oam enable

[Switch-GigabitEthernet1/0/1] oam remote-loopback start

関連コマンド

- **oam enable**
- **oam mode**
- **oam remote-loopback interface**

1.1.27 oam remote-loopback interface

Syntax

oam remote-loopback start interface *interface-type interface-number*

oam remote-loopback stop interface *interface-type interface-number*

デフォルト

無効

View

User view

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ポートのタイプと番号を指定します。

説明

oam remote-loopback start interface コマンドはポートで Ethernet OAM リモートループバックを有効にします。

oam remote-loopback stop interface コマンドはポートで Ethernet OAM リモートループバックを無効にします。

Ethernet OAM リモートループバックは、Ethernet OAM 接続が確立され、Ethernet OAM エンティティがアクティブ Ethernet OAM モードであるときのみ実行可能です。

user view あるいは system view で指定されたポート、あるいは port view で指定された現在のポート上で Ethernet OAM リモートループバックを有効にすることができます。これらのポートで行われた設定は同一の効果が適用されます。

例

アクティブ Ethernet OAM モードを設定し、GigabitEthernet 1/0/1 で Ethernet OAM を有効にします。system view で GigabitEthernet 1/0/1 の Ethernet OAM リモートループバックを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam mode active

[Switch-GigabitEthernet1/0/1] oam enable

[Switch-GigabitEthernet1/0/1] quit

[Switch] oam remote-loopback start interface gigabitethernet 1/0/1

関連コマンド

- **oam enable**
- **oam mode**
- **oam remote-loopback**

1.1.28 oam remote-loopback reject-request

Syntax

oam remote-loopback reject-request

undo oam remote-loopback reject-request

デフォルト

リモートポートからの Ethernet OAM リモートループバック要求を拒否しません。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

oam remote-loopback reject-request コマンドはリモートポートからの Ethernet OAM リモートループバック要求を拒否するように設定します。

undo oam remote-loopback reject-request コマンドはデフォルトに戻します。

oam remote-loopback reject-request コマンドを実行したときポートがループバックである場合、設定は次回のループバックを開始したときに適用されます。

例

GigabitEthernet 1/0/1 でリモートポートからの Ethernet OAM リモートループバック要求を拒否するように設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam remote-loopback reject-request

1.1.29 oam timer hello

Syntax

oam timer hello *interval*

undo oam timer hello

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: Ethernet OAM ハンドシェークパケットを転送する間隔を指定します。設定範囲は 500～5000 ミリ秒です。100 ミリ秒単位で指定します。

説明

oam timer hello コマンドは Ethernet OAM ハンドシェークパケットを転送する間隔を設定します。

undo oam timer hello コマンドはデフォルトに戻します。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 で Ethernet OAM ハンドシェークパケットを転送する間隔を 600 ミリ秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam timer hello 600

関連コマンド

- **display oam configuration**
- **oam global timer hello**

1.1.30 oam timer keepalive

Syntax

oam timer keepalive *interval*

undo oam timer keepalive

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: Ethernet OAM 接続のタイムアウトタイマを指定します。設定範囲は 1000～25000 ミリ秒です。100 ミリ秒単位で指定します。

説明

oam timer keepalive コマンドは Ethernet OAM 接続のタイムアウトタイマを設定します。

undo oam timer keepalive コマンドはデフォルトに戻します。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 で Ethernet OAM 接続のタイムアウトタイマを 6000 ミリ秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam timer keepalive 6000

関連コマンド

- **display oam configuration**
- **oam global timer keepalive**

1.1.31 reset oam

Syntax

reset oam [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートの Ethernet OAM パケットの統計情報とリンクエラーイベントを削除します。

説明

reset oam コマンドはポートの Ethernet OAM パケットの統計情報とリンクエラーイベントを削除します。

例

すべてのポートの Ethernet OAM パケットの統計情報とリンクエラーイベントを削除します。

<Switch> reset oam

関連コマンド

- **display oam**
- **display oam link-event**

目次

このセクションのページは **9-x-x** です。

2 章 CFD.....2-1
2.1 CFD 設定コマンド.....2-1
2.1.1 cfd cc enable.....2-1
2.1.2 cfd cc interval.....2-2
2.1.3 cfd enable.....2-3
2.1.4 cfd linktrace.....2-4
2.1.5 cfd linktrace auto-detection.....2-5
2.1.6 cfd loopback.....2-6
2.1.7 cfd md.....2-8
2.1.8 cfd mep.....2-9
2.1.9 cfd meplist.....2-11
2.1.10 cfd mip-rule.....2-12
2.1.11 cfd service-instance.....2-13
2.1.12 display cfd linktrace-reply.....2-15
2.1.13 display cfd linktrace-reply auto-detection.....2-16
2.1.14 display cfd md.....2-18
2.1.15 display cfd mep.....2-19
2.1.16 display cfd meplist.....2-23
2.1.17 display cfd mp.....2-23
2.1.18 display cfd remote-mep.....2-25
2.1.19 display cfd service-instance.....2-26
2.1.20 display cfd status.....2-28

2章 CFD

2.1 CFD設定コマンド

2.1.1 cfd cc enable

Syntax

cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。

説明

cfd cc enable コマンドは指定した MEP で CCM の送信を有効にします。

undo cfd cc enable コマンドは指定した MEP で CCM の送信を無効にします。

コマンドを使用するとき以下のガイドラインに従ってください。

- Ethernet interface view で設定されたコマンドは、Ethernet インタフェースでのみ適用されます。
- aggregate interface view で設定されたコマンドは、アグリゲートインタフェースとアグリゲーションメンバポートでのみ適用されます。
- MEP が VLAN 属性を持たない MA に属している場合、アグリゲーショングループ view のメンバポートに対する設定は、現在のメンバポートに対してのみ有効になります。
- MEP が VLAN 属性を持つ MA に属している場合、アグリゲーショングループのメンバポートでの設定は、メンバポートがアグリゲーショングループを出るときにのみ有効になります。

例

GigabitEthernet 1/0/1 において Ethernet サービスインスタンス 5 の MEP3 で CCM の送信を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] cfd cc service-instance 5 mep 3 enable

関連コマンド

cfd cc interval

2.1.2 cfd cc interval

Syntax

cfd cc interval *interval-value* **service-instance** *instance-id*

undo cfd cc interval [*interval-value*] **service-instance** *instance-id*

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: CCM メッセージの interval フィールドの値を指定します。設定範囲は 1～7 です。値を 1 あるいは 2 に設定すると、ハードウェアの制約により連続性チェックが正しく動作しない場合があります。

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

説明

cfd cc interval コマンドは CCM メッセージの interval フィールドの値を設定します。

undo cfd cc interval コマンドは CCM メッセージの interval フィールドの値を削除します。

CCM メッセージの interval フィールドの値を設定するとき、表 2-1 に示す値を使用します。

表 2-1 CCM interval フィールドの変換

CCM interval フィールドの値	CCM の送信間隔	最大 CCM ライフタイム
1	10/3ミリ秒	35/3ミリ秒
2	10ミリ秒	35ミリ秒
3	100ミリ秒	350ミリ秒
4	1秒	3.5秒
5	10秒	35秒
6	60秒	210秒
7	600秒	2100秒

例

Ethernet サービスインスタンス 2 の CCM メッセージの interval フィールドの値を 3 に設定します。

<Switch> system-view

[Switch] cfd cc interval 3 service-instance 2

関連コマンド

cfd cc enable

2.1.3 cfd enable

Syntax

cfd enable

undo cfd enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

cfd enable コマンドは CFD を有効にします。

undo cfd enable コマンドは CFD を無効にします。

例

CFD を有効にします。

<Switch> system-view

[Switch] cfd enable

2.1.4 cfd linktrace

Syntax

cfd linktrace service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**ttl** *ttl-value*] [**hw-only**]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

mep *mep-id*: 送信元 MEP の ID を指定します。設定範囲は 1～8191 です。

target-mac *mac-address*: 宛先 MAC アドレスを指定します。形式は H-H-H です。

target-map *target-mep-id*: 宛先 MEP の ID を指定します。設定範囲は 1～8191 です。

ttl *ttl-value*: TTL(time to live)の値を指定します。設定範囲は 1～255 です。デフォルトは 64 です。

hw-only: LTM が送信する hw-only ビットを設定します。hw-only を指定した場合、MIP は未知の宛先 MAC アドレスの LTM メッセージをフラッディングしません。

説明

cfd linktrace コマンドは送信元 MEP と宛先 MP 間の経路を検索します。経路の検出は、2 つの MEP 間における LTM の送信と、受信 LTR の検出を通じて行われます。

例

Ethernet サービスインスタンス 1 の送信元 MEP1101 と宛先 MEP2001 間の経路を定義します。

<Switch> cfd linktrace service-instance 1 mep 1101 target-mep 2001

```
Linktrace to MEP 2001 with the sequence number 1101-43361:
MAC Address             TTL    Last MAC        Relay Action
0010-fc00-6512           63     0010-fc00-6500   Hit
```

表 2-2 コマンド出力

フィールド	説明
Linktrace to MEP 2001 with the sequence number 1101-43361	宛先MEP2001をシーケンス番号1101-43361に関連づけます。
MAC Address	LTRメッセージの送信元MACアドレスです。
TTL	LTMが装置を通過するときのTTLの値です。
Last MAC	LTMメッセージの最終ホップの装置のMACアドレスです。
Relay Action	転送する装置がMACアドレステーブルから宛先MACアドレスを検出したかどうかを示します。 CFDの標準バージョン（IEEE 802.1ag）が使用されたとき、以下のことを示します。 • **Hit**—現在の装置は宛先装置です。 • **FDB**—転送する装置は宛先MACアドレスを検出しました。 • **MPDB**—宛先MACアドレスが見つかりませんでした。あるいは、MEPまたはMIPデータベースに宛先MACアドレスが検出されました。

関連コマンド

- **cfd linktrace auto-detection**
- **display cfd linktrace-reply**

2.1.5 cfd linktrace auto-detection

Syntax

cfd linktrace auto-detection [**size** *size-value*]

undo cfd linktrace auto-detection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

size *size-value*: 自動検出結果を保存するために使用するバッファサイズを指定します。設定範囲は 1～100(自動検出の回数)です。最新の自動検出の結果を保存するバッファサイズのデフォルトは 5 です。

説明

cfd linktrace auto-detection コマンドは linktrace メッセージ（LT メッセージ）を自動で送信することを有効にします。

undo cfd linktrace auto-detection コマンドは linktrace メッセージを自動で送信することを無効にします。

LT メッセージを自動で送信することを有効にしたのち、送信元 MEP が 3.5 回送信する間にターゲット MEP からの CCM フレームを受信しなれば、2 つの間のリンクは故障していると考えられ、LTM フレーム（LTM の宛先が宛先 MEP で、TTL は 255 です）が送信されます。MIP が応答した LTR にもとづいて、障害場所の特定ができます。

linktrace メッセージを自動で送信することを無効にすると、バッファ内の内容は削除されます。

例

LT メッセージを自動で送信することを有効にし、自動検出結果を保存するために使用するバッファサイズを 100 に指定します。

<Switch> system-view

[Switch] cfd linktrace auto-detection size 100

関連コマンド

- **cfd linktrace**
- **display cfd linktrace-reply auto-detection**

2.1.6 cfd loopback

Syntax

cfd loopback service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

mep *mep-id*: 送信元 MEP の ID を指定します。設定範囲は 1～8191 です。

target-mac *mac-address*: MP の宛先 MAC アドレスを指定します。形式は H-H-H です。

target-mep *target-mep-id*: 宛先 MEP の ID を指定します。設定範囲は 1～8191 です。

number *number*: LBM パケットを送信する数を指定します。設定範囲は 1～10 です。デフォルトは 5 です。

説明

cfd loopback コマンドはループバック(LB) 機能を有効にします。LB 機能は、LBM および LBR を使用して、送信元 MEP と宛先 MP 間のリンク接続を検証します。

例

Ethernet サービスインスタンス 1 の MEP1101 と MEP2001 間のリンク状態を確認するように LB を有効にします。（リンク状態が正常であると仮定します。）

<Switch> cfd loopback service-instance 1 mep 1101 target-mep 2001

```
Loopback to MEP 2001 with the sequence number start from 1101-43404:
Reply from 0010-fc00-6512: sequence number=1101-43404 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43405 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43406 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43407 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43408 Time=5ms
Sent: 5       Received: 5       Lost: 0
```

Ethernet サービスインスタンス 1 の MEP1101 と MEP2001 間のリンク状態を確認するように LB を有効にします。（リンク状態が異常であると仮定します）

<Switch> cfd loopback service-instance 1 mep 1101 target-mep 2001

```
Loopback to MEP 2001 with the sequence number start from 1101-43404:
Sent: 5       Received: 0       Lost: 5
```

表 2-3 コマンド出力

フィールド	説明
Loopback to MEP 2001 with the sequence number start from 1101-43404	1101-43404で始まるシーケンス番号でリモートMEP2001にLBMを送信します。
Reply from 0010-fc00-6512	MACアドレス0010-FC00-6512のMPからの応答です。

フィールド	説明
sequence number	LBRメッセージのシーケンス番号です。
Time=5ms	LBMメッセージが送信されてからLBRを受信するまでの間隔が5ミリ秒です。
Sent	LBMを送信した数です。
Received	LBRメッセージを受信した数です。
Lost	ロストLBRの数です。

2.1.7 cfd md

Syntax

cfd md *md-name* [**index** *index-value*] **level** *level-value* [**md-id** { **dns** *dns-name* | **mac** *mac-address subnumber* | **none** }]

undo cfd md *md-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

md *md-name*: MD の名前を指定します。設定範囲は 1～43 です。英字、数字、以下の記号を含むことができます。アポストロフィー（'）、チルダ（~）、感嘆符（!）、アットマーク（@）、シャープ（#）、ドル記号（$）、パーセント（%）、キャレット（^）、アンパサンド（&）、アスタリスク（*）、括弧（{ },( ),[ ],< >）、ハイフン（-）、アンダーライン（_）、プラス（+）、イコール（=）、垂直バー（|）、コロン（:）、セミコロン（;）、バッククォート（`）、コンマ（,）、ドット（.）、スラッシュ（/）

index *index-value*: MD インデックスを指定します。設定範囲は 1～4294967295 です。指定しない場合、使用されていないインデックスのもっとも小さい番号が自動的に割り当てられます。システムが自動で割り当てるインデックスを使用することを推奨します。

level *level-value*: MD レベルを指定します。設定範囲は 0～7 です。

md-id: MEP が送信したパケットによって運ばれる MD 名を指定します。指定しない場合、MD 名は *md-name* となります。

dns *dns-name*: DNS 名の形式で MD 名を指定します。*dns-name* は DNS 名を示します。

mac *mac-address subnumber*: MAC アドレスと整数から構成される MD 名を指定します。*mac-address* は MD の MAC アドレスを示します。*subnumber* の設定範囲は 0～65535 です。

none: MEP によって送信されたパケットに MD 名が運ばれないように設定します。

説明

cfd md コマンドは MD を作成します。

undo cfd md コマンドは MD を削除します。

MD 名は IEEE802.1ag-2007 の表 21-19 に準拠する必要があります。

指定レベルで 1 つの MD を作成することができます。不正な MD 名あるいは既存の MD 名を指定した場合、MD を作成することができません。また MD インデックスが使用中である場合、MD を作成することができません。

MD を削除するとき、MD に関連する設定も削除されます。

例

MD レベルが 3 の MD 名 **test_md1** を作成します。

<Switch> system-view

[Switch] cfd md test_md1 level 3

MD 名 **test_md2** を作成し、MEP が送信したパケットによって運ばれる MD 名を MAC アドレス 1-1-1、整数 1 で設定します。

<Switch> system-view

[Switch] cfd md test_md2 level 5 md-id mac 1-1-1 1

2.1.8 cfd mep

Syntax

cfd mep *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }

undo cfd mep *mep-id* **service-instance** *instance-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

inbound: 内側向きの MEP を作成します。

outbound: 外側向きの MEP を作成します。

説明

cfd mep コマンドは MEP を作成します。

undo cfd mep コマンドは指定された MEP を削除します。

MEP を作成する際、指定した Ethernet サービスインスタンスは、MEP が属している MD と MA を定義します。

MEP ID が関連する Ethernet サービスインスタンスの MEP リストに含まれていない場合、MEP を作成することはできません。

コマンドを使用するとき以下のガイドラインに従ってください。

- Ethernet interface view で設定されたコマンドは、Ethernet インタフェースでのみ適用されます。
- aggregate interface view で設定されたコマンドは、現在のアグリゲートインタフェースでのみ適用されます。
- MEP が VLAN 属性を持たないでいる MA に属している場合、アグリゲーショングループのメンバポートの設定は現在のメンバポートでのみ適用されます。
- MEP が VLAN 属性を持っている MA に属している場合、アグリゲーショングループのメンバポートの設定はメンバポートをアグリゲーショングループから削除したときのみ適用されます。

例

Ethernet サービスインスタンス 5 に MEP リストを設定し、GigabitEthernet 1/0/1 で Ethernet サービスインスタンス 5 の内側向きの MEP3 を作成します。

<Switch> system-view

[Switch] cfd md test_md level 3

[Switch] cfd service-instance 5 ma-id vlan-based md test_md vlan 100

[Switch] cfd meplist 3 service-instance 5

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] cfd mep 3 service-instance 5 outbound

関連コマンド

cfd meplist

2.1.9 cfd meplist

Syntax

cfd meplist *mep-list* **service-instance** *instance-id*

undo cfd meplist *mep-list* **service-instance** *instance-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

meplist *mep-list*: 最大 10 個の MEP ID あるいは *mep-list* = { *mep-id* [**to** *mep-id*] }&<1-10> という形式の MEP ID 範囲のリストを指定します。各項目は MEP ID あるいは MEP ID の範囲を mep-id1 から mep-id2 の形式で指定します。*mep-id* は MEP ID を示し、設定範囲は 1～8191 です。mep-id2 は、mep-id1 以上である必要があります。

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

説明

cfd meplist コマンドは MEP リストを作成します。

undo cfd meplist コマンドは既存の MEP リストを削除します。

MEP リストは、設定が許可されているローカル MEP と、同じ MA で監視されるリモート MEP の集合です。

MEP リストを作成する前に、関連する MD、MA、Ethernet サービスインスタンスを作成してください。

MEP リストを削除したのち、MEP リストをもとにしたすべてのローカルの MEP の設定が削除されます。

例

Ethernet サービスインスタンス 5 の MEP9～MEP15 が含まれる MEP リストを作成します。

<Switch> system-view

[Switch] cfd md test_md level 3

[Switch] cfd service-instance 5 ma-id vlan-based md test_md vlan 100

[Switch] cfd meplist 9 to 15 service-instance 5

関連コマンド

- **cfd md**
- **cfd service-instance**

2.1.10 cfd mip-rule

Syntax

cfd mip-rule { **default** | **explicit** } **service-instance** *instance-id*

undo cfd mip-rule [**default** | **explicit**] **service-instance** *instance-id*

デフォルト

MIP を作成するルールは設定されていません。システムは自動で MIP を作成しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

default: デフォルトルールを指定します。インタフェースで低レベルの MIP が存在しない場合、現在のレベルで MIP が作成されます。インタフェースで MEP が設定されていない場合でも MIP が作成されます。

explicit: 明示ルールを指定します。インタフェースで低レベルの MIP が存在しない場合、現在のレベルで MIP が作成されます。インタフェースで低レベルの MEP が作成されたときのみ MIP を作成することができます。

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

説明

cfd mip-rule コマンドは MIP を作成するルールを設定します。システムは設定されたルールに従い各ポートで MIP を自動的に作成します。

undo cfd mip-rule コマンドは Ethernet サービスインスタンスで作成された MIP と MIP の作成ルールを削除します。

例

Ethernet サービスインスタンス 5 の MIP 作成ルールをデフォルトに設定します。

<Switch> system-view

[Switch] cfd mip-rule default service-instance 5

2.1.11 cfd service-instance

Syntax

cfd service-instance *instance-id* **ma-id** { **icc-based** *ma-name* | **integer** *ma-num* | **string** *ma-name* | **vlan-based** [*vlan-id*] } [**ma-index** *index-value*] **md** *md-name* **vlan** *vlan-id*

undo cfd service-instance *instance-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

ma-id: MA を作成します。

icc-based *ma-name*: ICC で定義した MA を設定します。設定範囲は 1～13 文字です。

integer *ma-num*: 整数で定義した MA を設定します。設定範囲は 0～65535 です。

string *ma-name*: 文字列で MA を設定します。設定範囲は 1～45 です。英字、数字、以下の記号を含むことができます。アポストロフィー（'）、チルダ（~）、感嘆符（!）、アットマーク（@）、シャープ（#）、ドル記号（$）、パーセント（%）、キャレット（^）、アンパサンド（&）、アスタリスク（*）、括弧（{ },( ),[ ],< >）、ハイフン（-）、アンダーライン（_）、プラス（+）、イコール（=）、垂直バー（|）、コロン（:）、セミコロン（;）、バッククォート（`）、コンマ（,）、ドット（.）、スラッシュ（/）

vlan-based [*vlan-id*]: VLAN ID で MA を設定します。設定範囲は 1～4094 です。*vlan-id* を指定しない場合、**vlan** *vlan-id* で指定された VLAN ID が使用されます。**vlan** *vlan-id* が指定されていない場合、**vlan-based** [*vlan-id*]の *vlan-id* を指定する必要があります。

ma-index *index-value*: MA インデックスを指定します。設定範囲は 1～4294967295 です。指定しない場合、使用されていないインデックスのもっとも小さい番号が自動的に割り当てられます。システムが自動で割り当てるインデックスを使用することを推奨します。

md *md-name*: MD の名前を指定します。設定範囲は 1～43 です。英字、数字、以下の記号を含むことができます。アポストロフィー（'）、チルダ（~）、感嘆符（!）、アットマーク（@）、シャープ（#）、ドル記号（$）、パーセント（%）、キャレット（^）、アンパサンド（&）、アスタリスク（*）、括弧（{ },( ),[ ],< >）、ハイフン（-）、アンダーライン（_）、プラス（+）、イコール（=）、垂直バー（|）、コロン（:）、セミコロン（;）、バッククォート（`）、コンマ（,）、ドット（.）、スラッシュ（/）

vlan *vlan-id*: MA が提供する VLAN を指定します。設定範囲は 1～4094 です。

説明

cfd service-instance コマンドは MD 名で Ethernet サービスインスタンスを作成します。

undo cfd service-instance コマンドは Ethernet サービスインスタンスを削除します。

Ethernet サービスインスタンスは MD 内にある MA を示すため、数字で示されます。MD と MA は Ethernet サービスインスタンスの MP で処理されたメッセージのレベルの属性と VLAN の属性を定義します。MA インデックスは MD の中の MA を一意に識別します。MA インデックスは異なる MD で使用することができます。

MD 名は IEEE802.1ag-2007 の表 21-19 に準拠する必要があります。

このコマンドは **vlan-based** [*vlan-id*]あるいは **vlan** *vlan-id* を使用して VLAN 属性を持つ MA を作成します。**vlan-based** [*vlan-id*]あるいは **vlan** *vlan-id* を指定しない場合、MA は VLAN 属性を持ちません。

MD 名で Ethernet サービスインスタンスを作成する前に関連する MD と MA を作成する必要があります。

Ethernet サービスインスタンスを削除するとき、Ethernet サービスインスタンスに関連する設定を削除する必要があります。

Ethernet サービスインスタンスを削除すると、Ethernet サービスインスタンスと Ethernet サービスインスタンスに対応する MA との関係を解消します。MA も削除されます。

例

レベル 3 の MD 名が test_md の MD を作成し、VLAN100 で MA を識別する Ethernet サービスインスタンス 5 を作成します。

<Switch> system-view

[Switch] cfd md test_md level 3

[Switch] cfd service-instance 5 ma-id vlan-based md test_md vlan 100

関連コマンド

cfd md

2.1.12 display cfd linktrace-reply

Syntax

display cfd linktrace-reply [**service-instance** *instance-id* [**mep** *mep-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。指定しない場合、すべての Ethernet サービスインスタンスの LTR の情報を表示します。

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。指定しない場合、すべての MEP の LTR の情報を表示します。

説明

display cfd linktrace-reply コマンドは MEP で保存された LTR の情報を表示します。

このコマンドは **cfd linktrace** コマンドを実行して受信した LTR の情報のみを表示します。

例

各 Ethernet サービスインスタンスのすべての MEP の LTR の情報を表示します。

<Switch> display cfd linktrace-reply

```
Service instance: 1      MEP ID: 1003
MAC address             TTL    Last MAC         Relay action
0000-fc00-6505           63     0000-fc00-6504    MPDB
000f-e269-a852           62     0000-fc00-6505    FDB
0000-fc00-6508           61     000f-e269-a852    Hit
Service instance: 2      MEP ID: 1023
MAC address             TTL    Last MAC         Relay action
0000-fc00-6508           61     000f-e269-a852    Hit
```

表 2-4 コマンド出力

フィールド	説明
Service instance	LTMを送信するMEPが所属するEthernetサービスインスタンスです。
MEP ID	LTMを送信するMEPのIDです。

フィールド	説明
MAC address	LTRメッセージの送信元MACアドレスです。
TTL	LTMが装置を通過するときのTTLの値です。
Last MAC	LTMメッセージの最終ホップの装置のMACアドレスです。
Relay action	転送する装置がMACアドレステーブルから宛先MACアドレスを検出したかどうかを示します。 CFDの標準バージョン（IEEE 802.1ag）が使用されたとき、以下のことを示します。 • **Hit**—現在の装置は宛先装置です。 • **FDB**—転送する装置は宛先MACアドレスを検出しました。 • **MPDB**—宛先MACアドレスが見つかりませんでした。あるいは、MEPまたはMIPデータベースに宛先MACアドレスが検出されました。

関連コマンド

cfd linktrace

2.1.13 display cfd linktrace-reply auto-detection

Syntax

display cfd linktrace-reply auto-detection [**size** *size-value*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

size *size-value*: 自動検出結果を保存するために使用するバッファサイズを指定します。設定範囲は 1～100 です。指定しない場合、バッファのすべての情報が表示されます。

説明

display cfd linktrace-reply コマンドは自動的に送信された LTM への応答として、受信した LTR メッセージの内容を表示します。

このコマンドは **cfd linktrace auto-detection** コマンドを実行して受信した LTR の情報のみを表示します。

例

自動的に送信された LTM への応答として、受信した LTR メッセージの内容を表示します。

<Switch> display cfd linktrace-reply auto-detection

```
Service instance: 1      MEP ID: 1003    Time: 2013/05/22 10:43:57
Target MEP ID: 2005      TTL: 64
MAC address             TTL     Last MAC         Relay action
0000-fc00-6505           63      0000-fc00-6504    MPDB
000f-e269-a852           62      0000-fc00-6505    FDB
0000-fc00-6508           61      000f-e269-a852    Hit
Service instance: 2      MEP ID: 1023    Time: 2013/05/22 10:44:06
Target MEP ID: 2025      TTL: 64
MAC address             TTL     Last MAC         Relay action
0000-fc00-6508           61      000f-e269-a852    Hit
```

表 2-5 コマンド出力

フィールド	説明
Service instance	LTMを送信するMEPが所属するEthernetサービスインスタンスです。
MEP ID	LTMを送信するMEPのIDです。
Time	LTMを自動で送信した時間です。
Target MEP ID	宛先MEPのIDです。
TTL	LTMを自動で送信したときの初期TTLの値です。
MAC address	LTRメッセージの送信元MACアドレスです。
TTL	LTMが装置を通過するときのTTLの値です。
Last MAC	LTMメッセージの最終ホップの装置のMACアドレスです。

フィールド	説明
Relay action	転送する装置がMACアドレステーブルから宛先MACアドレスを検出したかどうかを示します。 CFDの標準バージョン（IEEE 802.1ag）が使用されたとき、以下のことを示します。 ● **Hit**—現在の装置は宛先装置です。 ● **FDB**—転送する装置は宛先MACアドレスを検出しました。 ● **MPDB**—宛先MACアドレスが見つかりませんでした。あるいは、MEPまたはMIPデータベースに宛先MACアドレスが検出されました。

関連コマンド

cfd linktrace auto-detection

2.1.14 display cfd md

Syntax

display cfd md

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display cfd md コマンドは MD の設定情報を表示します。

例

MD の設定情報を表示します。

<Switch> display cfd md

```
CFD is enabled.
Maintenance domains configured: 4 in total
Level  Index     Maintenance domain                  MD format  MD ID
0      1         md_0                            CHARSTRING md_0
1      2         md_1                            DNS        dns1
2      3         md_2                            MAC        0001-0001-0001-1
3      4         md_3                            NONE       Without ID
```

表 2-6 コマンド出力

フィールド	説明
Maintenance domains configured	設定されたMDの数です。
Level	MDのレベルです。
Index	MDのインデックスです。
Maintenance domain	MD名です。
MD format	MD名の形式です。 • **CHARSTRING**—文字列の形式です。 • **DNS**—DNS名です。 • **MAC**—MACアドレスと整数です。 • **NONE**—MD名が運ばれません。
MD ID	MD IDの値です。 • MDの形式が**CHARSTRING**である場合、文字列です。 • MDの形式が**DNS**である場合、DNS名です。 • MDの形式が**MAC**である場合、MACアドレス-整数です。 • MDの形式が**NONE**である場合、IDはありません。

2.1.15 display cfd mep

Syntax

display cfd mep *mep-id* **service-instance** *instance-id*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

説明

display cfd mep コマンドは MEP の属性と動作情報を表示します。

例

Ethernet サービスインスタンス 1 の MEP50 の属性と動作情報を表示します。

<Switch> display cfd mep 50 service-instance 1

```
Interface: GigabitEthernet1/0/2
Maintenance domain: md_0
Maintenance domain index: 1
Maintenance association: ma_0
Maintenance association index: 1
Level: 0       VLAN: 1        Direction: Outbound
Current state: Active         CCM send: Enabled
FNG state: FNG_DEFECT_REPORTED

CCM:
Current state: CCI_WAITING
Interval: 1s       SendCCM: 12018

Loopback:
NextSeqNumber: 8877
SendLBR: 0         ReceiveInOrderLBR: 0         ReceiveOutOrderLBR: 0

Linktrace:
NextSeqNumber: 8877
SendLTR: 0         ReceiveLTM: 0

No CCM received from some remote MEPs.

One or more streams of error CCMs is received. The last received CCM:
Maintenance domain: (Without ID)
Maintenance association: matest1
MEP ID: 5     Sequence Number:0x50A
MAC Address: 0011-2233-4402
Received Time: 2013/03/06 13:01:34

One or more streams of cross-connect CCMs is received. The last received CCM:
Maintenance domain: mdtest1
Maintenance association:matest1
MEP ID: 6     Sequence Number:0x63A
MAC Address: 0011-2233-4401
Received Time: 2013/03/06 13:01:34

Some other MEPs are transmitting the RDI bit.
```

表 2-7 コマンド出力

フィールド	説明
Interface	MDが属しているインタフェースです。
Maintenance domain	MEPが属しているMDです。（もしMD名がない場合、**Without ID** と表示されます。）
Maintenance domain index	MEPがある場所のMDのインデックスです。
Maintenance association	MEPが属しているMAです。
Maintenance association index	MEPがある場所のMAのインデックスです。
Level	MDのレベルです。
VLAN	MAが属しているVLANです。
Direction	MEPの方向です。
Current state	MEPの状態です。ActiveあるいはInactiveがあります。
CCM send	MEPがCCMを送信しているかどうかを示します。
FNG state	FNG(Fault Notification Generator)の状態です。 ● **FNG_RESET**—障害が解決されました。 ● **FNG_DEFECT**—障害が検出されました。 ● **FNG_REPORT_DEFECT**—障害を通知します。 ● **FNG_DEFECT_REPORTED**—障害が通知されました。 ● **FNG_DEFECT_CLEARING**—障害が解決されています。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
CCM	CCMに関連する情報です。
Current state	送信したCCMの状態です。 ● **CCI_IDLE**—初期状態です。 ● **CCI_WAITING**—送信状態です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Interval	CCMを送信する間隔です。
SendCCM	MEPによって送信されたCCMの数です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Loopback	ループバックに関連する情報です。

フィールド	説明
NextSeqNumber	次に送信されるLBMのシーケンス番号です。
SendLBR	送信されたLBRの数です。MEPが内向きである場合、LBRの数はカウントされません。
ReceiveInOrderLBR	正常な順番で受信したLBRメッセージの数です。
ReceiveOutOrderLBR	受信した不正なLBRメッセージの数です。
Linktrace	linktraceに関連した情報です。
NextSeqNumber	次に送信されるLTMのシーケンス番号です。
SendLTR	送信されたLTRの数です。MEPが内向きである場合、LBRの数はカウントされません。
ReceiveLTM	受信されたLTMの数です。
No CCM received from some remote MEPs.	あるリモートMEPからCCMを受信するのに失敗しました。（この情報はあるCCMがロストしたときのみ表示されます）
One or more streams of error CCMs is received. The last received CCM:	1つ以上のCCMが受信されたとき最後のエラーCCMの内容を表示します。（この情報はエラーCCMを受信したのみ表示されます）
Maintenance domain	最後のエラーCCMメッセージのMDです。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Maintenance association	最後のエラーCCMメッセージのMAです。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
MEP	最後のエラーCCMメッセージのMEPのIDです。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Sequence Number	最後のエラーCCMメッセージのシーケンス番号です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Received Time	最後のエラーCCMメッセージを受信した時間です。 このフィールドが未サポートの場合、ハイフン(-)が表示されます。
One or more streams of cross-connect CCMs is received. The last received CCM:	クロスコネクトのCCMを受信し、最後のクロスコネクトのCCMの内容を表示します。（クロスコネクトCCMを受信した場合のみ、この情報が表示されます。）
Some other MEPs are transmitting the RDI bit.	他のMEPから受信したRDIフラグビットのCCMです。（この情報は、このタイプのCCMを受信した場合にのみ表示されます）

2.1.16 display cfd meplist

Syntax

display cfd meplist [**service-instance** *instance-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。指定しない場合、すべての Ethernet サービスインスタンスの MEP リストを表示します。

説明

display cfd meplist コマンドは Ethernet サービスインスタンスの MEP リストを表示します。

例

Ethernet サービスインスタンス 5 の MEP リストを表示します。

<Switch> display cfd meplist service-instance 5

```
Service instance: 5
MEP list: 1 to 20, 30, 50.
```

2.1.17 display cfd mp

Syntax

display cfd mp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートタイプとポート番号でポートを指定します。指定しない場合、すべてのポートの MP の情報を表示します。

説明

display cfd mp コマンドは MP の情報を表示します。

表示される情報は、ポート名でソートされます。ポートで、VLAN を提供する MP を表示し、そして VLAN を提供しない MP を表示します。VLAN を提供する MP は VLAN ID の昇順で表示されます。同一 VLAN で、MIP と MEP（高いレベルから低いレベル）の昇順で表示します。VLAN を提供しない MEP は高いレベルから低いレベルでソートされます。

例

すべてのポートの MP の情報を表示します。

<Switch> display cfd mp

```
Interface GigabitEthernet1/0/1   VLAN 100
MIP            Level: 2    Service instance: 102
Maintenance domain: md_2
Maintenance domain index: 3
Maintenance association: ma_2
Maintenance association index: 3

MEP ID: 101     Level: 1    Service instance: 101    Direction: Inbound
Maintenance domain: md_1
Maintenance domain index: 2
Maintenance association: ma_1
Maintenance association index: 2

MEP ID: 100     Level: 0    Service instance: 100    Direction: Outbound
Maintenance domain: md_0
Maintenance domain index: 1
Maintenance association: ma_0
Maintenance association index: 1
```

表 2-8 コマンド出力

フィールド	説明
Interface GigabitEthernet1/0/1 VLAN 100	GigabitEthernet 1/0/1のVLANのMPの情報です。
MIP	MPのMIPです。
Level	MPが属しているMDのレベルです。

フィールド	説明
Service instance	MPが属しているEthernetサービスインスタンスです。
Maintenance domain	MPが属しているMDです。
Maintenance domain index	MPが属しているMDのインデックスです。
Maintenance association	MPが属しているMAです。
Maintenance association index	MPが属しているMAのインデックスです。
Direction	MEPの方向です。内側向き、外側向きがあります。

2.1.18 display cfd remote-mep

Syntax

display cfd remote-mep service-instance *instance-id* **mep** *mep-id*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-instance *instance-id*: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。

説明

display cfd remote-mep コマンドはリモート MEP の情報を表示します。

例

Ethernet サービスインスタンス 4 の MEP10 のリモート MEP の情報を表示します。

<Switch> display cfd remote-mep service-instance 4 mep 10

```
MEP ID   MAC address     State       Time                MAC status
20       f474-8800-6565  OK          2013/03/06 02:36:38   UP
30       f474-8827-6502  OK          2013/03/06 02:36:38   DOWN
40       f474-8800-6510  FAILED       2013/03/06 02:36:39   DOWN
50       f474-8852-baa0  OK          2013/03/06 02:36:44   DOWN
```

```
60      0010-fc00-6502   OK          2013/03/06 02:36:42   DOWN
```

表 2-9 コマンド出力

フィールド	説明
MEP ID	リモートMEPのIDです。
MAC address	リモートMEP装置のMACアドレスです。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
State	リモートMEPの動作状態です。OK、FAILEDがあります。
Time	最後にMEPがFAILEDあるいはOKの状態になったときの時間です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
MAC status	リモートMEPから最後に受信したCCMのインタフェースの状態です。 • **UP**—インタフェースがパケットを通過する準備ができています。 • **DOWN**—インタフェースがパケットを通過することができません。 • **TESTING**—インタフェースがあるテストモード中です。 • **UNKNOWN**—インタフェースの状態が不明です。 • **DORMANT**—インタフェースがパケットを通過する状態ではありません。そのかわり、ある外部イベントの待ち状態にあります。 • **NOT-PRESENT**—インタフェースのある構成が欠けています。 • **LLD**—下位レイヤのインタフェースの状態であるため、ダウンしています。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。

2.1.19 display cfd service-instance

Syntax

display cfd service-instance [*instance-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance-id: Ethernet サービスインスタンス ID を指定します。設定範囲は 1～32767 です。指定しない場合、すべての Ethernet サービスインスタンスの設定情報を表示します。

説明

display cfd service-instance コマンドは Ethernet サービスインスタンスの設定情報を表示します。

例

すべての Ethernet サービスインスタンスの設定情報を表示します。

<Switch> display cfd service-instance

```
Service instances configured (2 in total):
Service instance 5:
Maintenance domain: md_5
Maintenance domain index: 5
Maintenance association: ma_5
Maintenance association index: 5
Level: 5  VLAN: 5   MIP rule: NONE   CCM interval: 1s   Direction: Inbound
MEP ID: 730  Interface: GigabitEthernet1/0/1

Service instance 6:
Maintenance domain: (Without ID)
Maintenance domain index: 6
Maintenance association: ma_6
Maintenance association index: 6
Level: 6  VLAN: 6   MIP rule: NONE   CCM interval: 1s   Direction: Outbound
MEP ID: 731  Interface: GigabitEthernet1/0/2
```

表 2-10 コマンド出力

フィールド	説明
Service instances are configured.	設定されたEthernetサービスインスタンスの数です。
Service instance	EthernetサービスインスタンスのIDです。
Maintenance domain	EthernetサービスインスタンスのMDです。 （もしMD名がない場合、**Without ID**と表示されます。）
Maintenance domain index	Ethernetサービスインスタンスが属しているMDのインデックスです。

フィールド	説明
Maintenance association:	Ethernetサービスインスタンスの MA です。
Maintenance association index	Ethernetサービスインスタンスが属している MA のインデックスです。
Level	MD レベルです。
VLAN	MA が属している VLAN です。
MIP rule	Ethernetサービスインスタンスで設定された MIP の作成ルールです。
CCM interval	CCM を送信する間隔です。
Direction	Ethernetサービスインスタンスで設定された MEP の方向です。
MEP ID	Ethernetサービスインスタンスで設定された MEP の ID です。
Interface	Ethernetサービスインスタンスで設定された MEP のインタフェースです。

2.1.20 display cfd status

Syntax

display cfd status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display cfd status コマンドは CFD と AIS の状態を表示します。

例

CFD と AIS の状態を表示します。

<Switch> display cfd status

```
CFD is enabled.
AIS is disabled.
```

目次

このセクションのページは **9-x-x** です。

3 章 DLDP 3-1
3.1 DLDP 設定コマンド.....3-1
3.1.1 display dldp 3-1
3.1.2 display dldp statistics.....3-3
3.1.3 dldp authentication-mode.....3-5
3.1.4 dldp authentication-password.....3-6
3.1.5 dldp delaydown-timer.....3-7
3.1.6 dldp enable.....3-8
3.1.7 dldp global enable.....3-9
3.1.8 dldp interval.....3-9
3.1.9 dldp port unidirectional-shutdown.....3-10
3.1.10 dldp unidirectional-shutdown.....3-11
3.1.11 reset dldp statistics 3-12

3章 DLDP

3.1 DLDP設定コマンド

3.1.1 display dldp

Syntax

display dldp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、グローバルとポート指定の DLDP の設定を表示します。

説明

display dldp コマンドは DLDP の情報を表示します。

例

グローバルとポート指定の DLDP の設定を表示します。

<Switch> display dldp

```
DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 79
```

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

Interface GigabitEthernet1/0/2
 DLDP port state: Inactive
 DLDP port unidirectional-shutdown mode: None
 Number of the port’s neighbors: 0 (Maximum number ever detected: 1)
```

GigabitEthernet 1/0/1 の DLDP の設定を表示します。

<Switch> display dldp interface gigabitethernet 1/0/1

```
Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port’s neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 79
  Neighbor state: Confirmed
  Neighbor aged time: 13s
```

表 3-1 コマンド出力

フィールド	説明
DLDP global status	グローバルのDLDPの状態です。Enabled、Disabledがあります。
DLDP advertisement interval	接続先との関係を維持するためにAdvertisementパケットを送信する間隔です。単位は秒です。
DLDP authentication-mode	DLDP認証モードです。None、Simple、md5があります。
DLDP authentication-password	DLDP認証のパスワードです。 ● ******—パスワードが設定されています。 ● **Not configured**—認証モードが設定されていますが、パスワードは設定されていません。
DLDP unidirectional-shutdown mode	片方向リンクが検出されたのち、ポートがシャットダウンモードになりました。Auto、Manualまたはhybridがあります。
DLDP port unidirectional-shutdown mode	片方向リンクが検出されたのち、ポートがシャットダウンモードになりました。Auto、Manualまたはhybridがあります。ポートのシャットダウンモードが設定されていない場合、このフィールドには**None**と表示されます。
DLDP delaydown-timer value	DelayDownタイマの設定です。単位は秒です。
Number of enabled ports	DLDPが有効なポート数です。
Interface	DLDPが有効なポートのインデックスです。

フィールド	説明
DLDP port state	ポートのDLDPの状態です。 • **Bidirectional** • **Inactive** • **Initial** • **Unidirectional**
Number of the port's neighbors	ネイバの現在の番号です。
Maximum number ever detected	ポートで一度検出されたネイバの最大数です。 このフィールドは、ネイバの現在の数が、一度検出されたネイバの最大数と異なるときのみ表示します。
Neighbor MAC address	ネイバのMACアドレスです。
Neighbor port index	ネイバポートのインデックスです。
Neighbor state	ネイバ状態です。Confirmed、Unconfirmedがあります。
Neighbor aged time	ネイバのエージング時間です。

3.1.2 display dldp statistics

Syntax

display dldp statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべての DLDP が有効なポートを通過した DLDP パケットの統計情報を表示します。

説明

display dldp statistics コマンドはポートを通過した DLDP パケットの統計情報を表示します。

例

すべての DLDP が有効なポートを通過した DLDP パケットの統計情報を表示します。

<Switch> display dldp statistics

```
Interface GigabitEthernet1/0/1
 Packets sent: 6
 Packets received: 5
 Invalid packets received: 2
 Loopback packets received: 0
 Authentication-failed packets received: 0
 Valid packets received: 3

Interface GigabitEthernet1/0/2
 Packets sent: 7
 Packets received: 7
 Invalid packets received: 3
 Loopback packets received: 0
 Authentication-failed packets received: 0
 Valid packets received: 4
```

表 3-2 コマンド出力

フィールド	説明
Interface	ポートのインデックスです。
Packets sent	DLDPパケットを送信した総数です。
Packets received	DLDPパケットを受信した総数です。
Invalid packets received	不正パケットを受信した数です。
Loop packets received	ループバックパケットを受信した数です。
Authentication failed packets received	認証されなかったパケットを受信した数です。
Valid packets received	有効なパケットを受信した数です。

関連コマンド

reset dldp statistics

3.1.3 dldp authentication-mode

Syntax

dldp authentication-mode { **md5** | **none** | **simple** }

undo dldp authentication-mode

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

md5: MD5 認証モードを指定します。

none: 認証を行わないように指定します。

simple: プレーンテキストの認証モードを指定します。

説明

dldp authentication-mode コマンドは DLDP の認証を設定します。

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

DLDP を正常に動作させるため、リンクの両端で DLDP の認証モードとパスワードを同一にしてください。

認証モードを設定した後、認証のパスワードを設定しない場合、認証モードは **none** モードになります。

例

DLDP の認証モードをプレーンテキストで設定し、パスワードを **abc** に設定します。（Device A と Device B が DLDP リンクで接続されていると仮定します）

- Device A の設定

<DeviceA> system-view

[DeviceA] dldp authentication-mode simple

[DeviceA] dldp authentication-password simple abc

- Device B の設定

<DeviceB> system-view

[DeviceB] dldp authentication-mode simple

[DeviceB] dldp authentication-password simple abc

関連コマンド

- **display dldp**
- **dldp authentication-password**

3.1.4 dldp authentication-password

Syntax

dldp authentication-password { **cipher** | **simple** } *string*

undo dldp authentication-password

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号パスワードを設定します。

simple: プレーンテキストパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含むすべての DLDP 認証のパスワードは暗号テキストで保存されます。

string: パスワードを指定します。プレーンテキスト形式の設定範囲は 1～16 文字です。大文字と小文字を区別します。暗号化形式の設定範囲は 1～53 文字です。大文字と小文字を区別します。

説明

dldp authentication-password コマンドは DLDP 認証のパスワードを設定します。

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

DLDP を正常に動作させるため、リンクの両端で DLDP の認証モードとパスワードを同一にしてください。

認証モードを設定した後、認証のパスワードを設定しない場合、認証モードは **none** モードになります。

例

DLDP の認証モードをプレーンテキストで設定し、パスワードを **abc** に設定します。（Device A と Device B が DLDP リンクで接続されていると仮定します）

- Device A の設定

<DeviceA> system-view

[DeviceA] dldp authentication-mode simple

[DeviceA] dldp authentication-password simple abc

- Device B の設定

<DeviceB> system-view

[DeviceB] dldp authentication-mode simple

[DeviceB] dldp authentication-password simple abc

関連コマンド

- **display dldp**
- **dldp authentication-mode**

3.1.5 dldp delaydown-timer

Syntax

dldp delaydown-timer *time*

undo dldp delaydown-timer

デフォルト

1 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time: DelayDown タイマを指定します。設定範囲は 1～5 秒です。

説明

dldp delaydown-timer コマンドは DelayDown タイマを設定します。

undo dldp delaydown-timer コマンドはデフォルトに戻します。

このコマンドを使用して設定された DelayDown タイマはすべての DLDP が有効なポートに適用されます。

例

DelayDown タイマを 2 秒に設定します。

<Switch> system-view

[Switch] dldp delaydown-timer 2

関連コマンド

display dldp

3.1.6 dldp enable

Syntax

dldp enable

undo dldp enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dldp enable コマンドはポートで DLDP を有効にします。

undo dldp enable コマンドはデフォルトに戻します。

グローバルとポートで DLDP を有効にしたのち、DLDP が適用されます。

例

グローバルで DLDP を有効にし、GigabitEthernet 1/0/1 で DLDP を有効にします。

<Switch> system-view

[Switch] dldp global enable

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dldp enable

関連コマンド

- **display dldp**
- **dldp global enable**

3.1.7 dldp global enable

Syntax

dldp global enable

undo dldp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dldp global enable コマンドはグローバルで DLDP を有効にします。

undo dldp global enable コマンドはグローバルで DLDP を無効にします。

グローバルとポートで DLDP を有効にしたのち、DLDP が適用されます。

例

グローバルで DLDP を有効にします。

<Switch> system-view

[Switch] dldp global enable

関連コマンド

- **display dldp**
- **dldp enable**

3.1.8 dldp interval

Syntax

dldp interval *interval*

undo dldp interval

デフォルト

5 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: Advertisement パケットを送信する間隔を指定します。設定範囲は 1～100 秒です。

説明

dldp interval コマンドは Advertisement パケットを送信する間隔を設定します。

undo dldp interval コマンドはデフォルトに戻します。

このコマンドはすべての DLDP が有効なポートに適用されます。

DLDP を正常に動作させるため、リンクの両端で Advertisement パケットを送信する間隔を同一にしてください。

例

Advertisement パケットを送信する間隔を 20 秒に設定します。

<Switch> system-view

[Switch] dldp interval 20

関連コマンド

display dldp

3.1.9 dldp port unidirectional-shutdown

Syntax

dldp port unidirectional-shutdown { **auto** | **hybrid** | **manual** }

undo dldp port unidirectional-shutdown

デフォルト

グローバル設定が使用されます。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auto: ポートシャットダウンモードを自動モードとして指定します。このモードでは DLDP が片方向リンクを検出したとき、DLDP は片方向リンクのポートをシャットダウンします。リンクが双方向になると、DLDP はシャットダウンされたポートを起動します。

hybrid: ポートシャットダウンモードをハイブリッドモードとして指定します。このモードでは、DLDP が片方向リンクを検出すると、片方向ポートをシャットダウンし、リンク検出を停止します。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。リンクが双方向になると、ポートは双方向になります。

manual: ポートシャットダウンモードを手動モードとして指定します。このモードでは DLDP が片方向リンクを検出したとき、DLDP は関連したポートをシャットダウンしません。手動でシャットダウンする必要があります。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。リンクが双方向になると、ポートは双方向になります。

説明

dldp port unidirectional-shutdown コマンドはポートシャットダウンモードを設定します。

undo dldp port unidirectional-shutdown コマンドはデフォルトに戻します。

DLDP で片方向リンクが検出された場合は、インタフェースおよびケーブルの障害をトラブルシューティングする必要があります。

インタフェースのポートシャットダウンモードの設定は、現在のインタフェースにのみ有効で、グローバルポートシャットダウンモードの設定よりも優先されます。

例

GigabitEthernet 1/0/1 のポートシャットダウンモードを手動モードに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dldp port unidirectional-shutdown manual

関連コマンド

- **display dldp**
- **dldp unidirectional-shutdown**

3.1.10 dldp unidirectional-shutdown

Syntax

dldp unidirectional-shutdown { **auto** | **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。リンクが双方向になると、DLDP はシャットダウンされたポートを起動します。

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。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。リンクが双方向になると、ポートは双方向になります。

説明

dldp 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。

DLDP で片方向リンクが検出された場合は、インタフェースおよびケーブルの障害をトラブルシューティングする必要があります。

グローバルポートシャットダウンモードの設定はすべてのインタフェースに有効で、インタフェースのポートシャットダウンモードの設定よりも優先順位が低くなります。

例

ポートシャットダウンモードを手動モードに設定します。

<Switch> system-view

[Switch] dldp unidirectional-shutdown manual

関連コマンド

- **display dldp**
- **dldp port unidirectional-shutdown**

3.1.11 reset dldp statistics

Syntax

reset dldp statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべての DLDP が有効なポートを通過した DLDP パケットの統計情報を削除します。

説明

reset dldp statistics コマンドはポートを通過した DLDP パケットの統計情報を削除します。

例

すべての DLDP が有効なポートを通過した 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 **9-x-x** です。

4 章 RRPP 4-1
4.1 RRPP 設定コマンド 4-1
4.1.1 control-vlan 4-1
4.1.2 display rrpp brief 4-2
4.1.3 display rrpp ring-group 4-5
4.1.4 display rrpp statistics 4-6
4.1.5 display rrpp verbose 4-10
4.1.6 domain ring 4-14
4.1.7 protected-vlan 4-15
4.1.8 reset rrpp statistics 4-17
4.1.9 ring 4-17
4.1.10 ring enable 4-19
4.1.11 rrpp domain 4-20
4.1.12 rrpp enable 4-21
4.1.13 rrpp ring-group 4-22
4.1.14 snmp-agent trap enable rrpp 4-23
4.1.15 timer 4-24

4章 RRPP

4.1 RRPP設定コマンド

4.1.1 control-vlan

Syntax

control-vlan *vlan-id*

undo control-vlan

デフォルト

設定なし

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

vlan-id: プライマリコントロール VLAN の ID を指定します。設定範囲は 2～4093 です。

説明

control-vlan コマンドはRRPP ドメインのプライマリコントロールVLAN を設定します。

undo control-vlan コマンドは RRPP ドメインからプライマリコントロール VLAN を削除します。

RRPP ドメインのコントロール VLAN を設定するとき、プライマリコントロール VLAN のみを設定する必要があります。システムは自動でセカンダリコントロール VLAN を設定します。セカンダリコントロール VLAN ID としてプライマリコントロール VLAN ID に 1 を加算した VLAN を自動的に割り当てます。コントロール VLAN の設定を正常に行うため、2 つのコントロール VLAN の ID が連続し、ID が未割り当てであることを確認してください。

RRPP リングにアクセスするポートのデフォルト VLAN を制御 VLAN として設定しないでください。

RRPPDU を正しく転送するために、制御 VLAN で QinQ または VLAN マッピングを有効にしないでください。

RRPP ドメインに RRPP リングを設定した後は、そのドメインのプライマリ制御 VLAN を削除または変更することはできません。これを行うには、**undo control-vlan** コマンドを使用します。

例

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 100 を設定します。（VLAN100、VLAN101 が割り当てられていないと仮定します。）

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1] control-vlan 100

4.1.2 display rrpp brief

Syntax

display rrpp brief

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display rrpp brief コマンドは RRPP の概要情報を表示します。

例

RRPP の概要情報を表示します。

<Switch> display rrpp brief

```
Flags for node mode: M -- Master, T -- Transit, E -- Edge, A -- Assistant-edge

RRPP protocol status: Enabled

Domain ID    : 1
Control VLAN  : Primary 5, Secondary 6
Protected VLAN: Reference instance 0 to 2, 4
Hello timer   : 1 sec, Fail timer: 3 sec
Fast detection status: Disabled
Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
 Ring  Ring   Node  Primary/Common          Secondary/Edge          Enable
 ID    level  mode  port                   port                    status
```

```
--------------------------------------------------------------------------------
-
  1     1      M     GE1/0/1               GE1/0/2               Yes

 Domain ID     : 2
 Control VLAN  : Primary 10, Secondary 11
 Protected VLAN: Reference instance 0 to 2, 4
 Hello timer   : 1 sec, Fail timer: 3 sec
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
  Ring  Ring   Node  Primary/Common          Secondary/Edge          Enable
  ID    level  mode  port                   port                    status

--------------------------------------------------------------------------------
-
  1     0      T     GE1/0/3               GE1/0/4               Yes
  2     1      E     GE1/0/3               GE1/0/5               Yes
                     GE1/0/4
```

表 4-1 コマンド出力

フィールド	説明
Flags for node mode	RRPPノードモードです。 • **M**—マスタモードです。 • **T**—トランジットモードです。 • **E**—エッジモードです。 • **A**—アシスタントエッジモードです。
RRPP protocol status	RRPPの状態です。 • **Enabled**—グローバルで有効です。 • **Disabled**—グローバルで無効です。
Domain ID	RRPPのドメインIDです。
Control VLAN	RRPPドメインのプライマリ、セカンダリコントロールVLANです。
Protected VLAN	RRPPドメインによって保護されたVLANに対応するMSTIです。VLANインスタンスマッピングを表示する場合、**display stp region-configuration**コマンドを使用します。（コマンドマニュアルのセクション3 *アクセス* “*STP*”を参照してください。）
Hello timer	Helloタイマの値です。単位は秒です。

フィールド	説明
Fail timer	Failタイマの値です。単位は秒です。
Fast detection status	Fast detectionの状態です。**Enabled**あるいは**Disabled**があります。このフィールドは未サポートです。
Fast-Hello timer	Fast-Helloタイマの値です。単位はミリ秒です。 このフィールドは未サポートです。
Fast-Fail timer	Fast-Failタイマの値です。単位はミリ秒です。 このフィールドは未サポートです。
Fast-Edge-Hello timer	Fast-Edge-Helloタイマの値です。単位はミリ秒です。 このフィールドは未サポートです。
Fast-Edge-Fail timer	Fast-Edge-Failタイマの値です。単位はミリ秒です。 このフィールドは未サポートです。
Ring ID	RRPPリングのIDです。
Ring level	RRPPリングのレベルです。 • **0**—プライマリリングです。 • **1**—サブリングです。
Primary/Common port	ノードモードがマスタノードあるいはトランジットノードであるとき、このフィールドはプライマリポートを表示します。 ノードのモードがエッジノードあるいはアシスタンドエッジノードであるとき、このフィールドは共通ポートを表示します。 以下の状況が発生するときハイフン（-）を表示します。 • ポートがリングに設定されていません。 • ポートが属している拡張インタフェースカードが起動していません。 • ポートがリンクアグリゲーショングループのメンバです。
Secondary/Edge port	ノードモードがマスタノードあるいはトランジットノードであるとき、このフィールドはセカンダリポートを表示します。 ノードのモードがエッジノードあるいはアシスタンドエッジノードであるとき、このフィールドはエッジポートを表示します。 以下の状況が発生するときハイフン（-）を表示します。 • ポートがリングに設定されていません。 • ポートが属している拡張インタフェースカードが起動していません。 • ポートがリンクアグリゲーショングループのメンバで

フィールド	説明
	す。
Enable status	RRPPリングの状態です。 ● **Yes**—有効です。 ● **No**—無効です。

4.1.3 display rrpp ring-group

Syntax

display rrpp ring-group [*ring-group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ring-group-id: RRPP リンググループの ID を指定します。設定範囲は 1～64 です。指定しない場合、すべてのリンググループの設定を表示します。

説明

display rrpp ring-group コマンドはリンググループの設定を表示します。

エッジノードの RRPP リンググループでは、Edge-Hello パケットを送信するサブリングも表示します。

例

すべての RRPP リンググループの設定を表示します。

<Switch> display rrpp ring-group

```
Ring group 1:
 Domain 1 ring 1 to 3, 5
 Domain 2 ring 1 to 3, 5
 Domain 1 ring 1 is the sending ring

Ring group 2:
 Domain 1 ring 4, 6 to 7
 Domain 2 ring 4, 6 to 7
```

表 4-2 コマンド出力

フィールド	説明
Ring group 1	RRPPリンググループ1です。
Domain 1 ring 1 to 3, 5	RRPPドメイン1のリング1、2、3、5を含むリンググループのサブリングです。
Domain 1 ring 1 is the sending ring	RRPPドメイン1のリンググループの送信リングが1です。

4.1.4 display rrpp statistics

Syntax

display rrpp statistics domain *domain-id* [**ring** *ring-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

domain *domain-id*: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

ring *ring-id*: RRPP リングの ID を指定します。設定範囲は 1～128 です。指定しない場合、指定した RRPP ドメインのすべてのリングの RRPPDU の統計情報を表示します。

説明

display rrpp statistics コマンドは RRPPDU の統計情報を表示します。

ポートが 2 つ以上のリングに属している場合、RRPPDU の統計情報は、リングごとに取得され、表示します。

リングが非アクティブからアクティブ状態に遷移すると、リングのパケットのカウントを再開します。

例

RRPP ドメイン 2 のすべてのリングの RRPPDU の統計情報を表示します。

<Switch> display rrpp statistics domain 2

```
Ring ID      : 1
Ring level   : 0
Node mode    : Master
Active status : Yes
```

```
 Primary port  : GE1/0/3
 Fast-Hello packets: 0 Sent, 0 Received
 Fast-Edge-Hello packets: 0 Sent, 0 Received
  Direct Hello    Link    Common    Complete   Edge     Major    Total
                 down    flush FDB  flush FDB  hello    fault

-------------------------------------------------------------------------
-
  Out    16924    0       0         1         0        0        16925
  In     0        0       0         0         0        0        0
 Secondary port: GE1/0/4
 Fast-Hello packets: 0 Sent, 0 Received
 Fast-Edge-Hello packets: 0 Sent, 0 Received
  Direct Hello    Link    Common    Complete   Edge     Major    Total
                 down    flush FDB  flush FDB  hello    fault

-------------------------------------------------------------------------
-
  Out    0        0       0         0         0        0        0
  In     16878    0       0         1         0        0        16879

 Ring ID      : 2
 Ring level   : 1
 Node mode    : Edge
 Active status : No
 Common port   : GE1/0/3
 Fast-Hello packets: 0 Sent, 0 Received
 Fast-Edge-Hello packets: 0 Sent, 0 Received
  Direct Hello    Link    Common    Complete   Edge     Major    Total
                 down    flush FDB  flush FDB  hello    fault

-------------------------------------------------------------------------
-
  Out    0        0       0         0         0        0        0
  In     0        0       0         0         0        0        0
 Common port   : GE1/0/4
 Fast-Hello packets: 0 Sent, 0 Received
 Fast-Edge-Hello packets: 0 Sent, 0 Received
  Direct Hello    Link    Common    Complete   Edge     Major    Total
                 down    flush FDB  flush FDB  hello    fault

-------------------------------------------------------------------------
-
```

```
  Out    0        0       0         0         0        0        0
  In     0        0       0         0         0        0        0
 Edge port     : GE1/0/5
  Direct Hello     Link     Common     Complete   Edge      Major     Total
                 down     flush FDB  flush FDB  hello     fault

---------------------------------------------------------------------------
-
  Out    0        0       0         0         0        0        0
  In     0        0       0         0         0        0        0
```

表 4-3 コマンド出力

フィールド	説明
Ring ID	RRPPのリングIDです。
Ring level	RRPPのリングレベルです。 ● **0**—プライマリリングです。 ● **1**—サブリングです。
Node mode	ノードモードです。 ● マスタノードです。 ● トランジットノードです。 ● エッジノードです。 ● アシスタンドエッジノードです。
Active status	RRPPのリング状態です。 ● **Yes**—アクティブです。 ● **No**—非アクティブです。
Primary port	プライマリポートのフィールドは、ノードのモードがマスタノードあるいはトランジットノードであることを示します。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。

フィールド	説明
Secondary port	セカンダリポートのフィールドは、ノードのモードがマスタノードあるいはトランジットノードであることを示します。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。
Common port	共通ポートのフィールドは、ノードのモードがエッジノードあるいはアシスタントエッジノードであることを示します。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。
Edge port	エッジポートのフィールドは、ノードのモードがエッジノードあるいはアシスタントエッジノードであることを示します。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。
Fast-Hello packets	ポートのFast-Helloパケットの統計情報です。 ● **Sent**—ポートで送信したFast-Helloパケットの数です。 ● **Received**—ポートで受信したFast-Helloパケットの数です。 このフィールドは未サポートです。
Fast-Edge-Hello packets	ポートのFast-Edge-Helloパケットの統計情報です。 ● **Sent**—ポートで送信したFast-Edge-Helloパケットの数です。 ● **Received**—ポートで受信したFast-Edge-Helloパケットの数です。 このフィールドは未サポートです。

フィールド	説明
Packet direct	ポートのパケット転送方向です。 ● **Out**—パケットの送信方向です。 ● **In**—パケットの受信方向です。
Hello	ポートで送受信されたHelloパケットの統計情報です。
Link down	ポートで送受信されたLink-Downパケットの統計情報です。
Common flush FDB	ポートで送受信されたCommon-Flush-FDBパケットの統計情報です。
Complete flush FDB	ポートで送受信されたComplete-Flush-FDBパケットの統計情報です。
Edge hello	ポートで送受信されたEdge-Helloパケットの統計情報です。
Major fault	ポートで送受信されたMajor-Faultパケットの統計情報です。
Total	ポートで送受信された以下のパケットの総数です。 RRPPのHelloパケット、Link-Downパケット、Common-Flush-FDBパケット、Complete-Flush-FDBパケット、Edge-HelloパケットおよびMajor-FaultパケットのRRPPに変更します。

関連コマンド

reset rrpp statistics

4.1.5 display rrpp verbose

Syntax

display rrpp verbose domain *domain-id* [**ring** *ring-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

domain *domain-id*: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

ring *ring-id*: RRPP リングの ID を指定します。設定範囲は 1～128 です。指定しない場合、指定した RRPP ドメインのすべてのリングの詳細情報を表示します。

説明

display rrpp verbose コマンドは RRPP の詳細情報を表示します。

例

RRPP ドメイン 2 のすべてのリングの詳細情報を表示します。

<Switch> display rrpp verbose domain 2

```
Domain ID    : 2
Control VLAN  : Primary 10, Secondary 11
Protected VLAN: Reference instance 3, 5 to 7
Hello timer   : 1 sec, Fail timer: 3 sec
Fast detection status: Disabled
Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

Ring ID      : 1
Ring level    : 0
Node mode     : Master
Ring state    : Completed
Enable status : Yes, Active status: Yes
Primary port  : GE1/0/4                Port status: UP
Secondary port: GE1/0/5                Port status: BLOCKED

Ring ID      : 2
Ring level    : 1
Node mode     : Edge
Ring state    : -
Enable status : No, Active status: No
Common port   : GE1/0/4                Port status: -
             GE1/0/5                Port status: -
Edge port     : GE1/0/3                Port status: -
```

表 4-4 コマンド出力

フィールド	説明
Domain ID	RRPP ドメイン ID です。
Control VLAN	RRPP ドメインのコントロール VLAN です。 • **Primary**—プライマリコントロール VLAN です。 • **Secondary**—セカンダリコントロール VLAN です。

フィールド	説明
Protected VLAN	RRPPドメインによって保護されたVLANに対応するMSTIです。 VLANインスタンスマッピングを表示する場合、**display stp region-configuration**コマンドを使用します。（コマンドマニュアルのセクション3 *アクセス* “*STP*”を参照してください。
Hello timer	Helloタイマの値です。単位は秒です。
Fail timer	Failタイマの値です。単位は秒です。
Fast detection status	Fast detectionメカニズムの状態です。**Enabled**あるいは**Disabled**があります。このフィールドは未サポートです。
Fast-Hello timer	Fast-Helloタイマの値です。単位はミリ秒です。 このフィールドは未サポートです。
Fast-Fail timer	Fast-Failタイマの値です。単位はミリ秒です。 このフィールドは未サポートです。
Fast-Edge-Hello timer	Fast-Edge-Helloタイマの値です。単位はミリ秒です。 このフィールドは未サポートです。
Fast-Edge-Fail timer	Fast-Edge-Failタイマの値です。単位はミリ秒です。 このフィールドは未サポートです。
Ring ID	RRPPリングIDです。
Ring level	RRPP リングレベルです。 ● **0**—プライマリリングです。 ● **1**—サブリングです。
Node mode	ノードモードです。 ● マスタノードです。 ● トランジットノードです。 ● エッジノードです。 ● アシスタントエッジノードです。
Ring state	RRPPリング状態です。 ● **Completed**—リングが正常です。 ● **Failed**—リングが閉じていません。 マスタノードとして動作する装置でリングが有効でない、あるいは装置がリングのマスタノードでない場合、ハイフン（-）が表示されます。
Enable status	RRPPリングの状態です。 ● **Yes**—有効です。 ● **No**—無効です。

フィールド	説明
Active status	RRPPリングの状態です。 ● **Yes**—アクティブです。 ● **No**—非アクティブです。 RRPPとRRPPリングが有効である場合、RRPPリングのみアクティブにすることができます。このフィールドはRRPPが有効かどうかを識別します。
Primary port	プライマリポートのフィールドは、ノードのモードがマスタノードあるいはトランジットノードであることを示します。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。
Secondary port	セカンダリポートのフィールドは、ノードのモードがマスタノードあるいはトランジットノードであることを示します。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。
Common port	共通ポートのフィールドは、ノードのモードがエッジノードあるいはアシスタントエッジノードであることを示します。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。

フィールド	説明
Edge port	エッジポートのフィールドは、ノードのモードがエッジノードあるいはアシスタントエッジノードであることを示します。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。
Port status	ポートの状態です。Down、up、blockedがあります。 以下の状況が発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートが属している拡張インタフェースカードが起動していません。 ● ポートがリンクアグリゲーショングループのメンバです。

4.1.6 domain ring

Syntax

domain *domain-id* **ring** *ring-id-list*

undo domain *domain-id* [**ring** *ring-id-list*]

デフォルト

設定なし

View

RRPP ring group view

定義済みユーザロール

network-admin

パラメータ

domain-id: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

ring *ring-id-list*: RRPP サブリングの ID を指定します。半角スペースで区切り 10 まで指定するか、RRPP サブリングの ID の範囲を指定します。設定範囲は 1～128 です。指定しない場合、指定したドメインのリンググループからすべてのサブリングを削除します。

説明

domain ring コマンドは RRPP リンググループのサブリングを設定します。

undo domain ring コマンドは RRPP リンググループからサブリングを削除します。

エッジノード、アシスタントエッジノードの RRPP リンググループを設定するとき、以下のガイドラインに従ってください。

- リンググループにアクティブリングを割り当てるとき、最初にアシスタントエッジノードのグループを割り当て、次にエッジノードのグループを割り当ててください。
- リンググループからアクティブリングを削除する場合、最初にエッジノードを削除し、次にアシスタントエッジノードを削除してください。
- すべてのリンググループを削除する場合、最初にエッジノードを削除し、次にアシスタントエッジノードを削除してください。
- リンググループのリングをアクティブ状態にする場合、最初にエッジノードをアクティブ状態にし、次にアシスタントエッジノードをアクティブ状態にしてください。
- リンググループのリングを非アクティブ状態にする場合、最初にアシスタントエッジノードを非アクティブ状態にし、次にエッジノードを非アクティブ状態にしてください。

ガイドラインに従わない場合、アシスタントエッジノードは Edge-Hello パケットの受信に失敗する可能性があり、誤ってプライマリリングが故障したと認識します。

例

RRPP リンググループ 1 を作成し、ドメイン 1、ドメイン 2 にサブリング 1、2、3、5 を追加します。

<Switch> system-view

[Switch] rrpp ring-group 1

[Switch-ring-group1] domain 1 ring 1 to 3 5

[Switch-ring-group1] domain 2 ring 1 to 3 5

関連コマンド

- **display rrpp ring-group**
- **rrpp ring-group**

4.1.7 protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

デフォルト

設定なし

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

reference-instance *instance-id-list*: MSTI（Multiple Spanning Tree Instances）の ID を指定します。MSTI の ID を 10 まで指定するか、範囲で指定します。MSTI を範囲で指定する形式は *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>です。*instance-id* の設定範囲は 0～4094 です。VLAN インスタンスのマッピングを表示する場合、**display stp region-configuration** コマンドを使用します。パラメータを指定しない場合、RRPP ドメインによって参照されるすべての MSTI を削除します。

説明

protected-vlan コマンドは RRPP ドメインのプロテクト VLAN を設定します。

undo protected-vlan コマンドは RRPP ドメインからプロテクト VLAN を削除します。

装置のスパニングツリーの動作モードが PVST モードの場合、MSTI の ID の値は 0 だけです。

プロテクト VLAN のリングを設定する前後に、RRPP ドメインで設定したプロテクト VLAN を削除、あるいは修正することができます。しかしドメインで設定されたすべてのプロテクト VLAN の設定を削除することはできません。VLAN ドメイン用に構成されています。

VLAN インスタンスのマッピングを変更するとき、RRPP ドメインのプロテクト VLAN も変更します。

例

MSTI 1 に VLAN 1～VLAN 30 をマッピングし、MST リージョンの設定をアクティブ状態にします。RRPP ドメイン 1 のコントロール VLAN として VLAN 100 を設定します。RRPP ドメイン 1 のプライマリコントロール VLAN として MSTI 1 にマッピングされた VLAN を設定します。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] instance 1 vlan 1 to 30

[Switch-mst-region] active region-configuration

[Switch-mst-region] quit

[Switch] rrpp domain 1

[Switch-rrpp-domain1] control-vlan 100

[Switch-rrpp-domain1] protected-vlan reference-instance 1

関連コマンド

- **display stp region-configuration**（コマンドマニュアルのセクション 3 *アクセス*“*STP*”）
- **rrpp domain**

4.1.8 reset rrpp statistics

Syntax

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

domain *domain-id*: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

ring *ring-id*: RRPP リングの ID を指定します。設定範囲は 1～128 です。指定しない場合、指定した RRPP ドメインのすべての RRPP リングの RRPPDU の統計情報を削除します。

説明

reset rrpp statistics コマンドは RRPPDU の統計情報を削除します。

例

RRPP ドメイン 1 のリング 10 の RRPPDU の統計情報を削除します。

<Switch> reset rrpp statistics domain 1 ring 10

関連コマンド

display rrpp statistics

4.1.9 ring

Syntax

ring *ring-id* **node-mode** { { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value* | { **assistant-edge** | **edge** } [**edge-port** *interface-type interface-number*] }

undo ring *ring-id*

デフォルト

装置は RRPP リングのノードではありません。

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

ring-id: RRPP リングの ID を指定します。設定範囲は 1～128 です。

master: 装置を RRPP リングのマスタノードとして指定します。

transit: 装置を RRPP リングのトランジットノードとして指定します。

primary-port: プライマリポートを指定します。

interface-type interface-number: ポートのタイプと番号を指定します。

secondary-port: セカンダリポートを指定します。

level *level-value*: RRPP リングレベルを指定します。0 はプライマリリングで、1 はサブリングです。

assistant-edge: 装置を RRPP リングのアシスタントエッジノードとして指定します。

edge: 装置を RRPP リングのエッジノードとして指定します。

edge-port: ノードのエッジポートを指定します。

説明

ring コマンドは装置のノードモード、指定した RRPP ポートの役割、RRPP リングのレベルを設定します。

undo ring コマンドは RRPP リングを削除します。

ドメインの RRPP リングの ID は一意にする必要があります。

RRPP リングがアクティブ状態であるとき､RRPP ポートを設定することはできません。

エッジノード、アシスタントエッジノードを設定するとき、最初にプライマリリングを設定し、次にサブリングを設定してください。

設定した後、RRPP リングのノードモード、RRPP ポートの役割、リングレベルは変更することができません。設定を変更する場合、最初に現在の設定を削除してください。

エッジノードあるいはアシスタントエッジノードのプライマリリングの設定を削除する前に、すべてのサブリングの設定を削除してください。しかしアクティブ状態の RRPP リングは削除することができません。

装置で RRPP が有効であるとき、削除する前に、RRPP リングを無効にしてください。装置で RRPP が無効であるとき、**ring enable** コマンドの設定を使用して RRPP リングを直接削除することができます。

例

装置を RRPP ドメイン 1 のプライマリリング 10 のマスタノードとして指定します。プライマリポートとして GigabitEthernet 1/0/1 を指定し、セカンダリポートとして GigabitEthernet 1/0/2 を指定します。

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1] control-vlan 100

[Switch-rrpp-domain1] protected-vlan reference-instance 0 1 2

[Switch-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

装置を RRPP ドメイン 1 のプライマリリング 10 のトランジットノードとして指定します。プライマリポートとして GigabitEthernet 1/0/1 を指定し、セカンダリポートとして GigabitEthernet 1/0/2 を指定します。装置を RRPP ドメイン 1 のサブリング 20 のエッジノードとして指定します。エッジポートとして GigabitEthernet 1/0/3 を指定します。

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1] control-vlan 100

[Switch-rrpp-domain1] protected-vlan reference-instance 0 1 2

[Switch-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

[Switch-rrpp-domain1] ring 20 node-mode edge edge-port gigabitethernet 1/0/3

関連コマンド

ring enable

4.1.10 ring enable

Syntax

ring *ring-id* **enable**

undo ring *ring-id* **enable**

デフォルト

無効

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

ring-id: RRPP リングの ID を指定します。設定範囲は 1～128 です。

説明

ring enable コマンドは RRPP リングを有効にします。

undo ring enable コマンドは RRPP リングを無効にします。

RRPP リングをアクティブにする場合、RRPP、RRPP リングを有効にする必要があります。

装置でサブリングを有効にする前に、プライマリリングを有効にする必要があります。装置でプライマリリングを無効にする前に、すべてのサブリングを無効にする必要があります。そうでない場合、システムはエラーメッセージを表示します。

例

RRPP ドメイン 1 の RRPP リング 10 を有効にします。

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1] control-vlan 100

[Switch-rrpp-domain1] protected-vlan reference-instance 0 1 2

[Switch-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

[Switch-rrpp-domain1] ring 10 enable

関連コマンド

rrpp enable

4.1.11 rrpp domain

Syntax

rrpp domain *domain-id*

undo rrpp domain *domain-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-id: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

説明

rrpp domain コマンドは RRPP ドメインを作成し、RRPP domain view に移行するか、既存の RRPP domain view に移行します。

undo rrpp domain コマンドは RRPP ドメインを削除します。

RRPP ドメインを削除するとき、コントロール VLAN とプロテクト VLAN の設定が同時に削除されます。

RRPP ドメインを正常に削除するため、RRPP リングがないことを確認してください。

例

RRPP ドメイン 1 を作成し、RRPP domain 1 view に移行します。

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1]

関連コマンド

- **control-vlan**
- **protected-vlan**

4.1.12 rrpp enable

Syntax

rrpp enable

undo rrpp enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

rrpp enable コマンドは RRPP を有効にします。

undo rrpp enable コマンドは RRPP を無効にします。

RRPP ドメインをアクティブ状態にするため、RRPP と RRPP ドメインの RRPP リングを有効にします。

例

RRPP を有効にします。

<Switch> system-view

[Switch] rrpp enable

関連コマンド

ring enable

4.1.13 rrpp ring-group

Syntax

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ring-group-id: RRPP リンググループの ID を指定します。設定範囲は 1～64 です。

説明

rrpp ring-group コマンドは RRPP リンググループを作成し、RRPP ring group view に移行するか、既存の RRPP ring group view に移行します。

undo rrpp ring-group コマンドは RRPP リンググループを削除します。

リンググループを削除するとき、最初にエッジノードのリンググループを削除し、次にアシスタントエッジノードのリンググループを削除してください。そうでない場合、ア

シスタントエッジノードが Edge-Hello パケットの受信に失敗する可能性があり、誤ってプライマリリングが故障したと認識します。

リンググループが削除されたのち、リンググループのすべてのサブリングはいずれのリンググループに属していないことになります。

例

RRPP リンググループ 1 を作成し、RRPP ring group view に移行します。

<Switch> system-view

[Switch] rrpp ring-group 1

[Switch-ring-group1]

関連コマンド

- **display rrpp ring-group**
- **domain ring**

4.1.14 snmp-agent trap enable rrpp

Syntax

snmp-agent trap enable rrpp [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *

undo snmp-agent trap enable rrpp [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

major-fault: アシスタントエッジノードとエッジノード間の SRPT が切断されたとき、SNMP notification を送信します。

multi-master: RRPP リングに複数のマスタノードが設定されているとき、SNMP notification を送信します。

ring-fail: RRPP リングの状態が Health から Disconnect に遷移したとき、SNMP notification を送信します。

ring-recover: RRPP リングの状態が Disconnect から Health に遷移したとき、SNMP notification を送信します。

説明

snmp-agent trap enable rrpp コマンドは RRPP の SNMP notification を有効にします。

undo snmp-agent trap enable rrpp コマンドは RRPP の SNMP notification を無効にします。

NMS に重大な RRPP イベントを通知するため、RRPP の SNMP notification を有効にします。SNMP notification を送信するため、必要なパラメータを設定してください。SNMP notification の詳細は、オペレーションマニュアルのセクション 10 *システム管理* “*SNMP*”を参照してください。

パラメータを指定しない場合、**snmp-agent trap enable rrpp** コマンドは装置でサポートするすべての SNMP notification を有効にします。**undo snmp-agent trap enable rrpp** コマンドは装置でサポートするすべての SNMP notification を無効にします。

例

RRPP リングの状態が Disconnect から Health に遷移したとき、SNMP notification を送信します。

<Switch> system-view

[Switch] snmp-agent trap enable rrpp ring-recover

4.1.15 timer

Syntax

timer hello-timer *hello-value* **fail-timer** *fail-value*

undo timer

デフォルト

Hello タイマは 1 秒、Fail タイマは 3 秒です。

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

hello-timer *hello-value*: Hello タイマを指定します。設定範囲は 1～10 秒です。

fail-timer *fail-value*: Fail タイマを指定します。設定範囲は 3～30 秒です。

説明

timer コマンドは Hello タイマと Fail タイマを設定します。

undo timer コマンドはデフォルトに戻します。

Fail タイマは Hello タイマの 3 倍以上にする必要があります。

例

RRPP ドメイン 1 の Hello タイマを 2 秒、Fail タイマを 7 秒に設定します。

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1] timer hello-timer 2 fail-timer 7

目次

このセクションのページは **9-x-x** です。

5 章 Smart Link 5-1
5.1 Smart Link 設定コマンド 5-1
5.1.1 display smart-link flush 5-1
5.1.2 display smart-link group 5-2
5.1.3 flush enable 5-3
5.1.4 port 5-4
5.1.5 port smart-link group 5-5
5.1.6 port smart-link group track 5-7
5.1.7 preemption delay 5-9
5.1.8 preemption mode 5-10
5.1.9 protected-vlan 5-10
5.1.10 reset smart-link statistics 5-12
5.1.11 smart-link flush enable 5-12
5.1.12 smart-link group 5-13

5章 Smart Link

5.1 Smart Link設定コマンド

5.1.1 display smart-link flush

Syntax

display smart-link flush

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display smart-link flush コマンドは受信した flush メッセージの情報を表示します。

例

受信した flush メッセージの情報を表示します。

<Switch> display smart-link flush

```
Received flush packets                          : 10
 Receiving interface of the last flush packet      : GigabitEthernet1/0/1
 Receiving time of the last flush packet          : 19:19:03 2012/04/21
 Device ID of the last flush packet              : 000f-e200-8500
 Control VLAN of the last flush packet            : 1
```

表 5-1 コマンド出力

フィールド	説明
Received flush packets	受信したflushメッセージの情報の総数です。
Receiving interface of the last flush packet	最後にflushメッセージを受信したポートです。
Receiving time of the last flush packet	最後にflushメッセージを受信した時間です。
Device ID of the last flush packet	最後にflushメッセージを受信した装置のIDです。
Control VLAN of the last flush packet	最後にflushメッセージを受信した制御VLANのIDです。

関連コマンド

reset smart-link statistics

5.1.2 display smart-link group

Syntax

display smart-link group { *group-id* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: Smart Link グループの ID を指定します。設定範囲は 1～48 です。

all: すべての Smart Link グループの情報を表示します。

説明

display smart-link group コマンドは指定した Smart Link グループあるいはすべての Smart Link グループの情報を表示します。

例

Smart Link グループ 1 の情報を表示します。

<Switch> display smart-link group 1

```
Smart link group 1 information:
  Device ID      : 0011-2200-0001
  Preemption mode : None
  Preemption delay: 1(s)
  Control VLAN    : 1
  Protected VLAN  : Reference Instance 2, 4

  Member               Role     State   Flush-count    Last-flush-time

--------------------------------------------------------------------------------
  GE1/0/1              PRIMARY   ACTIVE  1            16:45:20 2012/04/21
  GE1/0/2              SECONDARY STANDBY 2             16:37:20 2012/04/21
```

表 5-2 コマンド出力

フィールド	説明
Preemption mode	Preemptionモードです。 ● **None**—Preemptionが無効です。 ● **Role**—Role preemptionモードです。 ● **Speed**—Speed preemptionモードです。
Preemption delay	Preemption delay時間です。単位は秒です。
Control-VLAN	制御VLAN IDです。
Protected VLAN	Smart Linkグループのプロテクトvlanです。参照するMSTI（Multiple Spanning Tree Instances）が表示されます。参照するMSTIにマッピングされるVLANを表示する場合、**display stp region-configuration**コマンドを使用します。
Member	Smart Linkグループのメンバポートです。
Role	ポートの役割です。primary、secondaryがあります。
State	ポート状態です。active、down、standbyがあります。
Flush-count	転送されたflushメッセージの数です。
Last-flush-time	最後にflushメッセージが転送した時間です。（flushメッセージが転送されていない場合、**NA**と表示されます。）

5.1.3 flush enable

Syntax

flush enable [**control-vlan** *vlan-id*]

undo flush enable

デフォルト

Smart Link グループの flush アップデートは有効です。flush メッセージの送信は VLAN 1 を使用します。

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

control-vlan *vlan-id*: flush メッセージを送信する制御 VLAN を指定します。設定範囲は 1 ～4094 です。

説明

flush enable コマンドは flush アップデートを有効にします。

undo flush enable コマンドは flush アップデートを無効にします。

Smart link グループで設定された制御 VLAN は、他の Smart Link グループに設定された制御 VLAN と異なるようにしてください。

- 設定された制御 VLAN が作成されていることを確認してください。制御 VLAN に Smart Link メンバポートを割り当ててください。
- Smart Link グループの制御 VLAN はプロテクト VLAN にしてください。制御 VLAN を削除しないでください。制御 VLAN を削除すると flush メッセージを正常に送信することができません。

例

Smart Link グループ 1 の flush アップデートを無効にします。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1] undo flush enable

関連コマンド

smart-link flush enable

5.1.4 port

Syntax

port *interface-type interface-number* { **primary** | **secondary** }

undo port *interface-type interface-number*

デフォルト

設定なし

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ポートのタイプと番号を指定します。ポートはレイヤ 2 Ethernet インタフェースあるいはアグリゲートインタフェースが設定できます。

primary: ポートを primary ポートとして指定します。

secondary: ポートを secondary ポートとして指定します。

説明

port コマンドはポートを Smart Link グループに割り当て、ポートの役割を指定します。

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 グループにメンバポートを設定する前に、Smart Link グループにプロテクト VLAN を設定する必要があります。

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と RRPP 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と RRPP を有効にすることができません。

ポートにアグリゲーショングループメンバと Smart Link グループメンバの両方を設定した場合、アグリゲーショングループの設定が適用されます。ポートは **display smart-link group** コマンドで表示されません。Smart Link グループの設定はアグリゲーショングループからポートを削除した後、適用されます。

interface view で **port smart-link group** コマンドを使用して Smart Link グループにポートを割り当てることができます。

例

GigabitEthernet 1/0/1 を Smart Link グループ 1 の secondary ポートとして設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo stp enable

[Switch-GigabitEthernet1/0/1] quit

[Switch] smart-link group 1

[Switch-smlk-group1] protected-vlan reference-instance 0

[Switch-smlk-group1] port gigabitethernet 1/0/1 secondary

関連コマンド

port smart-link group

5.1.5 port smart-link group

Syntax

port smart-link group *group-id* { **primary** | **secondary** }

undo port smart-link group *group-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-id: Smart Link グループの ID を指定します。設定範囲は 1～48 です。

primary: ポートを primary ポートとして指定します。

secondary: ポートを secondary ポートとして指定します。

説明

port smart-link group コマンドは現在のポートを指定された Smart Link グループのメンバポートとして設定します。

undo port smart-link group コマンドは指定された Smart Link グループからポートを削除します。

Smart Link グループにメンバポートを設定する前に、Smart Link グループにプロテクト VLAN を設定する必要があります。

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と RRPP 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と RRPP を有効にすることができません。

ポートにアグリゲーショングループメンバと Smart Link グループメンバの両方を設定した場合、アグリゲーショングループの設定が適用されます。ポートは **display smart-link group** コマンドで表示されません。Smart Link グループの設定はアグリゲーショングループからポートを削除した後、適用されます。

smart link group view で **port** コマンドを使用して Smart Link グループにポートを割り当てることができます。

例

GigabitEthernet 1/0/1 を Smart Link グループ 1 の primary ポートとして設定します。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1] protected-vlan reference-instance 0

[Switch-smlk-group1] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo stp enable

[Switch-GigabitEthernet1/0/1] port smart-link group 1 primary

アグリゲートインタフェース 1 を Smart Link グループ 1 の primary ポートとして設定します。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1] protected-vlan reference-instance 0

[Switch-smlk-group1] quit

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] undo stp enable

[Switch-Bridge-Aggregation1] port smart-link group 1 primary

関連コマンド

port

5.1.6 port smart-link group track

Syntax

port smart-link group *group-id* **track** *track-entry-number*

undo port smart-link group *group-id* **track** *track-entry-number*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-id: Smart Link グループの ID を指定します。設定範囲は 1～48 です。

track-entry-number: CFD の CC 機能に関連づけられる track エントリの ID を指定します。

説明

port smart-link group track コマンドは Smart Link グループメンバポートと track エントリ間のコラボレーションを設定します。

undo port smart-link group track コマンドはコラボレーションを削除します。

Smart Link は、トラックエントリを介してリンク検出プロトコルと連携します。リンク検出を実装するために CFD の CC 機能のみをサポートします。CFD の CC 機能をトラックエントリに関連付けるには、**track cfd** コマンドを使用します。

ポートで Smart Link と track 間のコラボレーションを設定する前に、指定した Smart Link グループにポートが追加されていることを確認してください。

例

リンクの状態を検出するため、GigabitEthernet 1/0/1 の Smart Link グループ 1 の primary ポートと、track エントリ 1 を通した CFD の CC 機能のコラボレーションを設定します。

<Switch> system-view

[Switch] track 1 cfd cc service-instance 100 mep 2

[Switch-track-1] quit

[Switch] smart-link group 1

[Switch-smlk-group1] protected-vlan reference-instance 0

[Switch-smlk-group1] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo stp enable

[Switch-GigabitEthernet1/0/1] port smart-link group 1 primary

[Switch-GigabitEthernet1/0/1] port smart-link group 1 track 1

リンクの状態を検出するため、ブリッジアグリゲーション 1 の Smart Link グループ 1 の primary ポートと、track エントリ 1 を通した CFD の CC 機能のコラボレーションを設定します。

<Switch> system-view

[Switch] track 1 cfd cc service-instance 100 mep 2

[Switch-track-1] quit

[Switch] smart-link group 1

[Switch-smlk-group1] protected-vlan reference-instance 0

[Switch-smlk-group1] quit

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] undo stp enable

[Switch-Bridge-Aggregation1] port smart-link group 1 primary

[Switch-Bridge-Aggregation1] port smart-link group 1 track 1

関連コマンド

track cfd

5.1.7 preemption delay

Syntax

preemption delay *delay*

undo preemption delay

デフォルト

1 秒

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

delay: preemption delay を指定します。設定範囲は 0～300 秒です。

説明

preemption delay コマンドは preemption delay を設定します。

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

preemption delay は上流装置の切り替えとのコラボレーションを引き継ぐ前に、primary ポートが待機する時間です。

preemption delay は preemption mode を有効にしたのち適用されます。

例

role preemption を有効にし、preemption delay を 10 秒に設定します。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1] preemption mode role

[Switch-smlk-group1] preemption delay 10

関連コマンド

preemption mode

5.1.8 preemption mode

Syntax

preemption mode role

undo preemption mode

デフォルト

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

role: role preemption モードを設定します。このモードは primary リンクが回復した後に primary ポートがフォワーディング状態に移行できるようにします。

説明

preemption mode コマンドは Smart Link グループの preemption モードを設定します。

undo preemption mode コマンドはデフォルトに戻します。

例

role preemption モードを有効にします。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1] preemption mode role

5.1.9 protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

デフォルト

設定なし

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

reference-instance *instance-id-list*: 最大 10 個の MSTI 項目を空白で区切ったリストを指定します。各項目は、*instance-id 1* から *instance-id 2* の形式で MSTI ID または MSTI ID の範囲を指定します。設定範囲は 0～4094 です。MSTI ID が 0 の場合、CIST（common internal spanning tree）です。*instance-id 2* は、*instance-id 1* 以上である必要があります。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属している VLAN は、Smart link グループのプロテクト VLAN として設定しなければなりません。

関連づけされた MSTI にマップされた VLAN が変更すると、プロテクト VLAN も変更されます。

プロテクト VLAN 設定を削除するには、次の制限および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* が指定されている場合、MSTP モードで指定された 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。
- **undo protected-vlan** コマンドで **reference-instance** *instance-id-list* を指定されている場合、PVST モードで指定された 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 の設定を削除します。
- Smart link グループにメンバポートがある場合は、プロテクト VLAN 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ない場合は、プロテクト VLAN 設定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、Smart link グループ 1 のプロテクト VLAN として MSTI 1 をマッピングします。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] instance 1 vlan 1 to 30

[Switch-mst-region] active region-configuration

[Switch-mst-region] quit

[Switch] smart-link group 1

[Switch-smlk-group1] protected-vlan reference-instance 1

関連コマンド

- **display stp region-configuration** (コマンドマニュアルのセクション 3 *アクセス*)
- **smart-link group**

5.1.10 reset smart-link statistics

Syntax

reset smart-link statistics

View

User view

定義済みユーザロール

network-admin

説明

reset smart-link statistics コマンドは flush メッセージの統計情報を削除します。

例

flush メッセージの統計情報を削除します。

<Switch> reset smart-link statistics

関連コマンド

display smart-link flush

5.1.11 smart-link flush enable

Syntax

smart-link flush enable [**control-vlan** *vlan-id-list*]

undo smart-link flush enable [**control-vlan** *vlan-id-list*]

デフォルト

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

control-vlan *vlan-id-list*: 最大 10 の flush メッセージを受信するために使用する制御 VLAN のスペース区切りリストを指定します。各項目は、*vlan-id1* から *vlan-id2* の形式で、制御 VLAN ID または制御 VLAN ID の範囲を指定します。設定範囲は 1～4094 です。デフォルトは 1 です。vlan-id2 は、vlan-id1 以上でなければなりません。

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 1 で受信することを GigabitEthernet 1/0/1 で有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] smart-link flush enable

flush メッセージを制御 VLAN 1 で受信することをアグリゲートインタフェース 1 で有効にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] smart-link flush enable

関連コマンド

flush enable

5.1.12 smart-link group

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: Smart Link グループの ID を指定します。設定範囲は 1～48 です。

説明

smart-link group コマンドは Smart Link グループを作成し、smart link group view に移行するか、デフォルトの smart link group view を移行します。

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 **9-x-x** です。

6 章 Monitor Link 6-1
6.1 Monitor Link 設定コマンド 6-1
6.1.1 display monitor-link group 6-1
6.1.2 monitor-link group 6-2
6.1.3 port 6-3
6.1.4 port monitor-link group 6-4

6章 Monitor Link

6.1 Monitor Link設定コマンド

6.1.1 display monitor-link group

Syntax

display monitor-link group { *group-id* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: Monitor Link グループの ID を指定します。設定範囲は 1～16 です。

all: すべての Monitor Link グループを指定します。

説明

display monitor-link group コマンドは Monitor Link グループの情報を表示します。

このコマンドはリンクアグリゲーショングループに所属しているポートの情報を表示しません。

例

すべてのモニタリンクグループの情報を表示します。

<Switch> display monitor-link group all

```
Monitor link protocol status: Disabled
Monitor link group 1 information:
  Group status    : N/A
  Downlink up-delay: 0(s)
  Last-up-time    : -
  Last-down-time  : -
  Up-port-threshold: 1

  Member                 Role      Status
  ---------------------------------------------
  GE1/0/1               UPLINK    UP
```

```
GE1/0/2                DOWNLINK   UP
```

表 6-1 コマンド出力

フィールド	説明
Monitor link protocol status	Monitor Link プロトコル状態です。 ● Enabled ● Disabled
Group status	Monitor Linkグループの状態です。 ● **Up** ● **Down** ● **N/A**－Monitor Linkがグローバルに無効になっていて、Monitor Linkグループが操作できません。
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ためのアップリンクインタフェースのしきい値です。
Member	Monitor Linkグループのメンバインタフェースです。
Role	インタフェースの役割です。アップリンクインタフェース、ダウンリンクインタフェースがあります。
Status	メンバリンクの状態です。up、downがあります。

6.1.2 monitor-link group

Syntax

monitor-link group *group-id*

undo monitor-link group *group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: Monitor Link グループの ID を指定します。設定範囲は 1～16 です。

説明

monitor-link group コマンドは Monitor Link グループを作成し、monitor link group view に移行するか、デフォルトの monitor link group view に移行します。

undo monitor-link group コマンドは Monitor Link グループを削除します。

例

Monitor Link グループ 1 を作成し、monitor link group view に移行します。

<Switch> system-view

[Switch] monitor-link group 1

[Switch-mtlk-group1]

6.1.3 port

Syntax

port *interface-type interface-number* { **downlink** | **uplink** }

undo port *interface-type interface-number*

デフォルト

設定なし

View

Monitor link group view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

downlink: ダウンリンクインタフェースを指定します。

uplink: アップリンクインタフェースを指定します。

説明

port コマンドは Monitor Link グループにインタフェースを割り当てます。

undo port コマンドは Monitor Link グループからインタフェースを削除します。

インタフェースは、1 つの monitor-link group に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。

アグリゲーショングループの Selected ポートを Monitor Link グループのダウンリンクインタフェースとして設定した場合は、アグリゲーショングループの Unselected ポートを Monitor Link グループのアップリンクインタフェースとして設定しないでください。

Monitor Link の動作の中断を防ぐため、アグリゲートインタフェースとアグリゲーショングループのメンバポートを同じ Monitor Link グループに割り当てないでください。

例

Monitor Link グループ 1 のアップリンクインタフェースとして GigabitEthernet 1/0/1 を設定し、ダウンリンクインタフェースとして GigabitEthernet 1/0/2 を設定します。

<Switch> system-view

[Switch] monitor-link group 1

[Switch-mtlk-group1] port gigabitethernet 1/0/1 uplink

[Switch-mtlk-group1] port gigabitethernet 1/0/2 downlink

関連コマンド

port monitor-link group

6.1.4 port monitor-link group

Syntax

port monitor-link group *group-id* { **downlink** | **uplink** }

undo port monitor-link group *group-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-id: Monitor Link グループの ID を指定します。設定範囲は 1～16 です。

downlink: ダウンリンクインタフェースを指定します。

uplink: アップリンクインタフェースを指定します。

説明

port monitor-link group コマンドはメンバインタフェースとして Monitor Link グループに現在のインタフェースを割り当てます。

undo port monitor-link group コマンドは Monitor Link グループから現在のインタフェースを削除します。

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。

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。

アグリゲーショングループの Selected ポートを Monitor link グループのダウンリンクインタフェースとして設定した場合は、アグリゲーショングループの Unselected ポートを Monitor link グループのアップリンクインタフェースとして設定しないでください。

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 **9-x-x** です。

7 章 BFD.....7-1
7.1 BFD 設定コマンド.....7-1
7.1.1 bfd authentication-mode.....7-1
7.1.2 bfd demand enable.....7-2
7.1.3 bfd detect-multiplier.....7-3
7.1.4 bfd echo enable.....7-4
7.1.5 bfd echo-source-ip.....7-5
7.1.6 bfd min-echo-receive-interval.....7-6
7.1.7 bfd min-receive-interval.....7-7
7.1.8 bfd min-transmit-interval.....7-8
7.1.9 bfd multi-hop authentication-mode.....7-9
7.1.10 bfd multi-hop destination-port.....7-10
7.1.11 bfd multi-hop detect-multiplier.....7-11
7.1.12 bfd multi-hop min-receive-interval.....7-12
7.1.13 bfd multi-hop min-transmit-interval.....7-13
7.1.14 bfd session init-mode.....7-14
7.1.15 display bfd session.....7-14
7.1.16 reset bfd session statistics.....7-18
7.1.17 snmp-agent trap enable bfd.....7-19

7章 BFD

7.1 BFD設定コマンド

7.1.1 bfd authentication-mode

Syntax

bfd authentication-mode { **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd authentication-mode

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

md5: MD5 アルゴリズムを指定します。

sha1: SHA1 アルゴリズムを指定します。

simple: simple 認証モードを指定します。

key-id: 認証 key ID を設定します。設定範囲は 1～255 です。

cipher: 暗号文パスワードを設定します。

plain: プレーンテキストパスワードを設定します。セキュリティ保護のため、プレーンテキスト形式で指定されたキーは暗号化された形式で保存されます。

string: キーを指定します。プレーンテキストパスワードです。大文字、小文字を区別し、設定範囲は 1~16 文字です。暗号化された形式は、大文字、小文字を区別します。設定範囲は 33～53 文字です。

説明

bfd authentication-mode コマンドはシングル hop BFD コントロールパケットの BFD 認証モードを設定します。

undo bfd authentication-mode コマンドは設定をデフォルトに戻します。

BFD セッションセキュリティを強化するためにこのコマンドを使用してください。

BFD バージョン 0 では、このコマンドはサポートされていません。設定を発効しません。

例

VLAN-interface 11 にシングル hop BFD コントロールパケットの simple 認証モードを設定します。key ID は **1** で、パスワードは **123456** です。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd authentication-mode simple 1 plain 123456

7.1.2 bfd demand enable

Syntax

bfd demand enable

undo bfd demand enable

デフォルト

Asynchronous モード

View

Interface view

定義済みユーザロール

network-admin

説明

bfd demand enable コマンドは Demand BFD セッションモードを有効にします。

undo bfd demand enable コマンドは設定をデフォルトに戻します。

Demand モードでは、装置は BFD コントロールパケットを周期的に送信します。ピアの片端がデフォルト設定の Asynchronous モードで動作する場合、BFD コントロールパケットの送信を停止します。片端が Demand モードで動作する場合、両端装置で BFD コントロールパケットの送信を停止します。別のシステムへの接続性が明示する必要がある際は、システムはネゴシエートした送信間隔で Poll(P)ビットがセットされた BFD コントロールパケットを数回送信します。検出時間内に応答がない場合、セッションがダウンしたとみなします。接続していると認識した場合、次のコマンドが送信されるまで BFD コントロールパケットを送信しません。

Asynchronous モードでは、装置は BFD コントロールパケットを周期的に送信します。指定した時間内に BFD コントロールパケットを受信しない場合、装置はセッションがダウンしたとみなします。

BFD バージョン 0 では、このコマンドはサポートされていません。設定を発効しません。

例

VLAN-interface 11 で Demand BFD セッションモードを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd demand enable

7.1.3 bfd detect-multiplier

Syntax

bfd detect-multiplier *value*

undo bfd detect-multiplier

デフォルト

5

View

Interface view

定義済みユーザロール

network-admin

パラメータ

value: シングル Hop 検出時間の乗数を指定します。設定範囲は 3～50 です。

説明

bfd detect-multiplier コマンドは制御パケットモードのシングル Hop 検出時間乗数とエコーパケットモードの検出時間乗数を設定します。

undo bfd detect-multiplier コマンドはデフォルトに戻します。

検出時間の乗数は、廃棄される同時 BFD パケット（コントロールパケットとエコーパケットを含みます）の最大数を決定します。

表 7-1 検出間隔の計算方法

モード	検出間隔
エコーパケットモード	送信側の検出時間の乗数×送信側の実際のパケット送信間隔
BFDセッションのasynchronousモードのコントロールパケットモード	受信側の検出時間の乗数×受信側の実際のパケット送信間隔

モード	検出間隔
BFDセッションのdemandモードのコントロールパケットモード	送信側の検出時間の乗数×送信側の実際のパケット送信間隔

例

VLAN インタフェース 11 のシングル Hop 検出時間の乗数とエコーパケットモードの検出時間乗数を 6 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd detect-multiplier 6

7.1.4 bfd echo enable

Syntax

bfd echo enable

undo bfd echo enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

bfd echo enable コマンドはエコーパケットモードを有効にします。

undo bfd echo enable コマンドは設定をデフォルトに戻します。

コントロールパケットが送信されてセッションがアップしている BFD セッションにエコーパケットモードを有効にした場合、BFD は以下を行います。

- リンク接続を検出するために周期的にエコーパケットを送信します。
- 同時にコントロールパケットの受信レートを下げます。

このコマンドはエコーパケットの受信機能と送信機能の両方を有効にします。

BFD バージョン 0 では、このコマンドはサポートされていません。設定を発効しません。

例

VLAN-interface 11 でエコーパケットモードを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd echo enable

7.1.5 bfd echo-source-ip

Syntax

bfd echo-source-ip *ip-address*

undo bfd echo-source-ip

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: BFD エコーパケットの送信元 IP アドレスを指定します。

説明

bfd echo-source-ip コマンドは BFD エコーパケットの送信元 IP アドレスを設定します。

undo bfd echo-source-ip コマンドは BFD エコーパケットの送信元 IP アドレスを削除します。

送信元 IP アドレスは、ローカルインタフェースの IP アドレスと同一ネットワークセグメントに属することができません。そうでなければ、大量の ICMP リダイレクトパケットがピアから送信され、リンクの衝突が発生する可能性があります。

例

BFD エコーパケットの送信元 IP アドレスを 8.8.8.8 に設定します。

<Switch> system-view

[Switch] bfd echo-source-ip 8.8.8.8

7.1.6 bfd min-echo-receive-interval

Syntax

bfd min-echo-receive-interval *interval*

undo bfd min-echo-receive-interval

デフォルト

400 ミリ秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

interval: BFD エコーパケットの最小受信間隔を指定します。単位はミリ秒です。設定範囲は 100～1000 ミリ秒、あるいは 0 です。

説明

bfd min-echo-receive-interval コマンドは BFD エコーパケットの最小受信間隔を設定します。

undo bfd min-echo-receive-interval コマンドはデフォルトに戻します。

このコマンドは BFD エコーパケットを受信する間隔を設定します。この間隔は実際の BFD エコーパケットを送信する間隔です。

次の条件が満たされると、ローカルエンドはリモートエンドとの自動ネゴシエーション後にエコーパケットの送信を停止します。

- ローカルエンドでエコーパケットモードが有効になっています。
- BFD エコーパケットを受信する最小間隔は、リモートエンドで 0 ミリ秒に設定されています。

例

VLAN インタフェース 11 の BFD エコーパケットの最小受信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd min-echo-receive-interval 500

7.1.7 bfd min-receive-interval

Syntax

bfd min-receive-interval *interval*

undo bfd min-receive-interval

デフォルト

400 ミリ秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

v7.1.8 を含むそれ以前

interval: シングル Hop BFD コントロールパケットの最小受信間隔を指定します。単位はミリ秒です。設定範囲は 100～1000 ミリ秒です。

v7.2.16 を含むそれ以降

interval: シングル Hop BFD コントロールパケットの最小受信間隔を指定します。単位はミリ秒です。設定範囲は 3～1000 ミリ秒です。

説明

bfd min-receive-interval コマンドはシングル Hop BFD コントロールパケットの最小受信間隔を設定します。

undo bfd min-receive-interval コマンドはデフォルトに戻します。

リモートエンド装置の BFD コントロールパケット送信レートが、ローカルエンド装置の BFD コントロールパケット受信レートを超過することを防止するため、このコマンドを設定します。

リモートエンド装置の実際の BFD コントロールパケットの送信間隔は、以下の値の間の大きい値を取ります。

- リモートエンド装置の BFD コントロールパケットの最小送信間隔
- ローカルエンド装置の BFD コントロールパケットの最小受信間隔

例

VLAN インタフェース 11 のシングル Hop BFD コントロールパケットの最小受信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd min-receive-interval 500

7.1.8 bfd min-transmit-interval

Syntax

bfd min-transmit-interval *interval*

undo bfd min-transmit-interval

デフォルト

400 ミリ秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

v7.1.8 を含むそれ以前

interval: シングル Hop BFD コントロールパケットの最小送信間隔を指定します。単位はミリ秒です。設定範囲は 100～1000 ミリ秒です。

v7.2.16 を含むそれ以降

interval: シングル Hop BFD コントロールパケットの最小送信間隔を指定します。単位はミリ秒です。設定範囲は 3～1000 ミリ秒です。

説明

bfd min-transmit-interval コマンドはシングル Hop BFD コントロールパケットの最小送信間隔を設定します。

undo bfd min-transmit-interval コマンドはデフォルトに戻します。

このコマンドは BFD パケットの送信レートがエンド装置の能力を超過しないようにします。

ローカルエンド装置の実際の BFD コントロールパケットの送信間隔は、以下の値の間で大きい方の値になります。

- ローカルエンド装置の BFD コントロールパケットの最小送信間隔
- リモートエンド装置の BFD コントロールパケットの最小受信間隔

例

VLAN インタフェース 11 のシングル Hop BFD コントロールパケットの最小送信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd min-transmit-interval 500

7.1.9 bfd multi-hop authentication-mode

Syntax

bfd multi-hop authentication-mode { **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd multi-hop authentication-mode

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

md5: MD5 アルゴリズムを指定します。

sha1: SHA1 アルゴリズムを指定します。

simple: simple 認証モードを指定します。

key-id: 認証 key ID を設定します。設定範囲は 1～255 です。

cipher: 暗号文パスワードを設定します。

plain: プレーンテキストパスワードを設定します。セキュリティ保護のため、プレーンテキスト形式で指定されたキーは暗号化された形式で保存されます。

string: をキー指定します。プレーンテキストパスワードです。大文字小文字を区別し、設定範囲は 1～16 文字です。暗号化された形式は、大文字、小文字を区別します。設定範囲は、33～53 文字です。

説明

bfd multi-hop authentication-mode コマンドはマルチ Hop BFD コントロールパケットの認証モードを設定します。

undo bfd multi-hop authentication-mode コマンドは設定をデフォルトに戻します。

BFD セッションセキュリティを強化するためにこのコマンドを使用してください。

BFD バージョン 0 では、このコマンドはサポートされていません。設定を発効しません。

例

VLAN-interface 11 にマルチ hop BFD コントロールパケットの simple 認証モードを設定します。key ID は 1 で、パスワードは **123456** です。

<Switch> system-view

[Switch] bfd multi-hop authentication-mode simple 1 plain 123456

7.1.10 bfd multi-hop destination-port

Syntax

bfd multi-hop destination-port *port-number*

undo bfd multi-hop destination-port

デフォルト

4784

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: マルチ hop BFD コントロールパケットの宛先ポート番号を、3784 または 4784 と指定します。

説明

bfd multi-hop destination-port コマンドはマルチ hop BFD コントロールパケットの宛先ポート番号を設定します。

undo bfd multi-hop destination-port コマンドは設定をデフォルトに戻します。

例

マルチ hop BFD コントロールパケットの宛先ポート番号を 3784 で指定します。

<Switch> system-view

[Switch] bfd multi-hop destination-port 3784

7.1.11 bfd multi-hop detect-multiplier

Syntax

bfd multi-hop detect-multiplier *value*

undo bfd multi-hop detect-multiplier

デフォルト

5

View

System view

定義済みユーザロール

network-admin

パラメータ

value: マルチ Hop 検出時間の乗数を指定します。設定範囲は 3～50 です。

説明

bfd multi-hop detect-multiplier コマンドはマルチ Hop 検出時間の乗数を設定します。

undo bfd multi-hop detect-multiplier コマンドは設定をデフォルトに戻します。

検出時間の乗数は、廃棄される同時 BFD コントロールパケットの最大数を決定します。

表 7-2 検出間隔の計算方法

モード	検出間隔
BFDセッションのasynchronousモードのコントロールパケットモード	受信側の検出時間の乗数×受信側の実際のパケット送信間隔
BFDセッションのdemandモードのコントロールパケットモード	送信側の検出時間の乗数×送信側の実際のパケット送信間隔

例

マルチ Hop 検出時間の乗数を 6 で設定します。

<Switch> system-view

[Switch] bfd multi-hop detect-multiplier 6

7.1.12 bfd multi-hop min-receive-interval

Syntax

bfd multi-hop min-receive-interval *interval*

undo bfd multi-hop min-receive-interval

デフォルト

400 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

v7.1.8 を含むそれ以前

interval: マルチ Hop BFD コントロールパケットの最小受信間隔を指定します。単位はミリ秒です。設定範囲は 100～1000 ミリ秒です。

v7.2.16 を含むそれ以降

interval: シングル Hop BFD コントロールパケットの最小受信間隔を指定します。単位はミリ秒で、設定範囲は 3～1000 ミリ秒です。

説明

bfd multi-hop min-receive-interval コマンドはマルチ Hop BFD コントロールパケットの最小受信間隔を設定します。

undo bfd multi-hop min-receive-interval コマンドは設定をデフォルトに戻します。

このコマンドは、リモート装置のパケット送信レートがローカルエンド装置の受信能力（コントロールパケットの最小受信間隔）を超えないようにするために使用します。受信能力を超えた場合、リモートエンド側は BFD コントロールパケットの送信間隔をローカルエンドのコントロールパケットの最小受信間隔に合わせて動的に調整します。

例

マルチ Hop BFD コントロールパケットの最小受信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] bfd multi-hop min-receive-interval 500

7.1.13 bfd multi-hop min-transmit-interval

Syntax

bfd multi-hop min-transmit-interval *interval*

undo bfd multi-hop min-transmit-interval

デフォルト

400 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

v7.1.8 を含むそれ以前

interval: マルチ Hop BFD コントロールパケットの最小送信間隔を指定します。単位はミリ秒です。設定範囲は 100～1000 ミリ秒です。

v7.2.16 を含むそれ以降

interval: シングル Hop BFD コントロールパケットの最小送信間隔を指定します。単位はミリ秒で、設定範囲は 3～1000 ミリ秒です。

説明

bfd multi-hop min-transmit-interval コマンドはマルチ Hop BFD コントロールパケットの最小送信間隔を設定します。

undo bfd multi-hop min-transmit-interval コマンドは設定をデフォルトに戻します。

このコマンドは BFD パケットの送信レートが装置の能力を超過しないようにするために使用します。

ローカルエンド装置の実際の BFD コントロールパケットの送信間隔は、以下の大きいほうの値になります。

- ローカルエンド装置の BFD コントロールパケットの最小送信間隔
- リモートエンド装置の BFD コントロールパケットの最小受信間隔

例

マルチ Hop BFD コントロールパケットの最小送信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] bfd multi-hop min-transmit-interval 500

7.1.14 bfd session init-mode

Syntax

bfd session init-mode { **active** | **passive** }

undo bfd session init-mode

デフォルト

アクティブ

View

System view

定義済みユーザロール

network-admin

パラメータ

active: アクティブモードを使用します。アクティブモードでは、リモートエンド装置から BFD コントロールパケットを受信するかどうかにかかわらず、BFD は BFD コントロールパケットをリモートエンド装置に能動的に送信します。

passive: パッシブモードを使用します。パッシブモードでは、BFD は BFD コントロールパケットをリモートエンド装置に能動的に送信しません。リモートエンド装置から BFD コントロールパケットを受信した後のみ BFD コントロールパケットを送信します。

説明

bfd session init-mode コマンドは BFD セッションを確立するためにモードを設定します。

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

BFD セッションを確立するため、少なくともアクティブモードで 1 つのエンド装置を動作させる必要があります。

BFD バージョン 0 では、このコマンドはサポートされていません。設定を発効しません。

例

セッションを確立するためにパッシブモードを設定します。

<Switch> system-view

[Switch] bfd session init-mode passive

7.1.15 display bfd session

Syntax

display bfd session [**discriminator** *value* | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

discriminator *value*: ローカル ID を指定します。設定範囲は 1～4294967295 です。指定しない場合、すべての BFD セッションの概要を表示します。

verbose: BFD セッションの詳細情報を表示します。指定しない場合、BFD セッションの概要情報を表示します。

説明

display bfd session コマンドは BFD セッションの情報を表示します。

例

すべての IPv4 BFD セッション情報を表示します。

<Switch> display bfd session

```
Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv4 session working in control packet mode:

LD/RD         SourceAddr      DestAddr        State    Holdtime    Interface
513/513       1.1.1.1         1.1.1.2         Up       2297ms      Vlan100
```

すべての IPv4 BFD セッションの詳細情報を表示します。

<Switch> display bfd session verbose

```
Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv4 session working in control packet mode:

     Local Discr: 513                Remote Discr: 513
       Source IP: 1.1.1.1          Destination IP: 1.1.1.2
   Session State: Up                    Interface: Vlan-interface100
    Min Tx Inter: 500ms               Act Tx Inter: 500ms
    Min Rx Inter: 500ms               Detect Inter: 2500ms
        Rx Count: 42                     Tx Count: 43
    Connect Type: Direct            Running Up for: 00:00:20
      Hold Time: 2078ms                 Auth mode: None
```

```
     Detect Mode: Async                    Slot: 0
       Protocol: STATIC
       Version:1
      Diag Info: No Diagnostic
```

すべての IPv6 BFD セッション情報を表示します。

<Switch> display bfd session

```
Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv6 session working in control packet mode:

     Local Discr: 513              Remote Discr: 513
       Source IP: FE80::20C:29FF:FED4:7171
  Destination IP: FE80::20C:29FF:FE72:AC4D
    Session State: Up                  Interface: Vlan100
       Hold Time: 2142ms
```

すべての IPv6 BFD セッションの詳細情報を表示します。

<Switch> display bfd session verbose

```
Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv6 session working in control packet mode:

     Local Discr: 513              Remote Discr: 513
       Source IP: FE80::20C:29FF:FED4:7171
  Destination IP: FE80::20C:29FF:FE72:AC4D
    Session State: Up                  Interface: Vlan-interface100
     Min Tx Inter: 500ms             Act Tx Inter: 500ms
     Min Rx Inter: 500ms             Detect Inter: 2500ms
       Rx Count: 38                    Tx Count: 38
     Connect Type: Direct           Running Up for: 00:00:15
       Hold Time: 2211ms               Auth mode: None
     Detect Mode: Async                    Slot: 0
       Protocol: STATIC6
       Version:1
      Diag Info: No Diagnostic
```

表 7-3 コマンド出力

フィールド	説明
Total Session Num	BFDセッションの総数です。

フィールド	説明
Up Session Num	アクティブのBFDセッションの総数です。
Init Mode	BFDの動作モードです。active、passiveがあります。
IPv4 session working in control packet mode	BFDセッションの種類と動作モードです。 ● IPv4セッションが制御パケットモードで動作しています。 ● IPv4セッションがエコーモードで動作しています。 ● IPv6セッションが制御パケットモードで動作しています。 ● IPv6セッションがエコーモードで動作しています。
Local Discr/LD	セッションのローカルIDです。
Remote Discr/RD	セッションのリモートIDです。
Source IP/SourceAddr	セッションの送信元IPアドレスです。
Destination IP/DestAddr	セッションの宛先IPアドレスです。
Session State/State	セッションの状態です。**up**、**Init**、**down**があります。
Interface	セッションのインタフェース名です。
Min Tx Inter	最小送信間隔です。
Min Rx Inter	最小受信間隔です。
Act Tx Inter	実際の送信間隔です。
Detect Inter	実際のセッション検出タイマです。
Rx Count	受信したパケット数です。
Tx Count	送信したパケット数です。
Hold Time/Holdtime	セッションタイマが終了するまでの時間です。単位はミリ秒です。**Down**状態のBFDセッションの場合、このフィールドには**0ms**が表示されます。
Auth mode	セッション認証モードです。
Connect Type	インタフェースの接続タイプです。direct、indirectがあります。
Running up for	セッションがアップとなる間隔です。

フィールド	説明
Detect Mode	検出モードです。 • **Async**—Asynchronousモードです。 • **Demand**—Demandモードです。 • **Async / Echo**—エコー検出が有効になっているAsynchronousモードです。 • **Demand / Echo**—エコー検出が有効になっているDemandモードです。
Slot	IRFスタックのメンバIDです。
Diag Info	セッションの診断情報です。 • **No Diagnostic**—BFDセッションがupの時は、BFDパケットを受信しません。 • **Control Detection Time Expired**—ローカル検出がタイムアウトしたため、制御パケットモードのBFDセッションが停止しました。 • **Echo Function Failed**—ローカル検出がタイムアウトするか、エコーパケットの送信元IPアドレスが削除されたため、エコーパケットモードのBFDセッションが停止します。 • **Neighbor Signaled Session Down**—リモートエンドはローカルエンドにBFDセッションダウンを通知します。 • **Administratively Down**—ローカルシステムはBFDセッションが確立されないようにします。

7.1.16 reset bfd session statistics

Syntax

reset bfd session statistics

View

User view

定義済みユーザロール

network-admin

説明

reset bfd session statistics コマンドは BFD セッションの統計情報を削除します。

例

BFD セッションの統計情報を削除します。

<Switch> reset bfd session statistics

7.1.17 snmp-agent trap enable bfd

Syntax

snmp-agent trap enable bfd

undo snmp-agent trap enable bfd

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable bfd コマンドは BFD の SNMP 通知を有効にします。

undo snmp-agent trap enable bfd コマンドは BFD の SNMP 通知を無効にします。

BFD で重要なイベントを NMS に通知するため、SNMP 通知を作成します。BFD のイベントの通知を正しく送信するため、SNMP の設定を行ってください。SNMP の詳細は、オペレーションマニュアルのセクション 10 *システム管理* “*SNMP*”を参照してください。

例

BFD の SNMP 通知を無効にします。

<Switch> system-view

[Switch] undo snmp-agent trap enable bfd

目次

このセクションのページは **9-x-x** です。

8 章 Track.....8-1
8.1 Track 設定コマンド 8-1
8.1.1 display track 8-1
8.1.2 track bfd 8-4
8.1.3 track interface.....8-6
8.1.4 track interface protocol.....8-7
8.1.5 track nqa 8-8

8章 Track

8.1 Track設定コマンド

8.1.1 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 状態のトラックエントリを指定します。

positive: Positive 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概要情報を表示します。

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 track エントリの情報を表示します。

<Switch> display track all

```
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 10
    Remote IP/URL: --
    Local IP: --
    Interface: --
```

```
Track ID: 2
  State: NotReady
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 192.168.40.1
    Local IP: 192.168.40.2
Track ID: 3
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface:  Vlan-interface3
    Protocol: IPv4
Track ID: 4
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    CFD service instance: MEP 2 in Ethernet service instance 1
Track ID: 5
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    IP route: 0.0.0.0/0 reachability
    VPN instance name: --
    Protocol: BGP
    Nexthop interface : Vlan-Interface4
```

Negative 状態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 negative brief

```
ID   Status   Type      Remote IP/URL   Local IP       Interface
1    Negative Interface --            --             Vlan2
10   Negative Interface --            --             Vlan3
```

表 8-1 コマンド出力

フィールド	説明
Track ID	trackエントリのIDです。

フィールド	説明
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。
Notification delay: Positive 20, Negative 30 (in seconds)	● trackモジュールは、trackエントリ状態が20秒の遅延時間後、Positiveに変更するとアプリケーションモジュールに通知します。 ● trackモジュールは、trackエントリ状態が30秒の遅延時間後、Negativeに変更するとアプリケーションモジュールに通知します。
Tracked object	trackエントリに関連づけられたtrackオブジェクトです。
NQA entry	trackエントリに関連づけられたNQAオペレーションです。
Reaction	trackエントリに関連づけられたリアクションエントリです。
BFD session mode	BFDセッションモードです。エコーモードのみサポートします。
Outgoing interface	BFDエコーモードパケットの送信インタフェースです。
VPN instance name	BFDセッションパケットが属しているVPNインスタンス名です。パケットがパブリックネットワークに属している場合、2つの連続したハイフン（--）が表示されます。
Remote IP/URL	リモートIPアドレスまたはURLです。リモートIPアドレスまたはURLが存在しない場合は、2つの連続したハイフン（--）が表示されます。
Local IP	ローカルIPアドレスです。ローカルIPアドレスが存在しない場合は、2つの連続したハイフン（--）が表示されます。
Interface	モニタされるインタフェースです。インタフェースをモニタしない場合は、2つの連続したハイフン(--)が表示されます。
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。

フィールド	説明
IP route	トラックエントリに関連付けられたルートです。
VPN instance name	ルートが属するVPNインスタンスの名前です。ルートがパブリックネットワークに属している場合は、2つの連続したハイフン(--)が表示されます。
Protocol	ルートのプロトコルタイプです。ルートが存在しない場合は、**N/A**と表示されます。
Nexthop interface	ルートのネクストホップです。ルートが存在しない場合は、**N/A**と表示されます。
LLDP interface	モニタされるLLDP インタフェースです。
Type	モニタされるオブジェクトのタイプです。 • BFD • CFD • Interface • LLDP • NQA • Route

関連コマンド

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

8.1.2 track bfd

Syntax

track *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip-address* **local ip** *local-ip-address* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface *interface-type interface-number*: BFD エコーパケットを送信するインタフェースのタイプと番号を指定します。

remote ip *remote-ip-address*: BFD エコーパケットの宛先 IP アドレスを指定します。

local ip *local-ip-address*: BFD エコーパケットの送信元 IP アドレスを指定します。

delay: トラックモジュールは、トラックエントリのステータスの変化を、指定した遅延時間後に、アプリケーションモジュールに通知します。指定しない場合、トラックモジュールは、トラックエントリのステータスが変化すると、すぐにアプリケーションモジュールに通知します。

negative *negative-time*: トラックエントリの状態が Negative に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

positive *positive-time*: トラックエントリの状態が Positive に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

説明

track bfd コマンドは track エントリを作成し、BFD セッションに関連づけます。

undo track コマンドは track エントリを削除します。

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 bfd delay** コマンドのみを使用することができます。**track bfd delay** 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。

track エントリの他の設定を変更するには、**undo track** コマンドを実行して track エントリを削除してから、再度 **track bfd** コマンドを実行します。

トラックを BFD に関連付けると、VRRP group の仮想 IP アドレスを BFD セッションのローカルアドレスまたはリモートアドレスに指定することはできません。

例

track エントリ 1 を作成します。リモート IP アドレス 1.1.1.1、ローカル IP アドレス 1.1.1.2 間のリンクをモニタするため、BFD を使用します。VLAN インタフェース 2 から BFD パケットを送信します。

<Switch> system-view

[Switch] track 1 bfd echo interface vlan-interface 2 remote ip 1.1.1.1 local ip 1.1.1.2

関連コマンド

display track

8.1.3 track interface

Syntax

track *track-entry-number* **interface** *interface-type interface-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

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。

delay: トラックモジュールは、トラックエントリのステータスの変化を、指定した遅延時間後に、アプリケーションモジュールに通知します。指定しない場合、トラックモジュールは、トラックエントリのステータスが変化すると、すぐにアプリケーションモジュールに通知します。

negative *negative-time*: トラックエントリの状態が Negative に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

positive *positive-time*: トラックエントリの状態が Positive に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

説明

track interface コマンドは track エントリを作成し、インタフェースのリンク状態に関連づけます。

undo track コマンドは track エントリを削除します。

トラックをインタフェース管理に関連付けてインタフェースのリンク状態をモニタすると、トラックのエントリ状態が次のように変化します。

- 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。

インタフェースのリンク状態を表示する場合、**display ip interface brief** コマンドを使用します。

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。**track interface delay** 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。

track エントリの他の設定を変更するには、**undo track** コマンドを実行して track エントリを削除してから、再度 **track interface** コマンドを実行します。

例

track エントリ 1 を作成し、VLAN インタフェース 10 のリンク状態に関連づけます。

<Switch> system-view

[Switch] track 1 interface vlan-interface 10

関連コマンド

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

8.1.4 track interface protocol

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** } [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

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。インタフェースの IPv4 プロトコル状態を表示する場合、**display ip interface brief** コマンドを使用します。

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。インタフェースの IPv6 プロトコル状態を表示する場合、**display ipv6 interface brief** コマンドを使用します。

delay: トラックモジュールは、トラックエントリのステータスの変化を、指定した遅延時間後に、アプリケーションモジュールに通知します。指定しない場合、トラックモジュールは、トラックエントリのステータスが変化すると、すぐにアプリケーションモジュールに通知します。

negative *negative-time*: トラックエントリの状態が Negative に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

positive *positive-time*: トラックエントリの状態が Positive に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

説明

track interface protocol コマンドは track エントリを作成し、インタフェースのプロトコル状態に関連づけます。

undo track コマンドは track エントリを削除します。

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 protocol delay** コマンドのみを使用することができます。**track interface protocol delay** 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。

track エントリの他の設定を変更するには、**undo track** コマンドを実行して track エントリを削除してから、再度 **track interface protocol** コマンドを実行します。

例

track エントリ 1 を作成し、VLAN インタフェース 2 の IPv4 プロトコル状態に関連づけます。

<Switch> system-view

[Switch] track 1 interface vlan-interface 2 protocol ipv4

関連コマンド

- **display track**
- **display ip interface brief** (コマンドマニュアルのセクション 4 *IP サービス*)
- **display ipv6 interface brief** (コマンドマニュアルのセクション 4 *IP サービス*)

8.1.5 track nqa

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

entry *admin-name operation-tag*: track エントリに関連づけられる NQA オペレーションを指定します。*admin-name* は NQA オペレーションを作成する NQA オペレーションの管理者名です。設定範囲は 1～32 文字です。大文字、小文字を区別しません。*operation-tag* は NQA オペレーションのタグです。設定範囲は 1～32 文字です。大文字、小文字を区別しません。

reaction *item-number*: track エントリに関連づけられるリアクションエントリを指定します。*item-number* はリアクションエントリの ID です。設定範囲は 1～10 です。

説明

track nqa コマンドは track エントリを作成し、NQA オペレーションのリアクションエントリに関連づけます。

undo track コマンドは track エントリを削除します。

track 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 track エントリを削除してから、再度 **track nqa** コマンドを実行します。

例

track エントリ 1 を作成し、NQA オペレーション **admin-test** のリアクションエントリ 3 に関連づけます。

<Switch> system-view

[Switch] track 1 nqa entry admin test reaction 3

関連コマンド

display track

QX-S5300G シリーズ Ethernet スイッチ

コマンドマニュアル

10. システム管理

本マニュアルは以下に示す章で構成されています。

01-システムの保守とデバッグ

02-NQA

03-NTP

04-SNMP

05-RMON

06-NETCONF

07-プロセスモニタリングとメンテナンス

08-ポートミラーリング

09-トラフィックミラーリング

10-sFlow

11-Information Center

12-NetMeister

目次

このセクションのページは **10-x-x** です。

1 章 システムの保守とデバッグ 1-1
1.1 システムの保守とデバッグ設定コマンド.....1-1
1.1.1 debugging 1-1
1.1.2 display debugging.....1-2
1.1.3 ping 1-3
1.1.4 ping ipv6.....1-6
1.1.5 tracert.....1-9
1.1.6 tracert ipv6.....1-10

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。サポートされているモジュールのリストについては、**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: すべてのモジュールを指定します。

説明

debugging コマンドはモジュールのデバッグを有効にします。

undo debugging コマンドは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装置インフォメーションセンターに送信し、そこでログ出力設定に基づいてメッセージが適切な宛先に送信されます。インフォメーションセンターの詳細は、オペレーションマニュアルのセクション 10 *システム管理* 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。サポートされているモジュールのリストについては、**display 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に対して有効な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: 宛先ホスト名が **i**、**ip**、**ipv**、**ipv6**、**l**、**ls**、または **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…feff010203….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名を使用する場合、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。

フィールド	説明
--- Ping statistics for 1.1.2.2 ---	pingで送受信した統計情報です。
5 packet(s) transmitted	送信したICMPエコー要求の数です。
5 packet(s) received	受信したICMPエコー要求の数です。
0.0% packet loss	送信したパケットに対して応答がないパケットの割合です。
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	最小/平均/最大/標準の応答時間です。単位はミリ秒です。

1.1.4 ping ipv6

Syntax

ping ipv6 [**-a** *source-ipv6* | **-c** *count* | **-i** *interface-type interface-number* | **-m** *interval* | **-q** | **-s** *packet-size* | **-t** *timeout* | **-v**] * *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名を使用する場合、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* | **-t** *tos* | **-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。

-t *tos*: プローブパケットの ToS 値を指定します。設定範囲は 0～255 です。デフォルトは 0 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。

宛先アドレスがプライベートネットワーク上にある場合、中間ホップのアドレス情報は、グローバルルーティングテーブルに格納されます。

tracert コマンドの出力情報には、パケットが送信元から宛先に向かう間に通過するすべてのルートの IP アドレスが含まれます。ICMP エラーメッセージで装置が応答しない場

合、アスタリスク（*.*.*）が表示されます。（宛先が到達不能あるいは ICMP タイムアウト/宛先到達不能パケットの送信が無効であることを示します。）

tracert コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

パケットが送信元から宛先（IP アドレス 1.1.2.2）へ向かうルートを表示します。

<Switch> tracert 1.1.2.2

```
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL_C
to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) [AS 100] 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) [AS 100] 580 ms 470 ms 80 ms	TTLが2のプローブパケットの結果です。2番目のホップに関する次の情報が含まれます。 ● Hopにドメイン名が設定されていない場合は、IPアドレスが表示されます。 ● HopのIPアドレスは括弧内に表示されます。 ● Hopが属するAS番号は、指定されたルーティングテーブル内のHopに対して見つかった場合にのみ表示されます。 ● 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* | **-t** *traffic-class* | **-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。

-t *traffic-class*: IPv6 プローブパケットのトラフィッククラスを指定します。設定範囲は 0～255 です。デフォルトは 0 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。

宛先アドレスがプライベートネットワーク上にある場合、中間ホップのアドレス情報は、グローバルルーティングテーブルに格納されます。

tracert ipv6 コマンドの出力情報には、パケットが送信元から宛先に向かう間に通過するすべてのレイヤ 3 の装置の IPv6 アドレスが含まれます。ICMPv6 エラーメッセージで装置が応答しない場合、アスタリスク（*.*.*）が表示されます。（宛先が到達不能あるいは ICMPv6 タイムアウト/宛先到達不能パケットの送信が無効であることを示します。）

tracert ipv6 コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

パケットが送信元から宛先（IPv6 アドレス 2001:3::2）へ向かうルートを表示します。

<Switch> tracert ipv6 2001:3::2

```
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets, press CTRL_C
to break
 1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
 2  2001:2::2 [AS 100]  0.861 ms  0.718 ms  0.679 ms
 3  2001:3::2 [AS 200]  0.822 ms  0.731 ms  0.708 ms
```

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 [AS 100]　0.861 ms　0.718 ms　0.679 ms	Hopリミットが2のプローブパケットの結果です。2番目のHopに関する次の情報が含まれます。 ● HopのIPv6アドレスです。 ● Hopが属するASの番号です。AS番号が表示されるのは、指定されたルーティングテーブルでHopが見つかった場合のみです。 ● 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 **10-x-x** です。

2 章 NQA 2-1
2.1 NQA クライアント設定コマンド 2-1
2.1.1 advantage-factor 2-1
2.1.2 codec-type 2-2
2.1.3 data-fill 2-2
2.1.4 data-size 2-4
2.1.5 description 2-5
2.1.6 destination ip 2-6
2.1.7 destination port 2-7
2.1.8 display nqa history 2-7
2.1.9 display nqa result 2-9
2.1.10 display nqa statistics 2-15
2.1.11 filename 2-22
2.1.12 frequency 2-23
2.1.13 history-record enable 2-24
2.1.14 history-record keep-time 2-25
2.1.15 history-record number 2-26
2.1.16 next-hop ip 2-27
2.1.17 nqa 2-27
2.1.18 nqa agent enable 2-28
2.1.19 nqa schedule 2-29
2.1.20 operation (FTP operation view) 2-30
2.1.21 operation (HTTP operation view) 2-32
2.1.22 password 2-33
2.1.23 probe count 2-34
2.1.24 probe packet-interval 2-35
2.1.25 probe packet-number 2-36
2.1.26 probe packet-timeout 2-37
2.1.27 probe timeout 2-37
2.1.28 reaction checked-element probe-fail (for trap) 2-38
2.1.29 reaction checked-element probe-fail (for trigger) 2-40
2.1.30 reaction trap 2-41
2.1.31 resolve-target 2-42
2.1.32 route-option bypass-route 2-43
2.1.33 source interface (ICMP echo operation view) 2-44
2.1.34 source ip 2-45

2.1.35 source port 2-46
2.1.36 statistics hold-time 2-47
2.1.37 statistics interval 2-48
2.1.38 statistics max-group 2-49
2.1.39 tos 2-50
2.1.40 ttl 2-50
2.1.41 type 2-51
2.1.42 url 2-52
2.1.43 username 2-53
2.1.44 version 2-54
2.2 NQA サーバ設定コマンド 2-55
2.2.1 display nqa server 2-55
2.2.2 nqa server enable 2-56
2.2.3 nqa server tcp-connect 2-57
2.2.4 nqa server udp-echo 2-58

2章 NQA

2.1 NQAクライアント設定コマンド

2.1.1 advantage-factor

Syntax

advantage-factor *factor*

undo advantage-factor

デフォルト

0

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

factor: アドバンテージファクタを指定します。設定範囲は 0～20 です。

説明

advantage-factor コマンドは MOS（Mean Opinion Scores）値と ICPIF（Calculated Planning Impairment Factor）値をカウントするのに使用されるアドバンテージファクタを設定します。

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

音声品質の評価は、ユーザの音声品質の許容度に依存します。音声品質に高い許容度を持つユーザの場合、アドバンテージファクタの設定を行う **advantage-factor** コマンドを使用します。システムが ICPIF 値を計算する場合、音声品質の評価用に ICPIF と MOS の値を修正するため、アドバンテージファクタが取りはずされます。

例

音声テストのアドバンテージファクタを 10 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type voice

[Switch-nqa-admin-test-voice] advantage-factor 10

2.1.2 codec-type

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

デフォルト

G.711 A-law

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

g711a: G.711 A-law コーデックタイプを指定します。

g711u: G.711 μ-law コーデックタイプを指定します。

g729a: G.729 A-law コーデックタイプを指定します。

説明

codec-type コマンドは音声テストのコーデックタイプを設定します。

undo codec-type コマンドはデフォルトに戻します。

例

音声テストのコーデックタイプを **g729a** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type voice

[Switch-nqa-admin-test-voice] codec-type g729a

2.1.3 data-fill

Syntax

data-fill *string*

undo data-fill

デフォルト

00010203040506070809

View

ICMP/UDP echo operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

string: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

data-fill コマンドは各プローブパケットのペイロードに埋め込まれる文字列を設定します。

undo data-fill コマンドはデフォルトに戻します。

ペイロード長が埋め込みデータより小さい場合、文字列の最初の部分を使用します。たとえば、埋め込みデータが **abcd** で、テストパケットのデータサイズが 3 バイトの場合、**abc** がパケットに埋め込まれます。

ペイロード長が埋め込みデータより大きい場合、一杯になるまで文字列を繰り返し埋め込みます。たとえば、埋め込みデータが **abcd** で、テストパケットのデータサイズが 6 バイトの場合、**abcdab** がパケットに埋め込まれます。

テストタイプに依存して文字列が埋め込まれます。

- ICMP エコーテストでは、設定された文字列は ICMP エコー要求の全ペイロードに埋め込まれます。
- UDP エコーテストでは、UDP パケットのペイロードの最初の 5 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- UDP ジッタテストでは、UDP パケットのペイロードの最初の 68 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- 音声テストでは、UDP パケットのペイロードの最初の 16 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。

例

ICMP エコー要求のペイロードに埋め込まれる文字列 **abcd** を設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] data-fill abcd

2.1.4 data-size

Syntax

data-size *size*

undo data-size

デフォルト

異なるテストのプローブパケットのデフォルトのペイロードサイズを表 2-1 に示します。

表 2-1 プローブパケットのデフォルトのペイロードサイズ

テストタイプ	コーデックタイプ	デフォルトサイズ（バイト）
ICMP echo	N/A	100
UDP echo	N/A	100
UDP jitter	N/A	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

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 コマンドは各プローブパケッ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、各 ICMP エコー要求のペイロードサイズを設定します。

UDP エコー、UDP ジッタ、音声の各操作では、UDP パケットごとにペイロードサイズを設定します。

例

各 ICMP エコー要求のペイロードサイズを 80 バイトに設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] data-size 80

2.1.5 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

すべての NQA operation view

定義済みユーザロール

network-admin

パラメータ

text: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

description コマンドはテストタイプや目的などの NQA テストの説明を設定します。

undo description コマンドは説明をデフォルトに戻します。

例

NQA テストの ICMP エコーテストの説明を **icmp-probe** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] description icmp-probe

2.1.6 destination ip

Syntax

destination ip *ip-address*

undo destination ip

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: テストの宛先 IP 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 IP アドレスを設定します。

undo destination ip コマンドは宛先 IP アドレスをデフォルトに戻します。

例

ICMP エコーテストの宛先 IPv4 アドレスを 10.1.1.1 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] destination ip 10.1.1.1

2.1.7 destination port

Syntax

destination port *port-number*

undo destination port

デフォルト

他のタイプのテストでは、宛先ポート番号は設定されません。

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 コマンドはデフォルトに戻します。

例

UDP エコーテストの宛先ポート番号を 9000 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-echo

[Switch-nqa-admin-test-udp-echo] destination port 9000

2.1.8 display nqa history

Syntax

display nqa history [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* は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。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 コマンドは次のテストの結果または統計情報は表示されません。

- UDP ジッタ
- 音声

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 オペレーションの履歴記録を表示します。

<Switch> display nqa history administrator test

```
NQA entry (admin administrator, tag test) history records:
  Index      Response     Status          Time
  10         329          Succeeded       2011-04-29 20:54:26.5
  9          344          Succeeded       2011-04-29 20:54:26.2
  8          328          Succeeded       2011-04-29 20:54:25.8
  7          328          Succeeded       2011-04-29 20:54:25.5
  6          328          Succeeded       2011-04-29 20:54:25.1
  5          328          Succeeded       2011-04-29 20:54:24.8
  4          328          Succeeded       2011-04-29 20:54:24.5
  3          328          Succeeded       2011-04-29 20:54:24.1
  2          328          Succeeded       2011-04-29 20:54:23.8
  1          328          Succeeded       2011-04-29 20:54:23.4
```

表 2-2 コマンド出力

フィールド	説明
Index	履歴記録のIDです。
TTL	プローブパケットのTTL値が表示されます。

フィールド	説明
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。
Hop IP	応答パケットを送信したノードのIPアドレスです。
Status	テスト結果の状態です。 ● **Succeeded**－成功しました。 ● **Unknown error**－未知のエラーです。 ● **Internal error**－内部エラーです。 ● **Timeout**－タイムアウトしました。
Time	テストが完了したときの時間です。

2.1.9 display nqa result

Syntax

display nqa result [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* は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。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

管理者名が **admin** で、テストタグが **test** である 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
```

管理者名が **admin** で、テストタグが **test** である UDP ジッタテストの最新の結果を表示します。

<Switch> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
   Send operation times: 10          Receive response times: 10
   Min/Max/Average round trip time: 15/46/26
   Square-Sum of round trip time: 8103
   Last packet received time: 2011-05-29 10:56:38.7
  Extended results:
   Packet loss ratio: 0%
   Failures due to timeout: 0
   Failures due to internal error: 0
   Failures due to other errors: 0
   Packets out of sequence: 0
   Packets arrived late: 0
  UDP-jitter results:
   RTT number: 10
   Min positive SD: 8                Min positive DS: 8
   Max positive SD: 18               Max positive DS: 8
   Positive SD number: 5             Positive DS number: 2
   Positive SD sum: 75               Positive DS sum: 32
   Positive SD average: 15           Positive DS average: 16
   Positive SD square-sum: 1189      Positive DS square-sum: 640
   Min negative SD: 8                Min negative DS: 1
   Max negative SD: 24               Max negative DS: 30
   Negative SD number: 4             Negative DS number: 7
   Negative SD sum: 56               Negative DS sum: 99
   Negative SD average: 14           Negative DS average: 14
   Negative SD square-sum: 946       Negative DS square-sum: 1495
```

```
  One way results:
    Max SD delay: 22                    Max DS delay: 23
    Min SD delay: 7                     Min DS delay: 7
    Number of SD delay: 10               Number of DS delay: 10
    Sum of SD delay: 125                 Sum of DS delay: 132
    Square-Sum of SD delay: 1805          Square-Sum of DS delay: 1988
    SD lost packets: 0                  DS lost packets: 0
    Lost packets for unknown reason: 0
```

管理者名が **admin** で、テストタグが **test** である最新の音声テスト結果を表示します。

<Switch> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
    Send operation times: 1000          Receive response times: 0
    Min/Max/Average round trip time: 0/0/0
    Square-Sum of round trip time: 0
    Last packet received time: 0-00-00 00:00:00.0
  Extended results:
    Packet loss ratio: 100%
    Failures due to timeout: 1000
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 0
    Min positive SD: 0                  Min positive DS: 0
    Max positive SD: 0                  Max positive DS: 0
    Positive SD number: 0                Positive DS number: 0
    Positive SD sum: 0                  Positive DS sum: 0
    Positive SD average: 0               Positive DS average: 0
    Positive SD square-sum: 0             Positive DS square-sum: 0
    Min negative SD: 0                  Min negative DS: 0
    Max negative SD: 0                  Max negative DS: 0
    Negative SD number: 0                Negative DS number: 0
    Negative SD sum: 0                  Negative DS sum: 0
    Negative SD average: 0               Negative DS average: 0
    Negative SD square-sum: 0             Negative DS square-sum: 0
  One way results:
    Max SD delay: 0                     Max DS delay: 0
    Min SD delay: 0                     Min DS delay: 0
    Number of SD delay: 0                Number of DS delay: 0
    Sum of SD delay: 0                  Sum of DS delay: 0
    Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
```

```
  SD lost packets: 0                DS lost packets: 0
  Lost packets for unknown reason: 1000
Voice scores:
  MOS value: 0.99                   ICPIF value: 87
```

表 2-3 コマンド出力

フィールド	説明
Data collecting in progress	テストは進行中です。
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。
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。

フィールド	説明
Min positive SD	送信元から宛先への最小ポジティブジッタです。
Min positive DS	宛先から送信元への最小ポジティブジッタです。
Max positive SD	送信元から宛先への最大ポジティブジッタです。
Max positive DS	宛先から送信元への最大ポジティブジッタです。
Positive SD number	送信元から宛先へのポジティブジッタの数です。
Positive DS number	宛先から送信元へのポジティブジッタの数です。
Positive SD sum	送信元から宛先へのポジティブジッタの合計数です。
Positive DS sum	宛先から送信元へのポジティブジッタの合計数です。
Positive SD average	送信元から宛先への平均ポジティブジッタです。
Positive DS average	宛先から送信元への平均ポジティブジッタです。
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和です。
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和です。
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値です。
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値です。
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値です。
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値です。
Negative SD number	送信元から宛先へのネガティブジッタの数です。
Negative DS number	宛先から送信元へのネガティブジッタの数です。
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計です。
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。

フィールド	説明
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和です。
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和です。
One way results	片方向遅延です。 このフィールドはUDPジッタテスト、音声テストで有効です。
Max SD delay	送信元から宛先への最大遅延です。
Max DS delay	宛先から送信元への最大遅延です。
Min SD delay	送信元から宛先への最小遅延です。
Min DS delay	宛先から送信元への最小遅延です。
Number of SD delay	送信元から宛先への遅延の数です。
Number of DS delay	宛先から送信元への遅延の数です。
Sum of SD delay	送信元から宛先への遅延の合計です。
Sum of DS delay	宛先から送信元への遅延の合計です。
Square-Sum of SD delay	送信元から宛先への遅延の2乗和です。
Square-Sum of DS delay	宛先から送信元への遅延の2乗和です。
SD lost packets	送信元から宛先への損失したパケット数です。
DS lost packets	宛先から送信元への損失したパケット数です。
Lost packets for unknown reason	不明な理由で損失したパケット数です。
Voice scores	音声パラメータです。 このフィールドは音声テストで有効です。
MOS value	音声テストの計算されたMOS値です。
ICPIF value	音声テストの計算されたICPIF値です。
TTL	受信した応答パケットのTTL値が表示されます。
Hop IP	応答パケットを送信したノードの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刻です。

2.1.10 display nqa statistics

Syntax

display nqa statistics [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* は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。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。結果フィールドには、以下のいずれかの条件でハイフン（-）が結果として表示されます。

- しきい値タイプが平均値ある場合。
- 音声テストのモニタリングした性能の値が ICPIF あるいは MOS である場合。

例

管理者名が **admin** で、operation タグが **test** である 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
```

管理者名が **admin** で、operation タグが **test** である 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
```

管理者名が **admin** で、operation タグが **test** である音声テストの統計情報を表示します。

<Switch> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
 NO. : 1
  Start time: 2007-01-01 09:33:45.3
  Life time: 120 seconds
  Send operation times: 10            Receive response times: 10
  Min/Max/Average round trip time: 1/12/7
  Square-Sum of round trip time: 620
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
 Voice results:
  RTT number: 10
  Min positive SD: 3                  Min positive DS: 1
  Max positive SD: 10                 Max positive DS: 1
  Positive SD number: 3               Positive DS number: 2
  Positive SD sum: 18                 Positive DS sum: 2
  Positive SD average: 6              Positive DS average: 1
  Positive SD square-sum: 134         Positive DS square-sum: 2
  Min negative SD: 3                  Min negative DS: 1
  Max negative SD: 9                  Max negative DS: 1
  Negative SD number: 4               Negative DS number: 2
  Negative SD sum: 25                 Negative DS sum: 2
  Negative SD average: 6              Negative DS average: 1
  Negative SD square-sum: 187         Negative DS square-sum: 2
```

```
One way results:
  Max SD delay: 0                    Max DS delay: 0
  Min SD delay: 0                    Min DS delay: 0
  Number of SD delay: 0               Number of DS delay: 0
  Sum of SD delay: 0                 Sum of DS delay: 0
  Square-Sum of SD delay: 0           Square-Sum of DS delay: 0
  SD lost packets: 0                 DS lost packets: 0
  Lost packets for unknown reason: 0
Voice scores:
  Max MOS value: 4.40                Min MOS value: 4.40
  Max ICPIF value: 0                 Min ICPIF value: 0
Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      ICPIF            -              -            -
  2      MOS              -              -            -
```

表 2-4 コマンド出力

フィールド	説明
No.	統計情報のグループIDです。
Start time	テストが開始した時間です。
Life time	テストの所要時間です。
Send operation times	送信したプローブパケットの数です。
Receive response times	受信した応答パケットの数です。
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイムです。単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和です。
Packet loss ratio	平均パケット損失レートです。
Failures due to timeout	テストでタイムアウトが発生した回数です。
Failures due to disconnect	ピアが切断した数です。
Failures due to no connection	ピアとの接続に失敗した数です。
Failures due to internal error	内部エラーによる故障の数です。
Failures due to other errors	他のエラーによる故障の数です。
Packets out of sequence	異なる順番のパケットによる故障の数です。

フィールド	説明
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。
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。

フィールド	説明
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。
One way results	片方向遅延です。 このフィールドはUDPジッタテスト、音声テストで有効です。
Max SD delay	送信元から宛先への最大遅延です。
Max DS delay	宛先から送信元への最大遅延です。
Min SD delay	送信元から宛先への最小遅延です。
Min DS delay	宛先から送信元への最小遅延です。
Number of SD delay	送信元から宛先への遅延の数です。
Number of DS delay	宛先から送信元への遅延の数です。
Sum of SD delay	送信元から宛先への遅延の合計です。
Sum of DS delay	宛先から送信元への遅延の合計です。
Square-Sum of SD delay	送信元から宛先への遅延の2乗和です。
Square-Sum of DS delay	宛先から送信元への遅延の2乗和です。
SD lost packets	送信元から宛先への損失したパケット数です。
DS lost packets	宛先から送信元への損失したパケット数です。
Lost packets for unknown reason	不明な理由で損失したパケット数です。
Voice scores	音声パラメータです。 このフィールドは音声テストで有効です。
Max MOS value	最大MOS値です。

フィールド	説明
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 2-5 DHCP/DLSw/DNS/FTP/HTTP/ICMP エコー/SNMP/TCP/UDP エコーテストに関するモニタリングフィールドの説明

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
probe-duration	accumulate	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
	average	–	–	–
	consecutive	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
probe-fail	accumulate	カウント期間のプローブ	完了したプローブ数	プローブ失敗数
	consecutive	カウント期間のプローブ	完了したプローブ数	プローブ失敗数

表 2-6 UDP ジッタ/音声テストの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 (available only for the voice operation)	–	–	–	–

関連コマンド

statistics interval

2.1.11 filename

Syntax

filename *filename*

undo filename

デフォルト

設定なし

View

FTP operation view

定義済みユーザロール

network-admin

パラメータ

filename: FTP サーバと FTP クライアント間で転送するファイル名を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。スラッシュ（/）は含むことができません。

説明

filename コマンドは FTP サーバと FTP クライアント間で転送するファイル名を指定します。

undo filename コマンドはデフォルトに戻します。

例

FTP テストで、FTP サーバと FTP クライアント間で転送するファイル名を **config.txt** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] filename config.txt

2.1.12 frequency

Syntax

frequency *interval*

undo frequency

デフォルト

2 つの連続する音声テスト間隔は 60000 ミリ秒です。他のテストの 2 つの連続するテスト間隔は 0 ミリ秒です。

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、NQA がテストを 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、次のテストは開始されません。

例

ICMP エコーテストを 1000 ミリ秒ごとに繰り返すように設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] frequency 1000

2.1.13 history-record enable

Syntax

history-record enable

undo history-record enable

デフォルト

無効

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

説明

history-record enable コマンドは NQA テストの履歴記録を保存することを有効にします。

undo history-record enable コマンドは NQA テストの履歴記録を保存することを無効にします。

NQA テストの履歴記録を表示する場合、**display nqa history** コマンドを使用します。

undo history-record enable コマンドは NQA テストの既存の履歴記録も削除します。

例

NQA テストの履歴記録を保存することを有効にします。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] history-record enable

関連コマンド

display nqa history

2.1.14 history-record keep-time

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

デフォルト

120 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

keep-time: 履歴記録を保存する期間を指定します。設定範囲は 1～1440 分です。

説明

history-record keep-time コマンドは NQA テストの履歴記録の有効期限を指定します。

undo history-record keep-time コマンドはデフォルトに戻します。

NQA テストが完了したとき、タイマが開始します。すべての記録は有効期限になったとき、削除されます。

例

ICMP エコーテストの履歴記録の有効期限を 100 分に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] history-record keep-time 100

2.1.15 history-record number

Syntax

history-record number *number*

undo history-record number

デフォルト

50

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

number: NQA テストで履歴記録を保存できる最大数を指定します。設定範囲は 0～50 です。

説明

history-record number コマンドは NQA テストで履歴記録を保存できる最大数を設定します。

undo history-record number コマンドはデフォルトに戻します。

NQA テストの履歴記録の数が最大数を超過した場合、もっとも古い履歴記録が削除されます。

例

ICMP エコーテストで履歴記録を保存できる最大数を 10 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] history-record number 10

2.1.16 next-hop ip

Syntax

next-hop ip *ip-address*

undo next-hop ip

デフォルト

設定なし

View

ICMP echo operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: ネクストホップ IPv4 アドレスを指定します。

説明

next-hop ip コマンドはプローブパケットのネクストホップ IPv4 アドレスを指定します。

undo next-hop ip コマンドは設定をデフォルトに戻します。

ネクストホップ IPv4 アドレスが設定されていない場合、装置はルーティングテーブルを検索し、プローブパケットのネクストホップ IPv4 アドレスを決定します。

例

ICMP エコーテストのネクストホップ IPv4 アドレスとして 10.1.1.1 を指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.1

2.1.17 nqa

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

all: すべての NQA テストを削除します。

説明

nqa コマンドは NQA テストを作成し、その view に移行します。

undo nqa コマンドはテストを削除します。

例

管理者 **admin** とテストタグ **test** の NQA テストを作成し、NQA operation view に移行します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test]

2.1.18 nqa agent enable

Syntax

nqa agent enable

undo nqa agent enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

nqa agent enable コマンドは NQA クライアントを有効にします。

undo nqa agent enable コマンドは NQA クライアントを無効にし、すべてのテストを停止します。

例

NQA クライアントを有効にします。

<Switch> system-view

[Switch] nqa agent enable

関連コマンド

nqa server enable

2.1.19 nqa schedule

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

undo nqa schedule *admin-name operation-tag*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

start-time: NQA テストの開始日時を指定します。

hh:mm:ss: NQA テストの開始時間を指定します。

yyyy/mm/dd: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

mm/dd/yyyy: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

now: すぐにテストを開始します。

lifetime: テストの有効期限を指定します。

lifetime: テスト期間を指定します。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。このキーワードを指定しない場合、NQA テストは指定した日時に 1 回だけ実行されます。

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 工程は、指定した開始時間と終了時間(開始時間+テスト時間)の間に実行されます。指定した開始時刻がシステム時刻より前の場合、テストはただちに開始されます。指定した開始時刻と終了時刻の両方がシステム時刻より前の場合、テストは開始されません。現在のシステム時刻を表示するには、**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。移行する場合は、**undo nqa schedule** コマンドを使用して、最初に NQA テストを停止します。

テストを完了させるため、十分長い有効期限を指定してください。

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、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** (コマンドマニュアルのセクション 1 *はじめに*)
- **nqa**
- **type**

2.1.20 operation (FTP operation view)

Syntax

operation { **get** | **put** }

undo operation

デフォルト

get

View

FTP operation view

定義済みユーザロール

network-admin

パラメータ

get: FTP サーバからファイルを取得します。

put: FTP サーバにファイルを転送します。

説明

operation コマンドは FTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

filename コマンドで **put** オペレーションを実行するとき、NQA クライアント上にファイルが存在していることを確認してください。

FTP サーバからファイルを取得する場合、FTP サーバの URL に指定されたファイルが存在していることを確認してください。NQA クライアントは FTP サーバから取得したファイルを保存しません。

FTP テストではファイルサイズが小さいファイルを使用してください。大きいサイズのファイルは、タイムアウトでテストが失敗したり、ネットワークの帯域幅以上を独占して他のサービスに影響を与えたりする可能性があります。

例

FTP テストのオペレーションタイプを **put** に指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] operation put

関連コマンド

- **password**
- **username**

2.1.21 operation (HTTP 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 テストでは、HTTP 要求をプローブパケットとして使用します。

HTTP の **get** あるいは **post** オペレーションの HTTP 要求の内容は **url** コマンドによって指定された URL から取得されます。

例

HTTP テストのオペレーションのタイプを **get** 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 get

関連コマンド

- **password**
- **username**

2.1.22 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。FTP、HTTP テストの場合、プレーンテキストのパスワードは、大文字、小文字を区別します。設定範囲は 1～32 文字です。パスワードの暗号化形式は、大文字、小文字を区別します。設定範囲は、1～73 文字です。

説明

password コマンドはパスワードを設定します。

undo password コマンドは設定をデフォルトに戻します。

例

FTP ログインパスワードを **ftpuser** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] password simple ftpuser

関連コマンド

- **operation**
- **username**

2.1.23 probe count

Syntax

probe count *times*

undo probe count

デフォルト

NQA クライアントはテストごとに 1 つのプローブを宛先に対して実行します。

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: プローブの時間を指定します。テストごとのターゲットに対するプローブの回数を指定します。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、またはスループットテストは、プローブフレームを宛先装置に送信して、ネットワークのフレーム損失率、遅延、またはスループットをテストします。

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テストでは無効です。これらのテストは 1 つのプローブのみ実行します。

例

ICMP エコーテストを実行する検査回数を 10 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] probe count 10

2.1.24 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 100 ミリ秒ごとに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-interval 100

2.1.25 probe packet-number

Syntax

probe packet-number *packet-number*

undo probe packet-number

デフォルト

UDP ジッタのプローブは 10 パケットを送信し、音声プローブは 1000 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。使用可能な値の範囲は以下のとおりです。

- UDP ジッタテストの設定範囲は 10～1000 です。
- 音声テストの設定範囲は 10～60000 です。

説明

probe packet-number コマンドは UDP ジッタテスト、音声テストで送信するパケットの数を設定します。

undo probe packet-number コマンドはデフォルトに戻します。

例

UDP ジッタテストで 100 パケットを送信するように設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-jitter

[Switch-nqa-admin-test-udp-jitter] probe packet-number 100

2.1.26 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: タイムアウト時間を指定します。単位はミリ秒です。設定範囲は 10～3600000 ミリ秒です。

説明

probe packet-timeout コマンドは UDP ジッタテスト、音声テストの応答を待つタイムアウト時間を設定します。

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

例

UDP ジッタテストの応答を待つタイムアウト時間を 100 ミリ秒に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-jitter

[Switch-nqa-admin-test-udp-jitter] probe packet-timeout 100

2.1.27 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。単位はミリ秒です。

- FTP テスト、HTTP テストの設定範囲は 10～86400000 ミリ秒です。
- DHCP テスト、DNS テスト、DLSw テスト、ICMP エコーテスト、SNMP テスト、TCP テスト、UDP エコーテストの設定範囲は 10～3600000 ミリ秒です。

説明

probe timeout コマンドはプローブのタイムアウト時間を設定します。

undo probe timeout コマンドはデフォルトに戻します。

プローブの時間以内にテストが完了しない場合、プローブがタイムアウトします。

例

DHCP テストのプローブタイムアウト時間を 10000 ミリ秒に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type dhcp

[Switch-nqa-admin-test-dhcp] probe timeout 10000

2.1.28 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

2.1.29 reaction checked-element probe-fail (for trigger)

Syntax

reaction *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**

undo reaction *item-number*

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

item-number: リアクションエントリに ID を割り当てます。設定範囲は 1～10 です。

threshold-type: しきい値タイプを指定します。

consecutive *consecutive-occurrences*: 連続してテストに失敗する最大数を指定します。設定範囲は 1～16 です。

action-type: トリガとなるアクションを指定します。

trigger-only: 一定の条件に対応するために他のモジュールを起動します。

説明

reaction checked-element probe-fail コマンドはプローブの失敗をモニタするためのリアクションエントリを設定します。

undo reaction コマンドは指定したリアクションエントリを削除します。

リアクションを作成した後、修正することはできません。リアクションエントリの属性を変更する場合、**undo reaction** コマンドを使用して最初にエントリを削除し、新しいリアクションエントリを再度設定してください。

例

リアクションエントリ 1 を作成します。連続してプローブが 3 回失敗した場合、コラボレーションを起動します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type tcp

[Switch-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only

関連コマンド

track (コマンドマニュアルのセクション 9 *高可用性* “*Track*”)

2.1.30 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

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP echo/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

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: プローブの失敗回数の総数が ac*cumulate-probe-failures* 以上になった場合、トラップを送信します。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。

accumulate-probe-failures: テストで失敗したプローブの総数を指定します。設定範囲は 1～15 です。

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。

reaction trap test-complete コマンドは UDP ジッタテスト、音声テストでのみ有効です。

例

ICMP エコーテストで連続して 5 回以上失敗した場合、トラップを送信するように設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] reaction trap probe-failure 5

2.1.31 resolve-target

Syntax

resolve-target *domain-name*

undo resolve-target

デフォルト

設定なし

View

DNS operation view

定義済みユーザロール

network-admin

パラメータ

domain-name: 解決されるドメイン名を指定します。設定範囲は 1～255 文字です。ドットで区切り、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます（たとえば、aabbcc.com です）。各部分の設定範囲は 1～63 文字です。連続したドット（.）は使用できません。

説明

resolve-target コマンドは DNS テストのドメイン名を設定します。

undo resolve-target コマンドはデフォルトに戻します。

例

解決されるドメイン名 **domain1** を設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type dns

[Switch-nqa-admin-test-dns] resolve-target domain1

2.1.32 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、直接接続されたネットワーク上の宛先に送信されます。
- プローブパケットの TTL 値は 1 に設定されます。**ttl** コマンドで設定された TTL は有効になりません。

例

ルーティングテーブルバイパス機能を有効にします。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] route-option bypass-route

2.1.33 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。

指定されたインタフェースは起動している必要があります。インタフェースがダウンしていると、プローブ要求を送信できません。

source interface コマンドと ICMP エコーテストの **source ip** コマンドを複数回実行すると、最後に行った設定が適用されます。

例

ICMP エコー要求パケットの送信元 IP アドレスとして VLAN インタフェース 1 の IP アドレスを設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] source interface vlan-interface 1

関連コマンド

source ip

2.1.34 source ip

Syntax

source ip *ip-address*

undo source ip

デフォルト

プローブパケットは、出力インタフェースのプライマリ IP アドレスを送信元 IP アドレスとして使用します。

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 IPv4 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 IPv4 アドレスを設定します。

undo source ip コマンドは設定をデフォルトに戻します。

指定する送信元 IPv4 アドレスは、ローカルインタフェースの IPv4 アドレスである必要があり、ローカルインタフェースは稼働している必要があります。そうしないと、プローブパケットを送信できません。

ICMP エコーテストのために **source interface** コマンドと **source ip** 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

ICMP エコー要求の送信元 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] source ip 10.1.1.1

関連コマンド

source interface

2.1.35 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 コマンドはデフォルトに戻します。

例

UDP エコーテストのプローブパケットで送信元ポートを 8000 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-echo

[Switch-nqa-admin-test-udp-echo] source port 8000

2.1.36 statistics hold-time

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

デフォルト

120 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

hold-time: 保持時間を指定します。設定範囲は 1～1440 分です。

説明

statistics hold-time コマンドは NQA テストの統計情報グループの保持時間を設定します。

undo statistics hold-time コマンドはデフォルトに戻します。

保持時間が終了したとき、統計情報グループは削除されます。

例

ICMP エコーテストの統計情報グループの保持時間を 3 分に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] statistics hold-time 3

2.1.37 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。これらの統計は統計グループを作ります。統計情報グループの情報を表示する場合、**display nqa statistics** コマンドを使用します。

例

ICMP エコーテストで統計情報を収集する間隔を 2 分に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] statistics interval 2

2.1.38 statistics max-group

Syntax

statistics max-group *number*

undo statistics max-group

デフォルト

最大で 2 つの統計情報グループを登録できます。

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

number: 統計情報グループの最大数を指定します。設定範囲は 0～100 です。統計情報の収集を無効にする場合、0 に設定します。

説明

statistics max-group コマンドは保存できる統計情報グループの最大数を設定します。

undo statistics max-group コマンドはデフォルトに戻します。

統計情報グループの数が最大数に到達し、新しいグループが保存されたとき、もっとも古い統計情報が削除されます。

例

ICMP エコーテストで保存できる統計情報グループの最大数を 5 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] statistics max-group 5

2.1.39 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 view で、プローブパケットの IP ヘッダの ToS を 1 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] tos 1

2.1.40 ttl

Syntax

ttl *value*

undo ttl

デフォルト

ホップの最大数のプローブパケットは 20 です。

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が通過できるホップの最大数を設定します。

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。あるテストに対して **route-option bypass-route** コマンドと ttl コマンドの両方を設定した場合、ttl コマンドは有効になりません。

例

ICMP エコーテストで、プローブパケットの最大ホップ数を 16 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] ttl 16

2.1.41 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

NQA テストタイプとして FTP を選択し、FTP operation view に移行します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp]

2.1.42 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。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パラメータは、宛先サーバのホスト名を表します。ホスト名は、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（.）疑問符は設定することができません。filenameパラメータの詳細は、オペレーションマニュアルのセクション1 *はじめに “ファイルシステム管理”* を参照してください。
FTPテスト	*ftp://host/filename* *ftp://host:port/filename*	

説明

url コマンドは宛先 URL を指定します。

undo url コマンドは URL を削除します。

例

HTTP テストの URL を **http://www.company.com/index.htm** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type http

[Switch-nqa-admin-test-http] url http://www.company.com/index.html

2.1.43 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。大文字、小文字を区別します。FTP、HTTP ユーザ名の設定範囲は 1～32 文字です。RADIUS 認証ユーザ名の設定範囲は 1～253 文字の文字列です。

説明

username コマンドはユーザ名を指定します。

undo username コマンドはデフォルトに戻します。

例

FTP ログインのユーザ名を **administrator** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] username administrator

関連コマンド

- **operation**
- **password**

2.1.44 version

Syntax

version { **v1.0** | **v1.1** }

undo version

デフォルト

1.0

View

HTTP operation view

定義済みユーザロール

network-admin

パラメータ

v1.0: HTTP バージョン 1.0 を使用します。

v1.1: HTTP バージョン 1.1 を使用します。

説明

version コマンドは HTTP テストで使用する HTTP バージョンを指定します。

undo version コマンドはデフォルトに戻します。

例

HTTP テストで使用する HTTP バージョンを 1.1 に指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type http

[Switch-nqa-admin-test-http] version v1.1

2.2 NQAサーバ設定コマンド

注意:

UDP ジッタテスト、TCP テスト、UDP エコーテスト、音声テストを行うため、NQA サーバを設定します。

2.2.1 display nqa server

Syntax

display nqa server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nqa server コマンドは NQA サーバの状態を表示します。

例

NQA サーバの状態を表示します。

<Switch> display nqa server

```
NQA server status: Enabled
TCP connect:
  IP address         Port     Tos    VPN instance
  2.2.2.2           2000     200    -
UDP echo:
  IP address         Port     Tos    VPN instance
  3.3.3.3           3000     255    -
```

表 2-7 コマンド出力

フィールド	説明
NQA server status	NQAサーバが有効かどうかです。
TCP connect	NQAサーバのTCPリスニングサービスの情報です。
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サーバによって送信された応答パケットのToSの値です。
VPN instance	NQAサーバが受信するIPアドレスが属するVPNインスタンスの名前です。NQAサーバがパブリックIPアドレスを受信する場合、このフィールドにはハイフン(-)が表示されます。VPNインスタンスはQX-S5300Gシリーズではサポートしていません。

関連コマンド

- **nqa server enable**
- **nqa server tcp-connect**
- **nqa server udp-echo**

2.2.2 nqa server enable

Syntax

nqa server enable

undo nqa server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

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

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

例

NQA サーバを有効にします。

<Switch> system-view

[Switch] nqa server enable

関連コマンド

- **display nqa server**
- **nqa server tcp-connect**
- **nqa server udp-echo**

2.2.3 nqa server tcp-connect

Syntax

nqa server tcp-connect *ip-address port-number* [**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。

TCP テストだけのために NQA サーバでコマンドを設定する必要があります。

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 サーバで一意に設定し、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。
- 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、IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし、応答するように設定します。

<Switch> system-view

[Switch] nqa server tcp-connect 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

2.2.4 nqa server udp-echo

Syntax

nqa server udp-echo *ip-address port-number* [**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。

UDP ジッタテスト、UDP エコーテスト、音声テストだけのために NQA サーバでコマンドを設定する必要があります。

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 サーバで一意に設定し、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。
- 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、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 **10-x-x** です。

3 章 NTP 3-1
3.1 NTP 設定コマンド 3-1
3.1.1 display ntp-service sessions 3-1
3.1.2 display ntp-service status 3-7
3.1.3 display ntp-service trace 3-11
3.1.4 ntp-service acl 3-12
3.1.5 ntp-service authentication enable 3-14
3.1.6 ntp-service authentication-keyid 3-14
3.1.7 ntp-service broadcast-client 3-16
3.1.8 ntp-service broadcast-server 3-17
3.1.9 ntp-service dscp 3-18
3.1.10 ntp-service enable 3-19
3.1.11 ntp-service inbound enable 3-19
3.1.12 ntp-service max-dynamic-sessions 3-20
3.1.13 ntp-service multicast-client 3-21
3.1.14 ntp-service multicast-server 3-22
3.1.15 ntp-service refclock-master 3-24
3.1.16 ntp-service reliable authentication-keyid 3-25
3.1.17 ntp-service source 3-26
3.1.18 ntp-service unicast-peer 3-27
3.1.19 ntp-service unicast-server 3-29

3章 NTP

NTP は VLAN インタフェースでサポートされています。

3.1 NTP設定コマンド

3.1.1 display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: すべての IPv4 NTP アソシエーションの詳細情報を表示します。指定しない場合、NTP アソシエーションの概要情報のみを表示します。

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 ブロードキャストサーバモードあるいはマルチキャストサーバモードで動作しているとき、**display ntp-service sessions** コマンドはブロードキャストサーバあるいはマルチキャストサーバに対応する IPv4 NTP アソシエーションの情報を表示しませんが、アソシエーションの総数がカウントされます。

例

すべての NTP アソシエーションの概要情報を表示します。

<Switch> display ntp-service sessions

```
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]LOCAL(0)       LOCL             0    1   64    - 0.0000 0.0000 7937.9
   [5]0.0.0.0         INIT            16    0   64    - 0.0000 0.0000 0.0000
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

表 3-1 コマンド出力

フィールド	説明
source	• 参照クロックがローカルクロックであるとき、**LOCAL**(*number*)と表示されます。ローカルクロックのIPアドレスは127.127.1.*number*です。*number*はNTPプロセス番号です。値の範囲は0～3です。 • 参照クロックが別の装置であるとき、NTPサーバのIPアドレスが表示されます。このフィールドが**0.0.0.0**である場合、NTPサーバのIPアドレスは正常に解決されていません。
reference	NTPサーバの参照クロックIDです。 • 参照クロックがローカルクロックであるとき、straフィールドに関連した値が表示されます。 ■ **stra**フィールドの値が0あるいは1である場合、**LOCL**と表示されます。 ■ **stra**フィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。 • 参照クロックがネットワーク上の他の装置のクロックである場合、このフィールドは装置のIPアドレスになります。装置がIPv6をサポートしている場合、装置のIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。**INIT**と表示される場合、ローカル装置はNTPサーバと接続を確立していません。
stra	クロックソースのstratumレベルです。stratumレベルはクロックの正確さを示します。値の範囲は1～16です。値が大きくなると精度が減少します。クロックの精度は1がもっとも高く、stratumが16は同期化されておらず、参照クロックを使用することができません。
reach	クロックソースの到達可能回数です。0はクロックソースが到達不能であることを示します。
poll	ポーリング間隔です。連続する2つのNTPメッセージ間の最大間隔です。

フィールド	説明
now	最後のNTPメッセージを受信、あるいはローカルクロックが最後に更新されてから現在までの時間です。 デフォルトの時間の単位は秒です。 • 時間の長さが2048秒を超えると、分で表示されます。 • 時間の長さが300分を超えると時間で表示されます。 • 時間の長さが96時間を越えると日の単位で表示されます。 • 時間の長さが999日を越えると年の単位で表示されます。 最後のNTPメッセージを受信した時間あるいはローカルクロックが最後に更新された時間が、現在時間より遅れている場合、ハイフン（-）が表示されます。
offset	リファレンスクロックに対するシステムクロックのオフセットです。単位はミリ秒です。
delay	ローカル装置からクロックソースまでのラウンドトリップ遅延です。単位はミリ秒です。
disper	リファレンスソースに対するローカルクロックの最大誤差です。単位はミリ秒です。
[12345]	• 1—システムが選択したクロックソースです（現在のリファレンスソースです）。 • 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
VPN instance: Not specified
Local mode: client, local poll interval: 6
Peer mode: server, peer poll interval: 6
Offset: 0.2862ms, roundtrip delay: 3.2653ms, dispersion: 4.5166ms
```

```
Root roundtrip delay: 0.0000ms, root dispersion: 10.910ms
Reachabilities:31, sync distance: 0.0194
Precision: 2^18, version: 3, source interface: Not specified
Reftime: d17cbba5.1473de1e  Tue, May 17 2011  9:17:25.079
Orgtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Rcvtime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Xmttime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Roundtrip delay samples: 0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
Offset samples: 5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
Filter order: 7    5    2    6    0    4    1    3

Total sessions: 1
```

表 3-2 コマンド出力

フィールド	説明
Clock source	NTPサーバのIPアドレスです。**0.0.0.0**が表示される場合、NTPサーバのIPアドレスは正常に解決されていません。
Clock stratum	NTPサーバのstratumレベルです。stratumレベルはクロックの正確さを示します。値の範囲は1～16です。値が大きくなると精度が減少します。クロックの精度は1がもっとも高く、stratumが16は同期化されておらず、参照クロックを使用することができません。

フィールド	説明
Clock status	アソシエーションに対応するクロックソースの状態です。 ● **configured**—アソシエーションが設定コマンドで作成されました。 ● **dynamic**—ダイナミックにアソシエーションが確立されました。 ● **master**—クロックソースは現在のシステムのプライマリ参照ソースです。 ● **selected**—クロックソースはクロック選定アルゴリズムに残りました。 ● **candidate**—クロックソースはクロックソースの候補です。 ● **sane**—クロックソースはsane認証にパスしました。 ● **insane**—クロックソースはsane認証に失敗しました。もしくは、sane認証にパスしたが、参照クロックとしては使用されません。 ● **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
VPN instance	NTPサーバが属するVPNインスタンスです。NTPサーバがパブリックネットワークにある場合、**Not specified**と表示されます。VPNインスタンスはQX-S5300Gシリーズではサポートしていません。
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2^6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2^6あるいは64秒です。
Offset	参照クロックに対するシステムクロックのオフセットです。単位はミリ秒です。
roundtrip delay	ローカル装置からクロックソースまでのラウンドトリップ遅延です。単位はミリ秒です。
dispersion	参照ソースに対するシステムクロックの最大誤差です。
Root roundtrip delay	ローカル装置からプライマリ参照ソースまでのラウンドトリップ遅延です。単位はミリ秒です。

フィールド	説明
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。
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。
Total sessions	アソシエーションの総数です。

3.1.2 display ntp-service status

Syntax

display ntp-service status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ntp-service status コマンドは NTP サービスの状態を表示します。

例

クロックの同期後の NTP サービスの状態を表示します。

<Switch> display ntp-service status

```
Clock status: synchronized
Clock stratum: 2
System peer: LOCAL(0)
Local mode: client
Reference clock ID: 127.127.1.0
Leap indicator: 00
Clock jitter: 0.000977 s
Stability: 0.000 pps
Clock precision: 2^-19
Root delay: 0.00000 ms
Root dispersion: 3.96367 ms
Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
System poll interval: 256 s
```

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^-19
Clock precision:
Root delay: 0.00000 ms
Root dispersion: 0.00002 ms
Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
System poll interval: 8 s
```

表 3-3 コマンド出力

フィールド	説明
Clock status	システムクロックの状態です。 ● **synchronized**—システムクロックが同期されています。 ● **unsynchronized**—システムクロックが同期されていません。
Clock stratum	システムクロックのstratumレベルです。
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。

フィールド	説明
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、**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。 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、**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。
Leap indicator	アラーム状態です。 ● **00**—正常です。 ● **01**—leap秒です。一日の最後の分が61秒であることを示します。 ● **10**—leap秒です。一日の最後の分が59秒であることを示します。 ● **11**—クロックが同期されていません。
Clock jitter	システムクロックと参照クロック間の相違です。単位は秒です。
Stability	クロック周波数の安定性です。値が低い場合、安定性が高いことを示します。
Clock precision	システムクロックの精度です。
Root delay	ローカル装置からプライマリ参照ソースまでのラウンドトリップ遅延です。単位はミリ秒です。
Root dispersion	プライマリ参照クロックに対するシステムクロックの最大誤差です。単位はミリ秒です。

フィールド	説明
Reference time	参照タイムスタンプです。
System poll interval	システムのポーリング間隔です。単位は秒です。

3.1.3 display ntp-service trace

Syntax

display ntp-service trace

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ntp-service trace コマンドはローカル装置からプライマリ参照ソース間の NTP サーバの概要情報を表示します。

送信元インタフェースからプライマリ参照ソースにトレースバックするには、送信元インタフェースと、ローカル装置からプライマリ参照ソースへの NTP サーバが互いに到達可能であることを確認します。

例

ローカル装置からプライマリ参照ソース間の NTP サーバの概要情報を表示します。

<Switch> display ntp-service trace

```
Server    127.0.0.1
Stratum   3, jitter  0.000, synch distance 0.0000.
Server    3000::32
Stratum   2 , jitter 790.00, synch distance 0.0000.
RefID     127.127.1.0
```

出力は、サーバ 127.0.0.1 がサーバ 3000::32 に同期しており、サーバ 3000::32 がローカルクロックに同期していることを示します。

表 3-4 コマンド出力

フィールド	説明
Server	NTPサーバのIPアドレスです。

フィールド	説明
Stratum	NTPサーバのstratumレベルです。
jitter	上位レベルクロックに対するクロックオフセットのRMS（Root mean square）です。単位は秒です。
synch distance	上位レベルのNTPサーバに対する同期間隔です。単位は秒です。ばらつきとラウンドトリップ遅延の値から計算されます。
RefID	プライマリ参照ソースの識別子です。プライマリ参照クロックのstratumレベルが0であるとき、**LOCL**と表示されます。そうでなければプライマリ参照クロックのIPアドレスが表示されます。

関連コマンド

- **ntp-service source**
- **ntp-service unicast-server**
- **ntp-service unicast-peer**

3.1.4 ntp-service acl

Syntax

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

デフォルト

peer

View

System view

定義済みユーザロール

network-admin

パラメータ

peer: タイム要求とピア装置からの NTP 制御クエリ（アラーム、認証状態、タイムサーバ情報など）を許可します。ローカル装置がピアの装置と同期することを許可します。

query: ピア装置からローカル装置の NTP 制御クエリのみ許可します。

server: タイム要求とピア装置からの NTP 制御クエリを許可します。ローカル装置がピアの装置と同期することを許可しません。

synchronization: ACL にパスするアドレスのシステムからのタイム要求のみ許可します。

acl *ipv4-acl-number*: IPv4 ACL を番号で指定します。IPv4 ACL に一致するピア装置には、コマンドで指定されたアクセス権があります。*ipv4-acl-number* の設定範囲は、2000～2999 です。IPv4 標準 ACL 番号、または IPv4 拡張 ACL 番号を表します。IPv4 拡張 ACL 番号の設定範囲は 3000～3999 です。

説明

ntp-service acl コマンドはローカル装置の 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 NTP サービスの NTP サービスアクセス制御権を削除します。

装置は IPv4 NTP 要求を受信すると、最も制限の厳しいものから順に **peer**、**server**、**synchronization**、および **query** の順にアクセス権と照合します。

- IPv4 NTP アクセス制御が設定されていない場合は、peer アクセス権が適用されます。
- ピア装置の IP アドレスが IPv4 ACL の **permit** ステートメントと一致すると、アクセス権がピア装置に付与されます。deny ステートメントまたは IPv4 ACL が一致しない場合、アクセス権は付与されません。
- アクセス権に IPv4 ACL が指定されていない場合、またはアクセス権に指定された IPv4 ACL が作成されていない場合、アクセス権は付与されません。
- アクセス権に指定された IPv4 ACL がどれも作成されていない場合は、peer アクセス権が適用されます。
- アクセス権に指定されている IPv4 ACL にルールが含まれていない場合、アクセス権は付与されません。

ntp-service acl コマンドは NTP が動作するシステムで最低限のセキュリティを提供します。より安全な方法は NTP 認証です。

例

サブネット 10.10.0.0/16 のピアの装置がローカル装置にフルアクセスできるように設定します。

<Switch> system-view

[Switch] acl basic 2001

[Switch-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[Switch-acl-ipv4-basic-2001] quit

[Switch] ntp-service peer acl 2001

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

3.1.5 ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ntp-service authentication enable コマンドは NTP 認証を有効にします。

undo ntp-service authentication enable コマンドは NTP 認証を無効にします。

認証された NTP サーバに NTP クライアントが同期できるように、クロック同期のセキュリティが必要なネットワークで NTP 認証を有効にしてください。

NTP サーバを認証するため、認証キーを設定し、トラステッドキーとして指定します。

例

NTP 認証を有効にします。

<Switch> system-view

[Switch] ntp-service authentication enable

関連コマンド

- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

3.1.6 ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string*

undo ntp-service authentication-keyid *keyid*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid: 認証キーを識別するため、キーID を指定します。設定範囲は 1～4294967295 です。

authentication-mode: 認証アルゴリズムを指定します。

- **md5**: MD5 アルゴリズムを指定します。

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。セキュリティの目的で、プレーンテキスト形式で指定された認証鍵は、暗号化された形式で保存されます。

string: 認証キーを指定します。大文字、小文字を区別します。プレーンテキスト形式の設定範囲は、1 文字～32 文字です。暗号化された形式の設定範囲は、1～73 文字です。

説明

ntp-service authentication-keyid コマンドは認証キーを設定します。

undo ntp-service authentication-keyid コマンドは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。

NTP 認証を成功させるには、タイムサーバとクライアントで同じ鍵 ID、認証アルゴリズム、および鍵を設定します。

NTP 認証鍵を指定したら、**ntp-service reliable authentication-keyid** コマンドは鍵を信頼される鍵として設定します。鍵を削除すると、鍵は自動的に信頼できない状態に変わります。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。

このコマンドを実行すると、最大 128 の認証キーを設定できます。

例

キーの ID が **10**、キーの値が **BetterKey** のプレーンテキスト MD5 認証キーを設定します。

<Switch> system-view

[Switch] ntp-service authentication enable

[Switch] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey

関連コマンド

- **ntp-service authentication enable**
- **ntp-service reliable authentication-keyid**

3.1.7 ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service broadcast-client コマンドは NTP ブロードキャストクライアントモードで動作するように設定し、現在のインタフェースで NTP ブロードキャストパケットを受信します。

undo ntp-service broadcast-client コマンドは設定を削除します。

コマンドを設定した後、装置は NTP ブロードキャストが送信した NTP メッセージを受信し、受信した NTP メッセージをもとに同期します。

このコマンドによって、装置のインタフェースがブロードキャストクライアントモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP ブロードキャストクライアントモードで動作するように設定し、VLAN インタフェース 1 で NTP ブロードキャストパケットを受信します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ntp-service broadcast-client

関連コマンド

ntp-service broadcast-server

3.1.8 ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

authentication-keyid *keyid*: ブロードキャストメッセージをクライアントに送信するために使用するキーID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置は NTP 認証が有効のブロードキャストクライアントを同期できません。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service broadcast-server コマンドは NTP ブロードキャストサーバモードで動作するように設定し、現在のインタフェースで NTP ブロードキャストパケットを送信します。

undo ntp-service broadcast-server コマンドは設定を削除します。

コマンドを設定した後、装置は定期的に NTP メッセージをブロードキャストアドレス 255.255.255.255 に送信します。

このコマンドによって、装置のインタフェースがブロードキャストサーバモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP ブロードキャストサーバモードで動作するように設定し、VLAN インタフェース 1 で暗号キーID が 4、NTP のバージョンが 4 の NTP ブロードキャストメッセージを送信します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 4

関連コマンド

ntp-service broadcast-client

3.1.9 ntp-service dscp

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: IPv4 NTP パケットの DSCP を設定します。設定範囲は 0～63 です。

説明

ntp-server dscp コマンドは IPv4 NTP パケットの DSCP を設定します。

undo ntp-server dscp コマンドはデフォルトに戻します。

パケットの優先度を識別するため、DSCP は IPv4 パケットの ToS フィールドに含まれます。

例

IPv4 NTP パケットの DSCP を **30** に設定します。

<Switch> system-view

[Switch] ntp-service dscp 30

3.1.10 ntp-service enable

Syntax

ntp-service enable

undo ntp-service enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ntp-service enable コマンドは NTP サービスを有効にします。

undo ntp-service enable コマンドは NTP サービスを無効にします。

例

NTP サービスを有効にします。

<Switch> system-view

[Switch] ntp-service enable

3.1.11 ntp-service inbound enable

Syntax

ntp-service inbound enable

undo ntp-service inbound enable

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service inbound enable コマンドはインタフェースで NTP メッセージの処理を有効にします。

undo ntp-service inbound enable コマンドは NTP メッセージの処理を無効にします。

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、ピアの装置を同期しないようにします。
- 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ないようにします。

例

VLAN インタフェース 1 で NTP メッセージの処理を無効にします。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] undo ntp-service inbound enable

3.1.12 ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

number: 確立できるダイナミック 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 コマンドは確立できるダイナミック 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。

単一の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。

このコマンドは、ダイナミック NTP アソシエーションの数を制限し、ダイナミック NTP アソシエーションが過剰なシステムリソースを占有しないようにします。

例

ダイナミック NTP アソシエーションの最大数を 50 に設定します。

<Switch> system-view

[Switch] ntp-service max-dynamic-sessions 50

関連コマンド

display ntp-service sessions

3.1.13 ntp-service multicast-client

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチキャスト IP アドレスを指定します。デフォルトは 224.0.1.1 です。マルチキャストサーバとクライアントは同一マルチキャスト IP アドレスで設定する必要があります。

説明

ntp-service multicast-client コマンドは NTP マルチキャストクライアントモードで動作するように設定し、現在のインタフェースで NTP マルチキャストパケットを受信します。

undo ntp-service multicast-client コマンドは設定を削除します。

コマンドを設定した後、装置は宛先アドレスとして指定したマルチキャストアドレスを使用し NTP メッセージを受信します。

このコマンドによって、装置のインタフェースがマルチキャストクライアントモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

IRF スタックユニットのマスタ装置の VLAN インタフェースの *ip-address* の範囲は 224.0.1.1～224.0.1.255 です。

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、VLAN インタフェース 1 で NTP マルチキャストパケットを受信し、マルチキャストアドレスを 224.0.1.1 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ntp-service multicast-client 224.0.1.1

関連コマンド

ntp-service multicast-server

3.1.14 ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチキャスト IP アドレスを指定します。デフォルトは 224.0.1.1 です。マルチキャストサーバとクライアントは同一マルチキャスト IP アドレスで設定する必要があります。

authentication-keyid *keyid*: マルチキャストメッセージをクライアントに送信するために使用するキーID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置は NTP 認証が有効のマルチキャストクライアントを同期できません。

ttl *ttl-number*: NTP マルチキャストメッセージの TTL を指定します。設定範囲は 1～255 です。デフォルトは 16 です。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service multicast-server コマンドは NTP マルチキャストサーバモードで動作するように設定し、現在のインタフェースで NTP マルチキャストパケットを送信します。

undo ntp-service multicast-server コマンドは設定を削除します。

コマンドを設定した後、装置は定期的に NTP メッセージをマルチキャストアドレスに送信します。

このコマンドによって、装置のインタフェースがマルチキャストサーバモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

IRF スタックユニットのマスタ装置の VLAN インタフェースでは *ip-address* の範囲は、224.0.1.1～224.0.1.255 です。

例

NTP マルチキャストサーバモードで動作するように設定し、VLAN インタフェース 1 で暗号キーID が 4､NTP のバージョンが 4 の NTP マルチキャストメッセージをマルチキャストアドレス 224.0.1.1 に送信します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 4 authentication-keyid 4

関連コマンド

ntp-service multicast-client

3.1.15 ntp-service refclock-master

Syntax

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

デフォルト

装置は参照クロックとしてローカルクロックを使用しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: ローカルクロックの IP アドレス 127.127.1.u を指定します。ここで u は NTP プロセス ID です。設定範囲は 0～3 です。指定しない場合デフォルトは 127.127.1.0 です。

stratum: ローカルクロックの stratum レベルを指定します。設定範囲は 1～15 です。デフォルトは 8 です。stratum レベルの値が低いほど高いクロックの精度を持ちます。

説明

ntp-service refclock-master コマンドは他の装置の参照ソースとしてローカルクロックを設定します。

undo ntp-service refclock-master コマンドは設定を削除します。

一般的に stratum レベル 1 の NTP サーバは、原子時計のような基準となるソースから時間を取得し、NTP サーバとしてネットワークの他の装置に時間を提供します。各サーバの精度は、最上位レベル(プライマリサーバ)に割り当てられた stratum のレベルは 1 で、階層化された下のレベル(セカンダリサーバ)に割り当てられた stratum のレベルは 2、そして下の階層に下がるにつれて stratum のレベルの値が大きくなります。

もしネットワークの装置がもっとも権威のあるサーバに同期することができない場合、以下の作業を行うことができます。

- ネットワークから相対的に精度のあるクロックを持つ装置を選択することができます。
- ネットワークの他の装置と同期させるため、その相対的に精度のある装置のローカルクロックを使用します。

タイムエラーを避けるため、このコマンドを使用する場合、注意してください。このコマンドを実行する前に、ローカルシステム時間を正しい値に設定することを推奨します。

例

参照ソースとして stratum レベル 2 のローカルクロックを指定します。

<Switch> system-view

[Switch] ntp-service refclock-master 2

3.1.16 ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid: 認証キーを指定します。設定範囲は 1～4294967295 です。

説明

ntp-service reliable authentication-keyid コマンドは作成された認証キーをトラステッドキーとして指定します。

undo ntp-service reliable authentication-keyid コマンドは設定を削除します。

NTP 認証が有効であるとき、クライアントは信頼された認証キーを提供するサーバにのみ同期することができます。

このコマンドを使用する前に、NTP 認証が有効で認証キーが設定されていることを確認してください。キーを削除した後、キーは自動で非トラステッドキーに変更します。この場合、**undo ntp-service reliable authentication-keyid** コマンドを実行する必要はありません。

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

NTP 認証を有効にし、キーの ID が 37、キーの値が **BetterKey** の MD5 アルゴリズムの認証キーを設定します。

<Switch> system-view

[Switch] ntp-service authentication enable

[Switch] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey

トラステッドキーとして指定します。

[Switch] ntp-service reliable authentication-keyid 37

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**

3.1.17 ntp-service source

Syntax

ntp-service source *interface-type interface-number*

undo ntp-service source

デフォルト

NTP メッセージのインタフェースは指定されていません。装置は以下の動作を行います。

- NTP メッセージの送信インタフェースをルーティングテーブルから検索します。
- NTP メッセージの送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

ntp-service source コマンドは NTP メッセージの送信元インタフェースを指定します。

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

NTP メッセージの送信元インタフェースを指定する場合、装置は NTP メッセージを送信するとき、指定されたインタフェースのプライマリ IP アドレスとして NTP メッセージの送信元 IP アドレスを設定します。したがって、NTP 応答メッセージの宛先アドレスは、送信元インタフェースのプライマリ IP アドレスになります。

装置が NTP 要求に応答するとき、NTP 応答の送信元 IP アドレスは常に NTP 要求を受信したインタフェースの IP アドレスです。

応答メッセージの宛先アドレスにローカル装置のインタフェースの IP アドレスを使用しない場合、コマンドを使用して、NTP メッセージの送信元インタフェースとして別のインタフェースを指定します。

NTP メッセージの送信元インタフェースは、次の方法でも指定できます。

- NTP client/server モードで、**ntp-service unicast-server** コマンドで NTP メッセージの送信元インタフェースを指定した場合、指定したインタフェースは NTP メッセージの送信元インタフェースとして機能します。
- NTP symmetric active/passive モードで、**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、指定したインタフェースは NTP メッセージの送信元インタフェースとして機能します。
- NTP multicast モードで、インタフェースに **ntp-service mulsicast-server** コマンドを設定している場合、そのインタフェースは NTP マルチキャストメッセージの送信元インタフェースとして機能します。
- NTP broadcast mode で、インタフェースに **ntp-service broadcast-server** コマンドを設定している場合、そのインタフェースは NTP ブロードキャストメッセージの送信元インタフェースとして機能します。

指定した送信元インタフェースが down している場合、装置は NTP メッセージを送信しません。

例

NTP メッセージの送信元インタフェースとして VLAN インタフェース 1 を指定します。

<Switch> system-view

[Switch] ntp-service source vlan-interface 1

3.1.18 ntp-service unicast-peer

Syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**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。*maxpoll-interval* の設定範囲は 4～17 です。これを基準にして、秒単位で間隔を取得します。最大ポーリング間隔は 2^4～2^{17}（16～131072）秒の範囲です。*maxpoll-interval* のデフォルト値は 6 です。デフォルトの最大ポーリング間隔は 2^6（64）秒です。

minpoll *minpoll-interval*: 最小ポーリング間隔を指定します。*minpoll-interval* の設定範囲は 4～17 です。ここから 2 を底とする秒単位の間隔が得られます。最小ポーリング間隔は、2^4～2^{17}(16 から 131072)秒の範囲です。*minpoll-interval* のデフォルト値は 6 です。デフォルトの最小ポーリング間隔は 2^6(64)秒です。

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。このオプションを指定しない場合、装置はルーティングテーブルから送信インタフェースを検索し、送信インタフェースのプライマリ IP アドレスを NTP メッセージの送信元 IP アドレスとして使用します。

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 コマンドは装置に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。

undo ntp-service unicast-peer コマンドはパブリックネットワークの IP アドレスでシンメトリックーパッシブピアを削除します。

装置に対称受動ピアを指定すると、装置は最小ポーリング間隔でその時間をピア装置にポーリングし、同期します。2 つの間の時間差が許容範囲内に維持される場合、システム

は最大ポーリング間隔に達するまでポーリング間隔を徐々に増やします。時間差が許容範囲を繰り返し超えると、ポーリング間隔は徐々に短くなります。

ポーリング間隔設定は、次のポーリングから有効になります。

例

装置のシンメトリックーパッシブピアとして IP アドレス 10.1.1.1 の装置を指定します。NTP バージョンを 4、NTP メッセージの送信元インタフェースを VLAN インタフェース 1 に設定します。

<Switch> system-view

[Switch] ntp-service unicast-peer 10.1.1.1 version 4 source-interface vlan-interface 1

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

3.1.19 ntp-service unicast-server

Syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**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。*maxpoll-interval* の設定範囲は 4～17 です。これを基準にして、秒単位で間隔を取得します。最大ポーリング間隔は 2^4～2^{17}（16～131072）秒の範囲です。*maxpoll-interval* のデフォルト値は 6 です。デフォルトの最大ポーリング間隔は 2^6（64）秒です。

minpoll *minpoll-interval*: 最小ポーリング間隔を指定します。*minpoll-interval* の設定範囲は 4～17 です。ここから 2 を底とする秒単位の間隔が得られます。最小ポーリング間隔は、2^4～2^{17}(16 から 131072)秒の範囲です。*minpoll-interval* のデフォルト値は 6 です。デフォルトの最小ポーリング間隔は 2^6(64)秒です。

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。このオプションを指定しない場合、装置はルーティングテーブルから送信インタフェースを検索し、送信インタフェースのプライマリ IP アドレスを NTP メッセージの送信元 IP アドレスとして使用します。

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。

undo ntp-service unicast-server コマンドはパブリックネットワークの IP アドレスで NTP サーバを削除します。

装置の NTP サーバを指定すると、装置はその時間をポーリングし、最小ポーリング間隔でサーバと同期します。2 つの間の時間差が許容範囲内に維持される場合、システムは最大ポーリング間隔に達するまでポーリング間隔を徐々に増やします。時間差が許容範囲を繰り返し超えると、ポーリング間隔は徐々に短くなります。

ポーリング間隔設定は、次のポーリングから有効になります

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 **10-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 4-5
4.1.5 display snmp-agent statistics 4-7
4.1.6 display snmp-agent sys-info 4-9
4.1.7 display snmp-agent trap queue 4-10
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 4-14
4.1.11 snmp-agent 4-15
4.1.12 snmp-agent { inform | trap } source 4-16
4.1.13 snmp-agent calculate-password 4-17
4.1.14 snmp-agent community 4-19
4.1.15 snmp-agent group 4-22
4.1.16 snmp-agent local-engineid 4-25
4.1.17 snmp-agent log 4-26
4.1.18 snmp-agent mib-view 4-27
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 4-30
4.1.22 snmp-agent sys-info location 4-31
4.1.23 snmp-agent sys-info version 4-32
4.1.24 snmp-agent target-host 4-33
4.1.25 snmp-agent trap enable 4-35
4.1.26 snmp-agent trap if-mib link extended 4-36
4.1.27 snmp-agent trap life 4-37
4.1.28 snmp-agent trap log 4-38
4.1.29 snmp-agent trap periodical-interval 4-39
4.1.30 snmp-agent trap queue-size 4-40
4.1.31 snmp-agent usm-user { v1 | v2c } 4-41
4.1.32 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（trap 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指定します。

write: 読み出しと書き込みコミュニティ情報を指定します。

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。read か write かを指定しない場合、作成されたすべての SNMPv1 と SNMPv2c のコミュニティ情報を表示します。

SNMPv1 と SNMPv2c のコミュニティは次の方法で作成できます。

- **snmp-agent community** コマンドを使用して作成します。
- 既存の SNMP グループに割り当てられている SNMPv1 と SNMPv2c のユーザ用に自動的に作成されます。

例

すべての SNMPv1 と 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。 ● VACMモードで**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名です。
ACL	ACLの番号です。 このフィールドはSNMPv1あるいはSNMPv2cユーザがACLルールに関連づけられたときのみ表示されます。これはACL nameフィールドと排他的です。
ACL name	ACLの名前です。 このフィールドは、SNMPv1あるいはSNMPv2cユーザがACLルールに関連づけられたときのみ表示されます。これはACLフィールドと排他的です。

フィールド	説明
Storage-type	記憶媒体のタイプです。 • **volatile**—システムが再起動したときに設定が失われます。 • **nonVolatile**—システムが再起動しても設定は失われません。 • **permanent**—システムが再起動しても設定は失われません。変更することができますが、削除することができません。 • **readOnly**—システムが再起動しても設定は失われません。変更あるいは削除することができません。 • **other**—他の記憶媒体のタイプです。
Context name	SNMPの内容です。 • SNMPコミュニティとSNMPの内容間のマッピング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の番号です。 このフィールドはACLが指定されている場合にSNMPグループに割り当てられたときのみ表示されます。これはACL nameフィールドと排他的です。
ACL name	ACLの名前です。 このフィールドはACLが指定されている場合にSNMPグループに割り当てられたときのみ表示されます。これはACLフィールドと排他的です。

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、プライバシー、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 エンジンを一意に識別します。

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 に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。*view-name* の設定範囲は、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内のオブジェクトにはアクセスできませんが、通知を送信できます。

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エージェントで設定されていないSNMPバージョンのメッセージ数です。
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。

フィールド	説明
ASN.1 or BER errors in the process of decoding	復号化の間にASN.1あるいはBERエラーがあるメッセージ数です。
messages passed from the SNMP entity	SNMPエージェントによって送信されたメッセージ数です。
SNMP PDUs had badValue error-status	BadValueエラーのPDU数です。
SNMP PDUs had genErr error-status	genErrエラーのPDU数です。
SNMP PDUs had noSuchName error-status	NoSuchNameエラーのPDU数です。
SNMP PDUs had tooBig error-status	TooBigエラーのPDU数です。（最大パケットサイズが1500バイトです）
MIB objects retrieved successfully	正常に読み込まれたMIBオブジェクト数です。
MIB objects altered successfully	正常に書き込まれたMIBオブジェクト数です。
GetRequest-PDU accepted and processed	読み込み、処理されたGetRequest要求の数です。
GetNextRequest-PDU accepted and processed	読み込み、処理されたgetNext要求の数です。
GetBulkRequest-PDU accepted and processed	読み込み、処理されたgetBulk要求の数です。
GetResponse-PDU accepted and processed	読み込み、処理されたget応答の数です。
SetRequest-PDU accepted and processed	読み込み、処理されたset要求の数です。
Trap PDUs accepted and processed	読み込み、処理された通知の数です。
alternate Response Class PDUs dropped silently	廃棄された応答パケットの数です。
forwarded Confirmed Class PDUs dropped silently	廃棄された転送パケットの数です。

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:
    NEC Corporation

The location information of the agent:
    Tokyo, Japan

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 キューの標準情報を表示します。

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 コマンドはモジュールの状態を有効にする SNMP 通知を表示します。

モジュールに複数のサブモジュールがあり、そのサブモジュールの 1 つに対して SNMP 通知が有効になっている場合、コマンド出力はそのモジュールが SNMP 通知に対応していることを示しています。

モジュールが SNMP 通知をサポートしているかどうかを判断するには、**snmp-agent trap enable ?**コマンドを実行します。

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

SNMP 通知を作成できるモジュールと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.
ifmonitor notification is enabled.
mac-address notification is enabled.
port-security notification is disabled.
radius notification is disabled.
standard notification is enabled.
stp notification is disabled.
syslog notification is disabled.
system notification is enabled.

Enabled notifications: 5; Disabled notifications: 5
```

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 を指定します。エンジン ID は大文字、小文字を区別しません。タイミングの SNMPv3 ユーザが作成されると、システムはローカル SNMP エンティティエンジン ID を記録します。エンジン ID が次の場合、ユーザは無効になります。変更、記録されたエンジン ID が復帰すると再び有効になります。

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。

フィールド	説明
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の番号です。 このフィールドは、SNMPv3ユーザにACLが指定されている場合にのみ表示されます。これはACL nameフィールドと排他的です。
ACL name	ACLの名前です。 このフィールドは、SNMPv3ユーザにACLが指定されている場合にのみ表示されます。これはACLフィールドと排他的です。

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

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、この IP アドレスを使用して、SNMP エージェントによって送信されるすべての inform または trap をフィルタリングできます。

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。*plain-password* の設定範囲は、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プライバシーアルゴリズムを指定します。装置は、HMAC-MD5 および HMAC-SHA1 認証アルゴリズムをサポートします。HMAC-MD5 アルゴリズムは、HMAC-SHA1 アルゴリズムよりも高速です。HMAC-SHA1 アルゴリズムは、HMAC-MD5 アルゴリズムよりも高いセキュリティを提供します。3DES、および DES プライバシーアルゴリズム(セキュリティ強度の高い順)を装置で使用できます。より安全なアルゴリズムでは、計算に時間がかかります。一般的なセキュリティ要件を満たすには、DES で十分です。

- **3desmd5**: 3DES プライバシーアルゴリズムと HMAC-MD5 認証アルゴリズムを使用して、プライバシーキーのプライバシー形式を計算します。
- **3dessha**: 3DES プライバシーアルゴリズムと HMAC-SHA1 認証アルゴリズムを使用して、プライバシーキーのプライバシー形式を計算します。
- **md5**: HMAC-MD5 認証アルゴリズムと AES あるいは DES プライバシーアルゴリズムを使用して、認証キーあるいはプライバシーキーのプライバシー形式を計算します。HMAC-MD5 認証アルゴリズムを使用すると、AES プライバシーアルゴリズムあるいは DES プライバシーアルゴリズムのどちらを使用するかに関係なく、プライバシー形式で同じ認証キーあるいはプライバシーキーを取得できます。
- **sha**: HMAC-SHA1 認証アルゴリズムと AES あるいは DES プライバシーアルゴリズムを使用して、認証キーあるいはプライバシーキーのプライバシー形式を計算します。HMAC-SHA1 認証アルゴリズムを使用すると、AES プライバシーアルゴリズムあるいは DES プライバシーアルゴリズムのどちらが使用されているかに関係なく、プライバシー形式で同じ認証キーあるいはプライバシーキーを取得できます。

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** コマンドで **cipher** キーワードを指定して SNMPv3 ユーザを作るときに、**snmp-agent calculate-password** コマンドを使って生成される暗号キーを使用してください。

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 ID 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: コミュニティの標準あるいは詳細な IPv4 ACL を指定します。

ipv4-acl-number: IPv4 の標準 ACL あるいは詳細 ACL を番号で指定します。標準 IPv4 ACL 番号の設定範囲は、2000～2999 です。詳細 IPv4 ACL 番号の設定範囲は、3000～3999 です。

name *ipv4-acl-name*: 標準あるいは拡張 IPv4 ACL を名前で指定します。設定範囲は 1 から 63 文字です。大文字、小文字を区別しません。

acl ipv6: コミュニティの標準あるいは詳細な IPv6 ACL を指定します。

ipv6-acl-number: 標準あるいは詳細な IPv6 ACL を番号で指定します。標準 IPv6 ACL 番号の設定範囲は、2000～2999 です。拡張 IPv6 ACL 番号の設定範囲は、3000～3999 です。

name *ipv6-acl-name*: 標準あるいは拡張 IPv6 ACL を名前で指定します。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 コミュニティあるいは SNMPv2c コミュニティを設定します。

undo snmp-agent community コマンドは SNMPv1 コミュニティあるいは SNMPv2c コミュニティを削除します。

network-admin あるいは level-15 ユーザロールを持つユーザだけがこのコマンドを実行できます。他のユーザロールを持つユーザは、これらの役割が SNMP 機能のコマンドあるいはこのコマンドへのアクセスを許可されている場合でも、このコマンドを実行できません。

SNMP コミュニティは、コミュニティ名で識別されます。NMS と SNMP エージェントのセットが含まれています。SNMP コミュニティ内の装置は、コミュニティ名を使用して相互に認証します。NMS と SNMP エージェントは、同じコミュニティ名を使用する場合にのみ通信できます。

通常、**public** は読み取り専用コミュニティ名として使用され、**private** は読み取りおよび書き込みコミュニティ名として使用されます。セキュリティを強化するために、SNMP コミュニティに **public** および **private** 以外の名前を割り当てることができます。

snmp-agent community コマンドを使用すると、次のいずれかのモードを使用して MIB オブジェクトへの SNMP コミュニティアクセスを制御できます。

- **View-based access control model**—VACM モードでは、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。

snmp-agent community コマンドを使用して、最大 10 の SNMP コミュニティを作成できます。

コマンドを複数回実行して、同じコミュニティ名を指定し、毎回異なる設定を指定すると、最新の設定が有効になります。

コミュニティ名をプレーンテキストで設定および保存するには、**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されます。

- ACL を指定しない場合、指定した ACL が存在しない場合、あるいは指定した ACL にルールがない場合は、コミュニティ名を使用するすべての NMS が SNMP エージェントにアクセスできます。
- ACL を指定し、ACL にルールがある場合、ACL によって許可された NMS のみが SNMP エージェントにアクセスできます。

ACL の詳細については、オペレーションマニュアルのセクション 7 *ACL and QoS* を参照してください。

snmp-agent usm-user { v1 | v2c }および **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もできます。これら 2 つのコマンドは、SNMPv1 あるいは SNMPv2c ユーザと、そのユーザが割り当てられているグループを作成します。システムは、SNMPv1 あるいは SNMPv2c ユーザ名を使用して SNMP コミュニティを自動的に作成します。

例

プレーンテキストで読み込み専用のコミュニティ **readaccess** を作成します。SNMPv1 あるいは SNMPv2c の NMS はデフォルト view の **ViewDefault** の MIB オブジェクトを読むため、コミュニティ **readaccess** を使用します。

<Switch> system-view

[Switch] snmp-agent sys-info version v1 v2c

[Switch] snmp-agent community read simple readaccess

プレーンテキストで読み込み、書き込みコミュニティ **writeaccess** を作成します。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

プレーンテキストで読み込み、読み取りと書き込みのコミュニティを作成します。これにより、IP アドレスが 1.1.1.2 の SNMPv2c NMS だけがデフォルト 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、SNMP v2c：

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent group { **v1** | **v2c** } *group-name*

SNMPv3：

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *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 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。大文字、小文字を区別します。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: グループの標準あるいは詳細な IPv4A CL を指定します。

ipv4-acl-number: IPv4 の標準 ACL あるいは詳細 ACL を番号で指定します。標準 IPv4 ACL 番号の設定範囲は、2000～2999 です。詳細な IPv4 ACL 番号の設定範囲は、3000～3999 です。

name *ipv4-acl-name*: 標準あるいは拡張 IPv4 ACL を名前で指定します。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: グループの標準あるいは詳細な IPv6 ACL を指定します。

ipv6-acl-number: 標準あるいは詳細な IPv6 ACL を番号で指定します。標準 IPv6 ACL 番号の設定範囲は、2000～2999 です。拡張 IPv6 ACL 番号の設定範囲は、3000～3999 です。

name *ipv6-acl-name*: 標準あるいは拡張 IPv6 ACL を名前で指定します。大文字、小文字を区別しません。設定範囲 1～63 文字です。

説明

snmp-agent group コマンドは SNMP グループを作成します。

undo snmp-agent group コマンドは SNMP グループを削除します。

network-admin あるいは level-15 ユーザロールを持つユーザだけがこのコマンドを実行できます。他のユーザロールを持つユーザは、これらの役割が SNMP 機能のコマンドあるいはこのコマンドへのアクセスを許可されている場合でも、このコマンドを実行できません。

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。

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。

ユーザとグループにそれぞれ ACL を指定して、不正な NMS をフィルタリングできます。ACL でユーザとグループの両方に対して許可されている NMS だけが SNMP エージェントにアクセスできます。ユーザおよびグループの ACL には、次のルールが適用されます。

- ACL を指定しない場合、指定した ACL が存在しない場合、あるいは指定した ACL にルールがない場合は、ユーザ名を使用するすべての NMS が SNMP エージェントにアクセスできます。
- ACL を指定し、ACL にルールがある場合、ACL によって許可された NMS のみがエージェントにアクセスできます。

ACL の詳細については、オペレーションマニュアルのセクション 7 *ACL and QoS* 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

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。各装置には一意の装置 ID 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

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のローカル SNMP エンジン ID 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 エンティティを一意に識別します。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 ユーザ名とプライバシーしたキーを無効にすることができます。

デフォルトのエンジン ID を使用するか、ネットワークプランに基づいて覚えやすいエンジン ID を設定できます。たとえば、建物 A の 1 階にある装置 1 のエンジン ID を 000Af0010001 に、装置 2 のエンジン ID を 000Af0010002 に設定できます。

例

SNMP 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 Get オペレーションと Set オペレーションのロギングを有効にします。

authfail: SNMP authfail 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 のロギングを有効にします。

undo snmp-agent log コマンドは SNMP 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 authfail 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。大文字と小文字を区別します。

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。大文字と小文字を区別します。OID は MIB ツリーのオブジェクトを一意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。大文字と小文字を区別しません。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)を表し、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同じ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 1.3.6.1.2.1.1)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(単位はバイト)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 応答の DSCP 値を設定します。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

snmp-agent packet response dscp コマンドは SNMP 応答の DSCP 値を設定します。

snmp-agent packet 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 応答の 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

Syntax

snmp-agent sys-info contact version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

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

all: SNMPv1、SNMPv2c、SNMPv3 を指定します。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

説明

snmp-agent sys-info version コマンドは SNMP のバージョンを有効にします。

undo snmp-agent sys-info version コマンドは SNMP のバージョンを無効にします。

NMS が SNMP エージェントと正常に通信するため、SNMP エージェントは NMS と同じ SNMP のバージョンを設定します。

例

SNMPv3 を有効にします。

<Switch> system-view

[Switch] snmp-agent sys-info version v3

関連コマンド

display snmp-agent sys-info

4.1.24 snmp-agent target-host

Syntax

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

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

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } **params securityname** *security-string*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

inform: inform として通知を送信します。

trap: trap として通知を送信します。

address: SNMP 通知の宛先アドレスを指定します。

udp-domain: トランスポートプロトコルとして UDP を指定します。

ipv4-address: ターゲットホストを IPv4 アドレスあるいはホスト名で指定します。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。文字列には、文字、数字、ハイフン(-)、アンダースコア(_)、ドット(.)のみが含まれます。ホスト名を指定する場合は、ターゲットホストの IPv4 アドレス取得できます。

ipv6 *ipv6-address*: ターゲットホストを IPv6 アドレスあるいはホスト名で指定します。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。文字列には、文字、数字、ハイフン(-)、アンダースコア(_)、ドット(.)のみが含まれます。ホスト名を指定すると、ターゲットホストの IPv6 アドレスを取得できます。IPv6 アドレスを指定する場合、そのアドレスをリンクローカルアドレスにすることはできません。

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。

dscp-value: ターゲットホストに送信されるトラップの DSCP 値を設定します。設定範囲は 0～63 です。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。DSCP 値が大きいほど、優先順位が高くなります。トラップのデフォルトの DSCP 値は 0 です。

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。大文字、小文字を区別します。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

- **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 通知のターゲットホストを設定します。

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。**snmp-agent trap enable ?**コマンドをクリックして、値を取得します。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 SNMP 通知を有効にします。

undo snmp-agent trap enable コマンドは SNMP 通知を無効にします。

重要なプロトコルイベントを NMS に報告するには、まずプロトコルを有効にし、次にプロトコルの SNMP 通知を有効にします。

SNMP 通知を正しく送信するには、必要に応じて通知送信パラメータも設定する必要があります。

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 エージェントが SNMP 認証失敗通知を送信できるようにします。

<Switch> system-view

[Switch] snmp-agent trap enable standard authentication

関連コマンド

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 trap 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 periodical-interval

Syntax

snmp-agent trap periodical-interval *interval*

undo snmp-agent trap periodical-interval

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

interval: SNMP alive trap を送信する間隔を指定します。設定範囲は 10～3600 または 0 です。設定単位は秒です。設定を 0 にすると、SNMP alive trap が無効になります。

説明

snmp-agent trap periodical-interval コマンドは SNMP alive trap を有効にし、送信間隔を設定します。

undo snmp-agent trap periodical-interval コマンドは 60 秒に設定します。

装置は指定された間隔で SNMP alive trap を送信して、SNMP が正常に動作していることを NMS に通知できます。

undo snmp-agent trap periodical-interval を使用しても、デフォルトに戻すことはできません。送信間隔を再設定するには、**snmp-agent trap periodical-interval 0** を使用する必要があります。

例

SNMP alive trap を有効にし、送信間隔を 10 秒に設定します。

<Switch> system-view

[Switch] snmp-agent trap periodical-interval 10

SNMP alive trap を無効にします。

<Switch> system-view

[Switch] snmp-agent trap periodical-interval 0

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**

4.1.30 snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

size: SNMP 通知のキューが保持できる通知の最大数を指定します。設定範囲は 1～1000 です。

説明

snmp-agent trap queue-size コマンドは SNMP 通知のキューのサイズを設定します。

undo snmp-agent trap queue-size コマンドはデフォルトのキューのサイズに戻します。

衝突が発生したとき、SNMP エージェントはキューに通知をバッファします。SNMP 通知のキューのサイズは SNMP 通知のキューが保持できる通知の最大数を設定します。キューのサイズが上限に到達したとき、新しい通知のために、古い通知が廃棄されます。

例

SNMP 通知のキューのサイズを 200 に設定します。

<Switch> system-view

[Switch] snmp-agent trap queue-size 200

関連コマンド

- **snmp-agent target-host**

- **snmp-agent trap enable**
- **snmp-agent trap life**

4.1.31 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: ユーザの標準あるいは詳細な IPv4 ACL を指定します。

ipv4-acl-number: IPv4 の標準 ACL あるいは詳細 ACL を番号で指定します。標準 IPv4 ACL 番号の設定範囲は、2000～2999 です。詳細な IPv4 ACL 番号の設定範囲は、3000 から 3999 です。

name *ipv4-acl-name*: 標準あるいは拡張 IPv4 ACL を名前で指定します。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*: ユーザの標準あるいは詳細な IPv6 ACL を指定します。

ipv6-acl-number: 標準あるいは詳細な IPv6 ACL を番号で指定します。標準 IPv6 ACL 番号の設定範囲は、2000～2999 です。拡張 IPv6 ACL 番号は、3000～3999 です。

name *ipv6-acl-name*: 標準あるいは拡張 IPv6 ACL を名前で指定します。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。

network-admin あるいは level-15 ユーザロールを持つユーザだけがこのコマンドを実行できます。他のユーザの役割を持つユーザは、これらの役割が SNMP 機能のコマンドあるいはこのコマンドへのアクセスを許可されている場合でも、このコマンドを実行できません。

SNMPv1 あるいは SNMPv2c ネットワーク、NMS、およびエージェントは、コミュニティ名を使用して相互に認証を行います。SNMPv3 ネットワーク、NMS、およびエージェントは、ユーザ名を使用して相互に認証を行います。

SNMPv1 あるいは SNMPv2c コミュニティを作成できます。次のいずれかの方法を使用します。

- **snmp-agent community** コマンドを実行します。
- **snmp-agent usm-user { v1 | v2c }**および **snmp-agent group { v1 | v2c }**コマンドを実行して、SNMPv1 あるいは SNMPv2c ユーザ、およびユーザが割り当てられているグループを作成します。システムは、SNMPv1 あるいは SNMPv2c ユーザ名を使用して SNMP コミュニティを自動的に作成します。

ユーザとグループにそれぞれ ACL を指定して、不正な NMS をフィルタリングできます。ACL でユーザとグループの両方に対して許可されている NMS だけが SNMP エージェントにアクセスできます。ユーザおよびグループの ACL には、次のルールが適用されます。

- ACL を指定しない場合、指定した ACL が存在しない場合、あるいは指定した ACL にルールがない場合は、ユーザ名を使用するすべての NMS が SNMP エージェントにアクセスできます。
- ACL を指定し、ACL にルールがある場合、ACL によって許可された NMS のみがエージェントにアクセスできます。

ACL の詳細については、オペレーションマニュアルのセクション 7 *ACL and QoS* 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

ユーザ **userv2c** を SNMPv2c グループ **readCom** に追加して、1.1.1.2 の NMS だけがプロトコル SNMPv2c と読み取り専用コミュニティ名 **userv2c** を使用して装置にアクセスできるようにします。

[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**

4.1.32 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。グループは、作成されたものでも作成されていないものでもかまいません。ユーザは、グループを作成した後でのみ有効になります。

cipher: *auth-password*、*priv-password* を暗号キーとして指定します。キーはプライバシーされた形式でダイジェストに変換され、装置に保存されます。

simple: *auth-password*、*priv-password* をプレーンテキストのキーとして指定します。キーはプライバシーされた形式でダイジェストに変換され、装置に保存されます。

authentication-mode: 認証アルゴリズムを指定します。キーワードを指定しないと、システムは認証を実行しません。

- **md5**: HMAC-MD5 認証アルゴリズムを指定します。
- **sha**: HMAC-SHA-1 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、小文字が区別されます。

- キーのプレーンテキスト形式の設定範囲は、1～64 文字です。この文字列には、数字、大文字、小文字、および特殊文字を含める必要があります。
- キーのプライバシー形式は、**snmp-agent calculate-password** コマンドを使用して計算できます。

privacy-mode: プライバシーアルゴリズムを指定します。このキーワードを指定しない場合、システムはプライバシーを実行しません。

- **3des**: 168 ビットキーを使用する 3DES プライバシーアルゴリズムを指定します。
- **aes128**: 128 ビットキーを使用する AES プライバシーアルゴリズムを指定します。
- **des56**: 56 ビットキーを使用する DES プライバシーアルゴリズムを指定します。

priv-password: プライバシーキーを指定します。大文字、小文字が区別されます。

- キーのプレーンテキスト形式の設定範囲は、1～64 文字です。この文字列には、数字、大文字、小文字、および特殊文字を含める必要があります。
- キーのプライバシー形式は、**snmp-agent calculate-password** コマンドを使用して計算できます。

acl: ユーザの標準または詳細な IPv4 ACL を指定します。

ipv4-acl-number: IPv4 の標準 ACL または詳細 ACL を番号で指定します。標準 IPv4 ACL 番号の設定範囲は、2000～2999 です。詳細な IPv4 ACL 番号の設定範囲は、3000～3999 です。

name *ipv4-acl-name*: 標準または拡張 IPv4 ACL を名前で指定します。大文字、小文字を区別しません。設定範囲は 1～63 文字です。

acl ipv6: ユーザの標準または詳細な IPv6 ACL を指定します。

ipv6-acl-number: 標準または詳細な IPv6 ACL を番号で指定します。標準 IPv6 ACL 番号の設定範囲は 2000～2999 です。拡張 IPv6 ACL 番号の設定範囲は、3000～3999 です。

name *ipv6-acl-name*: 標準または拡張 IPv6 ACL を名前で指定します。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。デフォルトでは SNMPv3 ユーザは、ローカル SNMP エンジンに関連付けられています。

engineid *engineid-string*: SNMP エンジン ID を指定します。*engineid-string* には、偶数個の 16 進文字を指定します。すべて 0 の文字列とすべて F の文字列は無効です。偶数の設定範囲は 10～64 です。ローカルエンジン ID を変更すると、デフォルトの SNMPv3 ユーザとキーは無効になります。ユーザ名に関連付けられたエンジン ID を **undo snmp-agent usm-user v3** コマンドは、無効なユーザ名を削除します。

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 ユーザを削除します。

network-admin または level-15 ユーザロールを持つユーザだけがこのコマンドを実行できます。他のユーザロールを持つユーザは、これらの役割が SNMP 機能のコマンドまたはこのコマンドへのアクセスを許可されている場合でも、このコマンドを実行できません。

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**—SNMP グループにユーザを割り当てることにより、MIB オブジェクトへのユーザアクセスを制御します。ユーザを有効にするには、グループが作成されていることを確認します。SNMP グループには、1 人または複数のユーザが含まれ、そのユーザの MIB view とセキュリティモデルを指定します。各ユーザの認証およびプライバシーアルゴリズムは、作成時に指定されます。

snmp-agent usm-user v3 コマンドを複数回実行して、VACM モードで異なる SNMPv3 ユーザを作成できます。ユーザ名を毎回変更しない場合は、最新の設定が有効になります。

ユーザとグループにそれぞれ ACL を指定して、不正な NMS がエージェントにアクセスしないようにフィルタリングできます。ACL でユーザとグループの両方に対して許可されている NMS だけが SNMP エージェントにアクセスできます。ユーザおよびグループの ACL には、次のルールが適用されます。

- ACL を指定しない場合、指定した ACL が存在しない場合、または指定した ACL にルールがない場合は、ユーザ名を使用するすべての NMS が SNMP エージェントにアクセスできます。
- ACL を指定し、ACL にルールがある場合、ACL によって許可された NMS のみがエージェントにアクセスできます。

ACL の詳細については、オペレーションマニュアルのセクション 7 *ACL and QoS* 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-SHA-1**、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-SHA-1**、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 **10-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 5-13
5.1.8 rmon event 5-16
5.1.9 rmon history.....5-17
5.1.10 rmon prialarm 5-19
5.1.11 rmon statistics.....5-21

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 ● delta
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）。
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	最初のサンプリングで生成可能なアラームです。 ● **risingAlarm** ● **fallingAlarm** ● **risingOrFallingAlarm** デフォルトは**risingOrFallingAlarm**です。
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。

イベントエントリには、次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。レコードが上限に達したとき、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はMIBオブジェクトです。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、ether History Table 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*.	履歴管理エントリのオーナと状態です。 ● *entry-number*—履歴管理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履歴管理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。 （MIBオブジェクトhistory Control Buckets Granted） **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	履歴サンプルインデックスです。
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。
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。

フィールド	説明
undersize packets	サンプリング間隔中に受信した過小サイズのエラーパケットの数です。 過小サイズエラーパケットはパケット長が64オクテット未満のパケットです。（フレームビットを除き、FCSオクテットを含みます）
oversize packets	サンプリング間隔中に受信した過大サイズのエラーパケットの数です。 過大サイズエラーパケットはパケット長が1518オクテットを超えるパケットです。(フレームビットを除き、FCSオクテットを含みます)
fragments	サンプリング間隔中に受信した過小サイズのCRCエラーパケットの数です。
jabbers	サンプリング間隔中に受信した過大サイズのCRCエラーパケットの数です。
collisions	サンプリング間隔中に受信したコリジョンパケットの数です。
utilization	サンプリング間隔中の帯域幅の使用率です。(単位は%です)

関連コマンド

rmon history

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 RMON 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 ● delta
Variable formula	変数の式です。
Description	アラームエントリの説明です。

フィールド	説明
Sampling interval	サンプルされるデータの間隔（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	最初のサンプリングで生成可能なアラームです。 • **risingAlarm** • **fallingAlarm** • **risingOrFallingAlarm** 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。

フィールド	説明
etherStatsBroadcastPkts	インタフェースで受信したブロードキャストパケットの総数です。
etherStatsMulticastPkts	インタフェースで受信したマルチキャストパケットの総数です。
etherStatsUndersizePkts	インタフェースで受信した過小サイズのエラーパケットの総数です。
etherStatsOversizePkts	インタフェースで受信した過大サイズのエラーパケットの総数です。
etherStatsFragments	インタフェースで受信した過小サイズのCRCエラーパケットの総数です。
etherStatsJabbers	インタフェースで受信した過大サイズのCRCエラーパケットの総数です。
etherStatsCRCAlignErrors	インタフェースで受信したCRCエラーパケットの総数です。
etherStatsCollisions	インタフェースで受信したコリジョンパケットの総数です。
etherStatsDropEvents	廃棄されたパケットのイベント総数です。 🕮 **メモ**: 統計情報は、廃棄が発生した回数です。廃棄したパケットの総数になるわけではありません。
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、INTEGER32、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 アラーム変数形式

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: 増加方向のしきい値または減少方向のしきい値に達したときまたは超えたときに、最初のサンプリング時に生成できるアラームを指定します。デフォルトでは、増加方向、減少方向のアラームが生成されます。

rising: 増加方向のアラームを作成します。

falling: 減少方向のアラームを作成します。

rising-falling: 増加方向または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一意のアラーム変数、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 etherStatsOctets1 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 etherStatsOctets5 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。このパラメータはサポートされていますが、現在のソフトウェアバージョンでは有効になりません。

none: イベントが発生したとき、アクションを行いません。

trap: イベントが発生したとき、SNMP 通知を送信します。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

🕮 **メモ**:

security-string の SNMP コミュニティの設定は､コマンドで設定することができますが適用されません。システムは RMON の SNMP 通知を送信するとき、SNMP の設定を使用します。SNMP 通知の詳細は、オペレーションマニュアルのセクション 10 *システム管理* “*SNMP*”を参照してください。

説明

rmon event コマンドは RMON イベントテーブルのエントリを作成します。

undo rmon event コマンドは RMON イベントテーブルからエントリを削除します。

最大 60 のイベントエントリを作成することができます。

アラーム状況が発生したとき、アクションを指定するため、イベントエントリを標準あるいはプライベートアラームエントリに関連づけることができます。設定に依存して、イベントのログを取得し、SNMP 通知を送信することができます。

複数のアラームエントリに 1 つのイベントを関連づけることができます。

例

RMON イベントテーブルのイベント **10**、エントリオーナ **user1** を作成します。

<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** *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 *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。

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。

Ethernet インタフェースに複数の RMON 履歴管理エントリを設定することができます。

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。正しい計算結果を得るには、次の条件が満たされていることを確認します。

- 式の変数の値は正の整数です。
- 各計算ステップの結果は、長整数の値の範囲内にあります。

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: 増加方向のしきい値または減少方向のしきい値を超えたときに、最初のサンプリング時に生成できるアラームを指定します。デフォルトでは、増加方向、減少方向のアラームが生成されます。

rising: 増加方向のアラームを作成します。

falling: 減少方向のアラームを作成します。

rising-falling: 増加方向または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一意のアラーム変数、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。

Ethernet インタフェースに作成できる RMON 統計情報テーブルエントリは 1 つだけです。

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 **10-x-x** です。

6 章 NETCONF 6-1
6.1 NETCONF 設定コマンド 6-1
6.1.1 netconf log.....6-1
6.1.2 netconf soap enable 6-2
6.1.3 xml 6-3

6章 NETCONF

6.1 NETCONF設定コマンド

6.1.1 netconf log

Syntax

netconf log source { { **agent** | **soap** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **verbose** }

undo netconf log source { { **agent** | **soap** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **verbose** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

source: プロトコルを使用するクライアントを表す NETCONF オペレーションソースを指定します。

- **agent**: SSH 経由で Telnet、SSH、コンソール、または NETCONF を使用するクライアントを指定します。
- **soap**: SOAP over HTTP または SOAP over HTTPS を使用するクライアントを指定します。

protocol-operation: 特定のタイプの NETCONF オペレーションに対するリクエストとリプライを記録します。

- **all**: NETCONF テストのすべてのタイプを指定します。
- **action**: <action>テストを指定します。
- **config**: <CLI>、<save>、<load>、<rollback>、<lock>、<unlock>、および<save-point>テストなど、設定に関連した NETCONF テストを指定します。
- **get**: <get>、<get-config>、<get-bulk>、<get-bulk-config>、および<get-sessions>の各テストを含む、データ取得関連の NETCONF テストを指定します。
- **session**: <kill-session>および<close-session>テスト、hello メッセージによる機能交換など、セッション関連の NETCONF テストを指定します。
- **set**: すべての<edit-config>テストを指定します。
- **syntax**: XML およびスキーマエラーを含む要求を指定します。

- **others**: **action**、**config**、**get**、**set**、**session**、および **syntax** で指定されたテスト以外の NETCONF テストを指定します。

verbose: NETCONF テストのタイプに対する要求と応答の詳細情報を記録します。これには、フォーマットが正しい要求のパケットの内容や、失敗した<edit-config>テストに関するエラー情報が含まれます。

説明

netconf log コマンドは NETCONF ロギングを有効にします。

undo netconf log コマンドは指定した NETCONF オペレーションソースおよび NETCONF オペレーションの設定を削除します。

protocol-operation を指定した場合、装置は一致したテストとその結果をそれぞれログに記録します。たとえば、VLAN3 から 5 を作成するために NETCONF オペレーションを実行すると、装置は以下のログメッセージを出力します。

```
%Mar 21 17:11:34:479 2017 NEC XMLSOAP/6/XML_REQUEST: test from 192.168.100.198,
session id 2,message-id 100, receive edit-config request.
%Mar 21 17:11:34:483 2017 NEC XMLSOAP/6/EDIT-CONFIG: test from 192.168.100.198,
session id 2,message-id 100, execute success.
```

NETCONF が作成されたログを information center に正しく送信するには、information center も設定する必要があります。information center の設定の詳細については、オペレーションマニュアルのセクション 10 *システム管理* を参照してください。

例

エージェントクライアントから送信された NETCONF の編集設定情報を記録するように装置を設定します。

<Switch> system-view

[Switch] netconf log source agent protocol-operation set

6.1.2 netconf soap enable

Syntax

netconf soap { **http** | **https** } **enable**

undo netconf soap { **http** | **https** } **enable**

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

http: HTTP 上の SOAP で NETCONF を指定します。

https: HTTPS 上の SOAP で NETCONF を指定します。

説明

netconf soap enable コマンドは SOAP 上で NETCONF を有効にします。

undo netconf soap enable コマンドは SOAP 上で NETCONF を無効にします。

このコマンドを使用すると、装置は HTTP あるいは HTTPS パケットの SOAP でカプセル化されている NETCONF メッセージを解決できます。

例

HTTP 上の SOAP で NETCONF を有効にします。

<Switch> system-view

[Switch] netconf soap http enable

6.1.3 xml

Syntax

xml

View

User view

定義済みユーザロール

network-admin

network-operator

説明

xml コマンドは XML view に移行します。

XML view では NETCONF メッセージを使用して装置を設定するか、装置からデータを取得します。実行できる NETCONF テストは、表 6-1 に示すように、ユーザロールによって異なります。

表 6-1 事前定義されたユーザ役割で使用可能な NETCONF テスト

ユーザの役割	NETCONF オペレーション
network-admin	すべてのNETCONFオペレーションです。

ユーザの役割	NETCONF オペレーション
network-operator	• Get • Get-bulk • Get-bulk-config • Get-config • Get-sessions • Close-session

XML view で NETCONF メッセージのフォーマットが正しいことを確認するには、NETCONF メッセージを手動で入力しないでください。メッセージをコピーして貼り付けます。

装置が NETCONF オペレーションを実行している間は、NETCONF メッセージの貼り付けや **Enter** キーの押下などの他のオペレーションを実行しないでください。

装置が NETCONF メッセージを識別するためには、各 NETCONF メッセージの最後にエンドマーク**]]>]]>**を追加する必要があります。

XML view に入ると、装置は自動的に NETCONF 機能をクライアントに配信します。それに応じて、サポートされている NETCONF 機能を装置に通知するようにクライアントを設定する必要があります。機能交換の後、クライアントを使用して装置を設定できます。

NETCONF メッセージは、装置の NETCONF XML API リファレンスの XML 形式の要件と意味および構文の要件に準拠している必要があります。サードパーティ製のソフトウェアを使用して NETCONF メッセージを作成し、設定を確実に成功させます。

XML view を終了するには、**quit** コマンドの代わりに NETCONF メッセージを使用してください。

ユーザ行またはユーザ行クラスの view で **escape-key** コマンドを使用してショートカットキー（デフォルトでは **Ctrl+C**）を設定している場合は、NETCONF メッセージにショートカットキーの文字列を含めないでください。NETCONF メッセージにショートカットキーの文字列が含まれている場合、XML view の関連設定が影響を受ける可能性があります。たとえば、ユーザライン view では、**escape-key a** コマンドを使用して「a」をショートカットキーとして設定しました。NETCONF メッセージに文字"a"が含まれていると、メッセージ内の最後の"a"以降の内容のみを処理できます

例

XML view に移行します。

<Switch> xml

```
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn
:ietf:params:netconf:base:1.1</capability><capability>urn:ietf:params:netconf
:writable-running</capability><capability>urn:ietf:params:netconf:capability:
notification:1.0</capability><capability>urn:ietf:params:netconf:capability:v
alidate:1.1</capability><capability>urn:ietf:params:netconf:capability:interl
```

```
eave:1.0</capability><capability>urn:nec:params:netconf:capability:nec-netcon
f-ext:1.0</capability></capabilities><session-id>1</session-id></hello>]]>]]>
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
          urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>]]>]]>
```

XML view を終了します。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session>
  </close-session>
</rpc>]]>]]>
```

<Switch>

目次

このセクションのページは **10-x-x** です。

7 章 プロセスモニタリングとメンテナンス.....7-1
7.1 プロセスモニタリングとメンテナンス設定コマンド 7-1
7.1.1 display exception context.....7-1
7.1.2 display exception filepath.....7-6
7.1.3 exception filepath.....7-7
7.1.4 process core.....7-8
7.1.5 reset exception context.....7-9

7章 プロセスモニタリングとメンテナンス

7.1 プロセスモニタリングとメンテナンス設定コマンド

display memory、**display process**、**display process cpu**、**monitor process**、および **monitor thread** コマンドを使用すると、ユーザプロセスとカーネルスレッドの両方に関する情報が表示されます。これらのコマンドでは、"process"はユーザプロセスとカーネルスレッドの両方を指します。

7.1.1 display exception context

Syntax

display exception context [**count** *value*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

count *value*: コンテキスト情報のエントリを指定します。設定範囲は 1～20 です。デフォルトは 1 です。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。指定しない場合、IRF スタックのマスタ装置のプロセス例外に関するコンテキスト情報を表示します。

説明

display exception context コマンドはプロセス例外に関するコンテキスト情報を表示します。

システムは、各コアファイルのコンテキスト情報エントリを作成します。コンテキスト情報エントリは、プロセス ID、クラッシュ時間、コアファイルのディレクトリ、スタック情報、レジスタ情報が含まれます。

例

x86 ベースの 32 ビット端末に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 ビット端末に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
```

PowerPC ベースの 32 ビット端末に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
```

PowerPC ベースの 64 ビット端末に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 ビット端末に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   t3:0xfffffff8
   t4:0x69766520   t5:0x00000000   t6:0x63cc6000   t7:0x44617461
   s0:0x7fd26f81   s1:0x00401948   s2:0x7fd268f8   s3:0x803e1db0
   s4:0x803e1da0   s5:0x803e1d88   s6:0x803e1d70   s7:0x803e1d60
   t8:0x00000008   t9:0x2af2fae0   k0:0x00000000   k1:0x00000000
```

```
   gp:0x2af9a3a0   sp:0x7fd267c0   s8:0x7fd267c0   ra:0x00406d8c
   sr:0x0000dc13   lo:0xef9db265   hi:0x0000003f  bad:0x2add2010
cause:0x00800020   pc:0x2af2faf4
```

MIPS ベースの 64 ビット端末に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 7-1 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**—例外ブレークポイントのトレースです。 • **SIGXCPU**—CPU使用率の制限が超過しました。 • **SIGXFSZ**—ファイルサイズの制限が超過しました。 • **SIGUNKNOW**—不明な理由です。
Crash time	コアファイルが作成された時間です。
Core file path	コアファイルが保存されているディレクトリです。
Backtrace stopped	すべてのスタック情報が表示されています。

関連コマンド

reset exception context

7.1.2 display exception filepath

Syntax

display exception filepath [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。指定しない場合、IRF スタックのマスタ装置のプロセス例外に関するコンテキスト情報を表示します。

説明

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

例

コアファイルのディレクトリを表示します。

<Switch> display exception filepath slot 1

```
The exception filepath on slot 1 is flash:.
```

7.1.3 exception filepath

Syntax

exception filepath *directory*

undo exception filepath *directory*

デフォルト

コアファイルを保存するディレクトリは、flash:/です。

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: コアファイルを保存するディレクトリを指定します。

説明

exception filepath コマンドはコアファイルを保存するディレクトリを設定します。

undo exception filepath コマンドは指定されたディレクトリを削除します。

指定するディレクトリは、マスタ上の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。

装置に異なるタイプの記憶媒体がある場合は、コマンドを使用してディレクトリを変更できます。

システムは、コアファイルを指定されたディレクトリのコアディレクトリに保存します。指定したディレクトリにコアディレクトリが存在しない場合は、コアファイルを保存する前にコアディレクトリが作成されます。

ディレクトリが指定されていないか、指定されたディレクトリにアクセスできない場合、システムはコアファイルを保存できません。

例

コアファイルを保存するディレクトリを flash:/に指定します。

<Switch> exception filepath flash:/

関連コマンド

- **display exception filepath**
- **process core**

7.1.4 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ファイルを作成し、続く例外のコアファイルを作成しません。

定義済みユーザロール

network-admin

パラメータ

off: コアファイルの作成を無効にします。

maxcore *value*: コアファイルの作成を有効にし、コアファイルの最大数を設定します。設定範囲は 1～10 です。

name *process-name*: プロセス名を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別しません。

job *job-id*: job ID でプロセスを指定します。設定範囲は 1～2147483647 です。プロセスを再起動しても、job ID は変わりません。

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックのマスタ装置の情報を表示します。

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。

このコマンドは、プロセスのすべてのインスタンスに適用されます。

コマンドは、コアファイルが最大数になるまで、指定されたプロセスがクラッシュするたびに、コアファイルを作成することを有効にします。コアファイルは例外情報を記録します。

コアファイルはシステムのストレージリソースを消費するため、例外情報を確認する必要のないプロセスについては、コアファイルの作成を無効にできます。

例

プロセス **routed** のコアファイルの作成を無効にします。

<Switch> process core off name routed

プロセス **routed** のコアファイルの作成を有効にし、コアファイルの最大数を 5 に設定します。

<Switch> process core maxcore 5 name routed

関連コマンド

- **display exception context**
- **exception filepath**

7.1.5 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*: IRF スタックメンバ装置の ID を指定します。指定しない場合、IRF スタックのマスタ装置上のプロセス例外のコンテキスト情報を削除します。

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 **10-x-x** です。

8 章 ポートミラーリング.....8-1
8.1 ポートミラーリング設定コマンド.....8-1
8.1.1 display mirroring-group.....8-1
8.1.2 mirroring-group.....8-2
8.1.3 mirroring-group mirroring-port (interface view).....8-3
8.1.4 mirroring-group mirroring-port (system view).....8-4
8.1.5 mirroring-group monitor-egress.....8-6
8.1.6 mirroring-group monitor-port (interface view).....8-7
8.1.7 mirroring-group monitor-port (system view).....8-8
8.1.8 mirroring-group reflector-port.....8-10
8.1.9 mirroring-group remote-probe vlan.....8-11

8章 ポートミラーリング

8.1 ポートミラーリング設定コマンド

8.1.1 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を番号で指定します。設定範囲は 1～7 です。

all: すべてのミラーリンググループを指定します。

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。

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 8-1 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 • Remote source • Remote destination
Status	ミラーリンググループの状態です。 • **Active**—ミラーリンググループが有効です。 • **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。

8.1.2 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を番号で指定します。設定範囲は 1～7 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

8.1.3 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を番号で指定します。設定範囲は 1～7 です。

both:受信パケットと送信パケットの両方をミラーします。

inbound: 受信パケットをミラーします。

outbound: 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 コマンドはデフォルトに戻します。

ローカルミラーリンググループあるいはリモート送信元グループにのみ送信元ポートを設定することができます。

レイヤ 2 アグリゲートインタフェースは、ミラーリンググループの送信元ポートとして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、1 つのミラーリンググループに対してのみ送信元ポートとして機能できます。ポートを送信元ポートとして複数のミラーリンググループに割り当てると、最新の設定が有効になります。

送信元ポートは、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

8.1.4 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を番号で指定します。設定範囲は 1～7 です。

interface-list: 最大 8 個のインタフェース項目をスペースで区切ったリストを指定します。各項目は、そのタイプと番号によってインタフェースを指定するか、*interface-type interface-number 1* **to** *interface-type interface-number 2* の形式で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を指定する場合、インタフェースは同じタイプで同じスロット上になければなりません。開始インタフェース番号は終了インタフェース番号以下でなければなりません。

both: 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: 受信されたパケットのみをミラーします。

outbound: 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。

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にのみ送信元ポートを設定することができます。

レイヤ 2 アグリゲートインタフェースをミラーリンググループの送信元ポートとして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、1 つのミラーリンググループに対してのみ送信元ポートとして機能できます。ポートを送信元ポートとして複数のミラーリンググループに割り当てると、最新の設定が有効になります。

送信元ポートは、リフレクタポート、モニタポート、出力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

8.1.5 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を番号で指定します。設定範囲は 1～7 です。
interface-type interface-number: ポートをタイプと番号で指定します。

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 コマンドはデフォルトに戻します。

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。

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ポートを送信ポートに設定しないでください。

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として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

8.1.6 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を番号で指定します。設定範囲は 1～7 です。

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 コマンドはデフォルトに戻します。

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にのみ設定することができます。

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しないでください。

レイヤ 2 アグリゲートインタフェースは、ミラーリンググループのモニタポートとして設定しないでください。

データをモニタする装置はミラーされたトラフィックのみを受信するように、モニタポートはポートミラーリングのみに使用してください。

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

8.1.7 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を番号で指定します。設定範囲は 1～7 です。

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にのみ設定することができます。

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しないでください。

レイヤ 2 アグリゲートインタフェースは、ミラーリンググループのモニタポートとして設定できません。

データをモニタする装置はミラーされたトラフィックのみを受信するように、モニタポートはポートミラーリングのみに使用してください。

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

8.1.8 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

ミラーリンググループのリフレクタポートは設定されていません。

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を番号で指定します。設定範囲は 1～7 です。

interface-type interface-number: ポートをタイプと番号で指定します。

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 コマンドはデフォルトに戻します。

リモート送信元グループにのみリフレクタポートを設定することができます。

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、ポートは工場デフォルト設定に戻ります。リフレクタポートに他の機能を設定することはできません。リフレクタポートで他の機能を設定することはできません。

次の場合 IRF ポートは単一の物理インタフェースにバインドされているため、物理インタフェースをリフレクタポートとして設定しないでください。それ以外の場合は、IRF が分割される可能性があります。

リフレクタポートのデュプレックスモード、通信速度、MDI の設定を変更することはできません。

アグリゲートインタフェースのメンバポートをリフレクタポートとして設定することはできません。

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

8.1.9 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を番号で指定します。設定範囲は 1～7 です。

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 コマンドはデフォルトに戻します。

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にのみリモートプローブ VLAN を設定することができます。

リモートプローブ VLAN として VLAN を設定したとき、ポートミラーリングのリモートプローブ VLAN は専用の VLAN として使用してください。

送信元装置と宛先装置のリモートミラーリンググループは同じリモートプローブ VLAN を使用してください。

既存のスタティック VLAN のみがリモートプローブ VLAN として設定することができます。リモートプローブ VLAN として設定された VLAN は 1 つのミラーリンググループでのみ使用できます。

リモートプローブ VLAN として設定された VLAN を削除する場合、最初にリモートプローブ VLAN の設定を削除してください。

例

リモート送信元グループ 1 を作成し、リモートプローブ VLAN として VLAN 10 を設定します。

<Switch> system-view

[Switch] mirroring-group 1 remote-source

[Switch] mirroring-group 1 remote-probe vlan 10

リモート宛先グループ 2 を作成し、リモートプローブ VLAN として VLAN 20 を設定します。

<Switch> system-view

[Switch] mirroring-group 2 remote-destination

[Switch] mirroring-group 2 remote-probe vlan 20

関連コマンド

mirroring-group

目次

このセクションのページは **10-x-x** です。

9 章 トラフィックミラーリング 9-1
9.1 トラフィックミラーリング設定コマンド.....9-1
9.1.1 mirror-to interface 9-1

9章 トラフィックミラーリング

9.1 トラフィックミラーリング設定コマンド

9.1.1 mirror-to interface

Syntax

mirror-to interface *interface-type interface-number*

undo mirror-to interface *interface-type interface-number*

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

mirror-to interface コマンドはインタフェース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。

undo mirror-to interface コマンドは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削除します。

トラフィックミラーリングが有効になるのは、QoS ポリシーが入力方向に適用されている場合だけです。トラフィック動作に対して **mirror-to interface** *interface-type interface-numbe*r コマンドを複数回実行すると、最新の設定が有効になります。

例

トラフィック動作 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 **10-x-x** です。

10 章 sFlow 10-1
10.1 sFlow 設定コマンド 10-1
10.1.1 display sflow 10-1
10.1.2 sflow agent 10-3
10.1.3 sflow collector 10-4
10.1.4 sflow counter collector 10-5
10.1.5 sflow counter interval 10-6
10.1.6 sflow flow collector 10-6
10.1.7 sflow flow max-header 10-7
10.1.8 sflow sampling-mode 10-8
10.1.9 sflow sampling-rate 10-9
10.1.10 sflow source 10-10

10章 sFlow

10.1 sFlow設定コマンド

10.1.1 display sflow

Syntax

display sflow

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display sflow コマンドは sFlow の設定と動作の情報を表示します。

例

sFlow の設定と動作の情報を表示します。

<Switch> display sflow

```
sFlow datagram version: 5
Global information:
Agent IP: 10.10.10.1(CLI)
Source address: 10.0.0.1 2001::1
Collector information:
ID    IP            Port  Aging     Size VPN-instance Description
1     22:2:20::10    6535  N/A       1400            netserver
2     192.168.3.5    6543  500       1400            Office
Port counter sampling information:
Interface   Instance   CID   Interval(s)
GE1/0/1     2          2     100
GE1/0/1     1          1     200
Port flow sampling information:
Interface   Instance   FID   MaxHLen Rate      Mode     Status
GE1/0/1     2          2     128     1000      Random   Active
GE1/0/1     1          1     128     1000      Random   Active
```

表 10-1 コマンド出力

フィールド	説明
sFlow datagram version	sFlowバージョンです。5のみ適用できます。装置はsFlowバージョンが5であるsFlowパケットだけを送ることができます。
Global information	グローバルのsFlowの情報です。
Agent IP	sFlowエージェントのIPアドレスです。 ● **CLI**—手動で設定されたIPアドレスです。 ● **Auto**—自動で設定されたIPアドレスです。
Source address	sFlowパケットの送信元IPアドレスです。
Collector information	sFlowコレクタの情報です。
ID	sFlowコレクタのIDです。
IP	sFlowコレクタのIPアドレスです。
Port	sFlowコレクタのポートです。
Aging	sFlowコレクタの残りのライフタイムです。**N/A**と表示されている場合、sFlowコレクタはエージアウトしません。
Size	sFlowパケットのsFlowデータ部の最大長です。
VPN-instance	sFlowコレクタに結合されたVPNの名前です。 QX-S5300Gシリーズではこのフィールドをサポートしていません。
Description	sFlowコレクタの説明です。
Port counter sampling information	カウンタサンプリングで設定されたインタフェースの情報です。
Port flow sampling information	フローサンプリングで設定されたインタフェースの情報です。
Interface	sFlowが設定されたインタフェースです。
Instance	カウンタまたはフローサンプリングパケットを送信するためのsFlowインスタンスのIDです。 QX-S5300Gシリーズではこのフィールドをサポートしていません。
CID	カウンタサンプリングのパケットを受信するsFlowコレクタのIDです。sFlowコレクタのIDが指定されていない場合、**0**と表示されます。
Interval(s)	カウンタサンプリングの間隔です。単位は秒です。

フィールド	説明
FID	フローサンプリングのパケットを受信するsFlowコレクタのIDです。sFlowコレクタのIDが指定されていない場合、**0**と表示されます。
MaxHLen	サンプリングパケットでコピーされるバイトの最大数です。（パケットヘッダから開始します）
Rate	フローサンプリングを使用してインタフェースがパケットをサンプリングするパケット数です。
Mode	フローサンプリングモードです。
Status	ポートのsFlowの状態です。 • **Suspended**—ポートがダウンしているため、sFlow機能が中断しています。 • **Active**—ポートがアップしているため、sFlow機能がアクティブです。

10.1.2 sflow agent

Syntax

sflow agent { **ip** *ipv4-address* | **ipv6** *ipv6-address* }

undo sflow agent { **ip** | **ipv6** }

デフォルト

sFlow エージェントの IP アドレスは設定されていません。装置は定期的に sFlow エージェントの IP アドレスがあるかどうかを確認します。ない場合、装置は自動で sFlow エージェントの IPv4 アドレスを選択します。選択された IPv4 アドレスは設定ファイルに保存されません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address:* sFlow エージェントの IPv4 アドレスを設定します。

ipv6 *ipv6-address*: sFlow エージェントの IPv6 アドレスを設定します。

説明

sflow agent コマンドは sFlow エージェントの IP アドレスを設定します。

undo sflow agent コマンドはデフォルトに戻します。

sFlow エージェントの IP アドレスを手動で設定することを推奨します。

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

sFlow エージェントの IP アドレスを 10.10.10.1 に設定します。

<Switch> system-view

[Switch] sflow agent ip 10.10.10.1

10.1.3 sflow collector

Syntax

sflow collector *collector-id* { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**datagram-size** *size*] [**time-out** *seconds*] [**description** *string*]

undo sflow collector *collector-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

collector-id: sFlow コレクタの ID を指定します。設定範囲は 1～10 です。

ip *ipv4-address*: sFlow コレクタの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: sFlow コレクタの IPv6 アドレスを指定します。

port *port-number*: sFlow コレクタのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 6343 です。

datagram-size *size*: sFlow パケットの sFlow データ部の最大長を指定します。設定範囲は 200～3000 バイトです。デフォルトは 1400 バイトです。

time-out *seconds*: sFlow コレクタのエージングタイマを指定します。設定範囲は 1～2147483647 秒です。エージングタイマが終了したとき、sFlow コレクタは削除されます。デフォルトで sFlow コレクタはエージアウトしません。

description *string*: sFlow コレクタの説明を指定します。設定範囲は 1～127 文字です。大文字と小文字が区別されます。デフォルトは CLI Collector.です。

説明

sflow collector コマンドは sFlow コレクタのパラメータを設定します。

undo sflow collector コマンドは sFlow コレクタを削除します。

例

sFlow コレクタ 2 のパラメータを以下のように設定します。

- **IP address**ー3.3.3.1
- **Port number**ーデフォルト
- **Description**ーネットサーバ
- **Aging timer**ー1200 秒
- **Maximum length of the sFlow data portion in the sFlow packet**ー1000 バイト

<Switch> system-view

[Switch] sflow collector 2 ip 3.3.3.1 description netserver time-out 1200 datagram-size 1000

10.1.4 sflow counter collector

Syntax

sflow counter collector *collector-id*

undo sflow counter collector

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

collector-id: コレクタを ID で指定します。設定範囲は 1～10 です。

説明

sflow counter collector コマンドはカウンタサンプリングの sFlow コレクタを指定します。

undo sflow counter collector コマンドはデフォルトに戻します。

例

カウンタサンプリングに、GigabitEthernet 1/0/1 の sFlow コレクタ 2 を指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow counter collector 2

10.1.5 sflow counter interval

Syntax

sflow counter interval *interval*

undo sflow counter interval

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: カウンタサンプリングの間隔を指定します。設定範囲は 2～86400 秒です。

説明

sflow counter interval コマンドはカウンタサンプリングを有効にし、カウンタサンプリングの間隔を設定します。

undo sflow counter interval コマンドはカウンタサンプリングを無効にします。

例

GigabitEthernet 1/0/1 でカウンタサンプリングを有効にし、カウンタサンプリングの間隔を 120 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow counter interval 120

10.1.6 sflow flow collector

Syntax

sflow flow collector *collector-id*

undo sflow flow collector

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

collector-id: sFlow コレクタの ID を指定します。設定範囲は 1～10 です。

説明

sflow flow collector コマンドはフローサンプリングの sFlow コレクタを指定します。

undo sflow flow collector コマンドはデフォルトに戻します。

例

#フローサンプリングに GigabitEthernet 1/0/1 の sFlow コレクタ 2 を指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow flow collector 2

10.1.7 sflow flow max-header

Syntax

sflow flow max-header *length*

undo sflow flow max-header

デフォルト

128 バイト

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

length: コピーできるパケットの最大バイト長を指定します。設定範囲は 18～512 バイトです。デフォルトで使用することを推奨します。

説明

sflow flow max-header コマンドはフローサンプリングでコピーできるパケットの最大バイト長を設定します。（パケットヘッダから開始します。）

undo sflow flow max-header コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 でコピーできるパケットの最大長を 60 バイトに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow flow max-header 60

10.1.8 sflow sampling-mode

Syntax

sflow sampling-mode random

undo sflow sampling-mode

デフォルト

random

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

random: ランダムサンプリングモードを指定します。たとえば、パケットサンプリング間隔が 4000(**sflow sampling-rate** コマンドを使用)に設定されている場合、装置は以下のようにランダムにパケットをサンプリングします。

- 装置は、最初の 4000 から 1 個のパケットをサンプリングします。
- 装置は、次の 4000 パケットから複数のパケットをサンプリングします。
- 装置は、3 番目の 4000 パケットからサンプリングしません。

装置は平均で 4000 パケット毎に 1 個のパケットをサンプリングします。

説明

sflow sampling-mode コマンドはサンプリングモードを指定します。

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

例

GigabitEthernet 1/0/1 でサンプリングモードを random に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow sampling-mode random

関連コマンド

sflow sampling-rate

10.1.9 sflow sampling-rate

Syntax

sflow sampling-rate *rate*

undo sflow sampling-rate

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

rate: インタフェースでパケットをサンプリングするパケットの数を指定します。設定範囲は 1000～500000 です。ベストプラクティスとして、サンプリング間隔を 8192 以上の 2^n、たとえば 32768 に設定します。

説明

sflow sampling-rate コマンドはフローサンプリングを有効にし、インタフェースでパケットをサンプリングするパケットの数を指定します。

undo sflow sampling-rate コマンドはフローサンプリングを無効にします。

例

フローサンプリングを有効にし、GigabitEthernet 1/0/1 でパケットをサンプリングするパケットの数を 32768 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow sampling-rate 32768

関連コマンド

sflow sampling-mode

10.1.10 sflow source

Syntax

sflow source { **ip** *ipv4-address* | **ipv6** *ipv6-address* } *

undo sflow source { **ip** | **ipv6** } *

デフォルト

sFlow パケットの送信元 IP アドレスはルーティングによって決定します。

View

System view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: sFlow パケットの送信元 IPv4 アドレスを指定します。

ipv6 *ipv6-address*: sFlow パケットの送信元 IPv6 アドレスを指定します。

説明

sflow source コマンドは sFlow パケットの送信元 IP アドレスを指定します。

undo sflow source コマンドはデフォルトに戻します。

例

sFlow パケットの送信元 IPv4 アドレスを 10.0.0.1 に設定します。

<Switch> system-view

[Switch] sflow source ip 10.0.0.1

目次

このセクションのページは **10-x-x** です。

11 章 Information Center 11-1
11.1 Information Center 設定コマンド 11-1
11.1.1 display info-center 11-1
11.1.2 display logbuffer 11-2
11.1.3 display logbuffer summary 11-4
11.1.4 display logfile summary 11-5
11.1.5 enable log updown 11-6
11.1.6 info-center enable 11-6
11.1.7 info-center logbuffer 11-7
11.1.8 info-center logbuffer size 11-8
11.1.9 info-center logfile directory 11-9
11.1.10 info-center logfile enable 11-9
11.1.11 info-center logfile frequency 11-10
11.1.12 info-center logfile size-quota 11-11
11.1.13 info-center loghost 11-12
11.1.14 info-center loghost source 11-13
11.1.15 info-center source 11-14
11.1.16 info-center synchronous 11-16
11.1.17 info-center syslog min-age 11-17
11.1.18 info-center timestamp 11-18
11.1.19 info-center timestamp loghost 11-19
11.1.20 logfile save 11-20
11.1.21 reset logbuffer 11-21
11.1.22 snmp-agent trap enable syslog 11-22
11.1.23 terminal debugging 11-23
11.1.24 terminal logging level 11-24
11.1.25 terminal monitor 11-25

11章 Information Center

11.1 Information Center設定コマンド

11.1.1 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,
   port number: 5000, host facility: local7
Log buffer: Enabled
   Max buffer size 1024, current buffer size 512,
   Current messages 0, dropped messages 0, overwritten messages 0
Log file: Enabled
Security log file: Enabled
Information timestamp format:
   Log host: Date
   Other output destination: Date
```

11.1.2 display logbuffer

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 11-1 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、システムの権限が終了しました。	**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**が実行されました。	**informational**
7	Debugging	デバッグメッセージです。	**debugging**

size *buffersize*: 表示される最新のログメッセージの数を指定します。設定範囲は 1～1024 です。指定しない場合、すべてのログ情報を表示します。

slot *slot-number*: IRF スタックメンバの ID を指定します。指定しない場合、すべてのメンバ装置の情報を表示します。

説明

display logbuffer 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 11-2 コマンド出力

フィールド	説明
Log buffer	ログバッファの状態です。 • **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**

11.1.3 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 11-1 を参照してください。

slot *slot-number*: IRF スタックメンバの ID を指定します。指定しない場合、すべてのメンバ装置の情報を表示します。

説明

display logbuffer summary コマンドはログバッファの概要を表示します。

例

ログバッファの概要を表示します。

<Switch> display logbuffer summary

```
Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
   1     0     0     0     7     0    34    38     0
```

表 11-3 コマンド出力

フィールド	説明
EMERG	emergencyを示します。詳細は表 11-1を参照してください。
ALERT	alertを示します。詳細は表 11-1を参照してください。
CRIT	criticalを示します。詳細は表 11-1を参照してください。
ERROR	errorを示します。詳細は表 11-1を参照してください。
WARN	warningを示します。詳細は表 11-1を参照してください。
NOTIF	notificationを示します。詳細は表 11-1を参照してください。
INFO	informationalを示します。詳細は表 11-1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 11-1を参照してください。

11.1.4 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。

このコマンドは、一般的なログファイル設定のみを表示します。

例

ログファイルの設定を表示します。

<Switch> display logfile summary

```
Log file: Enabled.
Log file size quota: 10 MB
Log file directory: flash:/logfile
Writing frequency: 24 hour 0 min 10 sec
```

表 11-4 コマンド出力

フィールド	説明
Log file	ログファイルの状態です。 • **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。

11.1.5 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

11.1.6 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.
```

11.1.7 info-center logbuffer

Syntax

info-center logbuffer

undo info-center logbuffer

デフォルト

ログバッファにログを出力します。

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を出力するように設定します。

undo info-center logbuffer コマンドはログバッファにログを出力することを無効にします。

例

ログバッファにログ情報を出力するように設定します。

<Switch> system-view

[Switch] info-center logbuffer

関連コマンド

- **display logbuffer**
- **info-center enable**

11.1.8 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。デフォルトは 512 です。

説明

info-center logbuffer size コマンドはログバッファに記憶できるログの最大数を設定します。

undo info-center logbuffer size コマンドはデフォルトに戻します。

例

ログバッファに記憶できるログサイズを 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**

11.1.9 info-center logfile directory

Syntax

info-center logfile directory *dir-name*

デフォルト

ログファイルディレクトリは **flash:/logfile** です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dir-name: ディレクトリ名を指定します。設定範囲は 1～64 文字です。

説明

info-center logfile directory コマンドはログファイルを保存するディレクトリを指定します。

指定したログファイルディレクトリが作成されている必要があります。

ログファイルでは log 拡張子を付けます。

このコマンドは、IRF の再起動またはマスタ/下位スイッチオーバーには耐えられません。

例

ログファイルディレクトリを **flash:/test** に設定します。

<Switch> mkdir test

```
Creating directory flash:/test... Done.
```

<Switch> system-view

[Switch] info-center logfile directory flash:/test

関連コマンド

info-center logfile enable

11.1.10 info-center logfile enable

Syntax

info-center logfile enable

undo info-center logfile enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center logfile enable コマンドはログファイル機能を有効にします。

undo info-center logfile enable コマンドはログファイル機能を無効にします。

例

ログファイルにログを出力することを有効にします。

<Switch> system-view

[Switch] info-center logfile enable

11.1.11 info-center logfile frequency

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

デフォルト

86400 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

freq-sec: ログファイルにシステムがログを保存する間隔を指定します。設定範囲は 1～86400 秒です。

説明

info-center logfile frequency コマンドはログファイルにログを保存する間隔を設定します。

undo info-center logfile frequency コマンドはデフォルトに戻します。

このコマンドはシステムが、指定した間隔でログファイルバッファのログをログファイルに自動的に保存することを有効にします。デフォルトでは、このコマンドを使用することを推奨します。

例

ログファイルにログを保存する間隔を 60000 秒に設定します。

<Switch> system-view

[Switch] info-center logfile frequency 60000

関連コマンド

info-center logfile enable

11.1.12 info-center logfile size-quota

Syntax

info-center logfile size-quota *size*

undo info-center logfile size-quota

デフォルト

10 MB

View

System view

定義済みユーザロール

network-admin

パラメータ

size: ログファイルの最大サイズを指定します。単位は MB です。設定範囲は 1～10 です。

説明

info-center logfile size-quota コマンドはログファイルの最大サイズを設定します。

undo info-center logfile size-quota コマンドはデフォルトに戻します。

例

ログファイルの最大サイズを 6MB に設定します。

<Switch> system-view

[Switch] info-center logfile size-quota 6

関連コマンド

info-center logfile enable

⚠ **注意:**

このコマンドを使用する前に、ストレージにログファイルサイズに対して十分なスペースがあるかどうかを確認してください。

11.1.13 info-center loghost

Syntax

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

undo info-center loghost { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

hostname: ログホストの名前を指定します。設定範囲は 1～253 文字の文字列です。大文字と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（.）などの特殊文字を含めることができます。

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。

dscp *dscp-value*: ログホストに送信されるログパケットの DSCP を指定します。設定範囲は 0～63 です。デフォルトは 0 です。パケットの DSCP 値はパケットの優先順位を定

義し、パケットの送信優先順位に影響します。DSCP 値が大きいほど優先順位が高くなります。

facility *local-number*: ログホストのロギング facility を指定します。設定範囲は local0～local7 です。デフォルトは local7 です。ロギング facility は異なるロギングの送信元、query、ログのフィルタリングを識別するために使用します。

説明

info-center loghost コマンドはログホストを指定し、出力パラメータを設定します。

undo info-center loghost コマンドはログホストを削除します。

info-center loghost コマンドは、**info-center enable** コマンドで information center を有効にした後、適用されます。

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

11.1.14 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

11.1.15 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 11-5 にデフォルトのログ出力ルールを示します。

表 11-5 デフォルト出力ルール

宛先	送信元モジュール	共通ログ	セキュリティログ	Diagnostic ログ	Hidden ログ
コンソール	サポートされるすべてのモジュールです。	debugging	無効	無効	無効
モニタ端末	サポートされるすべてのモジュールです。	debugging	無効	無効	無効
ログホスト	サポートされるすべてのモジュールです。	informational	無効	無効	informational
ログバッファ	サポートされるすべてのモジュールです。	informational	無効	無効	informational

宛先	送信元モジュール	共通ログ	セキュリティログ	Diagnostic ログ	Hidden ログ
ログファイル	サポートされるすべてのモジュールです。	informational	無効	無効	informational
セキュリティログファイル	サポートされるすべてのモジュール、フィルタすることはできません。	無効	debugging、フィルタすることはできません。	無効	無効
Diagnosticログファイル	サポートされるすべてのモジュール、フィルタすることはできません。	無効	無効	debugging、フィルタすることはできません。	無効

View

System view

定義済みユーザロール

network-admin

パラメータ

module-name: モジュール名を指定します。装置でサポートされているモジュールを表示する場合、**info-center source ?**コマンドを使用します。

default: サポートされている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。設定範囲は 0～7 です。severity レベルの値が小さいほど、severity レベルは高くなります。詳細は表 11-1 を参照してください。指定した severity レベル以上のログの出力を許可または拒否します。

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、モジュールはデフォルトの出力ルールを使用するか **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。

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、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。

デフォルトモジュール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

コンソールに emergency の severity レベルで 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

11.1.16 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。

システムログ出力は、以前に入力したコマンドを隠すなど、進行中の設定操作を中断します。同期情報出力には、隠されたコマンドが表示されます。また、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]”の文字列を表示し停止した場所から操作を続行できます。

例

情報の同期出力を有効にし、装置の現在の設定を表示する **display current-configuration** コマンドを行います。

<Switch> system-view

[Switch] info-center synchronous

```
Info-center synchronous output is on
```

[Switch] display current-

このとき、システムがログ情報を受信します。最初にログ情報を表示し、次に直前に入力したコマンドを表示します。この例では、**display current-**です。

```
%May 21 14:33:19:425 2007 Switch SHELL/4/LOGIN: VTY login from 192.168.1.44
```

[Switch] display current-

display current-configuration コマンドを完全に入力し、**Enter** キーを押下し、コマンドを実行します。

情報の同期出力を有効にし、現在の設定を保存します。（対話モードでインタラクティブの情報を入力します）

<Switch> system-view

[Switch] info-center synchronous

```
Info-center synchronous output is on
```

[Switch] save

```
The current configuration will be written to the device. Are you sure? [Y/N]:
```

このとき、システムがログ情報を受信します。最初にログ情報を表示し、次に“[Y/N]”を表示します。

```
%May 21 14:33:19:425 2007 Switch SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

入力を完了するため、“**Y**”あるいは“**N**”を入力します。

11.1.17 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時間で設定します。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ファイルに保存する最小保存期間を設定します。

undo info-center syslog min-age コマンドは設定をデフォルトに戻します。

例

ログ最小保存期間を 168 時間と設定します。

<Switch> system-view

[Switch] info-center syslog min-age 168

11.1.18 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

11.1.19 info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** | **iso** | **no-year-date** | **none** }

undo info-center timestamp loghost

デフォルト

date

View

System view

定義済みユーザロール

network-admin

パラメータ

date:タイムスタンプフォーマットを MMM DD hh:mm:ss YYYY に設定します。たとえば、Dec 8 10:12:21 2007 です。**date** の時刻は現在のシステム時刻を示します。

iso: iso 8601 タイムスタンプフォーマットを設定します。たとえば、2009-09-21T15:32:55 です。

no-year-date: タイムスタンプフォーマットを、年の情報を含まない現在のシステム日時に設定します。

none: タイムスタンプ情報が提供されないことを示します。

説明

info-center timestamp loghost コマンドはログホストに送信するログ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ログのタイムスタンプフォーマットを **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

11.1.20 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 コマンドは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、このコマンドはログファイルにログが保存されていなくても成功メッセージイベントを表示します。

例

ログファイルバッファからログファイルにログを手動で保存します。

<Switch> logfile save

```
The contents in the log file buffer have been saved to the file
flash:/logfile/logfile.log.
```

関連コマンド

- **info-center logfile enable**
- **info-center logfile directory**

11.1.21 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

11.1.22 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 通知を有効にします。

undo snmp-agent trap enable syslog コマンドはログメッセージの SNMP 通知を無効にします。

このコマンドは、装置が出力するログメッセージごとに SNMP 通知を送信できるようにします。装置は SNMP 通知をカプセル化し、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 通知を正常に送信するため、装置で SNMP の設定を行ってください。SNMP の設定については、オペレーションマニュアルのセクション 10 *システム管理* “*SNMP*”を参照してください。

ログトラップバッファ内のトラップを表示するには、MIB ログトラップバッファに対応します。ログトラップバッファサイズは、**info-center syslog trap buffersize** コマンドを使用して設定できます。

例

ログメッセージの SNMP 通知を有効にします。

<Switch> system-view

[Switch] snmp-agent trap enable syslog

関連コマンド

info-center syslog trap buffersize

11.1.23 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。

現在の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。

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 debugging** コマンドは、次の severity レベルのログの表示のみを有効にします。
  - 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レベル以上の severity レベル

例

現在の端末でデバッグ情報を表示することを有効にします。

<Switch> terminal debugging

```
The current terminal is enabled to display debugging information.
```

関連コマンド

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

11.1.24 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: ログの重大度レベルを指定します。有効な値は、alert、critical、debugging、emergency、error、informational、notification、warning、および 0～7 の数字です。

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 レベルのログが現在の端末に出力されます。

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デバッギングレベルより高いレベルで装置にログを出力するように設定します。

<Switch> terminal logging level 7

11.1.25 terminal monitor

Syntax

terminal monitor

undo terminal monitor

デフォルト

ログの監視はコンソールで有効、モニタ端末で無効です。

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のログの監視を有効にします。

undo terminal monitor コマンドは現在の端末のログの監視を無効にします。

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

現在の端末でログの監視を有効にします。

<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 **10-x-x** です。

12 章 NetMeister 12-1
12.1 Netmeister 設定コマンド 12-1
12.1.1 display netmeister 12-1
12.1.2 netmeister account 12-3
12.1.3 netmeister enable 12-4
12.1.4 netmeister event log enable 12-5
12.1.5 netmeister event syslog enable 12-6
12.1.6 netmeister management ip 12-7
12.1.7 netmeister parent ip 12-8
12.1.8 netmeister proxy 12-9
12.1.9 display netmeister parent-mode statistics 12-11
12.1.10 netmeister mode 12-15
12.1.11 netmeister parent-mode mqtt port 12-16
12.1.12 netmeister parent-mode sitename 12-17
12.1.13 reset netmeister parent-mode statistics 12-18

12章 NetMeister

🕮 メモ：

本機能は Version 7.2.15 を含む以降のソフトウェアから子機モードでの NetMeister への接続をサポートし、Version 7.4.35 を含む以降のソフトウェアから親機モードでの NetMeister への接続をサポートしています。
IRF スタックでの NetMeister 利用は、Version7.4.30 を含む以降のソフトウェアからサポートしています。IRF スタックで利用する場合、MAC アドレスが Master 選定によって変化しないように **irf mac-address persistent always** コマンドを設定してください。また、IRF 分裂によって同一 MAC の装置が複数登録されないように MAD 機能を利用して下さい。

12.1 Netmeister設定コマンド

12.1.1 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 情報を表示します。

例

NetMeisetr 情報を表示します。

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。

```
<Sysname> display netmeister
NetMeister state                             : Enabled
Connection state with NetMeister             : Connected
Account name                                 : nec
Proxy information:
  State                                  : Connected
  URL                                    : http://www.abc.com:80
  Username                               : admin

Parent 1:
  IP address                                 : 192.168.0.254
  Port number                                : 443
  Connection state                           : Connected
Parent 2:
  IP address                                 : 192.168.0.255
  Port number                                : 8443
  Connection state                           : Connected
```

表 12-1 コマンド出力

フィールド	説明
NetMeister state	• **Enabled**—有効 • **Disabled**—無効
Connection state with NetMeister	• **Connected**—接続 • **Disconnected**—切断
Account name	グループIDです。
Proxy information	NetMeisterプロキシサーバとの接続に関する情報です。
IP address	親機のIPアドレスです。
Port number	親機のポート番号です。
Connection state	NetMeister機能による親機への接続状態です。 • **Connected**—接続 • **Disconnected**—切断

フィールド	説明
Parent information	親機器の情報。
Site name	親機が属するサイトの名前。サイト名が設定されていない場合、このフィールドには--. と表示されます。
Interval	親機が登録パケットおよび更新パケットをクラウドプラットフォームに送信する間隔（秒単位）。デバイスが間隔の取得に失敗した場合、このフィールドには--. と表示されます。
MQTT interval	MQTTハートビート間隔（秒単位）。デバイスが間隔の取得に失敗した場合、このフィールドには--. と表示されます。
MQTT status	MQTT接続状態。MQTT接続が確立されていない場合、このフィールドには--. と表示されます。

関連コマンド

- **netmeister account**
- **netmeister enable**
- **netmeister parent ip**

12.1.2 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 を設定します。設定範囲は 2～31 文字の文字列です。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設定します。設定範囲は 41～73 文字の文字列です。

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設定します。設定範囲は 8～31 文字の文字列です。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 コマンドは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。デバイスで指定するユーザー名とパスワードは、親機および NetMeister で設定されているものと同じである必要があります。

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**

12.1.3 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 コマンドは NetMeister 機能を有効にします。

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

- この機能を有効にする前に、子デバイス、親機、および NetMeister で必要な設定を行います。
- この機能を有効にすると、親機関連の設定のみが親機モードで有効になり、子デバイス関連の設定のみが子機モードで有効になります。

例

NetMeister 機能を有効にします。

<Switch> system-view

[Switch] netmeister enable

12.1.4 netmeister event log enable

🕮 **メモ:**

netmeister event log enable コマンドは Version 7.4.48 を含む以降のソフトウェアからサポートしています。本コマンドはバージョンアップで自動的に有効になります。

Syntax

netmeister event log enable

undo netmeister event log enable

View

System-view

デフォルト

有効

定義済みユーザロール

network-admin

説明

netmeister event log enable コマンドは NetMeister 機能が有効な時、端末がアソシエーションフェーズまたは認証フェーズで接続に失敗した際のイベントログを 5 分間隔で NetMeister に通知します。

undo netmeister event log enable コマンドはイベントログの送信を停止します。

netmeister event log enable コマンドは **netmeister enable** が有効な状態でも変更できます。

例

イベントログの送信を停止する。

<system> system-view

[system] undo netmeister event log enable

12.1.5 netmeister event syslog enable

🕮 **メモ:**

netmeister event syslog enable コマンドは Version 7.4.48 を含む以降のソフトウェアからサポートしています。本コマンドはバージョンアップで自動的に有効になります。

Syntax

netmeister event syslog enable

undo netmeister event syslog enable

View

System-view

デフォルト

有効

定義済みユーザロール

network-admin

説明

netmeister event syslog enable コマンドは NetMeister 機能が有効な時、logbuffer に出力されたログを 5 分間隔で NetMeister にイベントログとして通知します。

undo netmeister event syslog enable コマンドは logbuffer に出力されるログを NetMeister にイベントログとして通知する動作を停止します。

netmeister event syslog enable コマンドは **netmeister enable** が有効な状態でも変更できます。

🕮 **メモ:**

netmeister event syslog enable コマンドは logbuffer に出力されたログを通知するため、**info-center source** *module-name* **logbuffer deny** コマンドによって logbuffer への出力をモジュール単位で無効にした場合はイベントログにも通知されなくなります。
Information Center の詳細はセクション 10 *システム管理* の“*Information Center*”を参照してください。

例

logbuffer に出力されたログをイベントログとして通知する動作を停止する。

<system> system-view

[system] undo netmeister event syslog enable

12.1.6 netmeister management ip

Syntax

netmeister management ip *ip-address*

undo netmeister management ip

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister management ip コマンドによって NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを設定します。

undo netmeister management ip コマンドによってデフォルトに戻します。

NetMeister 機能については NetMeister が提供している操作ガイドを参照してください。

例

NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを 10.1.1.10 に設定します。

```
<Sysname> system-view
[Sysname] netmeister management ip 10.1.1.10
```

🕮 **メモ:**

netmeister management ip コマンドは Version7.4.30 を含む以降のソフトウェアからサポートしています。

12.1.7 netmeister parent ip

Syntax

netmeister parent ip *ip-address* [**port** *port-number*]

undo netmeister parent ip *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 *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設定します。設定範囲は 1～65535 です。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 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**

12.1.8 netmeister proxy

🕮 **メモ**：

netmeister proxy コマンドは、**v7.2.23** を含むそれ以降のソフトウェアでサポートされています。

Syntax

netmeister proxy url *url* [**username** *username* **password** { **cipher | simple** } *string*]

undo netmeister proxy

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

url *url*:プロキシサーバの URL を指定します。*http://<domain>:<port>*形式で指定します。大文字と小文字を区別します。設定範囲は 8～128 文字の文字列です。*<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 1～65535 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。設定範囲は 1～31 文字です。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します。設定範囲は 1～31 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ます。設定範囲は 33～73 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 コマンドは、NetMiester 宛の https 通信がルーティングされるプロキシを指定します。

undo netmeister proxy コマンドはプロキシを削除します。

netmeister proxy コマンドを使用すると、装置は NetMeister 宛の https 通信のために指定されたプロキシサーバを利用します。親機への https 通信にはプロキシサーバを使用しません。

undo netmeister proxy を使用して、プロキシサーバの指定を削除します。

netmeister proxy コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister proxy 複数回実行した場合、最新の設定が有効になります。

例

IP アドレス 192.168.1.254 の親機に接続する子機とし、NetMeister にはプロキシサーバ 10.1.1.254 (ポート:8080)を使用するように設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

[Switch] netmeister proxy url http://10.1.1.254:8080

関連コマンド

- **netmeister enable**

- **display netmeister**

12.1.9 display netmeister parent-mode statistics

🕮 **メモ:**

netmeister mode コマンドは Version 7.4.35 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 netmeister parent-mode statistics [**failed**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

failed:親デバイスと NetMeister の間で送信に失敗したメッセージの統計情報を順番に表示します。システムは最大 5 つの最新メッセージを表示できます。このキーワードを指定しない場合、このコマンドは親デバイスと NetMeister 間のすべてのメッセージの統計情報を表示します。

説明

display netmeister parent-mode statistics を使用して、親デバイスと NetMeister の間で送信されるメッセージの統計情報を表示します。

例

#親デバイスと NetMeister 間のメッセージの統計情報を表示します。

<Sysname> display netmeister parent-mode statistics

```
Tasks and registration:
 145 total, 138 succeeded, 7 failed
 7 connection errors, 0 internal errors
MQTT:
 35 total, 34 succeeded, 1 failed
 1 connection errors, 0 internal errors
Alarm:
 10 occurred, 8 succeeded, 2 failed
 7 recovered, 7 succeeded
```

```
Report:
 10 total, 9 succeeded, 1 failed
```

Table 1 コマンド出力

フィールド	説明
Tasks and registration	タスクおよび登録メッセージの統計。
total	メッセージの合計数。
succeeded	正常に処理されたメッセージの数。
failed	処理に失敗したメッセージの数。
connection errors	処理に失敗したすべてのメッセージのうち、接続エラーのメッセージ数。
internal errors	処理に失敗したすべてのメッセージ中の内部エラー・メッセージの数。
MQTT	MQTTメッセージの統計。
Alarm	アラームメッセージの統計情報。
occurred	アラームがトリガーされたときのメッセージ数。
recovered	アラームがクリアされたときのメッセージ数。
Report	定期的に報告されるメッセージの統計。

#親機と NetMeister の間で送信に失敗したメッセージの統計を表示します。

<Sysname> display netmeister parent-mode statistics failed

```
Tasks and registration:
 Count: 1
  Type: register
  HTTP error code:503
  Inner error code:--
  Time: 2021/12/06 14:00
MQTT:
 Count: 1
  Type: subscribe
  HTTP error code:400
  Inner error code:--
  Time: 2021/12/06 15:10
Alarm:
 Count: 1
  Type: cpu
  HTTP error code:400
  Inner error code:--
  Time: 2021/12/06 15:00
Report:
 Count: 1
  Type: report
  HTTP error code:400
  Inner error code:--
```

```
 Time: 2021/12/07 15:00
Count: 2
 Type: report
 HTTP error code:400
 Inner error code:--
 Time: 2021/12/07 15:30
```

Table 2 コマンド出力

フィールド	説明
Tasks and registration	処理に失敗したタスクおよび登録メッセージの統計。
Count	処理に失敗したメッセージのシリアル番号。
Type	タスクおよび登録メッセージのタイプ。次のオプションがあります。 • register:登録メッセージ。 • update:更新メッセージ。 • get task:タスク取得メッセージ。 • update firmware:ファームウェアアップデートのタスク。 • acquire collective information of equipment:デバイスの集合情報を表示するタスク。 • get running config:デバイスの有効な設定を表示するタスク。 • get config:デバイスの実行コンフィギュレーションおよび次回起動用のスタートアップファイルを表示するタスク。 • get device list:デバイスリストを表示するタスク。 • get tab information:ポートおよび VLAN モジュールの有効な設定を表示するタスク。 • execution display command:デバイス情報を表示するタスク。 • set device list:デバイスリストを設定するタスク。 • execution setting command:デバイス情報を設定するタスク。 • apply config:次の起動用にスタートアップファイルを設定するタスク。 • save:次の起動用にスタートアップファイルに設定を保存するタスク。 • reboot:デバイスを再起動するタスク。 • new certificate:新しい証明書を取得するタスク。 • task result:毎回のタスク結果。

フィールド	説明
HTTP error code	HTTPメッセージエラーコード。次のオプションがあります。 • 1000:メッセージの送信に失敗しました。 • 1001:メッセージの送信に成功しましたが、応答がありません。 • 1002:MQTT パケットの内容が無効です。 • 200:正常に接続されましたが、デバイスの内部処理エラーが発生しました。 • 400:要求エラー。 • 401:認証に失敗しました。 • 403:メッセージは禁止されています。 • 404:メッセージは検出されません。 • 405:無効な方法です。 • 406:メッセージが拒否されました。 • 409:メッセージの競合。 • 429:要求が多すぎます。 • 500:サーバエラー。 • 502:ゲートウェイが正しくありません。 • 503:サービスは使用できません。
Inner error code	デバイス内部メッセージのエラーコード。次のオプションがあります。 • 1000:メッセージの送信に失敗しました。 • 1001:メッセージの送信に成功しましたが、応答がありません。 • 1002:MQTT パケットの内容が無効です。 • 1003:クライアント内部エラー。 • 1004:サービスエンドポイントから返された認識できないエラーコードなどの不明なクライアントエラー。
Time	メッセージが生成された時刻。
MQTT	処理に失敗したMQTTメッセージの統計。
Type	MQTTイベントタイプ。次のオプションがあります。 • subscribe:サブスクリプションイベント。 • unsubscribe:サブスクリプション解除イベント。 • publish:発行イベント。 • keepalive:ハートビートイベント。 • Connect:接続イベント。 • Disconnect:切断イベント。
Alarm	処理に失敗したアラームメッセージの統計。

フィールド	説明
Type	アラームタイプ。次のオプションがあります。 • cpu:プロセッサ使用率アラーム。 • Fan:ファンアラーム。 • Temperature:温度アラーム。 • memory:メモリ使用率アラーム。 • reboot:例外アラームを再起動します。
Report	処理に失敗した定期的に報告されるメッセージの統計。
Type	報告されるメッセージタイプ。このフィールドには、プロセッサ使用率、温度、メモリ使用率、およびデバイスが5分間隔でクラウドプラットフォームに報告するポートの情報を示すレポートが表示されます。

関連コマンド

reset netmeister parent-mode statistics

12.1.10 netmeister mode

🕮 **メモ:**

netmeister mode コマンドは Version 7.4.35 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

12.1.11 netmeister parent-mode mqtt port

🕮 **メモ:**

netmeister parent-mode mqtt port コマンドは Version 7.4.35 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。

netmeister enable の場合にのみ、このコマンドは有効になります。

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**

12.1.12 netmeister parent-mode sitename

🕮 **メモ:**

netmeister parent-mode sitename コマンドは Version 7.4.35 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

パラメータ

name:拠点名を 2 から 31 文字の文字列で指定します。小文字、数字、およびハイフン(-)のみを使用でき、文字列の先頭または末尾にハイフンを使用することはできません。

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。

親機デバイスの場合、NetMeister を有効にする前に拠点名を指定する必要があります。

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**

12.1.13 reset netmeister parent-mode statistics

🕮 **メモ:**

reset netmeister parent-mode statistics コマンドは Version 7.4.35 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 netmeister parent-mode statistic

View

User view

定義済みユーザロール

network-admin

説明

親デバイスと NetMeister の間のメッセージの統計情報をクリアするには、reset netmeister parent-mode statistics を使用します。

例

#親デバイスと NetMeister 間のメッセージの統計情報をクリアします。

<Sysname>reset netmeister parent-mode statistics

関連コマンド

- **display netmeister parent-mode statistics**