Future X Communications

Management Guide
FXC5210PE/5218PE/5224PE

FXC5210PE
FXC5218PE
FXC5224PE
Management Guide

2017年12月 Ver.1.0

FXC株式会社

FXC5210PE/5218PE/5224PE 本マニュアルについて

- 本マニュアルでは、FXC5210PE/FXC5218PE/FXC5224PE の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末を接続して、CLI（コマンドラインインタフェース）による簡易設定、または Web ブラウザにより設定を行います。
- 本マニュアルは FXC5210PE/FXC5218PE/FXC5224PE に対応したマニュアルとなっています。機能はどの製品も同一ですが、ポート構成の違いにより一部設定項目や設定画面が異なる場合があります。

この度は、お買い上げいただきましてありがとうございます。製品を安全にお使いいただくため、必ず最初にお読みください。

・下記事項は、安全のために必ずお守りください。

● 安全のための注意事項を守る

注意事項をよくお読みください。製品全般の注意事項が記載されています。

● 故障したら使わない

すぐに販売店まで修理をご依頼ください。

● 万一異常が起きたら

・煙が出たら
・異常な音、においがしたら
・内部に水・異物が入ったら
・製品を高所から落としたり、破損したとき

①電源を切る（電源コードを抜く）
②接続ケーブルを抜く
③販売店に修理を依頼する

- 下記の注意事項を守らないと、火災・感電などにより死亡や大けがの原因となります。

● 電源ケーブルや接続ケーブルを傷つけない

- 電源ケーブルを傷つけると火災や感電の原因となります。
- 重いものをのせたり、引っ張ったりしない。
- 加工したり、傷つけたりしない。
- 熱器具の近くに配線したり、加熱したりしない。
- 電源ケーブルを抜くときは、必ずプラグを持って抜く。

● 内部に水や異物を入れない

- 火災や感電の原因となります。
- 万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。

● 内部をむやみに開けない

本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。

● 落雷が発生したらさわらない

感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。

● 油煙、湯気、湿気、ほこりの多い場所には設置しない

本書に記載されている使用条件以外の環境でのご使用は、火災や感電の原因となります。

・下記の注意事項を守らないとけがをしたり周辺の物品に損害を与える原因となります。

● ぬれた手で電源プラグやコネクタに触らない

感電の原因となります。

● 指定された電源コードや接続ケーブルを使う

マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。

● 指定の電圧で使う

マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。

● コンセントや配線器具の定格を超えるような接続はしない

発熱による火災の原因となります。

● 通風孔をふさがない

・通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。

・毛足の長いジュウタンなどの上に直接設置しない。

・布などでくるまない。

● 移動させるときは、電源ケーブルや接続ケーブルを抜く

接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。

はじめに.....1

1 章 コマンドインタフェース.....2

1.1 コマンドラインインタフェースによる設定方法.....2
1.1.1 コンソール接続.....2
1.1.2 Telnet 接続.....3
1.1.3 コマンド上でのヘルプの表示.....4
1.2 コマンドモードによる設定.....9
1.2.1 基本コマンド.....9
1.2.2 config モードコマンド.....14
1.2.3 インタフェース設定コマンド.....66
1.2.4 VLAN 設定コマンド.....101
1.2.5 Show コマンド.....103

2 章 WEB による設定方法.....154

2.1 Telnet/SNMP 管理.....154
2.1.1 Telnet によるマネジメント管理.....154
2.1.2 SNMP によるマネジメント管理.....154
2.2 初期設定.....155
2.2.1 設定方法.....155
2.3 Configuration (各機能の設定).....157
2.3.1 System (システム情報).....157
2.3.2 Power Reduction (消費電力制御機能).....161
2.3.3 Ports(ポートの設定).....162
2.3.4 Security (セキュリティ機能).....165
2.3.5 Aggregation (アグリゲーション).....180
2.3.6 Loop Protection (ループプロテクション).....182
2.3.7 Spanning Tree(スパニングツリー).....183
2.3.8 MVR.....187
2.3.9 IPMC.....188
2.3.10 LLDP.....192
2.3.11 PoE.....193
2.3.12 MAC Table.....198
2.3.13 VLANs.....199
2.3.14 Private VLAN (プライベート VLAN).....202
2.3.15 Voice VLAN.....203
2.3.16 QoS.....205
2.3.17 Mirroring (ミラーリング).....216
2.3.18 sFlow.....217
2.4 Monitor(モニタリング).....218
2.4.1 System.....218

2.4.2 Ports (ポートの情報表示) 220
2.4.3 Security (セキュリティ) 223
2.4.4 LACP 232
2.4.5 Loop Protection (ループプロテクション) 234
2.4.6 Spanning Tree (スパニングツリー) 234
2.4.7 MVR 236
2.4.8 IPMC 237
2.4.9 LLDP 241
2.4.10 PoE 243
2.4.11 MAC Table 244
2.4.12 VLANs 245
2.4.13 sFlow 246
2.5 Diagnostics (診断機能) 247
2.5.1 ping 247
2.5.2 ping6 247
2.5.3 VeriPHY (ケーブル診断) 248
2.6 Maintenance (メンテナンス) 249
2.6.1 Restart (再起動) 249
2.6.2 Factory Defaults (工場出荷時設定) 249
2.6.3 Software (ソフトウェア) 250
2.6.4 Configuration (config ファイルの設定方法) 251

はじめに

この度は、弊社 FXC5210PE/FXC5218PE/FXC5224PE をお買い上げ頂き誠にありがとうございます。
お使いになる前に、本書をよくお読みください。
また、お読みになった後は、後日お役に立つこともありますので必ず保管してください。
本書は、本製品を正しくご利用頂く上で必要な機能説明および操作方法について記述しています。

本機は主な設定は、イーサネットポート経由で PC から WEB ブラウザにておこないますが、基本的な設定については、付属のコンソールケーブルを用いてコンソールポート経由でログインして行うことも可能です。

1 章 コマンドインタフェース

1.1 コマンドラインインタフェースによる設定方法

1.1.1 コンソール接続

コンソールポートへの接続は以下の手順で行います。

接続方法:

本体前面の右側にあるコンソールポートに同梱のコンソールケーブルの片方を接続し、もう片方を PC などの COM ポートに接続します。
その後 PC の COM ポートをターミナルエミュレータで開きます(COM ポート番号は PC で確認してください)。

ターミナルエミュレータは以下の通り設定してください。

ボーレート	115200 Baud
データ	8 Bit
パリティ	なし
ストップビット	1 Bit
フロー制御	なし

(1) コンソールプロンプトでユーザ名とパスワードを入力します。
初期設定のユーザ名は"admin"、パスワードも同じく"admin"となっています。

(2) ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、および統計情報の閲覧を行います。

(3) 終了時には"exit"コマンドを使用しセッションを終了します。

コンソールポートからシステムに接続すると以下のログイン画面を表示します。

```
------------------------------------------------------
Software Version  : FXC52xxPE Ver:
MAC Address       : 00-17-2E-xx-xx-xx
Number of Ports   : xx
Username          : admin
Password          :
Login in progress...
FXC52xxPE
------------------------------------------------------
```

1.1.2 Telnet 接続

Telnet を利用するとネットワーク経由での管理が可能となります。
Telnet を行うには管理端末側と本機側のどちらにも IP アドレスを事前に設定する必要があります。
また、異なるサブネットからアクセスする場合にはデフォルトゲートウェイもあわせて設定する必要があります。

[注意] :
工場出荷時には、本機は下記のアドレスが設定されています。

```
------------------------------------------------------------
IP Configuration:
=================

DHCP Client         : Disabled
IP Address          : 192.168.1.1
IP Mask             : 255.255.255.0
IP Router           : 0.0.0.0
DNS Server          : 0.0.0.0
VLAN ID             : 1
DNS Proxy           : Disabled
------------------------------------------------------------
```

IP アドレスとデフォルトゲートウェイの設定例は、以下のとおりです。

```
------------------------------------------------------------
FXC52xxPE# configure
FXC52xxPE(config)# interface vlan 1
FXC52xxPE(config-if)# ip address 192.168.1.100 255.255.255.0
FXC52xxPE(config-if)# exit
FXC52xxPE(config)# ip default-gateway 192.168.2.254
------------------------------------------------------------
```

本機の IP アドレスを設定した後、以下の手順で Telnet セッションを開始することができます。
(1)リモートホストから Telnet コマンドと本機の IP アドレスを入力します。
(2)ログインすると"FXC52xxPE"(xx は、機器名)と表示されます。
(3)ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び
　統計情報の閲覧を行います。
(4)終了時には"quit"又は"exit"コマンドを使用しセッションを終了します。

【注意】:
Telnet 接続は同時に最大 4 セッションまで可能です。

1.1.3 コマンド上でのヘルプの表示

コマンド上で"help"コマンドを入力することで、現在のコマンドクラスで使用可能なコマンドを、階層が分かれているもの含め全て表示します。
例:

```
------------------------------------------------------------
# help
  Commands available:
  exit              Exit from current mode
  help              Show available commands
  history           Show a list of previously run commands
  logout            Disconnect
  ping              Ping IPv4 address (ICMPv4 echo) packets to other
                    network nodes
  …
  …

  copy config running-config tftp <ip address> WORD Destination
  configuration file name
  copy config tftp running-config <ip address> WORD Source
  configuration file name
  copy firmware tftp running-firmware <ip address> WORD Source
  firmware file name
  firmware swap  Swap between Active and Alternate firmware image.
  terminal configuration length <0-512> Number of lines on screen
   (0 for no pausing)
#
------------------------------------------------------------
```

コマンド上で"?"と入力した場合は、現在のコマンドクラスの第一階層にあるすべてのキーワードが表示されます。
また特定のコマンドのキーワードを表示することもできます。例えば"show ?"、"account ?"と入力すると、"show"、"account"コマンド内で使用できるコマンド一覧が表示されます。
例:

```
------------------------------------------------------------
# ?
  exit              Exit from current mode
  help              Show available commands
  history           Show a list of previously run commands
  logout            Disconnect
  ping              Ping IPv4 address (ICMPv4 echo) packets to other
                    network nodes
  ping6             Ping IPv6 address (ICMPv6 echo) packets to other
                    network nodes
  quit              Quit commands
  reload            Halts and performs a warm restart
  show              Shows information
  calendar          Date and time information
  configure         Enter configuration mode
  copy              Copies from one file to another
  firmware          Firmware swap
  terminal          Set terminal line parameters
#
------------------------------------------------------------
```

1.1.3.1 ユーザアカウント

ユーザのアクセスレベルは、1～3 段階に分かれています。

デフォルト設定では、それぞれのアクセスレベルは以下のとおりです。

1. 管理者向けレベル（レベル 3）:
   すべての機能にアクセス可能であり、デバイスのすべてを管理可能です。

2. 標準ユーザ向けレベル（レベル 2):
   本機のステータスと設定内容の表示、並びに一部のメンテナンスコマンドを実行することができます。

3. ゲスト向けレベル（レベル 1):
   本機のステータスおよび設定内容を表示することのみ可能です。

【注記】: システムメンテナンス（ソフトウェアのアップロード、工場出荷時設定など）を行う場合は、「レベル 3(管理者向けアカウント)」が必要となります。

1.1.3.2 ユーザのアクセスレベルの設定方法

以下に、コマンドによるユーザレベルの設定方法について説明します。

【注記】:
この設定は、レベル 3 の管理者向けアカウントを持ったユーザのみ設定可能です。
初期設定時のユーザ名およびパスワードは"admin"/"admin"です。

1. 本機にログインすると、プロンプトは"#"と表示されます。

   コンソール用のコマンドラインをサポートしているため、"?"と入力すると下記のコマンドが表示されます。

```
------------------------------------------------------------
FXC52xxPE
  exit           Exit from current mode
  help           Show available commands
  history        Show a list of previously run commands
  logout         Disconnect
  ping           ping IPv4 address (ICMPv4 echo) packets to
                 other network nodes
  ping6          ping IPv6 address (ICMPv6 echo) packets to
                 other  network nodes
  quit           Quit commands
  reload         Halts and performs a warm restart
  show           Shows information
  calendar       Date and time information
  configure      Enter configuration mode
  copy           Copies from one file to another
  firmware       Firmware swap
  terminal       Set terminal line parameters
#
------------------------------------------------------------
```

2. 続けて、config モードに移行します。
   configure コマンドを入力すると、以下の画面が表示されます。
   システム設定は、この画面で行います。

```
# configure
(config)#
```

3. 次に、ユーザレベルを設定するには、“(config)#”に続いて、“username”コマンドを使用します。
   “username ?”と入力すると、以下の画面が表示されます。

```
(config)# username ?
  <string>        username
```

4. ユーザ名、パスワード、優先レベルをそれぞれ設定してください。

   ここでは、例としてユーザ名に”guest”、パスワードに“guest”、優先レベルに”1”を入力します。

```
(config)# username guest ?
  <string>     password
(config)# username guest guest ?
  <1-3>        privilege_level
(config)# username guest guest 1 ?
<cr>
```

5. 以上で、アクセスレベルの設定は完了です。

   アクセスレベルの設定が完了後、基本コマンドモードに移動して”logout”または”exit”コマンドにより一旦ログアウトした後、設定したユーザ名とパスワードを使ってログインしてください(この場合、ユーザ名:guest、パスワード:guest)

```
Username: guest
Password:
Login in progress...
>
```

1. 管理者向けレベル（レベル 3）

管理者レベルでは、本機のシステム全般の設定および情報を表示することが可能です。
本機にログインすると、プロンプトは“#”と表示されます。
コンソール用のコマンドラインをサポートしているため、“?”と入力すると下記のコマンドが表示されます。

```
------------------------------------------------------------
FXC52xxPE
  exit        Exit from current mode
  help        Show available commands
  history     Show a list of previously run commands
  logout      Disconnect
  ping        ping IPv4 address (ICMPv4 echo) packets to other
              network nodes
  ping6       ping IPv6 address (ICMPv6 echo) packets to other
              network nodes
  quit        Quit commands
  reload      Halts and performs a warm restart
  show        Shows information
  calendar    Date and time information
  configure   Enter configuration mode
  copy        Copies from one file to another
  firmware    Firmware swap
  terminal    Set terminal line parameters
#
------------------------------------------------------------
```

それぞれの設定方法については、以降の「1.2 コマンドによる設定」を参照して、設定を行ってください。

2. 標準ユーザ向けレベル（レベル 2）

標準ユーザ向けレベルでは、本機のステータスと設定内容の表示、並びに一部のメンテナンスコマンドを実行することができます。

標準ユーザ向けレベルとして設定されたユーザ名とパスワードを使ってログインします。
“>”のプロンプトに続いて“?”を入力すると、以下のコマンドリストが表示されます。

```
------------------------------------------------------------
   > ?
     exit    Exit from current mode
     help          Show available commands
     history       Show a list of previously run commands
     logout        Disconnect
     ping          Ping IPv4 address (ICMPv4 echo) packets to
      other network nodes
     ping6         Ping IPv6 address (ICMPv6 echo) packets to
      other network nodes
     quit          Quit commands
     reload        Halts and performs a warm restart
     show          Shows information
     copy          Copies from one file to another
   >
------------------------------------------------------------
```

それぞれの表示方法については、以降の「1.2 コマンドによる設定」を参照して、設定を行ってください。

3. ゲスト向けレベル（レベル 1）

ゲスト向けレベルのユーザは、本機のステータスおよび設定内容を表示することのみ可能です。

ゲストレベルとして設定されたユーザ名とパスワードを使ってログインします。
“>”のプロンプトに続いて“?”を入力すると、以下のコマンドリストが表示されます。

```
> ?
  exit          Exit from current mode
  help          Show available commands
  history       Show a list of previously run commands
  logout        Disconnect
  quit          Quit commands
  show          Shows information
>
```

ファンクションキー

ここでは、コンソール画面用のファンクションキーについて説明します。

ファンクションキー	概要
Tab	コマンドの最初の一部の文字を入力すると、コマンド名が正しく表示されます。例えば、″his″と入力した後に、″Tab″キーを押すと、コマンド名は“history”と表示されます。
Esc	メッセージ画面を改行したり、コマンドのプロンプト画面に戻ります。
↑	1つ前に入力したコマンドを表示します。
↓	1つ後に入力したコマンドを表示します。
←/→	カーソルを左右に移動します。
Backspace	カーソルの前の文字を削除します。
space キー	show コマンドなどで”-More-“と表示された際にそれ以降の情報を表示します。
?	コマンドリストを表示します。

1.2 コマンドモードによる設定

1.2.1 基本コマンド

username/password に“admin”/“admin”と入力すると、管理者モードに入ります。

“?”と入力すると、以下のとおりコマンドリストが表示されます。

```
------------------------------------------------------------
# ?
  exit              Exit from current mode
  help              Show available commands
  history           Show a list of previously run commands
  logout            Disconnect
  ping              Ping IPv4 address (ICMPv4 echo) packets to other
                    network nodes
  ping6             Ping IPv6 address (ICMPv6 echo) packets to
                    other network nodes
  quit              Quit commands
  reload            Halts and performs a warm restart
  show              Shows information
  calendar          Date and time information
  configure         Enter configuration mode
  copy              Copies from one file to another
  firmware          Firmware swap
  terminal          Set terminal line parameters
#
------------------------------------------------------------
```

1. exit コマンド

現在の操作を終了し、基本コマンド画面からログアウトします。

2. help コマンド

使用可能なコマンドが表示されます。

3. history コマンド

入力したコマンドの履歴が表示されます。

4. logout コマンド

ログアウト用のコマンドです。

5. ping コマンド

通信先に PING を送信し、ネットワーク接続および動作が正常に行われているかどうか確認します。

プロンプト画面で“ping ?”と入力すると、次のように表示されます。

```
------------------------------------------------------------
# ping ?
Syntax       : ping 「-n count」 「-l length]「-i ping interval]ip
-n count     : Number of echo requests to send.(1~60)
-l length    : Send buffer size, and length(2-1452)
-i           : ping interval(0-30)
ip           : IP address(xxx.xxx.xxx.xxx)
------------------------------------------------------------
```

6. ping6 コマンド

別のネットワークにPINGを送信し、IPv6アドレスによるネットワーク接続および動作が正常に行われているかどうか確認します。

プロンプト画面に“ping6 ?”と入力すると、次の画面を表示します。

```
------------------------------------------------------------
# ping6 ?
Syntax       : ping6 「-n count]「-l length]「-i ping interval]ip
-n count     : Number of echo requests to send.(1~60)
-l length    : Send buffer size, and length(2-1452)
-i           : ping interval(0-30)
ip           : IPV6 address For example,fc80::215:c5ff:fe03:4dc7
------------------------------------------------------------
```

7. quit コマンド

コンソール画面の設定を中止する際に使用します。Logout コマンドと同じ機能を持ちます。

8. reload コマンド

本機をリセットする際に使用します。

“reload”と入力し、メッセージが表示された後に″y″を入力すると、数秒以内に本機が再起動します。

```
------------------------------------------------------------
# reload
Are you sure you want to perform a Restart?(Y/N)y
System will reboot in a few seconds
------------------------------------------------------------
```

9. show コマンド

show ?”と入力すると、サブコマンドが表示されます。

```
------------------------------------------------------------
# show ?
  aaa                Show AAA service configuration
  acl                Packet Access Control List
  calendar           Date and time information
  ddmi               Digital Diagnostics Monitoring Interface
  dhcp-relay         DHCP Relay Configuration
  dot1x              802.1x content
  eee                Show eee configuration
  history            History information
  interface          Interface information
  ip                 IP information
  ip-source-guard    IP source guard
  lacp               LACP statistics
  line               TTY line information
  lldp               Show lldp Configuration
  log                Log records
  loopback-detection  Show loopback detection
  mac-address-table   Configuration of the address table
  mac-security       MAC Security Configuration
  management         Management IP filter
  map                Maps priority
  mvr                Show MVR Status
```

```
 ntp                Simple Network Time Protocol configuration
 poe                Power Over Ethernet
 port               Port characteristics
 queue              Priority queue information
 radius-server      RADIUS server information
 running-config     Information on the running configuration
 rate-limit         rate-limits
 rmon               Rmon
 sflow              Sampling flow
 snmp               Simple Network Management Protocol statistis
 spanning-tree      Spanning-tree configuration
 storm-control      Show storm control configuration
 system             System information
 tacacs-server      TACACS server settings
 trunk              Trunk information
 users              Show users configuration
 version            System hardware and software versions
 vlan               Virtual LAN settings
-------------------------------------------------------------
```

1) サブコマンドを使用すると、異なる設定画面を表示します。
help 情報の詳細を表示するには、“show xxxx ?”(xxxx はサブコマンド)と入力すると、以下のプロンプト画面が表示されます。

```
-------------------------------------------------------------
# show port ?
  monitor         Shows the configuration for a mirror port
-------------------------------------------------------------
```

2) ”show port monitor ?”と入力すると、次の help メッセージが表示されます。

```
-------------------------------------------------------------
# show port monitor ?
<cr>
-------------------------------------------------------------
```

3) ”show port monitor”と入力すると、ポートのミラーリングの設定が表示されます。

```
-------------------------------------------------------------
# show port monitor
Mirror Configuration:
=====================
Mirror Port: Disabled
Port  Mode
----   --------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled
CPU   Disabled
-------------------------------------------------------------
```

4) 複数のコンソール画面を表示する場合は、“Esc”キーを入力すると画面が分割されます。
詳細については、「Show コマンド」を参照してください。

10. calendar コマンド

システムの日時を手動で設定します。

```
-------------------------------------------------------------
# calendar set <hour> <minute> <second> <month> <date> <year>
-------------------------------------------------------------
```

11. configure コマンド

コンソール画面をグローバル config モードに変更すると、プロンプトに“(config)#”と表示されます。
このモードでは、管理者は本機のシステム設定を行うことが可能です。
グローバル config モードの設定方法については、次の項で説明します。
“exit”コマンドを使用して、現在設定しているモードを終了します。

12. copy コマンド

このコマンドにより、システムの config ファイルやソフトウェアを TFTP サーバにバックアップしたり、TFTP サーバからシステムの config ファイルをリストアしたり、ソフトウェアの更新を行います。

```
-------------------------------------------------------------
# copy ?
  config     Copies configuration file
  firmware   Copies run-time firmware
-------------------------------------------------------------
```

1) copy config

(1) copy config running-config tftp <ip address> yyy

現在動作している設定を IP”<ip address>”(IPv4、または IPv6 アドレス)の TFTP サーバに、”yyy”というファイル名でバックアップします。設定情報は、テキスト形式で表示されます。

(2) copy config tftp running-config <ip address> yyy

IP”<ip address>”(IPv4、または IPv6 アドレス)の TFTP サーバから“yyy”というテキスト設定ファイルをリストアします。

2) copy firmware

・ copy firmware tftp running-firmware <ip address> yyy

IP”<ip address>”(IPv4、または IPv6 アドレス)の TFTP サーバから“yyy”という動作中のソフトウェアを更新します。

13. firmware コマンド

現在有効になっているファームウェアと代替ファームウェアの切り替えを行います。

```
------------------------------------------------------------
# firmware ?
  swap        Swap between Active and Alternate firmware image.
------------------------------------------------------------
```

14. terminal コマンド

show running-config コマンドでの文字の出力時、一度に何行まで表示するかを設定します。
0、または<1-512>の範囲で設定します。
「0」の場合はコマンド実行後止まることなく最後の行まで文字が表示されます。
<1-512>の範囲で指定した場合、指定した値の行まで一度に文字が表示されます。
一度に表示し切れない場合は"---More---"と表示され、何等かのキーを入力することでそこから先の内容が表示されます。

```
------------------------------------------------------------
# terminal ?
  configuration    Configuration file
# terminal configuration length <0-512>
------------------------------------------------------------
```

1.2.2 config モードコマンド

コンソール画面に“configure”コマンドを入力すると、プロンプトが“(config)#”に切り替わります。
本機の一般的な設定については、このモードで設定を行います。

ポートの設定を行うには、グローバル config モードにて“interface”コマンドを使って設定します。
例えば、“interface ethernet 1/5”は、ポート5、“interface ethernet 1/5、6、10-15”はポート5, 6, 10, 11, 12, 13, 14, 15 の設定を行います。
このコマンドの詳細については、次の項を参照してください。

画面上に“?”と入力すると、以下のサブコマンドが表示されます。

```
---------------------------------------------------------------
(config)#?
 exit               Exit from current mode
 help               Show available commands
 history            Show a list of previously run commands
 logout             Disconnect
 quit               Quit commands
 aaa                AAA Service
 acl                Access Control List Configuration
 aggregation        Set aggregation mode configuration
 arp-inspection     Set ARP Inspection configuration
 default            Restore to factory default setting
 dhcp-relay         Configures DHCP Relay Configuration
 dhcp-snooping      Configures DHCP Snooping Configuration
 dot1x              Configures 802.1x port-based access control
 end                Exit from configure mode
 hostname           Sets system's network name
 interface          Enters privileged interface onfiguration
 ip                 Global IP configuration sub commands
 ip-source-guard    IP Source Guard Configuration
 lldp               LDP setting
 logging            Modifies message logging facilities
 loopback-detection Configures loopback detection
 mac-address-table  Configuration of the address table
 mac-auth-username Mac auth username format
 mac-security       Configuration of mac security
 management         Specifies management IP filter
 mirror             Configuration of mirror
 mvr                Multicast VLAN Registration
 no                 Negates a command or sets its defaults
 ntp                Simple Network Time Protocol configuration
 poe                Power Over Ethernet
 prompt             Sets system's prompt
 qos                Configuration of QoS
 radius-accounting-server     Configures RADIUS Accounting Server
 radius-authentication-server Configures RADIUS Authentication
                              Server
 rmon               Configures RMON function
 sflow              Configures sflow function
 snmp-server        Modifies SNMP server parameters
 spanning-tree      Configures spanning tree parameters
 storm-control      Configures storm control
 tacacs-authentication-server Configures TACACS+ Authentication
                    Server
```

```
  username          Establishes user name authentication
  vlan              Switch Virtual LAN interface
  voice-vlan        Voice VLAN Configuration
-------------------------------------------------------------
```

1. exit コマンド
   現在のオペレーションモードを終了し、前のモードに戻ります。

2. Help コマンド
   使用可能なコマンドをすべて表示します。

3. history コマンド
   入力したコマンドの履歴を表示します。

4. logout コマンド
   コンソール画面からログアウト時に使用します。

5. quit コマンド
   コンソール画面を終了します。logout コマンドと同じ機能です。

6. aaa コマンド
   console/telnet/ssh/web によるログイン時に、本機のユーザの認証方式を設定用に使用します。ローカルスイッチ、RADIUS サーバ、TACACS+サーバ、認証なし(ログイン不可)により認証可能です。

   設定用のコマンドは以下のとおりです。

   1) `aaa authentication login console [local|none|radius|tacacs+]`:
      コンソールへのログインする際の認証方式を設定します。

   2) `aaa authentication login ssh [local|none|radius|tacacs+]`:
      SSH 接続時のユーザによるログイン用の認証方式を設定します。

   3) `aaa authentication login telnet [local|none|radius|tacacs+]`:
      telnet 接続時のユーザによるログイン用の認証方式を設定します。

   4) `aaa authentication login web [local|none|radius|tacacs+]`:
      WEB 接続時のユーザによるログイン時の認証方式を設定します。

      ☞ [local|none|radius|tacacs+]は、認証方式です。
         local : 認証用のローカルユーザのデータ認証
         none : 認証無効かつログイン不可
         radius : 認証用のリモート RADIUS サーバのデータベース認証
         tacacs+ : 認証用のリモート TACACS+サーバのデータベース認証

      “radius”および“tacacs+”の後の“fallback”サブコマンド:
      認証方式が'none'または'local'以外の値に設定されているときに、フォールバック機能を有効にすると、ローカル認証が有効になります。
      認証サーバがない場合は、ローカルユーザのデータベースを認証用に使用します。

RADIUS サーバは、コマンドラインの radius-authentication-server コマンド、あるいは、WEB 用の”AAA”機能で設定します。
TACACS+サーバは、コマンドラインのtacacs-authentication-serverコマンド、あるいは、WEBインタフェースの”AAA”機能で設定します。

7. acl コマンド

本機の ACL(アクセスコントロールリスト)機能の設定を行うためのコマンドです。
ACL 設定を行う場合は、以下の手順に従ってください。

1. フィルタリングルールをまず設定してください。
レイヤ 2～4 のパケット(MAC アドレス、VLAN ID、イーサネットタイプ、IP アドレス、ARP パケット)が含まれます。

【注記】:
1 つのルールに複数のマッチング条件が設定可能です。条件のすべてがこのルールと一致する必要があります。

2. パケットがルールに一致した場合の処理方法(許可/破棄、あるいは他のポートへの伝送、レートリミット、ログ情報)を設定します。

“acl ?”コマンドを入力すると、以下のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# acl ?
  add             Add or modify Access Control Entry(ACE)
  delete          Delete ACE
  rate-limiter          Rate Limiter Configuration
-------------------------------------------------------------
```

1) acl add x

ACE(アクセスコントロールエントリ)の追加/修正を行うことが可能です。
“x”: 「1～256」までの値(ACE のインデックス)。
このコマンドにより、フィルタリングルールの ACL 設定用の画面“(config-ace-x)#”への切り替えが可能です。
この場合の“x”はこのルールのインデックス番号です。
ACL ルールを設定後、“(config-if)#”にてポート設定モードの“acl”コマンドを使って、ACL ルールを接続ポートに適用します。

2) acl delete x

ACE(アクセスコントロールエントリ)を削除します。この場合の“x”は、「1～256」までの範囲の値(ACE のインデックス)です。

3) acl rate-limiter x unit kbps rate y
acl rate-limiter x unit pps rate y

レートリミットを設定します。
単位は kbps(秒単位のキロビット)、あるいは pps(秒単位のパケット)です。
“x”:「1～16」までの値(レートリミットのインデックス)です。
“y”:pps 単位の場合は、「0-3276700」までのレートリミットの値、あるいは kbps 単位の場合は、「0, 100, 200, 300, ..., 1000000」の値となります。

レートリミットは、インデックスの番号により ACE、ポートごとに適用可能です。

1. まず、”acl add x”コマンドを使って、ACL ルール(ACE)を設定します。
   プロンプトは”(config-ace-x)#”と表示されます。

2. ”(config-ace-x)#”プロンプトに“?”と入力すると、以下の画面が表示されます。

```
-------------------------------------------------------------
(config)# acl add 10
(config-ace-10)?
   exit          Exit from current mode
   help          Show available commands
   history       Show  list of previously run commands
   logout        Disconnect
   quit          Quit commands
   action        Specify frames action
   destination-mac       Specify destination mac address
   destination-mac-type  Specify destination mac address type
   frame-type    Select the frame type for this ACE
   logging       Specify the logging operation of the
                 ACE
   mirror        Specify the mirror operation of the ACE
   next_id       Next ACE ID(1-256)
   no            Negates a command or sets its defaults
   policy        Policy ACE keyword
   port          Port list
   port-redirect port copy
   rate-limiter  Specify rule's rate
   shutdown      Specify the shut down operation of the
                 ACE
   source-mac    Specify source mac address
   tagged        Specify tagged/untagged frames tagged
   tag_prio      VLAN tag priority
   vid           Specify vlan id
-------------------------------------------------------------
```

サブコマンドの詳細は、以下のとおりです。

(1) exit:
ACL 設定画面を終了します。

(2) help :
設定可能なコマンドを表示します。

(3) history:
入力したコマンドの履歴のリストを表示します。

(4) logout:
コマンドラインの画面からログアウトします。

(5) quit:
コマンドラインの画面を終了します。

(6) action:
ACL ルールと一致するパケットを設定します。
- action permit : ACE の条件に合致するフレームを送出します。
- action deny : ACE の条件に合致するフレームを破棄します。

(7) destination-mac:

フィルタマッチング用のパケットの L2 宛先 MAC アドレスを指定します。
- destination-mac any: DMAC フィルタは指定しません。
- destination-mac xx-xx-xx-xx-xx-xx: ACE の宛先 MAC フィルタを指定します。

(8) destination-mac-type:

フィルタマッチングするパケットの L2 宛先 MAC アドレスのタイプを指定します。

destination-mac-type any
- 宛先 MAC アドレスのタイプを「any」に設定します。

destination-mac-type broadcast
- 宛先 MAC アドレスのタイプを「broadcast」に設定します。

destination-mac-type multicast
- 宛先 MAC アドレスのタイプを「multicast」に設定します。

destination-mac-type unicast
- 宛先 MAC アドレスのタイプを「unicast」に設定します。

(9) frame-type:

ACE を適用するパケットのフレームタイプを設定します。

```
-------------------------------------------------------
(config-ace-10)# frame-type ?
  any           Define Frame to any
  arp           Define Frame to ARP
  ethernet-type Ethernet Type: 0x600 - 0xFFFF or 'any'
                but excluding
0x800(IPv4)   0x806(ARP) and 0x86DD(IPv6)
  ipv4          Define Frame to IPv4 Frame
-------------------------------------------------------
```

(10) frame-type any

どのフレームもすべてこの ACE と一致します。

(11) frame-type arp

ARP フレームのみ、この ACE を適用します。
【注記】: ARP フレームは、イーサネットタイプの ACE は適用されません。

(12) frame-type ethernet-type

イーサネットタイプのみ、この ACE を適用します。
【注記】: 0x800(IPv4)、0x806(ARP)および 0x86DD(IPv6)は設定できません。

(13) frame-type ipv4

IPv4 フレームのみ、この ACE を適用します。
※IPv4 フレームは、ACE のイーサネットタイプの ACE は適用されません。

【注記】:
それぞれのコマンドにはさらに詳細に設定できるサブコマンドがあります。
コマンドラインにて“?”を入力し、サブコマンドの範囲をご確認ください。

(14) logging:

ACE のログ情報を指定します。ACE と一致するフレームは、syslog に保存されます。

システムのログメモリサイズおよびログ情報の通信速度は制限されますのでご注意ください。“logging”コマンドにより、この機能を有効にします。

(15) mirror:
ACE のミラーリングの動作を指定します。ACE と一致するフレームは宛先ミラーポートにミラーリングを行います。“mirror”コマンドにより、この機能を有効にします。

(16) next_id:
別の ACE 設定に移行します。”x”は「1～256」までのインデックス番号です。

(17) no:
コマンドを無効、またはデフォルト設定を行います。

(18) policy:
ACE 用のポートグループのポリシー番号を設定します。
ポートのポリシー番号は、“(config-if)#”にて設定します。
policy y 0xXX コマンドにより、ビットマスク“0xXX”(0x00~0xFF)のポリシー番号“y”(0～255)を設定します。
ACE には、この範囲内のポリシーID のポートが適用されます。

(19) port:
ACE が適用する入力ポートを設定します。
port w コマンドは、ACE 用の入力ポートのリストを設定可能です。
“w”の書式は、シングルポート、またはポートグループの 1/x, 1/x,y,z, 1/x-y, 1/x-y,z です。

(20) port-redirect:
ACE に一致したフレームは、ここで指定したポート番号に送信されます。
port-redirect disable：この機能を無効にします。
port-redirect w コマンド：ポートのリダイレクト番号を設定します。
シングルポート、ポートグループの“w”の書式は、1/x, 1/x,y,z, 1/x-y, 1/x-y,z です。

(21) rate-limiter:
ACE のレートリミットを指定します。
rate-limiter disable : この機能を無効にします。
rate-limiter x : ACE のレートリミットを指定します。
この場合の“x”は、レートリミットのインデックスです（「1～16」までの値）です。

(22) shutdown:
ACE の動作によるポートのシャットダウンを設定します。
shutdown コマンドにより、機能を有効にします。
フレームが ACE と一致する場合は、入力ポートは無効となります。

(23) source-mac:
ACE を適用するレイヤ 2 のパケットの送信元 MAC アドレスを指定します。
source-mac any:すべての送信元 MAC フィルタ(送信元アドレスはチェックしません)。
source-mac xx-xx-xx-xx-xx-xx:この ACE の MAC フィルタを指定します。
ACE と一致するフレームは、送信元の MAC 値と一致します。

(24) tagged:
802.1Q タグによるフレームの ACE 動作を設定します。
tagged any : すべての値が有効(チェックしない。)

tagged tagged : タグ付きフレームのみ
tagged untagged : タグなしフレームのみ

(25) tag_prio:
ACE が適合するフレームは、このプライオリティが適用されます(CoS 値)。
tag_prio any : タグのプライオリティが指定されていません(タグのプライオリティは照会しません)。
tag_prio x : ACE が適合するフレームは、このプライオリティが適用されます。
この場合、"x"は、タグのプライオリティです(有効範囲:0～7)。

(26) vid:
VLAN ID が一致するフレームに ACE を適用します。
vid any : VLAN の ID フィルタは指定されていません(VLAN ID フィルタのステータスは照会しません)。
vid x : VLAN ID が一致するフレームに ACE を適用します。
この場合の"x"は、VLAN ID です(有効範囲:1～4095)。

8. aggregation コマンド
このコマンドにより、アグリゲーションの hash モードを設定します。
hash 動作の結果に応じて、フレームはアグリゲーション接続ポートを通過します。

1) aggregation destination_mac_address:
宛先 MAC アドレスを使って、フレームの宛先ポートを算出します。

2) aggregation ip_address:
IP アドレスを使って、フレームの宛先ポートを算出します。

3) aggregation source_mac_address:
送信元 MAC アドレスを使って、フレームの宛先ポートを算出します。

4) aggregation tcp/udp_port_number:
TCP/UDP ポート番号を使って、フレームの宛先ポートを算出します。

5) no aggregation:
デフォルト設定値に戻します。

9. arp-inspection コマンド
ARP インスペクションは、ネットワークの ARP パケットを確認するセキュリティ機能です。
ARP キャッシュをポイズニングすることにより、レイヤ 2 ネットワークに接続されているホスト、またはデバイスが攻撃を受けた場合、この機能はそれらの攻撃をブロックするためのものです。
有効な ARP リクエストおよび応答のみスイッチへの通信が可能です。

1) arp-inspection mode
ARP インスペクション機能を有効にします。"no arp-inspection mode"により無効になります。グローバル config モードにてこの機能を有効に設定した後、"(config-if)#"プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

2) arp-inspection translation
ダイナミックエントリからスタティックエントリに変換します。

【注記】:
ダイナミック ARP エントリは、DHCP リクエストから学習します。ARP インスペクションを行う前に、DHCP スヌーピング機能をまず有効にしてください。
それ以外の場合は、ARP インスペクションに対してスタティック ARP エントリを設定してください。

10. default コマンド

工場出荷設定時の値にリストアします。
default : すべての設定を工場出荷時の状態に戻します。
default keep-ip : IP アドレスは保持し、それ以外の設定を工場出荷時の状態に戻します。

11. dhcp-relay コマンド

DHCP リレー機能を設定します。クライアントとサーバが同一のサブネットドメイン上にない場合、DHCP リレーを使って、クライアント/サーバ間で DHCP メッセージの送受信を行います。
DHCP サーバにクライアント DHCP パケットを送信する際、DHCP リレーエージェントは DHCP オプション 82 により、特定の情報を DHCP リクエストパケットに挿入します。また DHCP サーバが DHCP パケットを DHCP クライアントに送信する際、DHCP 応答パケットから特定の情報を取り除きます。
DHCP サーバは、この情報使って、IP アドレス、または他の割り当てられたポリシーを実行します。
特に、オプションは回線 ID(オプション 1)およびリモート ID(オプション 2)を設定することにより動作します。

回線 ID のサブオプションには、リクエストを受けた回線に固有の情報が含まれます。
リモート ID のサブオプションは、回線のリモートホスト側に関連のある情報を伝送するように設計されています。
本機の回線の ID の長さの設定は「4」バイト、書式は"vlan_id","module_id","port_no"です。
"vlan_id"のパラメータは、最初の 2 バイトが「VLAN ID」を表し、3 バイト目は"module_id"(スタッカブルスイッチは「スイッチ ID」を示します(スタンドアロンスイッチは「0」))。
"port_no"のパラメータは、4 バイト目であり、ポート番号を表します。
リモート ID は 6 バイトであり、その値は、DHCP リレーエージェントの MAC アドレスと同じです。

1) dhcp-relay information mode

DHCP のオプション 82 のオペレーションを有効("no dhcp-relay information mode"コマンドを入力した場合は無効となる)にします。
DHCP リレー情報モードのオペレーションを有効にすると、DHCP サーバに送信時にエージェントは特定の情報(オプション 82)を DHCP メッセージに挿入し、DHCP クライアントに伝送時に DHCP メッセージから取り除きます。
DHCP リレーオペレーションモードが有効の場合のみ動作します。
オプション 82 の回線 ID のフォーマットは、"[vlan_id][module_id][port_no]"です。
最初の 4 文字は「VLAN ID」、5 番目と 6 番目の文字は「モジュール ID」、スタッカブルデバイスの場合は「スイッチ ID」(スタンドアロンの場合は「0」)、最後の 2 文字は「ポート番号」を表します。

2) dhcp-relay information policy [drop|keep|replace]

DHCP リレー情報のオプションのポリシーを設定します。
DHCP リレー情報のモードを有効にすると、リレーエージェント情報を含む DHCP メッセージをエージェントが受信した場合に、ポリシーを実行します。
リレー情報が無効な場合は、'Replace'のオプションは無効となります。
"no dhcp-relay information policy"コマンドにより、デフォルト設定に戻します。
有効なポリシーは、以下のとおりです。

- drop : リレー情報を含む DHCP メッセージを受信すると、パッケージは破棄されます。
- Keep : リレー情報を含む DHCP を受信しても、元のリレー情報は保持されます。

・ Replace ：リレー情報を含む DHCP メッセージを受信すると、その情報に置き換えられます。

3) dhcp-relay mode

DHCP リレー機能を有効にします。“no dhcp-relay mode”コマンドにより、この機能を無効にします。
DHCP リレーモードを有効にすると、クライアント/サーバが同じサブネットドメイン内にない場合、エージェントによりその間の DHCP メッセージの送受信を行います。
DHCP ブロードキャストメッセージは、セキュリティ面を考慮してフラッディングされません。

4) dhcp-relay server x.x.x.x

DHCP の IP アドレスを設定します。この場合、“x. x. x. x”は DHCP の IP アドレスです。

5) dhcp-relay statistics clear

DHCP リレーの統計情報が消去されます。

12. dhcp-snooping コマンド

DHCP スヌーピング機能を有効にします。“no dhcp-snooping”コマンドにより、この機能を無効にします。
DHCP スヌーピングを使って、untrusted ポートへの侵入をブロックします。
DHCP クライアント/サーバ間の変換を行う際に、不正な DHCP 応答パケットを挿入して侵入した場合にその侵入をブロックします。
グローバル config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

13. dot1x コマンド

802.1x 機能の基本設定を行います。

“dot1x ?”と入力すると、以下の画面が表示されます。

```
------------------------------------------------------------
(config)# dot1x ?
agetime             Time in seconds between check for activity on
                    successfully authenticated MAC addresses
eapoltimeout        Max EAP request/identity packet
                    retransmissions
guest_vlan          Set enabledness and parameters of Guest VLAN
holdtime            Time in seconds before a MAC-address that
                    failed authentication gets a new authentication
                    chance
mode                Set dot1x enabledness
radius_qos          Set enabledness of RADIUS-assigned QoS
radius_vlan         Set enabledness of RADIUS-assigned VLAN
reauthentication    Set Reauthentication enabledness
reauthperiod        Set the period between reauthentications
------------------------------------------------------------
```

1) dot1x agetime x

エージングタイムの設定に使用します。この場合の”x”は、「10～10000000 秒」の範囲内の値となります。
MAC アドレスを確保するためにポートセキュリティ機能を用いて、以下のモードに適用されます。

・ Single 802.1X
・ Multi 802.1X

・ MAC-Based Auth

NASモジュールは、ポートのセキュリティモジュールを使用してMACアドレスを設定する際、指定した時間内にアクティビティが表示されない場合は、ポートのセキュリティモジュールにより定期的に該当の MAC アドレスのアクティビティを確認し、空きのリソースがないかどうかを確認する必要があります。
このパラメータは、この期間を制御し、値を「10～1000000 秒」の範囲内に設定します。
再認証が有効かつ、ポートが 802.1X ベースモードの場合は、次の再認証時に、ポートに接続されていないサプリカントは取り除かれるため、特に重要ではありません。
ただし再認証が無効な場合にリソースを解放する方法は、エントリがエージングタイムを超えた時のみです。
MAC ベース認証モードのポートの場合は、再認証により、スイッチ/クライアント間で直接通信を行わないため、クライアントがすでに接続済みの状態であるか否かについては検出されません。
リソースを解放するには、エントリをエージする方法のみ有効です。

2) dot1x eapoltimeout x

このコマンドにより、Request Identity EAPOL フレームの再送時間を決定します。
この場合、“x”は、「1～65535 秒」までの値です。MAC ベースのポートに対しても無効です。

3) dot1x guest_vlan

ゲスト VLAN 機能を有効にします。
“no dot1x guest_vlan”コマンドにより、この機能を無効にします。
この機能を有効にすると、個々のポート設定により、ポートのゲスト VLAN への移行が可能かどうか判別されます。
グローバル config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

ゲスト VLAN は特殊な VLAN です。
この VLAN は制限付きのネットワークアクセスです。ネットワーク管理者によって指定されたタイムアウトの後、802.1X-unaware クライアントに設定されます。

このオプションは、以下の EAPOL ベースモードでのみ有効です。
・ Port-based 802.1X
・ Single 802.1X
・ Multi 802.1X

ゲスト VLAN の場合、EAPOL フレームのリンクのモリタリングを行い、それらのフレームを受信した場合、本機はゲスト VLAN からポートを抽出し、ポートのモードに応じてサプリカントの認証を開始します。
EAPOL フレームを受信すると、"allow_if_eapol_seen"が無効な場合は、ポートはゲスト VLAN に戻ることはできません。

(1) dot1x guest_vlan allow_if_eapol_seen

EAPOL のゲスト VLAN を許可します。

(2) dot1x guest_vlan reauth_max x

再認証回数を 1-255 回で設定します。

(3) dot1x guest_vlan vid x

ゲスト VLAN の VLAN ID を設定します。
この場合、“x”は VLAN ID(「1～4095」までの値)です。

4) dot1x holdtime x

802.1x のホールドタイムを設定します。
この場合の“x”は、「10～10000000 秒」までの値となります。
MAC アドレスを取得する場合は、ポートセキュリティ機能を使って、以下のモードに適用します。
・Single 802.1X
・Multi 802.1X
・MAC-Based Auth

クライアントによるアクセスが拒否された場合：
RADIUS サーバによりクライアントへアクセスが拒否されたか、RADIUS サーバによりリクエストがタイムアウト(“AAA”で指定されているタイムアウトに応じて)したかのいずれかです。
クライアントは非認証状態を保持します。ホールドタイムは現在実行中の認証についてはカウントされません。
MAC ベース認証モードでは、ホールドタイム内はクライアントからの新規フレームは無視します。

5) dot1x mode

802.1x 機能を有効にします。“no dot1x mode”コマンドにより無効になります。

6) dot1x radius_qos

グローバル Config モードでは、QoS クラスの機能を RADIUS サーバへ割り当てられるようになります。
“no dot1x radius_qos”コマンドにより、この機能を無効にします。
この機能を有効にすると、前述の設定をされた個々のポートごとに、RADIUS サーバに登録された VLAN がそのポートで有効になっているかどうかを判断します。
無効の場合は、RADIUS サーバに登録された VLAN はすべてのポートで無効になります。
RADIUS に割り当てられた QoS は、スイッチ上で割り当てられ正常に認証されたサプリカントによって集中したトラフィッククラスを制御します。
RADIUS サーバは、この機能を使って特殊な RADIUS 属性が送信できるように設定を行う必要があります。

7) dot1x radius_vlan

グローバル config モードでは、VLAN の機能を RADIUS サーバへ割り当てられるようになります。
“no dot1x radius_vlan”コマンドにより、この機能を無効にします。
この機能を有効にすると、前述の設定をされた個々のポートごとに、RADIUS サーバに登録された VLAN がそのポートで有効になっているかどうかを判断します。
無効の場合は、RADIUS サーバに登録された VLAN はすべてのポートで無効になります。
RADIUS に割り当てられた VLAN は、本機に登録され正常に認証されたサプリカントによって集中したトラフィックのクラスを制御します。
受信したトラフィックはクラス分けされ、RADIUS により割り当てられた VLAN に変換されます。
RADIUS サーバは、この機能を使って特殊な RADIUS 属性が送信できるように設定を行う必要があります。

8) dot1x reauthentication

802.1x 機能の再認証機能を有効にします。
“no dot1x reauthentication”コマンドにより、この機能を無効にします。
この機能が有効な場合は、再認証時間に指定した時間後、正しく認証されたサプリカント/クライアントは再認証されます。
802.1X-enabled ポートの再認証により、本機に新しいデバイスが設定されり、サプリカントが接続されてないかどうかを検出します。

MAC ベースポートの場合は、RADIUS サーバの設定が変更された場合のみ有効です。スイッチ/クライアント間の通信は行われないため、ポート上にクライアントの有無を確認することはできません。

9) dot1x reauthperiod x

接続先のクライアントが再認証された後、再認証時間を秒単位で設定します。これは、再認証が可能な場合のみ有効となります。この場合の"x"は、「1～3600」秒までの値となります。

【注記】:

(1) 802.1x 機能の設定を行う場合は、グローバル config モードにて、"dot1x"コマンドを使用します。
グローバル config モードにてこの機能を有効に設定した後、"(config-if)#"プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

(2) RADIUS サーバを設定を行う場合は、"radius-accounting-server"および"radius-authentication-server"コマンドを使用します。

14. end コマンド

グローバル config モードを終了します。

15. hostname コマンド

ネットワーク上の本機の名前を設定します。この名前は、本機の SNMP エージェント機能のホスト名としても使用します。
ホストネームはテキストベースでアルファベットから記載します。
使用可能な文字は A-Z,a-z,0-9 及び-(ハイフン)です。

16. interface コマンド

インタフェース設定モードの入力に使用します。2 つのサブコマンドがあり、"ethernet"(ポート設定用)と、"vlan"(VLAN グループの特性の設定用)です。

```
-------------------------------------------------------------
(config)# interface ?
  ethernet          Ethernet port
  vlan               Switch Virtual LAN interface
-------------------------------------------------------------
```

ポート設定用コマンド(レートリミットの設定、通信速度の設定など)はすべてインタフェース設定モードに含まれます。VLAN グループの機能(IP アドレスの割り当てなど)の設定は、インタフェース設定モードで設定します。

ポート 5 の設定を行うには、"interface ethernet 1/5"と入力すると、次の画面を表示します。

```
-------------------------------------------------------------
(config)# interface ethernet 1/5
(config-if)#
-------------------------------------------------------------
```

"interface ethernet 1/5,6,10-13"コマンドは、ポート 5, 6, 10, 11, 12, 13 用のインタフェース設定画面を表示します。
インタフェース設定モードのコマンドの詳細については、「ポートインタフェース設定コマンド」を参照してください。

17. ip コマンド

このコマンドは、IP による管理機能の設定に使用します。”ip ?”と入力すると、次の画面を表示します。

```
------------------------------------------------------------
(config)# ip ?
 default-gateway          Specifies the default gateway
 dns                      Set the DNS server address
 dns-proxy                Setthe IP DNS Proxy mode
 ipv6-default-gateway     Specifies the default gateway
 https                    HTTPS server configuration
 igmp                     IGMP snooping
 mld                      MLD snooping
 ssh                      Configure ssh server
------------------------------------------------------------
```

1) ip default-gateway x.x.x.x

本機の IPv4 設定用のデフォルトのゲートウェイを指定します。

”x. x. x. x”: ゲートウェイデバイスの IP アドレスを示します。

2) ip ipv6-default-gateway <IPv6 address>

本機の IPv6 設定用のデフォルトゲートウェイを指定します。

“<IPv6 address>”:ゲートウェイデバイスの IP アドレスです。

3) ip dns x.x.x.x

DNS サーバの IP アドレスの設定用です。

“x. x. x. x”: DNS サーバの IP アドレスを示します。

4) ip dns-proxy

DNS Proxy 機能を有効にします。DNS Proxy を有効にすると、装置に現在設定されているネットワーク上の DNS サーバに DNS リクエストを送信し、ネットワーク上のクライアントデバイスへ DNS リゾルバとして応答します。

“no dns-proxy”コマンドにより、この機能を無効にします。

5) ip https

本機の https サービスを設定します。

“ip https ?”と入力すると、以下のサブコマンドが表示されます。

```
------------------------------------------------------------
(config)# ip https ?
  secure-server          Enable secure HTTP server
  automatic-redirect Automatically redirect web browser to
  HTTPS
------------------------------------------------------------
```

(1) ip https secure-server コマンド

本機の http サービス(https)の SSL 機能を有効にします。”no ip https secure-server”コマンドにより、この機能を無効にします。

(2) ip https automatic-redirect コマンド

HTTPS リダイレクトモードを有効にします。HTTPS が有効な場合のみ設定可能です。

HTTPS モードと自動リダイレクトが共に有効な場合、または無効な場合は、WEB ブラウザは HTTPS モードに自動的にリダイレクトされます。“no ip https automatic-redirect”コマンドにより、この機能を無効にします。

6) ip igmp snooping

本機の IGMP 機能を設定します。“no ip igmp snooping”コマンドを入力した場合、この機能を無効にします。

“ip igmp snooping ?”と入力すると、以下のようにサブコマンドが表示されます。

```
-----------------------------------------------------------
(config)# ip igmp snooping ?
  Vlan           Set Snooping VLAN Configuration
  leave-proxy    Enable Leave Proxy
  proxy          Set the mode of Proxy
  ssm-range      Set SSM (Source-Specific Multicast) Range
  unregflood     Enable unregister flood function
<cr>             Enable Snooping
-----------------------------------------------------------
```

7) ip igmp snooping vlan x

VLAN の IGMP 設定を有効にします。

”x”: 「1～4095」までの値を持つ VLAN ID です。

“ip igmp snooping vlan 10 ?”と入力すると、以下のようにサブコマンドが表示されます。

```
-----------------------------------------------------------
(config)# ip igmp snooping vlan 10 ?
  add            Add the snooping VLAN interface
  compatibility  Set Compatibility
  del            Delete the snooping VLAN interface
  parameter-llqi Set the IPMC Last Listener Query Interval
  parameter-qi   Set Query Interval
  parameter-qri  Set Query Response Interval
  parameter-rv    Set Robustness Variable
  parameter-uri  Set Unsolicited Report Interval
  querier        Set snooping querier mode for VLAN
  state          Set snooping state for VLAN
-----------------------------------------------------------
```

(1) ip igmp snooping vlan x add

新規の MLD VLAN を追加します。特定の MLD VLAN は対応するスタティック VLAN を設定後に動作を開始します。この場合の“x”は「1～4095」までの値をもつ VALN ID です。

(2) ip igmp snooping vlan x compatibility

IGMP オペレーション互換モードを設定します。ネットワーク内のホストおよびルータ上で動作中の IGMP のバージョンに応じて、適切な処理を行うホストやルータによって互換性が維持されます。

設定可能なモードは、「IGMP-Auto」、「Forced IGMPv1」、「Forced IGMPv2」、「Forced IGMPv3」です。デフォルトの互換性の値は「IGMP-Auto」です。

(3) ip igmp snooping vlan x del

IGMP の VLAN を削除します。

この場合の“x”は「1～4095」までの値を持つ VLAN ID です。

(4) ip igmp snooping vlan x parameter-llqi y

IPMC ラストリスナーのクエリーのインターバルを設定します。LLQI(Last Listener Query Interval)は、特定のクエリ内の最大応答コードを算出します。

これは、マルチキャストアドレス、またはソース用の最後のリスナーのデパーチャーを検出します。

IGMP では、このことを LMQI(Last Member Query Interval)と言います。
“x”:「1～4095」までの値を持つ VLAN ID。
”y”:「0～31744」までの 10 秒単位の値。

(5) ip igmp snooping vlan x parameter-qi y

IGMP クエリーのインターバルを設定します。
クエリーのインターバルは、クエリアにより送信された一般クエリーのインターバルです。
”x”:「1～4095」までの値を持つ VLAN ID。
”y”:「1～31744 秒」までの値。

(6) ip igmp snooping vlan x parameter-qri y

IGMP クエリー応答時間を設定します。クエリーレスポンスインターバルは、定期的な最大クエリ応答コードの算出に使用する最大応答遅延です。
“x”:「1～4095」までの値を持つ VLAN ID。
“y”:「0～31744」までの 0.1 秒単位の値。

(7) ip igmp snooping vlan x parameter-rv y

信頼性変数を設定します。信頼性変数により、ネットワークの許容範囲内のパケットロスを許可します。
“x”:「1～4095」までの値を持つ VLAN ID。
“y”:「1～255」までの信頼性変数の値。

(8) ip igmp snooping vlan x parameter-uri y

Unsolicited レポートインターバルを設定します。 Unsolicited レポートインターバルは、ホストのグループのメンバーの初期レポートを反復する間の時間です。
“x”:「1～4095」までの値を持つ VLAN ID。
”y”:「0～31744 秒」。

(9) ip igmp snooping vlan x querier

VLAN の IGMP スヌーピングクエリアを有効にします。
この場合の“x”は「1～4095」までの値を持つ VLAN ID です。
“no ip igmp snooping vlan x querier”コマンドにより、この機能を無効にします。

(10) ip igmp snooping vlan x state

VLAN をスヌーピング状態に設定します。
この場合の“x”は「1～4095」までの値を持つ VLAN ID です。

(11) ip igmp snooping leave-proxy

IGMP Leave Proxy を有効にします。“no ip igmp snooping leave-proxy”コマンドにより、この機能を無効にします。
この機能により、ルータ側への不要な leave メッセージが伝送されるのを回避することが可能です。

(12) ip igmp snooping proxy

IGMP Proxy が有効となります。
“no ip igmp snooping proxy”コマンドにより、この機能を無効にします。この機能により、ルータ側への不要な join/leave メッセージが伝送されるのを回避することが可能です。

(13) ip igmp snooping ssm-range x y

SSM(Source-Specific Multicast)の範囲を設定します。SSM の範囲に応じて、SSM-aware ホストおよびルータは、アドレスの範囲内のグループの SSM サービスモデルを起動することが可能です。
“x”:プレフィックス。
”y”:IGMP SSM 範囲の場合は「4～32」、MLD SSM 範囲の場合は「8～128」です。
例えば、x/y は「232.0.0.0/8」です。

(14) ip igmp snooping unregflood

登録されていない IPMCv4 のトラフィックをフラッディングします。
“no ip igmp snooping unregflood“コマンドにより、この機能を無効にします。
IGMP スヌーピングが有効な場合のみフラッディングは制御されます。
IGMP スヌーピングが無効な場合は、登録されていない IPMCv4 のトラフィックのフラッディングは、この設定にかかわらず常に有効になります。

8) ip mld

本機の MLD を設定します。
“ip mld snooping ?”と入力すると、以下のようにサブコマンドが表示されます。

```
(config)# ip mld snooping ?
  vlan           Set Snooping VLAN Configuration
  leave-proxy    Enable Leave Proxy
  proxy          Set the mode of Proxy
  ssm-range      Set SSM (Source-Specific Multicast) Range
  unregflood     Enable  unregister flood function
  <cr>           Enable Snooping
```

(1) ip mld snooping

本機の MLD 機能を有効にします。
“no ip mld snooping”コマンドにより、この機能を無効にします。

(2) ip mld snooping vlan x

VLAN の MLD 設定を有効にします。
“x”:「1～4095」までの値を持つ VLAN ID です。

“ip mld snooping vlan 10 ?”と入力すると、以下のようにサブコマンドが表示されます。

```
(config)# ip mld snooping vlan 10 ?
  add             Add the snooping VLAN interface
  compatibility   Set Compatibility
  del             Delete the snooping VLAN interface
  parameter-llqi  Set the IPMC Last Listener Query Interval
  parameter-qi    Set Query Interval
  parameter-qri   Set Query Response Interval
  parameter-rv    Set Robustness Variable
  parameter-uri   Set Unsolicited Report Interval
  querier         Set snooping querier mode for VLAN
  state           Set snooping state for VLAN
```

- `ip mld snooping vlan x add`
  新しい MLD の VLAN を追加します。対応するスタティック VLAN を設定すると、特定の MLD の VLAN の設定を行います。この場合の“x”は、「1～4095」までの値を持つ VLAN ID です。

- `ip mld snooping vlan x compatibility`
  MLD operation compatibility モードを設定します。
  ネットワーク内のホストおよびルータ上で動作中の MLD のバージョンに応じて、適切な処理を行うホストやルータによって互換性が維持されます。
  「MLD-Auto」、「Forced MLDv1」、「Forced MLDv2」、「Forced MLDv3」から選択することが可能です。
  デフォルトの互換性の値は「MLD-Auto」です。

- `ip mld snooping vlan x del`
  MLD の VLAN を削除します。
  “x”: 「1～4095」までの値を持つ VLAN ID です。

- `ip mld snooping vlan x parameter-llqi y`
  IPMC Last Listener のクエリーのインターバルを設定します。
  MA は、バージョン 1 の Multicast Listener Done メッセージに応じて送信されたマルチキャストアドレスの特定のクエリー内の最大応答コードを算出するために使用する最大応答遅延です。
  これは、マルチキャストアドレスおよびソースの特定クエリーのメッセージ内の最大応答コードを算出するための最大応答遅延でもあります。
  “x”:「1～4095」までの値を持つ VLAN ID です。
  “y”:「0～31744」までの値(0.1 秒単位)です。

- `ip mld snooping vlan x parameter-qi y`
  クエリーのインターバルを設定します。
  クエリーのインターバルは、クエリアによる一般クエリーの送信間隔です。
  ”x”:「1～4095」までの値を持つ VLAN ID。
  ”y”:「1～31744 秒」。

- `ip mld snooping vlan x parameter-qri y`
  クエリーレスポンスインターバルを設定します。
  クエリーレスポンスインターバルは、一般クエリーの最大応答コードを定期的に算出するために使用する最大応答遅延です。
  “x”:「1～4095」までの値を持つ VLAN ID です。
  “y”:「0～31744」の値(0.1 秒単位)です。

- `ip mld snooping vlan x parameter-rv y`
  信頼性変数を設定します。
  信頼性変数により、ネットワークの許容範囲内のパケットロスを許可します。
  ”x”:「1～4095」までの値を持つ VLAN ID です。
  “y”:信頼性変数(1～255 の値)です。

- `ip mld snooping vlan x parameter-uri y`
  Unsolicited レポートインターバルを設定します。
  Unsolicited レポートインターバルとは、マルチキャストアドレスのメンバーシップに関するホストの初期レポートの繰り返し間隔です。
  “x”:「1～4095」までの値を持つ VLAN ID です。
  ”y”:「0～31744 秒」です。

- `ip mld snooping vlan x querier`
  VLAN の MLD スヌーピングクエリアを有効にします。
  “no ip mld snooping vlan x querier”コマンドにより、この機能を無効にします。
  この場合の“x”は「1～4095」までの値を持つ VLAN ID です。

- `ip mld snooping vlan x state`
  VLAN のスヌーピング状態を設定します。
  この場合の“x”は「1～4095」までの値を持つ VLAN ID です。

- `ip mld snooping leave-proxy`
  MLD Leave Proxy を有効にします。“no ip mld snooping leave-proxy”コマンドにより、この機能を無効にします。
  この機能により、ルータへの不要な leave メッセージの伝送を回避することが可能です。

- `ip mld snooping proxy`
  MLD Proxy を有効にします。“no ip mld snooping proxy”コマンドにより、この機能を無効にします。
  この機能により、ルータへの不要な join/leave メッセージの伝送を回避します。

(3) `ip mld snooping ssm-range x y`
SSM(Source-Specific Multicast)の範囲を設定します。
SSM の範囲により、SSM-aware ホストおよびルータがアドレスレンジ内のグループの SSM サービスモデルを動作することが可能です。
“x”:プレフィックス
”y”:「4～32」までの IGMP SSM レンジを持つマスク。
【注記】:例えば、x/y は「ff3e::/96」となります。

(4) `ip mld snooping unregflood`
未登録の IPMCv6 トラフィックのフラッディングを有効にします。
“no ip mld snooping unregflood“コマンドにより、この機能を無効にします。
MLD スヌーピングが有効な場合のみ、フラッディングの制御を行うことが可能です。
MLD スヌーピングを無効な場合は、未登録の IPMCv6 トラフィックはすべてフラッディングされます。

9) `ip ssh server`
SSH サーバを有効にします。“no ip ssh server”コマンドにより、この機能を無効にします。
SSH はセキュアシェルの略です。2 つのネットワーク機器間でセキュアチャネルを使ってデータの交換を行うネットワークプロトコルです。
SSH による暗号化により、安全性の低いネットワーク上のデータの機密性と安全性を提供します。
SSH は、rlogin、TELNET および rsh プロトコルのリプレースを目的にしており、高度な認証、または機密性については保証されません。

18. ip-source-guard コマンド

IP セキュリティ機能を設定します。IP ソースガードは、DHCP スヌーピングテーブルに応じてトラフィックのフィルタリングを行ったり、手動で IP ソースバインディングを行ったりすることにより、DHCP スヌーピングの信頼性の低いポートの IP トラフィックの制限を行います。
ホストが不正を行ったり、別のホストの IP アドレスを不正に使用しようとする際、IP の攻撃から守ることができます。

【注記】:
Dynamic IP Source は、DHCP リクエストから学習を行います。IP ソースガードを設定する前に、スヌーピング機能をまず有効にしてください。
それ以外は、IP ソースガードに対してスタティック IP エントリを設定する必要があります。

1) ip-source-guard mode

IP ソースガード機能をグローバル config モードにて有効にします。
“no ip-source-guard mode”コマンドにより、この機能を無効にします。
グローバル config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。
指定したポート上でグローバルモードおよびポートモードの両方が有効な場合のみ、IP ソースガードは有効となります。

2) ip-source-guard translation

ダイナミックエントリをすべてスタティックエントリに変換します。

19. lldp コマンド

このコマンドにより、 LLDP 機能をグルーバル設定にて設定します。LLDP は、IEEE802.1AB の標準プロトコルです。この規格で指定されている LLDP(Link Layer Discovery Protocol)により、同じ IEEE802 の LAN に接続された他のステーションを検出し、識別します。

“lldp ?”と入力すると、次のコマンドが表示されます。

```
-------------------------------------------------------------
  (config)# lldp ?
 Interval          Specify transmit interval
 tx-hold           Specify hold time multiplier
 tx-delay          Specify delay interval
 reinit-delay      Specify reinit delay
-------------------------------------------------------------
```

1) lldp interval x

送信間隔を指定します。本機は、LLDP フレームをネイバー装置に定期的に送信し、ネットワーク検出情報を更新します。各 LLDP フレームの間隔は Tx インターバルの値により決定されます。
この場合の“x”は、Tx(送信)の間隔です。有効な値は、「5～32768 秒」までに制限されます。

2) lldp tx-hold x

”hold time multiplier”を指定します。各 LLDP フレームには、LLDP フレームの情報量に関する情報が含まれます。LLDP 情報の有効時間は、Tx Hold(Tx インターバル(秒単位)で増分)に設定されます。
この場合の“x”は、Tx ホールドタイムの乗数です。有効な値は、「2～10 回」までに制限されます。

3) lldp tx-delay x

遅延時間を指定します。設定を変更する場合(IP アドレスなど)は、新しい LLDP フレームを伝送しますが、LLDP フレームの送信間隔は Tx Delay の値(秒単位)になります。この場合の"x"は、Tx(送信)の間隔です。
Tx Delay は、Tx インターバルの値の 1/4 未満です。有効な値は、「1～8192 秒」までに制限されます。

4) lldp reinit-delay x

フレーム送信遅延間隔を指定します。
ポートを無効にすると、LLDP は無効になるか、あるいはスイッチはリブートされ、LLDP シャットダウンフレームがネイバー装置に伝送されるため、LLDP 情報のシグナル表示は無効になります。
送信遅延により、シャットダウンフレームと新規 LLDP 初期化の間の時間(秒単位)を制御します。この場合の"x"は、Tx(送信)遅延の間隔です。有効な値は、「1～10 秒」までに制限されます。
LLDP 機能はポート単位で有効/無効に設定します。伝送された情報もポート単位で設定されます。
グローバル config モードにてこの機能を有効に設定した後、"(config-if)#"プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

20. logging コマンド

本機のログ機能を設定します。
この操作を有効にすると、内部ログを有効にします。

"logging ?"と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
  (config)# logging ?
   log-level              Log level
   remote-log             Enable logging to remote host
   clear                  Clear logging table information
-------------------------------------------------------------
```

1) logging log-level x

イベントのログレベルを設定します。この場合の"x"は、「0～2」の範囲のログ用のレベルの値です。
syslog サーバに送信されたメッセージの種類が表示されます。
0: Info - 情報、警告、エラーを送信します。
1: Warning - 警告およびエラーを送信します。
2: Error - エラーを送信します。

2) logging remote-log

リモートによるログ機能を設定します。"no logging remote-log"コマンドを入力した場合、この機能を無効にします。
ここで設定した IP アドレスの syslog サーバに syslog メッセージが送信されます。
syslog プロトコルは、UDP 通信をベースにしており、UDP ポート「514」で送信されます。

"logging remote-log ?"と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------
  (config)# logging remote-log ?
  <1-1>              Index
  <cr>
-------------------------------------------------------
```

3) logging remote-log x host y.y.y.y
syslog サーバのインデックス x に IP アドレス(y.y.y.y)を設定します。
"x" : syslog サーバのインデックス番号です。1 または 1-*(任意数字列)で設定できますが、登録できるのは 1 台のみです。
"y.y.y.y": syslog サーバの IPv4 ホストアドレスです。

DNS が有効な場合は文字列で入力し、ホスト名とすることができます。

4) logging clear
ログ情報を消去します。"logging clear?"と入力すると、次のサブコマンドが表示されます。

```
(config)# logging clear ?
  <0-2>   Logging level
  <cr>    All
```

5) logging clear x
レベル"x"のログ情報を消去します。この場合の"x"は、「0～2」の範囲のログ用のレベルの値です。
0: Info : 情報、警告、エラーを消去します。
1: Warning : 警告およびエラーを消去します。
2: Error : エラーを消去します。
レベルを指定しない場合は、すべてのログ情報が消去されます。

21. loopback-detection コマンド
グローバル config モードでループバック検知およびプロテクション機能を設定します。ポート上でループが発生すると、ループバック検知およびプロテクション機能によりポートをシャットダウンします。
この機能を有効にすると、ループプロテクション用の PDU フレームが各ポートから送信されます。

"loopback-detection ?"と入力すると、次のサブコマンドが表示されます。

```
(config)# loopback-detection ?
 mode       Set the Loop Protection to be enabled
 shutdown   Set or show the Loop Protection shutdown time
 transmit   Set the Loop Protection transmit interval
```

1) loopback-detection mode
この機能をグローバル config モードにて有効にします。
"no loopback-detection mode"コマンドにより、この機能を無効にします。
グローバル config モードにてこの機能を有効に設定した後、"(config-if)#"プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

2) loopback-detection shutdown x
ループ状態が検出された際ポートが無効な状態(ポートのオペレーションがシャットダウンされている状態)となる時間を秒単位で示します。
この場合の"x"は、シャットダウンされている時間です。有効な値は、「0～604800 秒(7 日間)」、「0」の値は、ポートが無効な状態(次のデバイスが再起動するまでの状態)を示します。

3) loopback-detection transmit x

各ポートのループプロテクションのフレームの送信間隔を設定します。
この場合の“x”は、送信間隔を表し、有効な値は「1～10 秒」です。
ループ検知機能は、ポートごとに設定が必要です。
“(config-if)#”にて設定してください。

22. mac-address-table コマンド

本機の MAC アドレスの機能を設定します。

“mac-address-table ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# mac-address-table ?
  aging-time    Aging time for entries in the address table
  clear         Clears mac address table
  static        Sets MAC address table static information
-------------------------------------------------------------
```

1) mac-address-table aging-time x

本機のエージングタイムを設定します。
”x”の有効な値(秒単位)は「10～1000000 秒」です。

2) mac-address-table aging-time disable

MACアドレスのエージングは無効になります。

3) mac-address-table clear dynamic

ダイナミック MAC アドレステーブルの登録内容を消去します。

4) mac-address-table static x-x-x-x-x-x vlan y interface ethernet 1/z

スタティック MAC アドレス”x-x-x-x-x-x”を VLAN“y”のポート“z”に割り当てます。
スタティック MAC アドレスのエージングアウトは行いません。
スタティック MAC テーブルは「64 エントリ」までです。

23. mac-auth-username コマンド

MAC アドレス認証時、RADIUS サーバへ送信するユーザ名の書式を設定します。

“mac-auth-username ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# mac-auth-username ?
  with-hyphen         include "-" for example xx-xx-xx-xx-xx-xx
  without-hyphen       without "-"  for example, xxxxxxxxxxxx.
-------------------------------------------------------------
```

1) mac-auth-username with-hyphen lower-case

ユーザ名の書式を″-″(ハイフン)付き・小文字(a-f, 0-9)に設定します。

2) mac-auth-username with-hyphen upper-case

ユーザ名の書式を″-″(ハイフン)付き・大文字(A-F, 0-9)に設定します。

3) mac-auth-username without-hyphen lower-case

ユーザ名の書式を″-″(ハイフン)無し・小文字(a-f, 0-9)に設定します。

4) mac-auth-username without-hyphen upper-case
ユーザ名の書式を"-"(ハイフン)無し・大文字(A-F, 0-9)に設定します。

24. mac-security コマンド
ポートセキュリティのリミットコントロールシステムの設定を行うことができます。このリミットコントロールにより、指定したポートのユーザ数を制限することが可能です。ユーザは、MAC アドレスと VLAN ID ごとに識別されます。
リミットコントロールが有効な場合は、ポートのユーザ数の上限を指定します。上限を超えると、4 つの処理(None、Trap、Shutdown、Trap & Shutdown)のいずれかが実行されます。
リミットコントロールのモジュールは、ポートで学習した MAC アドレスを管理するレイヤ 2 モジュール、ポートセキュリティモジュールを対象としています。

"mac-security ?"と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config)# mac-security ?
  aging      Time in seconds between check for activity on learned
             MAC addresses
  mode       Set global enabledness
------------------------------------------------------------
```

1) mac-security aging x
セキュア MAC アドレスのエージングタイムを設定します。他のモジュールによりセキュア MAC アドレスの基本的なポートセキュリティが使用された場合は、エージングタイムへのその他の要求を行います。基本的なポートセキュリティは機能を用いるモジュールすべてが要求するエージングタイムより短くなります。
この場合の"x"は、エージングタイムを表し、「10～10000000 秒」までの値となります。

2) mac-security mode
ポートセキュリティのリミットコントロール機能はグローバル config モードで設定可能です。"no mac-security mode"コマンドにより、この機能を無効にします。ポートセキュリティのリミットコントロール機能はグローバル config モード/ポート単位ともに有効です。
ポートセキュリティのリミットコントロール機能は、ポートごとに設定を行う必要があります。
グローバル config モードにてこの機能を有効に設定した後、"(config-if)#"プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

24. management コマンド
管理インタフェースのセキュリティ機能を設定します。管理セキュリティ機能により、ネットワークから管理用の IP アドレスレンジ/リモート画面(http,telnet,snmp)を制限することが可能です。管理上のセキュリティを確保するために、管理者によって異なる管理用の権限を設定することが出来ます。(この機能は、上限「16」までの設定が可能です。)

1. "management x ?"と入力すると、次のサブコマンドが表示されます(この場合の"x"は「1～16」までのルールのインデックスです)。

```
------------------------------------------------------------
(config)# management ?
<1-16> access id
enable Enable the management security function
clear Clears access management statistics
------------------------------------------------------------
```

例えば、"management 1 ?"と入力すると、以下の画面が表示されます。

```
------------------------------------------------------------
(config)# management 1 ?
ipaddr Set IP and net mask for a specified set
protocol Set protocol for a specified set
------------------------------------------------------------
```

1) management enable

管理セキュリティ機能を有効にします。
この機能を有効にすると、制限ルールの設定に適合する IP アドレス・ネットワークプロトコル以外での接続ができなくなります。
“no management enable“コマンドにより、この機能を無効にします。
【注記】:
ルールを設定せずにこの機能を有効にした場合は、http/https | snmp | telnet/ssh の接続が不可になります。

2) management clear

アクセス管理の統計情報を消去します。

3) management x ipaddr y.y.y.y z.z.z.z

このルールの IP アドレスのレンジを設定します。
“x” : ルールのインデックス
“y.y.y.y” : 開始 IP アドレス
“z.z.z.z” : 終了 IP アドレス
ユーザの IP アドレスは本機の管理ネットワークの範囲内の IP アドレスに準じます。

4) management x protocol [http/https | snmp | telnet/ssh]

ルールのリモート管理ネットワークプロトコルを有効にします。
この場合の“x”は、ルールのインデックスです。
まず、“management x ipaddr y.y.y.y z.z.z.z”コマンドにより、ルールを設定します。
次に、“management x protocol [http/https | snmp | telnet/ssh]”コマンドにより、ルールに適応するネットワークプロトコルを割り当てます。
”no management x”コマンドにより、”x”のインデックスのルールを削除します。

25. mirror コマンド

本機のミラーリング機能を有効にします。
”no mirror”コマンドにより、この機能を無効にします。

26. mvr コマンド

MVR(Multicast VLAN Registration)機能を設定します。
MVR 機能により、VLAN グループごとにトラフィックを分離します。また各 VLAN の加入者の IP マルチキャストトラフィックを分離します。MVR 機能により、1 つのマルチキャスト VLAN が各 VLAN の加入者によって共有することが可能になります。これにより、VLAN のマルチキャストトラフィックを減少させることができます。
MVR 機能により、マルチキャスト VLAN 上のマルチキャストトラフィックの伝送が可能になります。
マルチキャスト VLAN ごとに対応するチャネルをもつ MVR VLAN を最大 8 つまで、チャンネル設定ごとにアドレスは「最大 256 グループ」まで設定可能です。

【注記】:
- MVR 機能を設定する前に、まず VLAN 設定を完了してください。
- MVR 機能を使用する場合は、まず IGMP スヌーピング機能を有効にしてください。

本機では、MVR VLAN を最大 8 つまでサポートしています。これらは、VLAN ID により参照します。
MVR 設定を行う場合は、コマンドで VLAN ID を指定してください。

“mvr ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# mvr ?
  <1-4095>          Create MVR Multicast VLAN and paramters
  Enabled           Enable the Global MVR
-------------------------------------------------------------
```

1) mvr enable

MVR 機能を有効にします。“no mvr enable”コマンドにより、この機能を無効にします。
“mvr x ?”と入力すると、サブコマンドが表示されます（この場合の”x”は、「1～4095」までの VLAN ID です）。

“mvr 10 ?”と入力すると、以下の画面が表示されます。

```
-------------------------------------------------------
(config)# mvr 10 ?
  Llqi     Define the maximun time to wait for IGMP/MLD report
           memberships on a receiver port before  removing the
           port from multicast group membership
  group    Create a multicast group for MVR VLAN
  mode     Specify the MVR mode of operation
  name     MVR Name is an optional attribute to indicate the
           name of the specific MVR VLAN
  priority Specify how the traversed IGMP/MLD control frames
             will be sent in prioritized manner
  status-clear Clear MVR operational status
  tagging  Specify whether the traversed IGMP/MLD control
           frames will be sent as Untagged or Tagged with MVR
           VID
-------------------------------------------------------
```

(1) mvr x llqi y

マルチキャストグループのメンバからポートを削除する前に、受信側のポート上の IGMP/MLD レポートメンバーシップの待機時間の上限を設定します。
LLQI（Last Listener Query Interval）は、特定のクエリ内の最大応答コードを算出するための最大応答時間です。
マルチキャストアドレス、またはソースアドレス用の最後のリスナーの送信時間を検出します。
IGMP の場合は、LMQI（Last Member Query Interval）と言います。
”x”：マルチキャストの VLAN ID。
”y”：「0～31744」までの範囲の値（デフォルト設定の LLQI は「0.5 秒」）。

(2) mvr x group yyy start-address <starting IPv4/IPv6 Multicast Group Address> end-address <ending IPv4/IPv6 Multicast Group Address>

MVR VLAN のマルチキャストグループを設定します。
”x”:マルチキャストの VLAN ID。
”yyy”: 特定のマルチキャスト VLAN のチャネル名。
チャネル名の長さは「32」文字以内です。チャネル名には、英数字のみ設定可能です。また英文字を 1 文字以上入れてください。“no mvr x group”コマンドにより、マルチキャスト VLAN x のチャネルを削除します。この場合の“x”は、マルチキャスト VLAN ID です。
MVR の VLAN を設定すると、IP マルチキャストグループ(ビデオチャネル)を MVR の VLAN に設定することが可能です。また複数のマルチキャストグループ(ビデオチャネル)を 1 つの MVR の VLAN に割り当てることが可能です。
たとえば、“mvr 10 group abc start-address 224.0.0.1 end-address 224.0.0.2”と表示されます。

(3) mvr x mode [compatible | dynamic]

MVR モードを指定します。Dynamic モードでは、MVR によりソースポートのダイナミック MVR メンバーシップレポートを有効にします。
Compatible モードは、ソースポートの MVR メンバーシップのレポートは禁止されます。この場合の“x”は、マルチキャスト VLAN ID です。

(4) mvr x name yyy

VLAN ID にマルチキャスト VLAN の名前を設定します。
”x” :マルチキャスト VLAN ID。
“yyy”: MVR の VLAN 名です。MVR 名は、特定の MVR の VLAN を示すオプションの属性です。
MVR の VLAN 名の長さは「32 文字」以内で設定します。MVR VLAN 名には、英数字のみ設定可能です。また MVR の VLAN 名を設定する場合は、英文字を「1 文字以上」入れてください。
“no mvr x”コマンドで MVR の VLAN を削除します。

(5) mvr x priority y

IGMP / MLD 制御フレームが通過する際の優先順位を指定します。
“x”:マルチキャスト VLAN ID。
“y”:「0～7」までの範囲のプライオリティの値。

(6) mvr x status-clear

MVR の動作状況およびマルチキャスト VLAN の”x”を消去します。この場合の“x”は、マルチキャスト VLAN ID です。

(7) mvr x tagging [tagged | untagged]

IGMP / MLD 制御フレームが通過する際に MVR VID タグ付けあり/なしで送信するかを指定します。
この場合の“x”は、マルチキャスト VLAN ID です。
MVR の VLAN を設定した後、IP マルチキャストのトラフィックのソースポートとマルチキャスト加入者の受信ポートを割り当てます。
グローバル config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。
詳細については「mvr コマンド設定」を参照してください。

27. no コマンド

機能を無効にするか、設定を初期設定値にリストアします。

“no ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config)# no ?
  aaa                 AAA Service
  aggregation         Set aggregation mode configuration
  arp-inspection      Set ARP Inspection configuration
  dhcp-relay          Configures DHCP Relay Configuration
  dhcp-snooping       Configures DHCP Snooping Configuration
  dot1x               Configures 802.1x port-based access control
  hostname            Sets system's network name
  ip                  Global IP configuration sub commands
  ip-source-guard     IP Source Guard Configuration
  lldp                LLDP setting
  logging             Modifies message logging facilities
  loopback-detection        Configures loopback detection
  mac-address-table         Configuration of the address table
  mac-auth-username Mac auth username format
  mac-security        Configuration of mac security
  management          Specifies management IP filter
  mirror              Configuration of mirror
  mvr                 Multicast VLAN Registration
  ntp                 Simple Network Time Protocol configuration
  poe                 Power Over Ethernet
  prompt              Sets system's prompt
  qos                 Configuration of QoS
  radius-accounting-server        Configures login to RADIUS server
  radius-authentication-server    Configures login to RADIUS server
  rmon                Configures RMON function
  sflow               Configures sflow function
  snmp-server         Modifies SNMP server parameters
  spanning-tree       Configures spanning tree parameters
  storm-control       Configures TACACS+ Authentication Server
  tacacs-authentication-server Configures TACACS+ Authentication
                               Server
  username            Sets system's network name
  voice-vlan          Voice VLAN Configuration
------------------------------------------------------------
```

例として、″no mirror″コマンドを入力した場合はミラーリング機能が無効となります。
また、″no ip default-gateway″と入力した場合は、デフォルトゲートウェイの設定が工場出荷時状態に戻ります。

28. ntp コマンド

本機の NTP プロトコルを設定します。

“ntp ?”と入力すると、次のサブコマンドが表示されます。

```
-----------------------------------------------------------------
(config)# ntp ?
  client            Accepts time from specified time server
  server            Specified one time server
  zone              Set time zone
  zone-acronym      Set time zone acronym
  dst               Config daylight saving time function
  dst-start-time    Set start time of daylight saving time
  dst-end-time      Set end time of daylight saving time
  dst-offset        Enter the number of minutes to add during
                    Daylight Saving Time
-----------------------------------------------------------------
```

1) ntp client

NTP プロトコルを有効にします。

″no ntp client″コマンドにより、この機能を無効にします。

2) ntp server x <IP address>

NTP プロトコルの NTP サーバの IP アドレスを設定します。

DNS 機能が有効な場合は、ホスト名を入力することも出来ます。

NTP サーバは最大 5 つまでサポートされています。この場合の“x”は、NTP サーバのインデックス(1～5)です。

<IP address>により、NTP サーバの IPv4、あるいは IPv6 アドレスをサポートしています。

3) ntp zone x

タイムゾーンオフセットを設定します。この場合の“x”は、システムのタイムゾーンオフセット(「-7200～7201 分」までの値)です。

4) ntp zone-acronym xxx

タイムゾーンの名称を設定します。この値は、タイムゾーン識別用のためにユーザにより設定可能です(設定可能範囲: 16 文字までの英数字および'-'、'_'、あるいは '.'を含む)

5) ntp dst [disable | non-recurring | recurring]

サマータイム設定機能モードを設定します。サマータイム機能は、設定されたサマータイムの設定に応じて時刻の調整を行うことが可能です。

“disable” : サマータイム機能を無効にします。

“non-recurring” : 一定期間のサマータイムを設定します。

”recurring” : 設定したサマータイムを毎年繰り返します。

(1) ntp dst-start-time v/w/x/y/z

サマータイムの開始時間を設定します。

“v”: 月(1～12 までの値)

“w”: 日(1～31 までの値)

“x”: 年(2000-2097 までの値)

“y”: 時間(0-23 までの値)

“z”: 分(0-59 までの値)

(2) ntp dst-end-time v/w/x/y/z

サマータイムの最終時間を設定します。
“v”: 月(1～12 までの値)
“w”: 日(1～31 までの値)
“x”: 年(2000-2097 までの値)
“y”: 時間(0-23 までの値)
“z”: 分(0-59 までの値)

(3) ntp dst-offset x

サマータイムを分単位で設定します。この場合の“x”は、「1～1440 分」までの値です。

29. poe コマンド

PoE 機能を設定します。

“poe ?”と入力すると、次のサブコマンドが表示されます。

```
-----------------------------------------------------------------
(config)# poe ?
auto-checking       PoE auto checking mode
management          Configure PoE power management method
supply              Specify the maximum power the power supply can
                    deliver
-----------------------------------------------------------------
```

- poe auto-checking

接続されている PoE 機器の接続確認を有効にします。
“no poe auto-checking”でこの機能を無効にできます。
このコマンドの Ping の IP アドレスや詳細な動作の設定は Port ごとに“(config-if)#”で設定します。
グローバル Config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

poe management xxx コマンドは、PoE 給電の管理方式を設定します。

“xxx”は、以下のとおりです。

“xxx”	ポートの許容電力	電源管理モード
allocation-consumption	分配モード	実消費電力
allocation-reserved	分配モード	許容電力
class-consumption	PoE クラスモード	実消費電力
class-reserved	PoE クラスモード	許容電力

1. 表中のポートの許容電力について

❑ allocated mode(分配モード):
このモードでは、各ポートで消費できる電力の量を設定します。ポート/受電側機器ごとに指定した電力を設定するには、ポート設定モード"(config-if)#で、"poe power limit x"コマンドを使用してください。

グローバル Config モードにてこの機能を有効に設定した後、"(config-if)#"プロンプトにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

❑ class mode(PoE クラスモード):
このモードでは、接続先の受電側機器のクラスに応じて、確保する電力の量を自動的に判別し、それに応じて電力を確保します。ポートはそれぞれ 4 クラス(それぞれ 4、7、15.4、30 ワット)のいずれかになります。

2. 表中の電源管理モードについて

❑ actual consumption(実消費電力):
このモードでは、すべてのポートの実際の消費電力が供給可能な上限を越えた場合、または指定したポートの消費電力がポートに対して供給可能な電力の上限を越えた場合、ポートはポートのプライオリティに応じてシャットダウンします。2 つのポートのプライオリティが同じ場合は、ポート番号の大きい方がシャットダウンします。

❑ reserved power(許容電力):
このモードでは、消費可能な電力量の合計が供給可能な上限を超えた場合にポートをシャットダウンします。電源から供給可能な電力よりも多くの電力を PoE 機器が要求している場合は、ポートの受電側機器は「OFF」の状態のままです。

❑ poe supply x
供給可能な PoE の電力の最大値を設定します。この場合の"x"は、供給可能な最大電力の値です。
尚、FXC5210PE/5218PE/5224PE はそれぞれ以下の範囲で設定可能です。
- FXC5210PE:0～150W
- FXC5218PE:0～220W
- FXC5224PE:0～370W

30. prompt コマンド
コマンドラインのプロンプトを設定します。

- prompt xxx
コマンドラインのプロンプトを設定します。
"xxx"は、新しいプロンプトの文字列です。"no prompt"コマンドにより、プロンプトをデフォルト設定値に戻します。

使用可能な文字は a-z, A-Z, 0-9 及び、「"」「%」「' 」「|」以外の記号で、18 文字までです。

31. qos コマンド

システムの QoS 機能を設定します。
グローバル Config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

1. ”qos ?”と入力すると、以下の画面が表示されます。

```
-------------------------------------------------------------
(config)# qos ?
  dscp            DSCP Configuration
  qcl             QoS Control List Configuration
-------------------------------------------------------------
```

最初のサブコマンドは DSCP 設定用、2 番目のサブコマンドは QCL(QoS Control List)設定用です。

2. ”qos dscp ?”と入力すると、以下の画面が表示されます。

```
-------------------------------------------------------------
(config)# qos dscp ?
  classification-map    Set DSCP ingress classification table
  classification-mode   Set DSCP ingress classification mode
  egressremap           Set DSCP egress remap table
  map                   Set DSCP mapping table
  translation           Set global ingress DSCP translation
                        table
  trust                 Set whether a specific DSCP value is
                        trusted
-------------------------------------------------------------
```

1) qos dscp classification-map x y z

QoS クラスおよび破棄優先度を内部 DSCP 値にマッピングします。
”x”:QoS クラス(0～7 までの値)
”y”:破棄優先度(0～1 までの値)
“z”:dscp(0～63 までの値)
フレームは QoS クラスを取得後(ポートのデフォルト、または VLAN Tag または DSCP のいずれか)、この QoS を内部 DSCP にマッピングします。ここで設定された DSCP 値は出力マップにより、送信フレームの DSCP 値に影響し、
Egress Rewrite が有効な場合は、出力 DSCP の値を上書きします。

2) qos dscp classification-mode x

クラス分類の入力 DSCP 値を設定します。この場合の“x”は、dscp の値は「0～63」です。ポートの入力クラスの設定が「selected」の場合は DSCP の値を選択して、内部 DSCP に対する QoS クラスを有効にします。
“no qos dscp classification-mode x”でこの機能を無効にします。

3) qos dscp egressremap x y z

DSCP 出力リマップテーブルを設定します。
“x”:dscp の値(0～63)。
“y”:「0」または「1」の DPL(破棄優先度)。
“z”: DPL 用の出力リマップ DSCP の値(0～63)。
このコマンドにより、DPL(破棄優先度)「0」または「1」の出力 DSCP 値のマッピングに内部 DSCP を設定します。本コマンドは“qos dscp egressremark”コマンドが設定されている場合に有効です。

4) qos dscp map x y z

DSCP ベース QoS 出力クラス分類を設定します。
“x”: dscp の値(0～63)。
”y”: QoS クラス(0～7)。
“z”: 破棄優先度(0～1)。
このコマンドにより、基本 DSCP ベースの QoS 入力クラス分類を設定します。
DSCP 値が有効な場合、設定が反映されます。

5) qos dscp translation x y

グローバル config モードで、入力 DSCP 変換テーブルを設定します。
”x”:変換前の DSCP の値(0～63)。
”y”:変換後の DSCP 値(0～63)です。入力側の DSCP は、QoS クラスと DPL マップの DSCP を使用する前に、新しい DSCP に変換されます。

6) qos dscp trust x

特定の DSCP 値が正しいかどうかを設定します。
この場合の“x”は、dscp 値「0～63」です。フレームの DSCP 値が正しい場合のみ特定の QoS クラスおよび DPL にマッピングします。フレームの DSCP 値が不正な場合は、non-IP フレームとして処理されます。

3. “qos qcl ?”と入力すると、以下の画面が表示されます。

```
-------------------------------------------------------------
(config)# qos qcl ?
  <1-256>            QCE ID
-------------------------------------------------------------
```

“qos qcl x”と入力すると、Queue Control Entry 設定用の“(config-QCE-x)#”になります。
この場合”x”は QCE(1～256)のインデックスになります。

“qos qcl 10 ?”と入力すると、以下の画面を表示します。

```
-------------------------------------------------------------
(config)# qos qcl 10
QCE ID 10 added last
(config-QCE-10) ?
  exit           Ext from current mode
  help           Show available commands
  history        Show a list of previously run commands
  logout         Disconnect
  quit           Quit commands
  action         Action Parameters
  ethernet       Port Members
  key            Key Parameters
  next_id        Next QCE ID
-------------------------------------------------------------
```

1) Exit コマンド

現行のオペレーションモードを終了し、元のモードに戻ります。

2) help コマンド

有効なコマンドを表示します。

3) History コマンド

入力したコマンドの履歴を表示します。

4) Logout コマンド

コンソール画面からログアウトします。

5) Quit コマンド

コンソール画面を終了(logout と同じ機能)します。

6) Action コマンド

QCE と一致する場合は、フレームの QoS の動作を設定します。

```
-------------------------------------------------------------
(config-QCE-10)# action ?
  class       Qos class
  dpl         DP Level
  dscp        DSCP
-------------------------------------------------------------
```

(1) action class x

QoS クラスの動作を設定します。この場合の“x”は、QoS クラス(0～7)です。
”action class default”コマンドにより、デフォルト設定に戻します。

(2) action dpl x

破棄優先度の動作を設定します。この場合の“x”は、破棄優先度(0～1)です。
”action dpl default”コマンドにより、デフォルト設定に戻します。

(3) action dscp x

DSCP 値の動作を設定します。この場合の“x”は、DSCP 値(0～63)です。
”action dscp default”コマンドにより、デフォルト設定に戻します。

(4) ethernet

ポートを QCL エントリに割り当てます。

```
-------------------------------------------------------------
(config-QCE-10)# ethernet ?
  <1-10>          Unit number: format 1/x   1/x,y,z  1/x-y
   1/x-y,z
-------------------------------------------------------------
```

- ethernet 1/x

  “Port x”を QCL エントリに割り当てます。
  この場合の”x”は、ポート番号(1/x, 1/x,y,z, 1/x-y, 1/x-y,z と記述)です。

7) key コマンド

QCL エントリのキーの値を設定します。キーの値は、フレームの L2～L4 までの情報です。

```
-------------------------------------------------------------
(config-QCE-10)# key ?
  dmac-type          Destination MAC type
  frame-type         Frame Type
  smac               Source MAC address
  tag                Value of Tag field
-------------------------------------------------------------
```

(1) key dmac-type [any | bc | mc | uc]

フレームの宛先 MAC アドレスのタイプによってキーの値を設定します。この値は、any（すべての MAC アドレス）、bc（ブロードキャスト）、mc（マルチキャスト）、uc（ユニキャスト）フレームのいずれかです。

(2) key frame-type [any | ethernet | ipv4 | ipv6 | llc | snap]

フレームのタイプごとにキーの値を設定します。
値は、以下のいずれかです。

- Any
- Ethernet Type(any/specific type(0x600-0xFFFF))
- IPv4(DSCP value/IP-Fragment or not/Protocol - Port Number of TCP,UDP, other/Source IP Address)
- IPv6(DSCP value/Protocol - Port Number of TCP, UDP, other/Source IP Address)
- LLC(SSAP/DSAP/Control)
- SNAP(PID)

【注記】: それぞれのコマンドにはさらに詳細に設定できるサブコマンドがあります。
コマンドラインにて“?”を入力し、サブコマンドの範囲をご確認ください。

(3) key smac [any | xx-xx-xx]

送信元の MAC アドレスごとにキーの値を設定します。
任意の値、または送信元 MAC アドレスの OUI に設定可能です。

(4) key tag [any | tag | untag]

フレームのタグ情報ごとにキーの値を設定します。

- Any
- tag(DEI, PCP, VID)
- untag

【注記】:
それぞれのコマンドにはさらに詳細に設定できるサブコマンドがあります。
コマンドラインにて“?”を入力し、サブコマンドの範囲をご確認ください。

8) next_id コマンド

QCL テーブルの QCL エントリの順番を設定します。

(1) next_id x

QCL エントリ"x"の後に QCL エントリを設定します。この場合の"x"は、QCL エントリの ID(1～256)です。

(2) next_id last

この QCL を QCL テーブルの最新のエントリに設定します。
その他の QoS 設定については、"interface ethernet 1/x"コマンドを使用してください。この場合の"x"はポート番号です。
グローバル Config モードにてこの機能を有効に設定した後、"(config-if)#"プロンプトにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。
詳細については、「ポートインタフェース設定コマンド」を参照してください。

32. radius-accounting-server コマンド

RADIUS アカウンティングサーバを設定します。RADIUS アカウンティングサーバを 5 つまでサポートします。

1. "radius-accounting-server ?"と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# radius-accounting-server ?
<1-5>           Server-Index
dead-time Specifies Dead Time of Common Servers
timeout         Specifies Time Out of Common Servers
-------------------------------------------------------------
```

2. "radius-accounting-server x ?"と入力すると、次のサブコマンドが表示されます(この場合の"x"は「1～5」までのサーバのインデックスです)。

```
-------------------------------------------------------------
(config)#       radius-accounting-server 1 ?
active    Active the RADIUS server
host      Specifies the RADIUS server
key       Sets the RADIUS encryption key
port      Sets the RADIUS server network port
-------------------------------------------------------------
```

1) radius-accounting-server x active

RADIUS アカウンティングサーバ"x"を有効にします。この場合の"x"は、サーバのインデックス番号「1～5」です。

2) radius-accounting-server x host y.y.y.y

RADIUS アカウンティングサーバ"x"に IP アドレスを割り当てます。
"x" :サーバのインデックス番号「1～5」
"y.y.y.y" :RADIUS アカウンティングサーバ"x"の IP アドレス

3) radius-accounting-server x key yyy

RADIUS アカウンティングサーバ"x"にシークレットキー"yyy"を割り当てます。
"x" : サーバのインデックス番号「1～5」
"yyy":シークレットキー(最大 29 文字)(※RADIUS アカウンティングサーバと本機の間で共有です。)

4) radius-accounting-server x port y

RADIUS アカウンティングサーバ上で使用する UDP ポートを割り当てます。
”x”:サーバのインデックス番号「1～5」。
“y”:「0～65535」までの UDP ポート番号。
※ポートが「0(zero)」に設定されると、デフォルトのポート(1813)が設定されます。

5) radius-accounting-server dead-time x

アカウンティングサーバのデッドタイムを指定します。この場合の“x”は、デッドタイム(0～3600)秒までの値です。デッドタイムは、前回のリクエスト応答に失敗したサーバへ新しいリクエストの送信を中断する時間です。
これにより、サーバが停止状態にあると判断し、通信を中断します。
デッドタイムを「0」よりも大きい値に設定すると、この機能が有効になります。但し、複数のサーバが設定されている場合のみこの機能は動作します。

6) radius-accounting-server timeout x

タイムアウト時間の設定をします。
この場合の“x”は、タイムアウトの値(3～3600)秒の値です。タイムアウトはサーバからの応答の最大待機時間です。
サーバが設定時間内に応答しない場合は、休止しているとみなして、次の有効なサーバとの通信を行います(可能な場合)。
RADIUS サーバは設計上信頼できない UDP プロトコルを使用しています。
ロストフレームに対応するために、タイムアウトの間隔は 3 等分されます。区間内に応答を受信しない場合は、リクエストを再送します。この方法により、RADIUS サーバは、サーバが「休止状態」とみなされるまで「最大 3 回」まで問い合わせを行います。

33. radius-authentication-server コマンド

RADIUS 認証サーバを設定します。RADIUS 認証サーバは最大 5 つまでサポートしています。

1. “adius-authentication-server ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# radius-authentication-server ?
<1-5>     Server-Index
dead-time       Specifies Dead Time of Common Servers
timeout         Specifies Time Out of Common Servers
-------------------------------------------------------------
```

2. “radius-authentication-server x ?”と入力すると、次のサブコマンドが表示されます(この場合の“x”は「1～5」までのサーバのインデックスです)。

例:“radius-authentication-server 1 ?”と入力すると以下の画面を表示します。

```
-------------------------------------------------------------
(config)# radius-authentication-server 1 ?
active    Active the RADIUS server
host      Specifies the RADIUS server
key       Sets the RADIUS encryption key
port      Sets the RADIUS server network port
-------------------------------------------------------------
```

1) radius-authentication-server x active

RADIUS 認証サーバ“x”を有効にします。この場合の“x”は、サーバのインデックス番号「1～5」です。

2) radius-authentication-server x host y.y.y.y
RADIUS 認証サーバ“x”に IP アドレスを割り当てます。
“x” : サーバのインデックス番号「1～5」
“y.y.y.y” : RADIUS 認証サーバ“x”の IP

3) radius-authentication-server x key yyy
RADIUS 認証サーバ“x”にシークレットキー“yyy”を割り当てます。
”x” : サーバのインデックス番号「1～5」
”yyy” : シークレットキー(最大 29 文字)です(RADIUS 認証サーバおよび本機間で共有)。

4) radius-authentication-server x port y
RADIUS 認証サーバに UDP ポートを割り当てます。
“x” : サーバのインデックス番号「1～5」。
”y” : UDP ポート番号(0～65535)。※ポートが「0」の場合は、デフォルトのポート(1812)を使用。

5) radius-authentication-server dead-time x
サーバのデッドタイムを指定します。
デッドタイム(0～3600)秒までの値となります。デッドタイムは、リクエストへの応答に失敗したサーバに対して新しいリクエストの送信が中断されるまでの時間です。これにより、サーバが停止状態にあると判断し、通信を中断します。
デッドタイムを「0」よりも大きい値に設定すると、この機能が有効になります。但し、複数のサーバが設定されている場合のみこの機能は動作します。

6) radius-authentication-server timeout x
タイムアウト時間の設定をします。
この場合の“x”は、タイムアウトの値(3～3600)秒の値です。タイムアウトはサーバからの応答の最大待機時間です。サーバが設定時間内に応答しない場合は、「休止」とみなして、次の有効なサーバに通信を行います(可能な場合)。

34. rmon コマンド
本機の RMON 機能を設定します。

1. それぞれ RMON グループ 1(統計情報)、2(履歴)、3(アラーム)、9(イベント)となっております。
RMON グループを設定するには、以下のコマンドを使用します。

```
-------------------------------------------------------------
(config)# rmon ?
  alarm                 Add RMON Alarm entry
  event                 Add RMON Event entry
  history               Add RMON Hisotry entry
  statistics            Add RMON Statistics entry
-------------------------------------------------------------
```

2. ”rmon alarm x ?”と入力すると、アラームのコンフィグレーションパラメータが表示されます。
この場合の“x”は、エントリのインデックスです。設定可能な範囲の値は「1～65535」です。

例:”rmon alarm 10 ?”と入力すると、以下のサブコマンドが表示されます。

```
-------------------------------------------------------------
# rmon alarm 10 ?
  falling-index         Falling event index
  falling-threshold     Falling threshold value
  Interval              Indicates the interval in seconds for
                sampling and comparing the rising and
                falling threshold
  rising-index          Rising event index
  rising-threshold      Rising threshold value
  sample-type           The method of sampling
  startup-alarm         The method of sampling
  variable              Indicates the particular variable to be
                sampled
-------------------------------------------------------------
```

(1) rmon alarm x falling-index y
下限アラームのイベントインデックスを設定します。
“x”:「1～65535」までのエントリのインデックスになります。
“y”:下限アラームのイベントインデックス(1～65535)です。

(2) rmon alarm x falling-threshold y
アラームの下限閾値を設定します。
“x”:「1～65535」までのエントリのインデックスになります。
“y”:下限閾値(-2147483648～2147483647)です。

(3) rmon alarm x interval y
サンプリング間隔、閾値と比較したサンプリング値の増減が表示されます。
“x”:「1～65535」までのエントリのインデックスになります。
“y”:間隔(1～2147483647 秒)です。

(4) rmon alarm x rising-index y
上限アラームのイベントインデックスを設定します。
”x”:「1～65535」までのエントリのインデックスになります。
“y”:上限アラームのイベントインデックス(1～65535)です。

(5)rmon alarm x rising-threshold y
アラームの上限閾値を設定します。
“x”:「1～65535」までのエントリのインデックスになります。
“y”:上限閾値(-2147483648～2147483647)です。

(6) rmon alarm x sample-type [absolute | delta]
選択したデータのサンプリングの算出、閾値と比較した場合の表示方法を選択します。
この場合の“x”は、「1～65535」までのエントリのインデックスになります。
サンプルのタイプは以下のとおりです。
- absolute : サンプリングしたデータを直接入手します。
- delt : サンプリングしたデータ間の差異を算出します。

(7) rmon alarm x startup-alarm [falling | rising | risingorfalling]

選択したデータのサンプリングの算出、閾値と比較した場合の表示方法を選択します。
この場合の”x”は、「1～65535」までのエントリのインデックスになります。
サンプルのタイプは以下のとおりです。
- falling: サンプリングしているデータが下限閾値よりも下回った場合、アラームを出します。
- rising : サンプリングしているデータが上限閾値を超えた場合、アラームを出します。
- rising or falling: サンプリングしているデータが下限閾値よりも下回った場合、あるいは上限閾値を超えた場合はアラームを出します

(8) rmon alarm x variable.1.3.6.2.2.2.2.2.1.y.z

サンプリングしたい特定の変数を表示します。
“x”:「1～65535」秒までのエントリのインデックス。
“y”:「10～21」。
“z”:「1～65535」。

3. “rmon event x ?”と入力すると、イベントのコンフィグレーションパラメータのコマンドが表示されます。
この場合の“x”は、エントリのインデックスです。設定可能な範囲の値は「1～65535」です。

例: ”rmon event 10 ?”と入力すると、以下のサブコマンドが表示されます。

```
-------------------------------------------------------------
  (config)# rmon event 10 ?
    Community    Specify the community when trap is sent
    desc         Indicates this event, the string length is
                 from 0 to 127
    type         Indicates the notification of the event
-------------------------------------------------------------
```

(1) rmon event x community yyy

トラップ送信時のコミュニティを指定します。
“x”:「1～65535」までのエントリのインデックス。
“yyy”は、コミュニティ名（0～127 文字）。

(2) rmon event x desc yyy

特定のイベントを指定してトラップを送信します。
“x” :「1～65535」までのエントリのインデックス
“yyy”:コミュニティ名（0～127 文字）。

(3) rmon event x type [log | log-trap | none | trap]

イベントの通知を行います。
この場合の“x”は、「1～65535」までのエントリのインデックスになります。
設定可能な通知は以下のとおりです。
- log : 各イベントのログテーブルにエントリが作成されます。
- log-trap : ″log″と″trap″の両方の動作が行われます。
- none : イベントの通知を行いません。
- trap : SNMP トラップが 1 つまたは複数の管理ステーションに送信されます。

4. “rmon history x ?”と入力すると、履歴のコンフィグレーションパラメータのコマンドが表示されます。
この場合の“x”は、エントリのインデックスです。設定可能な範囲の値は「1～65535」です。

“rmon history 10 ?”と入力すると、以下のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# rmon history 10 ?
Buckets   Indicates the maximum data entries associated
          this History control entry stored in RMON
data_sourceIndicates the port ID which wants to be
           monitored
interval    Indicates the interval in seconds for sampling
           the history statistics data
-------------------------------------------------------------
```

(1) rmon history x buckets y

RMON にストアされている履歴制御エントリに関連のある最大データエントリ数を表示します。
”x”:「1～65535」までのエントリのインデックスになります。
“y”:RMON にストアされている履歴制御エントリに関連のある最大データのエントリ数を表示します。設定可能な範囲の値は「1～3600」です。

(2) rmon history x data_source .1.3.6.1.2.1.2.2.1.1.y

モニタを行うポート ID を表示します。
“x”:「1～65535」までのエントリのインデックスになります。
”y”:モニタリングを行うポート ID です。

(3) rmon history x interval y

履歴の統計データのサンプリング間隔を秒単位で表示します。
“x”:「1～65535」秒までのエントリのインデックスになります。
“y”:履歴の統計データのサンプリング間隔（秒単位）です。設定可能な範囲の値は「1～3600」秒です。

5. “rmon statistics x ?”と入力すると、統計情報のコンフィグレーションパラメータのコマンドが表示されます。この場合の“x”は、エントリのインデックスです。
設定可能な範囲の値は「1～65535」です。

例：“rmon statistics 10 ?”と入力すると、以下のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# rmon statistics 10 ?
  data_source    Indicates the port ID which wants to be
          monitored
-------------------------------------------------------------
```

・ rmon statistics x data_source.1.3.6.1.2.1.2.2.1.1.y

モニタリング対象のポート ID を表示します。
“x”:「1～65535」までのエントリのインデックスになります。
“y”:モニタリングを行うポート ID です。

35. s-flow コマンド

sFlow コレクタの設定のモニタリング/修正を行うことができます。サポートしているコレクタは 1 個のみです。
ここでは、sFlow コレクタごとに、sFlow コレクタの IP タイプ、sFlow コレクタの IP アドレス、ポート番号を設定可能です。sFlow は、サンプリングベースの技術であり、パケットのサンプリング、リアルタイムトラフィック解析を行うことが可能です。サンプリングされたパケットおよびカウンタ(それぞれ"フローサンプル"、"カウンタサンプル"と呼ばれる)はセントラルネットワークトラフィックのモニタリングサーバに sFlow UDP データとして送信されます。
このセントラルサーバは、"sFlow レシーバ"、または"sFlow コレクタ"とも呼ばれ、本機の sFlow 機能の設定を行います。

"sflow receiver ?"と入力すると、以下のサブコマンドが表示されます。

```
-----------------------------------------------------------------
(config)# sflow receiver ?
Datagramsize Set the Reciever Data gram length for list of
             receiver ID
ip           Set the sFlow receiver IP and UDP Port for list
             of receiver ID
release      Release
time_out     Set the Receiver Time_out for list of receiver ID
-----------------------------------------------------------------
```

1) sflow receiver datagramsize x

レシーバ ID のリストにレシーバのデータの長さを設定します。この場合の"x"は、1つのサンプルデータが送信可能なデータの最大バイト数です。
sFlow データのフラグメンテーションを回避可能な値に設定します。設定可能な範囲の値は「200～1500」バイト、デフォルト設定値は「1400」バイトです。

2) sflow receiver ip <ip address> x

レシーバ ID のリストに sFlow レシーバの IP および UDP ポートを設定します。
<ip address> は、sFlow レシーバの IP アドレス、またはホスト名です。
IPv4 および IPv6 アドレスがサポートされています。
この場合の"x"は、sFlow レシーバが sFlow データを受信する UDP ポートです。有効なポート番号は「0～65535」です。「0」に設定する場合は、デフォルトのポート(6343)を使用します。

3) sflow receiver release

現行のオーナーを解除して、sFlow サンプルを無効にします。
sFlow は基本的に Web/CLI インタフェースを用いたローカル管理、または SNMP を介したリモート管理のいずれかの方法で設定できます。
現行の sFlow 設定のオーナーは、以下の値に設定可能です。

- sFlow が現在設定されていない場合、オーナーは<none>。
- sFlow が Web、または CLI に設定されている場合は、オーナーは<Configured through local management>。
- sFlow が SNMP を介して設定されている場合は、オーナーは sFlow レシーバを指す文字列(※この場合、不正なアクセスによる設定を避けるためにすべての制御は無効になります)。

4) sflow receiver time_out x

レシーバ ID のリストにレシーバのタイムアウトを設定します。
"x"はサンプリングを停止し、現行の sFlow オーナーが解除されるまでの残りの秒数です。
レシーバ ID のリストにレシーバのタイムアウトを設定します。
設定可能な範囲の値は「0～2147483647」秒です。

sFlow 機能は、ポート単位で有効となります。その他のポートの sFlow 設定については、“interface ethernet 1/x”コマンドを使用してください。

グローバル Config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。
詳細については、「sflow コマンド」を参照してください。

36.snmp-server コマンド

本機の SNMP 機能設定用に用います。

1. ”snmp-server ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# snmp-server ?
  <1-1>                 Index of Trap
  community             Defines SNMP community access string
  contact               Sets the system contact string
  enable                Enables SNMP function
  location              Sets the system location string
  snmpv3-access         Sets the snmpv3 community
  snmpv3-community      Sets the snmpv3 community
  snmpv3-group          Sets the snmpv3 group configuration
  snmpv3-user           Sets the snmpv3 user configuration
  snmpv3-view           Sets the snmpv3 view configuration
  version               Sets the snmp version
-------------------------------------------------------------
```

2. ”snmp-server 1 ?”コマンドを入力すると、SNMP トラップ設定用のコマンドが以下の画面で表示されます。

```
-------------------------------------------------------------
(config)# snmp-server 1 ?
  authentication-failure  Trap Community
  community      Trap Community
  enable         Enables this Trap function
  host           Specifies SNMP notification operation
          recipients
  host-ipv6      Specifies SNMP notification operation
                 recipients(for ipv6 addresss)
  link-up-down   Trap Link-up and Link-down
  version        Trap Version
-------------------------------------------------------------
```

1) snmp-server x authentication-failure

SNMP 本体は認証失敗トラップの生成を許可します。
この場合の“x”は、トラップ「1～1」のインデックスです。
“no snmp-server x authentication-failure“コマンドにより、この機能を無効にします。

2) snmp-server x community yyy

SNMP トラップパケット送信時のコミュニティアクセスストリングを設定します。
“x”:トラップ「1～1」のインデックス。
“yyy”: 「0～255」のコミュニティ名(ASCII 文字の場合は、「33～126」文字)。

3) snmp-server x enable

SNMP トラップを有効にします。この場合の“x”は、トラップ「1～1」のインデックスです。
“no snmp-server x enable“コマンドにより、この機能を無効にします。

4) snmp-server x host y.y.y.y

SNMP trap IPv4 の宛先アドレスを設定します。
“x” :トラップ「1～1」のインデックス。
”y.y.y.y”: SNMP トラップを送信する宛先の IPv4 アドレス。

5) snmp-server x host-ipv6 <IPv6 address>

SNMP trap IPv6 の宛先アドレスを設定します。
この場合の“x”は、トラップ「1～1」のインデックスです。
“<IPv6 address>”には、SNMP トラップを送信する宛先の IPv6 アドレスを指定します。

6) snmp-server x link-up-down

リンクアップ/ダウン時の SNMP トラップ送信を有効にします。
この場合の“x”は、トラップ「1～1」のインデックスです。
“no snmp-server x link-up-down”コマンドにより、この機能を無効にします。

7) snmp-server x version [v1 | v2c | v3]

SNMP trap のサポート可能なバージョンを選択します。この場合の“x”は、トラップ「1～1」のインデックスです。SNMP Trap のバージョンのオプションは、SNMP V1(v1)、SNMP V2c(v2c)および SNMP V3(v3)です。

【注記】: それぞれのコマンドにはさらに詳細に設定できるサブコマンドがあります。
コマンドラインにて“?”を入力し、サブコマンドの範囲をご確認ください。

8) snmp-server community get xxx

SNMP の get コマンドのコミュニティ名を設定します。
“xxx”は、コミュニティ名です。

9) snmp-server community set xxx

SNMP の set コマンドのコミュニティ名を設定します。
“xxx”は、コミュニティ名です。

10) snmp-server contact xxx

担当者情報を設定します。“xxx”は、担当者情報です。

11) snmp-server enable

SNMP 機能を有効にします。“no snmp-server enable“コマンドを使用すると、この機能は無効になります。

12) snmp-server location xxx

本機の設置場所情報を設定します。
“xxx”は、設置場所情報です。

13) snmp-server version [v1 | v2c | v3]

SNMP のバージョンを選択します。
SNMP バージョンのオプションは、SNMP V1(v1)、SNMP V2c(v2c)、SNMP V3(v3)です。

SNMP v3 設定用のコマンドは、以下のとおりです。

(1) snmp-server snmpv3-access group-name xxx security-model [any | v1 | v2c | usm]security-level [authnopriv | authpriv | noauthnopriv]read_view_name yyy write_view_name zzz

SNMPv3 アクセスエントリを設定します。
"xxx" : エントリが属するグループ名を示す文字列。
設定可能な文字列の値は「1～32」です。
ASCII 文字の場合は「33～126」。
"yyy" : 現行の値のリクエストを行う MIB オブジェクトを設定する MIB VIEW 名。
設定可能な文字列の値は「1～32」です。
ASCII 文字の場合は「33～126」。
"zzz" : 新しい値が設定可能なリクエストの MIB オブジェクトを設定する MIB VIEW の名前です。
設定可能な文字列の値は「1～32」、ASCII 文字の場合は「33～126」。

(2) no snmp-server snmpv3-access group-name xxx security-model [any | v1 | v2c | usm]security-level [authnopriv | authpriv | noauthnopriv]

コマンドを入力した場合、SNMPv3 アクセスエントリを削除します。

1) セキュリティモデルのオプションについては、以下のとおりです。
- "any" : セキュリティモデルはすべて可能(v1|v2c|usm)
- "v1" : SNMPv1 用
- "v2c" : SNMPv2c 用
- "usm" : User-based Security Model(USM).

2) セキュリティレベルのオプションについては、以下のとおりです。
- "authnopriv" : 認証あり/プライバシーなし
- "authpriv" : 認証あり/プライバシーあり
- "noauthnopriv": 認証なし/プライバシーなし

(3) snmp-server snmpv3-community community xxx source-ip y.y.y.y source-mask z.z.z.z

SNMPv3 コミュニティエントリを作成します。
"no snmp-server snmpv3-community community xxx"コマンドにより、SNMPv3 コミュニティエントリを削除します。
"xxx" : SNMPv3 エージェントへのアクセスが可能なコミュニティアクセスストリング。設定可能な文字列の値は「1～32」、ASCII 文字の場合は「33～126」です。
コミュニティ名は、セキュリティ名として扱われ、SNMPv1 または SNMPv2c コミュニティ名のいずれかをマッピングを行います。

“y.y.y.y” : SNMP サーバの IP アドレス。
“z.z.z.z” : SNMP サーバの IP アドレスのマスク。

(4) snmp-server snmpv3-group security-model [v1 | v2c | usm]security-name xxx group-name yyy

SNMPv3 グループを設定します。“no snmp-server snmpv3-group security-model [v1 | v2c | usm]security-name xxx“コマンドにより、SNMPv3 グループを削除します。
“xxx” : エントリが所属するセキュリティ名識別用の文字列。
設定可能な文字列の値は「1～32」、ASCII 文字の場合は「33～126」です。
“yyy” : エントリが所属するグループ名識別用の文字列。
設定可能な文字列の値は「1～32」、ASCII 文字の場合は「33～126」です。

Security Model のオプションは、以下のとおりです。
- v1 : SNMPv1 用
- v2c: SNMPv2c 用
- usm: User-based Security Model(USM)

(5) snmp-server snmpv3-user xxx yyy

「認証なし/プライバシーなし」セキュリティ SNMPv3 ユーザを設定します。
“xxx”: SNMPv3 Engine ID。
“yyy”: エントリが所属するユーザ名識別用の文字列。

(6) snmp-server snmpv3-user xxx yyy auth [md5 | sha]zzz

「認証あり/プライバシーなし」セキュリティレベルの SNMPv3 ユーザを設定します。
“xxx”: SNMPv3 Engine ID。
“yyy”: このエントリが所属するユーザ名識別用の文字列。
“zzz”: 認証パスワード識別用の文字列。

(7) snmp-server snmpv3-user xxx yyy auth-priv [md5 | sha]zzz des www

「認証あり/プライバシーあり」セキュリティレベルの SNMPv3 ユーザを設定します。
“xxx”: SNMPv3 Engine ID。
“yyy”: このエントリが所属するユーザ名識別用の文字列。
“zzz”: 認証パスワード識別用の文字列。
“www”: プライバシーパスワード識別用の文字列。

“no snmp-server snmpv3-user xxx yyy”コマンドにより、SNMPv3 ユーザを削除します。
この場合の“yyy”はユーザ名の為、追加したときに入力した文字列を入れなければなりません。

それぞれの用語については、以下を参照ください。

❑**SNMPv3 Engine ID:**

エントリが所属する engine ID 識別用の 8 桁(1 オクテット)の文字列。文字列には、「10～64」までの桁数(16 進数)を含む必要がありますが、”オール 0”および”オール F”は使用できません。
SNMPv3 ではメッセージセキュリティ用の User-based Security Model(USM)、アクセスコントロール用の View-based Access Control Model(VACM)を使用します。
USM エントリでは、usmUserEngineID および usmUserName がエントリーキーです。
シンプルエージェントの場合は、USM UserEngineID はエージェント独自の snmpEngineID の値です。
値は、ユーザが通信可能なリモート SNMP エンジンの SNMP EngineID の値に設定することも可能です。
つまり、ユーザエンジン ID がシステムエンジンの ID と同じ場合は、ローカルユーザになり、それ以外はリモートユーザです。

❑**ユーザ名:**

エントリが所属するユーザ名識別用の文字列です。設定可能な文字列の値は「1～32」、ASCII 文字の場合は「33～126」です。

❑**認証パスワード:**

認証パスワード識別用の文字列です。MD5 認証プロトコルの場合は、設定可能な文字列の値は「8～32」です。SHA 認証プロトコルの場合は、設定可能な文字列の値は「8～40」です。
ASCII 文字の場合は「33～126」です。

❑**プライバシーパスワード:**

プライバシーパスワード識別用の文字列です。設定可能な文字列の値は「8～32」、ASCII 文字の場合は「33～126」です。

(8) `snmp-server snmpv3-view view-name xxx view-type [excluded | included] oid-subtree yyy`

SNMPv3 View Entry を設定します。
“xxx”: エントリが所属するビュー名識別用の文字列です。設定可能な文字列の値は「1～32」、ASCII 文字の場合は「33～126」。
“yyy”: ビューを追加するためのサブツリーのルートを設定する OID です。
設定可能な OID の長さは、「1～128」です。
有効な文字列は数字、またはアスタリスク(*)です。

37. spanning-tree コマンド

本機のスパニングツリープロトコルを設定します。”spanning-tree ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# spanning-tree ?
  bpdufilter         Set edge port BPDU Filtering
  bpduguard          Set edge port BPDU Guard
  cname              Set configuration name and revision for MSTI
  forward-delay      Global STA forward time configuration. Range:
                     <4-30 seconds>
  hello-time         Global STA hello time configuration. Range:
                     <1-10 seconds>
  max-age            Gobal STA maximum age configuration. Range
                     <6-40 seconds>
  max-hop-count      Setthe MSTP Bridge Max Hop Count parameter
  mode               Select spanning tree operation mode
  msti               Compatible with old STP
  priority           Specifies spanning tree priority
  recovery           Set edge port error recovery timeout
  transmit-hop-count Set the STP Bridge Transmit Hold Count
                       parameter
 -------------------------------------------------------------
```

1) spanning-tree bpdufilter

ポートがエッジとして設定されている場合は、BPDU の送受信が可能になります。
“no spanning-tree bpdufilter”コマンドにより、この機能を無効にします。

2) spanning-tree bpduguard

ポートの BPDU Guard 機能を有効にします。この機能が有効な場合は、有効な BPDU を受信するとポートは無効になります。
ポートがエッジとして設定されている場合、BPDU の受信を無効にします。
ポートは「error-disabled」の状態となり、有効なトポロジーから外されます。“no spanning-tree bpduguard“コマンドにより、この機能を無効にします。

3) spanning-tree cname xxx y

MSTI 設定用の設定名およびリビジョンを設定します。“xxx”は、Configuration Name の文字列であり、MSTI マッピングへの VLAN 識別用の名前です。
ブリッジは、名前、リビジョン、VLAN-to-MSTI マッピング設定を共有し、また MSTI (リージョン内) のスパニングツリーを共用します。
”xxx” : 設定可能な文字列は「32」文字以内です
“y” : リビジョンの番号 (0～65535) です。

4) spanning-tree forward-delay x

グローバルモードの STA 伝送時間を設定します。
(STP 互換モードを設定している場合) ルートポートおよび指定ポートがフォワーディング状態に移行するまでの STP ブリッジでの遅延時間です。有効な値は、「4～30」秒です。

5) spanning-tree hello-time x

グローバル STA の hello time を設定します。hello time は、本装置が定期的に送信する BPDU の送信間隔を秒単位で設定します。有効な値は、「1～10 秒」の値、かつ (HelloTime+1)*2 <= MaxAge となります。

6) spanning-tree max-age x

STAの最大エージ (Max Age)を設定します。これは、ルートブリッジの場合にブリッジにより送信された情報の最大エージです。“x”は、最大エージ時間です。
有効な値は「6～40」秒、最大エージは(FwdDelay-1)*2 で算出した値に設定します。

7) spanning-tree max-hop-count x

MSTP Bridge Max Hop Count パラメータを設定します。
MSTI リージョン内で設定された MSTI 情報の残りのホップ数の初期値を設定します。
ルートブリッジが BPDU 情報を伝送するブリッジ数を設定します。
この場合の“x”は、最大ホップ数です。有効な値は、「4～60」までのホップ数です。

8) spanning-tree mode [mstp | rstp | stp]

スパニングツリーのオペレーションモード(MSTP、RSTP、STP)を選択します。

9) spanning-tree msti instance x vlan y

MSTI に VLAN を設定します。
”x”: MSTI を示す番号(1～7)です。
”y”: MSTI に追加した VLAN の VLAN ID(1～4095)です。VLAN は 1 つの MSTI にのみマッピング可能です。
未使用の MSTI は、VLAN マッピングされません。

10) spanning-tree msti priority x y

ブリッジインスタンスのプライオリティを設定します。
“x”:MSTI を示す番号(1～7)です。
”y”:ブリッジインスタンスのプライオリティ(0～61440)。
※4096 の倍数(例えば、”y”は 0, 4096, 8192, 12288, ...)です。値が小さくなると、プライオリティが高くなります。ブリッジのプライオリティと MSTI インスタンス番号を 6 バイトの MAC アドレスで連結すると、ブリッジの識別子を設定します。

11) spanning-tree priority x

スパニングツリーのプライオリティを指定します。
この場合の“x”は、スパニングツリーのプライオリティの値(0～61440)です。
※4096 の倍数(例えば、“x”は 0, 4096, 8192, 12288...)です。
値が小さくなると、プライオリティが高くなります。MSTP オペレーションの場合は、CIST のプライオリティです。それ以外は、STP/RSTP ブリッジのプライオリティです。ブリッジのプライオリティと MSTI インスタンス番号は 6 バイトの MAC アドレスで連結し、ブリッジの識別子を設定します。

12) spanning-tree recovery x

エッジポートのエラーリカバリのタイムアウトを設定します。
これは、error-disabled 状態のポートが有効になるまでの時間です。
この場合の“x”は、タイムアウトの値です。有効な値は「30～86400 秒」(24 時間)です。

13) spanning-tree transmit-hop-count x

STP Bridge Transmit Hold Count パラメータを設定します。これはブリッジポートが 1 秒間に送信可能な BPDU の数です。この値を超えると、次の BPDU の送信に遅延が生じます。
この場合の“x”は、Transmit Hold Count(転送保留カウント値)です。
有効な値は、「1～10(毎秒ごとに BDPU を送信する数)」です。

グローバル Config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

ポートのスパニングツリーの設定方法については、「ポートインタフェース設定コマンド」を参照してください。
ここでは、ブリッジのみ設定可能です。

38. storm-control コマンド

ストームコントロールレートを設定します。制御可能なパケットストームはブロードキャスト、マルチキャスト、ユニキャストのトラフィックのフラッディングです。レートは、毎秒ごとのパケット(pps)を算出します（※bps ではありません)。
フラッディングされたフレームにのみ適用されます（たとえば、MAC アドレステーブル上にないフレーム（VLAN ID，宛先 MAC))。

1) storm-control broadcast x

ブロードキャストのフラッディングを行うトラフィックの制御レートを設定します。
この場合の"x"は抑制レート(pps 単位)は、以下の値になります。
1，2，4，8，...，512，1k，2k，4k，...，512k，1024k

2) storm-control multicast x

マルチキャストのフラッディングを行うトラフィックの制御レートを設定します。
この場合の"x"は抑制レート(pps 単位)は、以下の値になります。
1，2，4，8，...，512，1k，2k，4k，...，512k，1024k

3) storm-control unicast x

ユニキャストのフラッディングを行うトラフィックの制御レートを設定します。
この場合の"x"は抑制レート(pps 単位)は、以下の値になります。
1，2，4，8，...，512，1k，2k，4k，...，512k，1024k

39. tacacs-authentication-server コマンド

TACACS+認証サーバを設定します。TACACS+認証サーバは最大 5 つまでサポートします。
コマンドの詳細について、以下を参照してください。

1. "tacacs-authentication-server ?"と入力すると、以下のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# tacacs-authentication-server ?
  <1-5>          Server-Index
  dead-time      Specifies Dead Time of Common Servers
  timeout        Specifies Time Out of Common Servers
-------------------------------------------------------------
```

2. "tacacs-authentication-server x ?"と入力すると、TACACS+認証サーバのコンフィグレーションパラメータが表示されます。この場合の"x"は、サーバのインデックスです。設定可能な範囲の値は「1～5」です。

例："tacacs-authentication-server 1 ?"と入力すると、以下のサブコマンドが表示されます。

```
-------------------------------------------------------------
#tacacs-authentication-server 1 ?
  active         Active the RADIUS server
  host           Specifies the RADIUS server
  key            Sets the RADIUS encryption key
  port           Sets the RADIUS server network port
-------------------------------------------------------------
```

1) tacacs-authentication-server x active
TACACS+認証サーバ"x"を有効にします。
この場合の"x"は、サーバのインデックス番号「1～5」です。

2) tacacs-authentication-server x host y.y.y.y
IP アドレスを TACACS+認証サーバ"x"に割り当てます。
"x" :サーバのインデックス番号「1～5」。
"y.y.y.y" : TACACS+認証サーバ"x"の IP アドレス。

3) tacacs-authentication-server x key yyy
TACACS+認証サーバ"x"にシークレットキー"yyy"を割り当てます。
"x" :サーバのインデックス番号「1～5」です。
"yyy":シークレットキー(最大 29 文字)- TACACS+ 認証サーバおよび本機間で共有します。

4) tacacs-authentication-server x port y
TACACS+認証サーバを使用する TCP ポートを割り当てます。
"x" :サーバのインデックス番号「1～5」です。
"y" :「0～65535」までの UDP ポート番号です。
ポートが「0(zero)」に設定されると、デフォルトのポート(49)が設定されます。

5) tacacs-authentication-server dead-time x
TACACS+認証サーバのデッドタイムを指定します。この場合の"x"は、デッドタイム(0～3600)秒までの値です。デッドタイムは、前回のリクエスト応答に失敗したサーバへ新しいリクエストの送信を中断する時間です。これにより、サーバが停止状態にあると判断し、通信を中断します。
デッドタイムを「0」よりも大きい値に設定すると、この機能が有効になります。但し、複数のサーバが設定されている場合のみこの機能は動作します。

6) tacacs-authentication-server timeout x
TACACS+認証サーバからの応答待ち時間の上限を設定します。サーバがタイムフレーム内に応答しない場合は、休止しているとみなして、次の有効なサーバとの通信を行います(可能な場合)。

40. username コマンド
新規ユーザの作成または既存ユーザの設定変更を行います。

1) username xxx yyy z
新規ユーザのユーザ名・パスワード・レベルの設定を行います。
なお、既存のユーザ名を入力した場合は、そのユーザのパスワードおよびレベルの変更ができます。
"xxx": ユーザ名です。設定可能な文字列の値は「1～31」です。
有効なユーザ名は、文字、数字、アンダースコアの組み合わせで使用します。
"yyy": パスワードです。設定可能な文字列の値は「0～31」です。
"z" : アクセスレベルです。設定可能な範囲は「1～3」です。

ユーザのプライオリティは 3 レベルのプライオリティ(管理者、オペレータ、ゲスト用は、それぞれレベル 3,2,1)です。管理者レベルの場合は、本機のすべての管理を行うことが可能です。
オペレータレベルでは、本機のステータスおよび設定画面を表示し、システムの一部のメンテナンスコマンドを設定することが可能です。

ゲストレベルでは、本機のステータス、設定の表示のみ可能で、setup/configure コマンドは設定できません。

41. vlan コマンド

VLAN データベースコマンドを入力すると、以下の画面が表示されます。

```
------------------------------------------------------------
(config)# vlan database
(config-vlan)#
------------------------------------------------------------------
```

VLAN の設定は、VLAN Config モードにて行います。
詳細については、「VLAN 設定コマンド」を参照してください。

42. voice-vlan コマンド

音声 VLAN 機能を設定します。音声 VLAN 機能により、IP Phone トラフィックの検出、 VLAN（設定可能なトラフィックのプライオリティをもつ）へのトラフィックを自動的に割り当てます。“voice-vlan ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config)# voice-vlan ?
  agetime           Indicates the Voice VLAN secure learning aging
                    time
  oui               Specify hold time multiplier
  traffic-class     Indicates the Voice VLAN traffic class
  vlan-id           Indicates the Voice VLAN ID
  <cr>              Enable Voice VLAN mode operation
-------------------------------------------------------------
```

1) voice-vlan
音声 VLAN 機能を有効にします。“no voice-vlan”コマンドにより、この機能を無効にします。

2) voice-vlan agetime x
音声 VLAN のセキュアラーニングのエージングタイムを設定します。
この場合の“x”は、エージングタイムです。設定可能な範囲は「10～10000000」秒です。セキュリティモード、または自動検出モードが有効な場合に使用します。それ以外の場合は、ハードウェアのエージングタイムにより異なります。実際のエージングタイムは「age_time; 2 * age_time」です。

3) voice-vlan oui add xx-xx-xx
記述なしの OUI エントリを追加します。

4) voice-vlan oui add xx-xx-xx yyy
記述ありの OUI エントリを追加します。
“xx-xx-xx”: 電話通信の OUI アドレス。電話通信の OUI アドレスは、IEEE によりベンダに割り当てられた固有の識別子です。これは 6 文字、かつ入力フォーマットは″xx-xx-xx″(x は 16 進数)です。
“yyy”: OUI アドレス。通常、電話通信装置のベンダーについて記載されます。設定可能な文字列の値は「0～32」です。

5) voice-vlan oui clear
OUI エントリはすべて削除されます。

6) voice-vlan oui delete xx-xx-xx
OUI エントリを削除します。”xx-xx-xx”は、電話通信用の OUI アドレスです。電話通信用の OUI アドレスは、IEEE によりベンダに割り当てられた固有の識別子です。これは「6 文字」、かつ入力フォーマットは″xx-xx-xx″(この場合の”x”は 16 進数)です。

7) voice-vlan traffic-class x
音声 VLAN トラフィックのクラスを設定します。音声 VLAN 上のトラフィックはすべてこのクラスに適用されます。
この場合の“x”は、traffic-class の値(0～7)です。

8) voice-vlan vlan-id x
音声 VLAN の VLAN ID を設定します。この場合の“x”は、VLAN ID(1～4095)です。

1.2.3 インタフェース設定コマンド

“(config)#”プロンプトに続いて、”interface ?”と入力します。
ポートの設定機能および VLAN グループ機能については、以下のように“interface”コマンドで設定を行ってください。

```
-----------------------------------------------------------------
(config)# interface ?
  ethernet          Ethernet port
  vlan              Switch Virtual LAN interface
-----------------------------------------------------------------
```

1) interface ethernet 1/x
Port x の設定を行います。
ポートの設定コマンドについての詳細については、以降の「ポートインタフェース設定コマンド」を参照してください。

2) interface vlan x
VLAN Group x インタフェース(この場合の”x”は VLAN ID)を設定します。
詳細については、「VLAN インタフェース Config コマンド」を参照してください。
このコマンドにより、 VLAN インタフェースに特性を割り当てます。
VLAN インタフェースへの IP アドレスの割り当てを行う場合は、このコマンドを使用してください。

※どちらのコマンドも、“(config)#”から“(config-if)#”プロンプトに移行します。

【注記】:
一般的な VLAN の作成は“vlan database”コマンドにて設定します。
詳細については、「VLAN 設定コマンド」を参照してください。

1.2.3.1 ポートインタフェース設定コマンド

グローバル config モードは、全般的なスイッチの設定を行います。“(config)#とプロンプト表示されます。
ポートの設定を行う場合は、このグローバル config モードにて“interface ethernet 1/x”コマンドを使用して設定を行います。例えば、”interface ethernet 1/5”の場合は、Port 5 に適用されます。

ポートの選択には、以下の指数が含まれます。

1) interface ethernet 1/x の”x”は、ポート番号です。
このコマンドに続く設定は、すべてこのポートに適用されます。

2) interface ethernet 1/x,y,z の“x”,”y”,”z”は、ポート番号です。
例えば、“interface ethernet 1/2,4,7”の場合は、Port 2, Port 4, Port 7 に適用されます。

3) interface ethernet 1/x-y の”x”,”y”は、ポート番号です。
このコマンドに続く設定は、x～yまでの全ポートに適用されます。
例えば、“interface ethernet 1/4-7”の場合は、Port 4～7 に適用されます。

4) interface ethernet 1/w,x,..,y-z の“w”,”x”,”y”,”z”は、ポート番号です。
このコマンドに続く設定は、選択したすべてのポートに適用されます。
例えば、“interface ethernet 1/1,2,4-7”の場合は、Port 1・2, Port 4～7 に適用されます。

(1) ”interface ethernet 1/5”と入力すると、以下のように表示されます。

```
-------------------------------------------------------
(config)# interface ethernet 1/5
(config-if)#
-------------------------------------------------------
```

(2) ”?”と入力すると、以下のようにサブコマンドが表示されます。

```
-------------------------------------------------------------
 (config-if)# ?
  exit           Exit from current mode
  help                 Show available commands
  history        Show a list of previously run commands
  logout         Disconnect
  quit           Quit commands
  acl            Access Control List Configuration
  arp-inspection Set ARP inspection configuration
  channel-group  Adds ports to a trunk
  clear          Clears the counters
  description    Interface specific description
  dhcp-snooping  Configures DHCP Snooping Configuration
  dot1x          Configures 802.1x port-based access control
  eee            Set the eee mode
  end            Exit from interface mode
  excessive      Configure port transmit collision behavior
  flowcontrol    Enables flow control during autoneg
  interface      Enters privileged interface configuration
  ip             Global IP configuration sub commands
  ip-source-guard      IP Source Guard Configuration
  lacp           Configures LACP status
  lldp           Configures lldp
```

```
 loopback-detection   Configures loopback detection
 mac-learn      mac learn
 maximum-packet-length  Configures the maximum packet
                  length of the port
 mdi/mdi-x      Set MDI crossover
 mvr            Multicast VLAN Registration
 no             Negates a command or sets its defaults
 poe            Power Over Ethernet
 port           Configures the characteristics of the port
 power-control  Decrease energy consumption
 private-vlan   Configures Port-Based VLAN
 qos            Configuration of QoS
 sflow          configured sFlow samplers
 shutdown       Shuts down the selected interface
 spanning-tree  Specifies spanning tree configuration
 speed          Configures speed operation
 switchport     Configures switching mode characteristics
 voice-vlan     Voice VLAN Configuration
-------------------------------------------------------------
```

1. exit コマンド

現在のオペレーションモードを終了し、前のモードに戻ります。

2. help コマンド

このコマンドモードで使用可能なコマンドをすべて表示します。

3. history コマンド

入力したコマンドの履歴を表示します。

4. logout コマンド

コンソール画面からログアウト時に使用します。

5. quit コマンド

コンソール画面を終了時に使用します。ログアウトと同じ機能です。

6. acl コマンド

インタフェースポートのACLパラメータ(ACE)を設定します。フレームが特定のACEと一致しない場合は、これらのパラメータに応じてフレームの受信が有効/無効になります。

1. "acl ?"と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# acl ?
action          Select whether forwarding is permitted or
          denied
logging         Logging operation of this port
mirror          Mirror operation of this port
policy          Select the policy to apply to this port
```

```
port-redirect   Select which port frames are copied on
rate-limiter    Select which rate limiter to apply on this port
shutdown        Shut down operation of this port
state           Specify the port state of this port.
-------------------------------------------------------------
```

1) acl action [deny | permit]
ポートのデータ伝送が許可(″permit″)、または拒否(″deny″)されます。

2) acl logging
ポートで受信したフレームを System Log に保存する設定を有効にします。 “no acl logging“コマンドにより、無効になります。

【注記】:System Log のメモリサイズおよログレートは制限されますので、ご注意ください。

3) acl mirror
ポートで受信したフレームをミラーリングする設定を有効にします。“no acl mirror”コマンドにより、この機能を無効にします。

4) acl policy x
ACL の Policy x グループに設定します。この場合の“x”は、ポリシーID(0～255)です。

5) acl port-redirect [disable | 1/x]
ポートのトラフィックリダイレクト機能を設定します。無効またはリダイレクトする特定のポート(“1/x”は”1/x 1/x,y,z 1/x-y 1/x-y,z”(複数ポート))を指定できます。この場合の”x”は、ポート番号です。
アクションが許可されている場合は、設定できません。

6) acl rate-limiter [disable | x]
ポートのレートリミット機能を設定します。
無効、またはレートリミット ID のいずれかを指定できます。

7) acl shutdown
ポートのシャットダウン機能を有効にします。フレームを受信すると、ポートは無効になります。
”no acl shutdown”により、この機能を無効にします。

8) acl state
ポートの状態を指定します。“acl state”により、ポートを有効にします。“no acl state”により、ポートを無効にします。

7. arp inspection コマンド

ポートの ARP インスペクション機能を設定します。

“arp inspection ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# arp inspection ?
  entry   add arp inspection static entry
  mode    set show the arp inspection port mode
-------------------------------------------------------------
```

1) arp inspection entry vid x mac yy-yy-yy-yy-yy-yy ip <ip address>

ポートのスタティック ARP エントリを設定します。この場合の“x”は、VLAN ID(1～4095)です。“yy-yy-yy-yy-yy-yy”は、ARP リクエストパケットの有効な Source MAC アドレスです。

<ip address>は、ARP リクエストパケットの有効な送信元 IP アドレスです。“no ARP Inspection entry vid x mac yy-yy-yy-yy-yy-yy ip <ip address>“により、エントリを削除します。

2) arp inspection mode

ポートの ARP インスペクション機能を有効にします。“no ARP Inspection mode”コマンドにより、この機能を無効にします。

【注記】:
ダイナミック ARP エントリは DHCP リクエストから学習します。ARP インスペクションを有効にする前に、DHCP スヌーピング機能をまず有効にしてください。
それ以外は、本 ARP インスペクション機能で、スタティック ARP エントリを設定してください。

8. channel-group コマンド

インタフェースポートをアグリゲーショングループに設定します。これは、スタティックアグリゲーショングループの割り当てです。アグリゲーションの通信モードは全二重のみで、グループに入るすべてのポートは同じ通信速度に設定してください。

- channel-group x

トランクグループ“x”にポートを追加します。この場合の“x”は、トランクグループ番号です。設定可能な範囲の値は「1～5」です。no channel-group コマンドにより、トランクグループからポートを取り除きます。

【注記】:アグリゲーション機能は 2 つのポート以上 10 ポート以内で設定してください。

9. clear コマンド

ポートのカウントをクリアにします。

“clear ?”と入力すると、次のサブコマンドが表示されます。

```
-----------------------------------------------------------
(config-if)# clear ?
interface           interface counters
loopback-detection  loopback-detection counters
-----------------------------------------------------------
```

1) clear interface counters

インタフェースのカウンターをクリアします。

2) clear loopback-detection status

ループバック機能のステータスカウンターをクリアします。

10. description コマンド

インタフェース名を設定します。各ポートに文字を記述することができます。

11. dhcp-snooping コマンド

ポートの DHCP スヌーピング機能を設定します。また本機能をポートで trusted/untrusted に設定します。

1) dhcp-snooping mode [untrusted | trusted]
DHCP メッセージのソース用のポートを”trusted”、または”untrusted”に設定します。

2) dhcp-snooping statistics clear
DHCP スヌーピングのポートの統計情報をクリアにします。

12. dot1x コマンド

ポートの 802.1x 機能を設定します。

“dot1x ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# dot1x ?
  authenticate   Refresh(restart) 802.1X authentication
          process
  clear          Clear 802.1X statistics
  guest_vlan     Guest VLAN Enabled
  port-control   Needs dot1x-aware client RADIUS server
          authentication
  radius-qos     RADIUS Assigned QoS Enabled
  radius-vlan    RADIUS Assigned VLAN Enabled
------------------------------------------------------------
```

1) dot1x authenticate
ポートの待機時間が過ぎた時の再認証のスケジューリングを行う設定をします(EAPOL ベース認証)。
MAC ベース認証の場合は、すぐに再認証を行います。このコマンドは、正しく認証されたクライアントにのみに有効です。このコマンドは、認証がグローバル config モードで設定され、かつポートの Admin State が EAPOL ベース、または MAC ベース認証モードの場合のみ有効です。

2) dot1x authenticate now
ポートのクライアントの再初期化を行うとともに即時再認証を行います。
クライアントは、再認証中は未認証の状態になります。
このコマンドは、認証がグローバル config モードで設定され、かつポートの Admin State が EAPOL ベース、または MAC ベース認証モードの場合のみ有効です。

3) dot1x clear
ポートの 802.1X 統計情報をクリアにします。

4) dot1x guest_vlan
ポートのゲスト VLAN 機能を有効にします。
“no dot1x guest_vlan“コマンドにより、この機能を無効にします。
ゲスト VLAN 機能は、ゲスト VLAN がグローバル config モードで有効に設定され、かつ設定したポートで有効な場合に動作します。このコマンドは、下記の EAPOL ベースモードでのみ有効です。

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

5) dot1x port-control [auto | force-authorized | force-unauthorized | mac-based | multi-802.1x | single-802.1x]

ポートの 802.1X オペレーションモードを選択します。

オペレーションモードの詳細については、以下のとおりです。

❒ auto:

dot1x-aware クライアントの RADIUS サーバ認証が必要です。このモードにより、ポートを“Port-based 802.1X”モードに設定します。

❒ force-authorized:

クライアントすべてのアクセスを許可できるよう設定します。
このモードでは、ポートがリンクアップすると、EAPOL Success フレームを送信し、すべてのクライアントによるネットワークアクセスが認証なしに許可されます。

❒ force-unauthorized:

すべてのクライアントへのアクセスを拒否するよう設定します。
このモードでは、ポートがリンクアップすると、EAPOL Failure フレームを送信し、すべてのクライアントによるネットワークアクセスが無効になります。

❒ mac-based:

ポートを MAC ベース認証に設定します。MAC ベース認証は、ポートベース 802.1X とは異なり標準的なものではありませんが、最良の方法として業界で採用されています。
MAC ベース認証の場合、ユーザは“クライアント”と呼ばれ、本機は、クライアントの代わりにサプリカントとして動作します。
クライアントによって送信された初期フレーム(フレームすべて)は本機によってスヌーピング(読み取り)され、クライアントの MAC アドレスをユーザ名とパスワードの両方に変換して RADIUS サーバに EAP 認証を行います。
6 バイトの MAC アドレスは、″xx-xx-xx-xx-xx-xx″の形式で記載し、小文字の 16 進数をハイフン(-)で区切ります。MD5 認証方式のみのサポートの為、RADIUS サーバも「MD5」に設定してください。
認証が完了すると、RADIUS サーバは成功/失敗の結果を送信し、この結果をもとに特定のクライアントのトラフィックを有効/無効にします。クライアントからスイッチへのフレームは送信されます。

この認証には EAPOL フレームは含まれないため、MAC ベース認証は 802.1X 規格とは関係ありません。
MAC ベース認証を利用する利点は、802.1X ベース認証と違いクライアントは認証用のサプリカントソフトウェアをは必要としないことです。
一方、欠点としては悪意のあるユーザによって MAC アドレスが偽装されても、MAC アドレスが有効であれば RADIUS ユーザとして誰でもネットワークに接続できてしまうことです。
また、MD5-Challenge 方式もサポートされています。ポートにアクセス可能な最大クライアント数は、ポートセキュリティのリミットコントロールによって制限することが可能です。

❒ multi-802.1x :
同じポート上で同時に 1 つ以上のサプリカントの認証が可能です。
Multi 802.1X は、Single 802.1X と同様に、IEEE 規格ではありませんが、同様の機能を多く備えています。Multi 802.1X の場合、同じポート上で同時に複数のサプリカントの認証が可能です。各サプリカントはそれぞれに認証され、ポートセキュリティを介して MAC テーブルに設定されます。
Multi 802.1X では、サプリカントはすべてポートに接続されてしまうため、本機からサプリカントに送信した EAPOL フレームの宛先 MAC アドレスとして、マルチキャスト BPDU の MAC アドレスを使用することはできません。
その代わりに、サプリカントから送信された最初の EAPOL Start フレーム、または EAPOL Response Identity フレームから取得したサプリカントの MAC アドレスを使用します。この場合、本機は宛先アドレスとして、BPDU マルチキャストの MAC アドレスを使って、EAPOL Request Identity フレームを送信します（ポート上のサプリカントを起動させるため）。
ポートに接続可能なサプリカントの上限は、ポートセキュリティのリミットコントロールにより制限することが可能です。

❒ single-802.1x:
ポートベースの 802.1X 認証については、サプリカントがポート上で一度正しく認証されると、ネットワークトラフィックに対してポート全体がオープンになります。これにより、認証されない場合でも、ポートに接続されたクライアント（例えば、ハブを介して）は正しく認証されたクライアント上で合致可能になり、認証されない場合でもネットワークアクセスを行います。セキュリティの違反を制御するには、シングル 802.1X 変数を使用します。
シングル 802.1X は、IEEE 規格ではなく、機能の多くはポートベースの 802.1X と同じ特性です。シングル 802.1X の場合は、ほとんど場合、サプリカントは一度に1つずつポート上で認証を行います。EAPOL フレームは、サプリカント/スイッチ間の通信に使用されます。複数のサプリカントがポートに接続されている場合は、ポートリンクがついている場合は、最初のポートとみなされます。サプリカントが特定の時間内で有効な証明書を提供しない場合は、その他のアプリカントがそのチャンスを得ます。
サプリカントが正しく認証されるとアクセスを許可し、サポートされているモードすべてのセキュリティが高くなります。この場合、ポートセキュリティモードを使用して、サプリカントの MAC アドレスを確保します。

❒ dot1x radius-qos
RADIUS に割り当てられた QoS 機能を有効にします。また“no dot1x radius-qos“コマンドにより、この機能は無効になります。RADIUS に割り当てられた QoS がグローバルモードおよびポート単位の両方で有効な場合は、一度サプリカントが正しく認証されると、RADIUS サーバにより RADIUS Access-Accept パケットが送信され、そのパケットの QoS クラス情報によって処理を行います。サプリカントポート上で受信したトラフィックは、指定の QoS クラスに分けられます。再認証に失敗したり、RADIUS Access-Accept パケットが QoS クラスに対応していなかったり、無効な場合、またはサプリカントがポート上に存在しない場合は、ポートの QoS クラスは、元の QoS クラス（ある一定時間 RADIUS に影響なく、管理者によって変更可能）に直ちに戻されます。
このオプションは、single-client モードでのみ有効です。
・Port-based 802.1X
・Single 802.1X

❒ dot1x radius-vlan

RADIUS 対応の VLAN 機能を有効にします。“no dot1x radius-vlan“コマンドにより、この機能は無効になります。

RADIUS 対応 VLAN がグローバル config モードおよびポート単位で有効な場合、本機は、サプリカントが正しく認証されると、RADIUS サーバにより RADIUS Access-Accept パケットが送信され、そのパケットの VLAN ID によって処理を行います。ポートの Port VLAN ID がこの VLAN ID に変更されると、そのポートは VLAN ID のメンバーに設定され、ポートは強制的に VLAN unaware モードになります。一度割り当てられると、ポートで受信したトラフィックはすべてクラス分けされ、RADIUS 対応の VLAN ID に変換されます。

このオプションは、single-client モードでのみ有効です。

・Port-based 802.1X

・Single 802.1X

12. eee コマンド

省電力機能である EEE(Energy Efficient Ethernet)機能(IEEE 802.3az にて定義)をポートで有効にします。

“eee ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# eee ?
queue-list          Queue list
<cr>                Enable eee
------------------------------------------------------------
```

1) eee

ポートのこの機能を有効にします。“no eee”コマンドにより、この機能を無効にします。

2) eee queue-list

すべてのキューを EEE Urgent キューに設定します。

“no eee queue-list“コマンドにより、EEE Urgent キューからすべてのキューを解除します。

EEE Urgent キューは、キューのセットで、データが有効になるとすぐにフレームの送信を行います。

それ以外は、キューは 3000 バイトが送信可能な状態になるまで待機します。

3) eee queue-list [x | x,y,z | x-y]

EEE Urgent Queues のキューを割り当てます。

[x | x,y,z | x-y] : キュー番号(1～8)

“x” : シングルキュー

“x,y,z” : キューリスト

“x-y” : キューの範囲

この設定を行うことで、既存の設定は消去されます。“no eee queue-list“コマンドにより、EEE Urgent キューリストからすべてのキューを解除します。

13. end コマンド

現在設定しているモードを終了します。

```
------------------------------------------------------------
(config-if)# end
(config)#
```

```
------------------------------------------------------------
```

14.excessive コマンド

半二重モードで、過度のコリジョンが発生した場合の動作を設定します。

“excessive ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# excessive ?
discard     Discard frame after 16 collisions
restart     Restart backoff algorithm after 16 collisions
------------------------------------------------------------
```

・excessive [discard | restart]
半二重モードで過度なコリジョンが発生した場合の動作を設定します。
- discard: 16 個のコリジョンが発生すると、フレームを破棄します。
- restart: 16 個のコリジョンが発生すると、バックオフ方式を再開します。

15. flowcontrol コマンド

ポートのフロー制御を有効にします。
”no flowcontrol”コマンドにより、フロー制御を無効にします。

16. Interface コマンド

連続してセットアップできるよう現在のポートから次のポートへすぐ移るためのコマンドです。
例:

```
------------------------------------------------------------------
(config-if)# interface ?
  ethernet Ethernet port
(config-if)# interface ethernet ?
<1-10>  Unit number: format 1/x   1/x,y,z  1/x-y    1/x-y,z
------------------------------------------------------------------
```

例:

- “(config)# interface ethernet 1/5”と入力すると、現在の設定を Port 5 に設定し、コマンドはすべて Port 5 に適用されます。

- “(config-if)# interface ethernet 1/6-7”は、現在の設定を Port 6-7 に設定し、コマンドはすべて Port 6-7 に適用されます。

詳細については、「インタフェース設定コマンド」を参照してください。

17. ip コマンド

ポートの IGMP/MLD スヌーピング機能を設定します。

“ip ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# ip ?
igmp            IGMP protocol
mld             mld Snooping
------------------------------------------------------------
```

(1) ip igmp snooping fastleave/ip mld snooping fastleave

ポートの fast-leave 機能を有効にします。“no ip igmp snooping fastleave“/“no ip mld snooping fastleave“コマンドにより、この機能を無効にします。マルチキャストスヌーピングの Fast Leave 処理は、グループ固有のクエリを先にインタフェースに送信することなく、インタフェースから forwarding-table エントリを削除できます。VLAN インタフェースは、元の leave メッセージに指定されているマルチキャストグループのマルチキャストツリーから削除されます。Fast-leave 処理は、複数のマルチキャストグループを同時に使用する場合でも、ネットワーク上のホストの帯域を最適な状態に確保します。この方法は、IGMP および MLD に適用されます。

(2) ip igmp snooping filtering group_addrress xxx / ip mld snooping filtering group_addrress xxx

IGMP/MLD フィルタリンググループを追加します。この場合の“xxx”は IP マルチキャストアドレスです。

no ip igmp snooping filtering group_addrress xxx / no ip mld snooping filtering group_addrress xxx コマンドにより、IGMP/MLD フィルタリンググループを削除します。

(3) ip igmp snooping router/ip mld snooping router

IGMP/MLD スヌーピングのルーターポートに設定します。”no ip igmp snooping router”/”no ip mld snooping router“コマンドにより、ルーターポート以外に設定します。ルーターポートは、レイヤ 3 のマルチキャストデバイス、または IGMP/MLD クエリアに向けて繋がる Ethernet スイッチ上のポートです。アグリゲーションメンバーポートをルーターポートに設定する場合は、アグリゲーション全体がルーターポートとして動作します。

(4) ip igmp snooping throttling [unlimited | x]/ip mld snooping throttling [unlimited | x]

ポートのマルチキャストグループ数を制限します。“unlimited”、または”x”（1～10）です。

18. ip-source-guard コマンド

IP ソースガード機能を設定します。

“ip-source-guard ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# ip-source-guard ?
  entry       Add IP Source Guard static entry
  limit       maximum number of dynamic clients that can be learned
  mode        Set show the IP Source Guard port mode
-------------------------------------------------------------
```

1) ip-source-guard entry vid x mac yy-yy-yy-yy-yy-yy ip <IP Address>

ポートにスタティックエントリを追加します。
”x”: VLAN ID(1～4095)
“yy-yy-yy-yy-yy-yy”: MAC アドレス
“no ip-source-guard entry vid x mac yy-yy-yy-yy-yy-yy ip <IP Address>“コマンドにより、エントリを削除します。

2) ip-source-guard limit [unlimited | x]

指定ポートで学習可能なダイナミッククライアントの最大数を設定します。値は、“unlimited”、または”x”(0～2)です。ポートモードが有効、かつダイナミッククライアントの最大値が「0」の場合、特定ポートのスタティックエントリに一致するよう IP パケットフォワーディングを行います。

3) ip-source-guard mode

ポートの機能を有効にします。“no ip-source-guard mode”コマンドにより、この機能を無効にします。

【注記】:
Dynamic IP Source エントリは、DHCP リクエストから学習します。IP ソースガードを有効にする前に、DHCP スヌーピング機能をまず有効にしてください。それ以外は、IP ソースガードに対してスタティック IP エントリを設定します。

19. lacp コマンド

ポート上で動作している LACP プロトコルを設定します。

“lacp ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# lacp ?
  Clear       Clear LACP Statistics
  key         The Key value incurred by the port
  mode        LACP enabled
  priority    Priority of the port
  role        LACP activity status
  timeout     The Timeout controls the period between  LACP
              transmissions
-------------------------------------------------------------
```

1) lacp clear

LACP 統計情報をクリアにします。

2) lacp key [auto | specific x]

ポートごとの key 値を指定します。
“auto”に設定した場合、物理上のリンク通信速度(10Mb = 1, 100Mb = 2, 1Gb = 3)によって key は適切な値に設定されます。“specific”に設定した場合、ユーザにより設定された値”x”(1～65535)を入力します。
同じ Key 値をもつポートは、同一のアグリゲーションググループに追加されますが、異なる Key をもつポートは追加できません。

3) lacp mode

ポートの LACP 機能を有効にします。“no lacp mode”コマンドにより、この機能を無効にします。

4) lacp priority x

ポートの LACP プライオリティを設定します。LACP パートナーが本デバイスでサポート可能なグループより大きくなる場合は、このパラメータを設定することでどのポートが動作中か、バックアップ状態かを制御します。
値が小さいほど、プライオリティが高くなります。

5) lacp role [active | passive]

LACP オペレーションに対するポートの役割を設定します。
“active”に設定すると、毎秒ごとに LACP パケットを送信しますが、“passive”に設定すると、パートナーからの LACP パケットの受信を待ちます(応答があった場合)。

6) lacp timeout [fast | slow]

LACP 送信間の時間を制御するためにタイムアウトを設定します。
“fast”に設定すると、毎秒単位で LACP パケットを送信しますが、“slow”に設定すると、LACP パケット送信間隔は「30 秒間」ごとになります。

20. lldp コマンド

ポートの LLDP 機能を設定します。

“lldp ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# lldp ?
Clear     Clear LLDP Statistics
disable   Configure to disable the port in a LLDP State
enable    Configure to enable rx_and_tx the port in a LLDP
          State
rx-only   Configure to rx_only the port in a LLDP State
tx-only   Configure to tx_only the port in a LLDP State
cdp-aware Select CDP awareness
port-description    Port capability is included in LLDP
                    information transmitted
system-name         System name is included in LLDP
                    information transmitted
system-description  System description is included in LLDP
                    information transmitted
system-capabilities  System capability is included in LLDP
                    information transmitted
management-address  management address is included in LLDP
                    information transmitted
```

---

1) lldp clear

LLDP 統計情報をクリアにします。

2) lldp [disable | enable | rx-only | tx-only]

ポートの LLDP オペレーションモードを設定します。

- disable: ポートの LLDP オペレーションを無効にします。
  本機は、LLDP 情報を送信せず、ネイバー装置から受信した LLDP 情報を破棄します。
- enable: ポートの LLDP オペレーションを有効にします。
  本機は LLDP 情報を送信し、ネイバー装置から受信した LLDP 情報を解析します。
- rx-only: LLDP オペレーションに対して Receive-Only に設定します。
  本機は LLDP 情報を送信しませんが、ネイバー装置から受信した LLDP 情報を解析します。
- tx-only: LLDP オペレーションに対して、Transmit-Only に設定します。
  本機は、ネイバー装置から受信した LLDP 情報を破棄しますが、LLDP 情報を送信します。

3) lldp cdp-aware

CDP-Aware 機能を有効にします(CDP は“Cisco Discovery Protocol”を指します) 。
“no lldp cdp-aware”コマンドにより、この機能を無効にします。
CDP オペレーションは受信した CDP フレームのデコード(復号化)に制限があります(本機から CDP フレーム送信はできません)。CDP フレームは、ポートの LLDP が有効な場合のみデコーディングされます。
CDP TLVs は LLDP ネイバーテーブルに対応するフィールドにマッピングした場合のみデコード(復号化)されます。
それ以外の TLVs はすべて破棄されます(認識不可能な CDP TLVs および破棄された CDP フレームは LLDP 統計情報には表示されません)。
CDP TLVs は LLDP ネイバーテーブルに下記のようマッピングします。

- CDP TLV の”Device ID: LLDP の″Chassis ID″に表示されます。
- CDP TLV の”Address″ : LLDP の″Management Address″にマッピングします。
  CDP アドレスの TLV には複数のアドレスが含まれますが、最初のアドレスのみ LLDP ネイバーテーブルに表示されます。
- CDP TLV の”Port ID″: LLDP の″Port ID″にマッピングします。
- CDP TLV の”Version and Platform″: LLDP の″System Description″フィールドにマッピングします。
- CDP と LLDP の両方にサポートされているシステムの機能
  LLDP 機能では、CDP 機能を部分的にしかカバーしていません。このため、LLDP ネイバーテーブルでは″others″と表示されます。

【注記】:
すべてのポートの CDP awareness が無効な場合は、本機はネイバー装置からの受信した CDP フレームを転送します。少なくとも一つのポートの CDP awareness が有効な場合は、CDP フレームは本機で終端します。

4) lldp port-description

送信された LLDP 情報に含まれる“port description”を有効にします。
“no lldp port-description“コマンドにより、この機能を無効にします。

5) lldp system-name
送信された LLDP 情報に含まれる“system name”を有効にします。
“no lldp system-name“コマンドにより、この機能を無効にします。

6) lldp system-description
送信された LLDP 情報に含まれる”system description”を有効にします。
“no lldp system-description“コマンドにより、この機能を無効にします。

7) lldp system-capabilities
送信された LLDP 情報に含まれる”system capabilities”を有効にします。
“no lldp system-capabilities“コマンドにより、この機能を無効にします。

8) lldp management-address
送信された LLDP 情報に含まれる“management address”を有効にします。
”no lldp management-address“コマンドにより、この機能を無効にします。

21. loopback-detection コマンド

ポートのループバック検知機能を設定します。

“loopback-detection ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# loopback-detection ?
action          Set the Loop Protection port action
mode            Set the Loop Protection port mode
transmit        Set the Loop Protection port transmit mode
-------------------------------------------------------------
```

1) loopback-detection action [log | shutdown | shut_log]
ポートでループを検知した場合の動作を設定します。
“有効な値は、“shutdown”(ポートをシャットダウンする)，”shut_log”(ポートをシャットダウンし、ログを送信する)または“log”(ログ送信のみ)です。

2) loopback-detection mode
ポートのループ検知機能を有効にします。“no loopback-detection mode”コマンドにより、この機能を無効にします。

3) loopback-detection transmit
ループ検知機能の送信モードを有効にします。
“no loopback-detection transmit”コマンドにより、この機能を無効にします。送信モードにより、ループプロテクションの PDU を送信するかどうかを設定します。

22. mac-learn コマンド

ポートの MAC アドレスの学習機能を設定します。

“mac-learn ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# mac-learn ?
auto      Learning is done automatically
disable   No learning
secure    static MAC entries are learned,all other are dropped.
------------------------------------------------------------
```

- `mac-learn [auto | disable | secure]`
  ポートの MAC アドレス学習機能を設定します。
  - auto : 未学習な送信元 MAC をもつフレームを受信すると、自動的に学習を行います。
  - disable: 学習が行われません。
  - secure : スタティック MAC エントリのみを学習し、その他のフレームはすべて破棄されます。

  【注記】:
  本機の管理用に使用するリンクが学習モードを変更する前に、スタティック MAC テーブルに追加されたかどうか確認します。それ以外は、マネジメントリンクが切れてしまうか、その他の non-secure ポートによって使用されるか、シリアルインタフェースを介して本機に接続することによってのみリストアすることができます。

  本モードを変更する前に本機の管理に使用するリンクがスタティック MAC テーブルに追加されているか確認してください。先に設定してしまうと管理リンクが切れてしまいます。復旧させるには他のポートを使用するか、シリアルポートでの接続を行ってください。

23. maximum-packet-length コマンド

ポートの最大パケットサイズを設定します。

- `maximum-packet-length x`
  ポートの最大パケットサイズを設定します。この場合の“x”は、最大パケットサイズ(「1518～9600」までの値)です。

24. mdi/mdi-x コマンド

ポートの MDI/MDI-X モードを設定します。

“mdi/mdi-x ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# mdi/mdi-x ?
auto      AUTO-MDI
mdi       Force MDI
mdi-x     Force MDI-X
------------------------------------------------------------
```

- mdi/mdi-x [auto | mdi | mdi-x]
  ポートの MDI/MDI-X モードを設定します。
  “mdi”は、Hub/Switch 接続用、“mdi-x”は、PC 接続用、“auto”は、接続の自動検知を行うことが可能です。

25. mvr コマンド

ポートの MVR 機能を設定します。

“mvr ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# mvr ?
immediate-leave    Enable the fast leave on the port.
vlan               MVR VLAN ID
------------------------------------------------------------
```

1) mvr immediate-leave
ポートの fast leave を有効にします。”no mvr immediate-leave“コマンドにより、この機能を無効にします。

2) mvr vlan x [inactive-port | receiver-port | source-port]
MVR VLAN のポート“x”の動作を設定します。この場合の”x”は、MVR VLAN ID(「1～4095」までの値)です。
- inactive-port : 指定ポートは MVR を行いません。
- receiver-port : 加入者ポート、かつマルチキャストデータの受信のみを行う場合は、ポートをレシーバーポートとして設定します。IGMP/MLD メッセージを発行することにより、マルチキャストグループのメンバになる場合以外は、データの受信は行いません。
- source-port : ソースポートとしてマルチキャストデータの送受信を行うアップリンクポートを設定します。加入者は直接ソースポートに接続することはできません。

【注記】: MVR ソースポートを、管理用 VLAN ポートと重複することは推奨されません。

26. no コマンド

機能を無効にするか、設定値を工場設定値に戻します。

“no ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# no ?
acl                     Access Control List Configuration
arp-inspection          Set ARP inspection configuration
channel-group           Adds ports to a trunk
description             Interface specific description
dhcp-snooping           Configures DHCP Snooping Configuration
dot1x                   Configures 802.1x port-based access
                        control
eee                     Set the eee mode
excessive               Configure port transmit collision
                        behavior
flowcontrol             Enables flow control during autoneg
ip                      Global IP configuration sub commands
ip-source-guard         IP Source Guard Configuration
lacp                    Configures LACP status
lldp                    Configures lldp
loopback-detection      Configures loopback detection
mac-learn               Configures the maximum packet length of
                        the port
maximum-packet-length   Configures the maximum packet length of
                        the port
mdi/mdi-x               Set MDI crossover
mvr                     Multicast VLAN Registration
poe                     Power Over Ethernet
port                    Configures the characteristics of the
                        port
power-control           Decrease energy consumption
private-vlan            Configures Port-Based VLAN
qos                     Configuration of QoS
sflow                   configured sFlow samplers
shutdown                Shuts down the selected interface
spanning-tree           Specifies spanning tree configuration
speed                   Configures speed operation
switchport              Configures switching mode
                        characteristics
voice-vlan              Voice VLAN Configuration
------------------------------------------------------------
```

例として、”no lacp mode”コマンドを入力した場合は、ポートの LACP 機能が無効となります。
また、”no maximum-packet-length”と入力した場合は、初期設定値「9600」に戻します。

27. poe コマンド

ポートの PoE 機能を設定します。

“poe ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# poe ?
  auto-checking    Setting POE auto checking
  mode             PoE mode
  power            Setting maximum power for port in  allocation
                   mode
  power-delay      Setting POE power delay
  priority         Interface priority
  scheduling       Setting POE scheduling
-------------------------------------------------------------
```

1) poe auto-checking

接続されている PoE 機器の接続確認を有効にします。
“no poe auto-checking”でこの機能を無効にできます。
グローバル Config モードにてこの機能を有効に設定した後、“(config-if)#”プロンプトにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

2) poe auto-checking failure-action xxx

受電側機器からの応答がない場合の動作を設定します。
“xxx”は、“nothing”、または“reboot-remote-pd”のいずれかになります。
“reboot-remote-pd”を設定すると(受電側機器から応答がない場合に)、本機は“reboot-time”の PoE の給電を中止し、受電側機器を再起動します。

3) poe auto-checking interval-time x

ping の間隔を設定します。この場合の“x”は、「10～120 秒」までの値となります。

4) poe auto-checking ping-ip-address x.x.x.x

受電側機器の IP アドレスを設定します。この場合の“x.x.x.x”は、IP アドレスです。

5) poe auto-checking reboot-time x

ping に失敗した場合、PoE の給電の中断時間を設定します。この場合の“x”は、「3～120」秒までの値となります。

6) poe auto-checking retry-time x

受電側機器からの応答のない場合の再試行回数を設定します。この場合の“x”は、「1～5」までの値となります。

7) poe mode xxx

ポートの PoE オペレーションモードを設定します。”xxx”は、以下の値のいずれかになります。
- disabled: PoE 機能を無効にします。
- plus : オペレーションモードを「PoE+」に設定します(最大出力:30.0W)。
- standard : オペレーションモードを「PoE」に設定(最大出力:15.4W)。

8) poe power limit x

allocation モードでのポートの最大出力を設定します。
この場合の“x”は、インタフェースの最大出力です(「0-15.4W」※PoE 標準モードの場合、「0-30.0W」※PoE+モードの場合)。

9) poe power-delay mode
本機の電源を「ON」にした後の PoE 給電の遅延機能を有効にします。“no poe power-delay mode“により、無効になります。

10) poe power-delay time x
本機の電源を「ON」にした後の PoE 給電の遅延時間を設定します。この場合の“x”は、「0～300 秒」までの値となります。

11) poe priority xxx
インタフェースの PoE プライオリティを設定します。“xxx”は、以下の値のいずれかになります。
- critical : プライオリティを”critical”に設定します。
- high : プライオリティを”high”に設定します。
- low : プライオリティを”low”に設定します。

12) poe scheduling mode
PoE 給電のスケジュール機能を有効にします。“no poe scheduling mode”コマンドにより無効になります。

13) poe scheduling hour x yyy
PoE 給電スケジュールを設定します。
“x” : 時間を表し、「0～23」までの値となります。
“yyy” : 曜日を表し、”monday,tuesday,Wednesday,thursday,friday,saturday,Sunday”で表記されます。

28. port コマンド

ポートのモニター機能、またはセキュリティ機能を設定します。

```
------------------------------------------------------------
(config-if)# port ?
  monitor        Monitors another interface
  security       Specifies port security
------------------------------------------------------------
```

1) port monitor
ポートのモニター機能を設定します。

“port monitor?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# port monitor ?
  cpu            CPU port
  ethernet       Ethernet port
------------------------------------------------------------
```

(1) port monitor cpu [disabled | enabled | rx | tx]
モニタを行うポートのリストに“cpu”を追加します。“no port monitor cpu”コマンドにより、リストから cpu のモニタを削除します。
- disabled:送信/受信フレームのミラーリングを行いません。
- enabled :ミラーポートで送受信フレームのミラーリングを行います。
- rx: 受信したフレームのみミラーリングをミラーポートで行います。
- tx: 送信フレームのみミラーリングをミラーポートで行います。

(2) port monitor ethernet 1/x [disabled | enabled | rx | tx]

モニタを行うポートのリストに“Port x”を追加します。“no port monitor ethernet 1/x”コマンドにより、リストから Port x のモニタを削除します。
この場合の”x”は、モニタリングを行うポート番号（1/x, 1/x,y,z, 1/x-y, 1/x-y,z.と記述）を表します。
- disabled:送信/受信フレームのミラーリングを行いません。
- enabled :ミラーポートで送受信フレームのミラーリングを行います。
- rx: 受信したフレームのみミラーリングをミラーポートで行います。
- tx: 送信フレームのみミラーリングをミラーポートで行います。

2) port security

ポートセキュリティ機能を設定します。

(1) port security action [none | shut | trap | trap_shut]

ポートセキュリティに違反した場合は、以下の処理を行います。
- none: 制限に達しても、何の処理も行いません。
- shut: 制限に達すると、ポートをシャットダウンします。
- trap: 制限に達すると、SNMP トラップを送信します。
- trap_shut: 制限に達すると、SNMP トラップを送信し、ポートをシャットダウンします。

(2) port security max-mac-count x

このポートで設定可能な MAC アドレスの最大値を設定します。この場合の”x”は MAC アドレスの最大値(1～1024)です。例えば、x=5 はこのポートでネットワーク機器または PC アクセスネットワークを最大 5 つまで許可します。ポートセキュリティは有効なポートに新しい MAC アドレスが表示されると、すべてのポートの MAC アドレスの総数が書き換えられます。同じプールからすべてのポートへ書き換えられた場合、残りのポートで既に使用可能な MAC アドレスを使用されていると、設定した最大値が適用できない場合があります。

(3) port security mode

このポートのリミットコントロールを有効にします。“no port security mode“コマンドにより、この機能を無効にします。
【注記】: まず本機能をグローバル Config モードにて有効に設定し、その後本コマンドにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

(4) port security reopen

ポートのセキュリティ機能によってシャットダウンされたポートを解除します。

29. power-control コマンド

ポートの省電力機能を設定します。

“power-control ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# power-control ?
actiphy                 Link down power savings enabled
disable                 Disable all power control
perfectreach            Link up power savings enabled
enable                  Both link up and link down power savings
-------------------------------------------------------------
```

- power-control [actiphy | disable | perfectreach | enable]

  ポートの省電力モードを設定します。
  - actiphy :ポートがリンクダウン状態の場合に省電力モードを有効にします。
  - disable :省電力モードを無効にします。
  - perfectreach :ポートがリンクアップ状態の場合に省電力モードを有効にします。
  - enable :ポートのリンク状態を問わず、省電力モードを有効にします。

30. private-vlan コマンド

ポートのプライベート VLAN 設定を行います。

“private-vlan ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# private-vlan ?
<1-10>          index
isolation       Set the port isolation mode
-------------------------------------------------------------
```

1) private-vlan x

ポートをプライベート VLAN ID ″x″に所属させます。
この場合の“x”は、プライベート VLAN の ID の値「1-10(FXC5210PE)、1-18(FXC5218PE)、1-24(FXC5224PE)」の範囲になります。
“no private-vlan x“コマンドにより、プライベート VLAN ID ″x″からインタフェースのポートを削除します。

2) private-vlan isolation

ポートをアイソレーションポートグループに設定します。アイソレーションポートグループのメンバーは同じ VLAN だったとしても、それぞれ単体となります。”no private-vlan isolation“コマンドにより、アイソレーションポートグループからポートを削除します。

31. qos コマンド

ポートの QoS 機能を設定します。

```
-------------------------------------------------------------
(config-if)# qos ?
  classification        QoS Ingress Port Classification
  dscp                  QoS Port DSCP Configuration
  policer               QoS Ingress Port Policers
  queueshaper           Queue Shaper
  scheduler             QoS Egress Port Schedulers
  shaper                QoS Egress Port Shapers
  tagremarking          QoS Egress Port Tag Remarking
-------------------------------------------------------------
```

1) qos classification

デフォルト QoS の入力ポートクラス分類を行います。

(1) qos classification class x

QoS クラスを設定します（クラス分けされていないフレームの QoS クラス）。
この場合の“x”は、 デフォルトのクラス(0～7)。

(2) qos classification dpl x

破棄優先度（クラス分けされてないフレームの DP レベル）を設定します。
この場合の“x”は、デフォルトの DP レベル(0～1)。

(3) qos classification dei x

タグなしフレーム用のデフォルトの識別子（※VLAN タグの 1-bit フィールド）です。
この場合の“x”は、デフォルトの識別子(0～1)です。

(4) qos classification dscp

DSCP ベース QoS の入力ポートのクラス分けを有効にします。“no qos classification dscp“コマンドにより、この機能を無効にします。

(5) qos classification map w x y z

タグクラス分類を有効にした時の((PCP、DEI)から(QoS クラス、DP レベル)へクラス分けした)入力マッピングを設定します。
“w”: pcp 値(0～7)
”x”: DEI 値(0～1)
“y”: QoS クラス（0～7）
“z”: DP レベル(0～1)

(6) qos classification pcp x

デフォルトのタグなし PCP(Priority Code Point)フレームの設定をします。この場合の“x”は、0～7 の値です。
【注記】: 3bit フィールドには、802.1Q フレームのプライオリティレベルがストアされています。
これは、タグなしフレームのユーザのプライオリティとしても用いられます。

(7) qos classification tag

タグ付き PCP および DEI フレームのマッピングを有効にします。”no qos classification tag“コマンドにより、この機能を無効にします。この機能が無効な場合は、タグフレームにもデフォルトの QoS クラスと DP レベルが適用されます。

2) qos dscp

QoS ポートの DSCP の設定を行います。

(1) qos dscp classification [all | none | selected | zero]

QoS クラスの Ingress DSCP の値を内部 DSCP マッピングに設定します。

- all : QoS クラスの DSCP 値をすべて内部 DSCP マッピングにクラス分けします。
- none : 入力 DSCP クラス分けなし。
- selected : 選択した DSCP のみクラス分けします。グローバル config モードの“qos dscp classification-mode”コマンドで選択されています。
- zero : 受信した DSCP(有効な場合は変換されます)が「0」の場合はクラス分けします。

(2) qos dscp egressremark [enable | remap_dp_aware | remap_dp_unaware]

DSCP Egress Rewrite モードを設定します。

- enable:
リマッピングを行わずにリライトを有効にします。新しい DSCP 値は、グローバル config モードのコマンドで設定されます。
- remap_dp_aware :
リマッピングにより、リライトを有効にします。リマッピングされた DSCP 値は、グローバル config モードの“qos dscp egressremap”コマンドで設定します。
- remap_dp_unaware:
リマッピングにより、リライトを有効にします。リマッピングされた DSCP 値は、グローバル config モードの“qos dscp egressremap”コマンド(DP level=0)で設定されます。

“no qos dscp egressremark”コマンドにより、この機能を無効にします。

【注記】:
まず本機能をグローバル Config モードにて有効に設定し、その後本コマンドにてポートの設定を行ってください。指定ポートのグローバル Config モードおよびポートモードの両方で設定を有効にすることで、設定した特定のポートで有効になります。

(3) qos dscp translation

ポートの入力変換を有効にします。”no qos dscp translation“コマンドにより、この機能を無効にします。

3) qos policer

QoS 入力ポートのポリシングを設定します。

(1) qos policer flowcontrol

ポートの入力ポリシングのフローコントロール機能を有効にします。フローコントロールが有効で、ポートがフローコントロールモードに設定されている場合は、フレームを破棄せずに、ポーズフレームが送信されます。

“no qos policer flowcontrol”コマンドにより、この機能を無効にします。

(2) qos policer mode

入力送信速度のポリシング機能を有効にします。Policer は受信したフレームの帯域を制限します。入力キューの前に設定されます。“no qos policer mode“コマンドにより、この機能を無効にします。

(3) qos policer rate x

ポートのポリシングレートを設定します。

”x”は、「100-3300000」の範囲内の値です。

(4) qos policer unit [kbps | fps]

ポートのレートの単位を設定します。“kbps”(kilo bit per second または“fps”(frame per second)のいずれかです。

5) qos queueshaper

送信キューのトラフィックのシェーピング機能を設定します。

(1) qos queueshaper mode x

送信キュー”x”のトラフィックシェーピングを設定します。この場合の”x”は、キューの値(0～7)です。

”no qos queueshaper mode x”コマンドにより、この機能を無効にします。

(2) qos queueshaper excess x

送信キューの帯域超過の許可を有効にします。この場合の”x”は、キューの値(0～7)です。

“no qos queueshaper excess x“コマンドにより、この機能を無効にします。

(3) qos queueshaper rate x y

送信キュー”x”のトラフィックシェーピングレート”y”を設定します。

”x”: キューの値(0～7)。

“y”: 送信速度の値(100～3300000kbps)。

6) qos scheduler

ポートの送信キューのトラフィックの調整を行います。

(1) qos scheduler mode [strict | weighted]

送信キューのトラフィック調整モード(“Strict Priority”あるいは”Weighted”)を設定します。

(2) qos scheduler weight x y

送信キュー”x”の重み付け”y”を設定します。

”x”: キューの値(0～7)です。

”y”: 「1～100」までの値で重み付けを設定します。

トラフィックの調整モードが「Weighted」の時のみ有効です。

7) qos shaper

ポートのトラフィックシェーピング機能を設定します。

(1) qos shaper mode

トラフィックのトラフィックシェーピング機能を有効にします。“no qos shaper mode“コマンドにより、この機能を無効にします。

(2) qos shaper rate x

トラフィックのシェーピングレートを”x”に設定します。

この場合の“x”は、送信速度の値(100～3300000kbps)です。

8) qos tagremarking

ポートの QoS 出力ポートのタグ・リマーキングを設定します。

(1) qos tagremarking dei x

tag-remarking モードがデフォルト設定の場合のデフォルトの識別子です。
※VLAN タグの 1-bit field です。この場合の“x”は、デフォルトの識別子の値(0～1)です。

(2) qos tagremarking map w x y z

tag-remarking モードが「Mapped」に設定されている場合は、QoS class, DP level から PCP, DEI へのマッピングを行います。
”w”: QoS Class(0～7)
”x”: DP レベル(0～1)
“y”: PCP(0～7)
”z”: DEI(0～1)

(3) qos tagremarking mode [classified | default | mapped]

tag-remarking の動作モードを設定します。
- classified : クラス分けした PCP/DEI 値を使用。
- default : デフォルトの PCP/DEI 値を使用。
- mapped : QoS クラスおよび DP レベルのマッピング情報を使用。

【注記】:
出力ポートはタグのリマーキング設定のタグ付きポートに設定してください。

(4) qos tagremarking pcp x

デフォルトの PCP(Priority Code Point)を設定します。
3bit フィールド(tag-remarking モードが「Default」に設定されている場合は、ポート上の 802.1Q フレームのプライオリティレベルがストアされます)です。
この場合の“x”は、PCP(「0～7」までの値)です。

32. sflow コマンド

ポートの sflow 機能を設定します。

“sflow ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config-if)# sflow ?
counterpoller   Set counter polling interval configuration
                per poller instance per port
flowsampler     Set flow sampler configuration per sampler
                instance per port
sampler         Clear per-port statistics
------------------------------------------------------------
```

1) sflow counterpoller enable

カウンタのポーリングを有効にします。”no sflow counterpoller enable“コマンドにより、この機能を無効にします。

- sflow counterpoller interval x

  カウンタポーリングのサンプリング間隔を（秒単位）で設定します。この場合の“x”は「0～3600 秒」までの値です。

2) sflow flowsampler enable

ポートのフローサンプリングを有効にします。

“no sflow flowsampler enable“コマンドにより、この機能を無効にします。

(1) sflow flowsampler max_hdr-size x

sFlow データにサンプリングされたパケットから最大何バイトコピーするかを設定します。この場合の“x”は最大値（「14～200 bytes」までの値）です。

最大データサイズがヘッダーの最大サイズに収まらない場合、サンプリングデータは破棄されます。

(2) sflow flowsampler sampling-rate x

パケットサンプリングの統計上のサンプリングレートを設定します。この場合の“x”はサンプリングレート(1～4294967295 の値)です。サンプルレートを N と設定し、ポートで送受信されたパケットの 1/N 番目で平均を算出します。サンプリングしたすべてのデータが算出されるわけではありません。

サポートされていないサンプリングレートを要求された場合は、一番近いサンプリングレートに自動的に調整します。

3) sflow sampler

ポートの sflow 統計情報をクリアにします。

33. shutdown コマンド

ポートを無効にします。
no shutdown コマンドにより、ポートを有効にします。

34. spanning-tree コマンド

ポートのスパニングツリー機能を設定します。

```
-----------------------------------------------------------------
(config-if)# spanning-tree ?
  autoedge          Set the STP autoEdge port
  bpduguard         Set the bpduGuard port
  clear             Clear STP port statistics
  edge-port         Specifies spanning tree edge port
  mcheck            Set the STP mCheck(Migration Check) variable fo
                    ports
  msti              Specifies spanning tree MSTI
  p2p               Set the STP point2point port
  restrictedrole    Set the MSTP restrictedRole port
  restrictedtcn     Set the MSTP restrictedTcn port
  <cr>              Enables the spanning tree
-----------------------------------------------------------------
```

1) spanning-tree autoedge
ブリッジポートで自動的にエッジポートを検出する機能を有効にします。ポートで BPDU が受信されたかどうかを検出することが可能になります。“no spanning-tree autoedge“コマンドにより、この機能を無効にします。

2) spanning-tree bpduguard
ポートの BPDU Guard 機能を有効にします。この機能が有効な場合は、有効な BPDU を受信するとポートは無効になります。
同様のブリッジ設定に反して、エッジポートのステータスはこの設定には影響しません。これは、error-disabled 状態のポートは、同様にブリッジポートのエラー回復の設定の対象となるからです。
“no spanning-tree bpduguard“コマンドにより、この機能を無効にします。

3) spanning-tree clear
STP ポートの統計情報を消去します。

4) spanning-tree edge-port
エッジポートで動作するフラグを有効に設定します。(ポートが初期化されると、初期状態ではエッジポートで動作します)。”no spanning-tree edge-port“コマンドにより、この機能を無効にします。
エッジポートフラグは、ポートがエッジ装置に直接接続されているかどうかを示すフラグです(ブリッジは接続されない)。フォワーディング状態に移行する速度は、エッジポート(PC などエッジ機器が接続されている場合)の方が他のポートよりも速くなります。

5) spanning-tree mcheck
ポートの STP Migration Check(移行チェック)を再開します。本機が STP BPDU を検出した場合は、STP 互換モードに自動的に設定されます。ただし、コマンドを使って、BPDU フォーマットを手動で再度チェックして、選択したインタフェースに送信することも可能です(RSTP、または STP 互換モード)。

6) spanning-tree msti x cost [auto | specific y]

MSTI "x"のポートにより生じたパスコストを設定します。
"x": MSTI のインデックス(0～7)までの値
"y": コストの値(1～200000000)
"auto"に設定することにより、802.1D に準じて、物理リンクスピードからパスとコストを設定します。

・ spanning-tree msti x port_priority y

MSTI"x"のポートのプライオリティを設定します。
"x":MSTI のインデックス(0～7)までの値
"y":プライオリティの値(0～240)までの値
これにより、ポートのコストが同じポートのプライオリティを制御します。

7) spanning-tree p2p [auto | false | true]

ポートのポイントツーポイント接続を設定します。
LAN によるポイントツーポイント接続だけでなく、共有媒体(マルチキャストなどの媒体)に接続する場合でもポイントツーポイントとみなされます。
"auto"で自動検出か"false"/"true"を設定できます。
フォワーディング状態に移行するのは、共有媒体よりLANでのポイントツーポイントのほうが高速です。

8) spanning-tree restrictedrole

MSTP での動作を制限します。この機能が有効な場合は、スパニングツリーのプライオリティが高い場合でも、CIST、MSTI などのルートポートとして選択することはできません。
このポートはルートポートが選択された後に、代替ポートとして選択されます。
代替ポートを設定すると、スパニングツリーの接続が切れる場合があります。
すべてのブリッジが管理者の制御下にない可能性があるので、ネットワーク管理者によりネットワークの中核領域外のブリッジがスパニングツリーのアクティブトポロジーに影響を与えないように設定を行うことができます。
この機能は、"ルートガード"と呼ばれます。"no spanning-tree restrictedrole"コマンドにより、この機能を無効にします。

9) spanning-tree restrictedtcn

MSTP の TCN でのポートの動作を制限します。この機能が有効な場合は、受信したトポロジーの変更通知およびその他のポートへのトポロジーの変更通知を送信しません。設定されると、スパニングツリーのアクティブトポロジーの変更の後、誤って学習した構成情報のために一時的に接続断が発生することがあります。
本設定は、ネットワークの中核領域外にあるブリッジがリージョン内へアドレスフラッシングさせないため、また、ネットワークの中核領域にあるブリッジは管理者の完全な制御下にない可能性があるか、物理的に接続されている LAN のリンク状態が頻繁に遷移するのを防ぐために、ネットワーク管理者によって設定されます。

10) spanning-tree

スパニングツリー機能を有効にします。"no spanning-tree"コマンドにより、この機能を無効にします。

35. speed コマンド

ポートの通信速度および通信モードを設定します。

```
-------------------------------------------------------------
(config-if)# speed ?
  auto              Set port speed to be auto
  10hdx             Set port speed to be 10M hdx
  10fdx             Set port speed to be 10M fdx
  100hdx            Set port speed to be 100M hdx
  100fdx            Set port speed to be 100M fdx
  1000fdx           Set port speed to be 1G fdx
-------------------------------------------------------------
```

speed auto	:auto-negotiation モードに設定します。
speed [10hdx | 10fdx]	:10M の通信速度、全二重/半二重モードに設定します。
speed [100hdx|100fdx]	:100M の通信速度、全二重/半二重モードに設定します。
speed 1000fdx	:1000M(1G)通信速度、全二重モードに設定します。

36. switchport コマンド

VLAN Port(スイッチポート)の設定を行います。

```
-------------------------------------------------------------
(config-if)# switchport ?
  acceptable-frame-types  Specifies frame type
  allowed                 Configures the VLAN port list
  ingressfilter           Set the port VLAN ingress filter
  mode                    Configures the port type
  native                  Configures the PVID of the port
  tx_tag                  Set the port egress tagging
-------------------------------------------------------------
```

1) `switchport acceptable-frame-types [all | tagged | untagged]`
   タグ付き/タグなしフレームの受け入れを設定します。
   - all :すべてのフレーム、タグ付き/タグなしフレームを受け入れます。
   - tagged :タグ付きフレームのみ受け入れます。
   - untagged:タブなしフレームのみ受け入れます。

2) `switchport allowed vlan [add x | remove x | forbidden add x | forbidden remove x]`
   VLAN x へのポートの追加、VLAN x からポートの削除、VLAN x への禁止の設定、VLAN x から禁止解除の設定を行うことができます。“x”の VLAN ID は「1～4095」までの値です。

3) `switchport ingressfilter`
   ポートの VLAN 入力フィルタ機能を有効にします。“no switchport ingressfilter“コマンドにより、この機能を無効にします。

4) `switchport mode [c-port | s-custom-port | s-port | unaware]`
   ポートの Port Type を設定します。"Port Type"により、プロバイダのブリッジ(Q-in-Q)モデルのポートのタイプを設定します。
   Customer VLAN は、TPID == 0x8100、Service VLAN は、TPID == 0x88A8 です。
   Q-in-Q がサポートされていないアプリケーションの場合は、S-port および S-custom-port は無視されます。
   - c-port: C-port に設定すると、タグ付きフレームはフレームのタグに応じて VLAN にクラス分けされます。

- s-custom-port: S-custom-port に設定すると、出力フレームタグの TPID は、Service VLAN の TPID に変更されます。これは、Q-in-Q アップリンク接続用です。
- s-port: S-port に設定すると、出力フレームタグの TPID は、Service VLAN の 0x88A8 が設定されます。これは、Q-in-Q アップリンク接続用です。
- unaware: 「Unaware」に設定すると、受信フレームはタグなしで処理されます。受信したフレームがタグありの場合でも、本機にペイロードとして処理されます。フレームはポートベース VLAN にクラス分けされます（PVID）。これは、802.1Q アクセス接続用か、Q-in-Q ダウンリンク接続用です。ポートベース VLAN を使用する場合は、PVID と同じく、“Unaware”に設定してください。

5) switchport native vlan [none | x]

入力ポートでタグなしフレームに分類するため、ネイティブ VLAN の VLAN ID を割り当てます。
”x” : ポートの VLAN ID(PVID)であり、かつ設定可能な範囲の値は「1～4095」です。
“none”: VLAN トランクポートに使用します。
タグなしフレームを受信すると、入力ポートの PVID を動作中の VLAN ID として使用します。PVID は、タグなしパケットをタグ付きパケットに変換する際に追加するタグの VLAN ID にも使用します。

6) switchport tx_tag [tag_all | untag_all | untag_pvid]

出力方向へのフレームのタグ付け方法を設定します（フレームが送信される場合）
- tag_all : タグ付き出力ポート。出力パケットはすべてタグ付きです。
- untag_all : タグなし出力ポート。出力パケットはすべてタグなしです。
- untag_pvid : hybrid 出力ポートです。PVID としてタグ付けされたもの以外の出力パケットはすべてタグ付けされます。

37. voice-vlan コマンド

ポートの音声 VLAN 機能を設定します。

```
-----------------------------------------------------------------
(config-if)# voice-vlan ?
  discovery-protocol   Set the Voice VLAN port discovery
                       protocol mode
  port-mode            Set the Voice VLAN port mode
  security             Set the Voice VLAN port security mode
   ---------------------------------------------------------
```

1) voice-vlan discovery-protocol [both | lldp | oui]

音声 VLAN ポートの検出プロトコルを設定します。自動検知モードが有効な場合のみ動作します。検出プロトコルが”LLDP”または”Both”に設定される前に、LLDP 機能を有効にしてください。検出プロトコルを OUI”または”LLDP”に変更すると、自動検出処理を再開します。

検出できるプロトコルは、以下のとおりです。
- oui : OUI アドレスによって、電話装置を検出します。
- lldp : LLDP によって、電話装置を検出します。
- both : OUI および LLDP の両方を使って、電話装置を検出します。

2) voice-vlan port-mode [auto | disable | force]

音声 VLAN の設定を行います。
- auto : 自動検出モードを有効にします。VoIP 電話装置が特定ポートに接続されているか、音声 VLAN メンバーが自動設定されているかどうかを検出します。
- disable : 音声 VLAN から解除します。
- force : 音声 VLAN に設定します。

3) `voice-vlan security`
ポートのセキュリティ機能を有効にします。
セキュリティ機能を有効にすると、音声 VLAN の電話装置以外の MAC アドレスが 10 秒間ブロックされます。“no voice-vlan security“コマンドにより、この機能を無効にします。

1.2.3.2 VLAN インタフェース Config コマンド

Config モードのコマンドは、“(config)#”プロンプトにて基本設定を行います。
VLAN グループを設定する場合は、“interface vlan x” コマンドを使用してください。例えば、
“interface vlan 100” は、VLAN100 の設定を行う場合です。

【注記】:
VLAN 作成/追加は、“vlan database”コマンドで行ってください。
詳細については、「VLAN 設定コマンド」を参照ください。

“interface vlan x”コマンドにより、VLAN グループ設定を行います。
例えば、VLAN に IP アドレスを割り当てる場合は、このコマンドを使用してください。

1) “interface vlan 100”と入力すると、以下のプロンプト画面が表示されます。

例:

```
---------------------------------------------------------------
(config)# interface vlan 100
(config-if)#
---------------------------------------------------------------
```

2) “?”と入力すると、以下のようにサブコマンドが表示されます。

```
---------------------------------------------------------------
 (config-if)?
  exit              Exit from current mode
  help              Show available commands
  history           Show a list of previously run commands
  logout            Disconnect
  quit              Quit commands
  interface         Enters privileged interface configuration
  ip                Set the IPv4 setup
  ipv6              Set othe IPv6 setup
  no                Negates a command or sets its defaults
---------------------------------------------------------------
```

1. exit コマンド

現在のオペレーションモードを終了し、前のモードに戻ります。

2. help コマンド

help コマンドにより、使用可能なコマンドが表示されます。

3. history コマンド

入力したコマンドの履歴が表示されます。

4. logout コマンド

ログアウト用のコマンドです。

5. quit コマンド

コンソール画面での設定を中止する際に使用します。ログアウトと同じ機能を持ちます。

6. interface コマンド

連続してセットアップできるよう現在のインタフェース VLAN グループから次のインタフェース VLAN グループへすぐ移るためのコマンドです。

```
------------------------------------------------------------
(config-if)# interface ?
  vlan          Switch Virtual LAN interface
------------------------------------------------------------
```

例えば:
“(config-if)# interface vlan 100”は、設定画面を「VLAN 100」に変更し、次のコマンドがすべて VLAN 100 に適用されます。

7. ip コマンド

VLAN インターフェイス上で本機の IP アドレスを設定します。VLAN のネットワークのユーザーのみがこの IP アドレスを使用して本機にアクセスすることができます。

```
------------------------------------------------------------
(config-if)# ip address ?
  dhcp              Dynamic host configuration protocol
  A.B.C.D           IP address
  renew             Renew IP
------------------------------------------------------------
```

1)ip address dhcp
DHCP クライアント機能を「有効」にします。
DHCP クライアント機能は、ネットワークの DHCP サーバから IP アドレスを取得します。
“no ip address dhcp“コマンドでこの機能を無効にします。
DHCP サーバからの IP アドレス取得に失敗し、設定された IP アドレスが「0」になった場合は再試行します。
DHCP サーバが 35 秒内に応答せず、設定された IP アドレスが「0 以外」の値の場合は、DHCP の再試行を中断し、設定されている IP を使用します。
DHCP クライアントは、DNS 参照するために設定した System Name をホスト名として通知します。

2)ip address x.x.x.x y.y.y.y
LAN で本機の IP アドレスを設定します。
“x.x.x.x”: 本機の IP アドレス。
“y.y.y.y”: 本機のサブネットマスク。
例えば “ip address 192.168.1.12 255.255.255.0”は、リモート管理用の VLAN グループに本機の IP アドレスを設定します。

3)ip address renew
DHCP によって取得した IP アドレスのリースタイムを更新します。ブートアップ時に、IP 設定が設定されていない場合は、このコマンドにより、再度 IP 設定を行います。

8. ipv6 コマンド

VLAN 用の本機の IPv6 アドレスを設定します。
VLAN のネットワークのユーザーのみが IPv6 アドレスにより本機にリモートアクセス可能です。

```
-------------------------------------------------------------
(config-if)# ipv6 address ?
  autoconfig     Set the IPv6 AUTOCONFIG mode
  renew          Renew IP
  <ipv6 address> IPv6 address For example,
                 fc80::215:c5ff:fe03:4dc7
-------------------------------------------------------------
```

1) ipv6 address autoconfig
IPv6 Auto Configuration 機能を「有効」にします。 “no ipv6 address autoconfig“ コマンドによりこの機能は「無効」となります。
システムがステートレスアドレスを入手できない場合は、設定されている IPv6 アドレスが使用されます。ルータは、数秒間ルータの内部処理に応じて遅延する場合があり、自動設定に要する合計時間は非常に長くなります。

2) ipv6 address renew
IPv6 自動設定機能により取得された IPv6 アドレスを更新します。

3) ipv6 address <ipv6 address>
この VLAN で本機の IPv6 アドレスを設定します。“<ipv6 address>”は IPv6 アドレスです。

9. no コマンド

機能を無効にするか、工場出荷時の値に戻ります。

“no ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-if)# no ?
  ip             Set the IPv4 setup
  ipv6           Set the IPv6 setup
-------------------------------------------------------------
```

- ip address dhcp
例として、“no ip address dhcp”コマンドを入力した場合は、DHCP クライアント機能が無効となります。
この場合、本機は vlan に設定された IP アドレスを使用します。
また、″no ip address″と入力した場合は、IP アドレスの設定が工場出荷時状態(192.168.1.1)に戻ります。

1.2.4 VLAN 設定コマンド

グローバル config モードのコマンドは、本機の基本設定用です。
プロンプト表示は、”(config)#”です。VLAN の作成/追加の場合は、グローバル config モードで、“vlan database”コマンドを用いて、まず VLAN 設定モードに入ります。
プロンプト画面は“(config-vlan)#”です。

【注記】:
いくつかの VLAN グループ(”VLAN ID”と呼ばれる)の設定の場合は、まず“interface vlan x”コマンド(”x”は VLAN ID)で、VLAN インタフェース Config モードで行ってください。
詳細については、「VLAN インタフェース Config モード」を参照してください。

1) ”vlan database”と入力すると、以下の画面が表示されます。

```
------------------------------------------------------------------
(config)# vlan database
(config-vlan)#
------------------------------------------------------------------
```

2) ”?”と入力すると、以下のようにサブコマンドが表示されます。

```
------------------------------------------------------------------
(config-vlan)?
  exit              Exit from current mode
  help              Show available commands
  history           Show a list of previously run commands
  logout            Disconnect
  quit              Quit commands
  end               Exit from vlan mode
  no                Negates a command or sets its defaults
  vlan              Switch Virtual LAN interface
------------------------------------------------------------------
```

1. exit コマンド

現在のオペレーションモードを終了し、前のモードに戻ります。

2. help コマンド

設定可能なコマンドをすべて表示します。

3. history コマンド

入力したコマンドの履歴を表示します。

4. logout コマンド

コンソール画面からログアウトします。

5. quit コマンド

コンソール画面を終了します。logout と同じ機能です。

6. end コマンド

VLAN Config モードを終了します。exit と同じ機能です。

```
-------------------------------------------------------------
(config-vlan)# end
(config)#
-------------------------------------------------------------
```

7. no コマンド

機能を無効にするか、工場出荷時の値にリストアします。

“no ?”と入力すると、次のサブコマンドが表示されます。

```
-------------------------------------------------------------
(config-vlan)# no ?
  vlan    Switch Virtual LAN interface
-------------------------------------------------------------
```

例として、″no vlan 100″コマンドを入力した場合、「VLAN 100」を削除します。

8. vlan コマンド

802.1Q VLAN、または Q-in-Q の Custom S-port の EtherType を設定します。

1) vlan x

VLAN 設定を行います。
この場合の“x”は VLAN ID（1～4095 までの値）です。“no vlan x”コマンドにより、VLAN”x”を削除します。

2) vlan x name yyy

VLAN ID :”x”の VLAN を作成し、VLAN 名”yyy”を設定します。
”x” : VLAN ID（1～4095 までの値）
“yyy” : 文字列

3) vlan etypecustomsport 0xXXXX

Q-in-Q の Custom S-port のイーサネットタイプを設定します。“0xXXXX”はイーサネットタイプ(16 進数)です。
”no vlan etypecustomsport”コマンドにより、この設定を削除します。

1.2.5 Show コマンド

Show コマンドにより、システムの基本設定や情報が表示されます。

“show ?”と入力すると、以下のサブコマンドが表示されます。

```
------------------------------------------------------------
# show ?
  aaa                     Show AAA service configuration
  acl                     Packet Access Control List
  calendar                Date and time information
  ddmi                    Digital Diagnostics Monitoring
                          Interface
  dhcp-relay              DHCP Relay Configuration
  dot1x                   802.1x content
  eee                     Show eee configuration
  history                 History information
  interface               Interface information
  ip                      IP information
  ip-source-guard         IP source guard
  lacp                    LACP statistics
  lldp                    Show lldp Configuration
  log                     Log records
  loopback-detection      how loopback detection
  mac-address-table       Configuration of the address table
  mac-security            MAC Security Configuration
  management              Management IP filter
  map                     Maps priority
  mvr                     Show MVR Status
  ntp                     Simple Network Time Protocol
                         configuration
  poe                     Power Over Ethernet
  port                    Port characteristics
  queue                   Priority queue information
  radius-server           RADIUS server information
  running-config          Information on the running configuration
  rate-limit              rate-limits
  rmon                    Rmon
  sflow                   Sampling flow
  snmp                    Simple Network Management Protocol
                         statistis
  spanning-tree           Spanning-tree configuration
  storm-control           Show storm control configuration
  system                  System information
  tacacs-server           TACACS server settings
  trunk                   Trunk information
  users                   Show users configuration
  version                 System hardware and software versions
  vlan                    Virtual LAN settings
------------------------------------------------------------
```

1. show aaa コマンド

AAA 認証の設定とステータスを表示します。

例:

```
------------------------------------------------------------
# show aaa authentication login

Auth Configuration:
===================
Client   Authentication Method   Local Authentication Fallback
-------  ----------------------  ----------------------------
console local              Disabled
telnet local               Disabled
ssh local                  Disabled
web local                  Disabled
------------------------------------------------------------
```

2. show acl コマンド

ACL 設定およびステータスを表示します。

例:

```
------------------------------------------------------------
# show acl ?
  ports                    Show the ACL port configuration
  rate                     Show the ACL rate limiter
  status                   Show ACL status
  <1-256>                  show an access list configuration
  <cr>                     show all access list configuration
------------------------------------------------------------
```

1) show acl

すべての ACE のステータスを表示します。

例:

```
------------------------------------------------------------
# show acl
ID   Type     Port    Policy   Frame  Action Rate L.  Port C.
  Mirror    Counter
   ------    ------    ---- -----  ------  --------   -----
1    User     All     Any      Any    Permit Disabled Disabled
  Disabled  31741
Number of ACEs: 1
------------------------------------------------------------
```

(1) show acl ports

ACL ポートの設定を表示します。

例:

```
------------------------------------------------------------
# show acl ports
ACL Configuration:
==================
Port  Policy   Action  Rate L.  Port C.   Mirror    Logging
   Shutdown  Counter
------    ------   -------    -------    --------
   --------
1     0      Permit  Disabled Disabled Disabled  Disabled
   Disabled    0
```

```
2    0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
3    0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
4    0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
5    0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
6    0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
7    0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
8    0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
9    0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
10   0      Permit  Disabled Disabled Disabled  Disabled
   Disabled   0
Port  State
----  -----
1    Enabled
2    Enabled
3    Enabled
4    Enabled
5    Enabled
6    Enabled
7    Enabled
8    Enabled
9    Enabled
10   Enabled
-------------------------------------------------------
```

(2) show acl rate

ACL レートリミットの設定情報を表示します。

例:

```
-------------------------------------------------------
# show acl rate
Rate Limiter   Rate
------------   ----
1           1 PPS
2           1 PPS
3           1 PPS
4           1 PPS
5           1 PPS
6           1 PPS
7           1 PPS
8           1 PPS
9           1 PPS
10          1 PPS
11          1 PPS
12          1 PPS
13          1 PPS
14          1 PPS
15          1 PPS
16          1 PPS
-------------------------------------------------------
```

(3) show acl status

ACL ステータスを表示します。

例:

```
-------------------------------------------------------
# show acl status
User
----
S  :  Static
IPMG: IP Management
IPSG: IP Source Guard
IPMC: IPMC
ARPI: ARP Inspection
DHCP: DHCP
LOOP: Loop Protect
User ID   Port    Frame  Action  Rate L.  Port C.  Mirror
   CPU    Counter Confl.
----   --   -------   -----    ------    --------   -----
S    1    All     Any    Permit  Disabled Disabled Disabled
   No    29794  No
Number of ACEs: 1
-------------------------------------------------------
```

- User : ACL ユーザ
- ID : ACE ID 番号
- Port : ACE の入力ポート
- Frame : ACE のフレームタイプ
- Action : ACE の動作
- Rate L : ACE のレートリミット番号
- Port C : ACE のポートリダイレクト設定
  ACE と一致するフレームは、ポート番号にリダイレクトされます。
- Mirror : ACE のミラー設定
- CPU : CPU に適用される ACE のパケット送信
- Counter : フレームにより検出される ACE の回数
- Confl. : 特定の ACE のハードウェアステータス
  特定の ACE によっては、制限によりハードウェアに適用されない場合があります。

(3) show acl x

ACE ステータスを表示します。この場合の“x”は ACE の ID(1～256 の値)です。

例:

```
-------------------------------------------------------
# show acl 1
ACE ID           : 1    Rate Limiter : Disabled
Ingress Port: All       Port Redirect: Disabled
                        Mirror       : Disabled
Policy/Bitmask   : Any  Logging      : Disabled
Type             : User Shutdown     : Disabled
Frame Type       : Any  Counter      : 31393
Action           : Permit
MAC Parameters                VLAN Parameters
---------------                 ---------------
                              802.1Q Tagged : Any
                              VLAN ID       : Any
                              Tag Priority  : Any
-------------------------------------------------------
```

(4) show calendar

現行のシステムタイムを表示します。

例:

```
-------------------------------------------------------
# show calendar
System Time      : 2012-01-01T05:09:39+00:00
System Uptime    : 05:09:39
-------------------------------------------------------
```

(5) show ddmi

DDMI のステータスを表示します。

例:

```
-------------------------------------------------------
# show ddmi ethernet
Digital Diagnostics Monitoring Interface of Eth 1/9
  Serial Info Table
  Status:                       N/A
  Vendor:
  PartNo:
  SerialNo:
  Revision:
  DateCode:
  Transceiver:                    N/A
  Ddm Info Table
  Type         AlarmMax  AlarmMin  WarnMax  WarnMin
    Current
  N/A           0.00      0.00      0.00     0.00     0.00
  N/A           0.00      0.00      0.00     0.00     0.00
  N/A           0.00      0.00      0.00     0.00     0.00
  N/A           0.00      0.00      0.00     0.00     0.00
  N/A           0.00      0.00      0.00     0.00     0.00
-------------------------------------------------------
```

3. show dhcp-relay コマンド

現行の DHCP リレーの設定およびステータスを表示します。

例:

```
------------------------------------------------------------
# show dhcp-relay
DHCP Relay Configuration:
=========================
DHCP Relay Mode                  : Disabled
DHCP Relay Server                : 192.168.1.100
DHCP Relay Information Mode      : Enabled
DHCP Relay Information Policy    : Replace
Server Statistics:
------------------
Transmit to Server    : 0   Transmit Error              :    0
Receive from Server   : 0   Receive Missing Agent Option:    0
Receive Missing Circuit ID : 0   Receive Missing Remote ID: 0
Receive Bad Circuit ID: 0   Receive Bad Remote ID    :      0
Client Statistics:
------------------
Transmit to Client  :  0   Transmit Error       :            0
Receive from Client :  0   Receive Agent Option :            0
Replace Agent Option: 0   Keep Agent Option    :            0
Drop Agent Option   :  0
------------------------------------------------------------
```

4. show dot1x コマンド

現行の 802.1x ネットワークアクセスサーバのステータスを表示します。

例:

```
------------------------------------------------------------
# show dot1x
Port   Admin State       Port State         Last Source     Last ID
----   ------------------      ---------------------
1     Force Unauthorized  Globally Disabled      -              -
2     Force Unauthorized  Globally Disabled      -              -
3     Force Unauthorized  Globally Disabled      -              -
4     Force Unauthorized  Globally Disabled      -              -
5     Force Unauthorized  Globally Disabled      -              -
6     Force Unauthorized  Globally Disabled      -              -
7     Force Unauthorized  Globally Disabled      -              -
8     Force Unauthorized  Globally Disabled      -              -
9     Force Unauthorized  Globally Disabled      -              -
10    Force Unauthorized  Globally Disabled      -              -
------------------------------------------------------------
```

Port : ポート番号
Admin State : 管理状態
Port State : ポートのステータス
Last Source : EAPOL ベース認証のために最後に受信した EAPOL フレーム、および MAC ベースの認証のために新たなクライアントから最後に受信したフレームの送信元 MAC アドレス
Last ID : EAPOL ベース認証のために最後に受信した Response Identity EAPOL フレーム、および MAC ベースの認証のために新たなクライアントから最後に受信したフレームの送信元 MAC アドレス

1) show dot1x configuration

本機の 802.1x 設定とステータスを表示します。

例:

```
-----------------------------------------------------
# show dot1x configuration
802.1X Configuration:
====================
Mode             : Disabled
Reauth.          : Disabled
Reauth. Period   : 3600
EAPOL Timeout    : 30
Age Period       : 300
hold time        : 10
RADIUS QoS       : Disabled
RADIUS VLAN      : Disabled
Guest VLAN       : Disabled
Guest VLAN ID    : 1
Max. Reauth Count: 2
Allow Guest VLAN if EAPOL Frame Seen: Disabled
Mac Auth Username Format: with-hyphen Lower-case
-----------------------------------------------------
```

2) show dot1x guest_vlan

ゲスト VLAN をポート単位で表示します。

例:

```
-----------------------------------------------------
# show dot1x guest_vlan
      Guest
Port   VLAN         Current
----    -------     -------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled
-----------------------------------------------------
```

3) show dot1x radius_qos

RADIUS-assigned QoS をポート単位で表示します。

例:

```
-----------------------------------------------------
# show dot1x radius_qos
     RADIUS
Port  QoS          Current
----   -------     -------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled
-----------------------------------------------------
```

4) show dot1x radius_vlan

RADIUS-assigned VLAN をポート単位で表示します。

例:

```
-----------------------------------------------------
show dot1x radius_vlan
     RADIUS
Port  VLAN     Current
----  -------  -------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled
-----------------------------------------------------
```

5) show dot1x statistics

802.1X 統計情報を表示します。

例:

```
# show dot1x statistics
Port 1 EAPOL Statistics:
Rx Total:                    0    Tx Total:       0
Rx Response/Id:              0   Tx Request/Id:   0
Rx Response:                 0   Tx Request:      0
Rx Start:                    0
Rx Logoff:                   0
Rx Invalid Type:             0
Rx Invalid Length:           0
Port 1 Backend Server Statistics:
Rx Access Challenges:        0   Tx Responses:    0
Rx Other Requests:           0
Rx Auth. Successes:          0
Rx Auth. Failures:           0
---More---
```

5. show eee コマンド

EEE(IEEE802.3az)設定を表示します。

例:

```
# show eee
EEE Configuration:
==================
Port  Mode     Urgent queues
----   -------     -------------
1     Disabled       none
2     Disabled       none
3     Disabled       none
4     Disabled       none
5     Disabled       none
6     Disabled       none
7     Disabled       none
8     Disabled       none
9     N/A            none
10    N/A            none
```

6. show history コマンド

入力したコマンドの履歴を表示します。

例:

```
# show history
  1. config
  2. interface valn 10
  3. ipv6 address state fc80::215:c5ff:fe03:4dc7
  4. exit
  5. show history
```

7. show interface コマンド

ポート情報およびステータスを表示します。

例:

```
-------------------------------------------------------------
# show interface ?
  counters                  Interface counters information
  description               Interface specific description
  detailed_counters         Interface detailed counters information
  dualMedia_fiberMode       Show the port speed for fiber ports
  psec                      Port security status
  sfp                       Show the detected sfp type
  status                    Interface status information
  switchport                Interface switchport information
  veriphy                   Run cable diagnostics
-------------------------------------------------------------
```

1) show interface counters

すべてのポートの統計情報の値を表示します。

・ show interface counters ethernet 1/x

Port x の統計情報の値を表示します(この場合の"x"はポート番号)。

例:

```
-------------------------------------------------------------
# show interface counters ethernet 1/5
Port: 1/5
=========================================
Rx Counter                  Statistics
Packets                        0
Octets                         0
Errors                         0
Drops                          0
Filtered                       0
=========================================
Tx Counter                  Statistics
Packets                        0
Octets                         0
Errors                         0
Drops                          0
-------------------------------------------------------------
```

2) show interface description

各ポートに設定されているインタフェース名を表示します。

例:

```
# show interface description

Port  Name
----  ----
1     Port 1
2     Port 2
3     Port 3
4     Port 4
5     Port 5
6     Port 6
7     Port 7
8     Port 8
9     Port 9
10    Port 10
```

3) show interface detailed_counters

すべてのポートの詳細な統計情報の値を表示します。

- show interface detailed_counters ethernet 1/x

  Port x の詳細な統計情報の値を表示します(この場合の"x"はポート番号)。

例:

```
# show interface detailed_counters ethernet 1/5
Rx Packets:            0   Tx Packets:                  0
Rx Octets:             0   Tx Octets:                   0
Rx Unicast:            0   Tx Unicast:                  0
Rx Multicast:          0   Tx Multicast:                0
Rx Broadcast:          0   Tx Broadcast:                0
Rx Pause:              0   Tx Pause:                    0
Rx 64:                 0   Tx 64:                       0
Rx 65-127:             0   Tx 65-127:                   0
Rx 128-255:            0   Tx 128-255:                  0
Rx 256-511:            0   Tx 256-511:                  0
Rx 512-1023:           0   Tx 512-1023:                 0
Rx 1024-1526:          0   Tx 1024-1526:                0
Rx 1527-  :            0   Tx 1527-  :                  0
```

4) show interface dualMedia_fiberMode

ポートごとに通信速度とモードのステータスを表示します。

例:

```
# show interface dualMedia_fiberMode

Port  Link  MDI/MDI-X
----  ----  ---------
1     1Gfdx  AUTO-MDI
2     Down  AUTO-MDI
3     Down  AUTO-MDI
4     Down  AUTO-MDI
```

```
5     Down  AUTO-MDI
6     Down  AUTO-MDI
7     Down  AUTO-MDI
8     Down  AUTO-MDI
9     Down  AUTO-MDI
10    Down  AUTO-MDI
------------------------------------------------------------
```

5) show interface psec port

ポートセキュリティによって学習された MAC アドレスを表示します。

例:

```
------------------------------------------------------------
# show interface psec port
Port 1:
MAC Address  VID  State    Added          Age/Hold Time
-------------------------
<none>
---More---
------------------------------------------------------------
```

- show interface psec switch

ポートセキュリティのステータスを表示します。

例:

```
------------------------------------------------------------
# show interface psec switch
Users:
L = Limit Control
8 = 802.1X
D = DHCP Snooping
V = Voice VLAN
Port  Users  State         MAC Cnt
----   -----   -------------       -------
1     ----   No users           0
2     ----   No users           0
3     ----   No users           0
4     ----   No users           0
5     ----   No users           0
6     ----   No users           0
7     ----   No users           0
8     ----   No users           0
9     ----   No users           0
10    ----   No users           0
------------------------------------------------------------
```

6) show interface sfp

検出した sfp タイプを表示します。

例:

```
------------------------------------------------------------
# show interface sfp
Port      SFP          MDI/MDI-X
----  ----------     ---------
1       AUTO-MDI        None
2       AUTO-MDI        None
3       AUTO-MDI        None
4       AUTO-MDI        None
5       AUTO-MDI        None
6       AUTO-MDI        None
7       AUTO-MDI        None
8       AUTO-MDI        None
9       AUTO-MDI        None
10      AUTO-MDI        None
------------------------------------------------------------
```

7) show interface status

ポートの設定情報を表示します。

例:

```
------------------------------------------------------------
# show interface status

Port Configuration:
===================

Port  State  Mode  Flow Control MaxFrame Power Excessive Link
  MDI/MDI-X
----  --------  -----------  ------------  --------  --------
1 Enabled  Auto   Disabled    9600   Disabled  Discard   1Gfdx
  AUTO-MDI
2 Enabled  Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
3 Enabled  Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
4 Enabled  Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
5 Enabled  Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
6 Enabled  Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
7 Enabled  Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
8 Enabled  Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
9 Enabled  Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
10 Enabled Auto   Disabled    9600   Disabled  Discard    Down
  AUTO-MDI
------------------------------------------------------------
```

8) show interface switchport

すべてのポートの VLAN 設定を表示します。

例:

```
-------------------------------------------------------------
#show interface switchport
VLAN Configuration:
===================
Port  PVID  Frame Type  Ingress Filter  Tx Tag     Port Type
----   ----    ----------     --------------    ----------
1     1       All         Disabled     Untag PVID  Unaware
2     1       All         Disabled     Untag PVID  Unaware
3     1       All         Disabled     Untag PVID  Unaware
4     1       All         Disabled     Untag PVID  Unaware
5     1       All         Disabled     Untag PVID  Unaware
6     1       All         Disabled     Untag PVID  Unaware
7     1       All         Disabled     Untag PVID  Unaware
8     1       All         Disabled     Untag PVID  Unaware
9     1       All         Disabled     Untag PVID  Unaware
10    1       All         Disabled     Untag PVID  Unaware
-------------------------------------------------------------
```

・show interface switchport status

VLAN ポートの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show interface switchport status
Port VLAN User PortType PVID Frame Type  Ing Filter Tx Tag VID
  Conflicts
----  -----------   -------------  ----  ----------
  -----------  ---
1    Static    Unaware   1    All   Disabled  Untag This  1
NAS                                                    No
MVR                                                    No
Voice VLAN                                             No
MSTP                                                   No
Combined Unaware        1    All   Disabled  Untag This   1
  No
---More---
-------------------------------------------------------------
```

9) show interface veriphy

ケーブル診断を実行します。

例:

```
------------------------------------------------------------
# show interface veriphy
Starting VeriPHY, please wait
Port   Pair A  Length  Pair B  Length  Pair C   Length   Pair D
  Length
-----   -------    -------     -------    -------    -------
1      Open     0       Open     0      Open     0      Open     0
2      Open     0       Open     0      Open     0      Open     0
3      Open     0       Open     0      Open     0      Open     0
4      Open     0       Open     0      Open     0      Open     0
5      Open     0       Open     0      Open     0      Open     0
6      Open     0       Open     0      Open     0      Open     0
7      OK       3       OK       3      Open     3      Open     3
8      Open     0       Open     0      Open     0      Open     0
------------------------------------------------------------
```

8. show ip コマンド

本機の IP 設定および現行の ARP インスペクション、DHCP スヌーピング、HTTP設定、IGMP/MLD スヌーピング、SSH、IP ソースガードのステータスを表示します。

例:

```
------------------------------------------------------------------
# show ip ?
  arp                       Address Resolution Protocol
  dhcp                      DHCP snooping
  http                      Show HTTP configuration
  igmp                      IGMP snooping
  interface                 Interface information
  mld                       MLD snooping
  ssh                       Secure shell server connections
------------------------------------------------------------------
```

1) show ip arp inspection

ARP インスペクションの設定およびステータスを表示します。

例:

```
------------------------------------------------------------
# show ip arp inspection
ARP Inspection Configuration:
============================
ARP Inspection Mode: Disabled
Port  Port Mode
----  -----------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled
ARP Inspection Entry Table:
Type     Port  VLAN  MAC Address       IP Address
```

```
------------------------------------------------------------
```

2) show ip dhcp snooping

DHCP スヌーピング設定を表示します。

```
------------------------------------------------------------
  -
# show ip dhcp snooping
DHCP Snooping Configuration:
============================
DHCP Snooping Mode: Disabled
Port Port Mode
---- -----------
1 trusted
2 trusted
3 trusted
4 trusted
5 trusted
6 trusted
7 trusted
8 trusted
9 trusted
10 trusted
------------------------------------------------------------
  -
```

3) show ip dhcp snooping statistics

DHCP スヌーピングの統計情報を表示します。

例:

```
------------------------------------------------------------
# show ip dhcp snooping statistics
Port 1 Statistics:
--------------------
Rx Discover:           0   Tx Discover:           0
Rx Offer:              0   Tx Offer:              0
Rx Request:            0   Tx Request:            0
Rx Decline:            0   Tx Decline:            0
Rx ACK:                0   Tx ACK:                0
Rx NAK:                0   Tx NAK:                0
Rx Release:            0   Tx Release:            0
Rx Inform:             0   Tx Inform:             0
Rx Lease Query:        0   Tx Lease Query:        0
Rx Lease Unassigned:   0   Tx Lease Unassigned:   0
Rx Lease Unknown:      0   Tx Lease Unknown:      0
Rx Lease Active:       0   Tx Lease Active:       0
---More---
------------------------------------------------------------
```

4) show ip http server secure status

現行の HTTP セキュリティモードのステータスを表示します。

例:

```
------------------------------------------------------------
# show ip http server secure status
HTTPS Configuration    :
====================
HTTPS Mode             : Enabled
HTTPS Redirect Mode    : Disabled
------------------------------------------------------------
```

5) show ip igmp

現行の IGMP スヌーピング情報を表示します。

例:

```
------------------------------------------------------------
# show ip igmp
IGMP Configuration:
===================
IGMP Mode              : Disabled
IGMP SSM Range         : 232.0.0.0/8
IGMP Leave Proxy       : Disabled
IGMP Flooding Control  : Enabled
IGMP Interface Setting
VID   Compatibility
----    -------------
(Please create IGMP Interfaces)
IGMP Port Status(Router-Port )
Port  Router    Dynamic Router
----   --------     --------------
1     Disabled  No
---More---
------------------------------------------------------------
```

6) show ip interface

現行の本機の IP 情報を表示します。

例:

```
------------------------------------------------------------
# show ip interface
IP Configuration:
=================
DHCP Client            : Disabled
IP Address             : 192.168.1.118
IP Mask                : 255.255.255.0
IP Router              : 0.0.0.0
DNS Server             : 0.0.0.0
VLAN ID                : 1
DNS Proxy              : Disabled
IPv6 AUTOCONFIG mode    : Disabled
IPv6 Link-Local Address: fe80::2c0:f9ff:fe66:6699
IPv6 Address           : fc80::215:c5ff:fe03:4dc0
IPv6 Prefix            : 120
IPv6 Router          :::
Active Configuration for IPv6:(Static with Stateless)
IPv6 Address: fe80:2::2c0:f9ff:fe66:6699/64 Scope:Link
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
IPv6 Address: fc80::215:c5ff:fe03:4dc0/128 Scope:Global
```

```
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
------------------------------------------------------------
```

7) show ip mld

現行の MLD スヌーピング設定を表示します。

例:

```
------------------------------------------------------------
# show ip mld
MLD Configuration:
==================
MLD Mode         : Disabled
MLD SSM Range          : ff3e::/96
MLD Leave Proxy        : Disabled
MLD Flooding Control   : Enabled
MLD Interface Setting
VID Compatibility
----    -------------
(Please create MLD Interfaces)
MLD Port Status(Router-Port )
Port  Router    Dynamic Router
----   --------    --------------
1    Disabled  No
---More---
------------------------------------------------------------
```

8) show ip ssh

現行の SSH 設定情報を表示します。

例:

```
------------------------------------------------------------
# show ip ssh
SSH Configuration  :
==================
SSH Mode   : Enabled
------------------------------------------------------------
```

9. show ip-source-guard コマンド

IP ソースガードの設定とステータスを表示します。
例:

```
------------------------------------------------------------------
# show ip-source-guard

IP Source guard Configuration:
==============================
IP Source Guard Mode: Disabled

Port  Port Mode    Dynamic Entry Limit
 ----  ----------  --------------------
1     Disabled    unlimited
2     Disabled    unlimited
3     Disabled    unlimited
4     Disabled    unlimited
5     Disabled    unlimited
6     Disabled    unlimited
7     Disabled    unlimited
8     Disabled    unlimited
9     Disabled    unlimited
10    Disabled    unlimited
---More---

IP Source Guard Entry Table:

Type     Port  VLAN  IP Address      MAC Address
-------  ----  ----  --------------  -----------------
------------------------------------------------------------------
```

10. show lacp コマンド

本機の現行の LACP 設定およびステータスを表示します。
例:

```
------------------------------------------------------------------
# show lacp ?
  config            Show LACP configuration
  statistics        Show LACP statistics
  status            Show LACP status
------------------------------------------------------------------
```

1) show lacp config

現行の LACP 設定を表示します。
例:

```
------------------------------------------------------------------
# show lacp config
LACP Configuration:
===================
System Priority:32768
Port  Mode     Key   Role    Timeout  Priority
----  --------  ----  ------  -------  --------
1     Disabled  Auto  Active  Fast     32768
2     Disabled  Auto  Active  Fast     32768
3     Disabled  Auto  Active  Fast     32768
4     Disabled  Auto  Active  Fast     32768
5     Disabled  Auto  Active  Fast     32768
```

```
6     Disabled  Auto  Active  Fast     32768
7     Disabled  Auto  Active  Fast     32768
8     Disabled  Auto  Active  Fast     32768
9     Disabled  Auto  Active  Fast     32768
10    Disabled  Auto  Active  Fast     32768
------------------------------------------------------------
```

2) show lacp statistics

現行の LACP 統計情報を表示します。

例:

```
------------------------------------------------------------
# show lacp statistics
Port  Rx Frames   Tx Frames   Rx Unknown  Rx Illegal
----  ----------  ----------  ----------  ----------
1     0           0           0           0
2     0           0           0           0
3     0           0           0           0
4     0           0           0           0
5     0           0           0           0
6     0           0           0           0
7     0           0           0           0
8     0           0           0           0
9     0           0           0           0
10    0           0           0           0
------------------------------------------------------------
```

3) show lacp status

現行の LACP ステータスを表示します。

例:

```
------------------------------------------------------------
# show lacp status
Port  Mode    Key   Aggr ID  Partner System ID  Partner Port
  Partner Port Prio
----   --------   -----    -------    -----------------
1    Disabled  1     -       -               -           -
2    Disabled  1     -       -               -           -
3    Disabled  1     -       -               -           -
4    Disabled  1     -       -               -           -
5    Disabled  1     -       -               -           -
6    Disabled  1     -       -               -           -
7    Disabled  2     -       -               -           -
8    Disabled  1     -       -               -           -
9    Disabled  1     -       -               -           -
10   Disabled  1     -       -               -           -
------------------------------------------------------------
```

11. show lldp コマンド

現行の LLDP 設定およびステータスを表示します。

1) show lldp

現行の LLDP 設定を表示します。

例:

```
------------------------------------------------------------
# show lldp
LLDP Configuration:
===================
Interval               : 30
Hold                   : 4
Tx Delay               : 2
Reinit Delay           : 2
Port Mode Port Descr System Name System Descr System Capa Mgmt
  Addr CDP awareness
----  --------  ----------   -----------    ------------
1   Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
2   Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
3   Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
4   Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
5   Disabled Enabled  Disabled  Enabled    Enabled  Enabled
  Disabled
6   Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
7   Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
8   Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
9   Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
10  Disabled Enabled  Enabled   Enabled    Enabled  Enabled
  Disabled
------------------------------------------------------------
```

2) show lldp info

LLDP ネイバー情報を表示します。

例:

```
------------------------------------------------------------
# show lldp info
Local port             : Port 6
Chassis ID             : 00-17-2E-1B-**-**
Port ID                : 2
Port Description       : Port #2
System Name            : FXC52xxPE-1
System Description     : FXC52xxPE Ver: x.xx.xx  xx-xx-xx
System Capabilities    : Bridge(+)
Management Address     : 192.168.***.***.(IPv4)
Power Over Ethernet    : PSE Device, Primary Power Source, Low
                         Priority, Power = 0.0 [W]
------------------------------------------------------------
```

3) show lldp statistics

LLDP 統計情報を表示します。

例:

```
# show lldp statistics
LLDP global counters
Neighbor entries was last changed at
  1970-01-01T00:00:00+00:00(23776 sec. ago).
Total Neighbors Entries Added       0.
Total Neighbors Entries Deleted     0.
Total Neighbors Entries Dropped     0.
Total Neighbors Entries Aged Out    0.
LLDP local counters
 Rx      Tx      Rx      Rx    Rx TLV   Rx TLV   Rx TLV
Port   Frames   Frames  Errors   Discards Errors   Unknown
  Organiz. Aged
----    ------     ------    ------   --------    ------     -
1     0       0       0       0       0       0       0      0
2     0       0       0       0       0       0       0      0
3     0       0       0       0       0       0       0      0
4     0       0       0       0       0       0       0      0
5     0       0       0       0       0       0       0      0
6     0       0       0       0       0       0       0      0
7     0       0       0       0       0       0       0      0
8     0       0       0       0       0       0       0      0
9     0       0       0       0       0       0       0      0
10    0       0       0       0       0       0       0      0
```

12. show log コマンド

現行の system log および system log 設定を表示します。

例:

```
# show log ?
  configuration     Logging configuration
  detailed          Detailed system log information
  error             Error level log records
  info              Information level log records
  warning           Warning level log records
  <cr>
```

1) show log

現行の system log の情報を表示します。

例:

```
# show log
Number of entries:
Info      : 2
Warning   : 0
Error     : 0
All       : 2
ID     Level            Time                    Message
----  ------  ------------------------         -------
1   Info   2011-01-01T00:00:00+00:00    Switch just made a cold
  boot.
```

```
2   Info   2011-01-01T00:00:03+00:00    Link up on port 7
-------------------------------------------------------------
```

2) show log configuration

現行の system log の設定を表示します。

例:

```
-------------------------------------------------------------
# show log configuration
System Log Configuration:
=========================
System Log Server Mode        : Disabled
System Log Server Address     :
System Log Level              : Error
-------------------------------------------------------------
```

3) show log detailed x

ログ ID を指定してログを表示させます。この場合の“ x ”はログ ID です。

指定した 1 つの ID のみ、または 1-10 のように範囲で指定できます。

例:

```
-------------------------------------------------------------
# show log detailed 15-20
ID    Level     Time                          Message
----  ------  -------------------------  -------
  15  Info 1970-01-01T09:00:04+09:00  PoE is enabled on port 4.
  16  Info 1970-01-01T09:00:04+09:00  PoE is enabled on port5.
  17  Info 1970-01-01T09:00:04+09:00  PoE is enabled on port 6.
  18  Info 1970-01-01T09:00:05+09:00  PoE is enabled on port 7.
  19  Info 1970-01-01T09:00:05+09:00  PoE is enabled on port 8.
  20  Info  1970-01-01T09:00:05+09:00  Link up on port 8.
-------------------------------------------------------------
```

(1) show log error

エラーレベルのログ情報を表示します。

(2) show log info

情報レベルのログ情報を表示します。

(3) show log warning

警告レベルのログ情報を表示します。

13. show loopback-detection コマンド

ループバック検知の設定およびステータスを表示します。

例:

```
-------------------------------------------------------------
# show loopback-detection ?
  config            Loop protect configuration
  ethernet          Show loop protection port configuration
  status            Show the loop protection status
-------------------------------------------------------------
```

1) show loopback-detection config

ループバック検知の設定を表示します。

例:

```
-------------------------------------------------------------
# show loopback-detection config
Loop Protection Configuration:
==============================
Loop Protection : Disabled
Transmission Time: 5
Shutdown Time   : 180
-------------------------------------------------------------
```

2) show loopback-detection ethernet

ループプロテクションのポートの設定を表示します。

例:

```
-------------------------------------------------------------
# show loopback-detection ethernet
Port  Mode     Action       Transmit
----   --------    ------------      --------
1     Enabled   Shutdown     Enabled
2     Enabled   Shutdown     Enabled
3     Enabled   Shutdown     Enabled
4     Enabled   Shutdown     Enabled
5     Enabled   Shutdown     Enabled
6     Enabled   Shutdown     Enabled
7     Enabled   Shutdown     Enabled
8     Enabled   Shutdown     Enabled
9     Enabled   Shutdown     Enabled
10    Enabled   Shutdown     Enabled
-------------------------------------------------------------
```

3) show loopback-detection status

ループプロテクションのステータスを表示します。

例:

```
------------------------------------------------------------
  # show loopback-detection status
Port   Action  Transmit  Loops  Status  Loop  Time of Last Loop
----   ------------      --------   --------  --------     -
1     Shutdown     Enabled     0  Down      -     -
2     Shutdown     Enabled     0  Down      -     -
3     Shutdown     Enabled     0  Down      -     -
4     Shutdown     Enabled     0  Down      -     -
5     Shutdown     Enabled     0  Down      -     -
6     Shutdown     Enabled     0  Down      -     -
7     Shutdown     Enabled     0  Up        -     -
8     Shutdown     Enabled     0  Down      -     -
9     Shutdown     Enabled     0  Down      -     -
10    Shutdown     Enabled     0  Down      -     -
------------------------------------------------------------
```

14. show mac-address-table コマンド

MAC アドレステーブルおよびその他の機能の情報を表示します。

例:

```
-------------------------------------------------------------
# show mac-address-table ?
  aging-time        Aging time for entries in the address table
  address           Address information
  learning          Show the port learn mode
  statistics        Show MAC address table statistics
  <cr>
-------------------------------------------------------------
```

1) show mac-address-table

MAC アドレステーブル情報を表示します。

例:

```
-------------------------------------------------------------
# show mac-address-table
Type    VID  MAC Address       Ports
------  ---  -----------------  -----
Static    1    00-17-2e-1b-b8-1b  None,CPU
Dynamic   1    00-17-2e-21-99-b6  1
Static    1    33-33-00-00-00-01  1-18,CPU
Static    1    33-33-00-00-00-02  1-18,CPU
Static    1    33-33-ff-1b-b8-1b  1-18,CPU
Static    1    33-33-ff-a8-01-01  1-18,CPU
-------------------------------------------------------------
```

2) show mac-address-table aging-time

MAC アドレステーブルのエージングタイムを表示します。

例:

```
-------------------------------------------------------------
# show mac-address-table aging-time
MAC Age Time: 300
-------------------------------------------------------------
```

3) show mac-address-table address x-x-x-x-x-x

MAC アドレステーブル内のアドレス"x-x-x-x-x-x"の情報を表示します。

例:

```
-------------------------------------------------------------
# show mac-address-table address 00-17-2e-21-99-b6
Type    VID  MAC Address       Ports
------  ---  -----------------  -----
Dynamic 1    00-17-2e-21-99-b6  1
-------------------------------------------------------------
```

4) show mac-address-table learning

ポートの学習モードを表示します。

例:

```
------------------------------------------------------------
  # show mac-address-table learning
Port  Learning
----  --------
1     Auto
2     Auto
3     Auto
4     Auto
5     Auto
6     Auto
7     Auto
8     Auto
9     Auto
10    Auto
------------------------------------------------------------
```

5) show mac-address-table statistics

MAC アドレステーブルの統計情報を表示します。

例:

```
------------------------------------------------------------
# show mac-address-table statistics
Port  Dynamic Addresses
----  -----------------
1     0
2     0
3     0
4     0
5     0
6     0
7     23
8     0
9     0
10    0
Total Dynamic Addresses : 23
Total Static Addresses  : 7
------------------------------------------------------------
```

15. show mac-security コマンド

ポートセキュリティのリミットコントロールを表示します。

例:

```
-------------------------------------------------------------
# show mac-security
Port Security Limit Control Configuration:
==========================================
Mode         : Disabled
Aging        : Disabled
Age Period   : 3600
Port  Mode     Limit  Action         State
----  --------     -----  ---------------      -------------
 1   Disabled     4 None           Disabled
 2   Disabled     4 None           Disabled
 3   Disabled     4 None           Disabled
 4   Disabled     4 None           Disabled
 5   Disabled     4 None           Disabled
 6   Disabled     4 None           Disabled
 7   Disabled     4 None           Disabled
 8   Disabled     4 None           Disabled
 9   Disabled     4 None           Disabled
10   Disabled     4 None           Disabled
-------------------------------------------------------------
```

16. show management コマンド

本機の管理セキュリティの設定および統計情報を表示します。

1) show management

管理用 IP フィルタの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show management
Access Mgmt Configuration:
==========================
System Access Mode: Disabled
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH
Idx VID  Start IP Address    End IP Address       W S T
-------------------------------------------------------------
  -
```

2) show management statistics

管理セキュリティの統計情報を表示します。

例:

```
-------------------------------------------------------------
# show management statistics
Access Management Statistics:
-----------------------------
HTTP      Receive:  0    Allow:       0    Discard:     0
HTTPS     Receive:  0    Allow:       0    Discard:     0
SNMP      Receive:  0    Allow:       0    Discard:     0
TELNET    Receive:  0    Allow:       0    Discard:     0
SSH       Receive:  0    Allow:       0    Discard:     0
-------------------------------------------------------------
```

3) show map

QoS ポートのクラス分けおよび QoS ポートのクラス分け Map (Tag Remarking モードが“Mapped”の場合は (QoS クラス、DP レベル) から (PCP、DEI) マッピング) を表示します。

例:

```
------------------------------------------------------------
# show map
QoS Port Classification:
========================
Port  QoS class  DP level  PCP  DEI  Tag class.
----  ---------  --------  ---  ---  ----------
1     0          0         0    0    Disabled
2     0          0         0    0    Disabled
3     4          0         0    0    Disabled
4     0          0         0    0    Disabled
5     0          0         0    0    Disabled
6     0          0         0    0    Disabled
7     0          0         0    0    Disabled
8     0          0         0    0    Disabled
9     0          0         0    0    Disabled
10    0          0         0    0    Disabled
QoS Port Classification Map:
============================
Port  PCP  DEI  QoS class  DP level
----  ---  ---  ---------  --------
1     0    0    1          0
      0    1    1          1
      1    0    0          0
      1    1    0          1
      2    0    2          0
      2    1    2          1
      3    0    3          0
      3    1    3          1
      4    0    4          0
      4    1    4          1
      5    0    5          0
      5    1    5          1
      6    0    6          0
      6    1    6          1
      7    0    7          0
      7    1    7          1
---More---
------------------------------------------------------------
```

17. show mvr コマンド

MVR 設定およびステータスを表示します。

例:

```
-------------------------------------------------------------
# show mvr ?
  config      Show MVR configuration
  group       Show MVR group addresses
  sfm         Show SFM(including SSM) related information for
              MVR
  statistics  Show MVR operational statistics
-------------------------------------------------------------
```

1) show mvr config

MVR 設定を表示します。

例:

```
-------------------------------------------------------------
# show mvr config
MVR Configuration:
==================
MVR Mode: Disabled
MVR Interface Setting
VID   Name    Mode     Tagging   Priority  LLQI
----   ---------------------------------
  ----------
10    aaa                  Dynamic   Tagged    0        5
[Port Setting of aaa(VID-10)]
Inactive Port    : 1-10
[Channel Setting of aaa(VID-10)]
Name             : aaa
Start Address    : 224.0.0.1
End Address      : 224.0.0.10
MVR Immediate Leave Setting
Port  Immediate Leave
----  ---------------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled
-------------------------------------------------------------
```

2) show mvr group

MVR グループを表示します。

3) show mvr sfm

MVR の SFM(SSM を含む)関連情報を表示します。

4) show mvr statistics

MVR 統計情報を表示します。

例:

```
-------------------------------------------------------------
# show mvr statistics
IPv4  Querier   Rx     Tx      Rx        Rx        Rx        Rx
VID   Status    Query  Query   V1 Join   V2 Join   V3 Join V2 Leave
----    -------    ----------    ----------     ----------
10    DISABLE  0         0         0         0         0
  0
IPv6  Querier  Rx        Tx        Rx        Rx        Rx
VID   Status   Query     Query     V1 Report  V2 Report  V1 Done
----    -------    ----------    ----------     ----------
10    DISABLE  0         0         0         0         0
-------------------------------------------------------------
```

18. show ntp コマンド

本機のシステムタイムの設定情報を表示します。

```
-------------------------------------------------------------
# show ntp ?
  config            Show NTP configuration
  dst               Show daylight Saving configuration
  zone              Show system timezone configuration
-------------------------------------------------------------
```

1) show ntp config

NTP 設定情報を表示します。

例:

```
-------------------------------------------------------------
# show ntp config
NTP Configuration:
==================
NTP Mode: Disabled
Idx   Server IP host address(a.b.c.d) or a host name string
---   ----------------------------------------------------
1     64.90.182.55
2     64.236.96.53
3
4
5
-------------------------------------------------------------
```

2) show ntp dst

サマータイムの設定を表示します。

例:

```
------------------------------------------------------------
# show ntp dst
System Daylight Saving Time(DST) Configuration:
================================================
Daylight Saving Time Mode: Non-Recurring.
Daylight Saving Time Start Time Settings:
       Week:     0
       Day:      0
     * Month:1
     * Date:     1
     * Year:     2000
     * Hour:     0
     * Minute:   0
Daylight Saving Time End Time Settings:
       Week:     0
       Day:      0
     * Month:1
     * Date:     1
     * Year:     2000
     * Hour:     0
     * Minute:0
Daylight Saving Time Offset: 1(minutes)

*: This symbol indicates the parameter needs to be set the
  reasonable value.
------------------------------------------------------------
```

3) show ntp zone

システムのタイムゾーンの情報を表示します。

例:

```
------------------------------------------------------------
# show ntp zone
System Timezone Configuration:
==============================
Timezone Offset: 5400(540 minutes)
Timezone Acronym: Japan
------------------------------------------------------------
```

19. show poe コマンド

PoE 設定およびステータスを表示します。

```
-------------------------------------------------------------
# show poe ?
  auto-checking     Show PoE auto checking
  config            Show PoE configuration
  ethernet          Show PoE port configuration
  power-delay       Show POE power delay
  scheduling        Show PoE scheduling
  status            Show the PoE status
-------------------------------------------------------------
```

1) show poe auto-checking

PoE オートチェックの設定とステータスを表示します。

例

```
-------------------------------------------------------------
show poe auto-checking

Ping Check
-----------
Disable

Port  Ping IP Address   Interval Time(sec)  Retry Time  Failure
  Log   Failure Action    Reboot Time(sec)
----  ---------------  ------------------  ----------
1     0.0.0.0    30     3   err=0  tot=0    Nothing          15
2     0.0.0.0    30     3   err=0  tot=0    Nothing          15
3     0.0.0.0    30     3   err=0  tot=0    Nothing          15
4     0.0.0.0    30     3   err=0  tot=0    Nothing          15
5     0.0.0.0    30     3   err=0  tot=0    Nothing          15
6     0.0.0.0    30     3   err=0  tot=0    Nothing          15
7     0.0.0.0    30     3   err=0  tot=0    Nothing          15

Port  Ping IP Address   Interval Time(sec)  Retry Time  Failure
  Log     Failure Action
Reboot Time(sec)
 ----------  ------------------  ----------------  ---------
8     0.0.0.0     30    3   err=0    tot=0    Nothing      15
9     PoE not supported
10    PoE not supported
-------------------------------------------------------------
```

2) show poe config

本機の PoE 設定を表示します。

例:

```
------------------------------------------------------------
# show poe config
PoE Configuration:
==================
Primary Power Supply
---------------------
220 [W]

Power management
-----------------
Max. port power determined by : class.
Power management mode         : consumption
------------------------------------------------------------
```

3) show poe ethernet

ポートの PoE 設定を表示します。

例:

```
------------------------------------------------------------
# show poe ethernet
Port  Mode  Priority Max.  Power [W]
----   -------   -------------    ---------
1     PoE     Low       15.4
2     PoE     Low       15.4
3     PoE     Low       15.4
4     PoE     Low       15.4
5     PoE     Low       15.4
6     PoE     Low       15.4
7     PoE     Low       15.4
8     PoE     Low       15.4
9     PoE not supported
10    PoE not supported
------------------------------------------------------------
```

4) show poe power-delay

PoE 給電遅延の設定とステータスを表示します。

例

```
------------------------------------------------------------
# show poe power-delay

Port  Delay Mode    Delay Time(0~300 sec)
----  ------------  ---------------------
1     Disabled          0
2     Disabled          0
3     Disabled          0
4     Disabled          0
5     Disabled          0
6     Disabled          0
7     Disabled          0
8     Disabled          0
9     PoE not supported
10    PoE not supported
------------------------------------------------------------
```

5) show poe scheduling

PoE のスケジューリングの設定を表示します。

例

```
------------------------------------------------------------
# show poe scheduling

Port  Status
----  ------
1     Disable
2     Disable
3     Disable
4     Disable
5     Disable
6     Disable
7     Disable
8     Disable
9     PoE not supported
10    PoE not supported
---More---

Port
1
Hour  Sun  Mon  Tue  Wed  Thu  Fri  Sat
----  ---  ---  ---  ---  ---  ---  ---
0     x    x    x    x    x    x    x
1     x    x    x    x    x    x    x
2     x    x    x    x    x    x    x
3     x    x    x    x    x    x    x
4     x    x    x    x    x    x    x
5     x    x    x    x    x    x    x
6     x    x    x    x    x    x    x
7     x    x    x    x    x    x    x
8     x    x    x    x    x    x    x
9     x    x    x    x    x    x    x
10    x    x    x    x    x    x    x
11    x    x    x    x    x    x    x
---More---
```

```
-------------------------------------------------------------
```

6) show poe status

現在の PoE ステータスを表示します。

例:

```
-------------------------------------------------------------
# show poe status
Port  PD Class  Port Status Power Requested[W]  Power Used [W]
  Current Used [mA]
----  --------  ---------------------------------------
  ---------------
1     0       PoE turned OFF    0.0          0.0          0
2     0       PoE turned OFF    0.0          0.0          0
3     0       PoE turned OFF    0.0          0.0          0
4     0       PoE turned OFF    0.0          0.0          0
5     0       PoE turned OFF    0.0          0.0          0
6     0       PoE turned OFF    0.0          0.0          0
7     0       PoE turned OFF    0.0          0.0          0
8     0       PoE turned OFF    0.0          0.0          0
9     PoE not supported
10    PoE not supported
-------------------------------------------------------------
```

20. show port monitor コマンド

ポートのミラーリング機能の設定情報を表示します。

例:

```
-------------------------------------------------------------------
# show port monitor
Mirror Configuration:
=====================
Mirror Port: 5
Port  Mode
----  --------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled
CPU   Disabled
-------------------------------------------------------------------
```

21. show queue コマンド

QCL(Queue Control List) 設定およびステータスを表示します。

例:

```
-------------------------------------------------------------
# show queue ?
  status             Show QCL status.
  <cr>
-------------------------------------------------------------
```

1) show queue

QCL 設定情報を表示します。

例:

```
-------------------------------------------------------------
# show queue
QoS QCL:
========
ID     Frame    SMAC     DMAC VID    PCP  DEI  Class DP DSCP
  Port
--    -----    --------    ----   ---------      ---    ---
  ---
10     Any      Any      Any  Any    Any  Any   0     -   -     5
Number of QCEs: 1
-------------------------------------------------------------
```

2) show queue status

QCL ステータスを表示します。

例:

```
-------------------------------------------------------------
# show queue status
User        ID  Frame  Class DP DSCP  Conflict  Port
----------      --   -----    -----  --  ---------  --------
Static       10   Any    0    -   -       No     5
Number of QCEs: 1
-------------------------------------------------------------
```

22. show radius-server コマンド

RADIUS サーバの設定情報および統計情報を表示します。

1) show radius-server

RADIUS サーバの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show radius-server
Server Timeout   : 15 seconds
Server Dead Time: 300 seconds
RADIUS Authentication Server Configuration:
=========================================
Server  Mode     IP Address      Secret           Port
 --------     ----------------------------------------
1       Disabled                                 1812
2       Disabled                                 1812
3       Disabled                                 1812
4       Disabled                                 1812
5       Disabled                                 1812
RADIUS Accounting Server Configuration:
```

```
=====================================
Server  Mode      IP Address       Secret             Port
------    --------     ---------------      ----------
1       Disabled                                  1813
2       Disabled                                  1813
3       Disabled                                  1813
4       Disabled                                  1813
5       Disabled                                  1813
------------------------------------------------------------
```

(2) show radius-server statistics x

RADIUS サーバの統計情報を表示します。この場合の“x”は RADIUS サーバのインデックス（1～5 の値）です。

```
------------------------------------------------------------
# show radius-server statistics 1

Server #1 (0.0.0.0:1812) RADIUS Authentication Statistics:
Rx Access Accepts:     0   Tx Access Requests:           0
Rx Access Rejects:     0   Tx Access Retransmissions:    0
Rx Access Challenges:  0   Tx Pending Requests:          0
Rx Malformed Acc. Responses: 0   Tx Timeouts:            0
Rx Bad Authenticators: 0
Rx Unknown Types:      0
Rx Packets Dropped:    0
State:                  Disabled
Round-Trip Time:       0 ms
Server #1 (0.0.0.0:1813) RADIUS Accounting Statistics:
Rx Responses:          0   Tx Requests:                  0
Rx Malformed Responses:0   Tx Retransmissions:           0
Rx Bad Authenticators: 0   Tx Pending Requests:          0
Rx Unknown Types:      0   Tx Timeouts:                  0
Rx Packets Dropped:    0
State:                 Disabled
Round-Trip Time:       0  ms
------------------------------------------------------------
```

23. show running-config コマンド

本機で現在動作している設定情報を表示します。

```
-----------------------------------------------------------------
# show running-config
!building running-config, please wait.....
!FXC52xxPE
calendar set 3 16 48 january 6 1970
!
……
……
interface ethernet 1/9
private-vlan 1
switchport allowed vlan add 1
!
interface ethernet 1/10
private-vlan 1
switchport allowed vlan add 1
!
exit
interface vlan 1
ip address 192.168.1.1 255.255.255.0
ipv6 address ::192.168.1.1 96
exit
exit
!
end
-----------------------------------------------------------------
```

24. show rate-limit ethernet コマンド

各ポートのレートリミット設定情報を表示します。

例:

```
-----------------------------------------------------------------
# show rate-limit ethernet
QoS Port Policer:
=================
Port  Parm                Policer
---- --------            ---------
1    Mode                Disabled
     Rate                500 kbps
     Unit                kbps
     Flow Ctl            Disabled
2    Mode                Disabled
     Rate                500 kbps
     Unit                kbps
     Flow Ctl            Disabled
3    Mode                Disabled
     Rate                500 kbps
     Unit                kbps
     Flow Ctl            Disabled

-----------------------------------------------------------------
```

25. show rmon コマンド

RMON の設定を表示します。

例:

```
-------------------------------------------------------------
# show rmon ?
  alarm             Show RMON alarm entries
  event             Show RMON event entries
  history           Show RMON history entries
  statistics        Show RMON statistics entries
-------------------------------------------------------------
```

1) show rmon alarm

RMON アラームの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show rmon alarm
Id    Interval       Alarm Variable          Alarm SampleType
-----   ---------   ------------------------
  ------------
1               30    .1.3.6.1.2.1.2.2.1.10.1    deltaValue
Number of entries: 1
-------------------------------------------------------------
```

2) show rmon event

RMON イベント情報を表示します。

例:

```
-------------------------------------------------------------
# show rmon event
Id    Description  Type  Community   LastSent
-----   ------------    -----    -----------    ---------
1     abc            none         public      Never
Number of entries: 1
-------------------------------------------------------------
```

3) show rmon history

RMON 履歴情報を表示します。

例:

```
-------------------------------------------------------------
# show rmon history
Id  Data Source controlBucketsRequested
  controlBucketsGranted  Interval
----- ------------------------------
10        .1.3.6.1.2.1.2.2.1.1.10    50       50     1800

Number of entries: 1
-------------------------------------------------------------
```

4) show rmon statistics

RMON 統計情報を表示します。

例:

```
# show rmon statistics
Id  Data Source          etherStatsOctets  etherStatsPkts
  therStatsCRCAlignErrors
----- -------------------------------- ------------------
  10  .1.3.6.1.2.1.2.2.1.1.10    0          0             0

Number of entries: 1
```

26. show sflow コマンド

sFlow 設定情報を表示します。

例:

```
# show sflow ?
  counter_poller    Show counter polling interval configuration per
                    port
  flow_sampler      Show flow sampler configuration per port.
  receiver          Show the sFlow receiver
  statistics        Show statistics
```

1) show sflow counter_poller

ポート単位の sFlow カウンタのポーリング間隔を表示します。

例:

```
# show sflow counter_poller
Counter Poller Configuration:
=============================
Port  Interval
----  --------
8     10
```

2) show sflow flow_sampler

ポート単位の sFlow サンプラの設定情報を表示します。

例:

```
# show sflow flow_sampler
Flow Sampler Configuration:
===========================
Port  Sampling  Rate  Max Hdr
----  ------------  -------
8     20      128
```

3) show sflow receiver

sFlow レシーバの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show sflow receiver
Receiver Configuration:
=======================
Owner            : <none>
Receiver         : 0.0.0.0
UDP Port         : 6343
Max. Datagram    : 1400 bytes
Time left        : 0 seconds
-------------------------------------------------------------
```

4) show sflow statistics receiver

レシーバの統計情報を表示します。

例:

```
-------------------------------------------------------------
# show sflow statistics receiver
Receiver Statistics:
====================
Tx Successes      Tx Errors    Flow Samples   Counter   Samples
---------------   ---------------  ---------------     ----
  0                 0                  0                  0
-------------------------------------------------------------
```

5) show sflow statistics samplers

ポート単位の統計情報を表示します。

例:

```
-------------------------------------------------------------
# show sflow statistics samplers
Per-Port Statistics:
====================
No non-zero counters.
-------------------------------------------------------------
```

27. show snmp コマンド

本機の SNMP 設定を表示します。

例:

```
-------------------------------------------------------------
# show snmp ?
  access             SNMPv3 access entry
  community          SNMPv3 community entry
  group              SNMPv3 group entry
  user               SNMPv3 user entry
  view               SNMPv3 view entry
  <cr>
-------------------------------------------------------------
```

1) show snmp

本機の SNMP 設定情報を表示します。

例:

```
# show snmp
SNMP Configuration:
==================
SNMP Mode                      : Enabled
SNMP Version                   : 2c
Read Community                 : public
Write Community                : private
Trap Mode                      : Disabled
Trap Version                   : 1
Trap Community                 : public
Trap Destination               : 192.168.1.10
Trap IPv6 Destination          :::
Trap Authentication Failure    : Disabled
Trap Link-up and Link-down     : Enabled
Trap Inform Mode               : Enabled
Trap Inform Timeout(seconds)   : 1
Trap Inform Retry Times        : 5
Trap Probe Security Engine ID  : Enabled
Trap Security Engine ID        :
Trap Security Name             : None
SNMPv3 Engine ID               : 800007e5017f000001
```

2) show snmp access

SNMPv3 アクセスエントリを表示します。

例:

```
# show snmp access
SNMPv3 Accesses Table:
Idx Group Name     Model  Level   ReadView    WriteView
---  ------------------------------  -----
1   default_ro_group  any   NoAuth, NoPriv  default_view
  None
2   default_rw_group  any   NoAuth, NoPriv  default_view
  default_view
Number of entries: 2
```

3) show snmp community

SNMPv3 コミュニティのエントリを表示します。

例:

```
# show snmp community
SNMPv3 Communities Table:
Idx  Community           Source IP     Source Mask
---  ------------------------------  ---------------
1   public                0.0.0.0         0.0.0.0
2   private               0.0.0.0         0.0.0.0
3   yyy                 192.168.1.11    255.255.255.0
Number of entries: 3
```

4) show snmp group

SNMPv3 グループエントリを表示します。

例:

```
# show snmp group
SNMPv3 Groups Table;
Idx Model Security Name         Group Name
--- ----- --------------------------------
1   v1    public                default_ro_group
2   v1    private               default_rw_group
3   v2c   public                default_ro_group
4   v2c   private               default_rw_group
5   usm   default_user          default_rw_group
Number of entries: 5
```

5) show snmp user

SNMPv3 ユーザのエントリを表示します。

例:

```
# show snmp user
SNMPv3 Users Table:
Idx Engine ID    User Name           Level          Auth
  Priv
--------   --------------------------------
  --------------
1      Local      default_user     NoAuth, NoPriv   None
  None
Number of entries: 1
```

6) show snmp view

SNMPv3 ビューエントリを表示します。

例:

```
# show snmp view
SNMPv3 Views Table:
Idx  View Name            View Type  OID Subtree
---  --------------------------------   ---------
1   default_view       included    .1
2   xxx                included    .1
3   yyy                included    .10
Number of entries: 3
```

28. show spanning-tree コマンド

本機のスパニングツリーの設定情報を表示します。

例:

```
# show spanning-tree ?
  ethernet          Show STP Port configuration
  mst               Show MSTP configuration
  statistics        Show STP port statistics
  status            Show STP Bridge status
  <cr>
```

1) show spanning-tree

システムのスパニングツリーの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show spanning-tree
STP Configuration      :
==================
Protocol Version       : MSTP
Hello Time             : 2
Max Age                : 20
Forward Delay          : 15
Tx Hold Count          : 6
Max Hop Count          : 20
BPDU Filtering         : Disabled
BPDU Guard             : Disabled
Error Recovery         : Disabled
-------------------------------------------------------------
```

2) show spanning-tree ethernet

ポートのスパニングツリーの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show spanning-tree ethernet
Port  Mode    AdminEdge  AutoEdge restrRole  restrTcn
  bpduGuard  Point2point
----   --------    ----------    --------    ---------
Aggr  Enabled  Disabled   Enabled   Disabled  Disabled
  Disabled   Enabled

Port  Mode    AdminEdge  AutoEdge restrRole restrTcn
  bpduGuard Point2point
----   --------    ----------    --------    ---------
1 Disabled  Disabled  Enabled Disabled  Disabled  Disabled
  Auto
2 Disabled  Disabled   Enabled   Disabled  Disabled  Disabled
  Auto
3  Disabled  Disabled   Enabled   Disabled  Disabled
  Disabled   Auto
4  Disabled  Disabled   Enabled   Disabled  Disabled
  Disabled   Auto
5  Disabled  Disabled   Enabled   Disabled  Disabled
  Disabled   Auto
6  Disabled  Disabled   Enabled   Disabled  Disabled
  Disabled   Auto
7  Disabled  Disabled   Enabled   Disabled  Disabled
  Disabled   Auto
8  Disabled  Disabled   Enabled   Disabled  Disabled
  Disabled   Auto
9  Disabled  Disabled   Enabled   Disabled  Disabled
  Disabled   Auto
10 Disabled  Disabled   Enabled   Disabled  Disabled  Disabled
  Auto
-------------------------------------------------------------
```

3) show spanning-tree ethernet x

ポートのマルチスパニングツリーの設定情報を表示します。この場合の"x"は、MSTI のインデックス(0～7 までの値)です。

例:

```
# show spanning-tree ethernet 0
MSTI  Port  Path Cost   Priority
----   ----   ----------    --------
CIST  Aggr  Auto       128
MSTI  Port  Path Cost   Priority
----   ----   ----------    --------
CIST  1    Auto       128
CIST  2    Auto       128
CIST  3    Auto       128
CIST  4    Auto       128
CIST  5    Auto       128
CIST  6    Auto       128
CIST  7    Auto       128
CIST  8    Auto       128
CIST  9    Auto       128
CIST  10   Auto       128
```

4) show spanning-tree mst

システムの MSTP の設定情報を表示します。

例:

```
# show spanning-tree mst
Configuration name: xxx
Configuration rev.: 10
MSTI#  Bridge Priority
-----   ---------------
CIST  32768
MSTI1 32768
MSTI2 32768
MSTI3 32768
MSTI4 32768
MSTI5 32768
MSTI6 32768
MSTI7 32768
MSTI   VLANs mapped to MSTI
----    --------------------
MSTI1  No VLANs mapped
MSTI2  No VLANs mapped
MSTI3  No VLANs mapped
MSTI4  No VLANs mapped
MSTI5  No VLANs mapped
MSTI6  No VLANs mapped
MSTI7  No VLANs mapped
```

5) show spanning-tree statistics

STP ポートの統計情報を表示します。

例:

```
-------------------------------------------------------------
# show spanning-tree statistics
Port Rx MSTP   Tx MSTP   Rx RSTP   Tx RSTP   Rx STP   Tx STP   Rx
  TCN   Tx TCN   Rx Ill.  Rx Unk.
---------  --------  --------  --------  --------  -------
-------------------------------------------------------------
```

6) show spanning-tree status x

MSTP ブリッジのステータスを表示します。この場合の"x"は、MSTI のインデックス(0～7 までの値)です。

例:

```
-------------------------------------------------------------
# show spanning-tree status 0
CIST Bridge STP Status
Bridge ID       :32768.00-17-2E-xx-xx-xx
Root ID         :32768.00-17-2E-xx-xx-xx
Root Port       : -
Root PathCost   : 0
Regional Root   :32768.00-17-2E-xx-xx-xx
Int. PathCost   : 0
Max Hops        : 20
TC Flag         : Steady
TC Count        : 0
TC Last         : -
Port   Port Role   State    Pri  PathCost  Edge  P2P  Uptime
--------  ------------  ---------  ---  --------  ----  ---  ------------
-------------------------------------------------------------
```

29. show storm-control コマンド

本機のストームコントロールの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show storm-control
QoS Storm Control:
==================
Storm Unicast       : Disabled    1 pps
Storm Multicast     : Disabled    1 pps
Storm Broadcast     : Disabled    1 pps
-------------------------------------------------------------
```

30. show system コマンド

本機のシステム情報および設定情報を表示します。

例:

```
-------------------------------------------------------------
# show system
System Contact     :
System Name        :
System Location    :
Software Version   : FXC52xxPE Ver:1.00.xx
Software Date      : xxxx-xx-xx
MAC Address        : 00-17-2e-xx-xx-xx
Number of Ports    : xx
```

```
Previous Restart    : Warm
------------------------------------------------------------
```

31. show tacacs-server コマンド

TACACS+ 認証サーバの設定情報を表示します。

例:

```
------------------------------------------------------------
# show tacacs-server
Server Timeout             : 15 seconds
Server Dead Time           : 300 seconds
TACACS+ Authentication Server Configuration:
==========================================
Server  Mode     IP Address      Secret                      Port
------    --------     ---------------
1       Disabled                                             49
2       Disabled                                             49
3       Disabled                                             49
4       Disabled                                             49
5       Disabled                                             49
------------------------------------------------------------
```

32. show trunk コマンド

本機のトランク設定情報を表示します。

例:

```
------------------------------------------------------------
# show trunk ?
  all           Shows all Trunking Group Configuration
  <cr>
------------------------------------------------------------
```

1) show trunk

システムのトランク情報を表示します。

例:

```
------------------------------------------------------------
# show trunk
Aggregation Configuration:
==========================
Aggregation Mode:
SMAC      : Enabled
DMAC      : Disabled
IP        : Enabled
Port      : Enabled
------------------------------------------------------------
```

2) show trunk all

すべてのトランキンググループ情報を表示します。

例:

```
------------------------------------------------------------
# show trunk all
Aggr ID   Name   Type    Configured   Ports   Aggregated
  Ports
-------    ------     ------   ---------------
1        LLAG1      Static   1,2                  None
------------------------------------------------------------
```

33. show users コマンド

ユーザの設定情報を表示します。

例:

```
-------------------------------------------------------------
# show users
Users Configuration:
====================
User Name                       Privilege Level
-----------------------------------------------
admin                               3
ad01                                3
op01                                2
gu01                                1
-------------------------------------------------------------
```

34. show version

システムのバージョン、およびモデル情報を表示します。

例:

```
-------------------------------------------------------------
# show version
Software Version: FXC52xxPE Ver:1.00.xx
Software Date   : xxxx-xx-xx
Number of Ports :
-------------------------------------------------------
```

35. show vlan コマンド

本機の VLAN 設定情報を表示します。

例:

```
-------------------------------------------------------------
# show vlan  ?
  id                VLAN interface
  isolation         Isolation VLAN entry
  name              VLAN interface name
  port-based        Port-Based Virtual LAN Configuration
  voice             Show voice VLAN configuration
  <cr>
-------------------------------------------------------------
```

1) show vlan

802.1Q VLAN 設定情報(VLAN ID、VLAN 名、割り当てポート)がすべて表示されます。

例:

```
-------------------------------------------------------------
# show vlan
TPID is 0x8888
VID   VLAN Name           Ports
----  -------------------------------  -----
1     default             1-10
10    aaa                 None
VLAN forbidden port list:
=========================
VID   VLAN Name               Ports
----  -------------------------------  -----
10    aaa                     2
-------------------------------------------------------------
```

2) show vlan id x

VLAN x の VLAN 設定情報を表示します。この場合の“x”は VLAN ID です。

例:

```
# show vlan  id 10
VID   VLAN Name  User     Ports     Conflicts  Conflict_Ports
----  ----------------  -------------
10    aaa         Static         None           No      None
                  MVR            None           No      None
                  Combined       None           No      None
VLAN forbidden port list:
=========================
VID   VLAN Name          Ports
----  --------------------------------  -----
10    aaa                 2
```

3) show vlan isolation

ポートアイソレーション設定情報を表示します。

例:

```
# show vlan isolation
Port  Isolation
----  ---------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled
```

4) show vlan name xxx

VLAN xxx の VLAN 設定情報を表示します。この場合の“xxx”は、VLAN 名です。

例:

```
# show vlan name aaa
VID   VLAN Name  User               Ports
  Conflicts  Conflict_Ports
-----------------------------------------
10    aaa         Static         None       No         None
                  MVR            None       No         None
                  Combined       None       No         None
VLAN forbidden port list:
=========================
VID   VLAN Name          Ports
----  --------------------------------  -----
10    aaa                 2
-----------------------------------------------
```

5) show vlan port-based

ポートベース VLAN 設定情報を表示します。

例:

```
------------------------------------------------------------
# show vlan port-based
PVLAN ID        Ports
--------        -----
1         1-10
------------------------------------------------------------
```

6) show vlan voice

音声 VLAN 設定情報を表示します。

例:

```
------------------------------------------------------------
# show vlan voice
Voice VLAN Configuration:
=========================
Voice VLAN Mode               : Disabled
Voice VLAN VLAN ID            : 1000
Voice VLAN Age Time(seconds)  : 86400
Voice VLAN Traffic Class      : 7
Voice VLAN OUI Table          :
=====================
Telephony OUI  Description
-------------      -----------
00-01-E3     Siemens AG phones
00-03-6B     Cisco phones
00-0F-E2     H3C phones
00-60-B9     Philips and NEC AG phones
00-D0-1E     Pingtel phones
00-E0-75     Polycom phones
00-E0-BB     3Com phones
Voice VLAN Port Configuration:
==============================
Port  Mode     Security   Discovery Protocol
----   --------     --------     ------------------
1     Disabled  Disabled    OUI
2     Disabled  Disabled    OUI
3     Disabled  Disabled    OUI
4     Disabled  Disabled    OUI
5     Disabled  Disabled    OUI
6     Disabled  Disabled    OUI
7     Disabled  Disabled    OUI
8     Disabled  Disabled    OUI
9     Disabled  Disabled    OUI
10    Disabled  Disabled    OUI
------------------------------------------------------
```

2 章 WEB による設定方法

2.1 Telnet/SNMP 管理

2.1.1 Telnet によるマネジメント管理

Telnet を介して本機のリモート管理を行う場合は、まず IP/NetMask/Gateway(任意)アドレスを設定し、コンソール画面を使って、操作を行ってください。

2.1.2 SNMP によるマネジメント管理

NMS を介して本機のリモート管理を行う場合は、IP/NetMask/Gateway アドレスを設定して、SNMP の設定を行ってください。

本機では、SNMP v1, v2c, v3 のエージェント機能および MIB II(Interface)、Bridge MIB、802.1Q MIB および Private MIB をサポートしています。
初期設定の GET コミュニティ名は“public”、および SET コミュニティ名は“private”です。

2.2 初期設定

ここでは、WEB ブラウザを用いて本製品の WEB マネジメント画面にログインする手順を説明いたします。

2.2.1 設定方法

WEB ブラウザを使用してログインするには以下の手順に従ってください。

Step 1. WEB ブラウザを起動します。

Step 2. WEB ブラウザのアドレスに本製品の IP アドレスを入力し、Enter キーを入力します。
(初期設定時は、IP アドレスは「192.168.1.1」に設定されています。)

Step 3. 認証用ダイアログボックスに、「ユーザー名」と「パスワード」を入力します。
(初期設定時は「ユーザー名」と「パスワード」ともに"admin"となります。)

IP アドレスを変更する場合は、以下の手順に従ってください。

1. プロンプトが"(config)#"になっている状態で、"interface vlan 1"コマンドを入力すると、"(config-if)#"がプロンプト表示されます。
"ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy"コマンド(xxx.xxx.xxx.xxx は IP アドレス、yyy.yyy.yyy.yyy はネットマスク)を入力して、本体の IP アドレスを変更します。

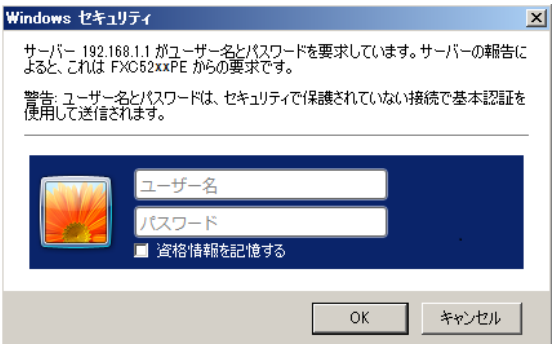
2. "exit"コマンドを入力して、"(config)#"に戻ります。

3. IP ゲートウェイを設定する場合は、"ip default-gateway xxx.xxx.xxx.xxx"コマンドを入力して、本体の IP ゲートウェイ(xxx.xxx.xxx.xxx は IP アドレス)を設定してください。
"exit"コマンドを入力して、"#"のプロンプト表示に切り替わります。
"show ip interface"を入力して、IP が正しく設定されているかどうか確認してください。

【初期設定値】

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	なし
Username	admin
Password	admin

【認証用ダイアログボックス】

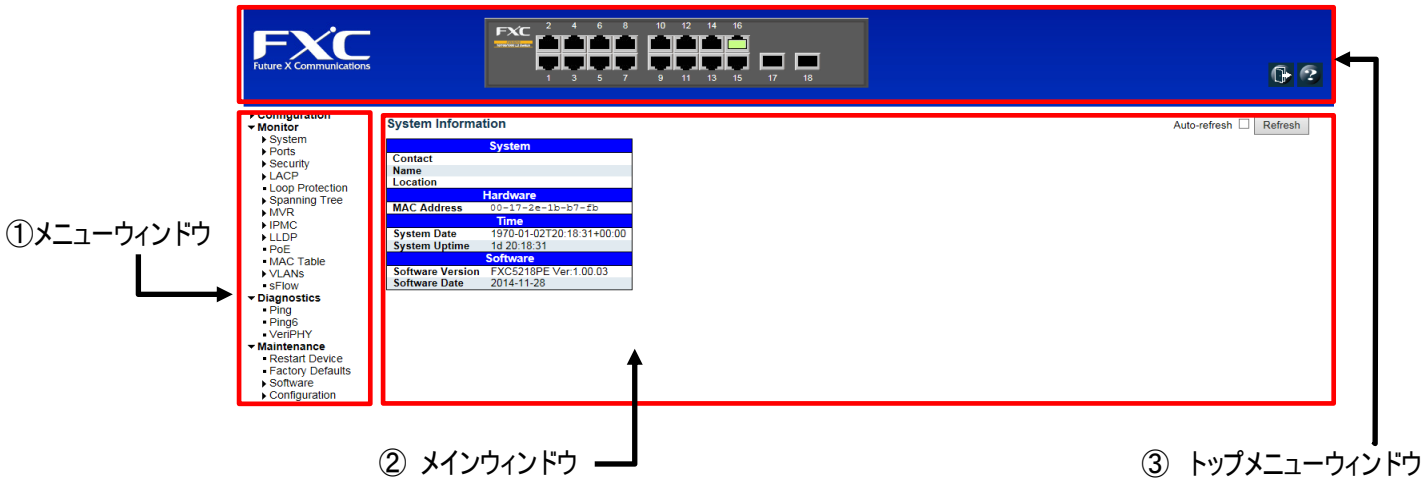


【注意】:
本機はユーザ管理機能をサポートしており、管理者のみがシステムを設定することが可能です。複数のユーザが管理者の ID を使用する場合は、システム設定を行うために最初にログインしたユーザのみ許可します。それ以外のユーザは、管理者の ID を使用しても、システムのモニタリングのみ可能です。最大 3 ユーザのみが同時にログインすることが可能です。

【注意】:
WEB ブラウザは“Microsoft IE 6.0”以上、”Netscape V7.1”以上、あるいは”Fire Fox V1.00”以上、またモニターは解像度を”1024x768”以上でご使用になることを推奨します。

1. 画面の構成

本製品の WEB マネジメント画面は以下のウィンドウで構成しています。



2. 設定/表示項目

① メニューウィンドウ
メニューウィンドウでは、本製品でサポートされる各メニューがツリー状に表示されます。

② メインウィンドウ
メニューウィンドウで選択したメニューの設定項目、及びステータス情報を表示します。

③ トップメニューウィンドウ
本製品のインターフェイスが表示されており、各ポートの状態を 10/100M でリンクアップしている場合は「橙」、1000M でリンクアップしている場合は「緑」で表します。また各ポートをクリックすることにより、カウンターのメニューが表示されます。
「Logout」ボタンをクリックすることにより、本製品からログアウトします。
「Show help」からは表示メニューの Help を別ウィンドウで表示することが可能です。

画面の右上に以下のアイコンが表示されます。


ログアウト用のボタンです。


ヘルプ情報を入手することができます。

HTTP 接続によるマネジメント方法の詳細は、以降の項で説明します。

2.3 Configuration (各機能の設定)

ここでは、本機の各種機能についての設定方法について説明します。

2.3.1 System （システム情報）

2.3.1.1 Information (システム情報の設定)

「Configuration」→「System」→「Information」をクリックすると、以下の画面が表示されます。
ここでは、システム名、設置場所、システム担当者名を設定します。

System Information Configuration

System Contact	
System Name	
System Location	

Save Reset

2.3.1.2 IP

「System」→「IP」をクリックすると、以下の画面が表示されます。

IP Configuration

	Configured	Current
DHCP Client	☐	Renew
IP Address	192.168.11.214	192.168.11.214
IP Mask	255.255.255.0	255.255.255.0
IP Router	192.168.11.1	192.168.11.1
VLAN ID	1	1
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy	☐

Save Reset

ここでは、本機の IP を設定することができます。
DHCP クライアント機能を有効にすると、DHCP サーバから自動的に IP が設定されます。
DHCP クライアント機能を無効にすると、手動にて IP を設定を行うことができます。

2.3.1.3 IPv6

「System」→「IPv6」をクリックすると、以下の画面が表示されます。
ここでは本機の IPv6 の設定を行うことが出来ます。

IPv6 Configuration

	Configured	Current
Auto Configuration	☐	Renew
Address	::192.168.1.1	::192.168.1.1 Link-Local Address: fe80::217:2eff:fe1b:b7fb
Prefix	96	96
Router	::	::

Save Reset

IPv6 ルータが接続されている状態の場合、「Auto Configuration」機能を有効にすると、自動的に IP が設定されます。また、手動で IP を設定することもできます。

2.3.1.4 NTP

「Configuration」→「System」→「NTP」をクリックすると、次の画面が表示されます。
ここでは本機の NTP の設定を行うことが出来ます。

NTP Configuration

Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Save Reset

本機は、NTP プロトコルをサポートしているため、NTP サーバから時刻情報を入手することができます。

1. 「Configuration」→「System」→「Time」をクリックして、"Get Time By"を"Time Server"に設定します。
   その後、本画面にて NTP サーバの IP を入力します。

【注記】:
NTP 機能を有効にするには、ネットワーク管理者によって、まず NTP サーバの IP を入手する必要があります。

2. 次に、「Configuration」→「System」→「Time」をクリックして、タイムゾーンおよびサマータイムの設定を行います。

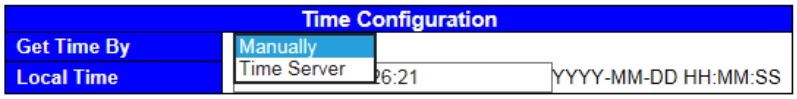
2.3.1.5 Time

「Configuration」→「System」→「Time」をクリックすると、以下の画面が表示されます。
ここでは時刻の設定を行うことができます。

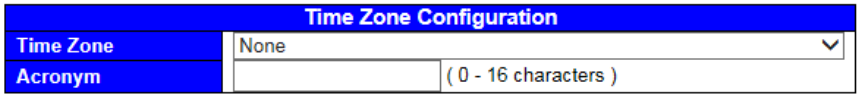
NTP を使用してタイムゾーンを設定することができます。NTP では、英国のグリニッジを通る地球の本初子午線（経度 0）を基準とする協定世界時が使用されます（協定世界時は、UTC と呼ばれるものであり、正式名称はグリニッジ標準時間（GMT））。デバイスの正確な時間を保持することにより、システムログはイベントエントリの日時を正確に記録します。

ローカルタイムに応じて現在の時刻を表示するには、お使いのタイムゾーンの設定を行ってください。

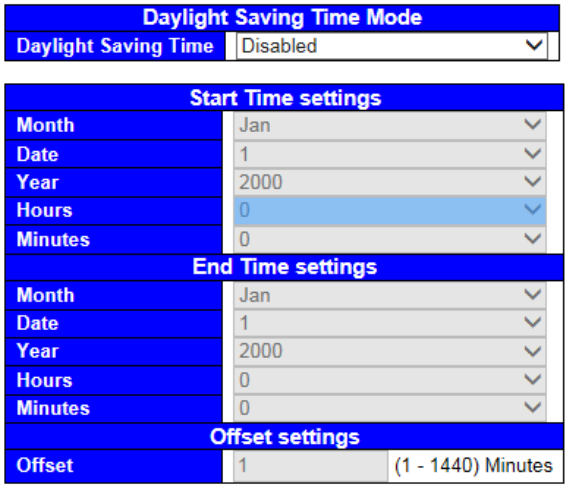
Time Configuration



Time Zone Configuration



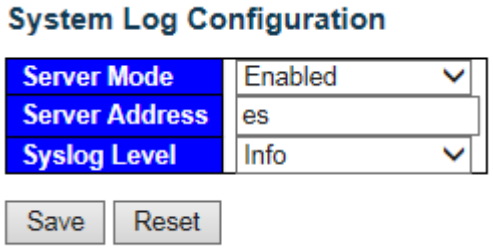
Daylight Saving Time Configuration



「サマータイム」機能により、通常の時刻より 1 時間早くシステムタイムを設定することが可能です。
開始時間と終了時間を設定することで、その期間サマータイム機能を有効化できます。

2.3.1.6 Log

「Configuration」→「System」→「Log」をクリックすると、以下の画面が表示されます。
ここでは、Syslog サーバを設定します。この機能を有効にすると、Syslog サーバにイベントが記録されます。



サーバアドレスに Syslog サーバのアドレスを設定します。これにより、syslog サーバへイベントが送信されます。本機の DNS 機能が有効な場合は、ホスト名としても使用可能です(IPv4 のみ対応)。

Syslog レベルでは、syslog サーバに送信されるメッセージの種類を選択できます。

有効なモードは以下のとおりです。
- Info : 情報、警告、エラーメッセージを送信します。
- Warning : 警告、エラーメッセージを送信します。
- Error : エラーメッセージを送信します。

2.3.2 Power Reduction (消費電力制御機能)

ここでは、消費電力制御機能の EEE の設定を行います。

2.3.2.1 EEE

「Configuration」→「Power Reduction」→「EEE」をクリックすると、以下の画面が表示されます。

EEE Configuration

		EEE Urgent Queues							
Port	Enabled	1	2	3	4	5	6	7	8
*	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	☐	☐	☐	☐	☐	☐	☐	☐	☐
15	☐	☐	☐	☐	☐	☐	☐	☐	☐
16	☐	☐	☐	☐	☐	☐	☐	☐	☐
17	☐	☐	☐	☐	☐	☐	☐	☐	☐
18	☐	☐	☐	☐	☐	☐	☐	☐	☐

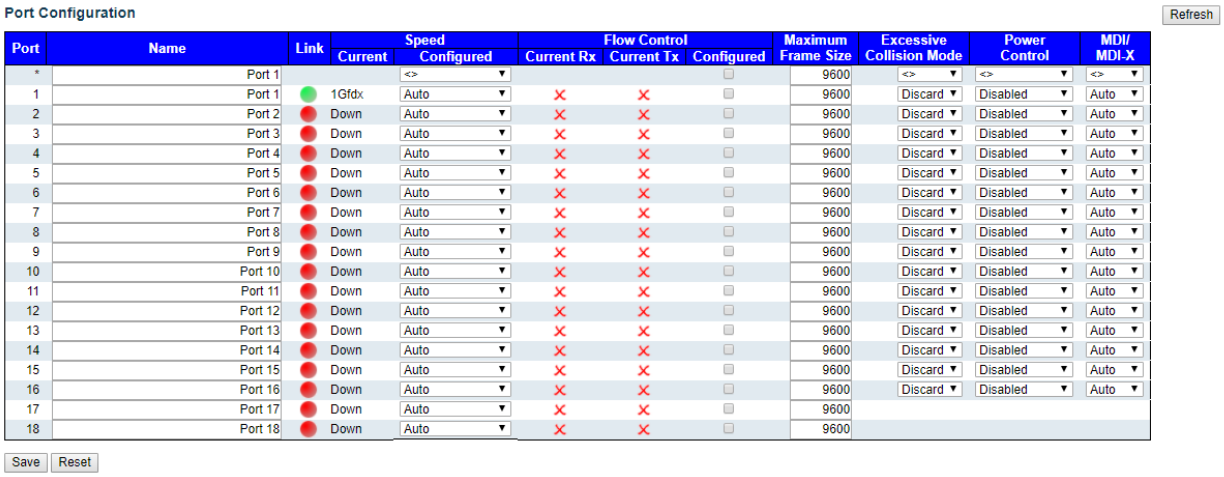
Save Reset

ここでは、本機の EEE を設定して、ポート単位で電源の消費を抑えます。
EEE Urgent Queues は、データが有効になると、フレームの送信を行います。
それ以外は、省エネを最大限にするために、「3000 バイト」までのデータが送信状態になるまで待機します。

2.3.3 Ports（ポートの設定）

2.3.3.1 Ports

ここでは、ポートのリンク状態の確認や、ポートネーム、通信速度、フローコントロール、最大フレームサイズ、コリジョンモード、パワーコントロール、MDI/MDI-Xなどの設定を行います。
「Configuration」→「Ports」→「Ports」をクリックすると、以下の画面が表示されます。

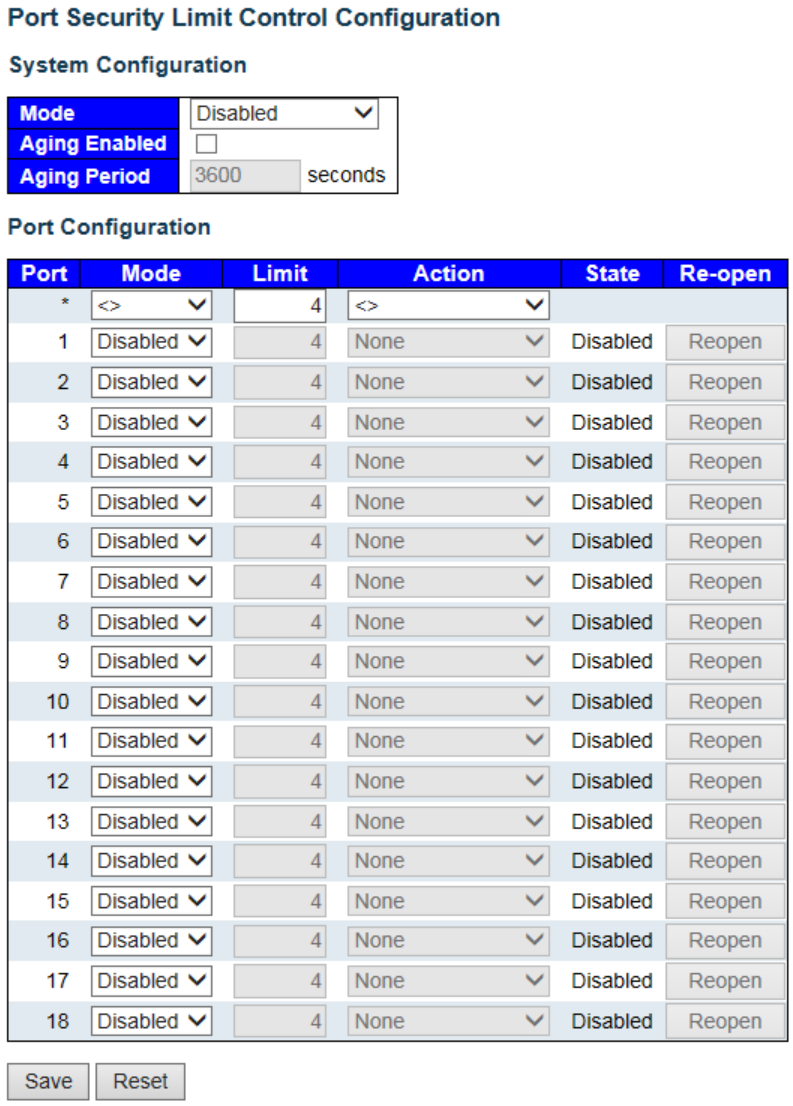


ポートの設定	
Name	インタフェース名を設定します。各ポートに文字を記述することができます。
Speed	通信速度および通信方式の設定を行います。
Flow Control	全二重通信時のフロー制御を設定します
Excessive Collision Mode	半二重通信時のコリジョン機能の設定をします。
Maximum Frame Size	最大フレームサイズを設定します。範囲は「1518-9600」バイトです。 尚、設定する場合は、本機に接続する他のネットワーク機器がジャンボフレーム機能に対応しているか確認してください。
Power Control	ポートの消費電力機能を設定します。 - Disabled : すべての消費電力方式を無効にします。 - ActiPHY : リンクしてない場合の消費電力を有効にします。 - PerfectReach: リンク時の消費電力を有効にします。 ショートケーブル使用時の消費電力を有効にします。 - Enabled : リンクアップ/ダウン時に消費電力を有効にします。
MDI/MDI-X	ポートのMDI/MDI-Xモード(Auto、MDI、MDI-Xのいずれか)を設定します。 MDI-Xはパソコン用、MDIはハブ/スイッチ用です。「Auto」に設定すると、自動検知を行います

2.3.3.2 Limit Control（リミットコントロール）

「Configuration」→「Ports」→「Limit Control」をクリックすると、以下の画面が表示されます。

ここでは、本機の各ポートのリミットコントロールの設定を行うことが出来ます。



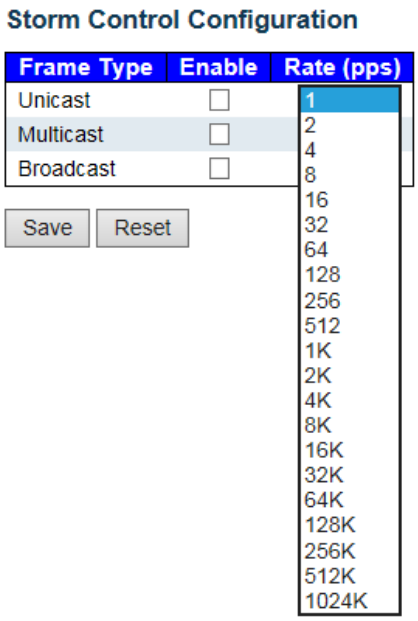
ポートのリミットコントロールが有効な場合は、指定ポートのユーザ数の上限を制限します。
ユーザは MAC アドレスおよび VLAN ID で識別されます。

上限を超えると以下の 4 つのいずれかのアクションが実行されます。
・None: 上限を超過した場合ユーザ接続を許可しません。但し、それ以外のアクションは実行されません。
・Trap : SNMP トラップを送信します。
・Shutdown: ポートをシャットダウンします。<Reopen>ボタンをクリックすると、ポートを復旧します。
・Trap & Shutdown: 上記の"Trap"および"Shutdown"アクションが実行されます。

2.3.3.3 Storm Control（ストームコントロール）

「Configuration」→「Ports」→「Storm Control」をクリックすると、以下の画面が表示されます。

ここでは、本機のストームコントロールの設定を行うことが出来ます。



ユニキャストストーム、マルチキャストストーム、ブロードキャストストームのそれぞれのレートコントロールの設定を行います。
これらの設定は、MAC アドレステーブル上にない VLAN ID, DMAC(宛先 MAC アドレス)などのフラッディングしたフレームを対象としています。
設定には、スイッチ間のユニキャスト、マルチキャスト、ブロードキャストのトラフィックの設定を行います。

2.3.4 Security (セキュリティ機能)

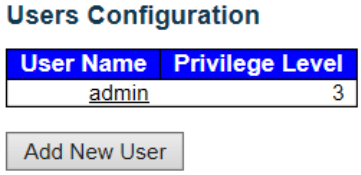
ここでは、本機のセキュリティ機能の設定について説明します。

2.3.4.1 Switch

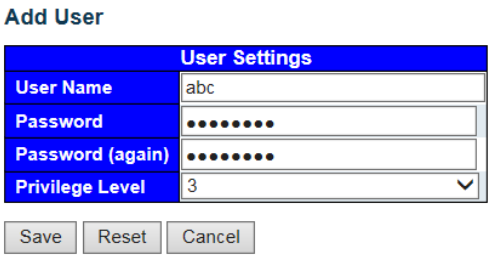
1) Users

各ユーザの設定を行うには、「Configuration」→「Security」→「Switch」→「Users」をクリックします。

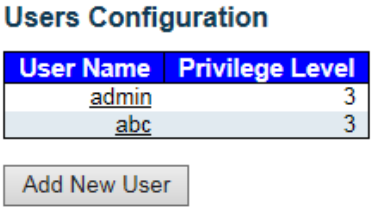
本機のユーザ情報を設定します。ユーザのレベルには以下のとおり 3 段階あります。
[3]： 管理者用。ユーザは本機の設定をすべて行うことができます。
[2]： オペレータ用。ユーザは本機の設定画面およびステータスを表示することが可能です。
ユーザは本機のメンテナンスを実行することができます。
[1]： ゲスト用。ユーザは、本機の設定画面およびステータスのみを表示することが可能です。



1. 新規ユーザを登録する場合は、<Add New User>ボタンをクリックすると、以下の画面が表示されるので
ユーザ名とパスワード、ユーザレベルをそれぞれ設定してください。
ユーザレベルは、1～3 までの 3 段階に設定可能です。

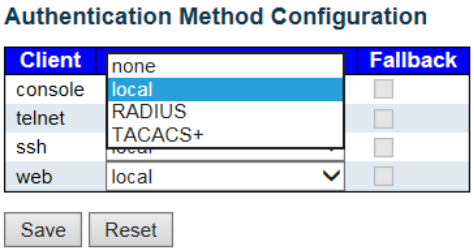


2. <Save>ボタンをクリックすると、ユーザの設定画面が表示されます。



2） Auth Method （認証方式）

「Configuration」→「Security」→「Switch」→「Auth Method」をクリックすると、以下の画面が表示されます。



ここでは、マネジメント用の認証方式を設定します。

認証方式は、以下のとおりです。

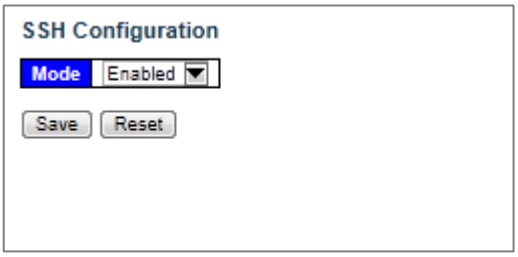
- none ： 認証は可能ですが、ログインは不可です。
- local ： 本機のローカルユーザ情報の認証のみ可能です。
- radius ： 認証用のリモート RADIUS サーバを設定します。
- tacacs+ ： 認証用のリモート TACACS+サーバを設定します。

「Fallback」メニューを選択すると、認証に失敗した場合には、ローカルのユーザデータによる認証が行われるようになります。

RADIUS サーバおよび TACACS+サーバの設定方法については、「Configuration」→「Security」→「AAA」を参照してください。

3） SSH

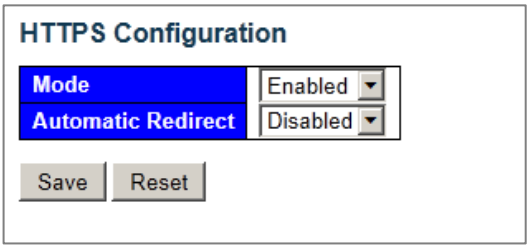
「Configuration」→「Security」→「Switch」→「SSH」をクリックすると、以下の画面が表示されます。



ここでは、リモート Telnet 用の SSH 機能を設定します。

4） HTTPS

「Configuration」→「Security」→「Switch」→「HTTPS」をクリックすると、以下の画面が表示されます。

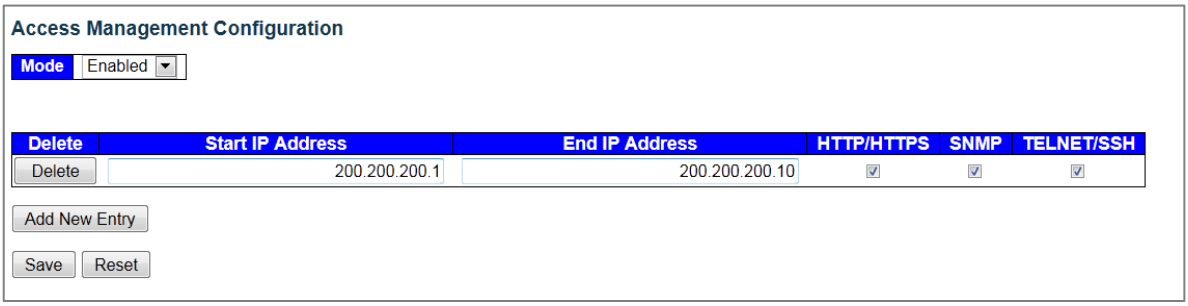


ここでは、WEB の HTTPS セキュリティ機能を有効にします。

HTTPS 設定の「mode」および「Automatic Redirect」の両方が有効、あるいは無効な場合は WEB ブラウザを HTTP 用に切り替えます。

5) Access Management (アクセス管理)

「Configuration」→「Security」→「Switch」→「Access Management」をクリックすると、以下の画面が表示されます。



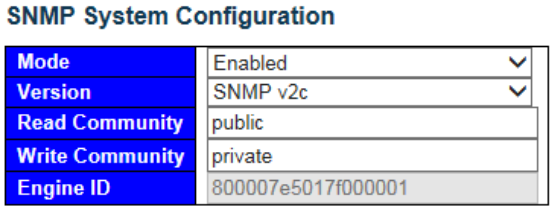
ここでは、リモート管理用に IP アドレスのレンジを設定することが可能です。リモート管理用インタフェースは、HTTP/HTTPS、SNMP、TELNET/SSH です。

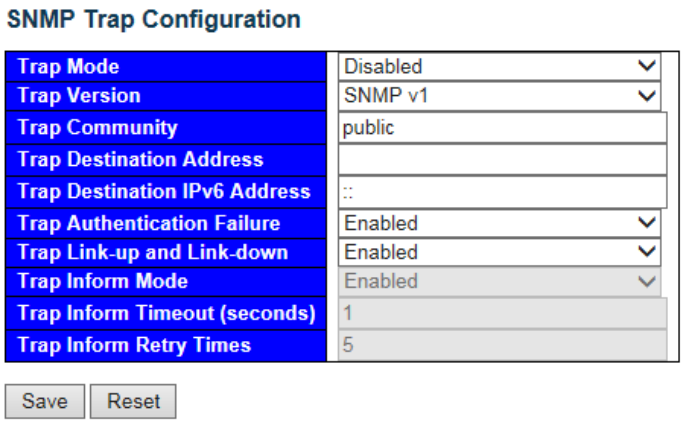
6) SNMP

ここでは、SNMP の設定について説明します。

6-1) System (SNMP システムの設定)

「Configuration」→「Security」→「Switch」→「SNMP」→「System」をクリックすると、以下の画面が表示されます。

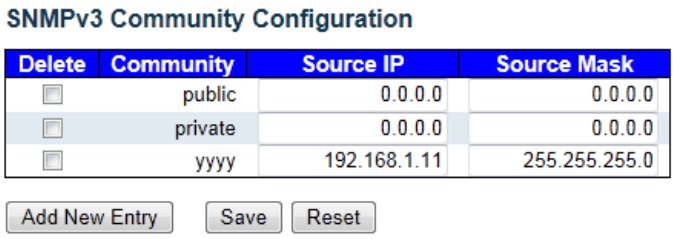




ここでは、SNMP システム情報およびトラップ機能を設定します。

6-2) Communities (SNMPv3 コミュニティの設定)

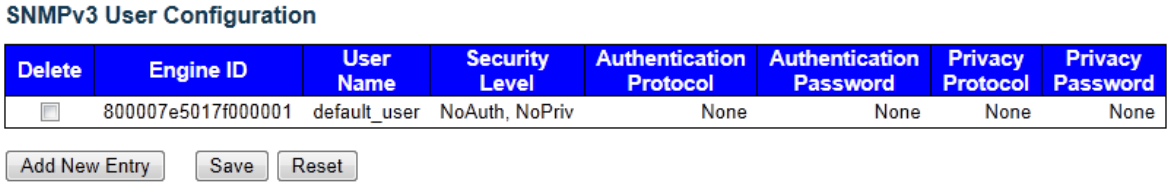
「Configuration」→「Security」→「Switch」→「SNMP」→「Communities」をクリックすると、以下の画面が表示されます。



ここでは、SNMPv3 コミュニティのエントリの追加および削除を行うことができます。

6-3) Users (SNMP ユーザを設定)

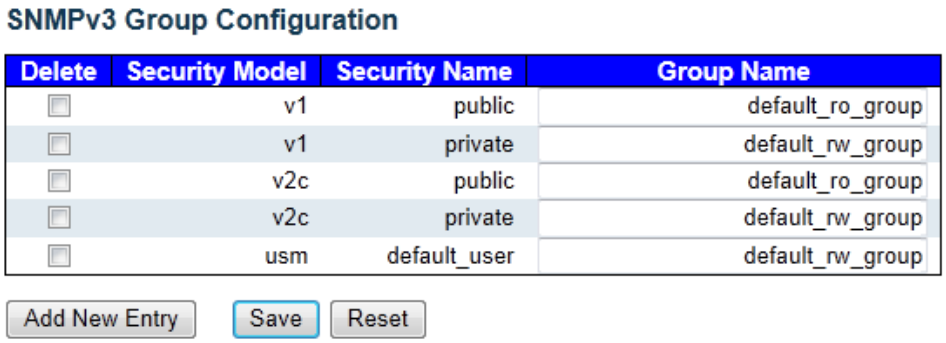
「Configuration」→「Security」→「Switch」→「SNMP」→「Users」をクリックすると、以下の画面が表示されます。



ここでは、SNMPv3 ユーザのエントリの追加/削除を行うことができます。

6-4) Groups (SNMPv3 グループの設定)

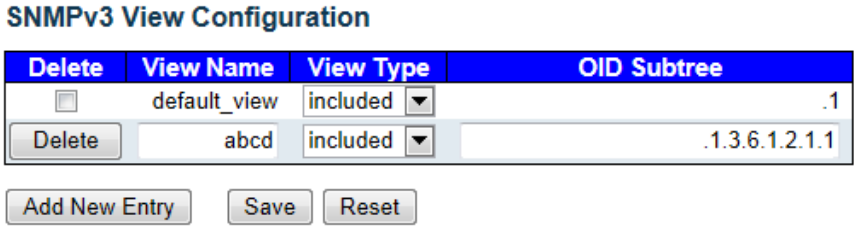
「Configuration」→「Security」→「Switch」→「SNMP」→「Groups」をクリックすると、以下の画面が表示されます。



ここでは、SNMPv3 グループのエントリの追加/削除を行うことができます。

6-5) Views (SNMPv3 View の設定)

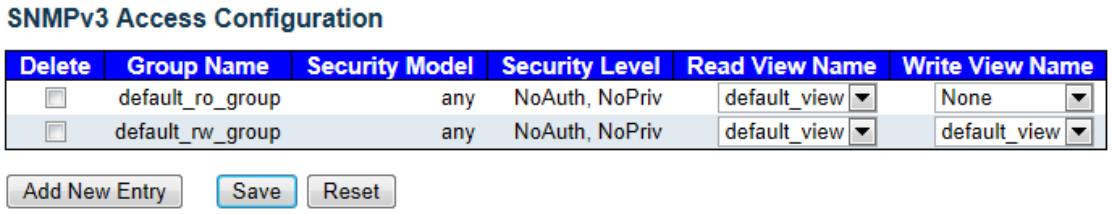
「Configuration」→「Security」→「Switch」→「SNMP」→「Views」をクリックすると、以下の画面が表示されます。



ここでは、SNMPv3 View のエントリの追加/削除を行うことができます。

6-6) Access (SNMPv3 Access の設定)

「Configuration」→「Security」→「Switch」→「SNMP」→「Access」をクリックすると、以下の画面が表示されます。



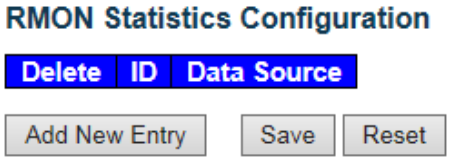
ここでは、SNMPv3 Access のエントリの追加/削除を行うことができます。

7) RMON

ここでは RMON の設定について説明します。

7-1) Statistics (RMON 統計情報)

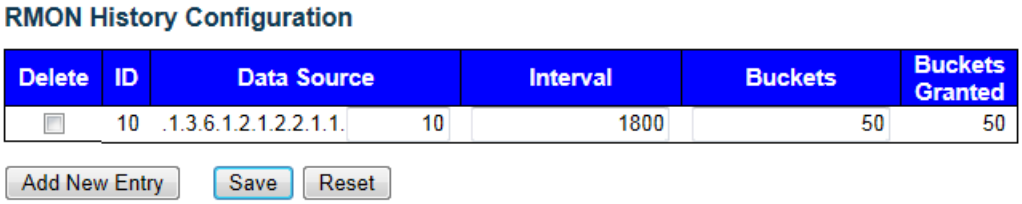
「Configuration」→「Security」→「Switch」→「RMON」→「Statistics」をクリックすると、以下の画面が表示されます。



ここでは、RMON 統計情報のエントリの追加/削除を行うことができます。

7-2) History (RMON 履歴)

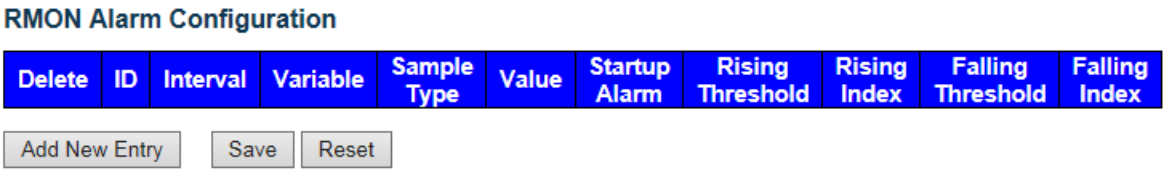
「Configuration」→「Security」→「Switch」→「RMON」→「History」をクリックすると、以下の画面が表示されます。



ここでは、RMON 履歴のエントリの追加/削除を行うことができます。

7-3) Alarm (RMON Alarm の設定)

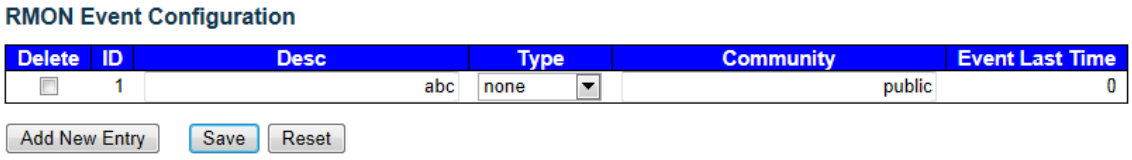
「Configuration」→「Security」→「Switch」→「RMON」→「Alarm」をクリックすると、アラームの設定画面が下記のように表示されます。



ここでは、RMON アラームのエントリの追加/削除を行うことができます。

7-4) Event (RMON イベントの設定)

「Configuration」→「Security」→「Switch」→「RMON」→「Event」をクリックすると、以下の画面が表示されます。



ここでは、RMON イベントのエントリの追加/削除を行うことができます。

2.3.4.2 Network(ネットワークの設定)

ここでは、ネットワークの設定について説明します。

1) NAS

「Configuration」→「Security」→「Network」→「NAS」をクリックすると、以下の画面が表示されます。

Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	☐
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	☐
RADIUS-Assigned VLAN Enabled	☐
Guest VLAN Enabled	☐
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	☐
Mac Auth Username Format	with-hyphen / Lower-case

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	☐	☐	☐			
1	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
17	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
18	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

Save Reset

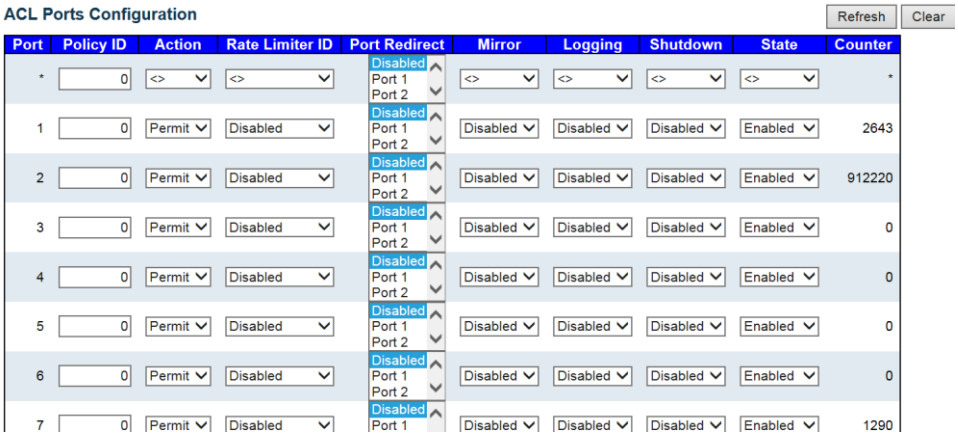
ここでは、802.1x ネットワークアクセスコントロール機能を設定します。ポートを介するネットワークアクセスにはまずユーザの認証が必要になります。RADIUS サーバにより認証を行います。

2） ACL

ここでは、ACL の設定について説明します。

2-1） Ports (ACL のポートの設定)

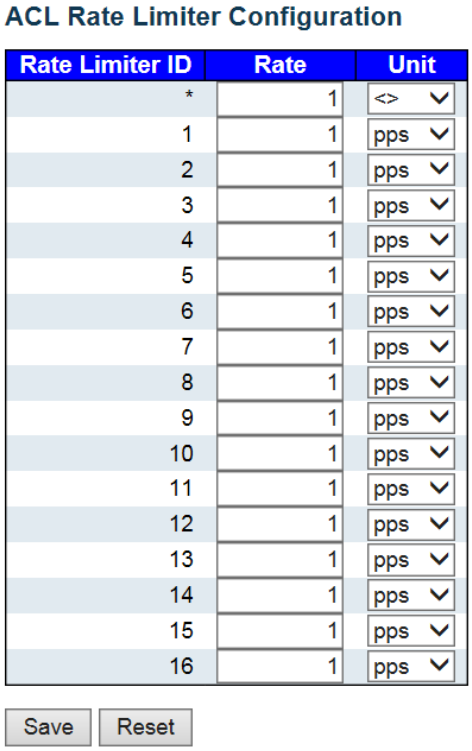
「Configuration」→「Security」→「Network」→「ACL」→「Ports」をクリックすると、以下の画面が表示されます。



ここでは、各ポートの ACL パラメータ(ACE:アクセスコントロールエントリ)を設定します。
これらのパラメータは、フレームが特定の ACE と一致しない場合は、ポートで受信したフレームに適用されます。

2-2） Rate Limiters (レートリミット機能の設定)

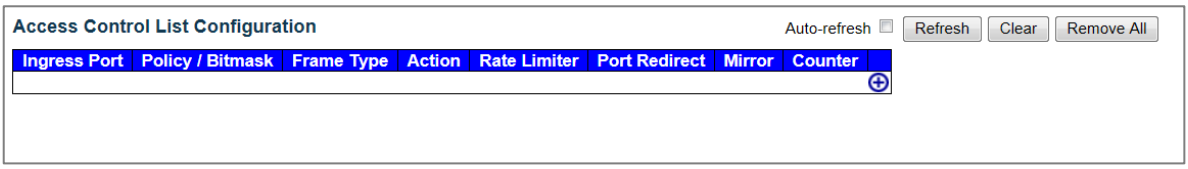
「Configuration」→「Security」→「Network」→「ACL」→「Rate Limiters」をクリックすると、以下の画面が表示されます。



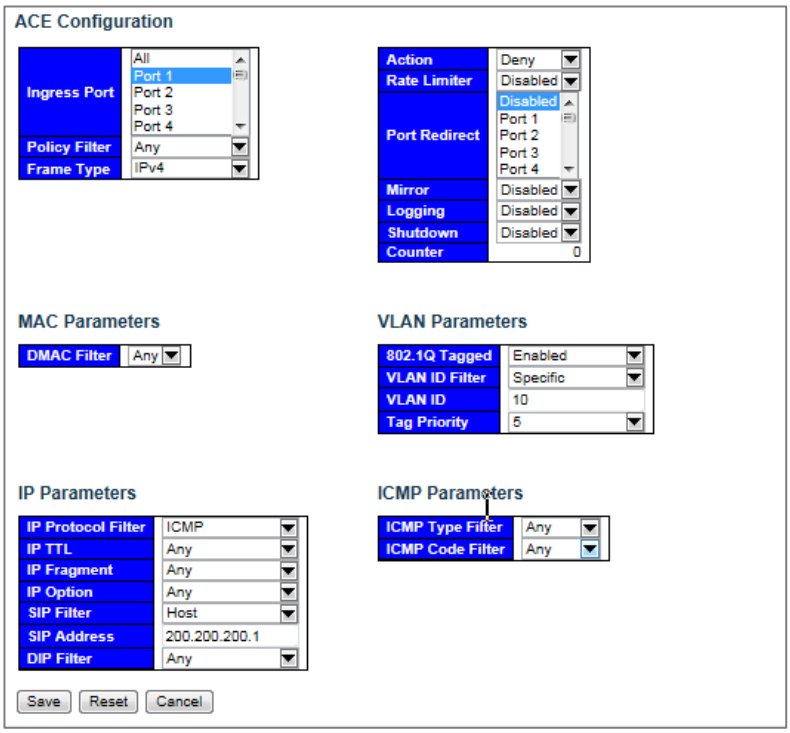
ACL のレートリミット機能を使用します。レートリミット機能は、pps(Packet per second)、または kbps(Kilo bit per second)単位で設定されます。なお、入力フレームのみの制御です。
イーサネットフレームに対しての制御のため、TCP セッションに対しては、設定値と異なるレートになる場合があります。

3) Access Control List (アクセスコントロールリストの設定)

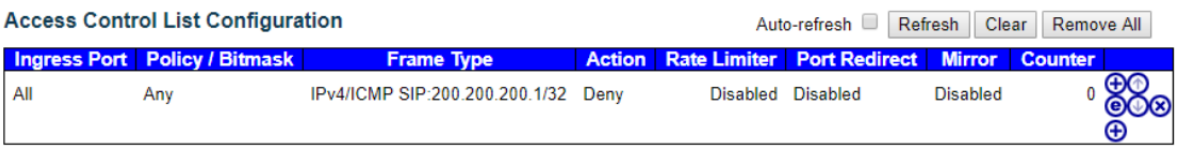
「Configuration」→「Security」→「Network」→「ACL」→「Access Control List」をクリックすると、以下の画面が表示されます。ここでは、アクセスコントロールリストの設定ができます。



1. "(+)"をクリックすると、以下の ACE 設定画面が表示されます。



2. パラメータに一致すると、ACE のパラメータを設定し、アクションを選択します。
＜Save＞ボタンをクリックして、ACE を設定します。



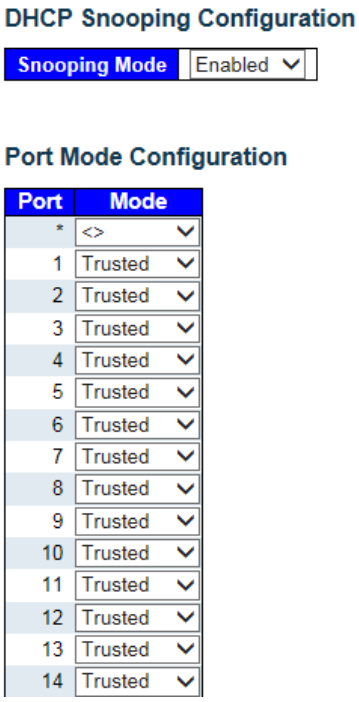
(+)をクリックすると、別の ACE が追加されます。(e)をクリックすると ACE の編集、(x)をクリックすると ACE が削除されます。↑/↓キーを使用することにより、ACE を移動します。

4） DHCP

ここでは、DHCP の設定について説明します。

4-1） DHCP Snooping (DHCP スヌーピング機能)

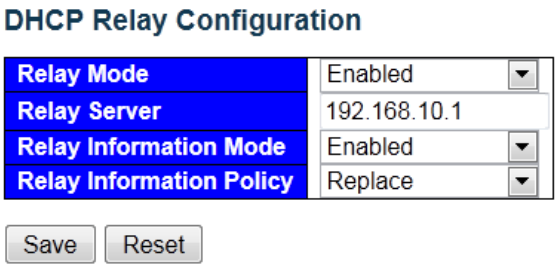
「Configuration」→「Security」→「Network」→「DHCP」→「Snooping」をクリックすると、以下の画面が表示されます。



ここでは、DHCP スヌーピング機能を設定します。DHCP スヌーピング機能を有効にすると、DHCP リクエストメッセージはトラストポート(″Mode″が″Trusted″に設定されているポート)にのみ転送され、トラストポートからの応答パケットにのみ許可します。これにより、不正な DHCP サーバからの接続から保護することができます。

4-2) DHCP Relay (DHCP リレー機能)

「Configuration」→「Security」→「Network」→「DHCP」→「Relay」をクリックすると、以下の画面が表示されます。



ここでは、DHCP リレーおよび DHCP のオプション機能 82 を設定します。

DHCP リレーモードを有効にすると、クライアント/サーバが同じサブネットドメイン内にない場合は、エージェントによりその間の DHCP メッセージを送信します。
セキュリティの問題上、DHCP ブロードキャストメッセージはフラッディングされません。

DHCP relay information モードを有効にすると、エージェントにより DHCP サーバへの送信時に特定情報(オプション 82)が DHCP メッセージに挿入され、DHCP クライアントへの送信時に、DHCP メッセージから削除されます。
これは、DHCP relay operation モードが有効な場合のみ適用されます。

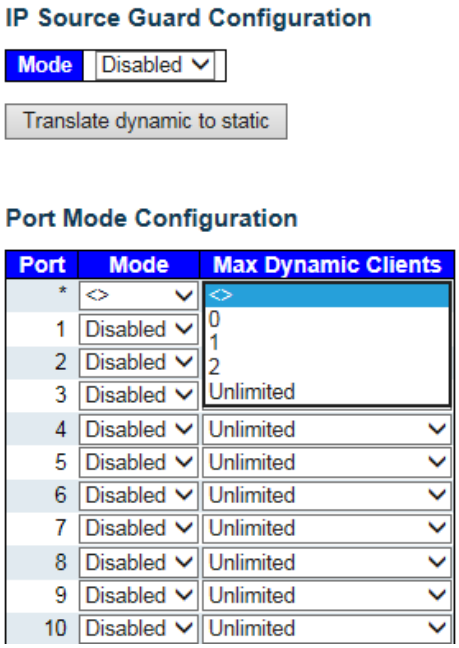
オプション 82 の回線 ID は"[vlan_id][module_id][port_no]"と表示されます。最初の 4 文字は VLAN ID、5 番目と 6 番目はモジュール ID(スタンドアロン時は通常「0」、スタッカブル装置の場合は「switch ID」を指します)。最後の 2 文字はポート番号を記します。
エージェントが受信する DHCP メッセージにポリシーを施行するリレーエージェント情報が含まれる場合は、relay information モードを有効にします。

5) IP Source Gurard（ソースガード）

ここでは、IP ソースガードの設定について説明します。

5-1） Configuration(IP ソースガードの設定)

「Configuration」→「Security」→「Network」→「IP Source Guard」→「Configuration」をクリックすると、以下の画面が表示されます。ここでは、IP ソースガードの設定を行うことができます。



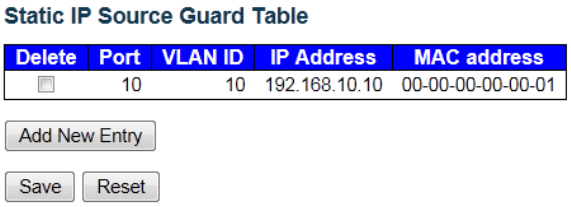
IP ソースガードは、DHCP スヌーピングテーブルに応じて、トラフィックのフィルタリングを行なったり、IP ソースブリッジを手動でバインドすることにより、DHCP スヌーピングのアントラストポートの IP トラフィックを制限したりすることができます。

これにより、別のホストの IP アドレスの不正使用から防ぐことができます。この機能により、指定ポートで学習可能な動的クライアント数の上限を制限します。

【注記】:
ダイナミック IP ソースのエントリは DHCP リクエストにより学習します。IP ソースガードを有効にする前に、まず DHCP スヌーピング機能を有効に設定してください。それ以外は、IP ソースガード機能に対して、スタティック IP ソースのエントリを設定してください。

5-2) Static Table (スタティック IP ソースの設定)

「Configuration」→「Security」→「Network」→「IP Source Guard」→「Static Table」をクリックすると、以下の画面が表示されます。



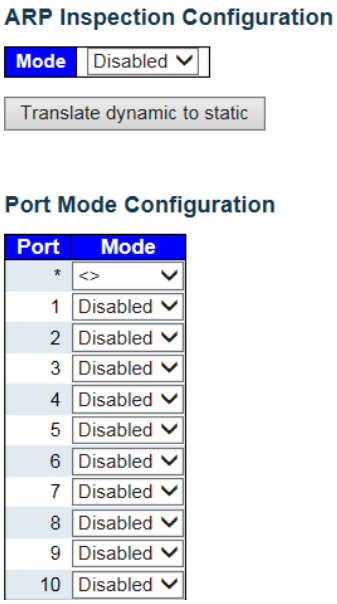
ここでは、スタティック IP ソースのエントリの追加/削除を行います。スタティック IP ソースのエントリは、ポート番号、VLAN ID、IP アドレス、MAC アドレスから構成されます。このスタティックテーブルを使って、別のホストの IP アドレスの不正使用から防ぐことができます。

6) ARP Inspection (ARP インスペクション)

ここでは、ARP インスペクションの設定について説明します。

6-1) Configuration (ARP インスペクションの設定)

「Configuration」→「Security」→「Network」→「ARP Inspection」→「Configuration」をクリックすると、以下の画面が表示されます。

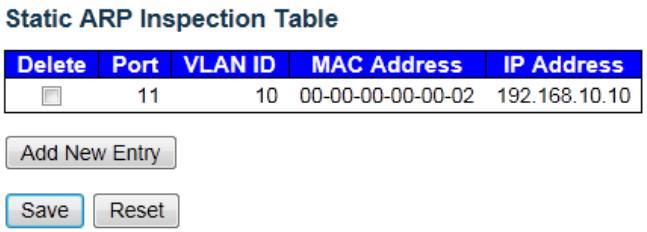


ここでは、ARP インスペクション機能の設定を行うことが出来ます。ARP インスペクションは、セキュリティのための機能です。ARP キャッシュをポイズニングすることによって、レイヤ 2 ネットワークに接続されているホスト、またはデバイスに対して攻撃を行われた場合にそれらの攻撃をブロックします。有効な ARP リクエストおよび応答のみ通過することができます。

【注記】:
ダイナミック IP ソースのエントリは DHCP リクエストにより学習します。IP ソースガードを有効にする前に、まず DHCP スヌーピング機能を有効に設定してください。それ以外は、IP ソースガード機能に対して、スタティック IP Source のエントリを設定してください。

6-2) Static Table(スタティックテーブルの設定)

「Configuration」→「Security」→「Network」→「ARP Inspection」→「Static Table」をクリックすると、以下の画面が表示されます。

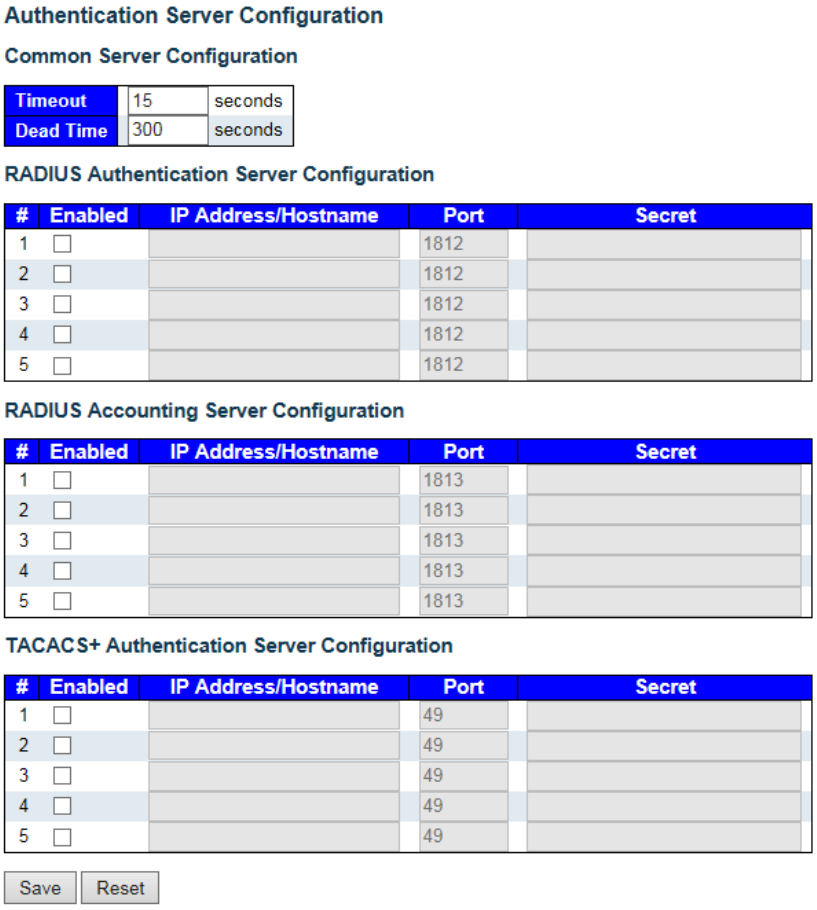


ここでは、スタティック ARP インスペクションテーブルのスタティック ARP エントリの追加/削除を行います。このテーブルは、ARP インスペクションセキュリティ機能用です。

2.3.4.3 AAA

ここでは、RADIUS および TACACS+サーバを設定します。
この設定は、802.1x ネットワークアクセス用、かつユーザはログイン認証用です。

「Configuration」→「Security」→「AAA」をクリックすると、以下の画面が表示されます。



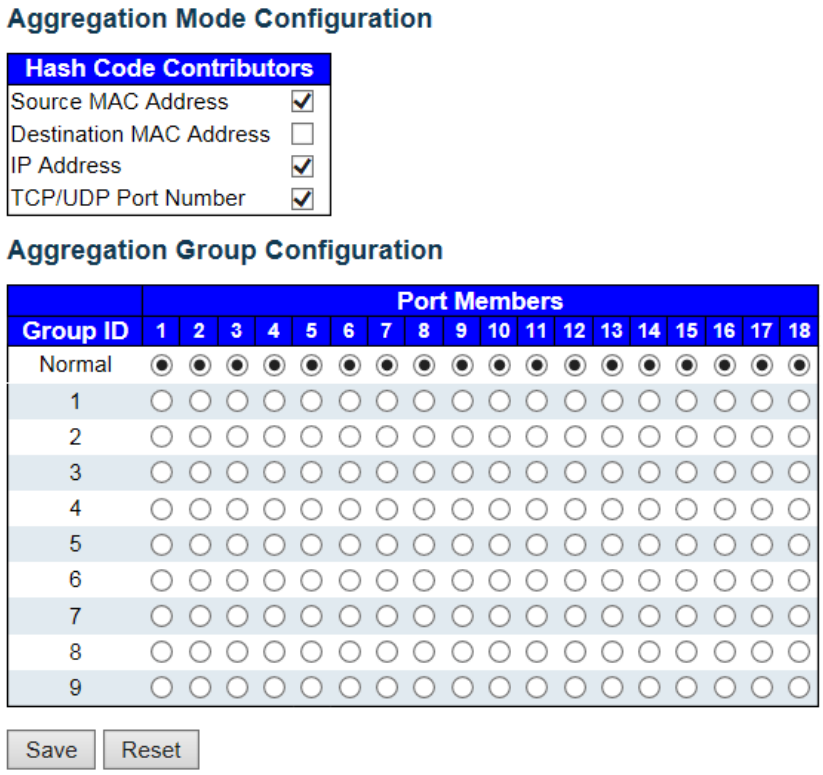
2.3.5 Aggregation (アグリゲーション)

ここでは、アグリゲーションの設定について説明します。

2.3.5.1 Static (固定設定)

ここでは、アグリゲーション機能の固定設定を行うことができます。
「Configuration」→「Aggregation」→「Static」をクリックすると、以下の画面が表示されます。

「Aggregation Hash」モードでは、「Hash Code Contributors」のメニューから選択して、フレームの宛先ポートを算出します。アグリゲーショングループは、最大 5 つまで固定設定が可能です。
「Aggregation Mode Configuration」のメニューの中から、お使いのユーザ環境に合わせてポートの設定を行ってください。



2.3.5.2 LACP

「Configuration」→「Aggregation」→「LACP」をクリックすると、以下の画面が表示されます。

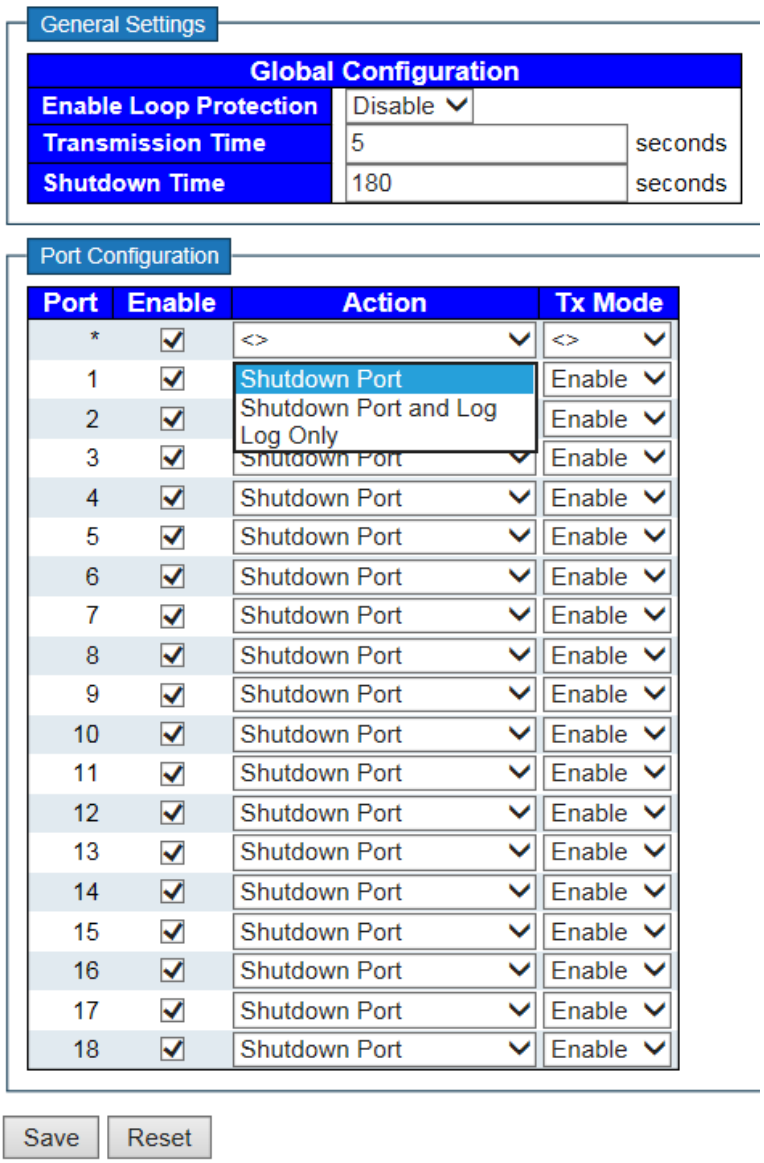
LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768
9	☐	Auto		Active	Fast	32768
10	☐	Auto		Active	Fast	32768
11	☐	Auto		Active	Fast	32768
12	☐	Auto		Active	Fast	32768
13	☐	Auto		Active	Fast	32768

ここでは、アグリゲーション用の LACP 機能を設定します。LACP は、IEEE802.3ad 規格のプロトコルです。
LACP により、複数の物理ポートを 1 つの論理ポートに束ねることが可能です。
本機を 2 台(または、LACP をサポートしている機器)を使って、LACP 機能を介してアグリゲーション接続を行うことが可能です。

2.3.6 Loop Protection (ループプロテクション)

「Configuration」→「Loop Protection」をクリックすると、以下の画面が表示されます。



ここでは、ループバック検知機能を設定します。ポートのループバック機能によりパケットストームが生じた場合、ポートの制御を行うことが可能です。
ループバック検知かつ"Tx Mode"を有効にすると、ループプロテクションの PDU を送信します。
ループバックを検出すると、ポートはシャットダウンするか、または情報がログに記録されます。
シャットダウンの時間は一定時間ごとに設定可能です。指定の時間を経過するとポートは有効になります。

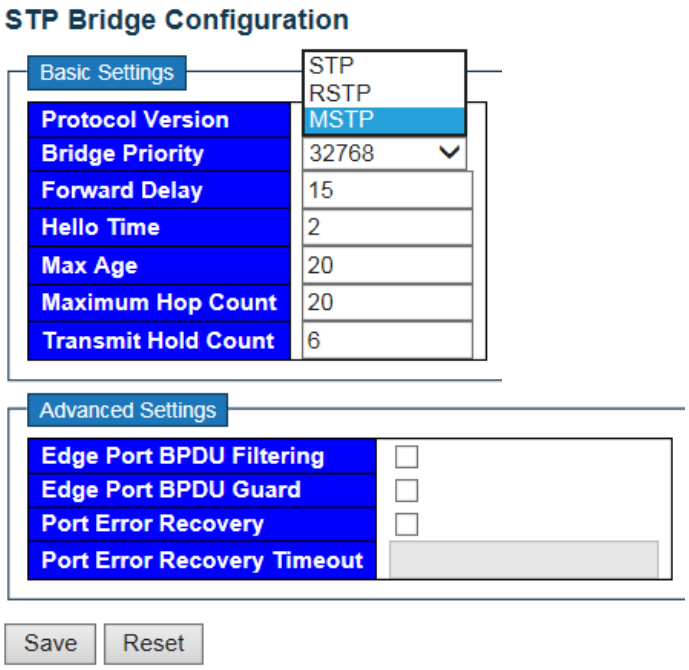
2.3.7 Spanning Tree(スパニングツリー)

ここでは、スパニングツリー機能の設定について説明します。

2.3.7.1 Bridge Settings

ここでは、スパニングツリーのブリッジの設定を行います。

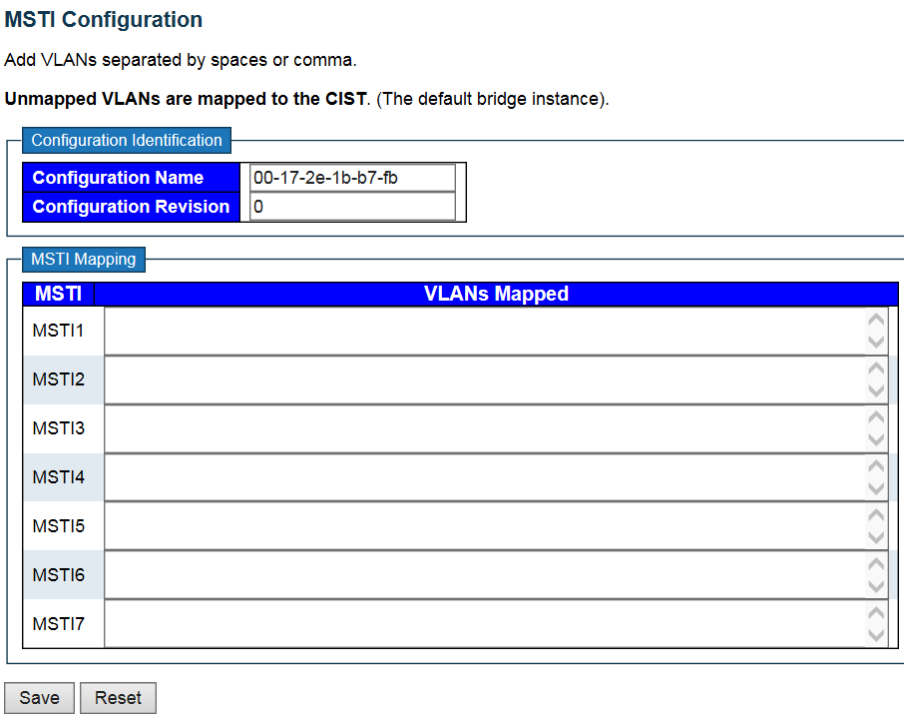
「Configuration」→「Spanning Tree」→「Bridge Settings」をクリックすると、以下の画面が表示されます。



本機では、STP(IEEE 802.1D)、RSTP(IEEE 802.1w)および MSTP(IEEE 802.1s)をサポートしています。ここでは、プロトコルのバージョンを選択することができます。

2.3.7.2 MSTI Mapping

「Configuration」→「Spanning Tree」→「MSTI Mapping」をクリックすると、以下の画面が表示されます。

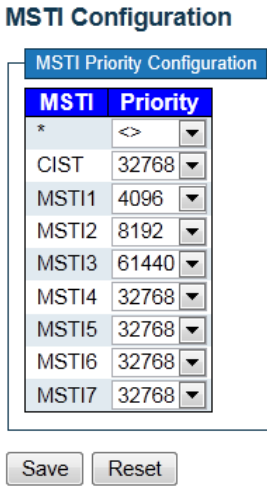


ここでは、MSTI/VLAN 間のマッピングを設定します。

ID は、VLAN から MSTI のマッピングを識別するために名前とリビジョンで構成されます。
ブリッジは、名前とリビジョンを共有し、同様に複数の MSTI 内のスパニングツリー用の VLAN-to-MSTI mapping 設定を共有する必要があります。

2.3.7.3 MSTI Priorities

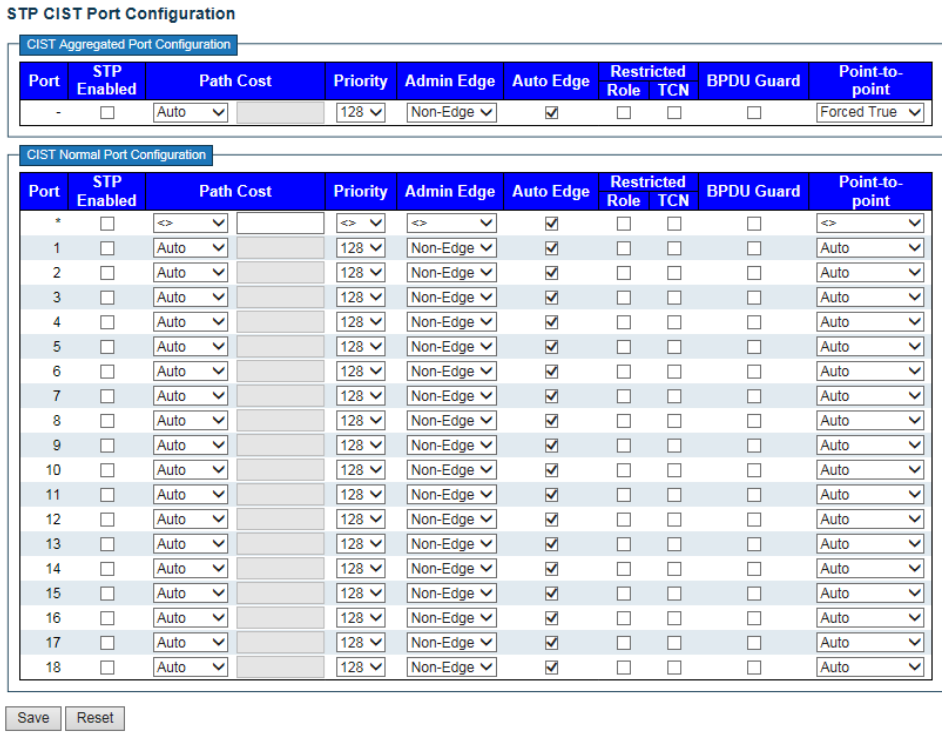
「Configuration」→「Spanning Tree」→「MSTI Priorities」をクリックすると、以下の画面が表示されます。



ここでは、MSTI プライオリティを設定します。値が低い方が、プライオリティが高くなります。
ブリッジのプライオリティと MST インスタンス番号は、6 バイトの MAC アドレスで連結され、ブリッジの識別子を構成します。

2.3.7.4 CIST Ports

「Configuration」→「Spanning Tree」→「CIST Ports」をクリックすると、以下の画面が表示されます。



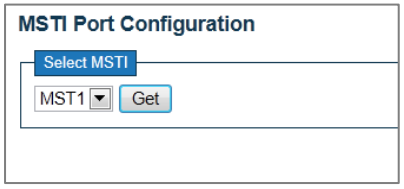
ここでは、CIST ポートの設定を行うことができます。

2.3.7.5 MSTI Ports

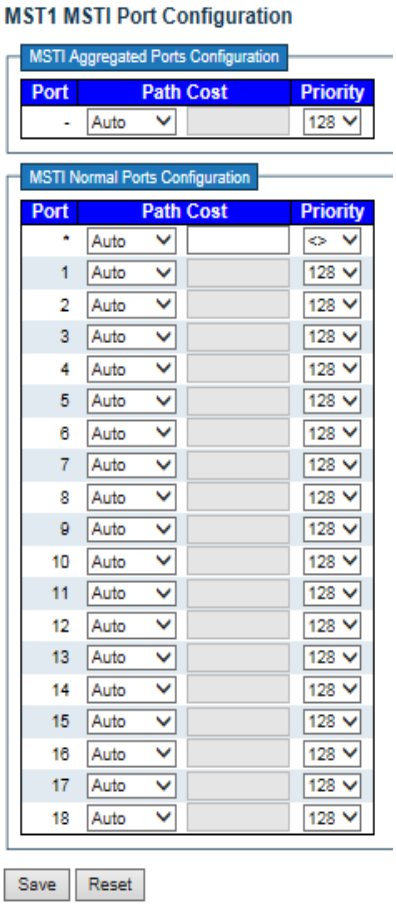
「Configuration」→「Spanning Tree」→「MSTI Ports」をクリックすると、以下の画面が表示されます。

ここでは、MSTI ポートの設定を行うことができます。

MSTI ポートは仮想ポートであり、ポート上の MSTI インスタンスごとに有効な CIST（物理）ポートそれぞれにインスタンスを生成します。MSTI インスタンスは、実際の MSTI ポートの設定オプションを表示する前に選択してください。



「MSTI」を選択して＜Get＞ボタンをクリックすると、以下の画面が表示されます。

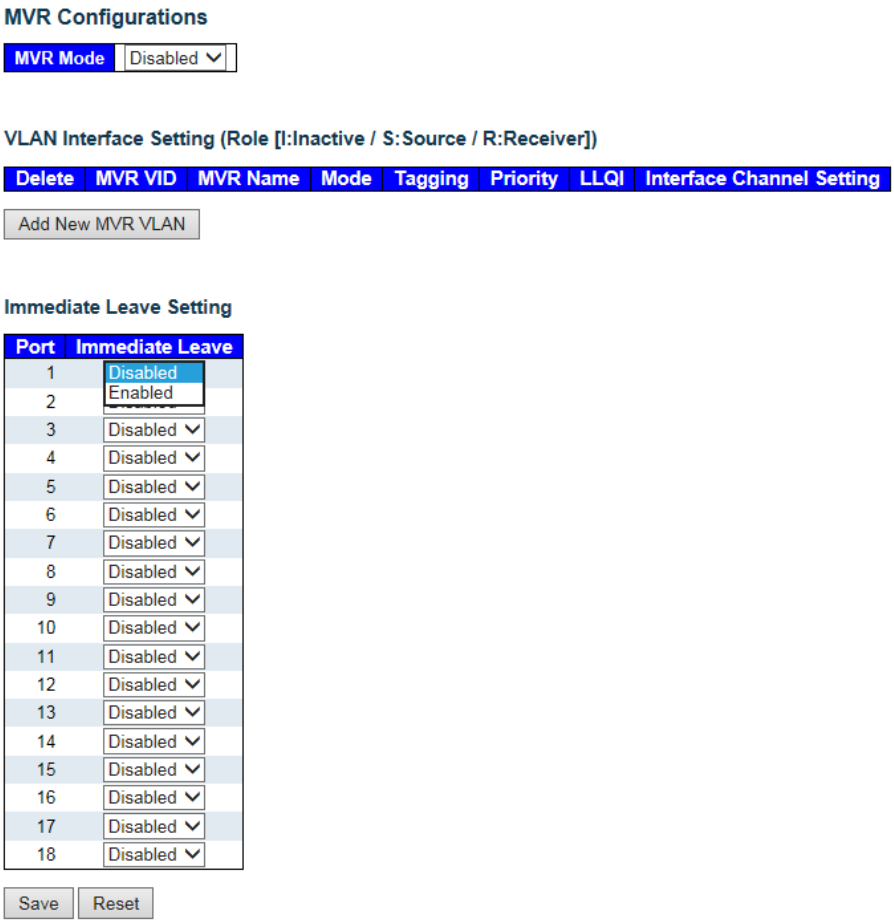


パスコストは、ポートのパスコストを設定します。
"Path Cost"を"Auto"に設定すると、802.1D の推奨値を用いて、物理リンク通信速度に応じて適切なコストを設定します。
"Path Cost"を"Specific"に設定した場合、「1-200000000」の範囲で、パスコストを任意に設定できます。ネットワークのトポロジーを設定時にパスコストを使用します。パスコストの低いポートを選択すると、パスコストの高いポートに設定されます。
「Priority」により、ポートのプライオリティが設定されます。同じポートコストを持つポートのプライオリティを設定することができます。

2.3.8 MVR

ここでは、MVR 機能の設定を行います。MVR 機能により、マルチキャストトラフィックをマルチキャスト VLAN に伝送を行うことが可能になります。

「Configuration」→「MVR」をクリックすると、以下の画面が表示されます。



マルチキャストテレビジョンアプリケーションの場合、PC またはネットワークテレビ、あるいはセットトップボックスによるマルチキャストストリームの受信が可能です。複数のセットトップボックスやPCを1つのサブスクライバーポートに接続可能であり、MVR レシーバポートとして設定します。
サブスクライバーがチャネルを選択する場合は、セットトップボックス、あるいはPCが IGMP/MLD レポートメッセージを”Switch A”に送信して、適切なマルチキャストグループアドレスを結合します。マルチキャスト VLAN 間にマルチキャストデータの送受信を行うアップリンクポートを”MVR ソースポート”と言います。マルチキャスト VLAN ごとに対応のチャネルを設定して、MVR VLAN を最大 8 つまで設定可能です。グループアドレスをチャネル設定ごとに最大「256」グループまで設定します。

設定を完了するには、以下の手順に従ってください。
Step 1: MVR VLAN を設定して、ポートに VLAN を割り当てます。
Step 2: (e)をクリックして、VLAN にチャネルを割り当てます。
Step 3: ポートの Immediate Leave 機能を有効/無効にします。

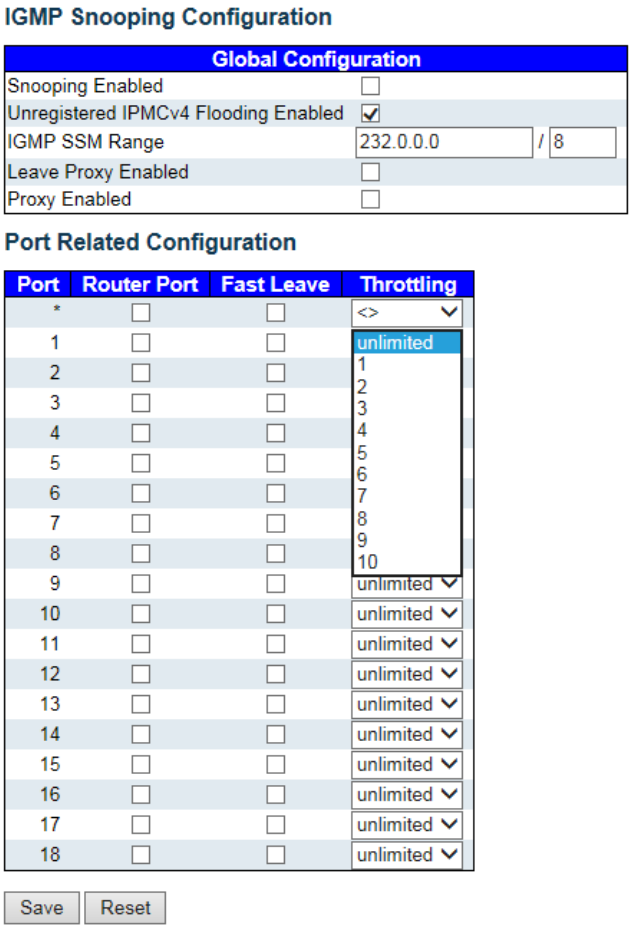
2.3.9 IPMC

ここでは、IPMC(マルチキャスト)の設定について説明します。

2.3.9.1 IGMP Snooping(IGMP スヌーピング)

1) Basic Configuration (基本設定)

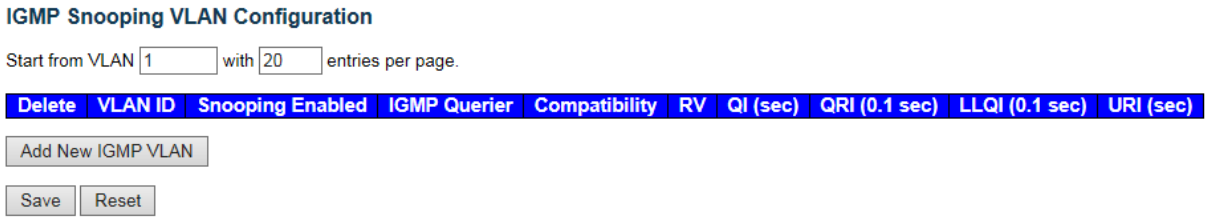
「Configuration」→「IPMC」→「IGMP Snooping」→「Basic Configuration」をクリックすると、以下の画面が表示されます。



ここでは、IGMP スヌーピング機能の基本設定を行います。ポート単位のスロットについては、10 段階に設定可能です。

2) VLAN Configuration (VLAN 設定)

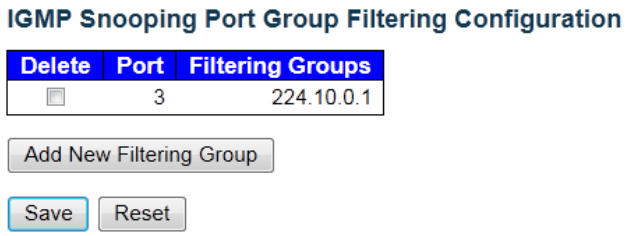
「Configuration」→「IPMC」→「IGMP Snooping」→「VLAN Configuration」をクリックすると、以下の画面が表示されます。



ここでは、IGMP スヌーピングの VLAN テーブルのメンテナンスを行います。
以下の機能をサポートしています。
- 新規 IGMP VLAN の追加/設定/保存
- IGMP VLAN の編集
- IGMP VLAN の削除

3) Port Group Filtering (ポートグループのフィルタリング)

「Configuration」→「IPMC」→「IGMP Snooping」→「Port Group Filtering」をクリックすると、以下の画面が表示されます。



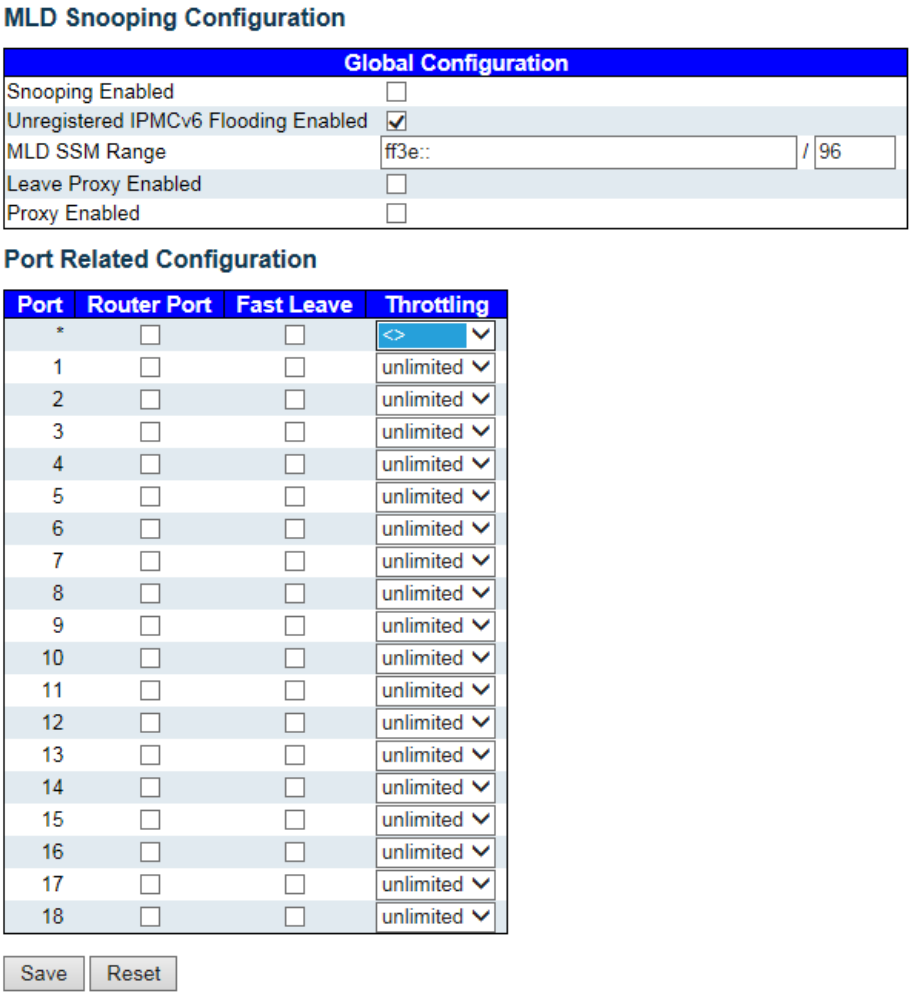
ここでは、ポートの IGMP フィルタリンググループのメンテナンスを行います。テーブル上の IP マルチキャストグループのフィルタリングを行います。

2.3.9.2 MLD Snooping(MLD スヌーピング)

ここでは、MLD スヌーピングの設定についての説明をします。

1) Basic Configuration (基本設定)

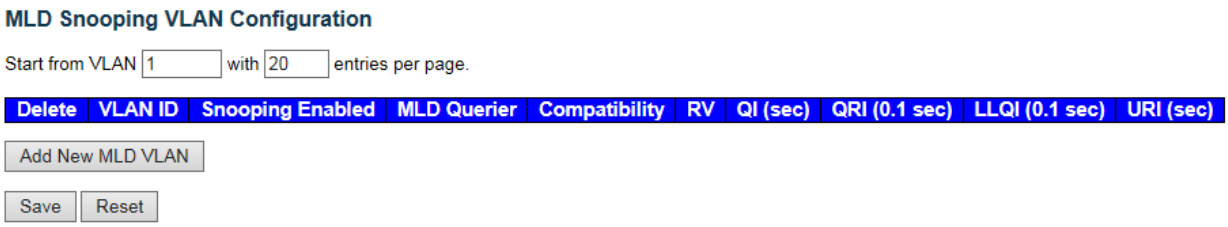
「Configuration」→「IPMC」→「MLD Snooping」→「Basic Configuration」をクリックすると、以下の画面が表示されます。



ここでは、MLD スヌーピング機能の基本設定を行います。

2） VLAN Configuration（VLAN 設定）

「Configuration」→「IPMC」→「MLD Snooping」→「VLAN Configuration」をクリックすると、以下の画面が表示されます。

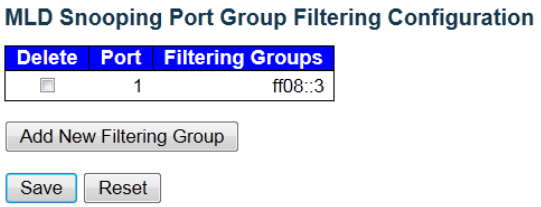


ここでは、MLD スヌーピングの VLAN テーブルのメンテナンスを行います。

以下の機能がサポートされています。
- 新規 MLD VLAN の追加/設定/保存
- MLD VLAN の編集
- MLD VLAN の削除

3) Port Group Filtering（ポートグループのフィルタリング）

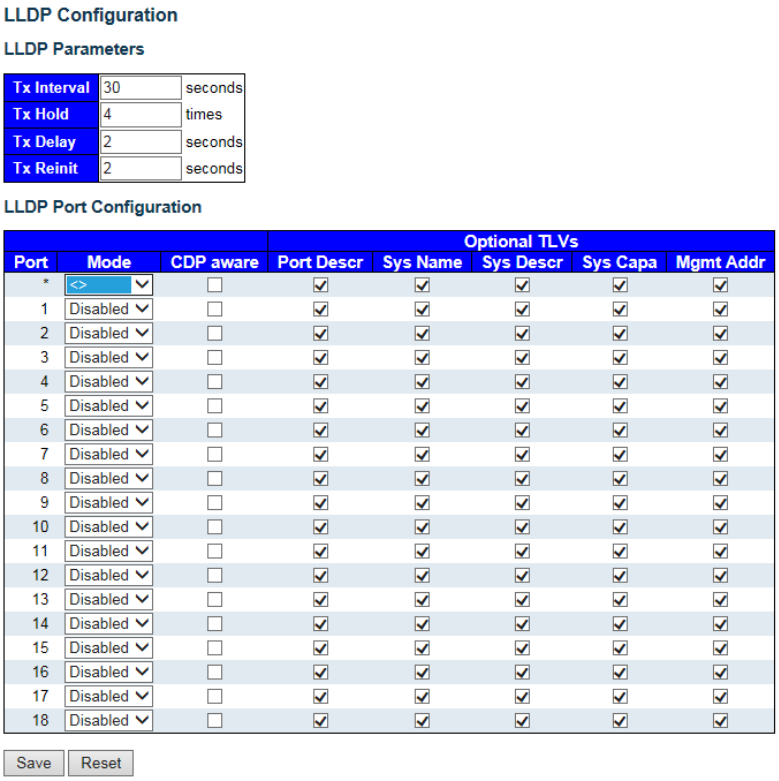
「Configuration」→「IPMC」→「MLD Snooping」→「Port Group Filtering」をクリックすると、以下の画面が表示されます。



ここでは、MLD フィルタリンググループのメンテナンスを行います。IP マルチキャストグループのフィルタリングを行います。

2.3.10 LLDP

ここでは、本機の LLDP 機能を設定します。
「Configuration」→「LLDP」をクリックすると、以下の画面が表示されます。



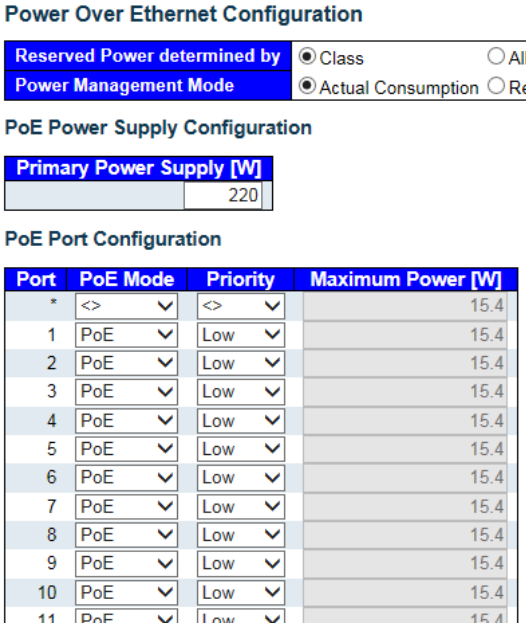
LLDP は、IEEE802.1ab 標準プロトコルです。
データリンク層の接続を検出/管理するプロトコルで IEEE802.1ab により標準化されています。
当機能で LAN に接続された機器を検出して各種の設定や管理を行うことができます。
LLDP は、IEEE802 の LAN の接続先のステーションが、同じ IEEE802 の LAN に接続されている他のステーションに、これらの機能の管理を行う本体の管理アドレス、管理用の本体に必要な IEEE802 への接続のステーションポイントの情報を取り込むシステムによって提供される主な機能を通知します。
プロトコルを介して送信されている情報は、MIB の受信側によってストアされ、SNMP などの管理プロトコルを使用して NMS による情報へのアクセスが可能になります。

2.3.11 PoE

PoE は、「Power Over Ethernet」の略称で、標準のイーサネットケーブルを利用してリモート先の装置に電力を供給するために使用します。例えば、電源を得るのが困難な場所に配置された IP 電話、無線 LAN アクセスポイント、その他の機器に電力を供給することが可能です。

2.3.11.1 Configuration(設定)

「Configuration」→「PoE」→「Configuration」をクリックすると、以下の画面が表示されます。
ここでは、PoE 機能の設定を行うことができます。



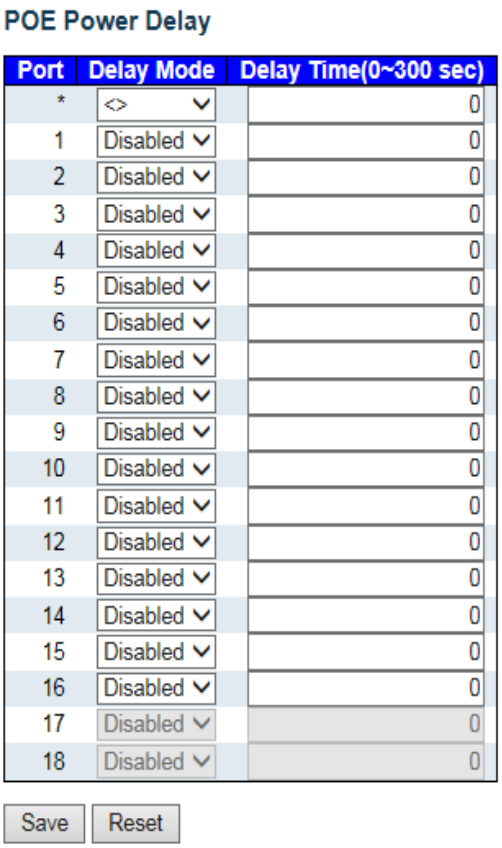
各機能の説明については、下記のとおりです。

Power Over Ethernet Configuration	
Reserved Power determined by	ポートおよび受電側機器による電力の予約方法については、以下の2つの方法があります。 1.Allocation: このモードでは、ユーザはポートごとに予約可能な電力を設定することが可能です。「Maximum Power [W]」の欄に各ポートの電源を設定してください。 2. Class: このモードでは、接続先の受電側機器が保有するクラスに応じて電力が自動的に設定されます。ポートクラスは、「4」、「7」、「15.4」、「30」に設定可能です。「Maximum Power [W]」の設定値は適用されません。

Power Management Mode.	ポートをシャットダウンするには 2 つの方法があります。 1. Actual Consumption: このモードでは、すべてのポートの実際の電力消費量が供給可能な範囲を越えた場合、あるいはポートごとの電力消費量が設定されたポートの電力を超えた場合は、ポートをシャットダウンします。ポートはプライオリティに応じてシャットダウンします。2つのポートのプライオリティが同じ場合は、ポート番号が大きい方がシャットダウンされます。 2. Reserved Power このモードでは、予約した電力の合計が供給可能な電力を越えた場合は、ポートをシャットダウンします。このモードでは、電源から使用可能な電力を要求された場合は、ポートの電源が「OFF」になります。
PoE Power Supply Configuration	
Primary Power Supply [W]	受電側機器が使用可能な電力の大きさを決定するには、電源から供給可能な電力の量を設定する必要があります。
PoE Port Configuration	
PoE Mode	・ポートの PoE の動作モードを設定します。 ・ Disabled: ポートの PoE は無効です。 ・ PoE : モードを IEEE802.3af(PoE：最大 15.4W までの給電)に設定します。 ・ PoE+: モードを IEEE802.3at(PoE+：最大 30W までの給電)に設定します。
Priority	Priority は、ポートのプライオリティを表します。それぞれの電力のプライオリティは 3 レベル（「Low」、「High」、「Critical」）に分けられます。このプライオリティは、リモート装置により要求された電力が供給可能な電力を超えた場合に使用します。この場合、プライオリティの低いポートについては、ポート番号の大きい順から電源が消えます。
Maximum Power [W]	ポートごとに、PD へ供給可能な最大電力を設定します。 "Reserved Power determined by"で"Allocation"が選択されている場合に設定が可能です。 "PoE Mode"が"PoE"のポートでは「0-15.4」の範囲で、また"PoE Mode"が"PoE+"のポートでは「0-30」の範囲でそれぞれ設定できます。

2.3.11.2 Power Delay(給電の遅延)

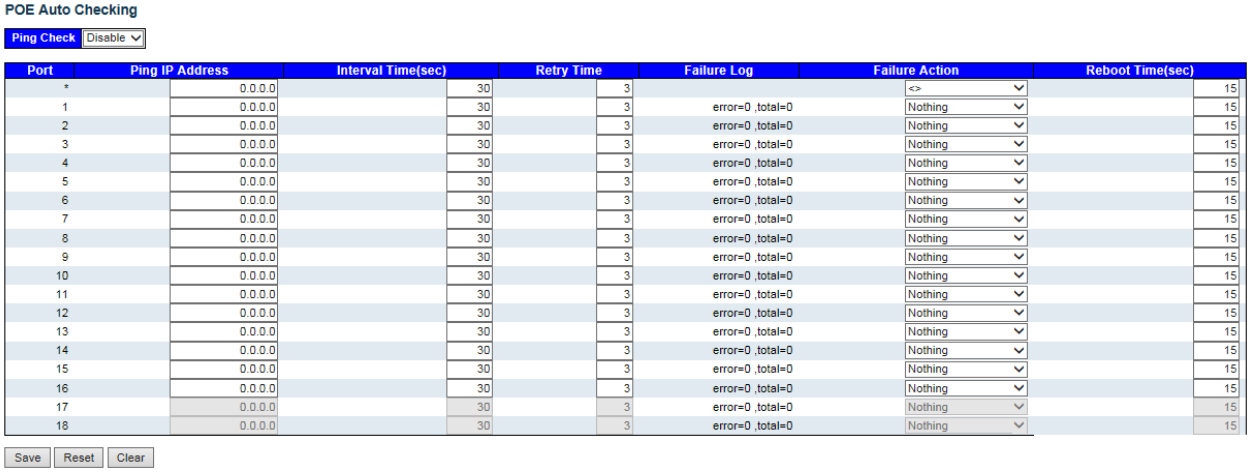
「Configuration」→「PoE」→「Power Delay」をクリックすると、以下の画面が表示されます。



ここでは、本機の電源を投入した時の PoE 給電の遅延時間を設定します。
本機に電源を投入して起動が完了すると、ここで設定した遅延時間の経過後に PoE 給電が行われます。

2.3.11.3 Auto Checking(自動チェック)

「Configuration」→「PoE」→「Auto Checking」をクリックすると、以下の画面が表示されます。
ここでは、PoE の自動チェックの設定を行うことができます。



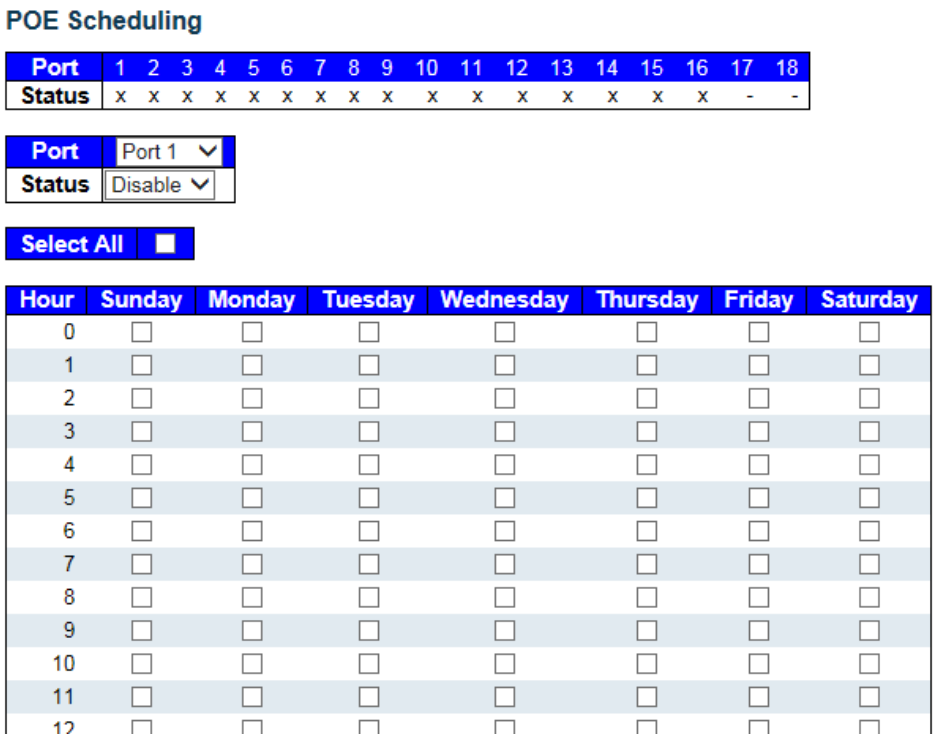
接続先の受電側機器のステータスをチェックします。遠隔の IP アドレスの受電側機器に ping を実行します。リトライしても受電側機器からの応答がない場合は、失敗したとみなしアクションを実行します。アクションが“Reboot Remote PD”に設定されている場合は、再起動時に PoE の給電を一度中止すると、PoE 電力を再度送信し、受電側機器を再起動します。

POE Auto Checking	
Ping Check	受電側機器のモニタリングの状態(動作可/動作不可)を有効/無効に設定します。
Port	ポート番号を表示します。
Ping IP Address	ping を行う受電側機器のIPアドレスを設定します。
Interval Time	モニタリング間隔を設定します。有効な値は「10-120」です。
Retry Time	受電側機器からの応答がない場合のモニタリングのリトライ回数を設定します。有効な値は、「1-5」です。
Failure Log	ping 失敗時のログを表示します。
Failure Action	リトライしても、受電側機器からの応答がない場合の動作を設定します。「Nothing」または「Reboot Remote PD」のいずれかを選択できます。
Reboot Time	再起動する時間を設定します。リブートの時間を設定している間は、PoE の出力をストップします。有効な値は、「3-120」です。

【注記】:
INTERVAL TIME は、受電側機器の起動時間を考慮して設定してください。
受電側機器の起動時間より短く設定してしまうと、Failure Action をいつまでも繰り返すことになります。

2.3.11.4 Scheduling(スケジュールの設定)

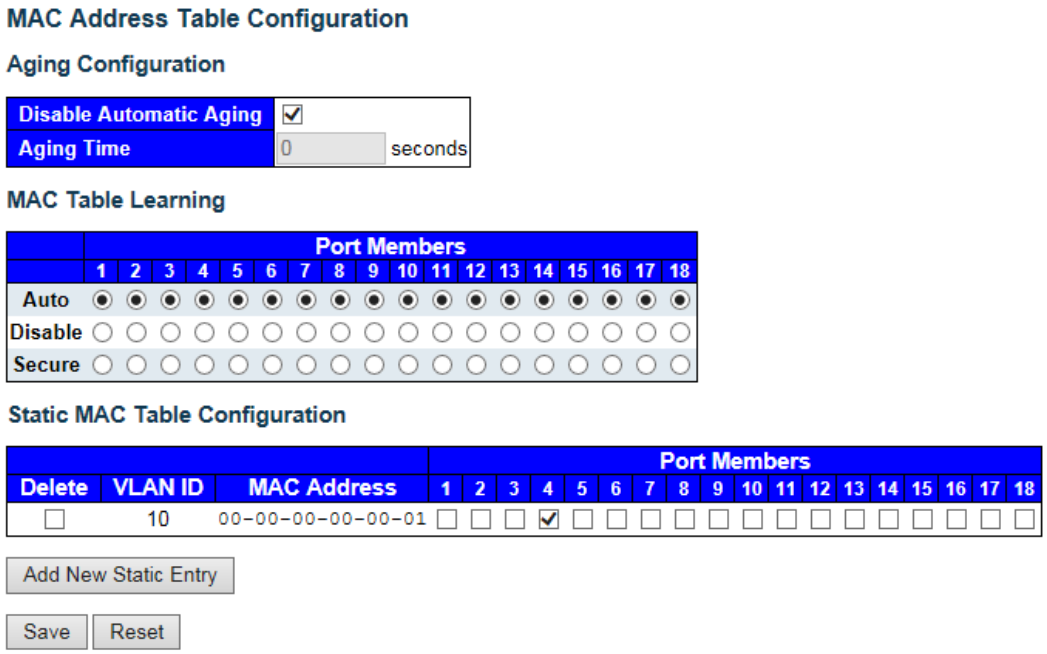
「Configuration」→「PoE」→「Scheduling」をクリックすると、以下の画面が表示されます。



ここでは、各ポートの PoE の給電スケジュールの状態を表示したり、PoE スケジュール機能をポート単位で有効/無効にすることができます。この機能を有効にすると、スケジュール表に応じて PoE の給電を行います。

2.3.12 MAC Table

ここでは、MAC テーブルの設定を行います。
「Configuration」→「MAC Table」をクリックすると、以下の画面が表示されます。



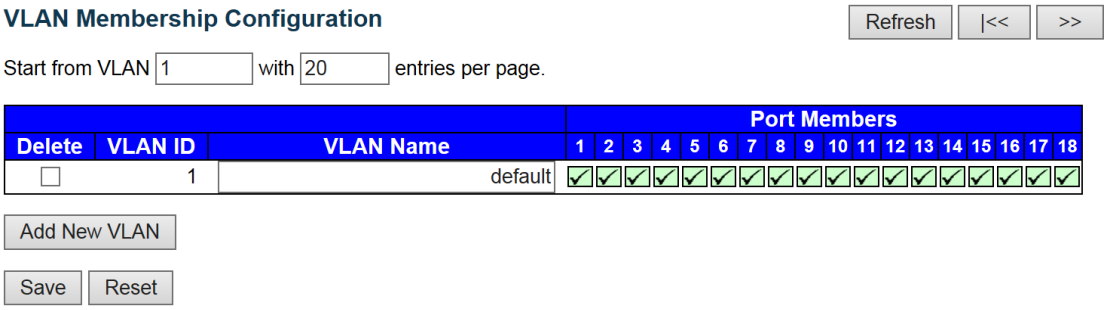
エージングタイム、MAC アドレス学習、スタティック MAC アドレスの設定を行います。
エージングタイムのデフォルト設定は、「300 秒」です。
MAC アドレステーブルのメニューの設定を”Secure”に設定すると、スタティック MAC エントリのみを学習し、
それ以外のフレームはすべて破棄されます。

2.3.13 VLANs

ここでは、VLAN の設定について説明します。

2.3.13.1 VLAN Membership (VLAN メンバー)

「Configuration」→「VLANs」→「VLAN Membership」をクリックすると、以下の画面が表示されます。



802.1Q VLAN グループのメンテナンスを行います。

- 新規 VLAN の追加/ VLAN ID/VLAN 名の設定
- VLAN の編集
- VLAN の削除

2.3.13.2 Ports (VLAN ポートの設定)

「Configuration」→「VLANs」→「Ports」をクリックすると、以下の画面が表示されます。

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	☐	<>	<>	1	<>
1	Unaware	☐	All	Specific	1	Untag_pvid
2	Unaware	☐	All	Specific	1	Untag_pvid
3	Unaware	☐	All	Specific	1	Untag_pvid
4	Unaware	☐	All	Specific	1	Untag_pvid
5	Unaware	☐	All	Specific	1	Untag_pvid
6	Unaware	☐	All	Specific	1	Untag_pvid
7	Unaware	☐	All	Specific	1	Untag_pvid
8	Unaware	☐	All	Specific	1	Untag_pvid
9	Unaware	☐	All	Specific	1	Untag_pvid
10	Unaware	☐	All	Specific	1	Untag_pvid
11	Unaware	☐	All	Specific	1	Untag_pvid
12	Unaware	☐	All	Specific	1	Untag_pvid
13	Unaware	☐	All	Specific	1	Untag_pvid
14	Unaware	☐	All	Specific	1	Untag_pvid
15	Unaware	☐	All	Specific	1	Untag_pvid
16	Unaware	☐	All	Specific	1	Untag_pvid
17	Unaware	☐	All	Specific	1	Untag_pvid
18	Unaware	☐	All	Specific	1	Untag_pvid

Save Reset

ここでは、ポートの 802.1Q VLAN および Q-in-Q 機能の設定を行います。

Port Type	
Unaware:	ポートは“Unaware”に設定されると、受信フレームは”タグなしフレーム”として処理されます。受信フレームがタグ付きの場合でも、タグはペイロードとして処理されます。フレームはポートベース VLAN – PVID にクラス分けされます。これは、802.1Q アクセス接続用、または Q-in-Q ダウンリンク接続用です。ポートベース VLAN を使用する場合、同じ PVID の場合は「Unaware」に設定してください。
C-port:	ポートが C-port,タグ付きフレームに設定されている場合は、タグ付きフレームはフレームのタグに応じて VLAN にクラス分けされます。 これは、802.1Q VLAN トランクです。
S-port:	S-port に設定されている場合は、出力フレームのタグの TPID は通常サービス VLAN として「0x88A8」です。これは、Q-in-Q アップリンク接続用です。
S-custom-port:	S-custom-port に設定されている場合は、出力フレームのタグの TPID はサービス VLAN としてカスタマイズされます。
Port VLAN	
None:	PVID は無視されます。クラス分けされた VLAN ID をもつタグがポート上で送信されたフレームに挿入されます。 このモードは、通常 802.1Q VLAN トランク接続として VLAN 認識スイッチに接続されているポートに使用されます。このモードを使用時には、”Tx Tag”は「Untag_pvid」に設定してください。

Specific:	ポートの VLAN ID を設定可能です。ポートで受信したタグなしフレームは、ポートの VLAN ID にクラス分けされます。VLAN の認識ができない場合（ポートタイプが非対応の場合）は、ポートで受信したフレームはすべてそのポートの VLAN ID にクラス分けされます。ポート上で送信されたフレーム内の"クラス分けされた VLAN ID"が"ポート VLAN ID"と異なる場合は、"クラス分けされた VLAN ID"と"VLAN タグ"がフレームに挿入されます。

"Tx_Tag"により、ポートからのフレームの送信時のタグ付け方法が設定されます。

802.1Q VLAN 設定において、各ポートの設定は下記の通りです。

- Access: [Port Type]-"Unaware", [Port VLAN Mode]-"Specific(set PVID)", [Tx Tag]-"Untag_all"
- Trunk : [Port Type]-"C-port", [Port VLAN Mode]-"None", [Tx Tag]-"Untag_pvid"
- Hybrid : [Port Type]-"Unaware", [Port VLAN Mode]-"Specific(set PVID)", [Tx Tag]-"Untag_pvid"

Q-in-Q 設定において、各ポートの設定は下記のとおりです。

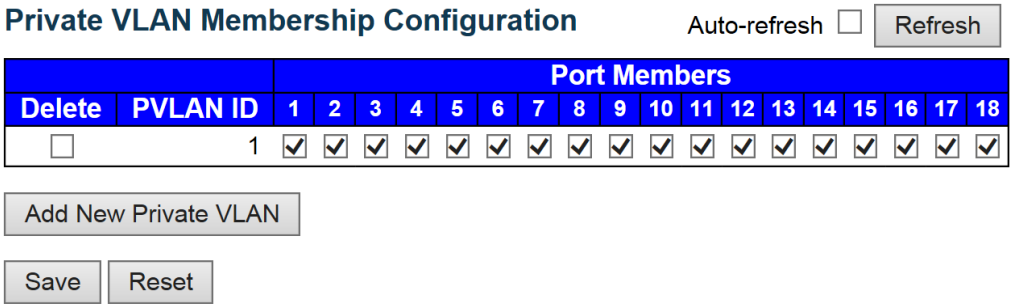
- Uplink: [Port Type]-"S-port"(あるいは、custom TPID をもつ"S-custom-port"), [Port VLAN Mode]-"None", [Tx Tag]-"Untag_pvid"
- Downlink: [Port Type]-"Unaware", [Port VLAN Mode]-"Specific(set PVID)", [Tx Tag]-"Untag_all"

2.3.14 Private VLAN (プライベート VLAN)

ここでは、プライベート VLAN 機能の設定について説明します。

2.3.14.1 PVLAN Membership (PVLAN メンバー)

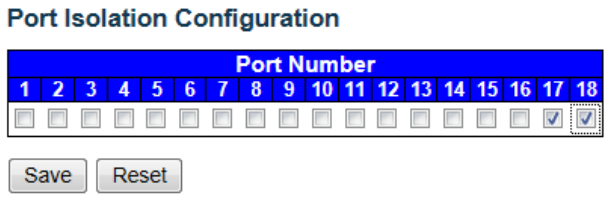
「Configuration」→「Private VLANs」→「PVLAN Membership」をクリックすると、以下の画面が表示されます。



ここでは、プライベート VLAN ID の設定/メンバー編集/削除を行います。

2.3.14.2 Port Isolation (ポートの分割)

「Configuration」→「Private VLANs」→「Port Isolation」をクリックすると、以下の画面が表示されます。



ここでは、ポートのアイソレーション機能を設定します。設定されたポートは、同じ VLAN 上でも互いに通信を行うことができなくなります。

2.3.15 Voice VLAN

ここでは、音声 VLAN(Voice VLAN)の設定について説明します。

2.3.15.1 Configuration (音声 VLAN の設定)

「Configuration」→「Voice VLAN」→「Configuration」をクリックすると、以下の画面が表示されます。

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

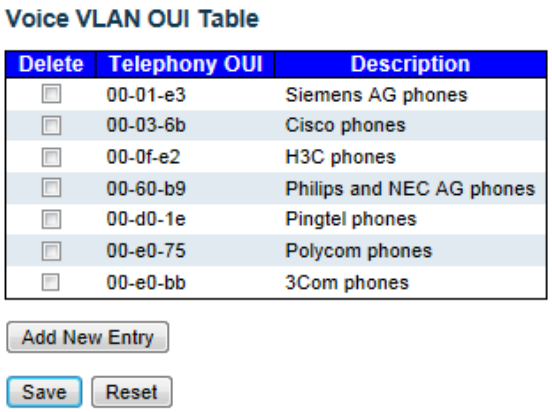
Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	LLDP
3	Disabled	Disabled	Both
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI
15	Disabled	Disabled	OUI
16	Disabled	Disabled	OUI
17	Disabled	Disabled	OUI
18	Disabled	Disabled	OUI

Save Reset

ここでは本機の音声 VLAN を設定します。
この機能を有効にすると、VoIP トラフィックを自動検知し、特定のプライオリティに応じて音声 VLAN トラフィックの伝送を行います。音声 VLAN ポート検出プロトコルは、OUI または LLDP により有効です(OUI は、MAC アドレスの最初の3バイトのベンダコードです)。

2.3.15.2 OUI

「Configuration」→「Voice VLAN」→「OUI」をクリックすると、以下の画面が表示されます。



ここでは、Voice IP トラフィックの OUI テーブルのメンテナンスを行います。OUI は、MAC アドレスの最初の3バイトです。OUI をもつパケットは音声トラフィックとして処理されます。

2.3.16 QoS

ここでは、QoS の設定について説明します。

2.3.16.1 Port Classification（ポートのクラス分け）

「Configuration」→「QoS」→「Port Classification」をクリックすると、以下の画面が表示されます。

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		
1	0	0	0	0	Disabled	
2	0	0	0	0	Disabled	
3	0	0	0	0	Disabled	
4	0	0	0	0	Disabled	
5	0	0	0	0	Disabled	
6	0	0	0	0	Disabled	
7	0	0	0	0	Disabled	
8	0	0	0	0	Disabled	
9	0	0	0	0	Disabled	
10	0	0	0	0	Disabled	
11	0	0	0	0	Disabled	
12	0	0	0	0	Disabled	
13	0	0	0	0	Disabled	
14	0	0	0	0	Disabled	
15	0	0	0	0	Disabled	
16	0	0	0	0	Disabled	
17	0	0	0	0	Disabled	
18	0	0	0	0	Disabled	

Save Reset

ここでは、QoS イングレスのクラス分けの基本設定を行います。以下のパラメータを設定します。

- タグなしフレームの Default QoS クラス、default DP(破棄優先度)レベル、default PCP(Priority Code Point)、default DEI(優先廃棄識別)、ポートへのタグ付きフレームのデフォルトの処理、DSCP ベース QoS.

□ タグのクラス分けについて

「Tag Class」は、802.1Q タグの PCP かつ DEI による QoS を有効/無効にします。
クリックすると、(PCP,DEI)から(QoS class, DP level)のマッピングが表示されます。有効にすると、ポートの入力タグのクラス分け QoS は、パケット伝送のマッピングに準じます。

□ DSCP クラス分けについて

「DSCP Based」は、IP ヘッダの DSCP により QoS を有効/無効にします。☑を入れると、有効になります。
入力 DSCP のクラス分けの設定方法については、「DSCP-Based QoS」を参照してください。
「DSCP-Based QoS」画面の「Trust」に☑を入れると、DSCP 値が確定されます。
「入力 DSCP クラス分けの変換方法」設定の詳細については、「DSCP Translation」および「Port DSCP」の項を参照してください。

「egress DSCP remarking configuration(出力 DSCP リマークの設定)」の詳細については、「Port DSCP」、「DSCP Classification」および「DSCP Translation」の項を参照してください。

QoS クラスおよび DP レベルの設定は、タグのクラス分けおよび DSCP クラス分けが無効な場合のみ有効です。タグなしパケットがタグ付きパケットに変換される場合に、PCP および DEI 設定が適用されます。
タグクラス分けおよび DSCP クラス分けが無効な場合は、QoS クラスおよび DP レベルは手動でポートに割り当てられます。
ポートで受信したフレームの QoS クラスおよび DP レベルは同じ値です。これは、ポートベース QoS です。

2.3.16.2 Port Policing(ポートのポリシング)

「Configuration」→「QoS」→「Port Policing」をクリックすると、以下の画面が表示されます。

QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☐	500	Mbps	☐
3	☐	500	fps	☐
4	☐	500	kfps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐
11	☐	500	kbps	☐
12	☐	500	kbps	☐
13	☐	500	kbps	☐

ここでは、ポート入力のレートリミットを設定します。ポートが有効(Enabled)、かつフローコントロールモードが選択されている場合は、上限値に達すると、フレームを破棄せずに、ポーズフレームが送信されます(イーサネットの入力制御のため TCP セッションの制御の場合は設定値と異なる場合があります)。
それぞれ、「kbps」、「Mbps」、「fps」、「kfps」から設定する単位を選択できます。

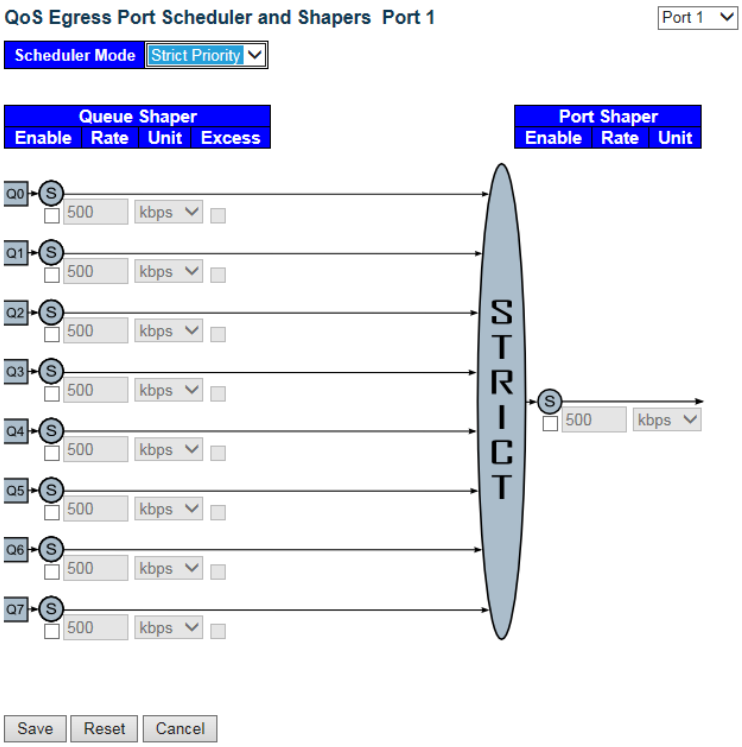
2.3.16.3 Port Scheduler

「Configuration」→「QoS」→「Port Scheduler」をクリックすると、以下の画面が表示されます。

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-

ここでは、各ポートのモード(「port egress scheduler」モード)および各キューの重み付け(Weight)が表示されます。
ポート番号をクリックすると、その出力ポートのスケジュールは以下のように表示されます。



ここでは、ポートの出力トラフィックのスケジューラおよび出力トラフィックのシェーピングを設定します。

トラフィックスケジューラは、「Strict Priority」モード、または「Weighted」モードで動作します。
「Weighted」モードの場合は、各キューの割り当てを設定することができます。

トラフィックシェーピングは、キューまたはポート単位で動作します。
この機能を選択すると制限値が設定され、設定値を超過した場合はフレームは破棄されます。

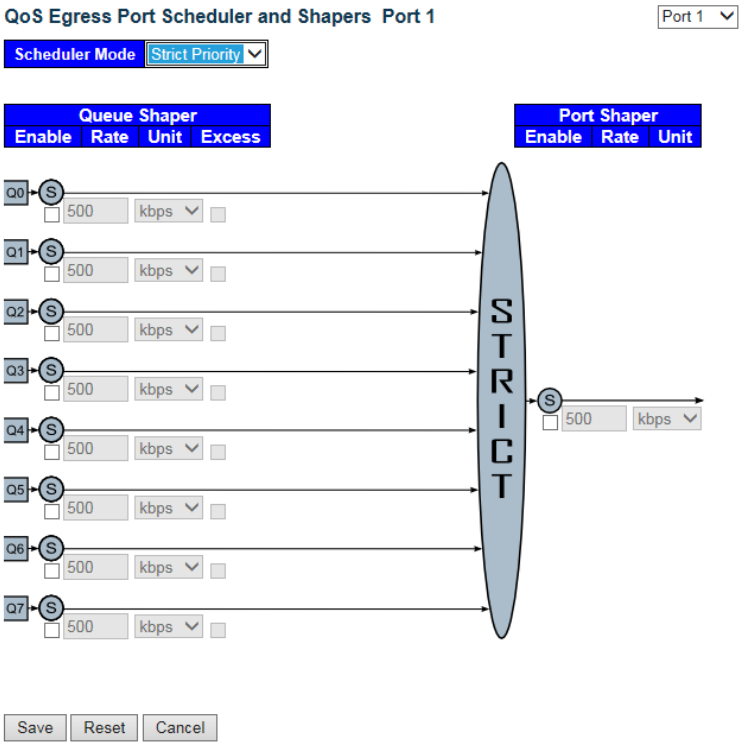
2.3.16.4 Port Shaping（ポートシェーピング）

「Configuration」→「QoS」→「Port Shaping」をクリックすると、以下の画面が表示されます。

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

ここでは、ポートおよびキューごとに出力シェーピングの設定が表示されます。
ポート番号をクリックすると、以下のように出力シェーピングの設定画面が表示されます。



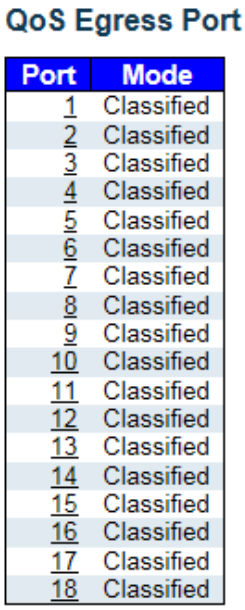
ここでは、ポートの出力トラフィックのスケジューラおよび出力トラフィックのシェーピングを設定します。

トラフィックスケジューラは、「Strict Priority」モード、または「Weighted」モードで動作します。
「Weighted」モードの場合は、キューごとに重み付けを設定可能です。
ただし、重み付けを設定できるのは「キュー5」までです。「キュー6」および「キュー7」のトラフィックが最優先されます。

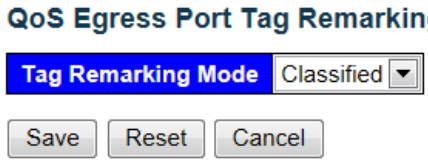
トラフィックシェーピングは、キューまたはポート単位で動作します。
この機能を選択すると制限値が設定され、設定値を超過した場合はフレームは破棄されます。

2.3.16.5 Port Tag Remarking

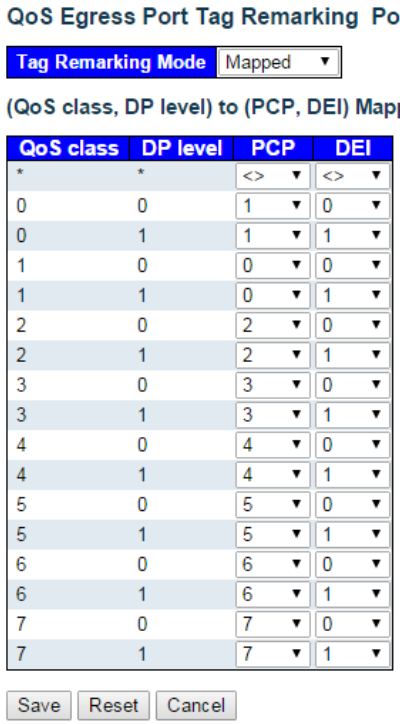
「Configuration」→「QoS」→「Port Tag Remarking」をクリックすると、以下の画面が表示されます。
ここでは、ポートのタグのリマーキングの設定を行うことができます。
この設定により、出力される際にフレームに PCP/DEI を追加および変更することが可能です。



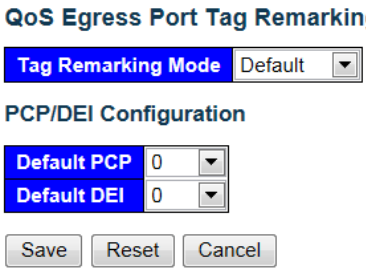
ポート番号をクリックすると、以下のように出力タグのリマーキング画面が表示されます。



※ Tag Remarking Mode が「Classified」の場合の画面



※ Tag Remarking Mode が「Mapped」の場合の画面



※ Tag Remarking Mode が「Default」の場合の画面

このモードは以下のとおりです。

- Classified: クラス分けされた PCP/DEI 値を使用 （追加・変更しない）
- Default : デフォルト設定の PCP/DEI 値を使用(出力 PCP/DEI はすべてここの設定値になる)
- Mapped : QoSクラスおよび DP レベルのマッピングのバージョンを使用(PCP/DEI 値により異なる PCP/DEI 値で出力する)

モードを選択し、パラメータを設定します。“Default”あるいは“Mapped”を選択すると、出力ポートがタグ付きポートの場合は、default/mapped PCP および DEI は出力タグ付きパケットに適用されます。
元の PCP および DEI の設定は、default/mapped PCP および DEI により再度マーク付されるか、default/mapped PCP および DEI により、ダブルタギング Q-in-Q アプリケーションのタグ以外に適用されます。

2.3.16.6 Port DSCP

「Configuration」→「QoS」→「Port DSCP」をクリックすると、以下の画面が表示されます。

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☐	DSCP=0	Disable
3	☐	Selected	Disable
4	☐	All	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable
11	☐	Disable	Disable
12	☐	Disable	Disable
13	☐	Disable	Disable
14	☐	Disable	Disable
15	☐	Disable	Disable
16	☐	Disable	Disable
17	☐	Disable	Disable
18	☐	Disable	Disable

Save Reset

ここでは、DSCP 入力および出力の設定を行います。入力設定の場合、ポートごとに入力変換、クラス分類の設定を変更できます。出力設定の場合は、各ポートのリライティング、リマッピングを行います。

☐ Ingress Translate(入力変換)について:
"Translate"が選択されている場合は、入力 DSCP 値は、QoS 設定用に別の DSCP 値に変換できます。変換用マッピングは「DSCP Translation」画面で設定し、変換した DSCP 値は入力 DSCP の QoS 設定に使用されます。

☐ Ingress Classify(入力クラス分け)について:
DSCP ingress classify は、DSCP から QoS へのクラス分けを行うことではありません(DSCP から QoS へのマッピングは「DSCP-Based QoS」画面では行われません)。「Port DSCP」の Ingress Classify は、QoS から内部 DSCP マッピングを行うのではなく、QoS クラス(「port default」、「VLAN タグ」、「DSCP」のいずれかから)を入手すると、Ingress Classify はこの QoS クラスを内部 DSCP にマッピングします。

フレーム送信時は、内部 DSCP は別の入力マッピングを行い DSCP 値に適用されます。
「Port DSCP」画面の「Egress Rewrite」メニューが"enable"/"Remap DP Unaware"/"Remap DP Aware"の場合は、Ingress Classify(入力クラス分け)の詳細については、以下のとおりです。

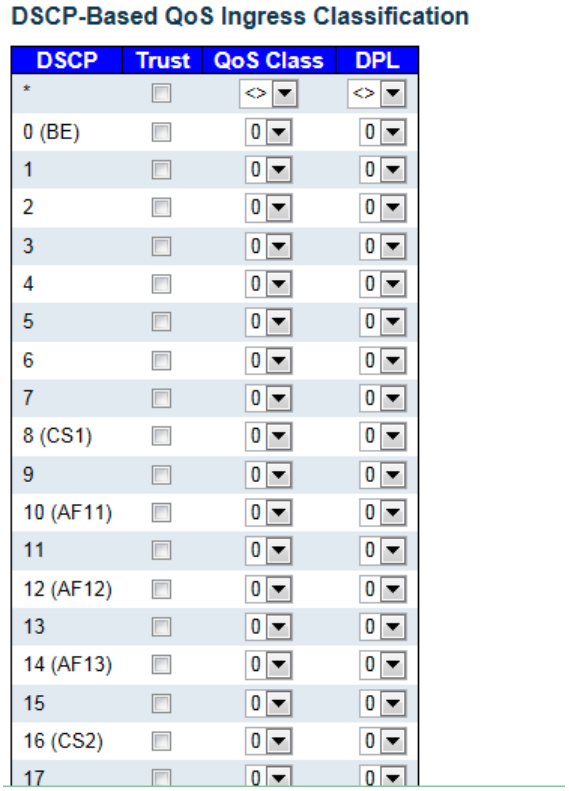
- Disable : 内部 DSCP への DSCP の QoS クラスのマッピング操作を無効にします。
- DSCP=0 : 受信 DSCP が「0」かどうかをクラス分けします(または有効な場合は変換されます)。
- Selected : 「DSCP Translation」画面で指定したクラス分類が有効な DSCP のみクラス分けします("classify"が選択されている場合のみ)
- All : すべての DSCP 値に有効。

Egress Rewrite（出力パケットの DSCP リライト）の詳細については、以下のとおりです。

- Disable：Egress rewrite なし。
- Enable ： リマッピングなしで、「DSCP Classification」画面での「Rewrite」の設定が有効になります。
- Remap DP Unaware: 内部 DSCP 値から「DSCP Translation」画面の“Remap DP0”設定をリマッピングします。
- Remap DP Aware ： 内部 DSCP 値から「DSCP Translation」画面の“Remap DP0”、または“Remap DP1”の設定をリマッピングします。

2.3.16.7 DSCP-Based QoS

「Configuration」→「QoS」→「DSCP-Based QoS」をクリックすると、以下の画面が表示されます。



ここでは、DSCP 値ごとに QoS 入力のクラス分けを設定します。

"Trust"にチェックを入れた DSCP 値をもつフレームのみが特定の QoS クラスにマッピングされ、不正な DSCP 値を持つ破棄優先度のフレームは、IP 以外のフレームとして処理されます。

2.3.16.8 DSCP Translation (DSCP 変換)

「Configuration」→「QoS」→「DSCP Translation」をクリックすると、以下の画面が表示されます。

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>		<>	<>
0 (BE)	0 (BE)		0 (BE)	0 (BE)
1	1		1	1
2	2		2	2
3	3		3	3
4	4		4	4
5	5		5	5
6	6		6	6
7	7		7	7
8 (CS1)	8 (CS1)		8 (CS1)	8 (CS1)
9	9		9	9
10 (AF11)	10 (AF11)		10 (AF11)	10 (AF11)
11	11		11	11
12 (AF12)	12 (AF12)		12 (AF12)	12 (AF12)
13	13		13	13
14 (AF13)	14 (AF13)		14 (AF13)	14 (AF13)
15	15		15	15
16 (CS2)	16 (CS2)		16 (CS2)	16 (CS2)
17	17		17	17
18 (AF21)	18 (AF21)		18 (AF21)	18 (AF21)
19	19		19	19

ここでは、すべての DSCP 値の QoS DSCP の基本変換を行います。DSCP は、"Ingress(入力)"、
または"Egress(出力)"で変換されます。

QoS クラスおよび DPL マップ用の DSCP を使用する前に、入力側の DSCP をまず新しい DSCP に変換します。

DSCP 変換方法には、以下の 2 つの設定方法があります。
- Translate : 入力側の DSCP は、DSCP 値(0～63 のいずれかの値)に変換可能です。
- Classify : 「Port DSCP」メニューで「Ingess Classify」が選択されている場合に、DSCP 値を選択すると、
内部 DSCP への QoS クラスのマッピングが有効にします。

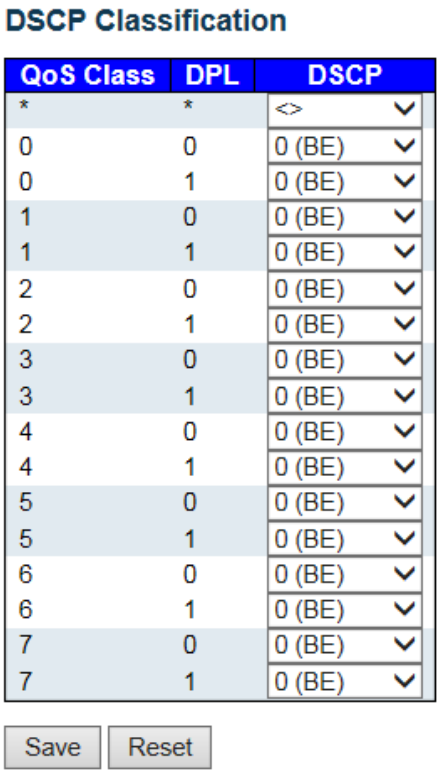
出力を行う場合に出力側で設定可能なパラメータは以下のとおりです。
- Remap DP0 により、「DP level 0」のフレームのリマッピングを制御します。
- Remap DP1 により、「DP level 1」のフレームのリマッピングを制御します。

この設定は、「Port DSCP」メニューの Egress Rewrite に適用されます。

詳細については、「Port DSCP」メニューの Egress Rewrite を参照してください。

2.3.16.9 DSCP Classification

「Configuration」→「QoS」→「DSCP Classification」をクリックすると、以下の画面が表示されます。



ここでは、QoS クラスおよび破棄優先度について内部 DSCP 値へのマッピングを設定します。

フレームを QoS クラス（port default、VLAN Tag、DSCP からのいずれか）から入手すると、この QoS を内部 DSCP へのマッピングを行います。内部 DSCP はフレーム送信時に別の出力マッピングを行い、DSCP の値に影響を与えます。
「Port DSCP」画面の「Egress Rewrite」が有効な場合は、出力 DSCP の値は上書きされます。

詳細については、「Port DSCP」の Egress Rewrite を参照してください。

2.3.16.10 QoS Control List (QoS コントロールリスト)

「Configuration」→「QoS」→「QoS Control List」をクリックすると、以下の画面が表示されます。

QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action		
								Class	DPL	DSCP

ここでは、QCL(QoS Control List)を設定します。それぞれの QCE は、パケットのパラメータおよび QoS アクションから構成されます。この機能により、特定のパケットのトラフィックは、設定されている QoS アクションを実行することが可能です。

(+)をクリックすると、以下の画面が表示されます。この画面にて QCE を作成します。

QCE Configuration

Port Members																	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

Tag	Any
VID	Any
PCP	Any
DEI	Any
SMAC	Any
DMAC Type	Any
Frame Type	Any

Action Parameters

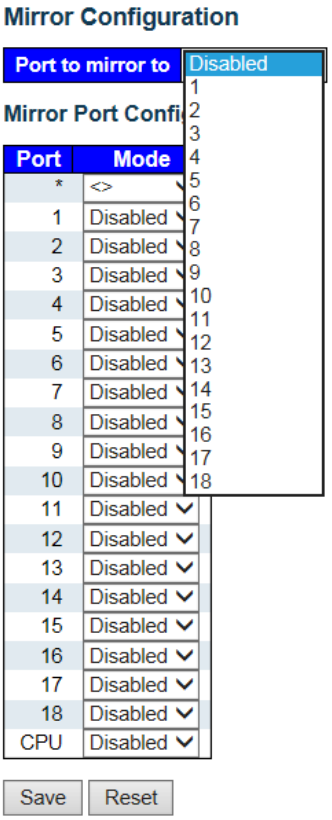
Class	0
DPL	Default
DSCP	Default

Save Reset Cancel

2.3.17 Mirroring (ミラーリング)

ここでは、本機のミラーリング機能を設定します。ネットワークの障害を解析するために、フレームフロー解析用としてフレーム測定器を接続したミラーポートにトラフィックをコピーしたり、ミラーリングを行ったりすることが可能です。

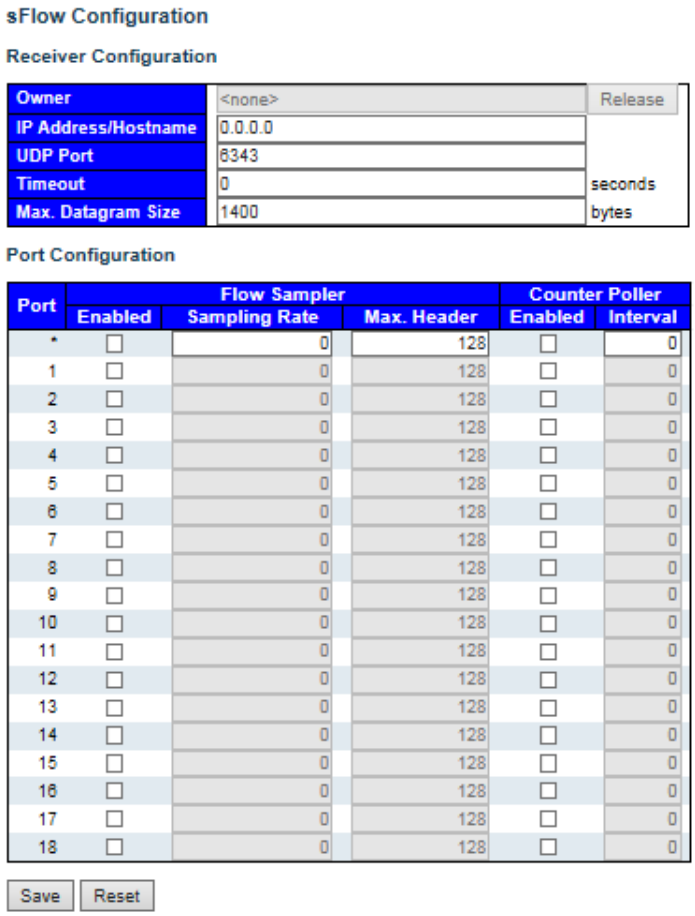
「Configuration」→「Mirroring」をクリックすると、以下の画面が表示されます。



ミラートラフィックは、パケットの送信/受信、あるいはその両方のフレームでミラーポートにミラーリングを行います。
モードを”Disabled”設定すると、ミラーリング機能は無効になります。

2.3.18 sFlow

「Configuration」→「sFlow」をクリックすると、以下の画面が表示されます。



ここでは、sFlow 機能を設定します。画面は sFlow レシーバの設定とポートごとの flow/カウンタサンプルの設定の 2 つに分けられます。

sFlow の設定は本体のメモリに保存されません。そのため、再起動時に sFlow サンプリングは無効となります。

2.4 Monitor（モニタリング）

ここでは、本機の設定のモニタリングについて説明します。

2.4.1 System

ここでは、システム情報やログ情報の表示について説明します。

2.4.1.1 Information（システム情報）

「Monitor」→「System」→「Information」をクリックすると、以下の画面が表示されます。

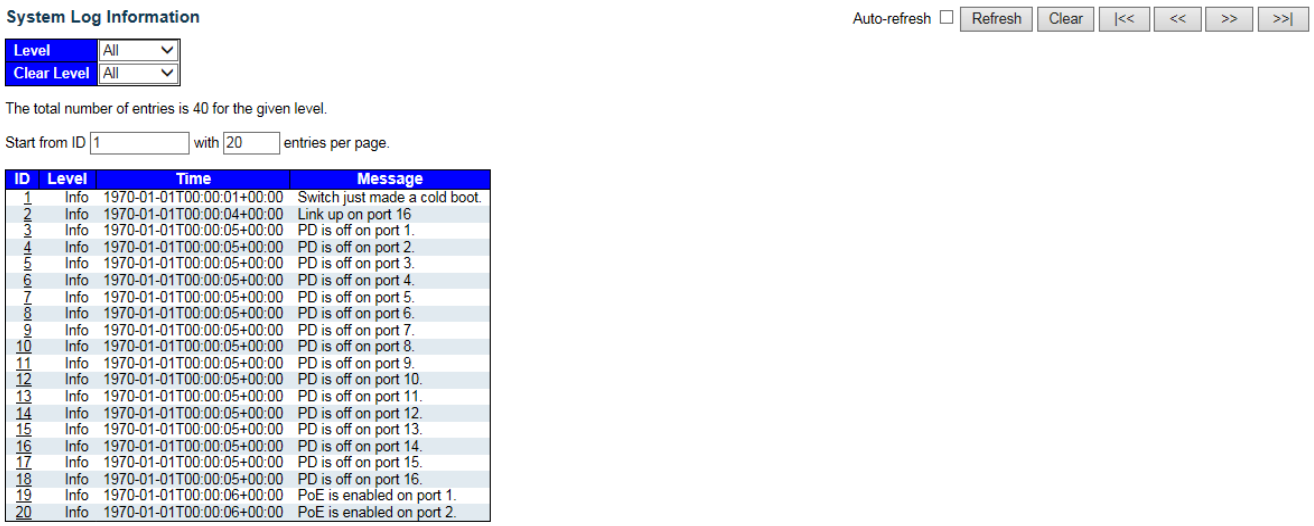
System Information

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-17-2e-1b-b7-fb
Time	
System Date	2014-12-15T14:02:28+09:00
System Uptime	2d 21:07:21
Software	
Software Version	FXC5218PE Ver:1.00.03
Software Date	2014-11-28

ここでは、システム情報が表示されます。

2.4.1.2 Log（システムログ情報）

「Monitor」→「System」→「Log」をクリックすると、以下の画面が表示されます。

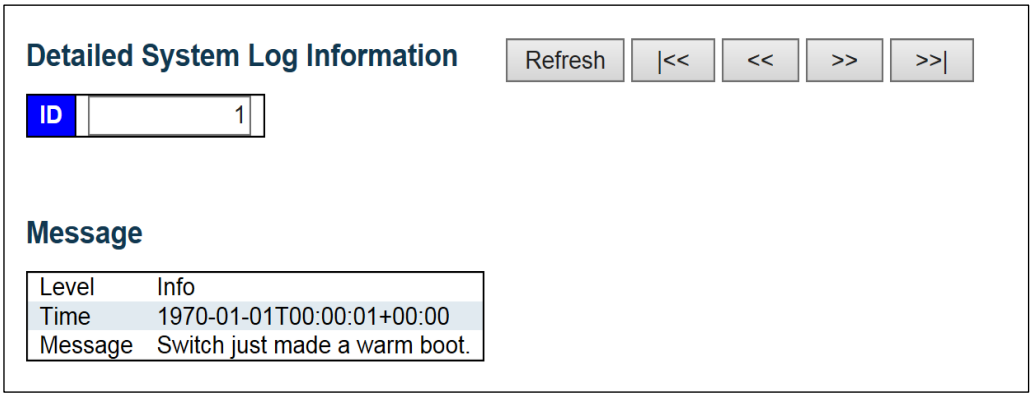


ここでは、本体のシステムログ情報が表示されます。

システムログ情報	
Level	選択したレベルのシステムログを表示します。
Clear Level	レベルを選択した後、<Clear>ボタンを押すと、選択したレベルのログを消去します。
ID	ID をクリックすると、ログの詳細(時刻とそのメッセージ)が表示されます。

2.4.1.3 Detailed Log(ログ情報の詳細)

「Monitor」→「System」→「Detailed Log」をクリックすると、以下の画面が表示されます。



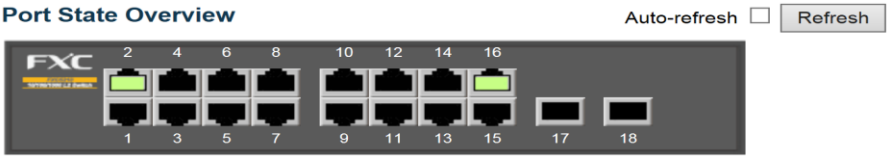
ここでは、ログの詳細が表示されます。ID を入力すると、その ID のログの詳細が表示されます。

2.4.2 Ports (ポートの情報表示)

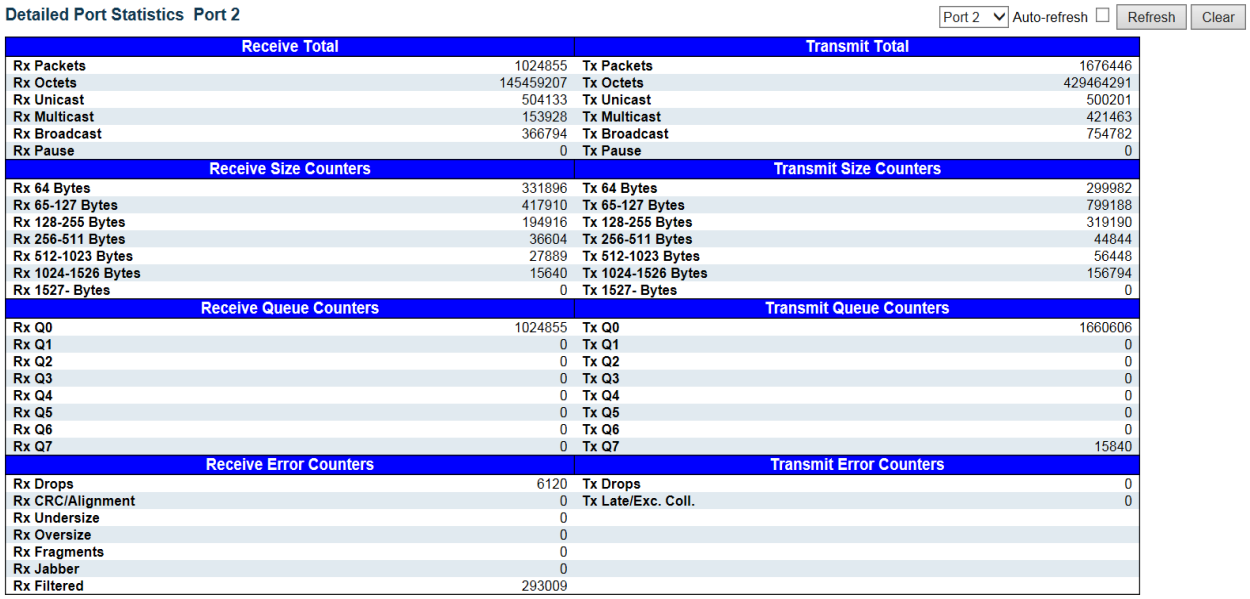
ここでは、ポートの状態の表示について説明します。

2.4.2.1 State (ポートの状態)

「Monitor」→「Ports」→「State」をクリックすると、以下の画面が表示されます。



ここでは、ポートのリンク状態を表示します。ポートをクリックすると、選択したポートの統計情報が表示されます。



Receive Total		Transmit Total	
Rx Packets	1024855	Tx Packets	1676446
Rx Octets	145459207	Tx Octets	429464291
Rx Unicast	504133	Tx Unicast	500201
Rx Multicast	153928	Tx Multicast	421463
Rx Broadcast	366794	Tx Broadcast	754782
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	331896	Tx 64 Bytes	299982
Rx 65-127 Bytes	417910	Tx 65-127 Bytes	799188
Rx 128-255 Bytes	194916	Tx 128-255 Bytes	319190
Rx 256-511 Bytes	36604	Tx 256-511 Bytes	44844
Rx 512-1023 Bytes	27889	Tx 512-1023 Bytes	56448
Rx 1024-1526 Bytes	15640	Tx 1024-1526 Bytes	156794
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	1024855	Tx Q0	1660606
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	15840
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	6120	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	293009		

2.4.2.2 Traffic Overview (トラフィック情報)

「Monitor」→「Ports」→「Traffic Overview」をクリックすると、以下の画面が表示されます。

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	3044	1461	392894	991467	0	0	0	0	731
2	1027875	1684714	145827138	431756026	0	0	6120	0	293009
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	1308	1798	915050	213879	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	569	4140	44026	473226	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	3589693	1187262	637677741	191257231	0	0	13037	0	636780
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0

ここでは、ポートごとの統計情報を表示します。

2.4.2.3 QoS Statistics (QoS 統計情報)

「Monitor」→「Ports」→「QoS Statistics」をクリックすると、以下の画面が表示されます。

Queuing Counters

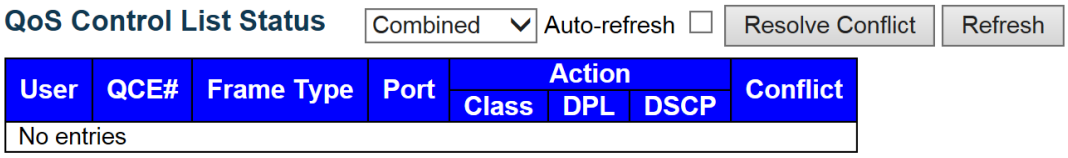
Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	2046487	0	0	0	0	0	0	0	0	0	0	0	0	0	0	395717
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ここでは、ポートごとにキューのトラフィック統計情報を表示します。ポートをクリックすると、そのポートの統計情報が表示されます。

2.4.2.4 QCL Status

「Monitor」→「Ports」→「QCL Status」をクリックすると、以下の画面が表示されます。

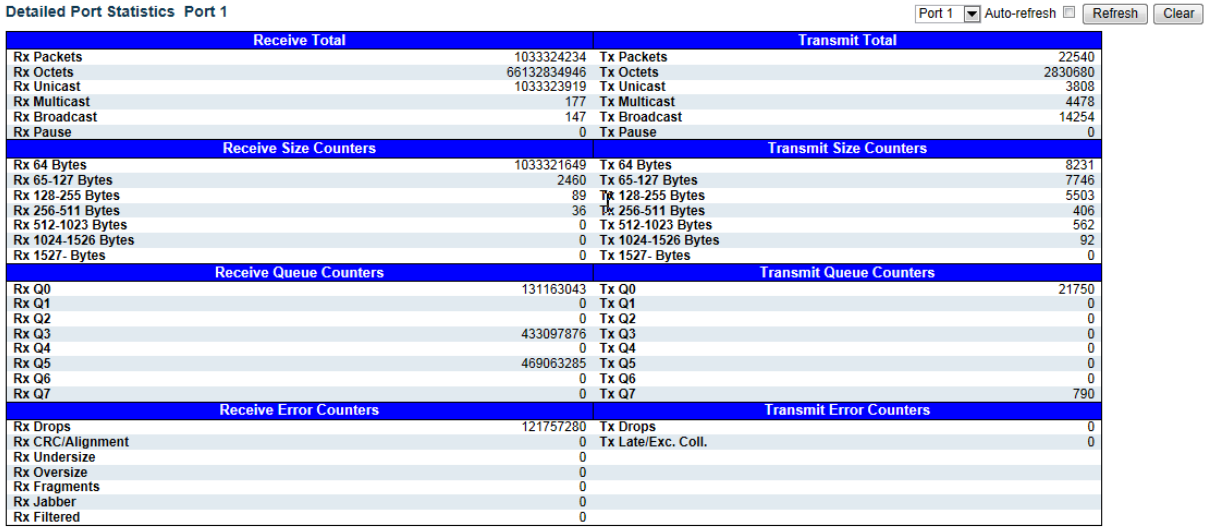


ここでは、QCL ユーザごとに QCL ステータスを表示します。
各行では、設定されている QCE について表示します。ハードウェア制限により特定の QCE がハードウェアに適用されない場合はコンフリクトが生じます。

Conflict(コンフリクト)について
QCL エントリのコンフリクトのステータスが表示されます。 H/W リソースが複数のアプリケーションで共用されるため、コンフリクトステータスが「Yes」の場合は QCE の追加に必要なリソースは利用できません。それ以外は「No」に設定されています。
<Resolve Conflict>ボタンをクリックすると、QCL エントリの追加に必要な H/W リソースを開放することにより、コンフリクトを回避することができます。

2.4.2.5 Detailed Statistics (統計情報の詳細)

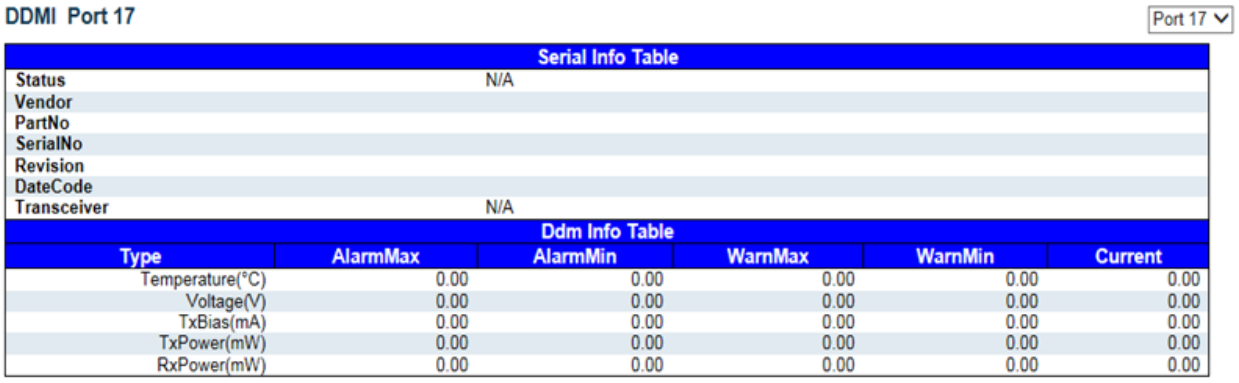
「Monitor」→「Ports」→「Detailed Statistics」をクリックすると、以下の情報が表示されます。



ここでは、ポートの統計情報の詳細を表示します。
ポートを選択すると、そのポートの統計情報の詳細が表示されます

2.4.2.6 DDMI

「Monitor」→「Ports」→「DDMI」をクリックすると、以下の画面が表示されます。



DDMI Port 17

Port 17

Serial Info Table	
Status	N/A
Vendor	
PartNo	
SerialNo	
Revision	
DateCode	
Transceiver	N/A

Ddm Info Table

Type	AlarmMax	AlarmMin	WarnMax	WarnMin	Current
Temperature(°C)	0.00	0.00	0.00	0.00	0.00
Voltage(V)	0.00	0.00	0.00	0.00	0.00
TxBias(mA)	0.00	0.00	0.00	0.00	0.00
TxPower(mW)	0.00	0.00	0.00	0.00	0.00
RxPower(mW)	0.00	0.00	0.00	0.00	0.00

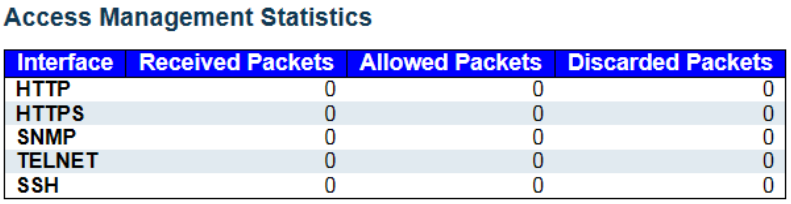
ここでは、DDMI(Digital Diagnostics Monitoring Interface)機能がサポートされている SFP トランシーバが本機に挿入されている場合に、その SFP トランシーバの情報とステータスが表示されます。

2.4.3 Security (セキュリティ)

ここでは、セキュリティの情報の表示について説明します。

2.4.3.1 Access Management Statistics (アクセス管理統計情報)

「Monitor」→「Security」→「Access Management Statistics」をクリックすると、以下の画面が表示されます。



Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

ここでは、インタフェースのトラフィック管理統計情報が表示されます。

2.4.3.2 Network

ここでは、ネットワークの情報の表示について説明します。

1) Port Security（ポートのセキュリティステータス）

1-1) Switch

「Monitor」→「Security」→「Network」→「Port Security」→「Switch」をクリックすると、以下の画面が表示されます。

Port Security Switch Status Auto-refresh ☐ Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-
11	----	Disabled	-	-

ここでは、ポートの現在の状態、および現在学習中の MAC アドレス数、ポートごとに学習可能な MAC アドレス数の上限が表示されます。

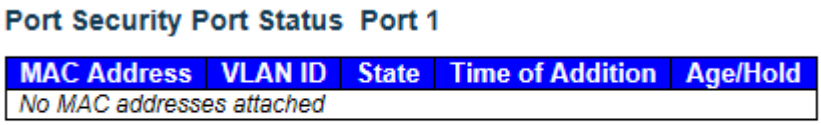
"state"はポートの状態を示しております。表示される内容は、以下のとおりです：

項目	説明
Disabled	現在ポートセキュリティサービスを使用しているユーザモジュールはありません。
Ready	ポートセキュリティサービスはユーザモジュールにより使用中、かつ未知の MAC アドレスからのフレームを受信するまで待機します。
Limit Reached:	ポートセキュリティサービスは、リミットコントロールユーザモジュールにより有効になります。モジュールは上限に達したことを示し、それ以上の MAC アドレスは設定できなくなります。
Shutdown:	ポートセキュリティサービスは、リミットコントロールユーザモジュールにより有効になります。モジュールは上限に達したことを示し、「Limit Control」画面にてポートの<Reopen>ボタンをクリックして復旧させるまで MAC アドレスの学習は出来なくなります。 「Limit Control」画面の詳細については、「2.3.3.2 Limit Control（リミットコントロール）」を参照してください。

1-2) Port

ここでは、ポートセキュリティによって設定された MAC アドレスが表示されます。ポートセキュリティは、直接設定を行うことができないため、モジュールから設定を行います。

「Monitor」→「Security」→「Network」→「Port Security」→「Ports」をクリックすると、以下の画面が表示されます。



ユーザモジュールによりポートセキュリティを有効にすると、ポートはソフトウェアベースの学習用に設定されます。このモードでは、未学習の MAC アドレスからのフレームをポートセキュリティモジュールで受信すると、すべてのユーザに対してこの MAC アドレスを送信するか、ブロックするかの問い合わせを行います。送信状態の MAC アドレスについては、すべての有効なユーザモジュールは合意すれば MAC アドレスは送信され、ユーザモジュールのうち1つでもブロックすると、ブロックされた状態になります。

□Age/Hold について： .

ユーザモジュールのうち1つでも MAC アドレスをブロックすると、待機時間(秒単位)が切れるまでブロック状態になります。ユーザモジュールは MAC アドレスの送信を許可すると、エージが有効になり、ポートセキュリティモジュールは、MAC アドレスがトラフィックを送信しているかどうかを定期的にチェックします。

エージングタイム(秒単位)が切れると、フレームは表示されなくなり、MAC アドレスは MAC テーブルから削除されます。それ以外は、新しいエージングタイムが開始されます。

エージが無効の場合、またはユーザモジュールが無制限に MAC アドレスを保持する場合は、(-)と表示されます。

2) NAS

ここでは、ネットワークアクセスサーバの情報の表示について説明します。

2-1) Switch

本機のネットワークアクセスサーバのスイッチのステータスを表示します。
「Monitor」→「Security」→「Network」→「NAS」→「Switch」をクリックすると、以下の画面が表示されます。

Network Access Server Switch Status

Auto-refresh ☐ Refresh

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				

2-2) Port

各ポートの NAS の統計情報を表示します。
「Monitor」→「Security」→「Network」→「NAS」→「Ports」をクリックすると、以下の画面が表示されます。

NAS Statistics Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Port 1 ▼ Auto-refresh ☐ Refresh

Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
Port 18

3) ACL Status

ACL ステータスを表示します。

「Monitor」→「Security」→「Network」→「ACL Status」をクリックすると、以下の画面が表示されます。

ACL Status

Combined Auto-refresh Refresh

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
IP Management	All	ARP	Permit	Disabled	Disabled	Disabled	Yes	No	422977	No
IP Management	All	IPv4/UDP 68 DHCP Server	Permit	Disabled	Disabled	Disabled	Yes	No	424	No

4) DHCP

4-1) Snooping Statistics （スヌーピング統計情報）

DHCP スヌーピングの統計情報を表示します。
「Monitor」→「Security」→「Network」→「DHCP」→「Snooping Statistics」をクリックすると、以下の画面が表示されます。

DHCP Snooping Port Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

4-2) DHCP Relay (リレー統計情報)

DHCP リレーの統計情報を表示します。

「Monitor」→「Security」→「Network」→「DHCP」→「Relay Statistics」をクリックすると、以下の画面が表示されます。

DHCP Relay Statistics

Auto-refresh Refresh Clear

Server Statistics

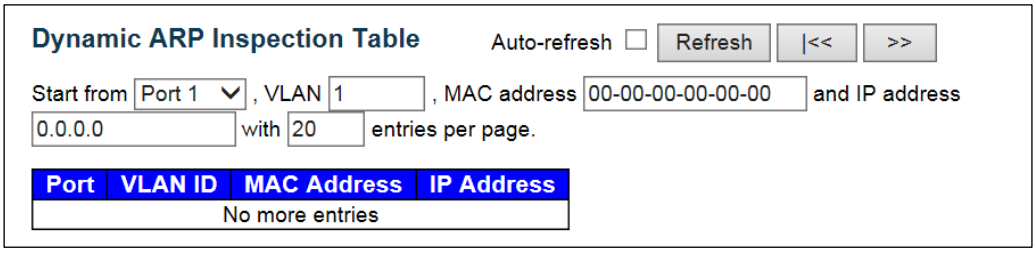
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

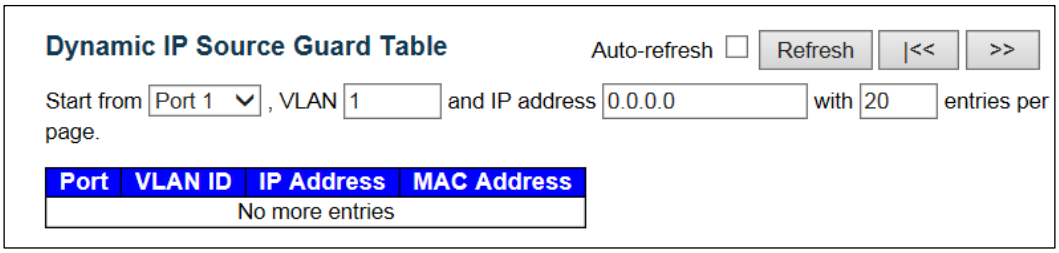
5) ARP Inspection (ARP インスペクション)

ダイナミック ARP インスペクションテーブルを表示します。
「Monitor」→「Security」→「Network」→「ARP Inspection」をクリックすると、以下の画面が表示されます。



6) IP Source Guard (IP ソースガード)

ダイナミック IP ソースガードテーブルを表示します。
「Monitor」→「Security」→「Network」→「IP Source Guard」をクリックすると、以下の画面が表示されます。



2.4.3.3 AAA

ここでは、AAA の情報の表示について説明します。

1) RADIUS Overview (RADIUS 概要)

「Monitor」→「Security」→「AAA」→「RADIUS Overview」をクリックすると、以下の画面が表示されます。

RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

ここでは、認証設定画面で設定可能な RADIUS サーバのステータス情報を表示します。

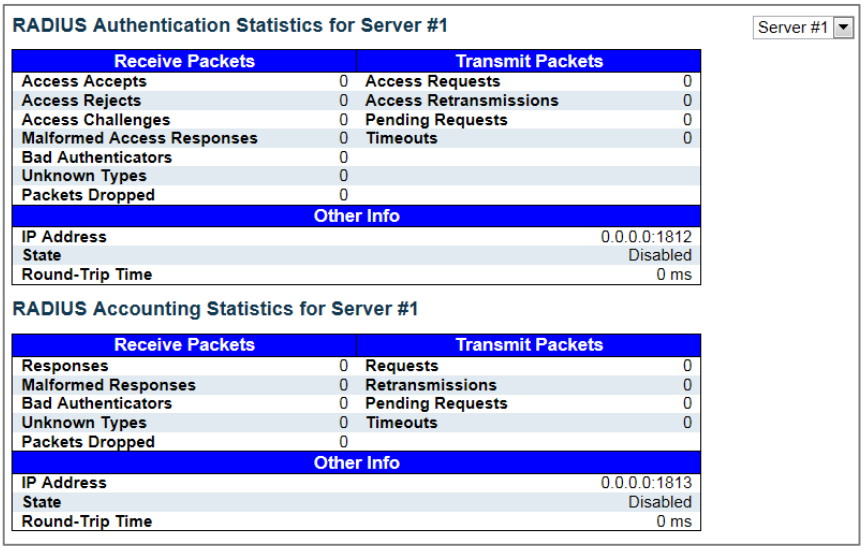
"Status"には、以下の情報が表示されます。

- Disabled : サーバは無効です。
- Not Ready : サーバは有効ですが、IP 通信は待機中です。
- Ready : サーバは有効、かつ IP 通信は動作中であり、RADIUS モジュールはアクセス許可された状態です。
- Dead(残り X 秒): このサーバにアクセスを行っても、設定したタイムアウト内で応答はありません。サーバは一時的に無効になりますが、"dead-time"が切れると、再度有効になります。この状態が起きるまでの秒数が"( )"内に表示されます。複数のサーバが有効な場合のみこの状態が発生します。

2) RADIUS Details (RADIUS 設定の詳細)

ここでは、RADIUS サーバについての統計情報の詳細が表示されます。

「Monitor」→「Security」→「AAA」→「RADIUS Details」をクリックすると、以下の画面が表示されます。



統計情報により、RFC4668 – RADIUS 認証クライアント MIB に指定されている近似値にマッピングします。
サーバのセレクトボックスを使って、詳細を表示するためにバックエンドサーバ間を切り替えます。

2.4.3.4 Switch

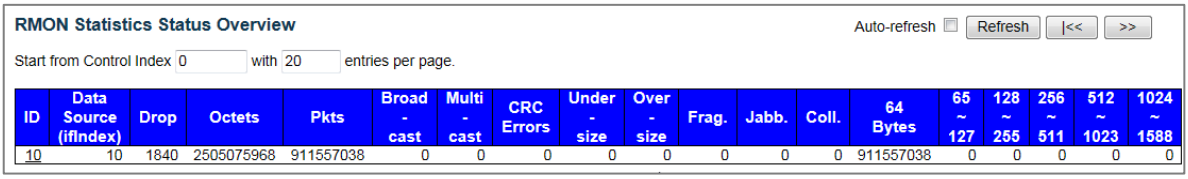
ここでは、スイッチセキュリティの情報の表示について説明します。

1) RMON

ここでは、RMON の情報の表示について説明します。

1-1) Statistics(統計情報)

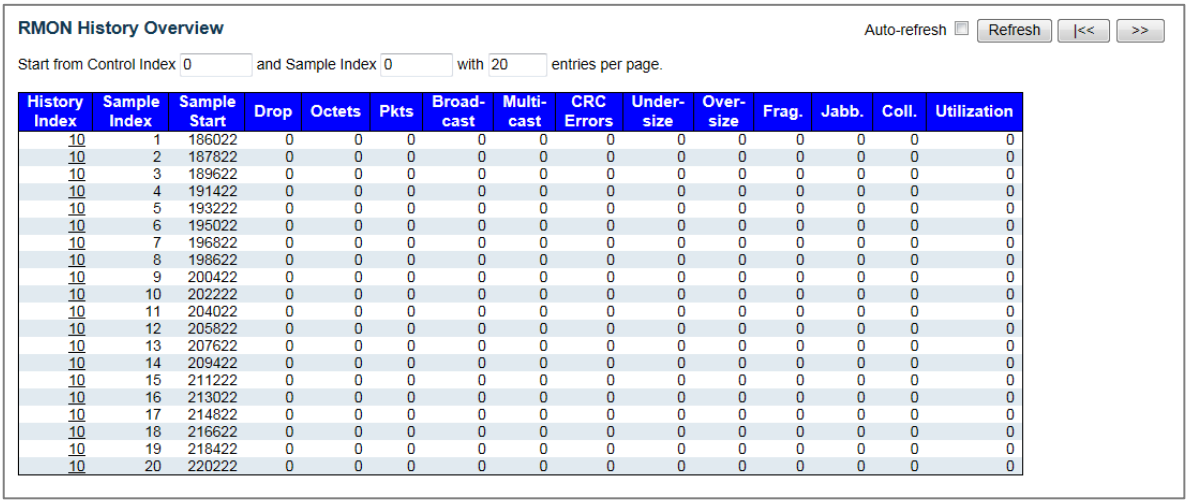
「Monitor」→「Security」→「Switch」→「RMON」→「Statistics」をクリックすると、以下の画面が表示されます。



ここでは、RMON 統計情報のエントリが表示されます。

1-2) History(履歴)

ここでは、RMON の履歴情報を表示します。
「Monitor」→「Security」→「Switch」→「RMON」→「History」をクリックすると、以下の画面が表示されます。



RMON History Overview

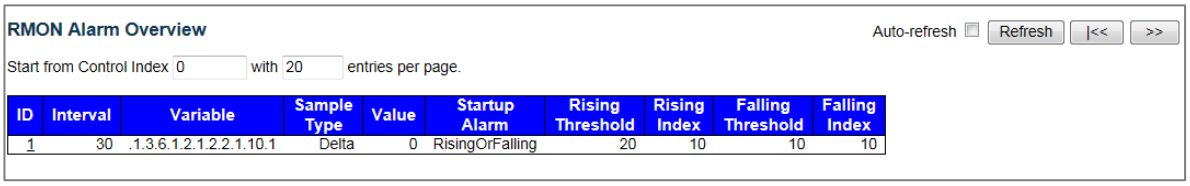
Auto-refresh Refresh |<< >>

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
10	1	186022	0	0	0	0	0	0	0	0	0	0	0	0
10	2	187822	0	0	0	0	0	0	0	0	0	0	0	0
10	3	189622	0	0	0	0	0	0	0	0	0	0	0	0
10	4	191422	0	0	0	0	0	0	0	0	0	0	0	0
10	5	193222	0	0	0	0	0	0	0	0	0	0	0	0
10	6	195022	0	0	0	0	0	0	0	0	0	0	0	0
10	7	196822	0	0	0	0	0	0	0	0	0	0	0	0
10	8	198622	0	0	0	0	0	0	0	0	0	0	0	0
10	9	200422	0	0	0	0	0	0	0	0	0	0	0	0
10	10	202222	0	0	0	0	0	0	0	0	0	0	0	0
10	11	204022	0	0	0	0	0	0	0	0	0	0	0	0
10	12	205822	0	0	0	0	0	0	0	0	0	0	0	0
10	13	207622	0	0	0	0	0	0	0	0	0	0	0	0
10	14	209422	0	0	0	0	0	0	0	0	0	0	0	0
10	15	211222	0	0	0	0	0	0	0	0	0	0	0	0
10	16	213022	0	0	0	0	0	0	0	0	0	0	0	0
10	17	214822	0	0	0	0	0	0	0	0	0	0	0	0
10	18	216622	0	0	0	0	0	0	0	0	0	0	0	0
10	19	218422	0	0	0	0	0	0	0	0	0	0	0	0
10	20	220222	0	0	0	0	0	0	0	0	0	0	0	0

1-3) Alarm(RMON アラームの表示)

ここでは、RMON のアラームに関する情報が表示されます。
「Monitor」→「Security」→「Switch」→「RMON」→「Alarm」をクリックすると、以下の画面が表示されます。



RMON Alarm Overview

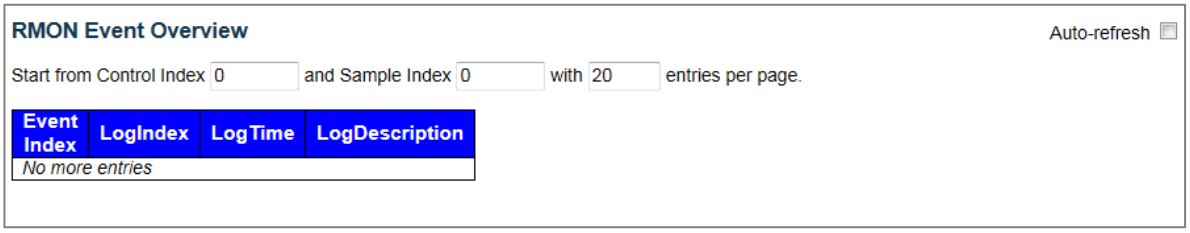
Auto-refresh Refresh |<< >>

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	30	.1.3.6.1.2.1.2.2.1.10.1	Delta	0	RisingOrFalling	20	10	10	10

1-4) Event(イベント情報の表示)

「Monitor」→「Security」→「Switch」→「RMON」→「Event」をクリックすると、以下の画面が表示されます。



RMON Event Overview

Auto-refresh

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

ここでは、RMON イベントテーブルのエントリが表示されます。

2.4.4 LACP

ここでは、LACP の情報の表示について説明します。

2.4.4.1 System Status(システムステータス)

ここでは、LACP インスタンスすべてのステータスを表示します。
「Monitor」→「LACP」→「System Status」をクリックすると、以下の画面が表示されます。

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
LLAG1	00-17-2e-21-99-b6	3	32768	0d 00:01:03	3,4

2.4.4.2 Port Status (ポートステータス)

「Monitor」→「LACP」→「Port Status」をクリックすると、以下の画面が表示されます。

LACP Status Auto-refresh ☐ Refresh

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-
14	No	-	-	-	-	-
15	No	-	-	-	-	-
16	No	-	-	-	-	-
17	No	-	-	-	-	-
18	No	-	-	-	-	-

ここでは、すべてのポートの LACP ステータスを表示します。

2.4.4.3 Port Statistics(ポートの統計情報)

ここでは、すべてのポートの LACP 統計情報を表示します。
「Monitor」→「LACP」→「Port Statistics」をクリックすると、以下の画面が表示されます。

LACP Statistics

Auto-refresh ☐ Refresh Clear

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0

2.4.5 Loop Protection (ループプロテクション)

ここでは、ループプロテクションのポートステータスが表示されます。
「Monitor」→「Loop Protection」をクリックすると、以下の画面が表示されます。

Loop Protection Status

Auto-refresh ☐ Refresh Clear

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

ループが発生すると、パケットストームが生成されます。これにより、ネットワーク障害が引き起こされる可能性がありますが、ループプロテクション機能により、ポート上で発生するこれらの障害を回避することができます。

2.4.6 Spanning Tree(スパニングツリー)

ここでは、スパニングツリーの情報の表示について説明します。

2.4.6.1 Bridge Status (ブリッジのステータス)

ここでは、すべての STP ブリッジインスタンスのステータスが表示されます。
「Monitor」→「Spanning Tree」→「Bridge Status」をクリックすると、以下の画面が表示されます。

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-17-2E-1B-B8-1B	32768.00-17-2E-1B-B8-1B	-	0	Steady	-

「CIST」あるいは「MSTIx」をクリックすると、以下のような画面が表示され、STP ブリッジのステータスが確認できます。

STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-17-2E-1B-B8-1B
Root ID	32768.00-17-2E-1B-B8-1B
Root Cost	0
Root Port	-
Regional Root	32768.00-17-2E-1B-B8-1B
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
3	-	Part of LLAG1	Forwarding				
4	-	Part of LLAG1	Forwarding				

2.4.6.2 Port Status(ポートステータス)

「Monitor」→「Spanning Tree」→「Port Status」をクリックすると、以下の画面が表示されます。

STP Port Status

Auto-refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-

ここでは、本機のポートの STP CIST ポートステータスを表示されます。

"CIST Role"には、「AlternatePort」、「BackupPort」、「RootPort」、「DesignatedPort」、「Disabled」のいずれかが表示されます。
"CIST State"には、「Discarding」、「Learning」、「Forwarding」のいずれかが表示されます。

2.4.6.3 Port Statistics(ポートの統計情報)

「Monitor」→「Spanning Tree」→「Port Statistics」をクリックすると、以下の画面が表示されます。

STP Statistics

Auto-refresh ☐ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

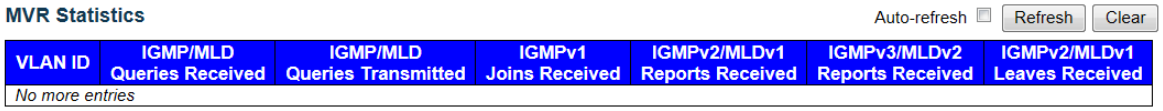
ここでは、ブリッジポートの STP ポートの統計情報のカウントが表示されます。
- MSTP : MSTP BPDU の送受信数
- RSTP : RSTP BPDU の送受信数.
- STP : legacy STP Configuration BPDU の送受信数.
- TCN:(legacy)Topology Change Notification(TCN:トポロジ変更通知)BPDU の送受信数
- Discarded Unknown : 未学習のスパニングツリーBPDU の受信(破棄)数
- Discarded Illegal : 不正なスパニングツリーBPDU の受信(破棄)数

2.4.7 MVR

ここでは、MVR の情報の表示について説明します。

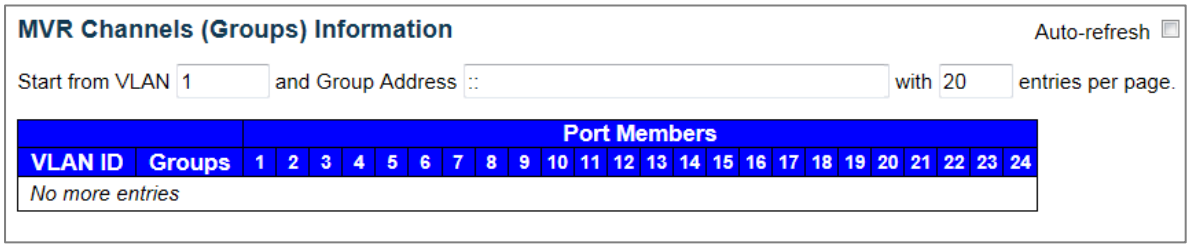
2.4.7.1 Statistics(統計情報)

「Monitor」→「MVR」→「Statistics」をクリックすると、以下の画面が表示されます。
ここでは、MVR 統計情報が表示されます。



2.4.7.2 MVR Channel Groups(MVR チャネルグループ)

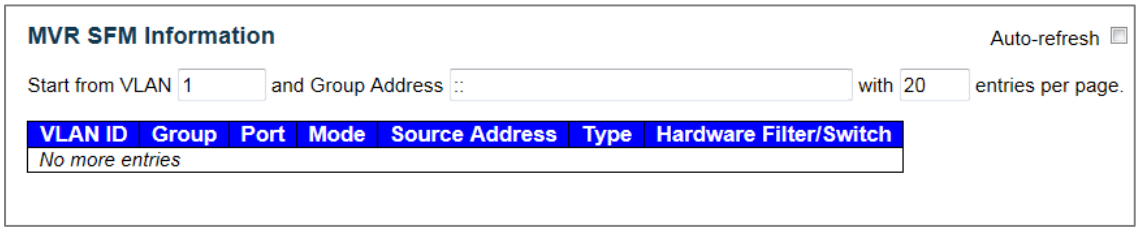
「Monitor」→「MVR」→「MVR Channel Groups」をクリックすると、以下の画面が表示されます。



「MVR Channels(Groups) Information」のエントリが表示されます。
「MVR Channels(Groups) Information」は、まず VLAN ID ごとに、次にグループごとにソートされます。

2.4.7.3 MVR SFM Information

「Monitor」→「MVR」→「MVR SFM Information」をクリックすると、以下の画面が表示されます。



「MVR SFM Information」テーブルのエントリが表示されます。「MVR SFM(Source-Filtered Multicast) Information」表には、SSM(Source-Specific Multicast)情報も含まれます。この表は、まず VLAN ID ごとに、次にグループごと、ポートごとにソートされます。
同じグループの異なるソースアドレスは、単一のエントリとして処理されます。

2.4.8 IPMC

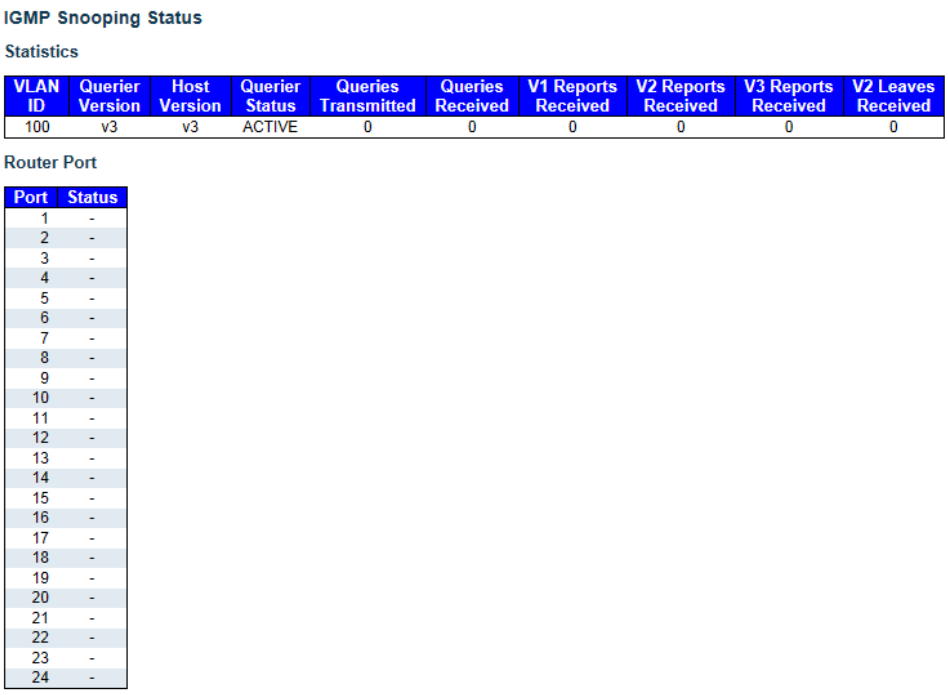
ここでは、IGMP スヌーピング及び MLD スヌーピングの情報の表示について説明します。

2.4.8.1 IGMP Snooping(IGMP スヌーピング)

ここでは IGMP スヌーピングの情報の表示について説明します。

1) Status(IGMP スヌーピングのステータス)

「Monitor」→「IPMC」→「IGMP Snooping」→「Status」をクリックすると、以下の画面が表示されます。



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
100	v3	v3	ACTIVE	0	0	0	0	0	0

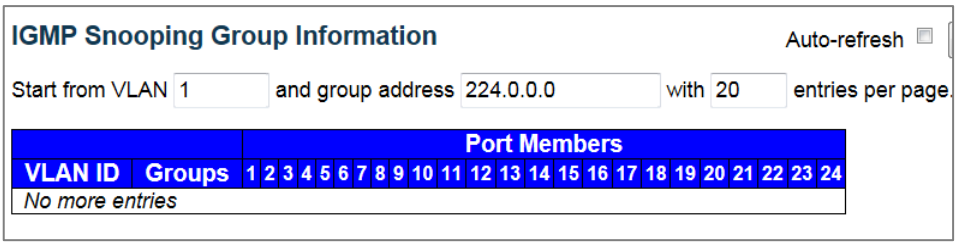
Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-

ここでは、IGMP スヌーピングのステータス(プロトコルステータス及び統計情報、ルータポートの状態)を表示します。

2) Groups Information （グループ情報）

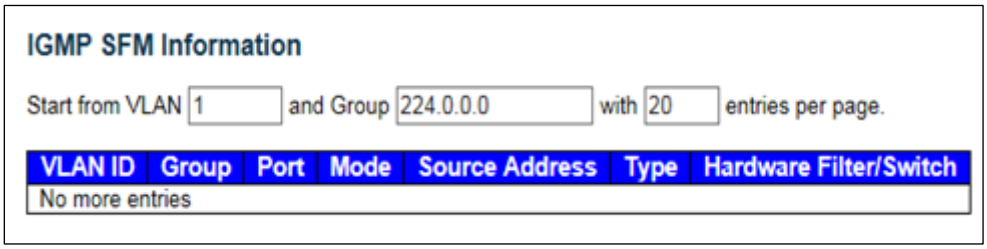
「Monitor」→「IPMC」→「IGMP Snooping」→「Groups Information」をクリックすると、以下の画面を表示します。



ここでは「IGMP Group」テーブルの情報が表示されます。
「IGMP Group」テーブルは、 まず VLAN ID、次にグループごとにソートされます。

3) IPv4 SFM Information （IPv4 SFM 情報）

「Monitor」→「IPMC」→「IGMP Snooping」→「IPv4 SFM Information」をクリックすると、以下の画面が表示されます。



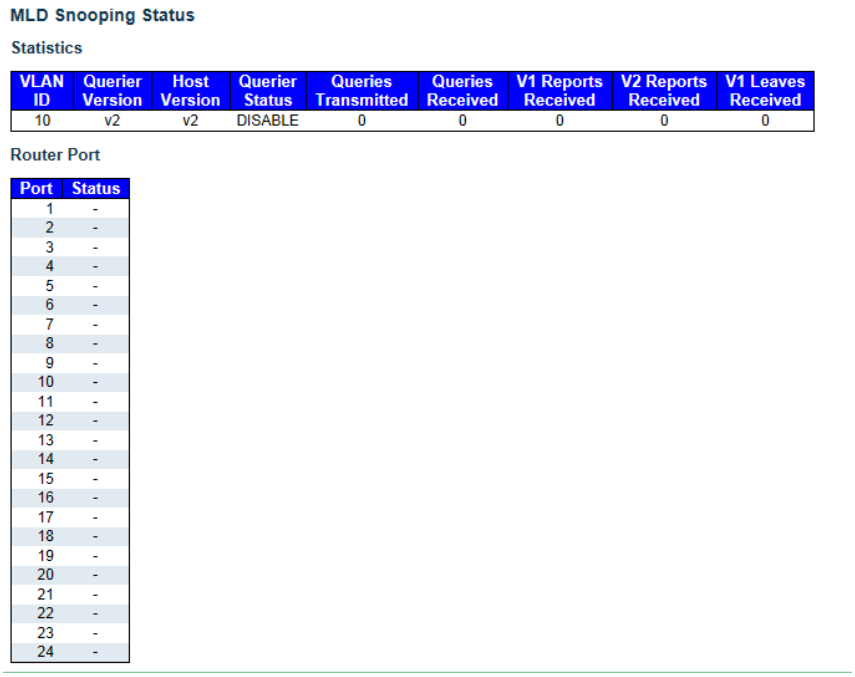
ここでは「IGMP SFM Information」テーブルのエントリの情報が表示されます。
「IGMP SFM(Source-Filtered Multicast) Information」テーブルには、SSM(Source-Specific Multicast) 情報も含まれます。この表は、まず VLAN ID ごとに、次にグループごと、ポートごとにソートされます。同じグループの異なるソースアドレスは、単一のエントリとして処理されます。

2.4.8.2 MLD Snooping (MLD スヌーピング)

MLD スヌーピングの情報を表示するには、「Monitor」→「IPMC」→「MLD Snooping」をクリックします。

1) Status (**MLD スヌーピングのステータス**)

「Monitor」→「IPMC」→「MLD Snooping」→「Status」をクリックすると、以下の画面が表示されます。



MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
10	v2	v2	DISABLE	0	0	0	0	0

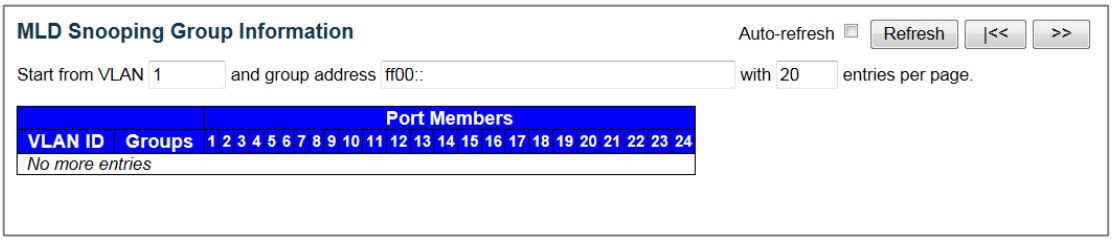
Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-

ここでは、MLD スヌーピングのステータス(プロトコルステータス及び統計情報、ルータポートの状態)が表示されます。

2) Groups Information (グループ情報の表示)

「Monitor」→「IPMC」→「MLD Snooping」→「Groups Information」をクリックすると、以下の画面が表示されます。



MLD Snooping Group Information

Auto-refresh Refresh |<< >>

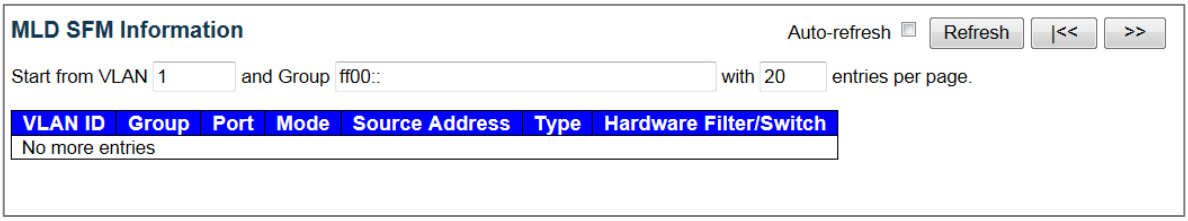
Start from VLAN 1 and group address ff00:: with 20 entries per page.

VLAN ID	Groups	Port Members 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
No more entries		

ここでは、MLD グループ情報が表示されます。
「MLD Group」テーブルは、まず VLAN ID ごとに、次にグループごとにソートされます。

3) IPv6 SFM Information(IPv6 SFM 情報)

「Monitor」→「IPMC」→「MLD Snooping」→「IPv6 SFM Information」をクリックすると、以下の画面が表示されます。



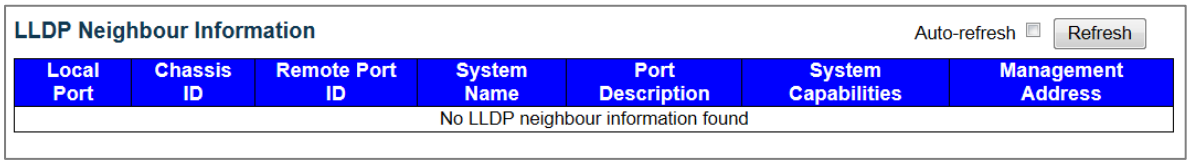
ここでは、「MLD SFM Information」テーブルのエントリの情報が表示されます。
「MLD SFM(Source-Filtered Multicast) Information」テーブルには、SSM(Source-Specific Multicast)情報も含まれます。
この表は、まず VLAN ID ごとに、次にグループごと、ポートごとにソートされます。
同じグループの異なるソースアドレスは、単一のエントリとして処理されます。

2.4.9 LLDP

ここでは、LLDP の情報の表示について説明します。

2.4.9.1 Neighbours (ネイバー情報)

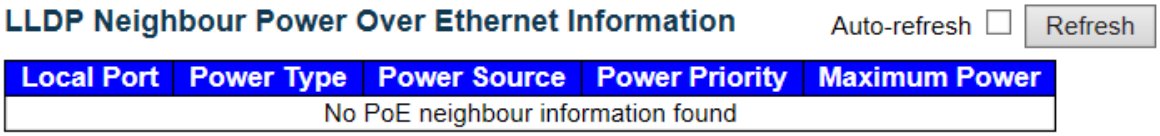
「Monitor」→「LLDP」→「Neighbours」をクリックすると、以下の画面が表示されます。



ここでは、すべての LLDP ネイバー装置(隣接装置)のステータスを表示します。
表には、検出した LLDP ネイバー装置がポートごとに表示されます。

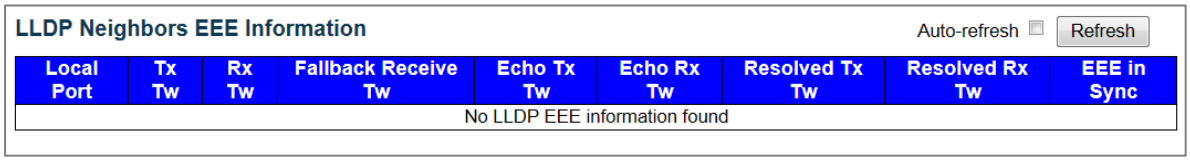
2.4.9.2 PoE

ここでは、PoE のネイバー情報が表示されます。
「Monitor」→「LLDP」→「PoE」をクリックすると、以下の画面が表示されます。



2.4.9.3 EEE

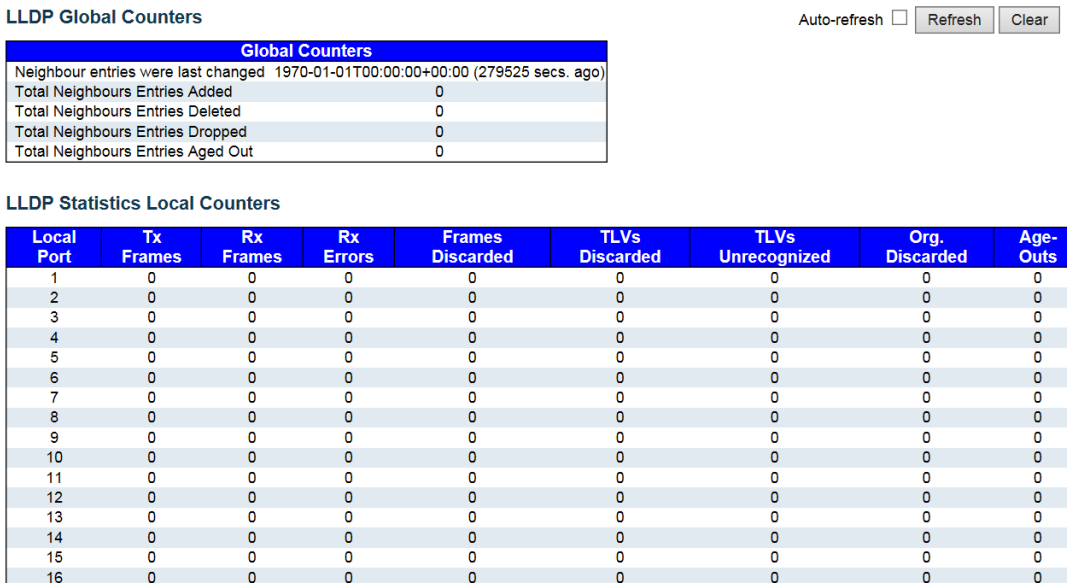
「Monitor」→「LLDP」→「EEE」をクリックすると、以下の画面が表示されます。



ここでは、LLDP によって交換される EEE 情報を表示します。
EEE の消費電力削減によって、トラフィックに遅延が発生します。
EEE は電力の消費を抑えるために回路の電源を切るため、リンク上のトラフィックを送信する際に再起動に要する時間が生じることにより遅延が生じます。この時間は"wakeup time"と言います。遅延を最小限に抑えるために、それぞれの tx/rx の"wakeup time"の情報を交換した上で、相互に必要な最小限の"wakeup time"を選択します。

2.4.9.4 Port Statistics (ポート統計情報)

「Monitor」→「LLDP」→「Port Statistics」をクリックすると、以下の画面が表示されます。



LLDP Global Counters

Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbour entries were last changed	1970-01-01T00:00:00+00:00 (279525 secs. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0

ここでは、すべての LLDP トラフィックを表示します。
それぞれ 2 タイプのカウンタが表示されます。
「LLDP Global Counters」画面にはスイッチ全体のカウンタが表示され、「LLDP Statistics Local Counters」画面にはポート単位のカウンタが表示されます。

2.4.10 PoE

PoE は、「Power Over Ethernet」の略称で、標準のイーサネットケーブルを利用してリモート先の装置に電力を供給するために使用します。例えば、電源を得るのが困難な場所に配置された IP 電話、無線 LAN アクセスポイント、その他の機器に電力を供給することが可能です。

「Monitor」→「PoE」をクリックすると、以下の画面が表示されます。

Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
2	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
3	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
4	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
5	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
6	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
7	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
8	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
9	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
10	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
11	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
12	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
13	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
14	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
15	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
16	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

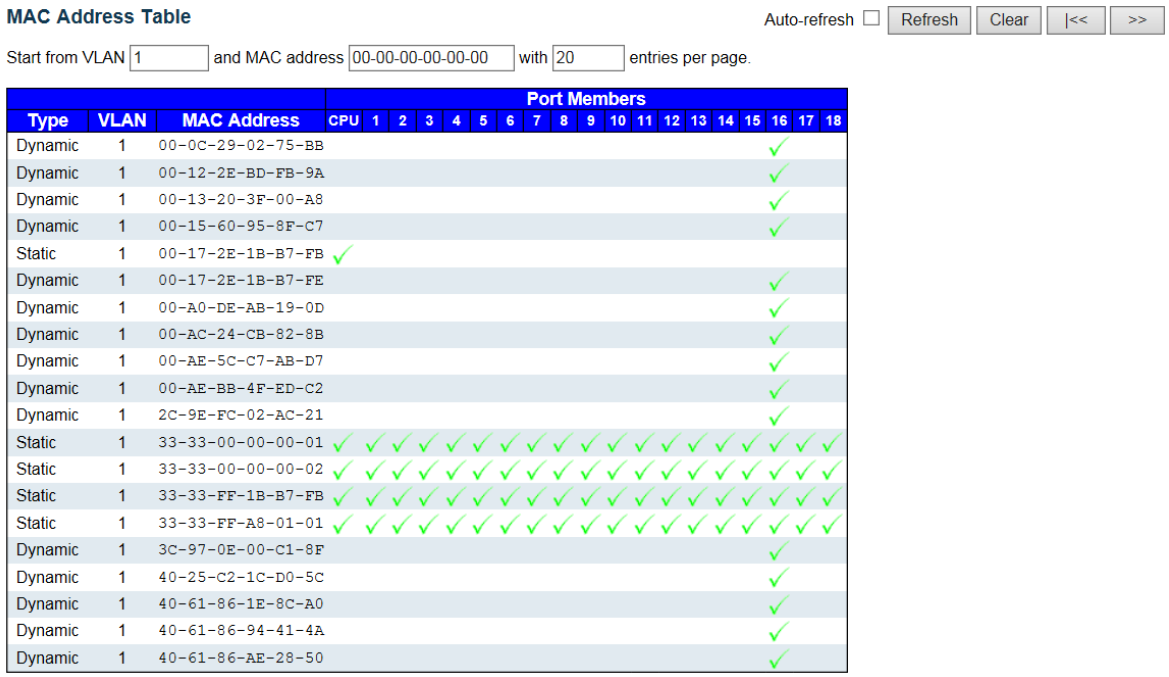
ここでは、各 PoE ポートの現行の状態を確認することが可能です。

Power Over Ethernet Status	
PD Class	受電側機器で使用されている最大電力を定義するクラスに応じてクラス分けされます。 以下の 5 クラスに定義されます。 ・ Class 0: Max. power 15.4 W ・ Class 1: Max. power 4.0 W ・ Class 2: Max. power 7.0 W ・ Class 3: Max. power 15.4 W ・ Class 4: Max. power 30.0 W
Power Requested	受電側機器に予約するために必要な電力量を表示します。
Power Allocated	本機により受電側機器に割り当てられた電力量を表示します。
Power Used	受電側機器で現在使用中の電力量を表示します。
Current Used	受電側機器で現在使用中の電流量を表示します。
Priority	Priority は、ポートのプライオリティを表します。それぞれの電流のプライオリティは 3 レベル(「Low」、「High」、「Critical」)に分けられます。 このプライオリティは、リモート装置により要求された電流が供給可能な電流を超えた場合に使用します。この場合、プライオリティの低いポートについては、ポート番号の大きい順から電源が消えます。

Port Status	ポートのステータスを表示します。ステータスは以下の値のいずれかになります: ・ PoE not available-No PoE chip found：PoE は未サポートです。 ・ PoE turned OFF-PoE disabled:PoE は使用不可です。 ・ PoE turned OFF-Power budget exceeded：受電側機器に必要な、または使用している電力が上限を超えた場合は、プライオリティの一番低いポートがダウンします。 ・ No PD detected:受電側機器は検出されません。 ・ PoE turned OFF- PD overload:許容可能な電力量を超えた場合は、電源はダウンします。 ・ PoE turned OFF - PD is off：Invalid PD - 受電側機器は検出されましたが、正しく動作しません。

2.4.11 MAC Table

「Monitor」→「MAC Table」をクリックすると、以下の画面が表示されます。



MAC テーブルには、エントリは「8192 個」まで含まれ、まず VLAN ID、次に MAC アドレスごとにソートされます。

2.4.12 VLANs

ここでは、VLAN の情報の表示について説明します。

2.4.12.1 VLAN Member

「Monitor」→「VLANs」→「VLAN Membership」をクリックすると、以下の画面が表示されます。

VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page. |<< >>

	Port Members																
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

ここでは、VLAN メンバーのステータスが表示されます。

2.4.12.2 VLAN Port

「Monitor」→「VLANs」→「VLAN Port」をクリックすると、以下の画面が表示されます。

VLAN Port Status for Static user

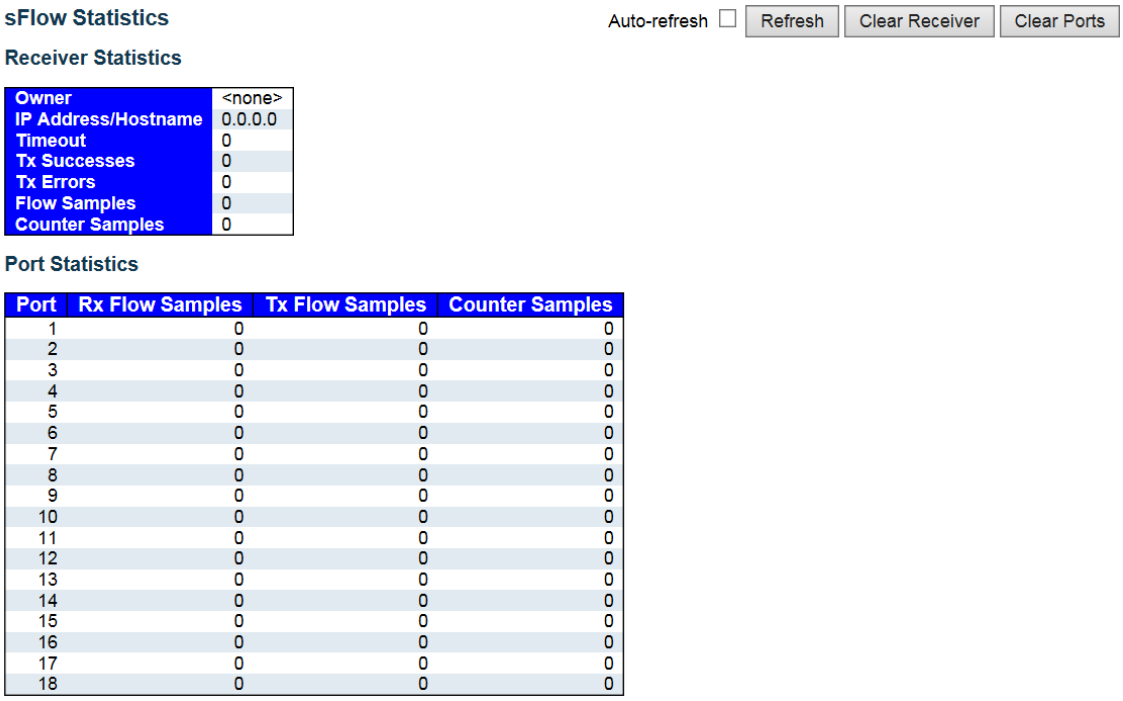
Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No
11	1	UnAware	Disabled	All	Untag_this	1	No
12	1	UnAware	Disabled	All	Untag_this	1	No
13	1	UnAware	Disabled	All	Untag_this	1	No
14	1	UnAware	Disabled	All	Untag_this	1	No
15	1	UnAware	Disabled	All	Untag_this	1	No
16	1	UnAware	Disabled	All	Untag_this	1	No
17	1	UnAware	Disabled	All	Untag_this	1	No
18	1	UnAware	Disabled	All	Untag_this	1	No

ここでは、VLAN ポートのステータスおよび設定が表示されます。

2.4.13 sFlow

「sFlow」は、トラフィックをリアルタイムにモニタリングするためのプロトコルです。sFlow はトラフィックのごく一部をサンプリングして統計的手法で解析するため、ネットワークや装置の負荷をかけずにモニタリングすることができます。

「Monitor」→「sFlow」をクリックすると、以下の画面が表示されます。



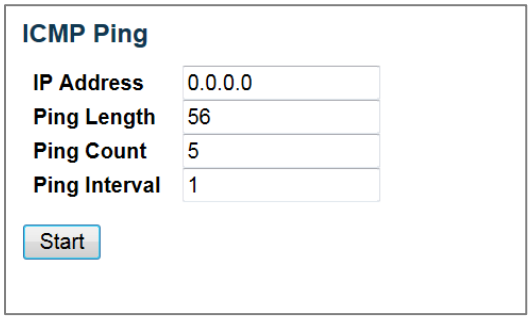
ここでは、レシーバおよびポート単位の sFlow 統計情報が表示されます。

2.5 Diagnostics（診断機能）

ここでは、本機の診断機能について説明します。

2.5.1 ping

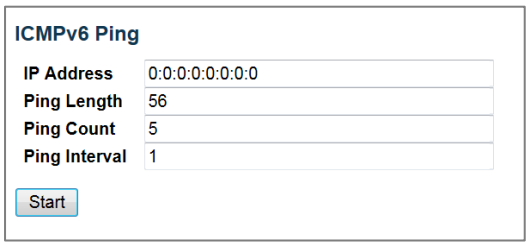
「Diagnostics」→「ping」をクリックすると、以下の画面が表示されます。



ここでは、IP 接続の問題解決のために、ICMP の PING パケットを送信することができます。
<Start>ボタンをクリックすると、ICMP パケットが送信され、応答を受信次第シーケンス番号および往復時間が表示されます。
ICMP ECHO_REPLY の IP パケットを受信したデータ量は常に要求したデータスペース（ICMP header）よりも大きく、8 バイトになります。この画面は、すべてのパケットからの応答を受信するまで、またはタイムアウトになるまで自動的に更新されます。

2.5.2 ping6

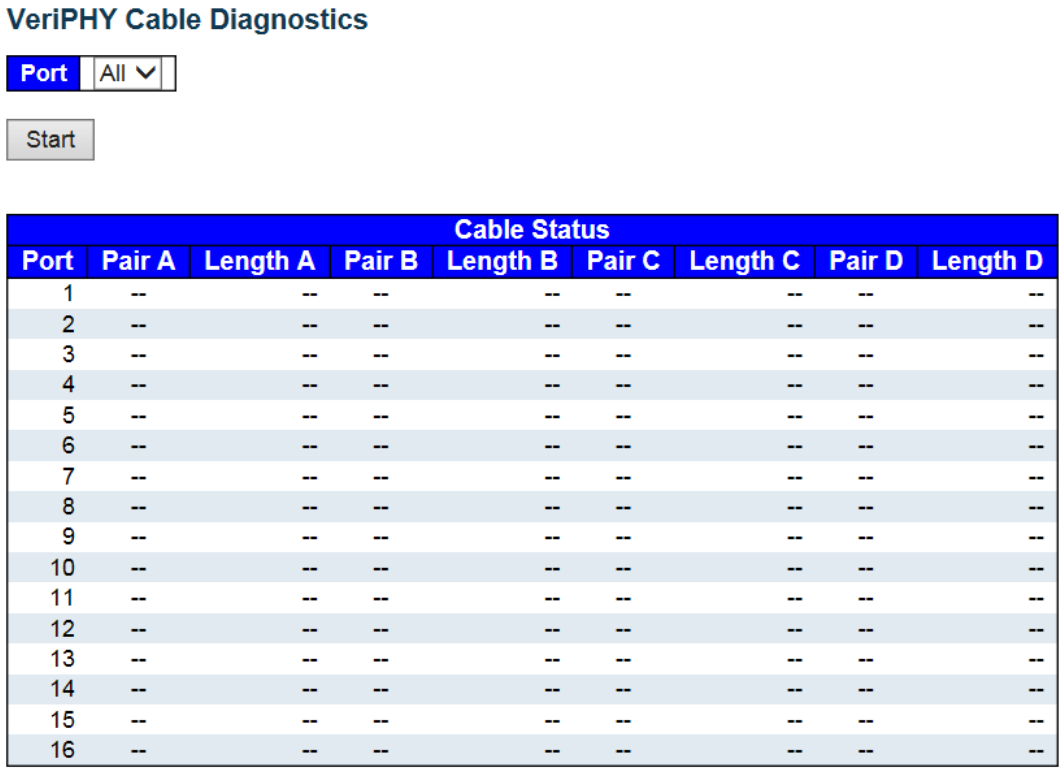
「Diagnostics」→「ping6」をクリックすると、下の画面が表示されます。



ICMPv6 接続の問題解決のために、ICMPv6 PING パケットを送信することができます。
<Start>ボタンをクリックすると、ICMPv6 パケットが送信され、応答を受信次第シーケンス番号および往復時間が表示されます。
この画面は、すべてのパケットからの応答が受信されるまで、またはタイムアウトになるまで自動的に更新されます。

2.5.3 VeriPHY (ケーブル診断)

「Diagnostics」→「VeriPHY」をクリックすると、以下の画面が表示されます。



ここでは、10/100/1000M ポートの VeriPHY(ケーブル診断)の設定を行います。
ポートを指定して<Start>をクリックすると、そのポートの診断が開始されます。診断には「約 5 秒」ほどかかります。
すべてのポートが選択されている場合は、診断に「約15秒」ほど要します。完了すると、画面が自動的に更新され、ケーブルステータス表にケーブル診断の結果が表示されます。

【注記】:
VeriPHY は、「7～140m」の長さのケーブルについては正しく実行可能です。
10/100Mbps ポートは、VeriPHY が動作時ではリンクダウンするため、10 Mbps または 100Mbps の管理ポートで VeriPHY を起動する場合は、VeriPHY が完了するまで応答しなくなります。

2.6 Maintenance（メンテナンス）

ここでは、メンテナンスの設定方法について説明します。

2.6.1 Restart （再起動）

「Maintenance」→「Restart Device」をクリックすると、以下の画面が表示されます。

ここでは、本機の再起動を行うことができます。
Yes ： 本機を再起動します。
No ： 再起動せずに、「Port State Overview」画面に戻ります。

2.6.2 Factory Defaults （工場出荷時設定）

「Maintenance」→「Factory Defaults」をクリックすると、以下の画面が表示されます。

ここでは、本機の設定を工場出荷時状態に戻すことができます(IP 設定のみ保持されます。)。
新しい設定はすぐに適用されるため、再起動する必要がありません。
Yes ： 本機の設定を工場出荷時の状態に戻します。
No ： 設定をリセットせずに、「Port State Overview」画面に戻ります。

2.6.3 Software (ソフトウェア)

ここでは、ソフトウェアのアップロードとソフトウェアの設定方法について説明します。

2.6.3.1 Upload(ソフトウェアの更新)

ここでは、ソフトウェアの更新を行います。

ソフトウェアのアップロードを行うには、＜Browse＞ボタンをクリックして、ソフトウェアの保存場所を選択し、＜Upload＞ボタンをクリックします。

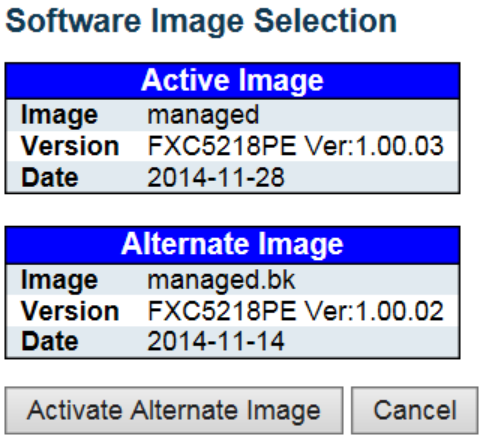
ソフトウェアの更新を行う場合、更新が開始されている旨のメッセージが表示されます。
約 1～2 分経過すると、ソフトウェアの更新が完了し、本機は再起動します。

本機では、ソフトウェアのバックアップ機能をサポートしています。ソフトウェアの更新後、古いソフトウェアは代替ソフトウェアに切り替わり、新規のソフトウェアを有効にします。古いバージョンのソフトウェアを使用したい場合は、「Image Select」画面の<Activate Alternate Image>ボタンをクリックすることによって有効にすることが可能です。

【警告】:
更新中は、Web へのアクセスが中断しているように見えますが、電源を再起動したり、電源を落としたりしないでください。
万が一更新中に電源を切った場合は、何らかの障害が起きる可能性があります。

2.6.3.2 Image Select(ソフトウェアの選択)

「Maintenance」→「Software」→「Image Select」をクリックすると、以下の画面が表示されます。



ここでは、本機で現在有効となっているソフトウェア(Active Image)と、代替ソフトウェア(Alternate Image)についての情報が表示され、使用するソフトウェアを選択することが可能です。

【注記】:
1. 現在実行中のソフトウェアが代替のソフトウェアの場合は、起動中のソフトウェアのみが表示され、
＜Activate Alternate Image＞ボタンは無効になります。

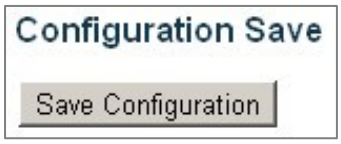
2. 代替ソフトウェアを使用している場合(元々有効な状態だったソフトウェアに問題がある場合や、手動でソフトウェアを切り替えた等の理由で)、新しいソフトウェアをアップロードすると、"Active Image"のスロットに新しいソフトウェアがインストールされ、これが有効となります。

2.6.4 Configuration (config ファイルの設定方法)

「Maintenance」→「Configuration」→「Save」をクリックすると、以下の画面が表示されます。
ここでは、本機の config ファイル(設定情報)の保存やアップロードについて説明します。

2.6.4.1 Save(保存)

「Maintenance」→「Configuration」→「Save」をクリックすると、以下の画面が表示されます。ここでは config ファイルをローカルに保存することができます。config ファイルはテキスト形式で保存されます。



2.6.4.2 Upload(アップロード)

「Maintenance」→「Configuration」→「Upload」をクリックすると、以下の画面が表示されます。
ここでは、config ファイルのアップロードをすることが出来ます。

FXC5210PE/FXC5218PE/FXC5224PE
Management Guide
(FXC17-DC-200009-R1.0)

初版　　2017 年 12 月

Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide
FXC5210PE/5218PE/5224PE
Management Guide

FXC株式会社