Future X Communications

FXC5210
FXC5218
FXC5224
Management Guide

2024 年 8 月 Ver.2.4

FXC株式会社

FXC5210/5218/5224 本マニュアルについて

- 本マニュアルでは、FXC5210/FXC5218/FXC5224 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FXC5210/FXC5218/FXC5224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。

この装置は､クラス A 情報技術装置です｡この装置を家庭環境で使用すると電波妨害を引き起こすことがあります｡この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

はじめに

この度は、弊社 FXC5210/5218/5224 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、基本的な設定を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マネジメント機能にログインすることも可能です。

1 章　コマンドインターフェース

1.1 コマンドラインインターフェースによる設定方法

1.1.1 コマンドラインインターフェースへのアクセス

コンソールポート、またはネットワークから Telnet 経由で管理インターフェースにアクセスする場合、コマンド（コマンドラインインターフェース/CLI）により本機の設定を行います。

1.1.2 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：

機器背面の左部のコンソールポートに同梱のコンソールケーブルを接続します。
片方を PC などの COM ポートに接続します。
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)。

下記設定値を設定してください。

- 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：なし
- 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  : FXC5218
Ver:1.00.03
MAC Address       : 00-17-2E-15-FB-8C
Number of Ports   : 18
Username          : admin
Password:
Login in progress...
FXC52XX#
------------------------------------------------------------
```

1.1.3 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。

FXC5218# configure
FXC5218(config)# interface vlan 1
FXC5218(config-if)# ip address 192.168.1.100 255.255.255.0
FXC5218(config-if)# exit
FXC5218(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 FXC52xx#”（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、およ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。

1.1.4 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、簡単なヘルプ情報が表示されます。
また"?"と入力するとキーワードやパラメータのコマンド文法が表示されます。

■コマンドの表示

コマンド上で"?"と入力すると、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。

```
------------------------------------------------------------
# ?
  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
  configure     Enter configuration mode
  copy          Copies from one file to another
#
------------------------------------------------------------
```

1. ユーザレベル

本機へのアクセスレベルには、管理者レベル（レベル 3）、オペレータレベル（レベル 2）、ゲストレベル(レベル 1)の 3 つのレベルに分けられます。
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。
システムの初期設定時のユーザは、“admin”（パスワードは“admin”）で管理者レベルです。

1)　管理者レベル

初期設定時のユーザ名およびパスワードは**"admin"** / ”**admin**”。
管理者レベルのユーザは、“(config)#”の下に“username”コマンドで設定します。
アクセスレベルは “3”です。

本機にログイン後、“FXC52XX**#**”とプロンプト表示されます。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。

```
---------------------------------------------------------------
#  ?
  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
  configure   Enter configuration mode
  copy        Copies from one file to another
#
---------------------------------------------------------------
```

本機の基本的なシステムコマンドは下記のとおりです。

システム設定には、“**configure**”コマンドを入力すると、以下の画面が表示されます。

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

configure モードでは、本機の一般的な設定を行うことができます。
“exit”コマンドを使用して、このモードを終了します。

ポートの設定を行う場合は、“**interface**”コマンドを使用すると、以下の画面が表示されます。

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

“ethernet 1/5”:イーサネットのスイッチ番号 1、ポート 5 番を意味します。

“interface”コマンドには、別のサブコマンド“vlan”があります。
このモードで本機の IP アドレスを設定することが可能です。

```
---------------------------------------------------------------
(config)# interface vlan 10
(config-if)#
---------------------------------------------------------------
```

“exit”コマンドでこのモードを終了します。

2) オペレータレベル

オペレータレベルのユーザは、アクセスレベルは、“2”です。

本機の基本的なシステムコマンドは以下のとおりです。

```
---------------------------------------------------------------
> ?
  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
>
---------------------------------------------------------------
```

オペレータレベルでは、本機のステータスおよび設定を表示し、システムのメンテナンスコマンドを実行します。

3) ゲストレベル

ゲストレベルのユーザは、アクセスレベルは”1”です。
本機にログインすると、以下のように “>“と表示されます。続けて、“?”コマンドを入力すると、以下の画面が表示されます。

```
---------------------------------------------------------------
 > ?
  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
>
-----------------------------------------------------------------
```

ゲストレベルでは、本機のステータス、一部の設定内容を表示することのみ可能です。

2. 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。

- [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 Tab キーを押すと、コマンド名が“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。
- ↑(上矢印キー): 最後に入力したコマンドを表示します。
- ↓(下矢印キー): 次に入力したコマンドを表示します。
- ←|→(左右矢印キー): カーソルを移動します。
- [Backspace]: カーソルの前の文字を削除します。
- [?]: コマンドリストを表示します。

3. コマンドモード

コンソール画面用のコマンドモードは、以下の 4 つです。

1) 基本コマンド

ログイン後の基本コマンドです。これらのコマンドには、ユーザは本機の設定/ステータス、ネットワークデバイスの ping、リブートなどがあります。
“#”:管理者用の(アクセスレベル 3 のユーザ)、“>“:オペレータ用(アクセスレベル 2 のユーザ)およびゲスト用(アクセスレベル1のユーザ)となります。

2) Configureモードコマンド

configure モードのコマンドは、本機の一般用の設定です。
“configure” コマンドを使用すると、グローバル config モードに移行します。
プロンプトは、“(config)#”と表示されます。

3) Port/VLANグループのインターフェース設定コマンド

ポートの設定を行うには、グローバル config モードの“interface ethernet 1/x”コマンドを使用します。
プロンプト表示は、“(config-if)#”と表示されます。
例えば、“interface ethernet 1/5:ポート 5 の設定用コマンドです。

VLAN インターフェースの設定を行うは、グローバル config モードで“interface vlan x”コマンドを使用します。
“プロンプト表示は、“(config-if)#”と表示されます。
例えば、“interface vlan 100” は、VLAN 100 の設定用コマンドです。

4) VLAN設定コマンド

VLAN 設定を行うには、グローバル config モードの“vlan database”コマンドを使用します。
プロンプト表示には、“**(config-vlan)#**”と表示されます。

1.2 基本コマンド

1.2.1 グローバルコマンド

username/password に“admin”/“admin”を使用する場合、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
  configure Enter configuration mode
  copy          Copies from one file to another
#
---------------------------------------------------------------
```

1)　exit command

現在の操作を終了します。基本コマンド画面からログアウトします。

2)　help command

使用可能なコマンドが表示されます。

3)　history command

入力したコマンドの履歴が表示されます。

4)　logout command

ログアウト用のコマンドです。

5)　ping command

PING を行い、ネットワーク接続および動作が正常に行われているか確認します。
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)
```

例: “ping 192.168.1.80”の場合 、” # ping 192.168.1.80”と表示されます。

6) ping6 command

別のネットワークに PING を行い、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。

プロンプト画面で“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
---------------------------------------------------------------
```

例:”ping6 2003::01”の場合は、” # ping6 2003::01”と表示されます。

7) quit command

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。

8) reload command

本機を再起動(ウォームスタート)する際に使用します。
“reload”と入力すると、数秒以内に本機が再起動(ウォームスタート)します。

```
---------------------------------------------------------------
# reload
System will reboot in a few seconds
---------------------------------------------------------------
```

9) show command

show ?”と入力すると、サブコマンドが表示されます。

```
------------------------------------------------------------
Enter “show ?” at the prompt, the sub-command list will be shown.
# 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
  lacp                LACP statistics
  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 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
------------------------------------------------------------
```

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、例えば”show port ?”と入力すると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
---------------------------------------------------------------
```

“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>
---------------------------------------------------------------
```

“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
---------------------------------------------------------------
```

画面には、複数のコンソール画面が表示される場合は、“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 commands」を参照してください。

10) calendar command

システムの日時を手動で設定します。

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

この設定は、揮発性メモリに記録されます。

11) configure command

コンソール画面をグローバル Config モードに変更すると、“(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。

12) copy command

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

■ **copy config running-config tftp <ip address> “yyy”**
現在動作している設定を IP “<ip アドレス>”(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、テキスト形式で保存されます。

■ **copy config tftp running-config <ip address> “yyy”**
コマンド: IP “<ip アドレス>”(IPv4、または IPv6 アドレス)の TFTP サーバから“yyy”という設定ファイルをリストアします。

■ **copy firmware tftp running-firmware <ip address> “yyy”**
IP “<ip アドレス>”(IPv4、または IPv6 アドレス)の TFTP サーバから“yyy”というソフトウェアをアップデートします。

1.2.2 Configureコマンド

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

ポートの設定を行うには、configure モードの“interface”コマンドを使って設定します。単独ポートの場合は、“interface ethernet 1/5 と指定し、ポート 5 の設定となります。複数ポート(範囲)の場合は、“interface ethernet 1/5,6,10-15”:ポート 5, 6, 10, 11, 12, 13, 14, 15 の設定となります。
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 configuration
 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-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
 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
----------------------------------------------------------------
```

1) exit command

現在のオペレーションを終了し、前のモードに戻ります。

2) help command

このコマンドで使用可能なコマンドをすべて表示します。

3) history command

入力したコマンドの履歴を表示します。

4) logout command

コンソール画面からログアウト時に使用します。

5) quit command

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) end command

グローバル config モードを終了します。

7) hostname command

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。
使用可能な文字列は、A-Z,a-z,0-9 および-（ハイフン）です

8) aaa command

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。

■ **aaa authentication login console [local|none|radius|tacacs+]**
コンソールへのユーザによるログイン用の認証方式を設定します。

■ **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。

■ **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。

■ **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で認証
  - 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で認証
  - tacacs+: 認証用のリモート TACACS+サーバのデータベースで認証

“radius”および“tacacs+”の後の“fallback”サブコマンドについて、
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。障害等でサーバで認証が出来ない場合は、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、もしくは、WEB 用の”AAA”機能で設定します。
TACACS+ サーバは、tacacs-authentication-server コマンド、もしくは、WEB 用の”AAA”機能で設定します。
TACACS+ サーバは、tacacs-authentication-server コマンド、あるいは、WEB 用の”AAA”機能で設定します。

9) acl command

本機の ACL（アクセスコントロールリスト）機能の設定の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定義する必要があります。
パケットのレイヤ2～レイヤ 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、log）を定義します。

“acl ?”コマンドを使用すると、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
 ----------------------------------------------------------------
```

■ **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）です。
フィルタリングルールの ACL 設定用の画面“**(config-ace-x)#**”に切り替えが可能です。
ACL ルールを定義される場合、“(config-if)#”にてポート設定モードのの“acl”コマンドを使って、接続ポートに ACL ルールを適用します。

■ **acl delete “x”**

ACE(アクセス制御エントリ)を削除します。
“x”:1～256 までの値（ACE のインデックス）です。

■ **acl rate-limiter “x” unit [pps/kbps] rate “y”**

帯域制御(レートリミット)を定義します。
単位は kbps(キロビット/秒) あるいは pps(パケット/秒)です。
“x”: 1～16 までの値（帯域制御(レートリミット)のインデックス）です。
“y”: pps 単位の 0-3276700 までのレートリミットの値あるいは
kbps 単位の 0, 100, 200,300, ..., 1000000 の値となります。

帯域制御(レートリミット)は、インデックスの番号ごとに、ACE、ポートに適用可能です。

1) “**acl add x**” コマンド ACL ルール (ACE)を定義します。
   プロンプト表示は、“**(config-ace-x)#**”となります。

2) “**(config-ace-x)#**”画面で“?”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)FXC52xx# ?
  exit              Exit from current mode
  help              Show available commands
  history           Show a list of previously run commands
  logout            Disconnect
  quit              Quit commands
  action            Specify frames action
  destination-mac Specify destination mac address
  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)
  policy            Policy ACE keyword
  port              Port list
  port-redirect     port copy
  Rate Limiterspecify 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。

- exit :
  ACL 設定画面を終了します。

- help :
  設定可能なコマンドを表示します。

- history :
  入力したコマンドの履歴のリストを表示します。

- logout :
  コマンドラインの画面からログアウトします。

- quit :
  コマンドラインの画面を終了します。

- action :
  ACL ルールと一致するパケットを定義します。
  - action permit - ACE と一致するフレームは、ACE の動作を許可します。
  - action deny - ACE に一致するフレームを破棄します。
  -

- 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 -すべての宛先 MAC フィルタを指定します
  - destination-mac xx-xx-xx-xx-xx-xx -ACE 用の宛先 MAC フィルタを指定します
    (マスク指定(範囲指定)は不可です)。

- destination-mac-type:
  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-type any -宛先 MAC アドレスタイプをすべてに設定します。
  - destination-mac-type broadcast - 宛先 MAC アドレスタイプを「broadcast」に設定します。
  - destination-mac-type multicast - 宛先 MAC アドレスタイプを「multicast」に設定します。
  - destination-mac-type unicast - 宛先 MAC アドレスタイプを「unicast」に設定します。

- frame-type :
  フィルタマッチング用のパケットのフレームタイプを設定します。
  frame-type any :すべてのフレームに ACE を適用します。
  frame-type arp :ARP フレームのみ ACE を適用します。
  frame-type ethernet-type :
  イーサネットタイプ(0x600 - 0xFFF) で ACE を適用します。
  イーサネットタイプ 0x800(IPv4)、0x806(ARP)、0x86DD(IPv6)は

指定できません。
frame-type ipv4　: IPv4 フレームのみ ACE を適用します。

◆ logging :
ACE のログ機能を有効にします。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レートは制限されます。
◆ mirror :
ACE のミラーリングの動作を有効します。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。

◆ next_id “x” :
別の ACE 設定に移動します。
”x”:「1～256」までのインデックス値です。

◆ 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)#”のポート設定画面の下に定義されます。
・ policy “y” “0xXX” : 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。

◆ port “w” :
ACE が適用される入力ポートのリストを設定します。
“w”は、シングルポート(1/x)、またはポートのグループ(1/x,y,z, 1/x-y, 1/x-y,z)です。

◆ port-redirect :
ACE に一致するフレームは、以下に指定したポート番号に送信します。
・ port-redirect disable:この機能は無効となります。
・ port-redirect “w” :ポートのリダイレクト番号(送信先)が設定されます。
“w”は、シングルポート(1/x)、またはポートのグループ(1/x,y,z, 1/x-y, 1/x-y,z)です。

◆ rate-limiter :
ACE の帯域制御(レートリミット)を指定します。
・ rate-limiter disable:この機能は無効となります。
・ rate-limiter “x” :ACE の帯域制御(レートリミット)を指定します。
“x”: 帯域制御(レートリミット)の index です（1～16 までの値）.
◆ shutdown :
ポートの ACE の動作をシャットダウンします。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。

◆ source-mac :
フィルタマッチング用のレイヤ 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 アドレスを指定します。
（送信元 MAC アドレスをチェックしない)
・ source-mac “xx-xx-xx-xx-xx-xx” – ACE の送信元 MAC アドレスを指定します
マスク指定(範囲指定)は不可です。

◆ tagged :
フィルタマッチング用の 802.1Q タグの有無を指定します。
- 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

◆ tag_prio:
フィルタマッチング用の 802.1Q タグプライオリティ値を指定します。(COS 値)。
- **tag_prio any** : すべての値を指定します。(タグプライオリティ値をチェックしない。)
- **tag_prio "x"** : タグプライオリティ値を指定します。(COS 値(0~7))
  "x":タグのプライオリティです（設定可能な値は(0～7)）

◆ vid :
フィルタマッチング用の VLAN の ID のを指定します。
vid any : すべての値を指定します。(VLANID をチェックしない)
- **vid "x"** : VLAN の ID を指定します。
  "x":VLAN の ID です（設定可能な値は(1～4095)）。

10) aggregation command

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のポートを通ります。

■ **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。

■ **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。

■ **aggregation source_mac_address :**
ソース 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。

■ **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。

■ **no aggregation :**
デフォルト設定値に戻します。

11) arp-inspection command

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。

ARP インスペクショントランスレーションコマンドにより、ダイナミックエントリからスタティックエントリにすべて切り替え可能です。

【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 検査を有効にする前に、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、ARP インスペクション用にスタティック ARP エントリを作成してください。

■ **arp-inspection mode:**
ARP インスペクション機能を有効にします。”no”コマンドにより無効になります。

■ **arp-inspection translation :**
ダイナミックARPエントリからスタティックARPエントリに変換します。

12) default command

工場出荷設定時の値にリストア(初期化)します。

■ **default:**
すべての設定を工場出荷時の状態にリストア(初期化)します。

■ **default keep-ip :**
IPアドレスは保持し、それ以外を工場出荷時の状態にリストア(初期化)します。

13) dhcp-relay command

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/サーバ間の DHCP メッセージの送信を行います。
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。サーバが DHCP パケットを DHCP クライアントに送信時に、DHCP 応答パケットからの特定の情報を取り除きます。
DHCP サーバは、この情報を用いて、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、オプションは次の 2 つのサブオプションを設定することにより動作します。
回路 ID（オプション 1）およびリモート ID(オプション 2)

回路 ID のサブオプションには、リクエストを受けた回路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、回路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。
本機のオプション 82 の回路 ID の長さの設定は「4」バイトす。
回路 ID のフォーマットは、"[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」を表します。

3 バイト目は"module_id"（スタンドアロンスイッチは「0」）を表します。
4 バイト目は"port_no"のパラメータは、ポート番号を表します。
リモート ID は 6 バイト、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。

■ **dhcp-relay mode:**
DHCP リレー機能は有効になります。”no”コマンドにより無効になります。
ブロードキャスト DHCP メッセージを受信しても、本機からリレーメッセージは同一ネットワーク内にフラッディングされません。

■ **dhcp-relay information mode:**
DHCP のオプションの 82 のオペレーションを有効にします。”no”コマンドにより無効になります。
DHCP リレー情報モードの動作を有効にすると、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。

■ **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。”no”コマンドによりデフォルトに戻ります。
DHCP リレー情報のモードを有効にすると、エージェントがリレーエージェント情報を含む DHCP メッセージを受信した場合は、ポリシーを実行します。
リレー情報が無効な場合、’replace’オプションは無効となります。
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 パケットは破棄されます。
Keep ：リレー情報を含む DHCP メッセージを変更せずにそのまま転送します。
replace: リレー情報を含む DHCP メッセージを上書き/変更して転送します。

■ **dhcp-relay server “x.x.x.x” :**
DHCP サーバの IP アドレスを設定します。
“x.x.x.x”は、DHCP サーバの IP アドレスです。

■ **dhcp-relay statistics clear :**
DHCP リレーの統計情報をクリアします。

14) dhcp-snooping command

DHCP Snooping 機能を有効にします。
DHCP Snooping を使って、Untrusted(不信)ポートに接続された不正な DHCP サーバからの DHCP 応答メッセージをブロックします。
DHCP クライアント/サーバ間の変換を行う際に、不正な DHCP 応答メッセージ(Offer/ACK/NACK)を送信しようとした場合に、そのスイッチの Untrusted(不信)ポートで不正なDHCP応答メッセージをブロックします。
DHCP Snooping を有効にした後、インターフェース（(config-if)#”プロンプト）にて Trusted(信頼)ポートを設定し、正規の DHCP サーバを Trusted(信頼)ポートに接続します。
DHCP クライアントを Untrust(不信)ポートに接続してもDHCP要求メッセージはブロックされません。

■ **dhcp-snooping:**
DHCP Snooping 機能を有効にします。
”no”コマンドにより無効になります。

15) dot1x command

802.1x 認証機能のグローバル設定を行います。
“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             Set enabledness and parameters of Guest VLAN
  guest_vlan               Max EAP request/identity packet retransmissions
       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
-----------------------------------------------------------------
```

802.1x 機能の設定を行う場合は、config モードで、“dot1x”コマンドを使用します。
グローバル config モードで機能を有効にした後、インターフェース”(config-if)#”プロンプトにて、ポートの設定を行ってください。
グローバル config モードおよび、指定のポートの両方で設定を有効にすることで設定した特定ポートで動作します。

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

■ **dot1x agetime “x”:**
エージングタイムを設定に使用します。
“x”:「10～10000000 秒」の範囲内の値です。

ポートセキュリティ機能を使用して MAC アドレスを保護するモードに適用されます。
• Single 802.1X
• Multi 802.1X
• MAC-Based Auth

NAS（Network Access Server）モジュールがポートセキュリティ機能を使用してMACアドレスを保護する場合、ポートセキュリティ機能は、一定の間隔で問題のMACアドレスのアクティビティをチェックし、指定した時間内にアクティビティが見られない場合は、空きのリソースを必要があります。指定時間範囲は、「10～1000000秒」です。
再認証を有効、ポートが802.1X-basedモードの場合は、再認証時に、ポートに接続されていないサプリカントは削除されるため、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を超えた時のみです。
MAC-based 認証モードのポートは、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されているかどうかは検出されません。リソースを解放するには、エントリを経過させることです。

■ **dot1x eapoltimeout:**
このコマンドは、Request Identity EAPOL フレームの再送時間を決定します。
“x”:「1～65535 秒」の範囲なの値です。 MAC ベースポートに対しては無効です。

■ **dot1x guest_vlan:**
ゲスト VLAN 機能が有効になります。
”no”コマンドにより無効になります。

この機能を有効にした後、指定のポートの設定により、ポートはゲスト用VLANへの移行が可能かどうかを判別します
ポートの設定は、インターフェース“(config-if)#”にて設定します。
グローバルConfigモード及びポートの両方で設定を有効にすることで設定が有効になります。
ゲストVLANは特殊なVLANで制限付きのネットワークアクセスになります。
802.1X-unawareクライアントはネットワーク管理者により定義されたタイムアウト後に設定されます。このオプションは、以下のEAPOL-based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、本機は、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のポートを抽出し、ポート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"が無効の場合は、ポートはゲスト用VLANに戻ることはできません。

■ **dot1x guest_vlan allow_if_eapol_seen:**
EAPOL のゲスト VLAN を許可します。

■ **dot1x guest_vlan reauth_max:**
802.1X 認証の EAPOL パケット再認証回数<1-255>を設定します。

■ **dot1x guest_vlan vid “x”:**

ゲスト VLAN の VLAN ID を設定します。
“x”:「1～4095」の範囲内の値を持つ VALN ID です。

■ **dot1x holdtime “x”:**
802.1x 動作用の保持時間を設定します。
“x”:「10～10000000 秒」の範囲内の値です。
この設定は、MAC アドレスを取得するためにポートセキュリティ機能を使って、以下のモードに適用されます。
• 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は、
RADIUS サーバによりクライアントの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）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。
保持時間は現在実行中の認証についてはカウントしません。
MAC-based 認証モードでは、保持時間内にクライアントからの新規フレームは無視します。

■ **dot1x radius_qos:**
RADIUS サーバによる QoS クラスの割り当てが可能になります。
RADIUS に割り当てられた QoS は、認証されたサプリカントからのトラフィックがスイッチに割り当てられるトラフィッククラスを集中管理できるようになります。
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。

■ **dot1x radius_vlan:**
グローバル設定で RADIUS サーバにより割り当てられた VLAN 機能を有効にします。
この機能が有効な場合は、個々のポートの設定により、RADIUS サーバに登録された VLAN が有効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 はすべて無効になります。
RADIUS に割り当てられた VLAN は、認証されたサプリカントがスイッチ上に設定されている VLAN を集中管理できるようになります。受信トラフィックは割り当てられた VLAN にクラス分けされ、転送されます。
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。

■ **dot1x reauthentication:**
802.1x 機能の再認証機能が有効になります。
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 が有効なポートの再認証により、本機に新しいデバイスが接続されたか、または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-based 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、ポートのクライアントを確認することはできません。

■ **dot1x reauthperiod “x”:**
接続クライアントの再認証時間を秒単位で設定します。再認証機能が有効な場合のみ有効となります。
“x”:「1～3600」秒です。

16) interface command

インター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 インターフェース設定用)です。

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

ポート設定用コマンド設定、通信速度の設定など）はすべてインターフェース設定モードに含まれます。VLAN の機能（IP アドレスの割り当てなど）の設定は、インターフェース設定モードで設定されます。
例えば、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)#
-------------------------------------------------------------
```

複数のポートを設定を行うには、“interface ethernet 1/5,6,10-13”と入力すると、
ポート 5, 6, 10, 11, 12, 13 用のインターフェース設定画面を設定します。
インターフェース設定モードのコマンドの詳細については、「Interface Configuring Command」を参照してください。

17) ip command

このコマンドは、IP に依存される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
-------------------------------------------------------------
```

■ **ip default-gateway “x.x.x.x”:**
IPv4 デフォルト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 アドレスです。

■ **ip ipv6-default-gateway “<IPv6 address>”:**
IPv6 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 IPv6 アドレスです。

■ **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 アドレスです。

■ **ip dns-proxy:**
DNS Proxy 機能を有効にします。
”no”コマンドにより無効になります。
DNS Proxy を有効にすると、スイッチにより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に DNS リゾルバとして応答します。

■ **ip https command**
https サービスを設定します。
この機能を使うには、サブコマンドを入力します。
“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
-----------------------------------------------------------------
```

- ip https secure-server:
  http サービスの SSL 機能（HTTPS）を有効にします。
  ”no”コマンドにより無効になります。

- ip https automatic-redirect:
  HTTPS リダイレクトモードを有効にします。
  SSL機能(HTTPS)が有効の場合のみ有効になります。
  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”コマンドにより無効になります。

■ **IP igmp command:**
本機の IGMP 機能を設定します。

- ip igmp snooping :
  IGMP スヌーピング機能を有効にします。”no”コマンドにより無効になります。

“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  filtering
  proxy                 Set the mode of Proxy
  ssm-range             Enable IGMP query function
  unregflood            Enable  unregister flood function
  <cr>                  Enable Snooping
-------------------------------------------------------------
```

■ **ip igmp snooping vlan “x” command:**

VLAN の IGMP スヌーピング設定をします。

”x”:「1～4095」の範囲内の値を持つ VALN ID です。

この機能を使うには、サブコマンドを入力します。

“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
-------------------------------------------------------------
```

- ip igmp snooping vlan “x” add :

  新規の IGMP スヌーピングを動作させる VLAN を追加します。

  特定の IGMP スヌーピング VLAN は対応する VLAN 定義後に動作を開始します。

  - “x”:「1～4095」の範囲内の値を持つ VALN ID です。

- 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。デフォルトの値は「IGMP-Auto」です。

  - “x”:「1～4095」の範囲内の値を持つ VALN ID です。

- ip igmp snooping vlan “x” del :

  IGMP スヌーピングを動作させるVLANから削除します。

  - “x”:「1～4095」の範囲内の値を持つ VALN ID です。

◆ ip igmp snooping vlan “x” parameter-llqi “y” :
LLQI（LastListenerQueryInterval）は受信ポートをマルチキャストグループメンバーシップから削除する前に、ポートの IGMP レポートメンバーシップを待機する最大時間です。
・ “x”:「1～4095」の範囲内の値を持つ VALN ID です。
・ “y”:「0～31744」まで単位は 10 秒です。

◆ ip igmp snooping vlan “x” parameter-qi “y” :
IGMP の Query 間隔を設定します。
QI(Query Interval)は、クエリアにより送信されたジェネラルクエリの間隔です。
・ “x”:「1～4095」の範囲内の値を持つ VALN ID です。
・ “y”:「0 ～31744」の値で単位は 1 秒です。

◆ ip igmp snooping vlan “x” parameter-qri “y” :
IGMP の QRI(Query Response Interval)を設定します。QRI は、定期的に送信されるジェネラルクエリに対する応答までの最大時間を指定します。
・ “x”:「1～4095」の範囲内の値を持つ VALN ID です。
・ “y”:「0 ～31744」の値で単位は、0.1 秒です。

◆ ip igmp snooping vlan “x” parameter-rv “y” :
IGMP の RV（Robustness Variable）を設定します。RV は、ネットワーク上のパケットロスを考慮するためのパラメータであり、パケットロスの耐性を調整します。
・ “x”:「1～4095」の範囲内の値を持つ VALN ID です。
・ “y”:「1 ～255」の RV 値になります。

◆ ip igmp snooping vlan “x” parameter-uri “y” :
IGMP の URI（Unsolicited Report Interval）を設定します。URI は、ホストがグループメンバーシップの初期レポートを再送する間隔を指定するパラメータです。
・ “x”:「1～4095」の範囲内の値を持つ VALN ID です。
・ “y”:「0～31744」の値で単位は 1 秒です。

◆ ip igmp snooping vlan “x “ querier :
VLAN の IGMP snooping　クエリアを有効にします。
”no”コマンドにより無効になります。
・ “x”:「1～4095」の範囲内の値を持つ VALN ID です。

◆ ip igmp snooping vlan “x” state :
VLAN をスヌーピング状態に設定します。”no”コマンドにより無効になります。
・ “x”:「1～4095」の範囲内の値を持つ VALN ID です。

■ **ip igmp snooping leave-proxy :**
IGMP Leave Proxy が有効になります。
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。

■ **ip igmp snooping ssm-range “x”/“y” :**
SSM (Source-Specific Multicast)の範囲を設定します。SSM (Source-Specific Multicast)範囲により、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”:プレフィックスです。
- “y”: IGMP SSM のマスク範囲は「4～32」です。
  例えば、”x”/”y”は「232.0.0.0/8」です。

■ **ip igmp snooping unregflood :**
登録されていない IPMCv4 のトラフィックのフラッディングが可能になります。
IGMP Snooping が有効な場合はのみフラッディングの制御が行われます。
IGMP Snooping 自体が無効な場合は、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常に可能になります。

■ **ip mld command**
本機の MLD 機能を設定します。

- ip mld snooping :
  本機の MLD スヌーピング機能が有効になります。”no”コマンドにより無効になります。

“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  filtering
  proxy         Set the mode of Proxy
  ssm-range     Enable IGMP query function
  unregflood    Enable  unregister flood function
  <cr>          Enable Snooping
------------------------------------------------------------
```

- ip mld snooping vlan “x” add :
  MLD スヌーピングを動作させる VLAN を追加します。
  特定の MLD スヌーピング VLAN は対応する VLAN 定義後に動作を開始します。
  - “x”:「1～4095」の範囲内の値を持つ VALN ID です。

- ip mld snooping vlan “x” compatibility :
  MLD 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 MLD のバージョンに応じて、適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、「MLD-Auto」、「Forced MLDv1」、「Forced MLDv2」で、デフォルトの値は「MLD-Auto」です。
  - “x”:「1～4095」の範囲内の値を持つ VALN ID です。
- ip mld snooping vlan “x” del :
  MLD スヌーピングを動作させるVLANから削除します。
  - “x”:「1～4095」の範囲内の値を持つ VALN ID です。

◆ ip mld snooping vlan “x” parameter-llqi “y” :
IPMC Last Listener Query Interval を設定します。LLQI（Last Listener Query Interval）は、バージョン 1 の Multicast Listener Done メッセージに応じて送信される特定のマルチキャストアドレスに対するクエリ内で使用される最大応答遅延時間を指定します。この設定は、特定のマルチキャストアドレスおよびソースに関するクエリメッセージ内の Maximum Response Code を計算するための最大応答遅延時間としても使用されます。
- “x”:「1～4095」の範囲内の値を持つ VALN ID です。
- “y”:「0～31744」まで単位は 0.1 秒単位です。

◆ ip mld snooping vlan “x” parameter-qi “y” :
Query Interval を設定します。
QI(Query Interval)は、クエリアによるジェネラルクエリの送信間隔です。
- ”x”:「1～4095」の範囲内の値を持つ VALN ID です。。
- “y”:「0～31744」まで単位は 1 秒単位です。

◆ ip mld snooping vlan “x” parameter-qri “y” :
Query Response Interval を設定します。
QRI(Query Response Interval)を設定します。QRI は、定期的に送信されるジェネラルクエリに対する応答までの最大時間を指定します。
- “x”:「1～4095」の範囲内の値を持つ VALN ID です。
- “y”:「0～31744」まで単位は 0.1 秒単位です。

◆ ip mld snooping vlan “x” parameter-rv “y” :
RV(Robustness Variable)を設定します。
RV は、ネットワーク上のパケットロスを考慮するためのパラメータであり、パケットロスの耐性を調整します。
- “x”:「1～4095」の範囲内の値を持つ VALN ID です。
- ”y”:「1～255」の RV の値です。

◆ ip mld snooping vlan “x” parameter-uri “y” :
URI(Unsolicited Report Interval)を設定します。
URI は、ホストがグループメンバーシップの初期レポートを再送する間隔を指定する設定です。
- “x”:「1～4095」の範囲内の値を持つ VALN ID です。
- “y”:「0～31744」まで単位は.1 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”コマンドにより無効になります。
- “x”:「1～4095」の範囲内の値を持つ VALN 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。”no”コマンドにより無効になります。
- “x”:「1～4095」の範囲内の値を持つ VALN ID です。

■ **ip mld snooping leave-proxy :**
MLD Leave Proxy を有効にします”no”コマンドにより無効になります。
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”コマンドにより無効になります。
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。

■ **ip mld snooping ssm-range “x”/”y”:**
SM (Source-Specific Multicast)の範囲を設定します。
SSM (Source-Specific Multicast)範囲により、SSM-aware ホストおよびルータがアドレスの範囲内のグループの SSM サービスモデルを動作することが可能です。
“x”：IPv6 プレフィックスです。
”y”:「8～128」までの MLD SSM レンジを持つマスクです。
例えば、”x”/”y”は「ff3e::/96」となります。

■ **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。
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 スヌーピング機能が無効な場合は、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。
”no”コマンドにより無効になります。

18) ip ssh server command

SSH 機能を有効にします。

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。

■ **ip ssh server :**
SSH サーバ機能を有効にします。
”no”コマンドにより無効になります。

19) ip-source-guard command

I IP セキュリティ機能を設定します。IP Source Guard 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、不正な IP の攻撃から守ることができます。

ダイナミック IP ソースガードは、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する必要があります。
もしくは、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

■ **ip-source-guard mode:**
この機能をグローバル設定にて有効にします。
IP Source Guard は、インターフェース“(config-if)#”プロンプトの設定モードでポートの設定してください。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 Source Guard は有効となります。
”no”コマンドにより無効になります。

■ **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することができます。

20) lldp command

LLDP 機能をグルーバル設定にて設定します。
LLDP(Link Layer Discovery Protocol)は、IEEE 802.1ab の標準プロトコルです。この規格で指定されている LLDP により、同じネットワークに接続された他の機器や端末を検出し、識別します。

LLDP 機能はポート単位で有効/無効に設定します。送信された情報もポート単位で設定されます。
グローバル config モードで有効にした後、インターフェース“(config-if)#”プロンプトでポートの設定をしてください。両方を有効にすることで設定したポートで有効になります

“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
-------------------------------------------------------------
```

■ **lldp interval “x”:**
LDP フレームの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 Interval 値により決定されます。
“x”:「5～32768」まで単位は 1 秒です。

■ **lldp tx-hold “x”:**
隣接デバイスから受信した情報のLLDPフレームの受信失敗回数を指定します。
LLDP 情報の有効時間は、Tx Interval(送信間隔)×Tx Hold(失敗回数) です。
“x”:「2～10」まで単位は回です。

■ **lldp tx-hold “x”:**
隣接デバイスから受信した情報のLLDPフレームの受信失敗回数を指定します。
LLDP 情報の有効時間は、Tx Interval(送信間隔)×Tx Hold(失敗回数) です。
“x”: 「2～10 回」まで単位は回です。

■ **lldp tx-delay “x”:**
LLDP フレームの送信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。
“x”: 「1～8192」まで単位は 1 秒です。
Tx Delay:Tx Interval 値の 1/4 未満で指定してください。

■ **lldp reinit-delay “x”:**
LLDP 情報の初期化遅延時間を指定します。
ポートを無効にするか、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隣接デバイスに送信され、LLDP 情報のシグナル表示は無効となり、遅延時間経過後、初期化されます。
シャットダウンフレームと新規 LLDP の初期化の間の時間（秒単位）を制御します。
“x”:「1 ～10」まで単位は 1 秒です。

21) logging command

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

■ **logging log-level “x”:**
イベントのログレベルを定義します。
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。
“x”の有効な値は「0～2」です。

■ **logging remote-log command:**
リモートによるログ機能を設定します。
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>
---------------------------------------------------------------
```

◆ logging remote-log “x”
リモートによるログ機能が有効になります。イベントは syslog サーバに送信されます。
・ “x”:インデックス番号を指定します。
”no”コマンドにより無効になります。

◆ logging remote-log “x” host “y.y.y.y”:
syslog サーバの index “x”に IP アドレス(“y.y.y.y”)を設定します。
・ “x”:インデックス番号を指定します。
・ “y.y.y.y”: ログを送信する syslog サーバの IPv4 ホストアドレスです。
DNS 機能が有効な場合は、ホスト名で指定可能です。

◆ logging remote-log “x” host “y.y.y.y”:
syslog サーバの index “x”に IP アドレス(“y.y.y.y”)を設定します。

■ logging clear command
ログ情報をクリアします。

“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
---------------------------------------------------------------
```

◆ logging clear “x”:
レベル”x”のログ情報をクリアします。
・ ”x”:「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
1: Warning : 警告およびエラー
2: Error　　: エラー

◆ logging clear :
ログ情報をすべてクリアします。

22) loopback-detection command

グローバル設定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フレームが各ポートから送信されます。
この機能を実行するには、ループ保護 PDU が各ポートに送信されます。

各ポートには、インターフェース“(config-if)#”プロンプトで設定します。

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

```
-------------------------------------------------------------
(config)# 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
-------------------------------------------------------------
```

■ **loopback-detection mode :**
この機能をグローバル設定にて有効にします
”no”コマンドにより無効になります。

■ **loopback-detection shutdown “x” :**
ループ状態のポートをシャットダウンします。
ループ状態が検出された際ポートが無効な状態（ポートの動作がシャットダウンされている状態）の時間を秒単位で示します。
“x”: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、デバイスが再起動するまでポートが無効な状態を示します。

■ **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。
“x”:送信間隔を表し、有効な値は「1～10 秒」です。

23) mac-address-table command

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
  static          Sets MAC address table static information
-------------------------------------------------------------
```

■ **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):「10～1000000 秒」です。

■ **mac-address-table aging-time disable**
エージングは無効になります。

■ **mac-address-table static “x-x-x-x-x-x” vlan “y” interface ethernet “1/z”**
本機のMACアドレススタティックエントリ(静的割当)を設定します。
スタティックの MAC アドレス “x-x-x-x-x-x”を VLAN“y”のポート“1/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 テーブルには、64 エントリ設定可能です。

“x-x-x-x-x-x”：スタティックエントリするMACアドレス
“y”: <1-4094>の値です。所属する VLANID を指定します。
“1/z”：所属するポートを指定します。
単独ポートの場合は、“interface ethernet 1/5 と指定し、ポート 5 の設定となります。
複数ポート(範囲)の場合は、“interface ethernet 1/5,6,10-15”と指定し
　ポート 5, 6, 10, 11, 12, 13, 14, 15 の設定となります。

24) mac-security command

ポートセキュリティの Limit Control システムの設定を行うことができます。
この Limit Control 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。
Limit Control 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、以下の 4 つの処理が行われます。
・None :指定以上の MAC アドレスを許可しない。
・Trap：指定以上の MAC アドレスを許可せず、Trap を送信する。
・Shutdown：指定以上の MAC アドレスを許可せず、ポートをシャットダウンする。
・Trap&Shutdown：指定以上の MAC アドレスを許可せず Trap を送信しポートをシャットダウンする。
Limit Control モジュールは、ポートで学習した MAC アドレスを管理する低レイヤーモジュール、ポートセキュリティモジュールを対象としています。
ポートセキュリティの Limit Control 機能は、ポートごとに設定が必要です。
ポートには、インターフェース“(config-if)#”プロンプトで設定します。

■ mac-security aging “x”

ポートセキュリティの MAC アドレスのエージングタイムを設定します。
他のモジュールがセキュア MAC アドレスの基本的なポートセキュリティを使用する場合は、エージング時間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。
“x”: エージングタイムを表し、「10～10,000,000 秒」までの範囲内の値です。

■ mac-security mode

ポートセキュリティの Limit Control 機能を有効にします。
ポートセキュリティの Limit Control 機能はグローバル設定/ポート単位を共に有効にすることで動作します。
”no”コマンドにより無効になります。

25) management command

管理インター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持ちます（この機能は、最大 16 までの設定が可能です。

“management ?”と入力すると、次のサブコマンドが表示されます。

```
------------------------------------------------------------
(config)# management ?
  <1-16>                access id
  enable                Enable the management security function
(config)# management  1 ?
  ipaddr                Set IP and net mask for a specified set
  protocol              Set protocol for a specified set
------------------------------------------------------------
```

■ **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 http/https | snmp | telnet/ssh の接続が不可になります。
管理者用にプロトコルや IP アドレスやレンジで制限を設定してください。
”no”コマンドにより無効になります。

■ **management clear :**

アクセス管理の統計情報をクリアします。

■ **management “x” ipaddr “y.y.y.y” “z.z.z.z” :**

この規則の IP アドレスのレンジを設定します。
IP アドレス範囲内のユーザは管理ルールに準じ設定してください。
“x”：ルールの index
“y.y.y.y”:開始 IP アドレス
“z.z.z.z”:終了 IP アドレス

■ **management x protocol “y” :**

この規則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。
“x”：このルールの index です。
“y”: [http/https | snmp | telnet/ssh]

26) mirror command

ミラーリング機能を設定します。本機能はポートごとに設定が必要です。
ポートには、インターフェース“(config-if)#”プロンプトで設定します。

■ **mirror**

本機のミラーリング機能を有効にします。
”no”コマンドにより無効になります。

27) mvr command

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、Multicast VLAN 上で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各マルチキャスト 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最大 256 グループアドレスまで設定可能です。

・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。
・MVR VLAN へのソースポートおよび受信側のポートの割り当ては、
ポートごとに設定が必要です。ポートには、インターフェース“(config-if)#”プロンプトで設定します。

“mvr ?”と入力すると、次のサブコマンドが表示されます。

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

■ mvr enable

MVR 機能が有効になります。
”no”コマンドにより無効になります。

■ mvr “x” command

“mvr x ?”と入力すると、次のサブコマンドが表示されます。

- “x”:「1～4095」までの範囲内の VLAN ID です。

```
------------------------------------------------------------
(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
------------------------------------------------------------
```

■ **mvr “x” llqi “y”**
マルチキャストグループのメンバー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定義します。
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 です。 “y”:0.1 秒単位の「0～31744」までの範囲の値になります。
デフォルト設定の LLQI は「0.5 秒」です。

■ **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 のチャネル名です。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”コマンドにより無効になります。
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 239.0.0.1 end-address 239.0.0.2”と割当てます。

■ **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が有効になります。
Compatible モードでは、MVR メンバーシップレポートはソースポート上では禁止されます。
“x”:マルチキャスト VLAN ID です。

■ **mvr “x” name “yyy” :**
マルチキャスト VLAN の名前を設定します。
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。
“x”:マルチキャスト VLAN ID です
“yyy”: MVR の VLAN 名です。

■ **mvr “x” priority “y”:**
traversed IGMP/MLD 制御フレームが優先順に送信されます。
“x”:マルチキャスト VLAN ID です。
”y”: 「0～7」までの範囲のプライオリティの値です。

■ **mvr “x” status-clear:**
MVR の動作状況およびマルチキャスト VLAN の”x”をクリアにします。
”x”:マルチキャスト VLAN ID です。

■ **mvr “x” tagging [tagged | untagged]:**
トラバースされた IGMP/MLD 制御フレームを MVR VID のタグ付き/タグなしで送信するかどうかを指定します。
“x”:マルチキャスト VLAN ID です。

28) no command

機能を無効に設定するか、設定を初期設定値(工場出荷状態)にリストアします。

```
------------------------------------------------------------------
(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-security                 Configuration of mac security
  management                   Specifies management IP filter
  mirror                       Configuration of mirror
  mvr                          Multicast VLAN Registration
  ntp                          Simple Network Time Protocol configuration
  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:
  - “no mirror” コマンド:機能は無効になります。
  - “no ip default-gateway”:工場出荷時の設定値に戻します。

29) ntp command

本機の NTP 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 function
  dst-start-time        Set start time of Daylight Saving
  dst-end-time          Set end time of Daylight Saving
  dst-offset            Enter the number of minutes to add during Daylight Saving
-------------------------------------------------------------
```

■ ntp client
NTP プロトコルを有効にします。”no”コマンドにより無効になります。

■ **ntp server “x” “<IP address>” :**
NTP プロトコルのネットワークタイムサーバの IP アドレスを設定します。
タイムサーバは最大 5 つまでサポートしています。
”x”:タイムサーバの index(1～5)です。
“<IP address>” :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。

■ ntp zone x**:**
タイムゾーンオフセットを設定します。
”x”:システムのタイムゾーンオフセット(「-7200～7201 分」の範囲の値)です。
(日本の場合は、5400 分(+9 時間)で設定します。)

■ **ntp zone-acronym “xxx”:**
タイムゾーンの略称を設定します。
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
“xxx”:16 文字までの英数字および'-'、'_' あるいは '.'を使用可能です。
例えば日本標準時の場合、「Japan Standard Time」から「JST」と記載します。

■ **ntp dst [disable | non-recurring | recurring]**
サマータイム(Daylight Saving Time)機能モードを設定します。サマータイム機能は、定義されたサマータイムの設定に応じてクロック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:毎年設定したサマータイムを繰り返し行うよう設定します。

■ **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）

■ **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）

■ **ntp dst-offset “x”:**
サマータイムを分単位で設定します。
”x”:分（1～1440 までの値）

30) prompt command

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**:新しいプロンプトの文字列です。
”no”コマンドによりデフォルト設定値に戻します。

31) qos command

システムのQoS機能を設定します。
Port-based QoS設定は、ポートごとに設定が必要です。
ポートには、インターフェース“(config-if)#”プロンプトで設定します。

“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。

■ qos dscp command

“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
------------------------------------------------------------
```

- qos dscp classification-map “x” “y” “z”
  QoS クラスおよび Drop Precedence Level をインターナル DSCP 値にマッピングします。
  “x”:QoS クラス（0～7 の範囲の値）です。
  “y”:Drop Precedence Level（0～1 の範囲の値）です。
  “z”:dscp（0～63 までの値）です。
  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 をインターナル DSCP にマッピングします。ここで設定された DSCP 値は egress map により、送信フレームの DSCP 値に影響し、Egress Rewrite が有効な場合、DSCP 値は書き換わります。
  Egress Rewrite が有効の場合は、出力 DSCP の値を上書きします。

- qos dscp classification-mode “x”:
  クラシフィケーションモードの入力 DSCP 値を設定します。
  “”no”コマンドによりデフォルト設定値に戻します。
  “x”:dscp の値は「0～63」です。
  ポートの Ingress Classify の設定が「selected」の場合は DSCP の値を選択して、インターナル DSCP に対する QoS Class を有効にします。

- **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）です。
  “y”:「0」または「1」の DPL(Drop Precedence Level:破棄優先度) です。
  “z”:DPL 用の出力リマップ dhcp の値 (0～63)です。
  このコマンドにより、DPL(破棄優先度)「0」または「1」の出力 DSCP 値のマッピングにインターナル 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。

- qos dscp map “x” “y” “z”:
  DSCP ベース QoS 出力クラスを設定します。
  “x”:dscp の値（0～63）です。
  ”y”:QoS クラス(0～7)です。
  ”z”:Drop Precedence Level(0～1）です。

このコマンドにより、基本 DSCP ベースの QoS 入力クラスを設定します。
DSCP 値が有効な場合に設定が反映されます。

◆ qos dscp translation “x” “y” :
グローバル設定で、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)です。
”y”:変換後の DSCP 値(0～63)です。
入力側の DSCP は、QoS クラスおよび DPL マッピングの DSCP を使用する前に、まず新しい DSCP に変換されます。

◆ qos dscp trust “x”:
特定の DSCP 値が正しいかどうかを設定します。
“x”:dscp 値「0～63」です。
受信フレームの DSCP 値を信頼する場合のみ特定の QoS クラスおよび DPL にマッピングされます。受信フレームの DSCP 値を信頼しない場合は、IP以外のフレームとして処理されます。

■ qos qcl command

QCL(QoS Control List)を設定します。

QCL 設定は、ポートごとに設定が必要です。
ポートには、インターフェース“(config-if)#”プロンプトで設定します。

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。
“x”:QCE(1～256)の index になります。
たとえば、“qos qcl 10”と入力すると以下の画面を表示します。

```
-------------------------------------------------------------
(config)# qos qcl 10
(config-QCE-10)# ?
  exit                  Exit 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
-------------------------------------------------------------
```

exit command
　　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。

help command
　　設定モードで有効なコマンドを表示します。

history command
　　入力したコマンドの履歴を表示します。

logout command
　　コンソール画面からログアウトします。

quit command
　　コンソール画面を終了(ログアウトと同じ機能)します。

action command
　　QCE と一致する場合は、フレームの QoS の動作を定義します。

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

- action class “x”
  QoS クラスの動作を定義します。
  ”x”:QoS クラス(0～7)です。

- action dpl “x”
  Drop Precedence レベルの動作を定義します。
  “x”:Drop Precedence レベル(0～1)です。
- action dscp “x”
  DSCP 値の動作を定義します。
  ”x”:DSCP 値(0～63)です。

ethernet command
　　QCL エントリにポートを割り当てます。
　　単独ポートの場合は、“ethernet 1/5”と指定し、ポート 5 の設定となります。
　　複数ポート(範囲)の場合は、“ethernet 1/5,6,10-15”と指定し、ポート 5, 6, 10, 11, 12, 13, 14, 15 の設定となります。

key command
　　QCL エントリのキーパラメータを定義します。キーパラメータは、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

◆ key dmac-type [any | bc | mc | uc]
宛先 MAC アドレスのタイプによってキーパラメータを定義します。
値は、以下の任意の値から設定可能です。
・any(全て)
・bc(ブロードキャスト)
・mc(マルチキャスト)
・uc(ユニキャスト)

◆ key frame-type [any | ethernet | ipv4 | ipv6 | llc | snap]
タイプごとにキーパラメータを定義します。
値は、以下の任意の値から設定可能です。
・any
・Ethernet Type (any / specific type<0xXXXX>)
・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)

◆ key smac [any | xx-xx-xx]
送信元 MAC アドレスごとにキーパラメータを定義します。
任意の値、または送信元 MAC アドレスの OUI に設定可能です。

◆ key tag [any | tag | untag]
フレームのタグ情報ごとにキーパラメータを定義します
・any
・tag (DEI, PCP, VID)
・untag：タグ無）
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。

next_id command
QCL テーブルの QCL エントリの順番を設定します。

◆ next_id “x”
QCL エントリ”x”の後に QCL エントリを設定します。
”x”:QCL エントリの ID（1～256）です。

◆ 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。

32) radius-accounting-server command

RADIUS Accounting サーバを設定します。
RADIUS Accounting サーバを 5 つまでサポートします。
コマンドの詳細については、以下のとおりです。

■ **radius-accounting-server “x” active:**
RADIUS Accounting サーバを有効にします。
”x”:、サーバの index 番号「1～5」です。

■ **radius-accounting-server “x” host “y.y.y.y”**
RADIUS Accounting サーバ “x”の IP アドレスを指定します。
”x”:、サーバの index 番号「1～5」です。
“y.y.y.y”: RADIUSAccountingサーバの IP アドレスです。

■ **radius-accounting-server “x” key “yyy”**
本機に RADIUS Accounting サーバのシークレットキーを設定します。
”x”:サーバの index 番号「1～5」です。
“yyy”: シークレットキー（最大 30 文字）です。
(※RADIUS Accounting サーバと本機の間で共有される秘密キー。)

■ **radius-accounting-server “x” port “y”**
RADIUS Accounting サーバで使用する UDP ポートを割り当てます。
”x”: サーバの index 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 (1813)が設定されます。

■ **radius-accounting-server dead-time “x”**
RADIUS Accounting サーバのデッドタイムを指定します。
”x” : (0～3600) 秒の値です。
デッドタイムは、リクエストへの応答に失敗したサーバへの新しいリクエストの送信を中断する間の時間です。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し、複数のサーバが設定されている場合のみ、この機能が有効になります。

■ **radius-accounting-server timeout “x”**
タイムアウトはサーバからの応答の最大待機時間です。
サーバがタイムフレーム内に応答しない場合は、次の有効なサーバに通信を行います。
“x” : タイムアウトの値（3～3600）秒の値です。

* 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。部分区間内に応答が受信されない場合は、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 command

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。
コマンドの詳細は、以下とおりです。

■ **radius-authentication-server “x” active**
RADIUS 認証サーバ “x”を有効にします。
“x”: サーバの index 番号「1～5」です。

■ **radius-authentication-server “x” host “y.y.y.y”**
RADIUS 認証サーバ の IP アドレスを指定します。
“x”: サーバの index 番号「1～5」です。
“y.y.y.y”: RADIUS 認証サーバ の IP アドレスです。

■ **radius-authentication-server “x” key “yyy”**
本機に RADIUS 認証サーバ のシークレットキーを設定します。
“x”: サーバの index 番号「1～5」です。
“yyy”: シークレットキー（最大 30 文字）です
（RADIUS 認証サーバおよび本機間で共有される秘密キー）。

■ **radius-authentication-server “x” port “y”**
RADIUS 認証サーバに UDP ポート番号を割り当てます。
“x”: サーバの index 番号「1～5」です。
”y”:UDP ポート番号(0～65535)です。
ポートが「0」の場合は、デフォルトのポート(1812)を使用します。

■ **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）秒の範囲内の値です。
デッドタイムは、リクエストへの応答に失敗したサーバへの新しいリクエストの送信を中断する間の時間です。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し、複数のサーバが設定されている場合のみ、この機能が有効になります。

■ **radius-authentication-server timeout “x”**
タイムアウトはサーバからの応答の最大待機時間です。
サーバがタイムフレーム内に応答しない場合は、有効なサーバに通信を行います。
“x”：タイムアウトの値（3～3600）秒の値です。

34) rmon command

本機の RMON 機能を設定します。
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)。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
------------------------------------------------------------
```

■ rmon alarm command

“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。

- “x”:エントリの index で、設定可能な範囲の値は「1～ 65535」です。

例えば、“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
------------------------------------------------------------
```

◆ rmon alarm “x” falling-index “y”
下限アラームのイベント index を設定します。

- “x”:「1～65535」のエントリの index になります。
- “y”: 下限アラームのイベント index (1-65535)です。

◆ rmon alarm “x” falling-threshold “y”
アラームの下限閾値を設定します。

- “x”:「1～65535」のエントリの index になります。
- “y”:下限閾値(-2147483648-2147483647)です。

◆ rmon alarm “x” interval “y”
サンプリング間隔を設定します。。

- “x”:「1～65535」のエントリの index になります。
- ”y”:間隔（1～2147483647）です。

◆ rmon alarm “x” rising-index “y”
上限アラームのイベント index を設定します。

・ “x”:「1～65535」のエントリの index になります。
・ “y”: 上昇アラームのイベント index (1-65535)です。

◆ rmon alarm “x” rising-threshold “y”
アラームの上限閾値を設定します。
・ “x”:「1～65535」のエントリの index になります。
・ “y”:上限閾値(-2147483648-2147483647)です。

◆ rmon alarm x sample-type [absolute | delta]
選択したデータのサンプリングとの算出、閾値と比較した表示方法を選択します。
・ “x”:「1～65535」のエントリの index になります。
サンプルのタイプは以下のとおりです。
- absolute : サンプリングデータを直接入手します。
- delta : サンプリングデータ間の差異を算出します。

◆ rmon alarm x startup-alarm [falling | rising | risingorfalling]
閾値と比較して、選択した変数のサンプリングと値の算出方法を選択します。
・ ”x”:「1～65535」のエントリの index になります。
サンプルのタイプは以下のとおりです。
- falling : 下限閾値 に満たない場合は、アラームを出します。
- rising : 上限閾値を超えた場合は、アラームを出します。
- rising or falling : 下限閾値 に満たない場合、または上限閾値を超えた場合はアラームを出します。

◆ 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」のエントリの index になります。
・ “y”:「10～21」
・ ”z”:「1～65535」

■ rmon event command

“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。
・ “x”:エントリの index です。設定可能な範囲の値は「 1～ 65535」です。
“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
---------------------------------------------------------------
```

◆ 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 秒」の範囲内のエントリの index になります。
・ “yyy”: コミュニティストリング（0～127）です。

◆ 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 秒」の範囲内のエントリの index を示します。
- “yyy”: 「0～127」の範囲内の値です。

◆ rmon event “x” type [log | log-trap | none | trap]
イベントの通知を行います。
- “x”:「1～65535 秒」の範囲内のエントリの index になります。

設定可能な通知は以下のとおりです。
- log : 上位層プロトコルに送信されたユニキャストパケット
- log-trap : パケットの送信が正常な場合でも、破棄されたインバウンドパケットの数
- none　: 受信したオクテットの総数（framing characters を含む）
- trap　: 上位層プロトコルに送信されたブロードキャスト/マルチキャストパケット数

■ rmon history command

“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。
- “x”:エントリの index です。設定可能な範囲の値は「1～ 65535」です。

例えば、“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_source Indicates the port ID which wants to be monitored interval Indicates the interval in seconds for sampling the history statistics data
----------------------------------------------------------------
```

◆ rmon history “x” buckets “y”
RMON にストアされている制御履歴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」のエントリの index になります。
- “y”:RMON にストアされている 制御履歴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。設定可能な範囲の値は「1～ 3600」です。

◆ rmon history “x” data_source .1.3.6.2.2.2.2.2.1.1.y
コマンド:モニタを行うポート ID を表示します。
- “x”:「1～65535」のエントリの index になります。
- “y”：モニタリングを行うポート ID です。

◆ 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」秒の範囲内のエントリの index 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。

■ **rmon statistics command**

“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。

- “x”:エントリの index です。設定可能な範囲の値は「1～65535」です

例えば、“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.1.3.6.2.2.2.2.2.1.1.”y”

モニタリング行うポート ID を表示します。

- “x”:「1～65535 秒」の範囲内のエントリの index になります。
- “y”:モニタリングを行うポート ID です。

35) s-flow command

スイッチの 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 データグラムとして送信されます。
このセントラルサーバは、”sFlowr レシーバ”、または”sFlow コレクタ”と呼ばれ、本機の sFlow 機能の設定を行います。
sFlow 機能は、ポート単位で有効となります。
各ポートには、インターフェース“(config-if)#”プロンプトで設定します。

“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 for list of receiver ID
 release       Release
 time_out      Set the Receiver Time_out for list of receiver ID
-----------------------------------------------------------------
```

■ **sflow receiver datagramsize “x”**

レシーバ ID のリストにレシーバのデータ長を設定します。
”x”：1つのサンプルデータグラムに送信可能なデータの最大バイト数です。
sFlow データグラム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「200～1468」バイト、デフォルト設定値は 1400 バイトです。

■ **sflow receiver ip “<ip address>” “x”**

レシーバ ID のリストに sFlow レシーバ IP および UDP ポートを設定します。
“<ip address>”:sFlow receiver 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。
”x”：sFlow receiver が sFlow データグラムを受信する 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。

■ **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 インターフェースを用いたローカル管理
・SNMP を用いたリモート管理
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>です。
・sFlow を Web、または CLI で設定を行う場合、
　オーナーは<Configured through local management>です。
・sFlow は、SNMP を介して設定を行う場合、オーナーは sFlow レシーバを指す文字列です。不正アクセスによる設定を避けるため、すべての制御は無効になります。

■ **sflow receiver time_out “x”**

receiver ID のリストに Receiver タイムアウトを設定します。
“x”：サンプリングを行う残りの秒数です。
設定可能な範囲の値は「0～2147483647」秒です。
タイムアウトすると sFlow オーナーがリリースされます。
0 秒で設定した場合は、常に sFlow オーナーをリリースした状態になり sFlow データグラムは送信されません。

36) snmp-server command

本機の SNMP 機能設定用に用います。

“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
-------------------------------------------------------------
```

“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が表示されます。

```
-------------------------------------------------------------
(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
-------------------------------------------------------------
```

■ snmp-server “x” authentication-failure

SNMP エンティティは認証失敗トラップの生成を許可します。

- “x”:トラップ「1～1」の index です。

■ snmp-server “x” community “yyy”

SNMP トラップパケット送信時に、コミュニティ名を設定します。

- ”x”:トラップ「1～1」の index です。
- “yyy”:「0 ～ 255」文字のコミュニティ名です。
  ASCII 文字の場合は、「33 ～ 126」文字です。

■ snmp-server “x” enable

SNMP トラップを有効にします。

- ”x”:トラップ「1～1」の index です。

■ snmp-server “x” host “y.y.y.y”

SNMP トラップ の IPv4 の宛先アドレスを設定します。

- “x”:トラップ「1～1」の index です。
- “y.y.y.y”: IPv4SNMPサーバアドレスです。

■ **snmp-server “x” host-ipv6 “<IPv6 address>”**

SNMP トラップ IPv6 の 宛先アドレスを設定します。

- “x”:トラップ「1～1」の index です。
- “<IPv6 address>”:IPv6SNMP サーバアドレスです。

■ **snmp-server “x” link-up-down**

SNMP トラップの link-up/ link-down をトラップ送信を許可します。
“x”:トラップ「1～1」の index です。

■ **snmp-server “x” version [v1 | v2c | v3]**

SNMP トラップのバージョンを選択します。
”x”:トラップ「1～1」の index です。
SNMP トラップのバージョンは、SNMP V1(v1)、SNMP V2c(v2c)および SNMP V3(v3)です。

■ **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”:コミュニティ名です。

■ **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”:コミュニティ名です。

■ **snmp-server contact “xxx”**

コンタクト情報(担当者情報)を設定します。
“xxx”:担当者情報です。

■ **snmp-server enable**

SNMP 機能を有効にします。

■ **snmp-server location “xxx”**

本機の設置場所情報を設定します。
“xxx”:設置場所情報です。

■ **snmp-server version [v1 | v2c | v3]**

SNMP のバージョンを選択します。
SNMP バージョンは、SNMP V1(v1)、SNMP V2c(v2c)および SNMP V3(v3)です。

■ **snmp-server snmpv3-“xxx” command**

SNMP v3 設定用のコマンドは、以下のとおりです。
“xxx”は、各コマンドが入ります。

■ **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です。
設定可能な文字列の値は「1～ 32」です。ASCII 文字の場合は「33～126」です。
“yyy”:現行の値のリクエストを行う MIB オブジェクトを定義する MIB VIEW の名前です。
設定可能な文字列の値は「1～ 32」です。ASCII 文字の場合は「33 ～126」です。
“zzz”:新しい値が設定可能なリクエストの MIB オブジェクトを定義する 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」です。

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

■ **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。
“xxx”:SNMPv3 エージェントへのアクセス可能なコミュニティアクセス名です。
設定可能な文字列の値は「1～32」、ASCII 文字の場合は「33 ～126」です。
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 アクセス送信元アドレスです。
“z.z.z.z”:SNMP アクセス送信元アドレスマスクです。

■ **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。
“xxx: エントリが所属するセキュリティ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。
“yyy”:エントリが所属するグループ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。

■ **snmp-server snmpv3-user “xxx” “yyy”**
“認証なし/暗号化なし”セキュリティ SNMPv3 ユーザを設定します。
“xxx”:SNMPV3 Engine ID です。
“yyy”: エントリが所属するユーザ名識別用の文字列。

■ **snmp-server snmpv3-user “xxx” “yyy” auth [md5 | sha] “zzz”**
“認証あり/暗号化なし”セキュリティレベルの SNMPv3 ユーザを設定します。
“xxx:SNMPV3 Engine ID です。
“yyy”: このエントリが所属するユーザ名識別用の文字列です。
“zzz:認証パスワード識別用の文字列です。

■ **snmp-server snmpv3-user “xxx” “yyy” auth-priv [md5 | sha] “zzz” des “www”**
“認証あり/暗号化あり”セキュリティレベルの SNMPv3 ユーザを設定します。
“xxx”:SNMPV3 Engine ID です。
“yyy”: このエントリが所属するユーザ名識別用の文字列です。
“zzz”:認証パスワード識別用の文字列です。
“www”:プライバシーパスワード識別用の文字列です。

- SNMPV3 Engine ID

エントリが所属する engine ID 識別用の 8 桁の文字列。文字列には、10～64 までの偶数（16 進数）を含む必要がありますが、「全て 0」および「全てF」は許可されません。
SNMPv3 の構造はメッセージセキュリティ用の User-based Security Model (USM)、アクセス制御用の View-based Access Control Model (VACM)です。
USM エントリについては、usmUserEngineID および usmUserName はエントリキーです。シンプルエージェントの場合は、usmUserEngineID 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 snmpEngineID 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。

- User Name(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。

- Authentication Password (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。

- Privacy Password(暗号化パスワード)
  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。

■ **snmp-server snmpv3-view view-name “xxx” view-type “[excluded | included]” oid-subtree “yyy”.**

SNMPv3 ビューエントリを設定します。
“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」です。
“yyy”:ビューを追加するためのサブツリーのルートを定義する OID です。設定可能な OID の長さは、「1～ 128」です。
有効な文字列はデジタル番号、またはアスタリスク(*)です。

37) spanning-tree command

本機のスパニングツリプロトコルを設定します。

スパニングツリーは、ポートごとにも設定が必要です。
ポートには、インターフェース“(config-if)#”プロンプトで設定します。
ここでの設定は、ブリッジのみです。
“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>
        max-age   Global 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
 ------------------------------------------------------------
```

■ **spanning-tree bpdufilter**

BPDU フィルタ機能を有効にします。
ポートが Edge として設定されている場合は、BPDU の送信しなくなります。
AutoEdge の場合は、Edge と確定するまで BPDU の送信を行います。

■ **spanning-tree bpduguard**

BPDU ガード機能を有効にします。
ポートが Edge として設定し、BPDU を受信した場合、ポートは「error-disabled」の状態となります。

■ **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。
設定名は、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。

■ **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。
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。
“x”:は、「4～30」秒です。

■ **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 送信間隔を秒単位で設定します。
“x”は、「1～10 秒」の値で、(HelloTime+1)*2 <= MaxAge となります。

■ **spanning-tree max-age “x”**
STA の最大エージを設定します。ルートブリッジの場合、ブリッジにより送信された情報の最大エージです。
“x”:最大エージタイムは「6～40」秒で、MaxAge は<= (FwdDelay-1)*2 に設定します。

■ **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定義します。
ルートブリッジが BPDU 情報を伝送するブリッジ数を定義します。
”x”:最大ホップ数は、「6～40」hops です。

■ **spanning-tree mode [mstp | rstp | stp]**
スパニングツリーの動作モード（MSTP、RSTP あるいは STP）を選択します。
142. 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(1～4094)です。
VLAN は MSTI にのみマッピング可能です。
未使用の MSTI は、VLANs マッピングされていません。

■ **spanning-tree msti priority “x” “y”**
MSTI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）です。
※有効な値は、4096 の倍数(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、Bridge Identifier を設定します。

■ **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。
“x”:スパニングツリーのプライオリティの値（0～61440）※4096 の倍数、例えば、”x”: 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(Instans 0)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 インスタンス番号を 6 バイトの MAC アドレスで連結し、Bridge Identifier を設定します。

■ **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。
“x”:タイムアウトの値です。
有効な値は「30～86400」秒 (24 hours)。

■ **spanning-tree transmit-hop-count “x”**

STP 送信ホールド回数のパラメータを設定します。
ブリッジポートが秒単位で送信可能な BPDU の数です。
これを超えると、次の BPDU の送信に遅延が生じます。
”x”の値は、「1～10」（毎秒ごとにBPDUの送信数）です。

38) storm-control command

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量(PPS：パケット/秒)を算出します。
フラッディングされたフレームに適用されます（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)）。

■ **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。
“x”: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, 2048k, ..., 32768k.

■ **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。
“x”: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, 2048k, ..., 32768k.

■ **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。
“x”: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, 2048k, ..., 32768k.

39) tacacs-authentication-server command

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、以下を参照ください。

■ **tacacs-authentication-server “x” active**
TACACS+認証サーバ”x”を有効にします。
“x”:サーバの index 番号「1～5」です。

■ **tacacs-authentication-server “x” host “y.y.y.y”**
TACACS+認証サーバの IP アドレスを指定します。
”x”:サーバの index 番号「1～5」です。
“y.y.y.y”: IP アドレスです。

■ **tacacs-authentication-server “x” key “yyy”**
TACACS+ 認証サーバ “x”の秘密キー“yyy”を指定します。
“x”: サーバの index 番号「1～5」です。
“yyy”: シークレットキー（最大 30 文字）-
TACACS+ 認証サーバおよび本機間で共有する秘密キーです。

■ **tacacs-authentication-server “x” port “y”**
TACACS+ 認証サーバで使用する TCP ポートを割り当てます。
“x”: サーバの index 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 (ゼロ)」に設定されると、デフォルトのポート (49)が設定されます。

■ **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。
“x”：デッドタイム（0～3600）秒の範囲内の値です。デッドタイムは、前回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を中断する間の時間です。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し、複数のサーバが設定されている場合のみこの機能が有効になります。

■ **tacacs-authentication-server timeout “x”**
タイムアウトはサーバからの応答の最大待機時間です。
“x”：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。
サーバが最大待機時間内に応答しない場合は、次の有効なサーバへの通信を行います。

40) username command

ユーザおよびユーザ名の割り当て、パスワード、レベルの設定を行います。

■ username “xxx” “yyy” “z”

ユーザおよびユーザ名の割り当て、パスワード、レベルの設定を行います。

- “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、有効なユーザ名は、文字、数字、_(アンダースコア)の組み合わせを使用します。
- “yyy”: パスワードです。設定可能な文字列の値は「0～31」です。
- “z”:privilege_level 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 つのレベルのプライオリティです。
管理者レベル(3)の場合は、本機のすべての設定/管理を行うことが可能です。
オペレータレベル(2)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を行うことが可能です。
ゲストレベル(1)では、本機のステータス、設定の表示のみ可能で、管理/設定を行うことが出来ません。

41) vlan command

VLAN の設定を行います。

■ vlan database

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 モード及びインターフェース Config モードで行います。
詳細については、「VLAN Config コマンド」を参照してください。

42) voice-vlan command

Voice VLAN 機能を設定します。Voice 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
------------------------------------------------------------
```

■ **voice-vlan**
Voice VLAN 機能を有効にします。“no”コマンドでこの機能は無効となります。

■ **voice-vlan agetime “x”**
Voice VLAN secure learning のエージングタイムを設定します。
“x”：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。

■ **voice-vlan oui add “xx-xx-xx”**
記述なしの OUI エントリを追加します。
“xx-xx-xx”: OUI アドレスです。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。

■ **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”: 電話通信用の OUI アドレスです。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 アドレスです。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。

■ **voice-vlan oui clear**
OUI テーブルをクリアします。
OUI エントリはすべて削除されます。

■ **voice-vlan oui delete “xx-xx-xx”**
OUI エントリを削除します。
“xx-xx-xx”: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" (“x”:16 進数)です。

■ **voice-vlan traffic-class “x”**
Voice VLAN トラフィックのクラスを設定します。
Voice 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。
“x”:traffic-class の値(0～7)です。

■ **voice-vlan vlan-id “x”**
Voice VLAN の VLAN ID を設定します。
“x”:VLAN ID(1～4095)です。

1.2.3 Interface Configureコマンド

基本設定モード“(config)#”プロンプトからインターフェースモードに入ります。

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

■ **interface ethernet 1/”x”**
Port x のインターフェースモードに入ります。
“(config)#”から“(config-if)#” プロンプトに移行します。
“x”は、ポート番号です。

■ **interface vlan “x”**
VLAN インターフェースモードに入ります。
“(config)#”から“(config-if)#” プロンプトに移行します。
“x”:VLAN ID です。

VLAN インターフェースモードに前に、
まず VLAN の作成を“vlan database”コマンドにて行います。
詳細については、「VLAN Configuring Commands」を参照してください。

例えば、VLAN インターフェースへの IP アドレスの割り当ては、このコマンドで設定してください。

```
------------------------------------------------------------
(config)# interface vlan 1
(config-if)# ip address 192.168.11.198 255.255.255.0
------------------------------------------------------------
```

1.2.3.1 ポートの Interface Configure コマンド

Configureモードは、“(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、configureモードで“**interface ethernet 1/x**” コマンドを使用して設定を行います。

ポートの選択には、以下の書式を使用します。

■ **単独ポート指定**
interface ethernet 1/”x”
“x”:ポート番号です。
コマンド以降の設定はすべてこのポートに適用されます。
例えば、“interface ethernet 1/5”の場合は、Port 5 の設定を行います。

■ **複数ポート個別指定**
interface ethernet 1/”x”,”y”,”z”,...
“x”, “y”, “z",…はポート番号です。
このコマンド以降の設定はすべてポートに適用されます。
例えば、“interface ethernet 1/2,4,7” の場合は、Port 2, Port 4 および Port 7 に適用されます。

■ **複数ポート範囲指定**
interface ethernet 1/”x”-“y”
“x”および”y”: ポート番号です。
このコマンド以降の設定はすべて x～y の範囲内のポートすべてに適用されます。
例えば、“interface ethernet 1/4-7”の場合は、Port 4, Port 5, Port 6, Port 7 (Port 4～7)に適用されます。

“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)#
----------------------------------------------------------------
```

“?”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)FXC52xx# ?
  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
  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
port                    Configures the characteristics of the port
port-vlan               Configures Port-Based VLAN
power-control           Decrease energy consumption
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 command

現在のオペレーションモードを終了します。前のモードに戻ります。

2) help command

このコマンドで使用可能なコマンドをすべて表示します。

3) history command

入力したコマンドの履歴を表示します。

4) logout command

コンソール画面からログアウト時に使用します。

5) quit command

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) end command

現在設定しているモードを終了します。

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

7) acl command

インターフェースポートの 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。

“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 Limiterselect which rate limiter to apply on this port
  shutdown        Shut down operation of this port
------------------------------------------------------------
```

■ **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。

■ **acl logging**
システム Log にストアされているポート上でのフレームの受信を有効にします。
他のシステム Log を使用している場合とメモリサイズおよびログレートが制限されます。

■ **acl mirror**
ミラーリングを行うポートでのフレームの受信を有効にします。

■ **acl policy “x”**
ACL の Policy x グループに設定します。
“x”：Policy ID(0～255)です。

■ **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。
リダイレクトするポートは、“1/x”もしくは、“1/x 1/x,y,z 1/x-y 1/x-y,z”で指定します。
アクションが許可されている場合は、設定できません。

■ **acl rate-limiter [disable | x]**
ポートのレートリミット機能を設定します。
“x”：レートリミット ID(1～16)です。

■ **acl shutdown**
ポートのシャットダウン機能を有効にします。

マッチしたフレームを受信すると、ポートは無効になります。

■ **acl state**
指定したポートのポート状態を指定します。
指定したポートを有効にします。
無効にする場合は、no acl state コマンドを使用します。

8) ARP Inspection command

ポートの ARP インスペクション機能を設定します。

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、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。

“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
-------------------------------------------------------------
```

■ **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。
”x”：VLAN ID (1～4095)です。
“yy-yy-yy-yy-yy-yy”: 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 Source IP アドレスです。

■ **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”コマンドにより無効となります。

9) channel-group command

インターフェースポートをスタティックアアグリゲーショングループに設定します。全二重設定のポートはアグリゲーションの設定を行い、ポートの通信速度を各グループ内で同じ速度にしてください。
no channel-group は、アグリゲーショングループからポートを削除します。

■ **channel-group “x”**
アグリゲーショングループ“x”にポートを追加します。
“x”: アグリゲーショングループ番号です。設定可能な範囲の値は「1～5」です。
アグリゲーションポート数は 2～10 ポートまでです。

10) dhcp-snooping command

ポートの DHCP スヌーピング機能を設定します。
DHCP オペレーションに対して、ポートを trusted、あるいは untrusted します。

■ **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。

■ **dhcp-snooping statistics clear**
DHCP Snooping のポートの統計情報をクリアします。

11) dot1x command

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

■ **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。

■ **dot1x authenticate now**
ポートのクライアントの再初期化により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、認証がグローバル設定されている場合、かつポートの Admin State が EAPOL-based、または MAC-based モードの場合のみ有効です。

■ **dot1x clear**
ポートの 802.1X 統計情報をクリアします。

■ **dot1x guest_vlan**
ポートのゲスト用 VLAN 機能を有効にします。
ゲスト用 VLAN 機能は、ゲスト用 VLAN がグローバル設定、かつ指定ポートで有効な場合に動作します。

このオプションは、EAPOL-based モードでのみ有効です。

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

■ **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。
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、ポートリンクが「ON」になると、EAPOL Success フレームを送信し、ポートのクライアントはすべて認証なしでネットワークアクセスが許可されます。

- 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リンクが「ON」になると、EAPOL Failure フレームを送信し、ポートのクライアントはすべてネットワークアクセスを無効にします。

- 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。
欠点としては、MAC アドレスが有効な RADIUS ユーザーの装置は、誰にでもアクセス可能です。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、Single 802.1X 変数を使用します。Single 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。Single 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-Assigned QoS 機能を有効にします。
“no “コマンドによりこの機能は無効となります。
RADIUS-Assigned QoS が指定したポートで有効な場合、サプリカントが正しく認証されると、RADIUS サーバによって送信された RADIUS Access-Accept パケットの QoS クラス情報に対応します。
有効な場合は、サプリカントポートで受信したトラフィックは、指定した QoS クラスに分類されます。認証（再認証）に失敗したり、RADIUS Access-Accept パケットが QoS クラスを持たない場合、または情報が不正な場合、あるいはサプリカントがポートに存在しない場合は、ポートの QoS クラスは直ちに元の QoS クラスに戻ります（RADIUS-assigned に影響を与えることなく、管理者によって変更可能)。

このオプションは、single-client モードで有効です。
• Port-based 802.1X
• Single 802.1X

■ **dot1x radius-vlan**

RADIUS-Assigned VLAN 機能を有効にします。
“no “ コマンドによりこの機能は無効となります。
RADIUS-Assigned VLAN がグローバル設定およびポート単位で有効な場合は、本機は、サプリカントが正しく認証されると、RADIUS サーバによって送信された RADIUS Access-Accept パケットの VLAN ID に対応します。
情報が有効な場合は、ポートの Port VLAN ID がこの VLAN ID に変更されると、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。
一旦割り当てを行うと、ポートで受信したトラフィックはすべて RADIUS-assigned VLAN ID にクラス分けされ、変換されます。
認証（再認証）に失敗した場合や、RADIUS Access-Accept パケットが VLAN ID を持たない場合、その情報が不正な場合、サプリカントがポートに存在しない場合は、ポートの VLAN ID は直ちに元の VLAN ID に戻ります（RADIUS-assigned に影響を与えることなく、管理者によって変更可能)。

このオプションは、single-client モードで有効です。
• Port-based 802.1X
• Single 802.1X

12) eee command

ポートのパワーセービング機能である、EEE(Energy Efficient Ethernet)機能(IEEE 802.3az)を有効にします。

■ **eee**

ポートのこの機能を有効にします。
“no” コマンドにより:この機能は無効となります。

■ **eee queue-list**
すべてのキューを「EEE Urgent Queues」に設定します。
EEE Urgent Queues は、Queues 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。

■ **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]は、キュー番号（1～8）です。
シングルキュー：“x”、キューリスト：x,y,z、キューの範囲：x-y です。
既存の設定は消去されます。

13) excessive command

半二重モードで、過度のコリジョンが発生した場合の処置を設定します。

■ **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に設定します。
- 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。

14) flowcontrol command

ポートのフロー制御を有効にします。

■ **flowcontrol**
フロー制御を有効にします。

■ **no flowcontrol**
フロー制御を無効にします。

15) interface ethernet 1/“z” command

次のポートのインターフェースの設定用にインターフェースを変更します。

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

interface ethernet1/”z”コマンドから interface vlan “x”コマンドへ直接 VLAN インターフェースへの変更は出来ません。”exit”コマンドでグローバル config に戻り、再度 interface vlan “x”コマンドを入力してください。

16) ip [IGMP/MLD] Snooping command

ポートの IGMP/MLD Snooping 機能を設定します。

■ i ip [igmp/mld] snooping fastleave

ポートのファストリーブ機能を有効にします。

マルチキャストスヌーピングのファストリーブ処理により、forwarding-table からインターフェースを取り除いた後、グループ固有のクエリーを送信します。

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 VLAN インターフェースを取り除きます。Fast-leave のプロセスにより、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、ネットワーク上のすべてのホストにとって最適な帯域管理を確保します。この処理は、IGMP および MLD に適用されます。

■ ip [igmp/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。
“xxx”:IP マルチキャストアドレスです。

■ ip [igmp/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 “ 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、マルチキャストルータ向け、または IGMP/MLD クエリア向けののポートに設定します。
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。

■ ip [igmp/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。

17) ip-source-guard command

IP ソースガード機能を設定します。
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。

■ ip-source-guard entry vid “x” mac “yy-yy-yy-yy-yy-yy” ip <IP Address>

ポートに IP ソースガードスタティックエントリを追加します。
”x”:VLAN ID(1～4094)です。
“yy-yy-yy-yy-yy-yy”: Mac アドレスです。

■ 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。

■ **ip-source-guard mode**
ポートの機能を有効にします。“no “ コマンドにより無効にします。

18) lacp command
各ポートに LACP を設定します。

■ **lacp clear**
LACP 統計情報をクリアします。

■ **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 は適切な値に設定します。
“specific”に設定した場合、ユーザにより定義された値 “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。

■ **lacp mode**
ポートの LACP 機能を有効にします。“no “ コマンドにより無効にします。

■ **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、このパラメータは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。値が小さくなると、プライオリティが高くなります。

■ **lacp role [active | passive]**
LACP の動作に対するポートの役割を設定します。
“active” に設定すると、定期的に LACP パケットを送信します。
“passive”に設定すると、対向機器からの LACP パケットの受信した場合のみ、LACP パケットを送信します。

■ **lacp timeout [fast | slow]**
Timeout を設定し、LACP 通信間の時間を制御します。
“fast”に設定すると、1 秒ごとに LACP パケットを送信します。
“slow”に設定すると、30 秒ごとに LACP パケット送信します。

19) lldp command
ポートの LLDP 機能を設定します。

lldp clear
LLDP 統計情報をクリアします。

■ **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(送受信しない)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(送受信する)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 :

ポートの LLDP オペレーションを Receive-Only(受信のみ)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 :

ポートの LLDP オペレーションを Transmit-Only(送信のみ)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。

■ **l lldp cdp-aware**

CDP-Aware 機能を有効にします。

本機 CDP の受信 CDP フレーム送信はできません。

CDP のオペレーションには、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 フレームの送信はできません）。CDP フレームは、ポートの LLDP が有効な場合のみデコードされます。

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され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、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以下のようにマッピングされます。

- CDP TLV の”Device ID"は、LLDP の"Chassis ID"に表示されます。 CDP - CDP TLV の”Address"は、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"は、LLDP の"Port ID"にマッピングします。

- CDP TLV の”Version and Platform"は、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"system capabilities"LLDP capabilities では、CDP capabilities 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。

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。

複数のポートの CDP awareness が有効な場合は、CDP フレームはすべて本機によって終結します。

■ **lldp port-description**

送信された LLDP 情報に含まれる“port description”パラメータを有効にします。

■ **lldp system-name**
送信された LLDP 情報に含まれる“system name” パラメータを有効にします。

■ **lldp system-description**
送信された LLDP 情報に含まれる “system description” パラメータを有効にします。

■ **lldp system-capabilities**
送信された LLDP 情報に含まれる “system capabilities” パラメータを有効にします。

■ **lldp management-address**
送信された LLDP 情報に含まれる“management address” パラメータを有効にします。

20) loopback-detection command

ポートのループ検知機能を設定します。

■ **loopback-detection action [log | shutdown | shut_log]**
ポートでループを検知した場合のアクションを設定します。
“shutdown”: ポートシャットダウン
“shut_log”:　ポートシャットダウン及びログ送信
“log”:ログ送信

■ **loopback-detection mode**
ポートのループ検知機能を有効にします。
“no” コマンドによりこの機能は無効となります。

■ **loopback-detection transmit**
ループ検知機能の送信モードを有効にします。
送信モードにより、ループ検知 PDU を送信するかどうかを設定します。
no loopback-detection transmit　コマンドでループ検知 PDU を送信しなくなります。

21) mac-learn command

ポートの Mac アドレスの学習機能を設定します。

■ **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　: 未学習送信元 MAC の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。(その他のフレームはすべて破棄されます。)

【注記】:
本機能を設定すると管理用の接続が切れてしまう可能性があります。

本機の管理用に接続しているポートが学習モードを変更する前に、スタティック MAC テーブルに追加したかどうか確認します。管理接続が切れてしまう場合は、その他の未設定ポートを使用するか、シリアルインターフェース(Console)を使用して本機に接続してください。引き続き設定/初期化することができます。

22) maximum-packet-length command

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。
”x”：1518～9600 です。

23) mdi/mdi-x command

ポートの MDI/MDI-X モードを設定します。

■ **mdi/mdi-x [auto | mdi | mdi-x]**

ポートの MDI/MDI-X モードを設定します。
“mdi”: スイッチングHUB等のネットワーク中継機器接続用
“mdi-x”:PC、ルータ等のネットワーク終端機器接続用、
“auto”: MDI/MDI-X の自動検知を行うことが可能です。

24) mvr command

ポートの MVR 機能を設定します。

■ **mvr immediate-leave**

ポートの fast leave を有効にします。
“no “ コマンドによりこの機能は無効となります。

■ **mvr vlan “x” [inactive-port | receiver-port | source-port]**

MVR VLAN のポート“x”の役割を設定します。

- ”x”：MVR VLAN ID（1～4094 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 ソースポートは、管理用 VLAN ポートと重複するのは推奨されていません。

25) no command

機能を無効にするか、設定値を初期値(工場設定値)に戻します。

```
------------------------------------------------------------
(config-if)# no ?
  acl                     Access Control List Configuration
  ARP Inspection          Set ARP Inspection configuration
  channel-group           Adds ports to a trunk
  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
  mvr                     Multicast VLAN Registration
  port                    Configures the characteristics of the port
  port-vlan               Configures Port-Based VLAN
  power-control           Decrease energy consumption
  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
------------------------------------------------------------
```

26) port command

ポートのモニター機能の設定および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
------------------------------------------------------------
```

■ 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:リストから Port x を取り除きます。
“x”: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 : 送信フレームのミラーリングをミラーポートで行います。受信したフレームのミラーリングは行います。

■ **port security action [none | shut | trap | trap_shut]**
ポートセキュリティに違反した場合の処理を設定します。以下の処理を行います。
- none :接続制限のみ、他に何も実行しません。
- shut : 接続制限し、ポートをシャットダウンします。
- trap : 接続制限し、SNMP トラップを送信します。
- trap_shut : 接続制限し、ポートに SNMP トラップ&シャットダウンを送信します。

■ **port security max-mac-count "x"**
このポートで確保可能な MAC アドレスの最大値を設定します。
"x":最大値、かつ設定可能な範囲の値は「0-1024」です。
例えば、x=5 は、ポートを介してネットワーク機器/PC 等のアクセス用端末を最大 5 つまで接続可能です。制限を超えた場合は、該当する処理を行います。
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 アドレスの最大値を超えて設定されていると、新たな設定が適用できない場合があります。

■ **port security mode**
このポートセキュリティを有効にします。
"no" コマンドによりこの機能は無効となります。
この機能を使うにはグローバル Config モードでポートセキュリティを有効に設定してください。

■ **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 shutdown ポートを解除します。

27) power-control command

ポートの省電力機能を設定します。

■ **power-control [actiphy | disable | perfectreach | enable]:**
省電力モードを設定します。
- **actiphy** : リンクダウン中の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** : リンクアップ中の省電力モードを有効にします。
- **enable**: リンクアップ/ダウン中の省電力モードを有効にします。

28) private-vlan command

プライベート VLAN を設定します。

本機能は、タグ VLAN(unaware モード/C-port モード/S-port モード)とは別で動作します。
同一のプライベート vlan-ID 以外のポートと通信できなくなります。
通信させる場合には、必ず、同じプライベート vlan-ID を設定してください。

■ private-vlan “x”

プライベート VLAN を設定します。
”x”：プライベート VLAN の index（1-10 までの値）です。
“no “コマンドによりプライベート VLAN からポートを除外します。

■ port-vlan isolation

ポートを isolation ポート(隔離ポート)グループに設定します。
isolation ポート同士は、同じ VLAN 内でも相互に通信できません。
“no“ コマンドにより isolation ポートグループからポートを除外します。

29) qos command

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

■ qos classification command:

ポートの QoS の入力クラス分類を設定します。

- 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）。
  - ”x”:デフォルトのクラス(0～7)。

- 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。
  - ”x”:デフォルトの DP レベル(0～1)。

- 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。
  - “x”：識別子(DEI の値(0～1))です。

◆ 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“ コマンドによりこの機能は無効となります。

◆ 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)

◆ 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。
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。
”x”:0～7 の値です。

◆ 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“ コマンドによりこの機能は無効となります。
この機能が無効な場合は、デフォルトの QoS クラスと DP レベルが、タグフレームに適用されます。

■ **qos dscp command :**
QoS ポートの DSCP の設定を行います。

◆ 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る)が「0」の場合はクラス分けします。

◆ qos dscp egressremark [enable|remap_dp_aware|remap_dp_unaware]:
DSCP Egress Rewrite モードを設定します。
“no” コマンドによりこの機能は無効となります。
- **enable** : リマッピングを行わずにリライトを有効にします。
- **remap_dp_aware** : リマッピングにより、リライトを有効にします。
- **remap_dp_unaware** : リマッピングにより、リライトを有効にします。

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。

各 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。

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

■ qos policer command:

QoS 入力ポートのポリシングを設定します。。

- 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” コマンドによりこの機能は無効となります。

- qos policer mode:
入力トラフィックレートの policer 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します。
“no” コマンドによりこの機能は無効となります。

- qos policer rate “x”:
ポートのポリシングレートを設定します。
”x”:の値は、単位が kbps、または fps の場合は、「100-1000000」の範囲内の値、
単位が Mbps、または kfps の場合は「1-3300」の範囲内の値です。

- qos policer unit [kbps | fps] :
ポートのレートの単位を設定します。“kbps”(kbit/秒)または“fps”(frame/秒)

■ qos queueshaper command :

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。

- 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。
“no” コマンドによりこの機能は無効となります。
・ ”x”:キューの値（0～7）です。

- qos queueshaper excess “x” :
送信キュー”x”の帯域超過を許可します。
“no” コマンドによりこの機能は無効となります。
”x”:キューの値（0～7）です。

- 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”: はキューの値(0～7）です。

・ “**y**”:トラフィックレートの値(100～3,300,000kbps)です。

■ **qos scheduler command:**

ポートの送信キューのトラフィックの調整を行います。

◆ 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。

◆ 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。

■ **qos shaper command:**
ポートのトラフィックシェーピング機能を設定します。

◆ 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” コマンドによりこの機能は無効となります。

◆ 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。。
・ “x”: 送信速度の値(100～3300000kbps)です。

■ **qos tagremarking command :**
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。

◆ 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。
・ ”x”:デフォルトの DEI の値(0～1)です。※VLAN タグの 1-bit field)です。

◆ qos tagremarking map “w” “x” “y” “z” コマンド:
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)

◆ 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 tag remarking 設定のタグ付きポートに設定してください。

◆ 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をストアします）です。
・ “x”：PCP（0～7 までの値）です。

30) sflow command

ポートの sflow 機能を設定します。

■ **sflow counterpoller enable:**
カウンタのポーリングを有効にします。“no “ コマンドによりこの機能は無効となります。

■ **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。
・ ”x”:「0～3600 秒」までの値です。

■ **sflow flowsampler enable:**
ポートのフローサンプリングを有効にします。
“no“ コマンドによりこの機能は無効となります。

■ **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。
最大データサイズがヘッダの最大値を考慮しない場合は、サンプルは破棄されます。
・ ”x”：最大値（14～200 bytes までの値）です。

■ **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。
・ ”x”：サンプルレート(1～4294967295 までの値)です。
サンプリングレートは、”x”に指定して、 ポートで送受信されたパケットの 1/”x”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。

■ **sflow sampler:**
ポートの sflow 統計情報をクリアします。

31) shutdown command

ポートを無効にします。

■ **shutdown :**
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。
無効化した状態で LAN ケーブルを接続しても、リンクアップしません。

32) spanning-tree command

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
  edge-port      Specifies spanning tree edge port
  mcheck         Set the STP mCheck (Migration Check) variable for 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
---------------------------------------------------------------
```

■ **spanning-tree autoedge:**
ブリッジポートの自動エッジポート検出機能を有効にします。
ポート上で 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 “ コマンドによりこの機能は無効となります。

■ **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に BPDU を受信すると、ポートは無効になります。
BPDU Guard はポートのエッジステータスと連動し、エラーが発生するとポートは error-disabled 状態になります。この設定により、ポートはブリッジのエラー復旧の設定にも従います。
“no “ コマンドによりこの機能は無効となります。

■ **spanning-tree clear**
ポートの STP 統計情報をクリアします。

■ **spanning-tree edge-port:**
エッジポートで動作を開始するように設定します。
(ポートが初期化されると、初期状態ではエッジポートフラグが有効になります)。
“no“ 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。

■ **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、選択したインター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）。

■ **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)、
  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。

■ **spanning-tree p2p [auto | false | true] コマンド:**
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。

■ **spanning-tree restrictedrole コマンド:**
MSTP での動作を制限します。この機能は、“ルートガード”とも呼ばれます。
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。
“no “コマンドにより、この機能を無効にします。

■ **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。

■ **spanning-tree:**
スパニングツリー機能を有効にします。
“no” コマンドによりこの機能は無効となります。

33) speed command

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 fdx
  100fdx        Set port speed to be 100M fdx
  1000fdx               Set port speed to be 1G fdx
------------------------------------------------------------
```

■ **speed auto:**
auto-negotiation モード(自動判別モード)に設定します。

■ **speed [10hdx | 10fdx]:**
10M の通信速度、半二重[hdx]]/全二重[fdx]モードに設定します。

■ **speed [100hdx | 100fdx]:**
100M の通信速度、半二重[hdx]]/全二重[fdx]モードに設定します。

■ **speed 1000fdx:**
1000M 通信速度、全二重[fdx]モードに設定します。

34) switchport command

ポートにVLAN等のスイッチポートの動作の設定を行います。

```
------------------------------------------------------------
(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
------------------------------------------------------------
```

■ 一般的なスイッチポート設定は、下表の通り設定します。

設定項目	Mode	native(PVID)	Ingressfilter[任意]	tx_tag[任意]
802.1QVLAN				
Access ポートベース VLAN	unaware	ポートの VLANID	無効	untag_pvid (untag_all)
Trunk(native なし) VLAN タギングポート	C-port	None	有効	tag_all (untag_pvid)
Trunk(native あり) Hybrid ポート	C-port	ポートの VLANID	有効	untag_pvid
Q-in-Q				
UpLink (サービスポート)	S-port/ s-custom-port	None/ポートの VLANID	有効	untag_pvid (tag_all)
Downlink (カスタマポート)	unaware	S-port で付与 する VLANID	無効	untag_pvid (untag_all)

※ingressfilter 設定及び、tx_tag 設定は、オプション設定です。
必要に応じ設定をしてください。

■ **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。

■ **switchport allowed vlan [add “x” | remove “x” | forbidden add “x” | forbidden remove “x”]　:**
ポートに VLAN “x” の追加/削除、VLAN “x”の禁止を追加/解除の設定を行うことができます。

- add “x” :ポートに VLAN“x”を追加します。
- remove “x” :ポートからVLAN“x”を削除します。
- forbidden add “x”:ポートにVLAN”x”の追加を禁止します。
- forbidden remove “x” :ポートからVLAN”x”の禁止を解除します。
- “x”の VLAN ID は「2～4095」までの値です。

Forbidden add “x”コマンドで禁止VLANの設定をすると、動的 VLAN プロトコル等により選択した VLAN がポートメンバーに自動的に含められることを禁止します。

■ **switchport ingressfilter:**
ポートの VLAN 入力フィルタ機能を有効にします。
この機能は、タグ付けされたフレーム転送に影響します。
“no“ コマンドによりこの機能は無効となります。
有効な場合は、ポートに所属していないVLANは破棄されます。
無効な場合は、ポートに所属していなくても VLAN データベースにある場合は、他の所属しているポートへ転送されます。VLAN データベースにない VLAN は破棄されます。

■ **switchport mode [c-port | s-custom-port | s-port | unaware]:**
ポートの動作モード(Port Type)を設定します。
- c-port : 受信フレームは、タグ付きフレームはタグ情報に応じて VLAN に分類されます。出力フレームにタグをつける場合は、802.1QVLAN タグ(TPID0x8100)が付与されます。これは、802.1Q VLAN(トランク)接続用になります。
- s-custom-port : 受信フレームは、タグ付きフレームはタグ情報に応じて VLAN に分類されます。出力フレームには、Service VLAN タグ(カスタム TPID)を付与します。カスタム TPID は、VLAN データベースで指定します。これは、Q-in-Q アップリンク接続用になります。
- s-port : 受信フレームは、タグ付きフレームはタグ情報に応じて VLAN に分類されます。出力フレームには、Service VLAN タグ(TPID0x88A8)が付与されます。これは、Q-in-Q アップリンク接続用になります。
- unaware :すべての受信フレームはポートの VLAN ID（PVID）に分類されます。受信したフレームにタグある場合でも、本機にペイロード(データ部)として処理されポートの VLAN ID に分類されます。

これは、802.1Q の場合はアクセス接続用になり、Q-in-Q の場合にはダウンリンク接続用になります。また、ポートベース VLAN を使用する場合にも、“Unaware”に設定します。

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。

■ **switchport native vlan [none | “x”] :**
ネイティブ VLAN の VLAN ID を割り当てて、入力ポートのタグなしフレームをクラス分けします。
- ”x”：ポート VLAN ID (PVID)で値は「1～4095」の範囲で設定可能です。
- “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 に使用します。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。

■ **switchport tx_tag [tag_all | untag_all | untag_pvid] :**
出力フレームのタグ付き方法を定義します。
- tag_all: タグ付き出力ポートです。出力フレームトはすべてタグ付きです。
- untag_all: タグなし出力ポートです。出力フレームはすべてタグなしです。
- untag_pvid: ポート VLAN ID(PVID)に所属するフレームは、タグなしで送信し、その他の VLAN に所属するフレームはすべてタグ付けし、出力されます。

35) voice-vlan command

ポートの Voice 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
------------------------------------------------------------
```

■ **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 の両方を検出します。

■ **voice-vlan port-mode [auto | disable | force]:**

Voice 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 phone が特定ポートに接続されているか、Voice 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** : Voice VLAN から解除します。
- **force** : VLAN に設定します。

■ **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、Voice 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 “ コマンドによりこの機能は無効になります。

1.2.3.2 VLAN Interface Configure コマンド

Configure モードのコマンドは、本機の基本設定です(プロント表示“(config)#”)。
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。

【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 Configure 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。
“x”:「1～4095」はVLAN-IDです
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。

“interface vlan 100”は、VLAN 100の設定を行う場合です。
“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。

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

“?”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 command
現在のモードを終了し、前のモードに戻ります。

2) help command
使用可能なコマンドが表示されます。

3) history command
入力したコマンドの履歴が表示されます。

4) logout command
ログアウト用のコマンドです。

5) quit command

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 command

次のセットアップコマンド用にインターフェース VLAN グループを変更します。

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

例：“(config-if)# interface vlan 100: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 command

VLAN インターフェースで IP アドレスを設定します。
この IP アドレスへ通信可能なユーザのみが IP アドレスへリモートで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
------------------------------------------------------------
```

■ **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 設定を行います。
“no” コマンドによりこの機能は無効となります。
DHCP サーバが 35 秒内に応答しない場合は、DHCP は再試行を中断し、設定された IP アドレスもしくは、デフォルトの IP アドレス「192.168.1.1/24」を使用します。DHCP クライアントは、DNS 参照する為、設定した System Name をホスト名として通知します。

■ **ip address “x.x.x.x” “y.y.y.y”:**
VLAN インターフェースの固定 IP アドレスの設定をします。
“x.x.x.x”:IP アドレス
“y.y.y.y”: サブネットマスクです。
例えば “ip address 192.168.1.12 255.255.255.0:リモート管理用の VLAN グループの本機の IP アドレスを設定します。

■ **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 command

VLAN 用の本機の IPv6 アドレスを設定します。
この IPv6 アドレスへ通信可能なユーザのみが 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
------------------------------------------------------------
```

■ **ipv6 address autoconfig:**
IPv6 Auto Configuration 機能を有効にします。
“no“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。

■ **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。

■ **ipv6 address <ipv6 address>:**
この VLAN の固定 IPv6 アドレスを設定します。

- “**<ipv6 address>**“:IPv6 アドレスです。

9) no command

機能を無効にするか、工場出荷時の値にリストアします。

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

例：“no ip address dhcp” コマンド:この機能は無効になります。

1.2.4 VLAN Configureコマンド

Configure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、configure 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】: VLAN グループ（VLAN ID と呼ばれる）の IP 設定は、“interface vlan x”コマンド（“x” VLAN ID）で、VLAN インターフェース configure モードに入ってください。

“vlan database” 以下の画面が表示されます。

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

“?”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 command

現在のモードを終了し、前のモードに戻ります。

2) help command

設定可能なコマンドをすべて表示します。

3) history command

入力したコマンドの履歴を表示します。

4) logout command

コンソール画面からログアウトします。

5) quit command

コンソール画面を終了します。ログアウトと同じ機能です。

6) end command

VLAN Configure モードを終了します。

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

7) no command

機能を無効にするか、工場出荷時の値にリストアします。

```
------------------------------------------------------------
(config-vlan)# no ?
  vlan              Switch Virtual LAN interface
------------------------------------------------------------
```

例: "**no vlan 100**": VLAN 100 を削除します。

8) vlan command

VLAN の定義及び、Q-in-Q のカスタム TPID の設定をします。

■ **vlan x コマンド:**

VLAN の定義を行います。

- "x":VLAN ID(1～4095 までの値)です。
- "no" コマンドにより VLAN "x"を削除します。

■ **vlan x name yyy :**

VLAN ID "x" を定義し、VLAN"x"の名前を "yyy"に設定します。

- "x":VLAN ID(1～4095 までの値)
- "**yyy**":VLAN 名

■ **vlan etypecustomsport 0xXXXX コマンド:**

Q-in-Q の Custom S-port のイーサネットタイプ(TPID)を設定します。

- "**0xXXXX**": EtherType(16 進数)です。
- "no" コマンドにより VLAN "x"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コマンドが表示されます。

“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
  lacp                LACP statistics
  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
  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 acl command

ACL 設定およびステータスを表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ show acl port :

ACL ポートの設定を表示します。

```
------------------------------------------------------------
# show acl port
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
------------------------------------------------------------
```

■ show acl rate:

ACL 帯域制御の設定情報を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **show acl status:**

ACL ステータスを表示します。

```
------------------------------------------------------------
# show acl status
User
----
S   : Static
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
------------------------------------------------------------
```

表示項目については、以下を参照してください。

- 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 の帯域制御(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。

■ **show acl “x” :**

ACE ステータスを表示します。

- ”x”:ACE の ID(1～256 の値)です。

```
---------------------------------------------------------------
# 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
---------------------------------------------------------------
```

■ **show acl:**

ACE ステータスのすべてを表示します。

```
---------------------------------------------------------------
# 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
---------------------------------------------------------------
```

2) show calendar command

現在のシステムタイムを表示します。

```
---------------------------------------------------------------
# show calendar
System Time     : 2012-01-01T05:09:39+00:00
System Uptime   : 05:09:39
---------------------------------------------------------------
```

3) show ddmi ethernet command

SFP の DDMI のステータスを表示します。

```
---------------------------------------------------------------
# show ddmi ethernet
Digital Diagnostics Monitoring Interface of Eth 1/9
Serial Info Table
  Status:                   ok_with_DDM
  Vendor:                    FXC Inc.
```

```
PartNo:                  MGB-SX
SerialNo:                SECS12345678
Revision:                C
DateCode:                150128
Transceiver:             1000BASE-SX
Ddm Info Table
Type              AlarmMax  AlarmMin  WarnMax  WarnMin  Current
Temperature(∧)     85.00    -10.00    80.00    -5.00    33.40
Voltage(mV)        3.60     2.90      3.50     3.00     3.28
TxBias(mA)         50.00    0.50      40.00    1.00     23.48
TxPower(mW)        3.21     0.24      2.55     0.31     0.70
RxPower(mW)        3.10     0.02      2.46     0.03     0.00
-----------------------------------------------------------------
```

4) show dhcp-relay command

現行の DHCP Relay の設定およびステータスを表示します。

```
-----------------------------------------------------------------
# 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
-----------------------------------------------------------------
```

5) show dot1x command

802.1x の設定を表示します。

■ show dot1x :

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。

```
------------------------------------------------------------
# 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      -         -
------------------------------------------------------------
```

表示項目については、以下を参照してください。

- 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 ベース認証用に新しい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の受信した Response Identity EAPOL フレーム、および MAC ベース認証のために新しい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。

■ show dot1x configuration :

本機の 802.1x 設定を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **show dot1x guest_vlan :**

ゲスト用 VLAN をポート単位で表示します。

```
-----------------------------------------------------------------
# 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
-----------------------------------------------------------------
```

■ **show dot1x radius_qos :**

RADIUS-assigned QoS をポート単位で表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **show dot1x radius_vlan:**

RADIUS-assigned VLAN をポート単位で表示します。

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

■ **show dot1x statistics:**

802.1X 統計情報を表示します。

```
------------------------------------------------------------
# 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           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
-------------------------------------------------------------
```

6) show eee command

EEE (IEEE 802.3az)設定を表示します。

```
-------------------------------------------------------------
# show eee
EEE Configuration:
==================
Port  Mode     Urgent queues
----  -------  -------------
1     Disabled   none
2     Disabled   none
3     Disabled   none
4     Disabled   none
5     Disabled   1
6     Disabled   none
7     Disabled   none
8     Disabled   none
9     N/A        none
10    N/A        none
-------------------------------------------------------------
```

7) show history command

入力したコマンドの履歴を表示します。

```
-------------------------------------------------------------
# show history
  1. config
  2. interface valn 10
  3. ipv6 address state fc80::215:c5ff:fe03:4dc7
  4. exit
  5. show history
-------------------------------------------------------------
```

8) show interface command

ポート情報およびステータスを表示します。

```
-------------------------------------------------------------
# show interface ?
  counters                Interface counters information
  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
-------------------------------------------------------------
```

■ **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 (“x”:ポート番号)。

```
-------------------------------------------------------------
# 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
-------------------------------------------------------------
```

- 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”の統計情報の値を表示します(“x”:ポート番号)。

```
-------------------------------------------------------------
# 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
-------------------------------------------------------------
```

- show interface dualMedia_fiberMode:
  ポートごとの通信速度とモードのステータスを表示します。

```
------------------------------------------------------------- # show interface
dualMedia_fiberMode

Port  Link  MDI/MDI-X
----  ----  ---------
```

```
1     Down  AUTO-MDI
2     Down  AUTO-MDI
3     Down  AUTO-MDI
4     Down  AUTO-MDI
5     Down  AUTO-MDI
6     1Gfdx  AUTO-MDI
7     Down  AUTO-MDI
8     Down  AUTO-MDI
9     Down  AUTO-MDI
10    Down  AUTO-MDI
#
------------------------------------------------------------
```

◆ 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。

```
------------------------------------------------------------
# show interface psec switch
Users:
L = Limit Control
8 = 802.1X
D = DHCP Snoopin
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
------------------------------------------------------------
```

■ **show interface sfp :**
検出した sfp タイプを表示します。

```
  ------------------------------------------------------------
# show interface sfp
Port  SFP
----  ----------
1     None
2     None
3     None
4     None
5     None
6     None
7     None
8     None
9     None
10    None
```

■ **show interface status:**

ポートの設定情報を表示します。

```
# show interface status
Port Configuration:
===================
Port  State     Mode      Flow Control  MaxFrame  Power   Excessive  Link
----  --------  ----------  ------------  --------  --------
1     Enabled   Auto      Disabled      9600      Disabled  Discard    Down
2     Enabled   Auto      Disabled      9600      Disabled  Discard    Down
3     Enabled   Auto      Disabled      9600      Disabled  Discard    Down
4     Enabled   Auto      Disabled      9600      Disabled  Discard    Down
5     Enabled   Auto      Disabled      9600      Disabled  Discard    Down
6     Enabled   Auto      Disabled      9600      Disabled  Discard    Down
7     Enabled   Auto      Disabled      9600      Disabled  Discard    100fdx
8     Enabled   Auto      Disabled      9600      Disabled  Discard    Down
9     Enabled   Auto      Disabled      9600      Disabled  Discard    Down
10    Enabled   Auto      Disabled      9600      Disabled  Discard    Down
```

■ **show interface switchport:**

すべてのポートの VLAN 設定を表示します。

```
#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。

```
# show interface switchport status
Port VLAN User PortType  PVID Frame Type  Ing Filter  Tx Tag   UVID  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
-------------------------------------------------------------
```

■ **show interface veriphy**

ケーブル診断を実行します。

```
-------------------------------------------------------------
# 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
-------------------------------------------------------------
```

9) show ip command

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。

```
-------------------------------------------------------------
# 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
  verify              IP Source Guard
-------------------------------------------------------------
```

■ **show ip ARP Inspection :**

ARP 検査の設定およびステータスを表示します。

```
-------------------------------------------------------------
# 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
-------     ----   ----    -----------------        -------------
-------------------------------------------------------------
```

■ **show ip dhcp snooping :**

DHCP Snooping 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
------------------------------------------------------------
```

◆ show ip dhcp snooping statistics :

DHCP Snooping の統計情報を表示します。

```
------------------------------------------------------------
# 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---
------------------------------------------------------------
```

■ **show ip http server secure status**

現行の HTTPS(セキュリティモード)のステータスを表示します。

```
------------------------------------------------------------
# show ip http server secure status
HTTPS Configuration:
====================
HTTPS Mode          : Enabled
HTTPS Redirect Mode : Disabled
------------------------------------------------------------
```

■ **show ip igmp:**
現行の IGMP スヌーピング情報を表示します。

```
------------------------------------------------------------
# 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---
------------------------------------------------------------
```

■ **show ip interface:**
現行の本機の IP 情報を表示します。

```
------------------------------------------------------------
# show ip interface
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

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

■ **show ip mld:**
現行の MLD Snooping 設定を表示します。

```
---------------------------------------------------------------
# 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---
---------------------------------------------------------------
```

■ **show ip ssh:**
現行の SSH 設定情報を表示します。

```
---------------------------------------------------------------
# show ip ssh
SSH Configuration:
==================
SSH Mode : Enabled
---------------------------------------------------------------
```

■ **show ip verify source:**
IP Source Guard の設定を表示します。

```
---------------------------------------------------------------
# show ip verify source
IP Source guard Configuration:
==============================
IP Source Guard Mode : Enabled
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
```

```
IP Source Guard Entry Table:
Type     Port  VLAN  IP Address       MAC Address
-------  ----  ----  ---------------  -----------------
------------------------------------------------------------
```

10) show lacp command

本機の現行の LACP 設定およびステータスを表示します。

```
------------------------------------------------------------
# show lacp ?
  config          Show LACP configuration
  statistics      Show LACP statistics
  status          Show LACP status
------------------------------------------------------------
```

■ show lacp config:

現行の LACP 設定を表示します。

```
------------------------------------------------------------
# show lacp config
LACP Configuration:
===================
System Priority: 32768

Port  Mode     Key   Role   Timeout
----  --------    ----  ------    -------
1     Disabled  Auto  Active  Fast
2     Disabled  Auto  Active  Fast
3     Disabled  Auto  Active  Fast
4     Disabled  Auto  Active  Fast
5     Disabled  Auto  Active  Fast
6     Disabled  Auto  Active  Fast
7     Disabled  Auto  Active  Fast
8     Disabled  Auto  Active  Fast
9     Disabled  Auto  Active  Fast
10    Disabled  Auto  Active  Fast
------------------------------------------------------------
```

■ **show lacp statistics:**

現行の LACP 統計情報を表示します。

```
---------------------------------------------------------------
# show lacp statistics
System Priority: 32768

Port  Timeout  PriorityRx Frames  Tx Frames   Rx Unknown  Rx Illegal
----  -------  ------------------      ----------      ----------      1     Fast     327680          0
0          0
2     Fast     327680          0          0          0
3     Fast     327680          0          0          0
4     Fast     327680          0          0          0
5     Fast     327680          0          0          0
6     Fast     327680          0          0          0
7     Fast     327680          0          0          0
8     Fast     327680          0          0          0
9     Fast     327680          0          0          0
10    Fast     327680          0          0          0
---------------------------------------------------------------
```

■ **show lacp status:**

現行の LACP ステータスを表示します。

```
---------------------------------------------------------------
# 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 command

現行の LLDP 設定およびステータスを表示します。

■ show lldp:

現行の LLDP 設定を表示します。

```
------------------------------------------------------------
# show lldp
LLDP Configuration:
==================
Interval                    : 30
Hold            : 4
Tx Delay        : 2
Reinit Dela                 : 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
------------------------------------------------------------
```

■ **show lldp info:**

LLDP ネイバー情報を表示します。

```
---------------------------------------------------------------
# show lldp info
No LLDP entries found
---------------------------------------------------------------
```

■ **show lldp statistics:**

LLDP 統計情報を表示します。

```
---------------------------------------------------------------
# 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 command

現行の system log および system log 設定を表示します。

```
------------------------------------------------------------
# show log ?
  configuration       logging configuration
  <cr>
------------------------------------------------------------
```

■ show log:

現行の system log の情報を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ show log configuration:

現行のシステムのログ情報を表示します。

```
------------------------------------------------------------
# show log configuration
System Log Configuration:
========================
System Log Server Mode                  : Disabled
System Log Server Address       :
System Log Level                        : Error
------------------------------------------------------------
```

13) show loopback-detection command

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。

```
------------------------------------------------------------
# show loopback-detection ?
  config          Loop protect configuration
  ethernet         Show loop protection port configuration
  status          Show the loop protection status
------------------------------------------------------------
```

■ show loopback-detection config :

ループバック検知の設定を表示します。

```
------------------------------------------------------------
# show loopback-detection config
Loop Protection Configuration:
==============================
Loop Protection  : Disabled
```

```
Transmission Time: 5
Shutdown Time    : 180
------------------------------------------------------------
```

■ **show loopback-detection ethernet:**

ループ保護のポートの設定を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **show loopback-detection status :**

ループ保護のステータスを表示します。

```
------------------------------------------------------------
# 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 command

Mac アドレステーブルおよびその他の機能を設定します。

```
------------------------------------------------------------
# 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>
------------------------------------------------------------
```

■ **show mac-address-table :**
MAC アドレステーブル情報を表示します。

```
------------------------------------------------------------
# show mac-address-table
Type    VID     MAC Address       Ports
------  ---  ----------------  -----
Dynamic 1       00-17-2E-15-FB-8C  7
Dynamic 1       00-0a-79-b9-a2-c3  7
Dynamic 1       00-0d-87-26-f4-3b  7
Dynamic 1       00-c0-f6-55-09-9b  7
Dynamic 1       00-c0-f6-74-25-01  7
Static  1       00-c0-f9-66-66-99  None,CPU
Static  1       33-33-00-00-00-01  1-8,10,CPU
Static  1               33-33-00-00-00-02  1-8,10,CPU
Static  1               33-33-ff-03-4d-c0  1-8,10,CPU
Static  1               33-33-ff-66-66-99  1-8,10,CPU
Dynamic 1               70-5a-b6-f8-32-ea  7
Static  1       ff-ff-ff-ff-ff-ff  1-10,CPU
Static  10      00-00-00-01-02-03  5
------------------------------------------------------------
```

■ **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。

```
------------------------------------------------------------
# show mac-address-table aging-time
MAC Age Time: 300
------------------------------------------------------------
```

■ **show mac-address-table address “x-x-x-x-x-x”:**
MAC アドレス“x-x-x-x-x-x”の MAC アドレステーブルを表示します。

```
------------------------------------------------------------
# show mac-address-table address 00-17-2E-15-FB-8C
Type    VID   MAC Address       Ports
------    ---    ----------------       -----
Dynamic  1    00-17-2E-15-FB-8C    7
------------------------------------------------------------
```

■ **show mac-address-table learning :**
ポートの学習モードを表示します。

```
------------------------------------------------------------
# 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
-------------------------------------------------------------
```

■ **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。

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

# 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 command

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。

```
-------------------------------------------------------------
# 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 command

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。

■ show management :

管理用 IP フィルタの設定情報を表示します。

```
-------------------------------------------------------------
# show management
Access Mgmt Configuration:
==========================
System Access Mode : Disabled
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx  Start IP Address            End IP Address            W S T
 ------------------------------------------------------------------
2   192.168.1.100               192.168.2.200             N N N
-------------------------------------------------------------
```

■ show management statistics :

管理セキュリティの統計情報を表示します。

```
-------------------------------------------------------------
# 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
-------------------------------------------------------------
```

17) show map command

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。

```
------------------------------------------------------------
# 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---
------------------------------------------------------------
```

18) show mvr command

MVR 設定およびステータスを表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ show mvr config:

MVR 設定を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ show mvr group コマンド:

MVR グループを表示します。

■ show mvr sfm コマンド:

MVR の SFM (SSM を含む)関連情報を表示します。

■ show mvr statistics :

MVR 統計情報を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

19) show ntp command

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

■ show ntp config:

NTP 設定情報を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ show ntp dst:

サマータイム(Daylight Saving)の設定を表示します。

```
------------------------------------------------------------
# show ntp dst
System Daylight Saving(DST) Configuration:
================================================
Daylight Saving Mode : Non-Recurring.
Daylight Saving Start Time Settings :
       Week: 0
       Day: 0
     * Month: 1
     * Date: 1
     * Year: 2000
     * Hour: 0
```

```
    * Minute: 0
Daylight Saving End Time Settings :
      Week: 0
      Day: 0
    * Month: 1
    * Date: 1
    * Year: 2000
    * Hour: 0
    * Minute: 0
Daylight Saving Offset : 1 (minutes)
------------------------------------------------------------
```

■ **show ntp zone :**

システムのタイムゾーンの情報を表示します。

```
------------------------------------------------------------
# show ntp zone
System Timezone Configuration:
==============================
Timezone Offset : 5400 ( 540 minutes)
Timezone Acronym : Japan
------------------------------------------------------------
```

20) show port command

ポートのミラーリング機能の設定情報を表示します。

■ **show port monitor:**

ポートのミラーリング機能の設定情報を表示します。

```
------------------------------------------------------------
# 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 command

QCL (Queue Control List) 設定およびステータスを表示します。

```
------------------------------------------------------------
# show queue ?
  status            Show QCL status.
  <cr>
------------------------------------------------------------
```

■ show queue:

QCL 設定情報を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ show queue status:

QCL ステータスを表示します。

```
------------------------------------------------------------
# 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 command

RADIUS サーバ の設定情報および統計情報を表示します。

■ show radius-server:

RADIUS サーバの設定情報を表示します。

```
------------------------------------------------------------
# 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
-----------------------------------------------------------------
```

■ **show radius-server statistics “x” :**

RADIUS サーバの統計情報を表示します。

- ”x”:RADIUS サーバの index(1～5 の値)です。

23) show running-config command

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.....
!
……
!
!
interface ethernet 1/5
qos tagremarking map 2 1 0 0
exit
!
interface ethernet 1/1
switchport allowed vlan add 1
exit
!
interface vlan 1
ip address 192.168.1.118 255.255.255.0
ipv6 address fc80::215:c5ff:fe03:4dc0 120
end
-----------------------------------------------------------------
```

24) show rate-limit command

各ポートの帯域制限(レートリミット)設定情報を表示します。

```
-----------------------------------------------------------------
# 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 command

RMON の設定を表示します。

```
-------------------------------------------------------------
# show rmon ?
  alarm          Show RMON alarm entries
  event          Show RMON event entries
  history        Show RMON history entries
  statistics     Show RMON statistics entries
-------------------------------------------------------------
```

■ show rmon alarm :

RMON アラームの設定情報を表示します。

```
-------------------------------------------------------------
# show rmon alarm
abc# show rmon alarm
Id    Interval  Alarm Variable          Alarm SampleType
-----  ---------  ----------------------------------
1     30     .1.3.6.2.2.2.2.2.1.10.1     deltaValue

Number of entries: 1
-------------------------------------------------------------
```

■ show rmon event:

RMON イベント情報を表示します。

```
-------------------------------------------------------------
# show rmon event
Id    Description  Type  Community   LastSent
-----  -----------  -----  -----------    ---------
1    abc          none  public      Never
Number of entries: 1
-------------------------------------------------------------
```

■ show rmon history:

RMON 履歴情報を表示します。

```
-------------------------------------------------------------
# show rmon history
Id  Data Source          controlBucketsRequested  controlBucketsGranted  Interval
----- ------------------------------  ------------------------      10  .1.3.6.2.2.2.2.2.1.1.10    50
50        1800

Number of entries: 1
-------------------------------------------------------------
```

■ **show rmon statistics :**

RMON 統計情報を表示します。

```
---------------------------------------------------------------
# show rmon statistics
Id  Data Source          etherStatsOctets  etherStatsPkts  therStatsCRCAlignErrors
----- -------------------------------- -----------------     10  .1.3.6.2.2.2.2.2.1.1.10    0
0             0

Number of entries: 1
---------------------------------------------------------------
```

26) sflow command

sFlow 設定情報を表示します。

```
---------------------------------------------------------------
# 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
---------------------------------------------------------------
```

■ **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。

```
---------------------------------------------------------------
# show sflow counter_poller
Counter Poller Configuration:
=============================
Port  Interval
----  --------
8     10
---------------------------------------------------------------
```

■ **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。

```
---------------------------------------------------------------
# show sflow flow_sampler
Flow Sampler Configuration:
===========================
Port  Sampling  Rate  Max Hdr
----  -------------  -------
8     20      128
---------------------------------------------------------------
```

■ **show sflow receiver:**

sFlow レシーバの設定情報を表示します。

```
---------------------------------------------------------------
# show sflow receiver
Receiver Configuration:
=======================
Owner                        : <none>
Receiver         : 0.0.0.0
```

```
UDP Port        : 6343
Max. Datagram           : 1400 bytes
Time left       : 0 seconds
-------------------------------------------------------------
```

■ **show sflow statistics receiver:**

レシーバの統計情報を表示します。

```
-------------------------------------------------------------
# show sflow statistics receiver
Receiver Statistics:
====================
Tx Successes  Tx Errors    Flow Samples  Counter Samples
------------  -----------  --------------  ---------------
      0           0           0             0
-------------------------------------------------------------
```

■ **show sflow statistics samplers:**

ポート単位の統計情報を表示します。

```
-------------------------------------------------------------
# show sflow statistics samplers
Per-Port Statistics:
====================

No non-zero counters.
-------------------------------------------------------------
```

27) show snmp command

本機の SNMP 設定を表示します。

```
-------------------------------------------------------------
# show snmp ?
  access        SNMPv3 access entry
  community             SNMPv3 community entry
  group         SNMPv3 group entry
  user          SNMPv3 user entry
  view          SNMPv3 view entry
  <cr>
-------------------------------------------------------------
```

■ **show snmp :**

本機の SNMP 設定情報を表示します。

```
-------------------------------------------------------------
# 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
-------------------------------------------------------------
```

■ **show snmp access :**

SNMPv3 アクセスエントリを表示します。

```
-------------------------------------------------------------
# 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
-------------------------------------------------------------
```

■ **show snmp community:**

SNMPv3 コミュニティエントリを表示します。

```
-------------------------------------------------------------
# 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
-------------------------------------------------------------
```

■ **show snmp group コマンド:SNMPv3 グループエントリを表示します。**

```
-------------------------------------------------------------
# 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
```

■ **show snmp user:**

SNMPv3 ユーザのエントリを表示します。

```
# 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
```

■ **show snmp view:**

SNMPv3 ビューエントリを表示します。

```
# 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 command

本機のスパニングツリーの設定情報を表示します。

```
# show spanning-tree ?
  ethernet                  Show STP Port configuration
  mst                       Show MSTP configuration
  statistics                Show STP port statistics
  status                    Show STP Bridge status
  <cr>
```

■ **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。

```
# show spanning-tree
STP Configuration:
==================
Protocol Version: MSTP
Max Age         : 20
Forward Delay           : 15
Tx Hold Count           : 2
Max Hop Count           : 20
BPDU Filtering          : Disabled
BPDU Guard              : Disabled
```

```
Error Recovery            : Disabled
------------------------------------------------------------
```

■ **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。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **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。

- “x”:MSTI の index(0～7 までの値)です。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **show spanning-tree mst:**

システムの MSTP の設定情報を表示します。

```
------------------------------------------------------------
# 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
-------------------------------------------------------------
```

■ show spanning-tree statistics:

STP ポートの統計情報を表示します。

```
-------------------------------------------------------------
# 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.
---------  --------  --------  --------  --------  ------  ---
-------------------------------------------------------------
```

■ show spanning-tree status “x”:

MSTP ブリッジのステータスを表示します。

- “x”：MSTI の index(0～7 までの値)です。

```
-------------------------------------------------------------
# show spanning-tree status 0
CIST Bridge STP Status
Bridge ID                    : 32768.00-17-2E-15-FB-8C
Root ID          : 32768.00-17-2E-15-FB-8C
Root Port        : -
Root PathCost : 0
Regional Root : 32768.00-17-2E-15-FB-8C
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:

本機のストームコントロールの設定情報を表示します。

```
------------------------------------------------------------
# show storm-control

QoS Storm Control:
==================
Storm Unicast          : Disabled    1 fps
Storm Multicast        : Disabled    1 fps
Storm Broadcast        : Disabled    1 fps
------------------------------------------------------------
```

30) show system :

本機のシステム情報および設定情報を表示します。

```
------------------------------------------------------------
# show system
System Contact         :
System Name            : abc
System Location        :
Software Version       : 10-P Ver:1.00.00
Software Date          : 2012-08-17T14:31:24+08:00
MAC Address            : 00-17-2E-15-FB-8C
Number of Ports        : 10
Previous Restart       : Cold
------------------------------------------------------------
```

31) show tacacs-server command

TACACS+ 認証サーバの設定情報を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **storm-control:**

本機のストームコントロールの設定情報を表示します。

```
------------------------------------------------------------
# show storm-control

QoS Storm Control:
==================
Storm Unicast          : Disabled    1 fps
Storm Multicast        : Disabled    1 fps
Storm Broadcast        : Disabled    1 fps
------------------------------------------------------------
```

■ 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。

```
------------------------------------------------------------
# show system
System Contact         :
System Name            : abc
System Location        :
Software Version       : 10-P Ver:1.00.00
Software Date          : 2012-08-17T14:31:24+08:00
MAC Address            : 00-17-2E-15-FB-8C
Number of Ports        : 10
Previous Restart       : Cold

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

32) show trunk command

本機のトランク設定情報を表示します。

```
------------------------------------------------------------
# show trunk ?
  all              Shows all Trunking Group Configuration
  <cr>
------------------------------------------------------------
```

■ show trunk:

システムのトランク情報を表示します。

```
------------------------------------------------------------
# show trunk
Aggregation Configuration:
==========================
Aggregation Mode:

SMAC           : Enabled
DMAC           : Disabled
IP     : Enabled
Port   : Enabled
------------------------------------------------------------
```

■ **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。

```
---------------------------------------------------------------
# show trunk all
Aggr ID  Name    Type   Configured Ports  Aggregated Ports
------   ------     ------   ------------     -------------
1        LLAG1         Static  1,2              None
---------------------------------------------------------------
```

33) show users command

ユーザの設定情報を表示します。

```
---------------------------------------------------------------
# show users
Users Configuration:
====================
User Name                    Privilege Level
-----------------------------------------
admin                          3
ad01                            3
op01                           2
gu01                           1
---------------------------------------------------------------
```

34) show version command

システムのバージョン、およびモデル情報を表示します。

```
---------------------------------------------------------------
# show version
Software Version: 10-P Ver:1.00.00
Software Date   : 2012-08-17T14:31:24+08:00
Number of Ports : 10
---------------------------------------------------------------
```

35) show vlan command

本機の VLAN 設定画面を表示します。

```
---------------------------------------------------------------
# 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>
---------------------------------------------------------------
```

■ **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。

```
------------------------------------------------------------
# show vlan
TPID is 0x88A8

VID   VLAN Name          Ports
----  -------------------------------  -----
1     default             1-10
10    aaa                  None

VLAN forbidden port list:
=========================
VID   VLAN Name          Ports
----  -------------------------------  -----
10    aaa                2
------------------------------------------------------------
```

■ **show vlan id ”x”:**

VLAN ”x”の VLAN 設定画面を表示します。

・ ”x”:VLAN ID です、

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **show vlan isolation:**

ポートの切り分けに(isolation)設定画面を表示します。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **show vlan name “xxx”:**

VLAN “xxx”の VLAN 設定画面を表示します。
“xxxx”は VLAN 名。

```
------------------------------------------------------------
# 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
------------------------------------------------------------
```

■ **show vlan port-based:**

Port-Based VLAN 設定画面を表示します。

```
------------------------------------------------------------
# show vlan port-based
PVLAN ID  Ports
--------     -----
1         1-10
------------------------------------------------------------
```

■ **show vlan voice:**

Voice VLAN 設定画面を表示します。

```
------------------------------------------------------------
# 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
-------------       -----------

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

1.3 ソフトウェアのアップデートおよびバックアップ

本機では、ソフトウェアのアップデートおよび設定のバックアップ/アップデート/リストアを行うことができます。

1.3.1 コンソール/telnetコマンドによるアップデート

TFTP プロトコル、および“copy”コマンドを使って設定します。詳細については、“*copy*”コマンドを参照してください。

本機では、ファームウェアのバックアップ機能をサポートしています。現在まで使用していたFW は、代替 FW(バックアップ FW)になり、新規ファームウェアの FW が“Active”になります。

1.4 Telnet/SNMP管理

1.4.1 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、次に接続されているデバイスから"telnet <IP>"コマンドを使って、本機に接続します。
コンソール画面を使って、操作を行ってください。

1.4.2 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 章 WEB による設定方法

2.1 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 動作環境

本製品の動作環境は、下記のとおりです。

❑本製品の対応 OS:
- Windows 10/11（32 ビット/64 ビット）
- MacOS

❑対応ブラウザ
- Microsoft Edge
- Google Chrome:
- Firefox :

※最新の対応情報は、当社ホームページをご確認ください。

2.3 設定方法(Configuration)

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、192.168.1.1 に設定されています。)

■ **Step 3. 認証用アクセス画面で「ユーザ名」と「パスワード」を入力します。**
(初期設定時は「ユーザ名」と「パスワード」ともに"admin"となります。)

初期設定値

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	admin

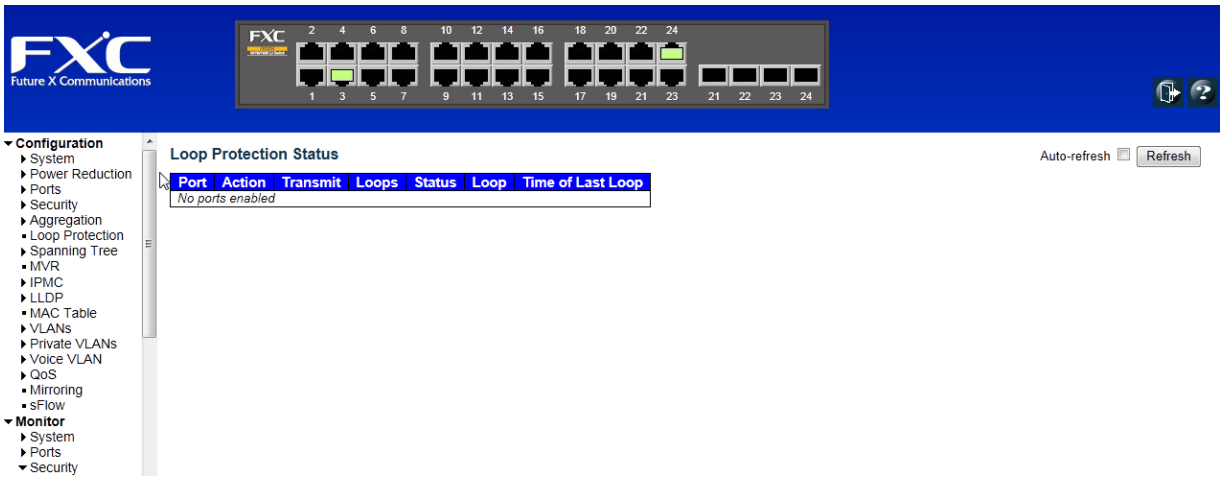
認証用アクセス画面

【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 ブラウザは対応ブラウザをご使用ください。
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。

■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。



■設定/表示項目

1) トップメニューウィンドウ

本製品のインターフェースが表示されており、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メニューを表示します。
Auto-Logout からは自動的に WEB マネジメントからログアウトする時間を設定します。
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。
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。

2) 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。

3) メインウィンドウ

メニューウイン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。

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。

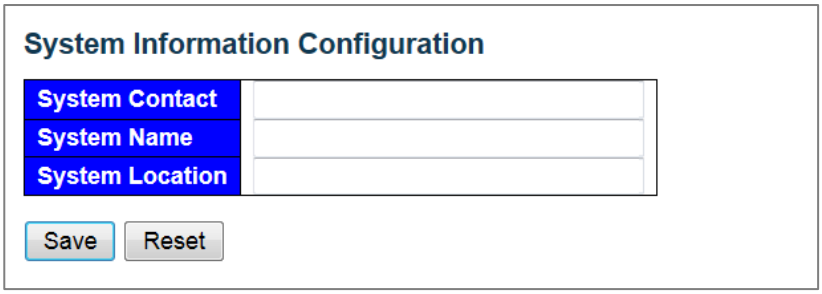
 ヘルプ情報を入手することができます。

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。

2.3.1 システム情報設定(system)

1) システム情報の設定(Information)

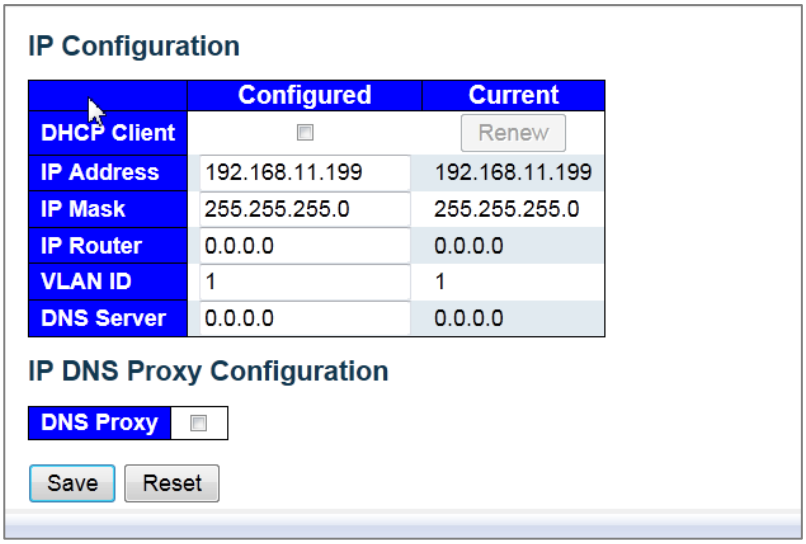
システム名、設置場所、システム担当者を設定します。
[Configuration] →[System] →[Information]をクリックします。



2) IP 設定方法(IP)

本機の IPを設定します。

[System] →[IP]をクリックします。

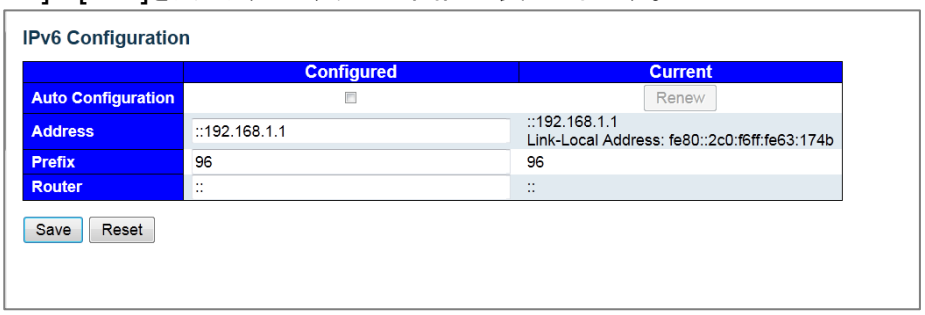


DHCP クライアント機能を有効にすると、DHCP サーバから自動的に IP が設定されます。DHCP クライアント機能を無効にすると、IP を手動にて設定を行うことができます。

3) IPv6 の設定方法(IPv6)

本機のIPv6 の設定を行います。

[System]→[IPv6]をクリックすると、以下の画面が表示されます。

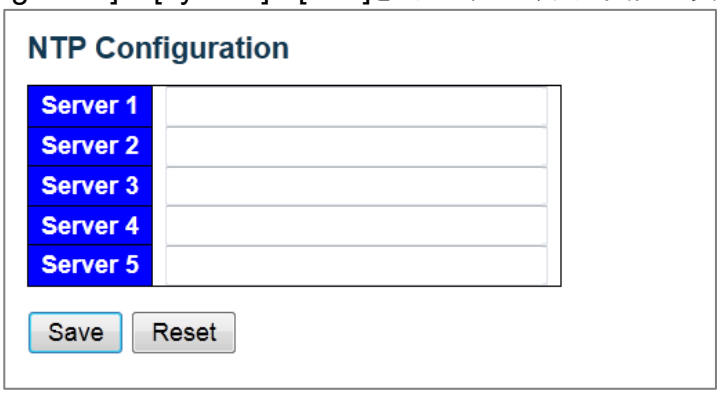


IPv6 ルータが接続されている状態の場合、「Auto Configuration」機能を有効にすると、自動的に IP が設定されます。

または、手動で IP を設定することができます。

4) NTP の設定(NTP)

NTPサーバの設定を行います。
[Configuration] →[System]→[NTP]をクリックすると、次の画面が表示されます。



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(システム時刻の同期)ができます。事前に NTP サーバの IP を入手する必要があります。

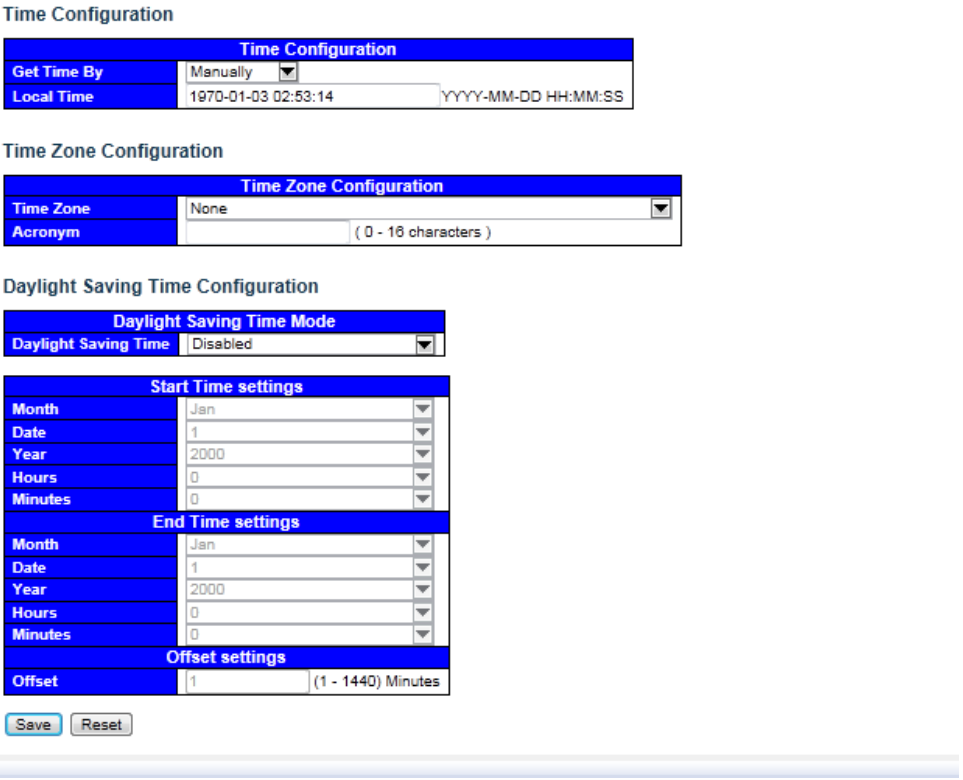
機能を有効にするには、[Configuration]→[System]→[Time]ページで[Time Configuration]を[Time Server]に設定します。入力した後、[Save]ボタンをクリックします。
NTP サーバの IP アドレスを入力します。
入力した後、[Save]ボタンをクリックします。

次に、[Configuration]→[System]→[Time]ページをクリックすると、タイムゾーンおよびサマータイム(デイライトセービングタイム)の設定を行います。

5)　システム時刻設定(Time)

時刻の設定をするには、[Configuration]→[System]→[Time]をクリックします。

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た現在の時刻を表示するには、タイムゾーンの設定を行ってください。



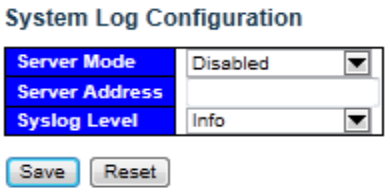
「Time Configuration」でシステム時刻の手動設定もしくは、自動設定を選択します。
手動設定の場合は、システム時刻の調整ができます。

「Time Zone Configuration」でローカルタイム/ローカルタイム名を設定します。
例：「TimeZone」：(GMT+9:00) Osaka,Sapporo,Tokyo
　　「Acronym」：JST

サマータイム(デイライトセービングタイム)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により、タイムを分割することが可能です。

6) ログ情報（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。



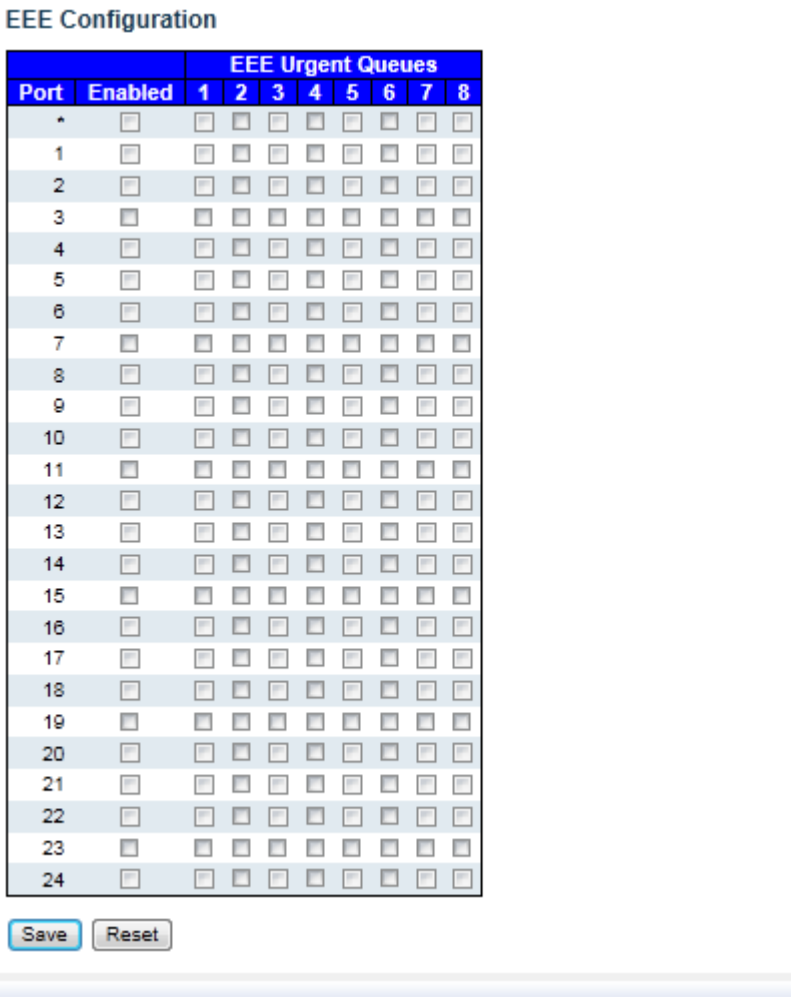
サーバアドレスに Syslog サーバのアドレスを設定します。これにより、syslog サーバへイベントが送信されます。
本機の DNS 機能が有効な場合は、ホスト名としても使用可能です(IPv4 のみ対応)。

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 消費電力制御（EEE）機能設定（Power Reduction）

消費電力制御（EEE）を設定するには、[Configuration]→[Power Reduction]→[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、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、データを入手次第、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 ポートの設定(Ports)

ここでは、ポートのリンク状態の確認や、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。

1) ポートの設定(Ports)

Port Configuration

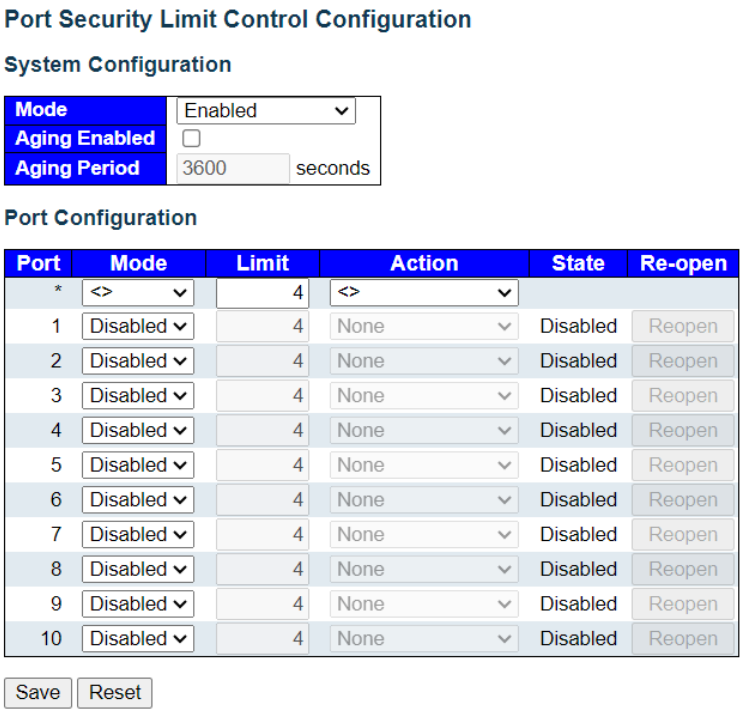
Port	Link	Speed		Flow Control			Maximum	Excessive	Power	MDI/
		Current	Configured	Current Rx	Current Tx	Configured	Frame Size	Collision Mode	Control	MDI-X
*			<>				9600	<>	<>	<>
1		Down	Auto	×	×		9600	Discard	Disabled	Auto
2		1Gfdx	Auto	×	×		9600	Discard	Disabled	Auto
3		Down	Auto	×	×		9600	Discard	Disabled	Auto
4		Down	Auto	×	×		9600	Discard	Disabled	Auto
5		Down	Auto	×	×		9600	Discard	Disabled	Auto
6		Down	Auto	×	×		9600	Discard	Disabled	Auto
7		Down	Auto	×	×		9600	Discard	Disabled	Auto
8		Down	Auto	×	×		9600	Discard	Disabled	Auto
9		Down	Auto	×	×		9600	Discard	Disabled	Auto
10		Down	Auto	×	×		9600	Discard	Disabled	Auto
11		Down	Auto	×	×		9600	Discard	Disabled	Auto
12		Down	Auto	×	×		9600	Discard	Disabled	Auto
13		Down	Auto	×	×		9600	Discard	Disabled	Auto
14		Down	Auto	×	×		9600	Discard	Disabled	Auto
15		Down	Auto	×	×		9600	Discard	Disabled	Auto
16		Down	Auto	×	×		9600	Discard	Disabled	Auto
17		Down	Auto	×	×		9600	Discard	Disabled	Auto
18		Down	Auto	×	×		9600	Discard	Disabled	Auto
19		Down	Auto	×	×		9600	Discard	Disabled	Auto
20		Down	Auto	×	×		9600	Discard	Disabled	Auto
21		Down	SFP_Auto_AMS	×	×		9600	Discard	Disabled	Auto
22		Down	SFP_Auto_AMS	×	×		9600	Discard	Disabled	Auto
23		Down	SFP_Auto_AMS	×	×		9600	Discard	Disabled	Auto
24		1Gfdx	SFP_Auto_AMS	×	×		9600	Discard	Disabled	Auto

Save　Reset

ポートの設定(Port Configuration)	
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を設定します。
Maximum Frame Size	最大フレームサイズ(ジャンボフレーム)を設定します。変更する場合は、接続先のネットワーク機器がジャンボ機能に対応しているか確認してください。
Power Control	下記のとおり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。ショートケーブルを使用時に消費電力が有効になります。 - 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	UTP ポートの MDI/MDI-X モードを設定します。 「MDI-X」はパソコン等の終端装置用、「MDI」はスイッチ等の中継装置用です。「Auto」に設定すると、自動検知を行います。

2) リミットコントロール(Limit Control)

「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。

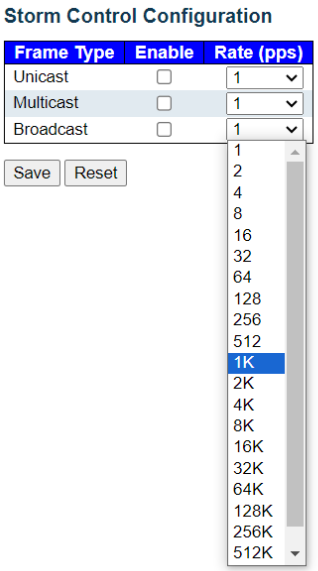


ここでは、ポートセキュリティのリミットコントロール機能を設定します。
リミットコントール機能: 指定ポートのユーザ数を制限することができます。MAC アドレスおよび VLAN ID を使ってユーザを識別することができます。
リミットコントール機能を有効にすると、ポートのユーザの上限を指定することができます。

この上限を超えると、以下のような 4 つの異なる処理の 1 つが行われます。。
- None : 上限を超過した場合ユーザ接続を許可しません。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。

3) ストームコントロール(Storm Control)

「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。

設定可能な値は、1pps～1024Kpps(パケット/秒)です。

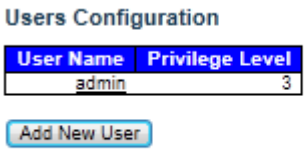
2.3.4 セキュリティ設定(Security)

セキュリティ機能の設定を行います。

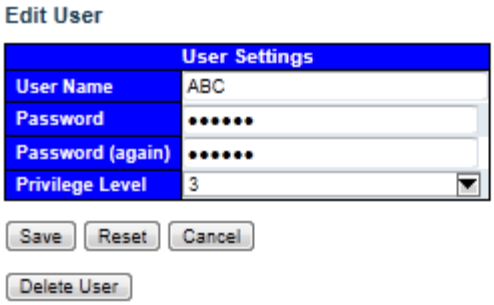
2.3.4.1 スイッチの管理設定（switch）

1) ユーザの設定(users)

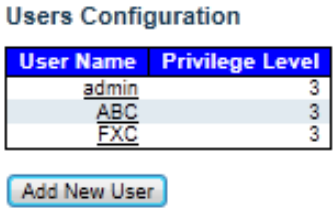
[configuration]→[Security]→[Switch]→[Users]をクリックします。



<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、それぞれ設定を行ってください。



<Save>ボタンをクリックするとユーザ設定画面が表示されます。

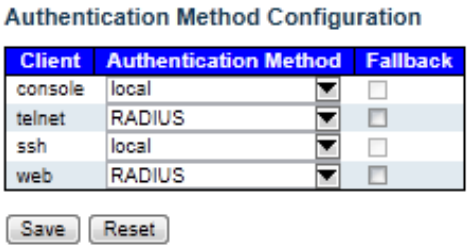


本機のユーザ情報を設定します。
ユーザのレベルには、以下のとおり 3 段階あります。

- 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。

2)　認証設定(Auth Method)

[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。

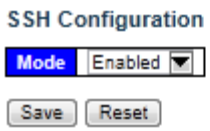
認証方式は、以下のとおりです。
- none: 認証は可能ですが、ログインは不可です。
- local: 本機のローカルユーザ情報の認証のみ可能です。
- radius: 認証用のリモート RADIUS サーバを設定します。
- tacacs+:認証用のリモート TACACS+サーバを設定します。

Fallback を選択すると、認証失敗した場合、ローカルのユーザデータで認証します。

RADIUS サーバおよび TACACS+サーバの設定方法については、
[Configuration]→[Security]→[AAA page]を参照してください。

3)　SSH 設定(SSH)

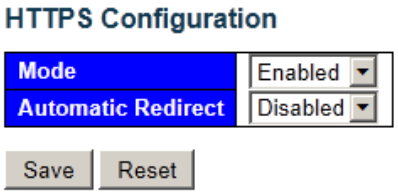
[Configuration]→[Security]→[Switch]→[SSH]をクリックすると、以下の画面が表示されます。



ここでは、リモート Telnet 用に SSH 機能を設定します。

4)　HTTPS 設定(HTTPS)

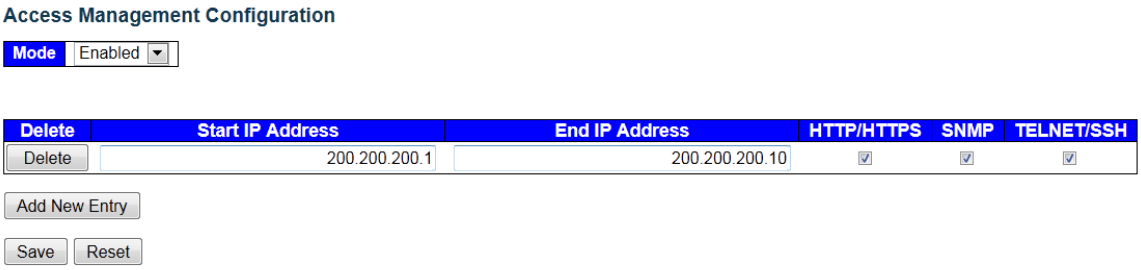
[Configuration]→[Security]→[Switch]→[HTTPS]をクリックすると、以下の画面が表示されます。



ここでは、WEB の HTTPS セキュリティ機能を有効にします。
「Automatic Redirect」: HTTPS モードおよび「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 の設定(Access)

Access Managemen を設定するには
[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。



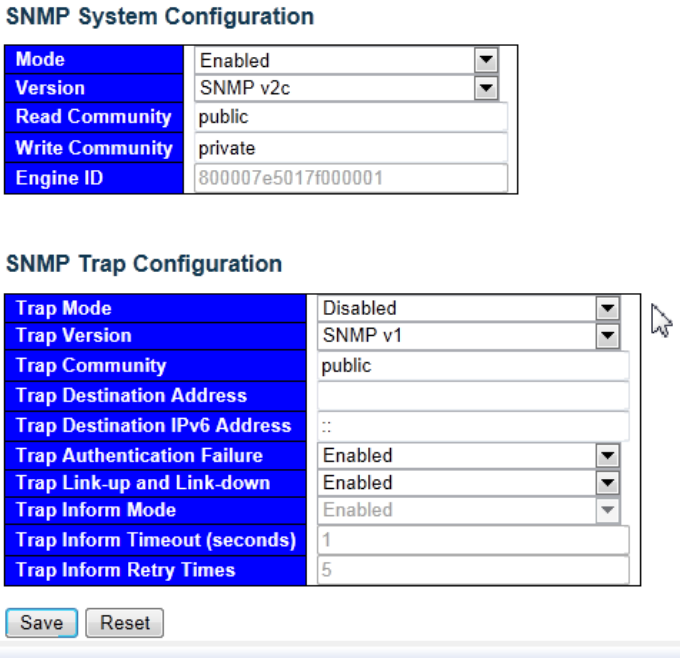
ここでは、リモート管理用に IP アドレスのレンジを設定することが可能です。リモート管理用インターフェースは、HTTP/HTTPS、SNMP、TELNET/SSH です。

6) SNMP 設定 (SNMP)

SNMP 設定を行います。

6-1) SNMP システムの設定(system)

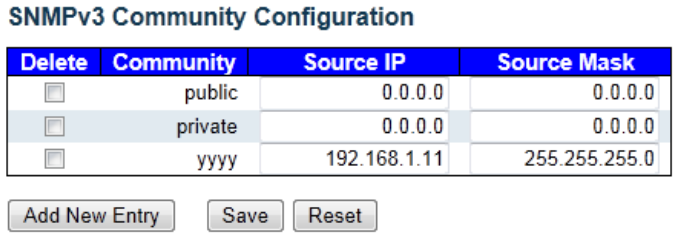
[Configuration]→[Security]→[Switch]→[SNMP]→[System]をクリックすると、以下の画面が表示されます。



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) SNMPv3 コミュニティの設定方法(communities)

[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。



SNMPv3 コミュニティのエントリの追加/削除を行うことができます。

6-3) SNMP ユーザを設定(users)

[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。

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Add New Entry　Save　Reset

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) SNMPv3 グループの設定(Groups)

[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。

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

Add New Entry　Save　Reset

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) SNMPv3 View の設定(Views)

[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。

SNMPv3 View Configuration

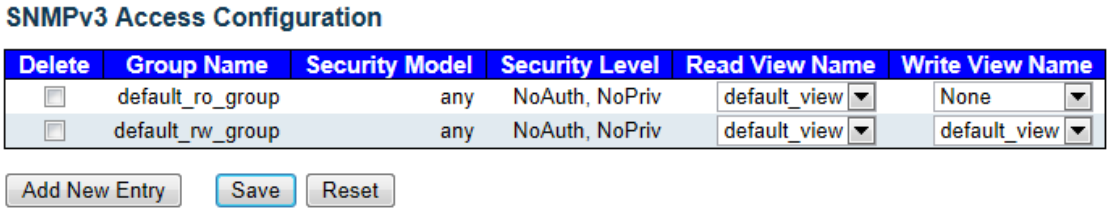
Delete	View Name	View Type	OID Subtree
☐	default_view	included	.1
Delete	abcd	included	.1.3.6.1.2.1.1

Add New Entry　Save　Reset

SNMPv3 ビューのエントリの追加/削除を行うことができます。

6-6) SNMPv3 Access の設定(Access)

[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。



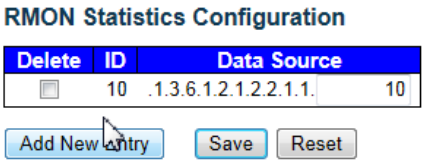
SNMPv3 認証の有/無及び、暗号化の有/無のエントリの追加/削除を行うことができます。

7) RMON 統計情報の設定（RMON）

[Configuration]→[Security]→[Switch]→[RMON]をクリックします。

7-1) RMON 統計情報(Statics)

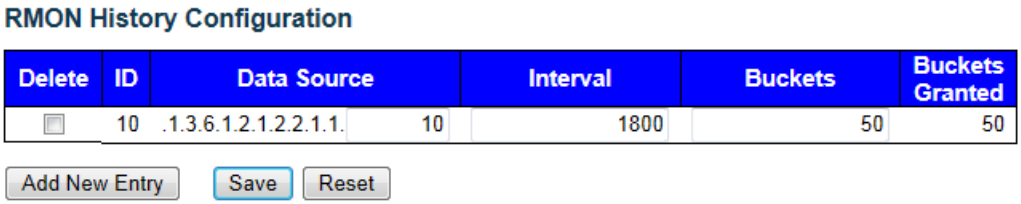
[Configuration]→[Security]→[Switch]→[RMON]→[Statistics]をクリックすると、以下の画面が表示されます。



RMON 統計情報エントリの追加/削除を行うことができます。

7-2) RMON 履歴(History)

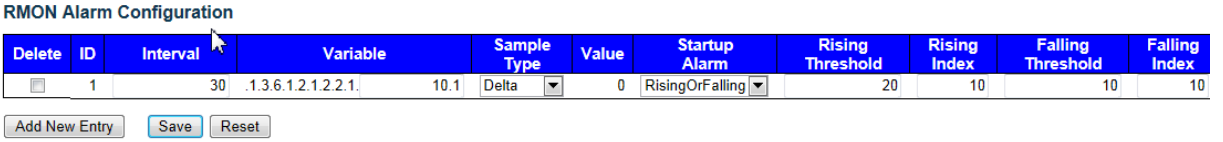
[Configuration]→[Security]→[Switch]→[RMON]→[History]をクリックすると、以下の画面が表示されます。



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) RMON Alarm の設定(Alarm)

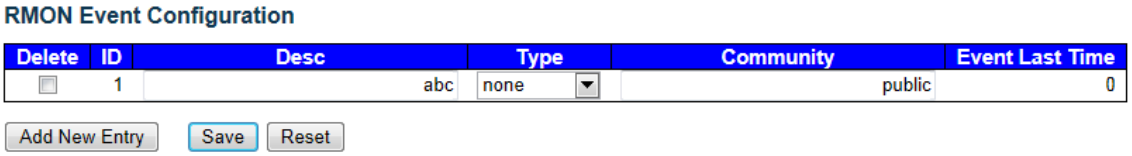
[Configuration]→[Security]→[Switch]→[RMON]→[Alarm]をクリックすると、
以下の画面が表示されます。



RMON 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) RMON イベントの設定(Event)

[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。



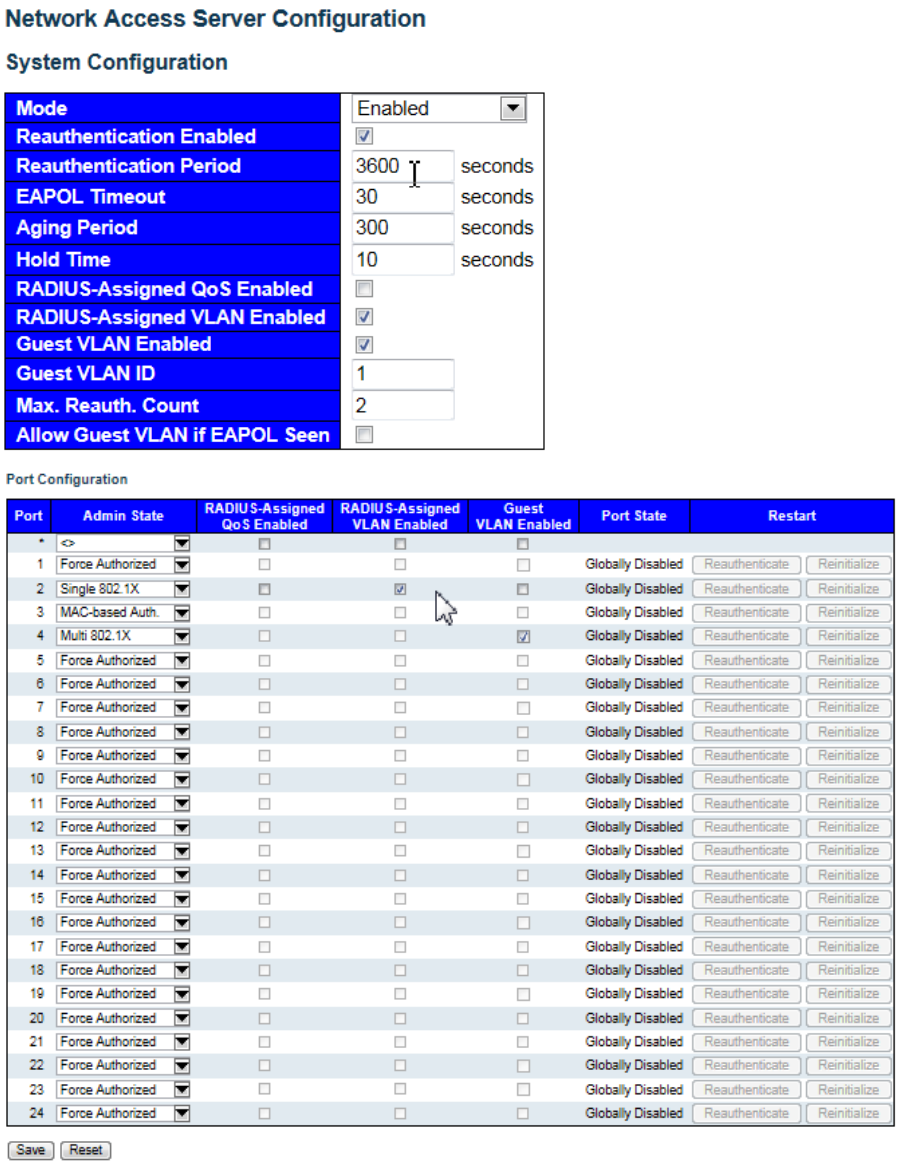
RMON イベントのエントリの追加/削除を行うことができます。

2.3.4.2 ネットワークの設定(Network)

ネットワークの設定を行います。

1) NAS(Network Access Server)の設定（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。



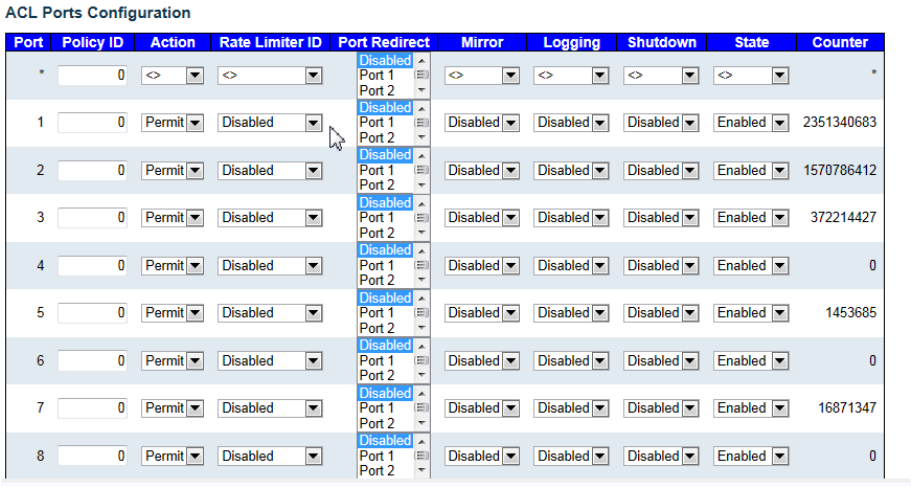
802.1x ネットワークアクセス制御機能を設定します。ポートを介するネットワークアクセスにはまずユーザの認証が必要になります。RADIUS サーバにより認証を行います。
RADIUS 等の認証サーバを設定するには、[Configuration]→[Security]→[AAA page]より行います。

2)　ACL の設定(ACL)

ここでは、ACL(アクセスコントロールリスト)の設定を行います。

2-1)　ACL のポートの設定(Ports)

ACL のポートを設定するには、
[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。

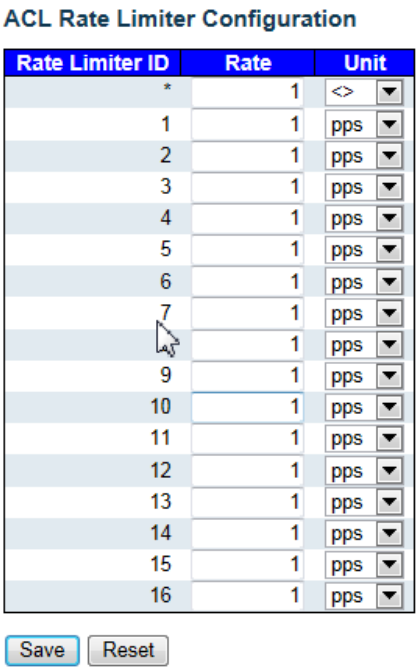


ここでは、各ポートの ACL パラメータ(ACE)を設定します。
これらのパラメータは、フレームが特定の ACE と一致しない場合は、これらのパラメータに応じてフレームの受信が有効/無効になります。

-Action: ポートのデータ伝送が許可("permit")、または拒否("deny")されます。
-RateLimiter:受信フレームの帯域制御レートリミット機能(無効/ID(1～16)を行います。
-Port Redirect: 該当フレームの対象のポートへトラフィックリダイレクトを行います。
-Mirror:ミラーリングを行うポートでの該当フレーム受信を有効にします。
-Logging:システムログに記録する機能を有効にします。
-shutdown：該当フレームを受信するとポートを無効にします。
-state：ACL の状態を有効/無効にします。

2-2) 帯域制御(レートリミット)機能の設定(Rate Limiters)

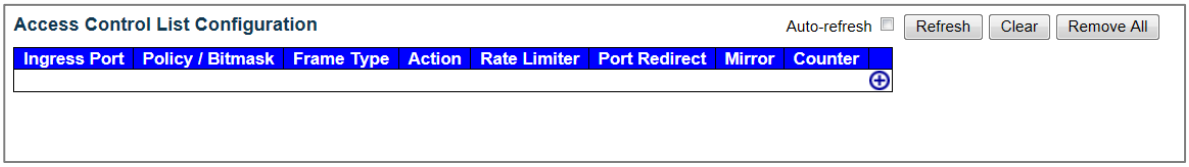
[Configuration]→[Security]→[Network]→[ACL]→[Rate Limiters]をクリックすると、以下の画面が表示されます。



ACL のレートリミットを定義します。
レートリミット機能は、pps(パケット/秒)、または kbps (キロビット/秒)単位で定義されます。
受信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、実際の設定値と異なるレートになる場合があります。

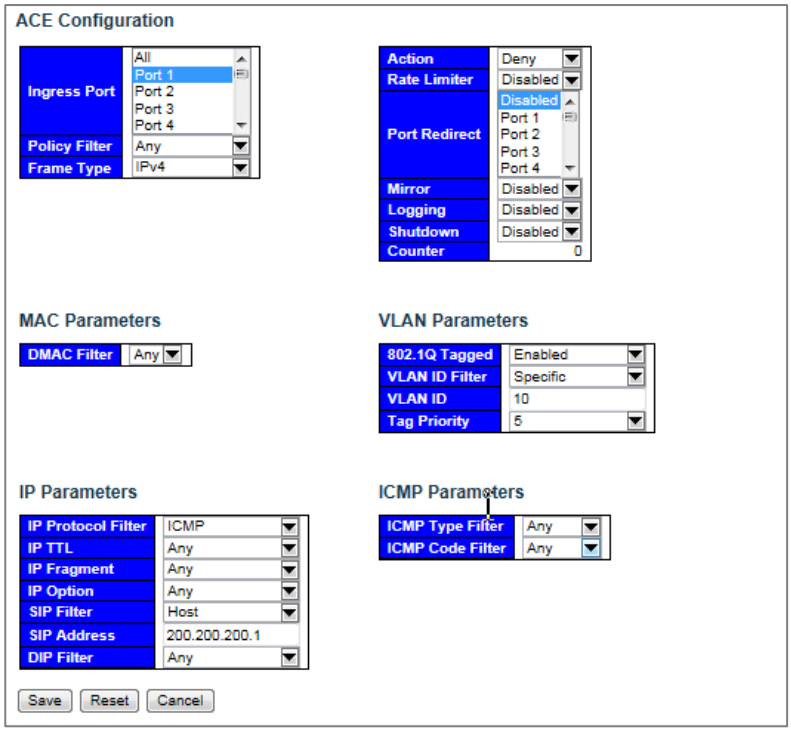
2-3) アクセス制御リストの設定(Access Control List)

[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。

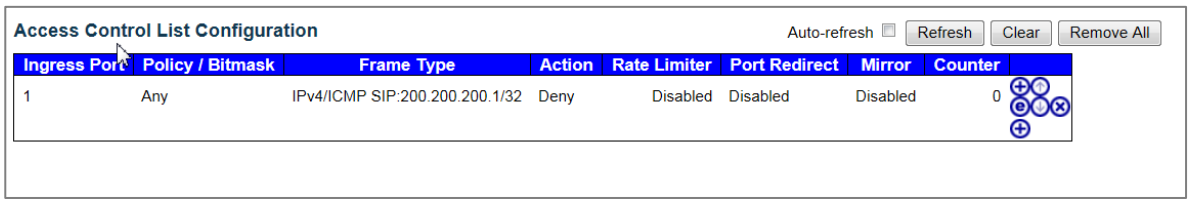


アクセス制御リストを設定するには、“(+)”をクリックします。

“(+)”をクリックすると、以下の ACE(Access Control Entry)設定画面が表示されます。



パラメータに一致すると、ACE のパラメータを定義し、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。



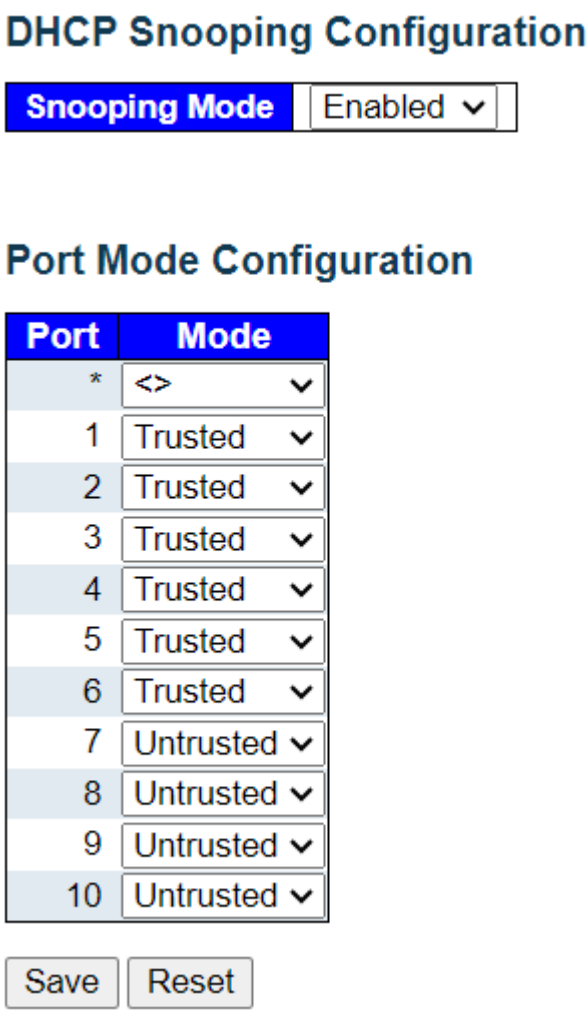
(+)をクリックすると、別の ACE が追加されます。(e)をクリックすると ACE の編集、(x)をクリックすると ACE が削除されます。
(↑)/(↓) を使用することにより、ACE を移動し優先順を変更します。

3)　DHCP

DHCP機能の設定を行います。

3-1) DHCP スヌーピング機能(Snooping)

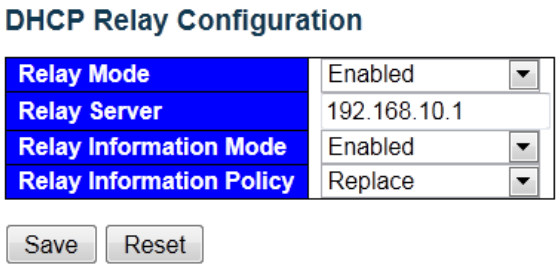
DHCP スヌーピング機能を設定するには、
[Configuration]→[Security]→[Network]→[DHCP]→[Snooping]をクリックすると、
以下の画面が表示されます。



「Snooping Mode」で機能の有効/無効を設定します。
DHCP スヌーピング機能を有効にすると、DHCP サーバからの DHCP 応答メッセージは Trusted(信頼)ポートからのみ転送され、Untrusted(不信)ポートに接続された不正な DHCP サーバから保護することができます。
DHCP クライアントを Untrusted(不信)ポートに接続してもDHCP要求メッセージはブロックされません。

3-2) DHCP リレー機能(Relay)

DHCP リレー機能を設定するには、
[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、リレー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、同じサブネットドメインの DHCP ブロードキャストメッセージはリレー(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、DHC 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 の回路 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。

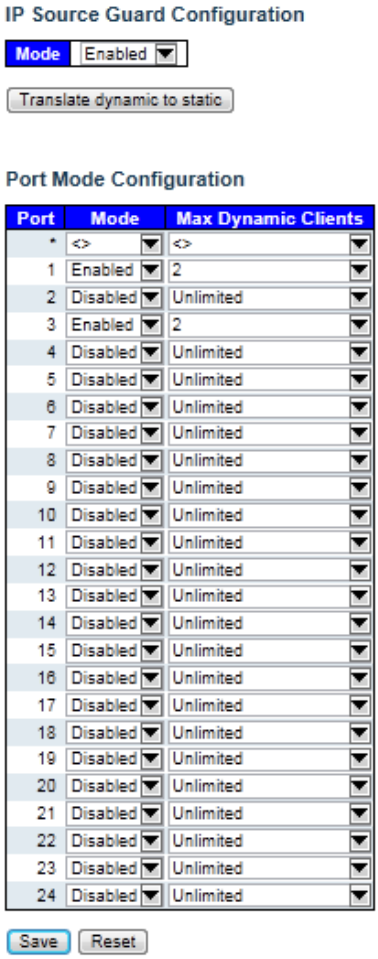
有効なポリシーは、以下のとおりです。
Drop ：リレー情報を含む DHCP メッセージ パケットは破棄されます。
Keep ：リレー情報を含む DHCP メッセージを変更せずにそのまま転送します。
replace: リレー情報を含む DHCP メッセージを上書き/変更して転送します。
リレー情報が無効な場合、'replace'オプションは無効となります。

4)　IP ソースガード(IP Source Guard)

IP ソースガード機能の設定を行います。

4-1)　IP Source Guard の設定(Configuration)

[Configuration]→[Security]→[Network]→[IP Source Guard]→[Configuration] クリックすると、以下の画面が表示されます。



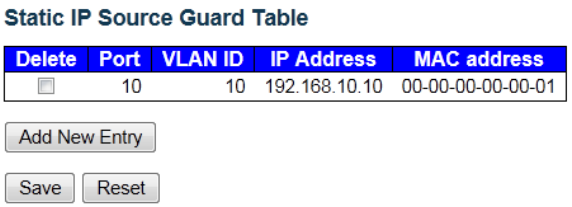
IP ソースガードは、DHCP スヌーピングテーブルに応じて、トラフィックのフィルタリングを行ったり、IP ソースブリッジを手動でバインドすることにより、DHCP スヌーピングの Untrusted ポートの IP トラフィックを制限します。

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。

4-2) IP ソースガードスタティックテーブル追加(Static Table)

[Configuration]→[Security]→[Network]→[IP Source Guard]→[Static Table]クリックすると、以下の画面が表示されます。



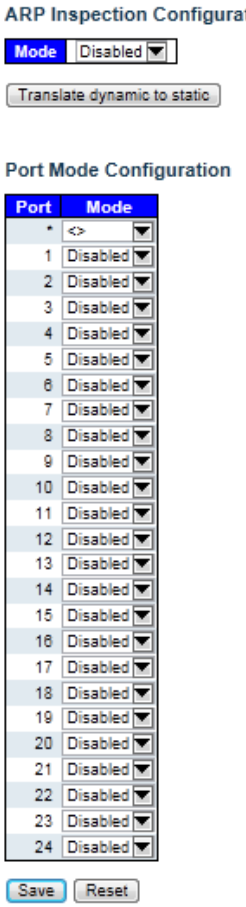
スタティック IP ソースのエントリの追加/削除を行います。スタティック IP ソースエントリは、ポート、VLAN ID、IP アドレス、Mac アドレスから構成されます。このスタティックテーブルを使って、別のホストの IP アドレスの不正使用を行う場合防ぐことができます。

5) ARP インスペクション機能(ARP Inspection)

ARPインスペクション機能の設定を行います。

5-1) ARP インスペクション機能(Configuration)

[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。

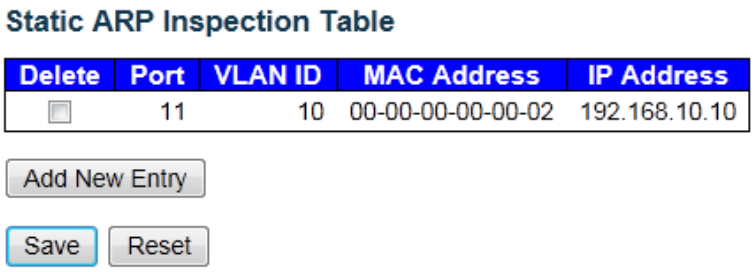


ARP インスペクションは、ネットワークの ARP パケットを確認するセキュリティ機能です。ARP キャッシュをポイズニングすることにより、レイヤ 2 ネットワークに接続されているホスト、またはデバイスが攻撃を受けた場合、この機能はそれらの攻撃をブロックするためのものです。有効な ARP リクエストおよび応答のみスイッチへの通信が可能です。

【注記】:
ダイナミック ARP エントリは DHCP リクエストにより学習します。ARP インスペクションを有効にする前に、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、ARP インスペクション機能に対して、スタティック ARP エントリを設定してください。

5-2) スタティックテーブルの設定(Static Table)

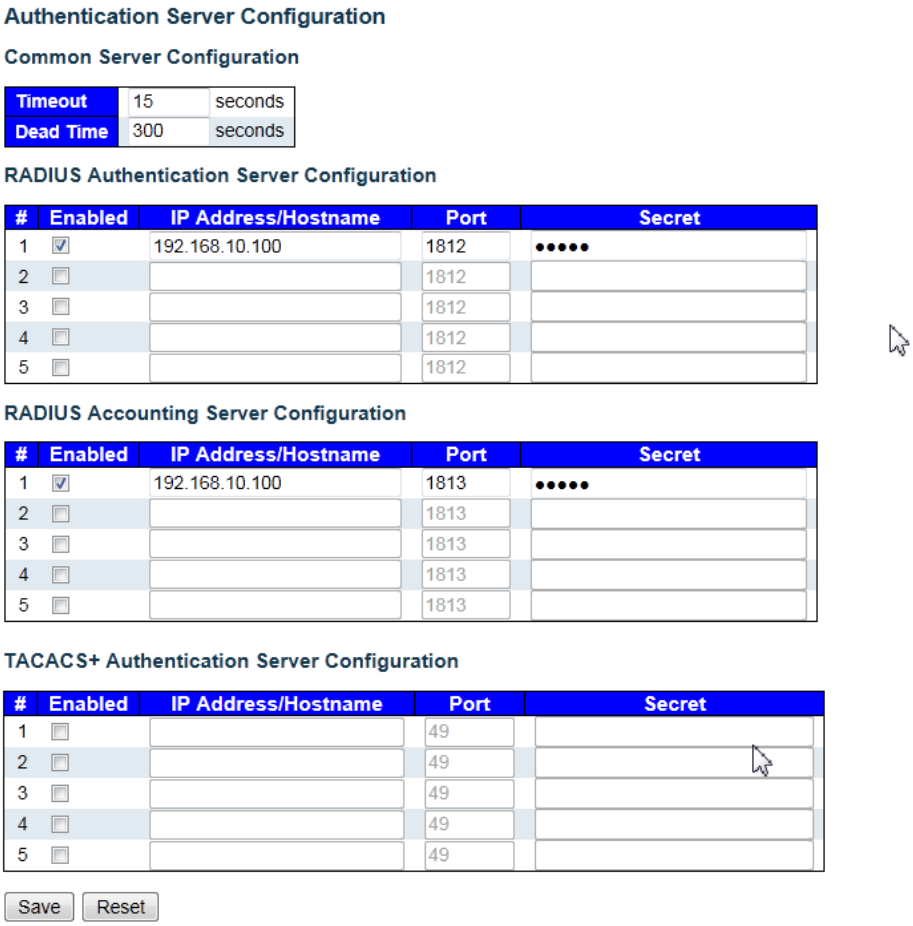
スタティックテーブルを設定するには、[Configuration]→[Security]→[Network]→[ARP Inspection]→[Static Table]をクリックすると、以下の画面が表示されます。



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 機能（AAA）

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。

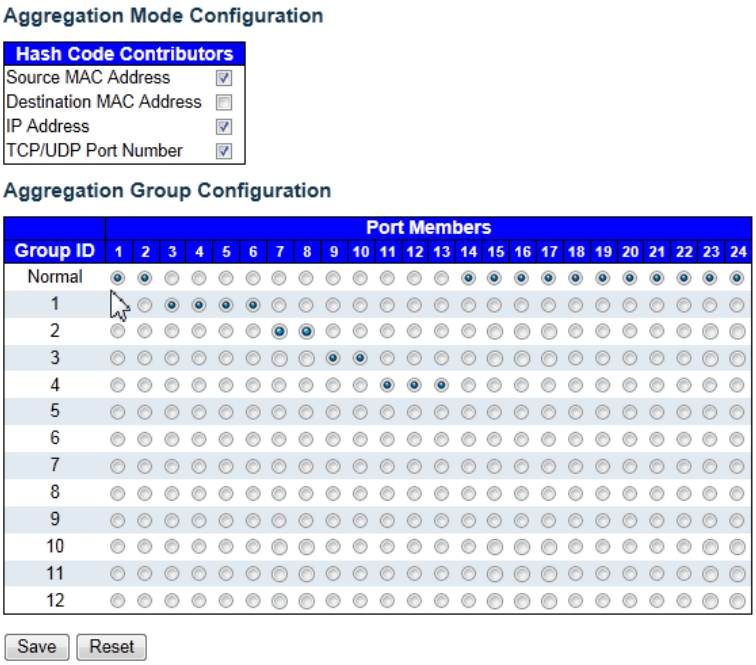


2.3.5 アグリゲーション設定(Aggregation)

アグリゲーション機能の設定を行います。

2.3.5.1 スタティックアグリゲーション機能の設定(Static)

[Configuration]→[Aggregation]→[Static]をクリックすると、以下の画面が表示されます。



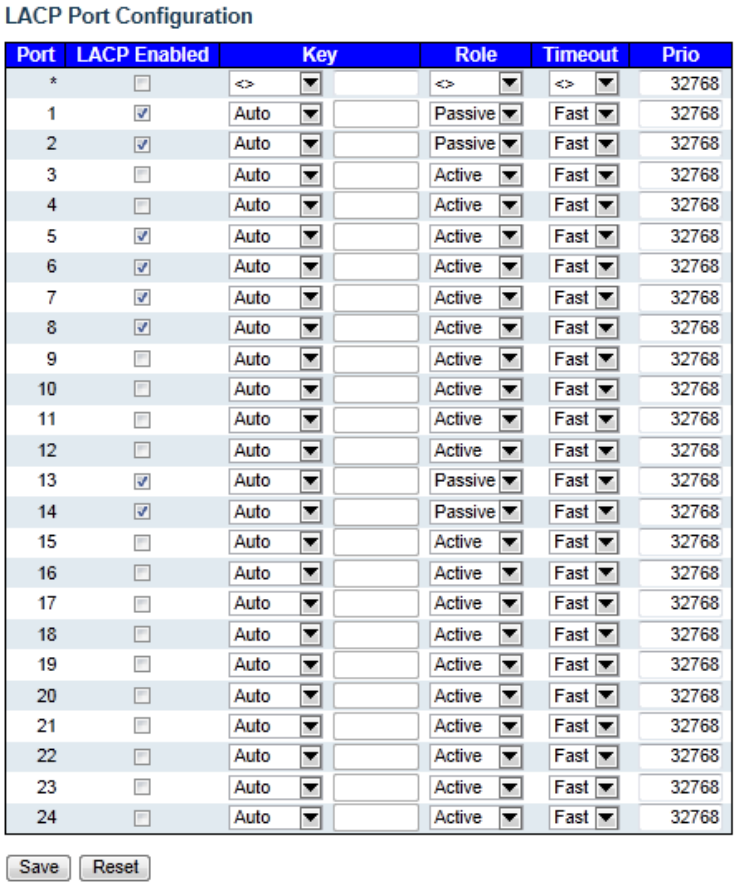
Aggregation Hash モード、及び、スタティックアグリゲーショングループを設定します。

Hash Code Contributors は、
source_mac_address:送信元 MAC アドレスを使って、送信ポートを算出します。
destination_mac_address:宛先 MAC アドレスを使って、送信ポートを算出します。
ip_address:IP アドレスを使って、送信ポートを算出します。
tcp/udp_port_number:TCP/UDP ポート番号を使って、送信ポートを算出します。

スタティックアグリゲーショングループは「最大ポート数÷2」まで設定可能です
（例えば、FXC5224 の場合は、「最大 12 グループ」まで設定可能)。

2.3.5.2 LACP 設定(LACP)

LACP 機能を設定するには、[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		Passive	Fast	32768
2	☑	Auto		Passive	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		Passive	Fast	32768
14	☑	Auto		Passive	Fast	32768
15	☐	Auto		Active	Fast	32768
16	☐	Auto		Active	Fast	32768
17	☐	Auto		Active	Fast	32768
18	☐	Auto		Active	Fast	32768
19	☐	Auto		Active	Fast	32768
20	☐	Auto		Active	Fast	32768
21	☐	Auto		Active	Fast	32768
22	☐	Auto		Active	Fast	32768
23	☐	Auto		Active	Fast	32768
24	☐	Auto		Active	Fast	32768

Save　Reset

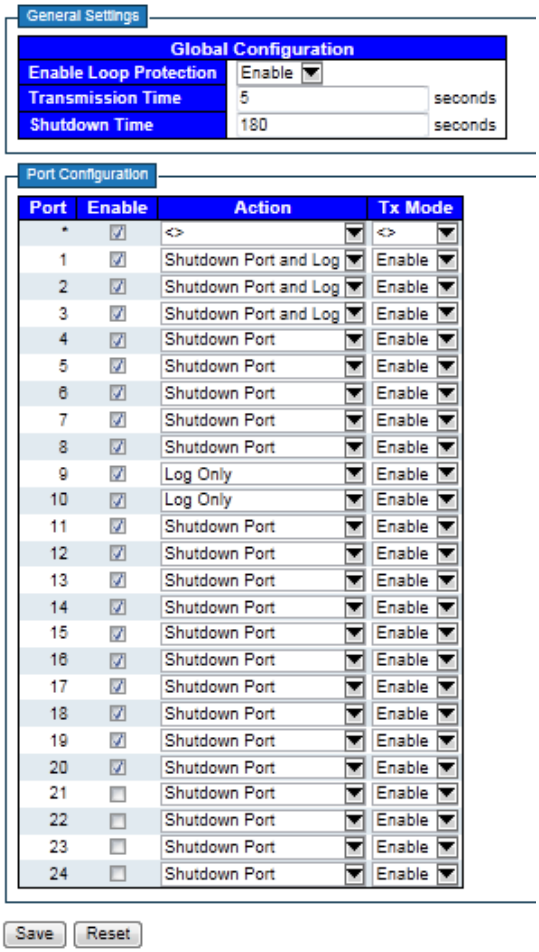
ここでは、アグリゲーション用の LACP 機能を設定します。LACP は、IEEE 802.3ad 規格のプロトコルです。
LACP により、複数の物理ポートを 1 つの論理ポートに束ねることが可能です。
本機2台(または、LACP をサポートしている機器)を使って、LACP 機能を介してアグリゲーション接続を行うことが可能です。

Lacp　Role は、自機/対向機で Active/Avtive もしくは、
Active/Passive(Passive/Active)の組み合わせで設定してください。

Timeout は、
SLOW モードは LACPDU が 30 秒ごとに送信されタイムアウトは 90 秒、
FAST モードは LACPDU が1秒ごとに送信されタイムアウトは3秒となります。

2.3.6 ループ検知/遮断設定(Loop Protection)

ループプロテクションを行うには、[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、ループ検知の PDU を送信します。
ループバックを検出すると、Action に設定した処理が行われます。
- shutdown は、ポートをシャットダウンする。
- shut_log は、ポートをシャットダウンし、ログを送信する。
- log は、ログ送信のみ。

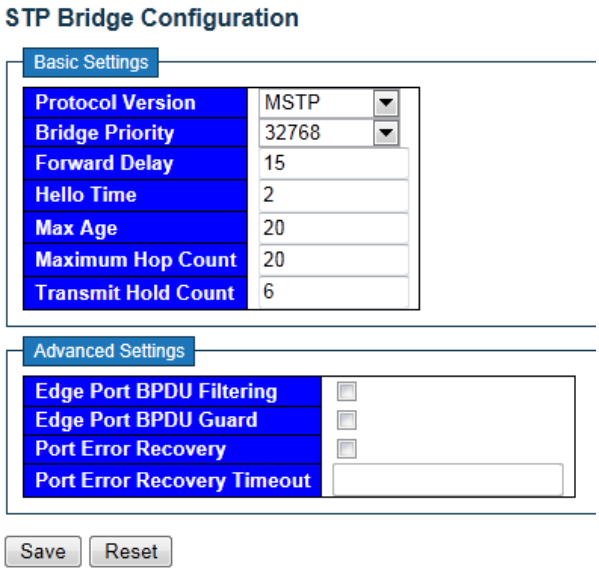
シャットダウンの時間は一定時間ごとに設定可能です。指定の時間を経過するとポートは有効になります。

2.3.7 スパニングツリー設定(spanning-tree)

スパニングツリー機能を設定を行います。

2.3.7.1 STP 機能（Bridge Settings）

[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。



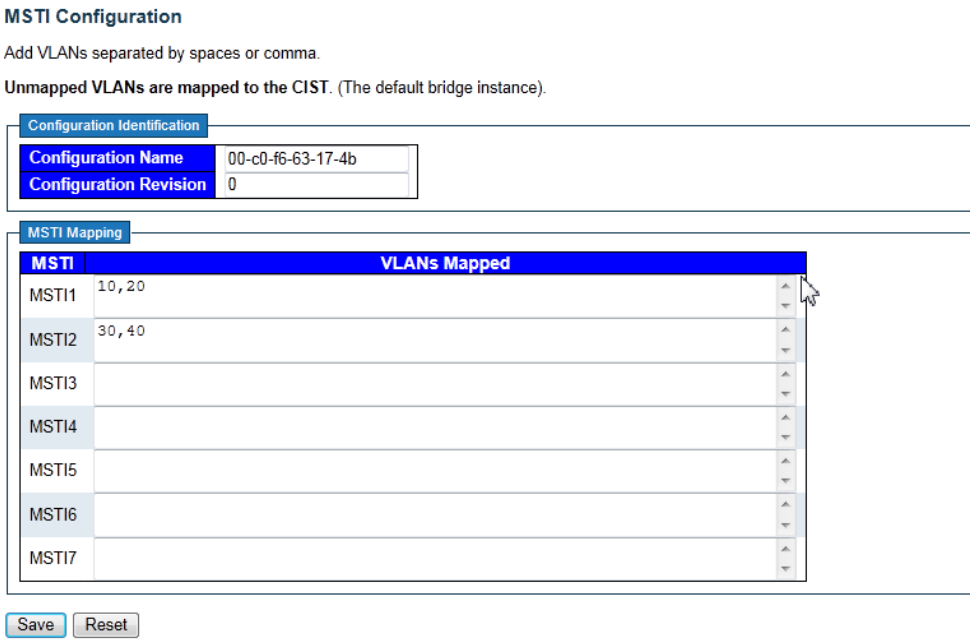
ここでは、スパニングツリーのブリッジの設定を行います。

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。
プロトコルのバージョンを選択することができ、各パラメータの調整を行えます。

Advanced Setting では、BPDU フィルタリング機能、BPDU ガード機能、ポート自動復旧機能を有効/無効に設定できます。
復旧時間は、30 秒から 86400 秒(1 日)で設定が行えます。

2.3.7.2 MSTI/VLAN マッピング(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。

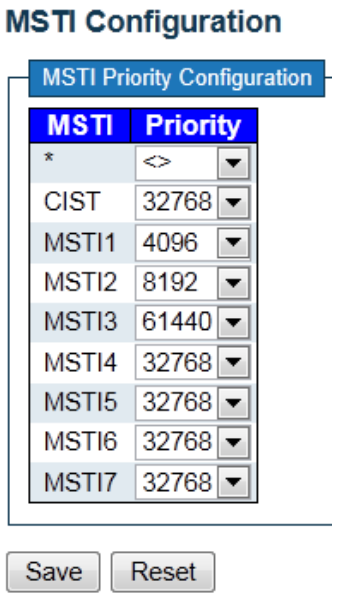


ここでは、MSTI/VLAN 間のマッピングを設定します。

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から構成されます。
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 プライオリティ (MSTI Priorities)

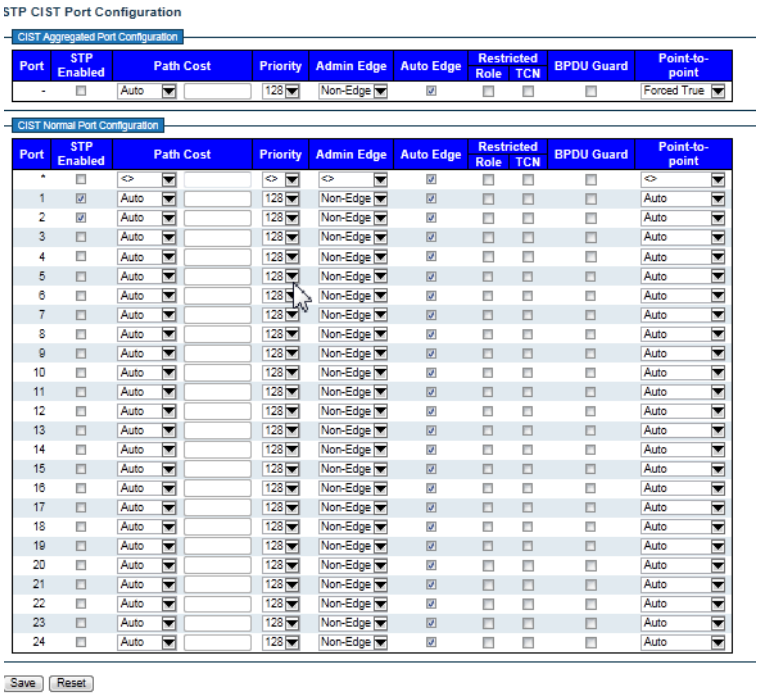
[Configuration]→[Spanning Tree]→[MSTI Priorities]をクリックすると、
以下の画面が表示されます。



ここでは、MSTI ブリッジ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。
0 から 61440 まで 4096 の倍数で設定が行えます。

2.3.7.4 CIST ポートの設定(CIST Port)

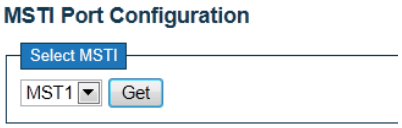
[Ports Configuration]→[Spanning Tree]→[CIST Ports」をクリックすると、以下の画面が表示されます。



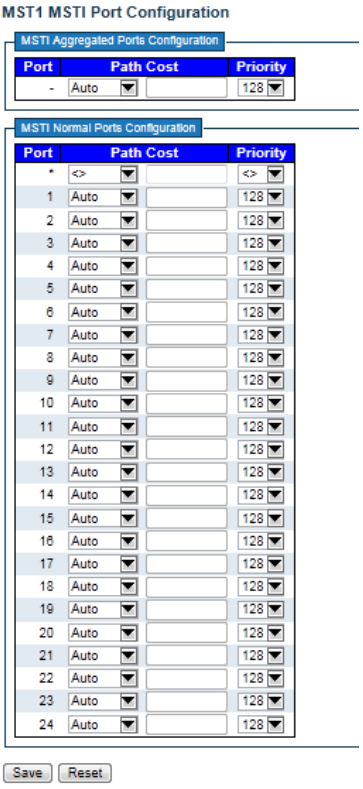
ここでは、ポートのスパニングツリー機能を設定します。

2.3.7.5 MSTI ポート

[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。



「MSTI」を選択して「Get」ボタンをクリックすると、「MSTI Port Configuration」が表示されます。



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。

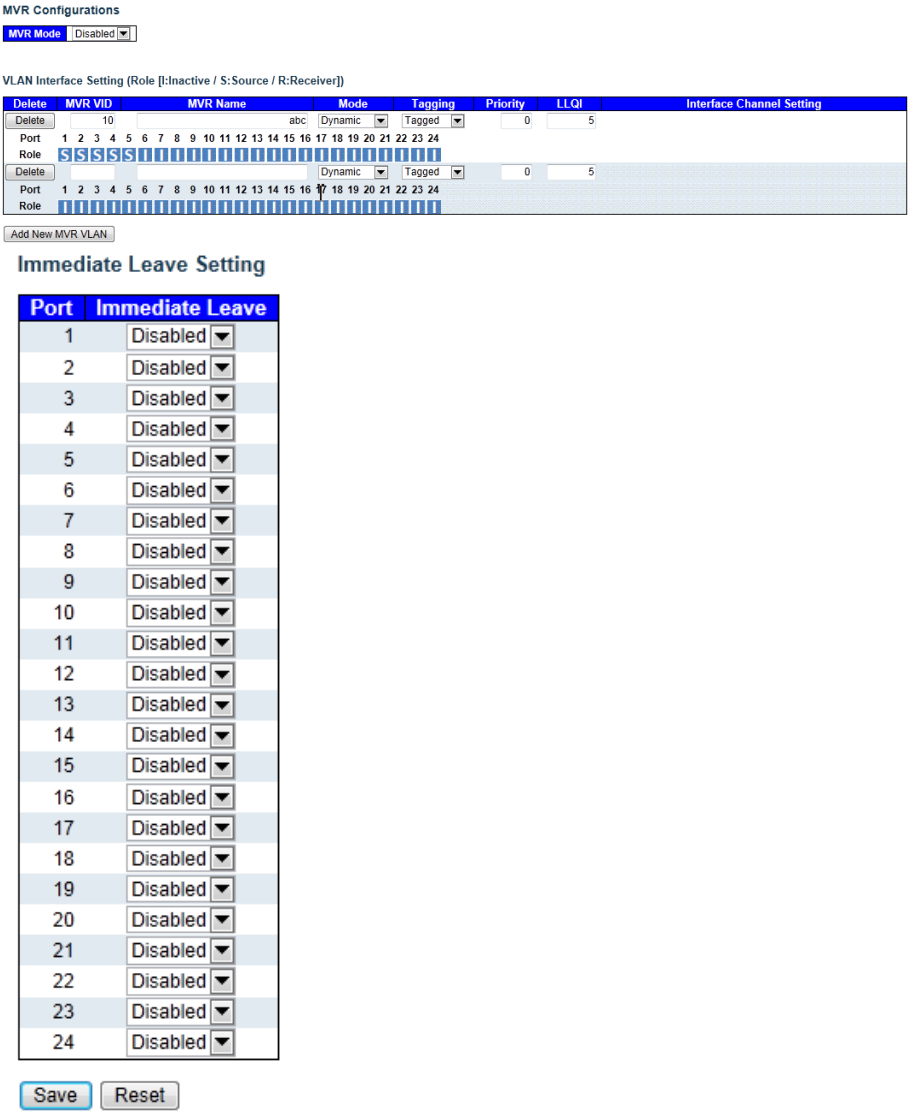
パスコストは、ポートのパスコストを設定します。
パスコストを「Auto」に設定すると、802.1D の推奨値を用いて、物理リンク通信速度に応じて適切なコストを設定します。
パスコストをユーザ定義(Specific)に設定すると、任意の値(1-200000000)が入力可能です。ネットワークのトポロジーを設定時にパスコストを使用します。パスコストの低いポートがルート選出の優先度が高いポートに設定されます。

「Priority」により、ポートのプライオリティが制御されます。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設定(MVR)

MVR(Multicast VLAN Registration)の設定を行います。

[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 を有効して、ポートに VLAN を割り当てます。
Step 2: MVR VLAN の設定を保存(save ボタン)します。
Step 3: (e)をクリックして、VLAN に MVR チャネルを割り当てます。
Step 4:ポートの Immediate Leave 機能を有効/無効にします。

2.3.9 IPマルチキャスト設定(IPMC)

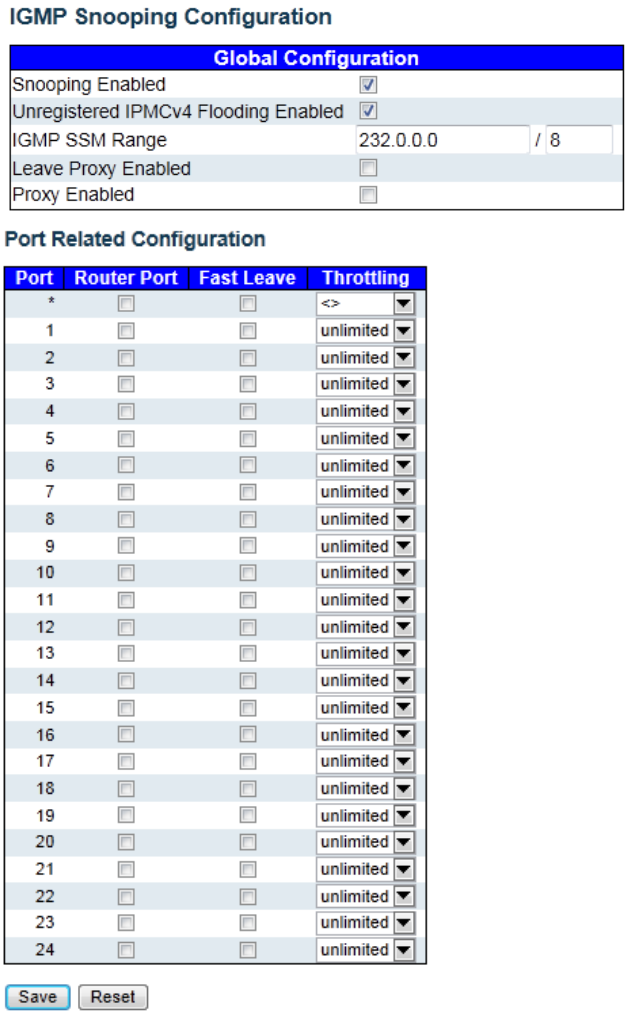
IPMC(IPマルチキャスト)設定を行います。

2.3.9.1 IGMP Snooping の設定

IGMP スヌーピングの設定を行います。

1) 基本設定(Basic Configuration)

[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。

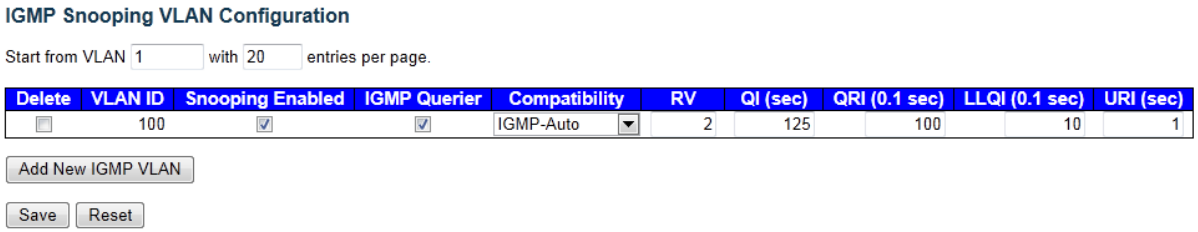


ここでは、IGMP Snooping 機能の基本設定を行います。

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 設定(VLAN Configuration)

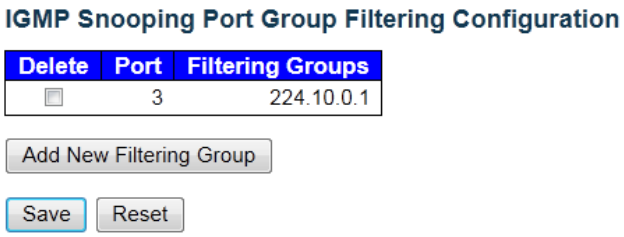
[Configuration]→[IPMC]→[IGMP Snooping →[VLAN Configuration]をクリックすると、以下の画面が表示されます。



ここでは、IGMP Snooping の VLAN テーブルの設定及び、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。
- IGMP VLAN の新規追加/設定/保存
- IGMP VLAN の編集
- IGMP VLAN の削除

3)　ポートグループのフィルタリング(Port Group Filtering)

ポートグループのフィルタリングを行うには、[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。



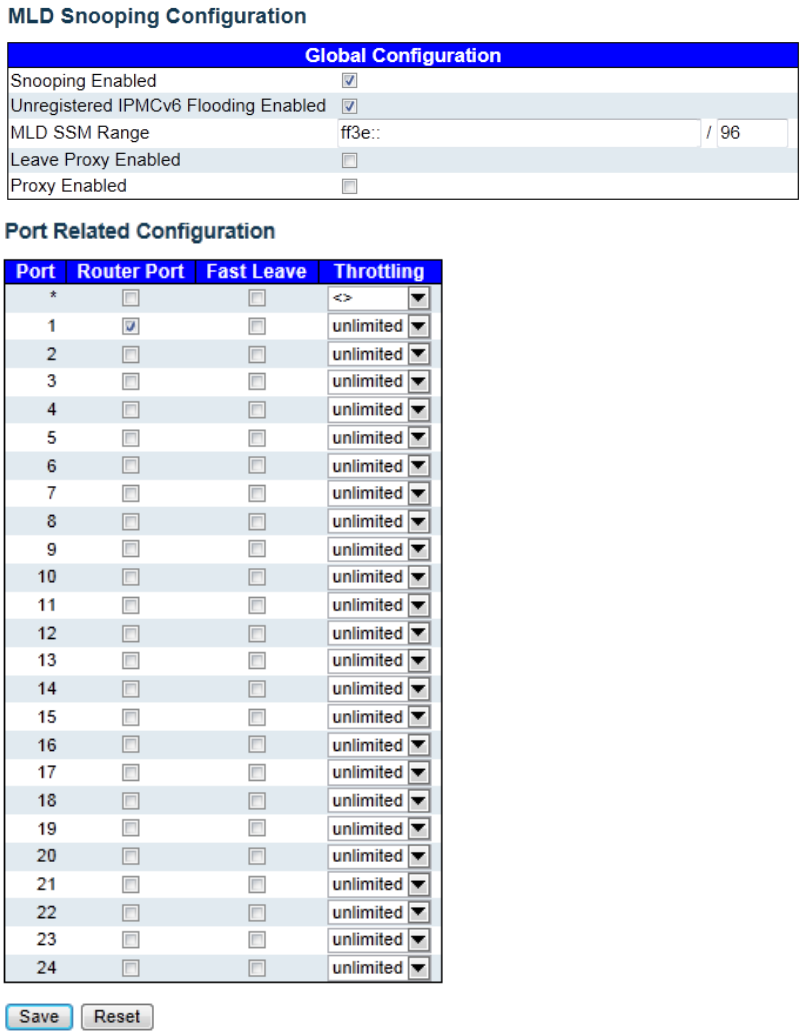
ここでは、ポートの IGMP フィルタリンググループの設定及び、メンテナンスを行います。
テーブル上の IP マルチキャストグループのフィルタリングを行います。

2.3.9.2 MLD Snooping の設定

MLD Snooping 設定を行います。

1) 基本設定(Basic Configuration)

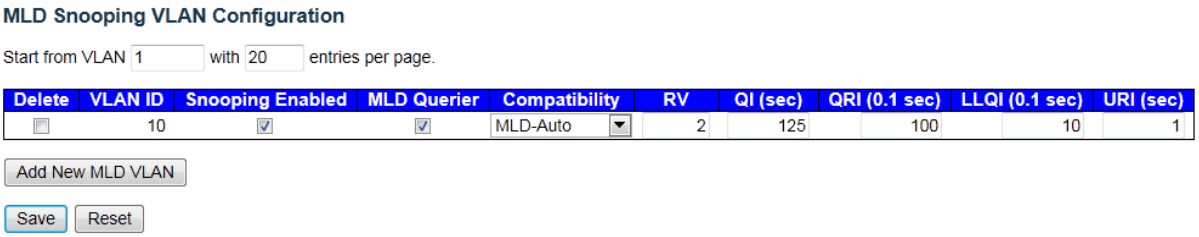
[Configuration]→[IPMC]→[MLD Snooping]→[Basic Configuration]をｸﾘｯｸすると、以下の画面が表示されます。



ここでは、MLD Snooping 機能の基本設定を行います。

2) VLAN 設定(VLAN Configuration)

[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。

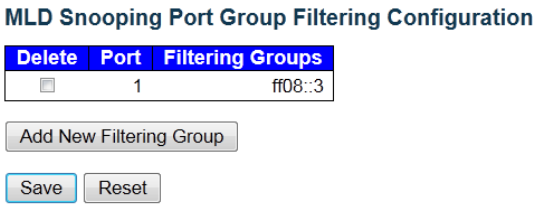


ここでは、MLD Snooping の VLAN テーブルの設定及び、メンテナンスを行います。
以下の機能がサポートされています。

- - MLD VLAN の新規追加/設定/保存
- - MLD VLAN の編集
- - MLD VLAN の削除

3) ポートグループのフィルタリング設定(Port Group Filtering)

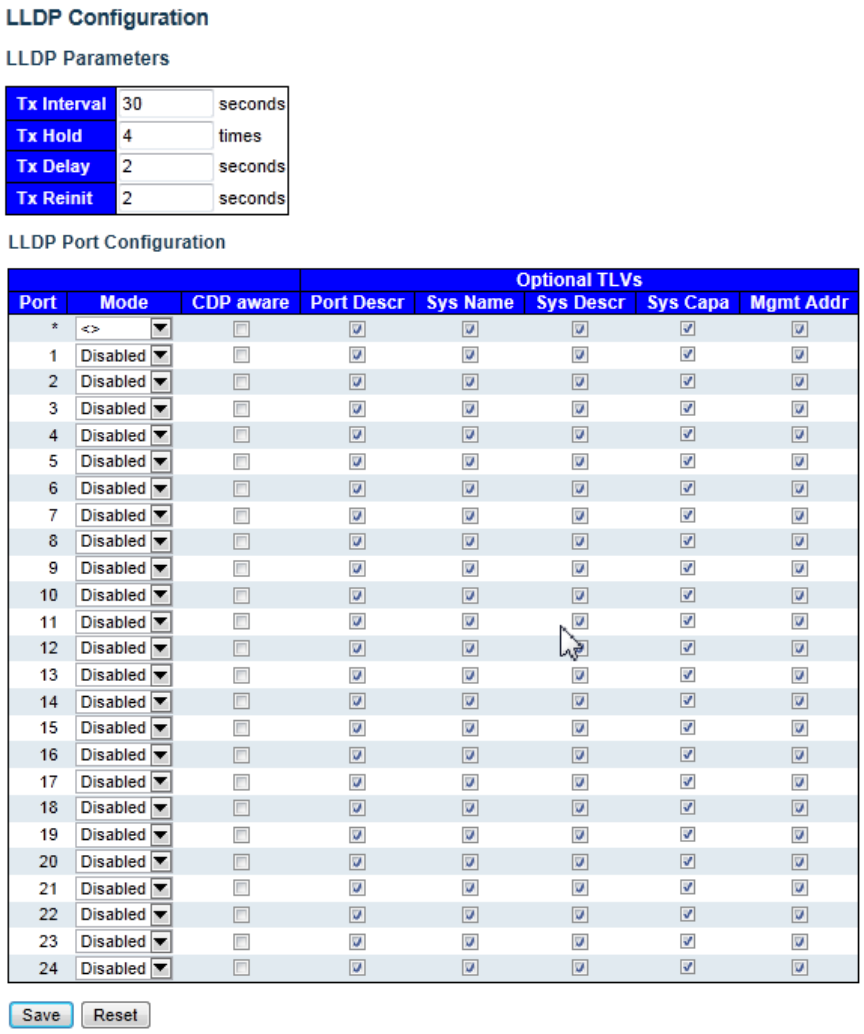
[Configuration]→[IPMC]→[MLD Snooping]→[Port Group Filtering]をクリックすると、以下の画面が表示されます。



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設定(LLDP)

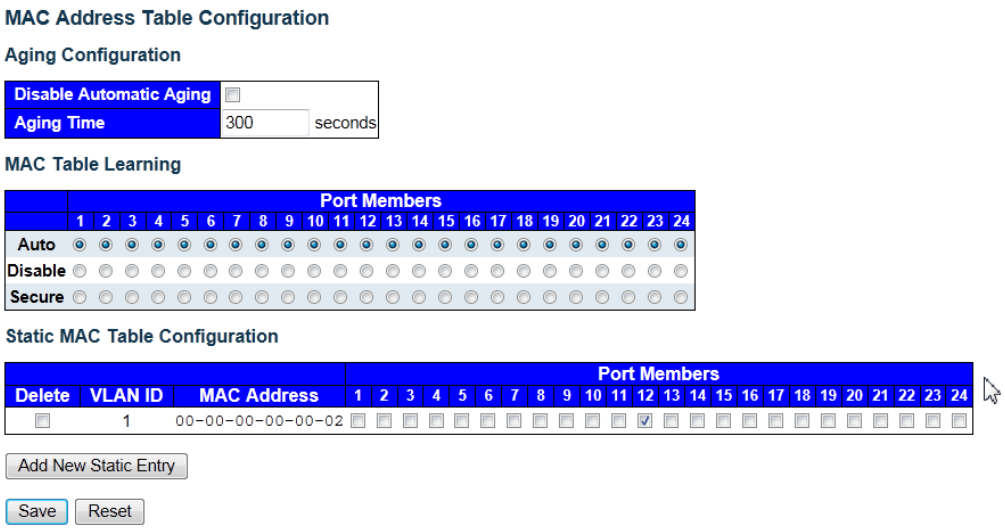
LLDP 機能の設定を行います。
[Configuration]→[LLDP]をクリックすると、以下の画面が表示されます。



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。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 MACテーブル設定(MAC Table)

MAC アドレス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。



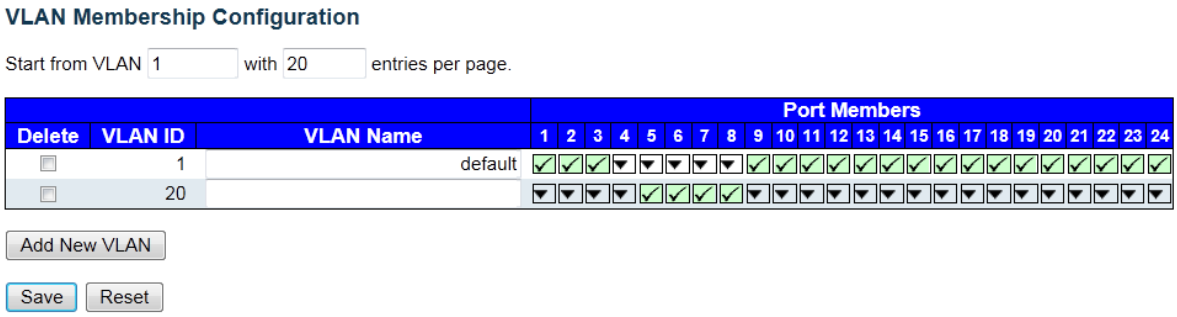
エージングタイム、MAC アドレス学習、スタティック MAC アドレスの設定を行います。
エージングタイムのデフォルト設定は、「300 秒」です。
MAC アドレステーブルのメニューの設定を”Secure”に設定すると、スタティック MAC エントリのみを学習し、それ以外のフレームはすべて破棄されます。

2.3.12 VLAN設定(VLANs)

VLAN(802.1Q VLAN　及び　Q-in-Q)を設定を行います。

2.3.12.1 VLAN メンバー(VLAN Membership)

[Configuration]→[VLANs]→[VLAN Membership]をクリックすると、以下の画面が表示されます。

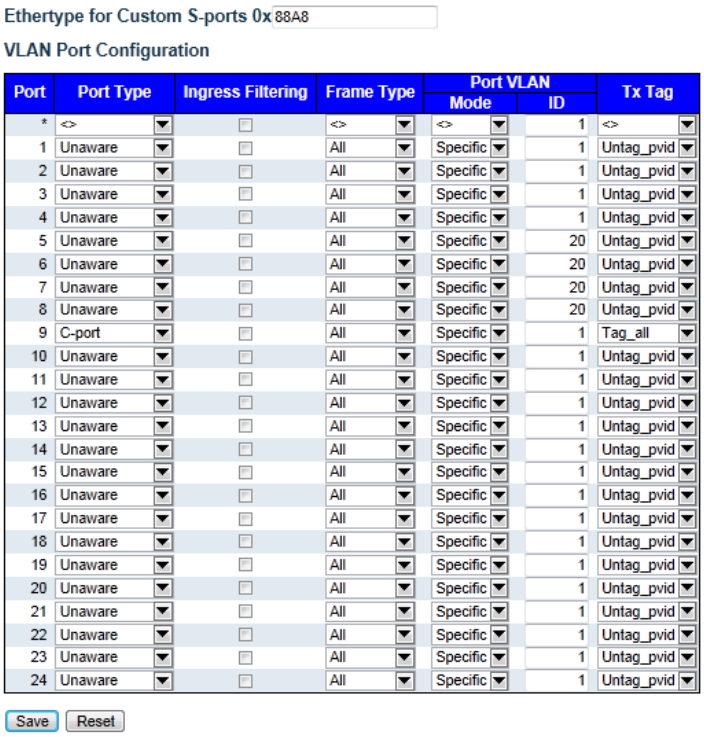


802.1Q VLAN グループのメンテナンスを行います。

- 新規 VLAN の追加/ VLAN ID/VLAN 名の設定
- VLAN の編集
- VLAN の削除
- VLAN のポートへ割り当て

2.3.12.2 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。



ポートの VLAN (802.1Q VLAN および Q-in-Q)の設定を行います。

1)　ポートタイプ

各ポートの設定については、以下のメニューより設定することができます。
Port VLAN

- Unaware:
  ポートを Unaware に設定すると、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)に分類されます。
- C-port:
  ポートを C-port に設定すると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 に分類されます。
- S-port:
  ポートを S-port にする場合は、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。
- S-custom-port:
  ポートを S-custom-port に設定する場合は、出力フレームのタグは「Ethertype for Costom S-ports 0xXXXX」で設定した TPID(Tag Protocol Identifier：タグプロトコル識別子)を持つサービス VLAN としてカスタマイズされます。

2) ポートのVLANモード:

各ポートの VLAN 設定については、以下のメニューより設定することができます。

Ingress Filter:

受信フレームの VLAN 入力フィルタを有効/無効にします。

Frame Type:

受信フレームのすべて/タグ付き/タグなしを指定します。

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 タグは「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 の認識はできない場合（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ポートの VLAN ID にクラス分けされます。送信されたフレームのクラス分けされた VLAN ID はポートの VLAN ID と異なり、VLAN ID を持つ VLAN がフレームに挿入されます。

Tx_Tag:

"Tx_Tag"により、フレームを送信時のタグ付け方法が定義されます。

■ ポート設定例

802.1Q VLAN 設定において、各ポートの設定例は下記の通りです。

- 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(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通りです。

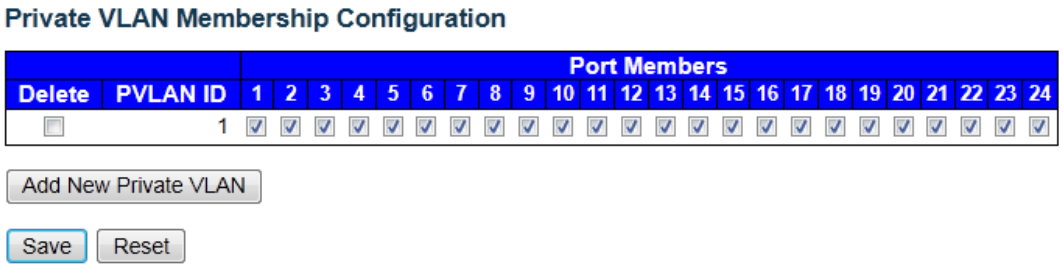
- Uplink:
  [Port Type]-S-port(S-custom-port), [Port VLAN Mode]-None, [Tx Tag]-Untag_pvid.
- Downlink:
  [Port Type]-Unaware, [Port VLAN Mode]-Specific(サービス VLAN ID を”PVID”に設定し、サービス VLAN を設定)、[Tx Tag]-Untag_all

2.3.13 プライベートVLAN設定(PrivateVLANs)

プライベート VLAN の設定を行います。

2.3.13.1 PVLAN メンバー設定(PVLAN Membership)

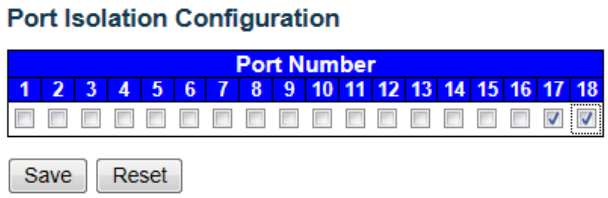
PVLAN メンバーを設定するには、[Configuration]→[PrivateVLANs]→[PVLAN Membership]をクリックすると、以下の画面が表示されます。



プライベート VLAN の設定/編集/ 削除を行います。
PVLAN ID が違う場合は通信できません。
アップリンクを共有する場合は、対象のポートに複数の PVLAN ID に所属させてください。

2.3.13.2 隔離ポートの設定(Port Isolation)

[Configuration]→[Port-Based VLANs]→[Port Isolation]をクリックすると、以下の画面が表示されます。



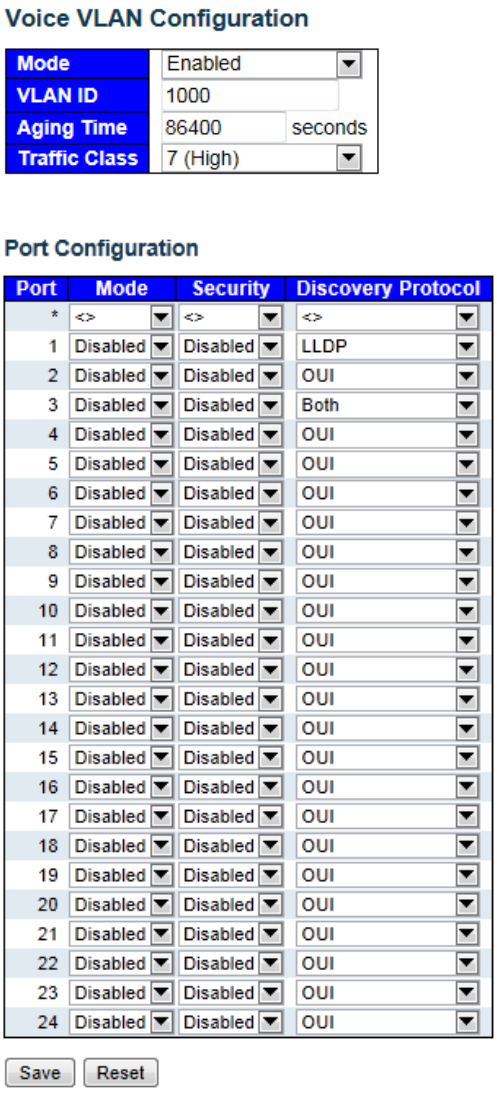
ここでは、ポートのアイソレーション機能を設定します。
ポートは、隔離ポートとしてマーク付けされ、同じ PrivateVLAN 上でも隔離ポート同士で互いに通信を行うことができません。

2.3.14 音声VLAN(Voice VLAN)

音声 VLAN の設定を行います。

2.3.14.1 基本設定(Configuration)

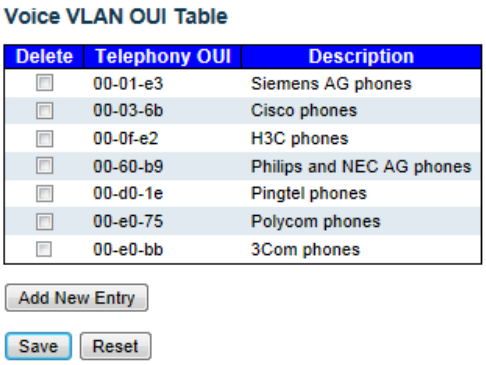
[Configuration]→[Voice VLAN]→[Configuration]をクリックすると、
以下の画面が表示されます。



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 トラフィックの自動検知、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。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、ベンダコード(Mac アドレスの最初 6 桁の 3 バイト)です)。

2.3.14.2OUI 設定

[Configuration]→[Voice VLAN]→[OUI]をクリックすると、
以下の画面が表示されます。



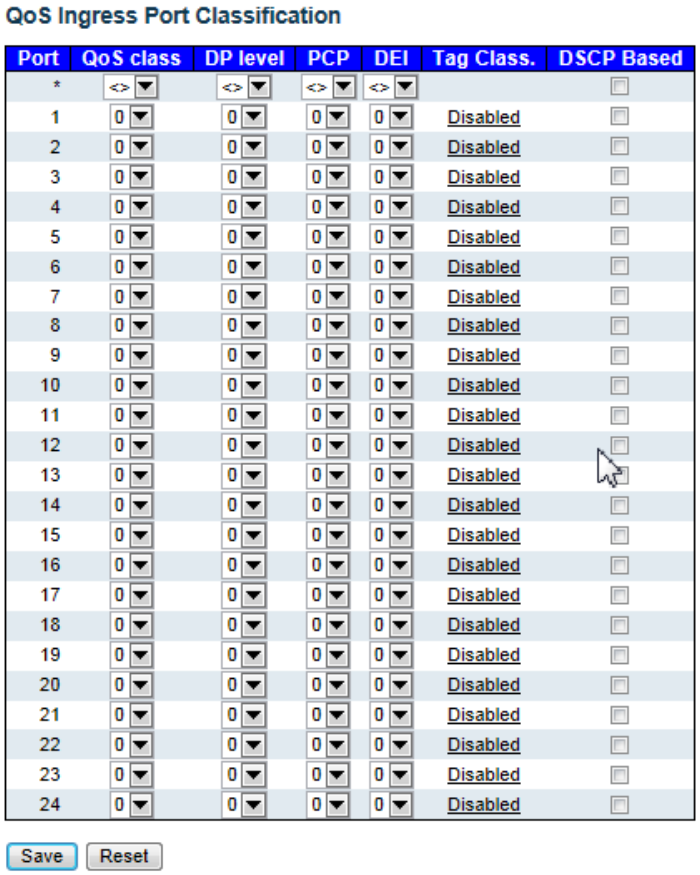
ここでは、Voice IP トラフィックの OUI テーブルのメンテナンスを行います。
OUI は、ベンダコード(Mac アドレスの最初 6 桁の 3 バイト)です。
Packets with OUI をもつパケットが Voice トラフィックとして処理されます。

2.3.15 品質設定(QoS)

QoS の設定を行います。

2.3.15.1 ポートのクラス分け(Port Classification)

[Configuration]→[QoS]→[Port 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 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。

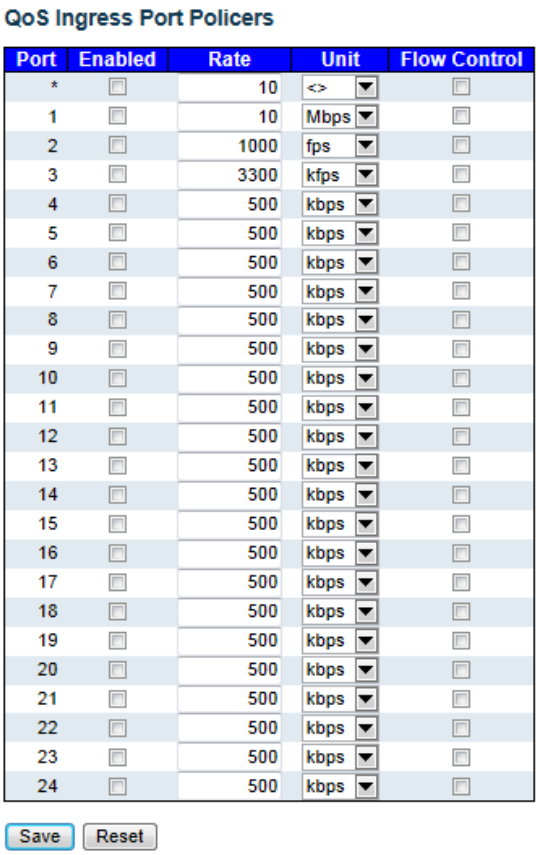
タグのクラス分けについて
「Tag Class」は、802.1Q タグの PCP かつ DEI による QoS を有効/無効にします。
クリックすると、(PCP,DEI)から(QoS class, DP level)のマッピングが表示されます。有効にすると、ポートの入力タグのクラス分け QoS は、パケット伝送のマッピングに準じます。

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」、「DSCPClassification」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。

2.3.15.2 Port Policing

[Configuration]→[QoS]→[Port Policing]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。

2.3.15.3 ポートスケジューラ(Port Scheduler)

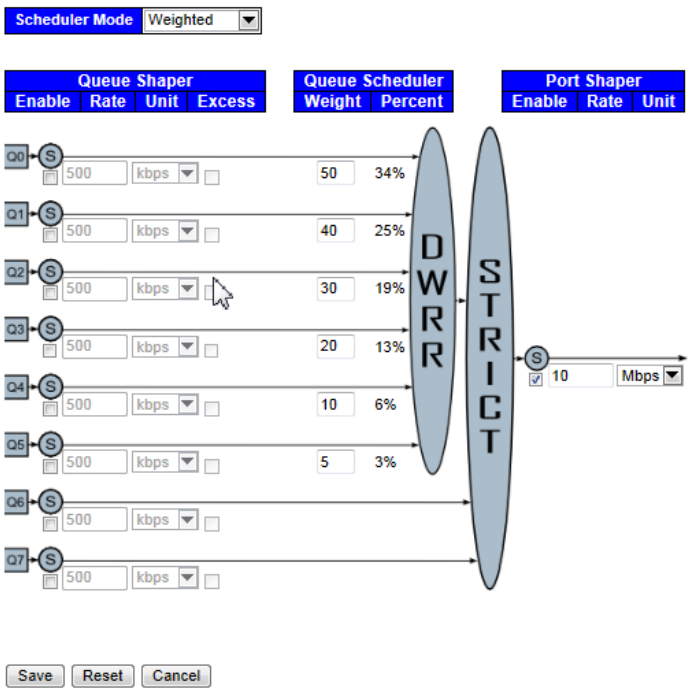
[Configuration]→[QoS]→[Port Scheduler]をクリックすると、
以下の画面が表示されます。

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Weighted	34%	25%	19%	13%	6%	3%
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	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-
24	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。。

QoS Egress Port Scheduler and Shapers Port 2



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。
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、フレームは破棄されます。

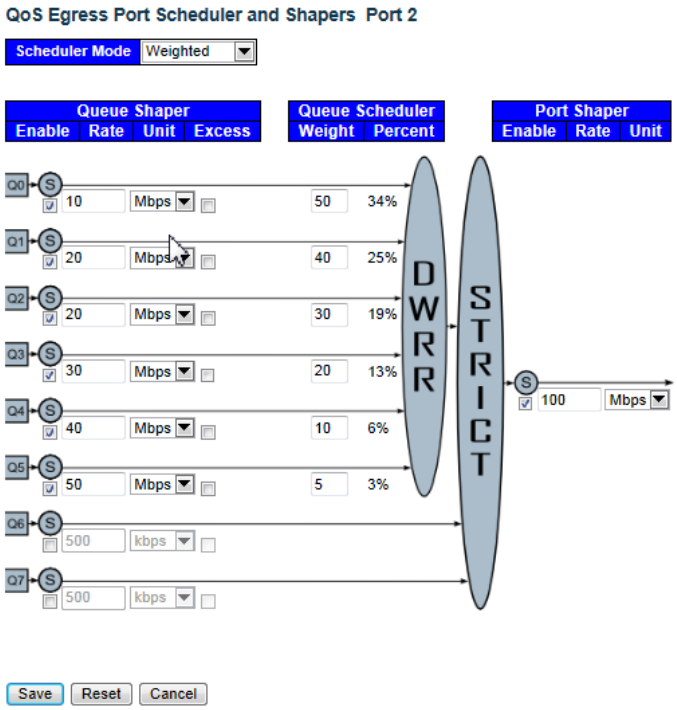
2.3.15.4 ポートシェーピング(Port Shaping)

[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	10 Mbps	20 Mbps	20 Mbps	30 Mbps	40 Mbps	50 Mbps	disabled	disabled	100 Mbps
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
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
24	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イパー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イパーを設定します。



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、フレームは破棄されます。

2.3.15.5 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。

この設定により、出力される際にフレームに PCP/DEI を追加・変更することが可能です。

QoS Egress Port Tag Remarking

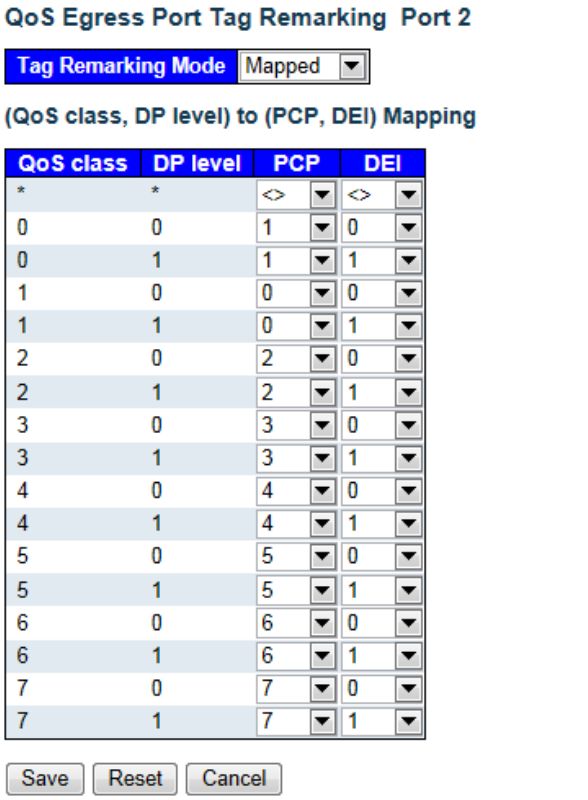
Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified

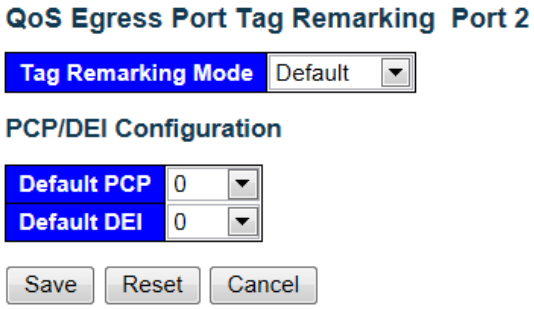
ポート番号をクリックすると、「Egress Tag Remarking」モードが表示されます。

QoS Egress Port Tag Remarking Port 2

Tag Remarking Mode	Classified

Save　Reset　Cancel



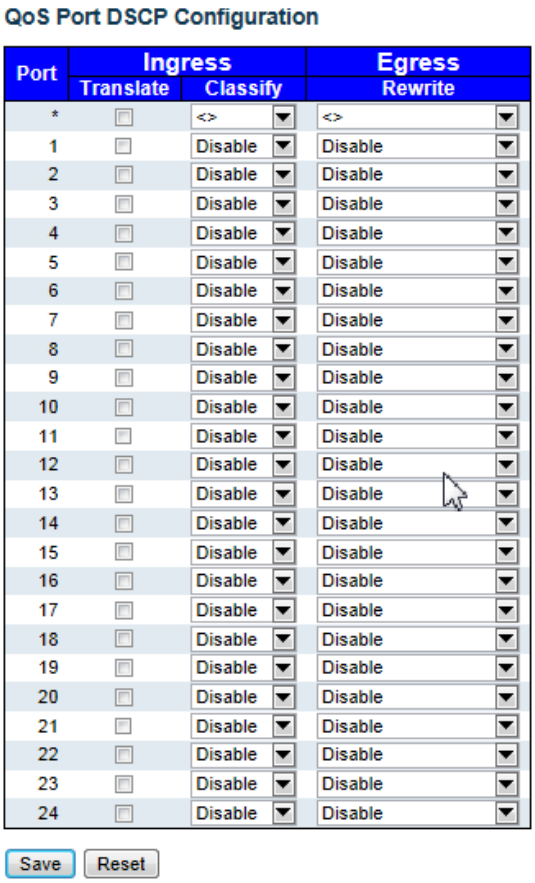


このモードは以下のとおりです。
- Classified : クラス分けされた PCP/DEI 値を使用（追加・変更しない）
- Default : デフォルト設定の PCP/DEI 値を使用(出力 PCP/DEI はすべてここの設定値になる)
- Mapped : QoSクラスおよび DP レベルのマッピングのバージョンを使用(PCP/DEI 値により異なる PCP/DEI 値で出力する)

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 VLAN 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、defaulf/mapped PCP および DEI により再度マーク付されるか、defaulf/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。

2.3.15.6 ポートの DSCP 設定(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。



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、IngressClassify 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、入力クラス分けされます。

■ **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。**

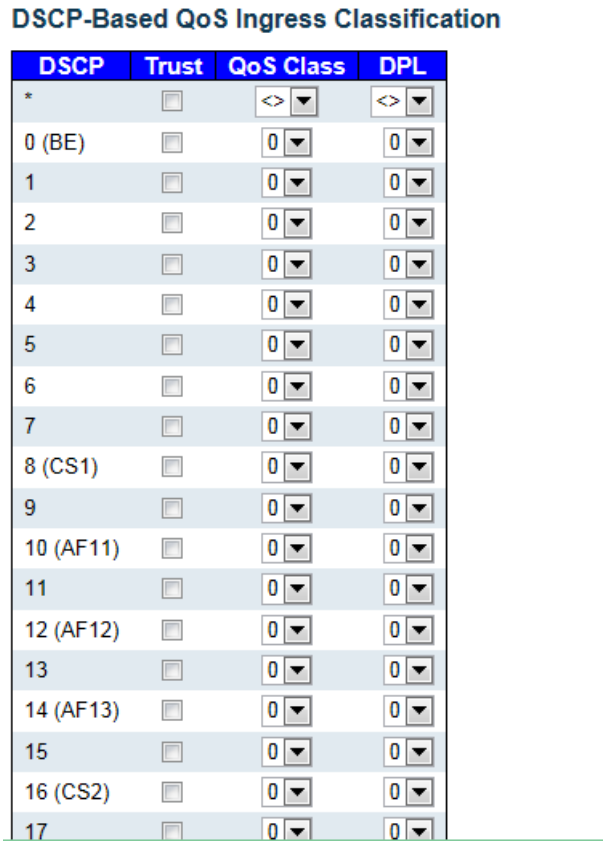
- Disable : 内部 DSCP への DSCP の QoS クラスのマッピング操作を無効にします。
- DSCP=0 : 受信 DSCP が「0」かどうかをクラス分けします(または有効な場合は変換されます)。「DSCP Translation」画面で指定したクラス分類が有効な DSCP のみクラス分けします（“classify”が選択されている場合のみ）
- All : すべての DSCP 値に有効。

■ **Egress Rewrite：出力パケットの DSCP リライトを設定します。**

- 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。

2.3.15.7 DSCP ベース QoS の設定(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。

2.3.15.8 DSCP 変換(DSCP Translation)

[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 変換には、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なります。

- 出力を行うには、出力側で設定可能なパラメータは以下のとおりです。
  1. Remap DP0: DP level 0 のフレームのリマッピングを制御します。
  2. Remap DP1: 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。
  「Port DSCP」メニューの Egress Rewrite について詳細を参照してください。

2.3.15.9 DSCP クラシフィケーション(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。

DSCP Classification

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

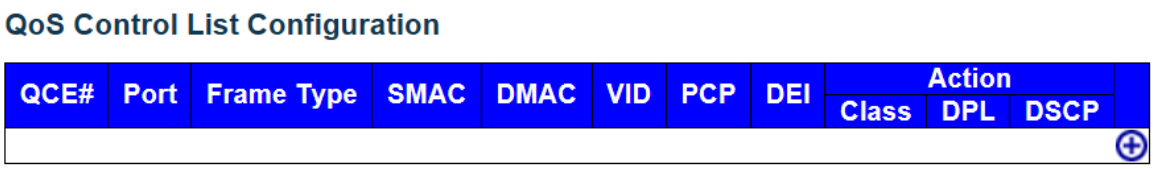
Save　Reset

ここでは、QoS クラスおよび破棄優先度を内部 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 または 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 の値に適用します。
「Port DSCP」画面の Egress Rewrite が有効な場合は、出力 DSCP の値を上書きします。

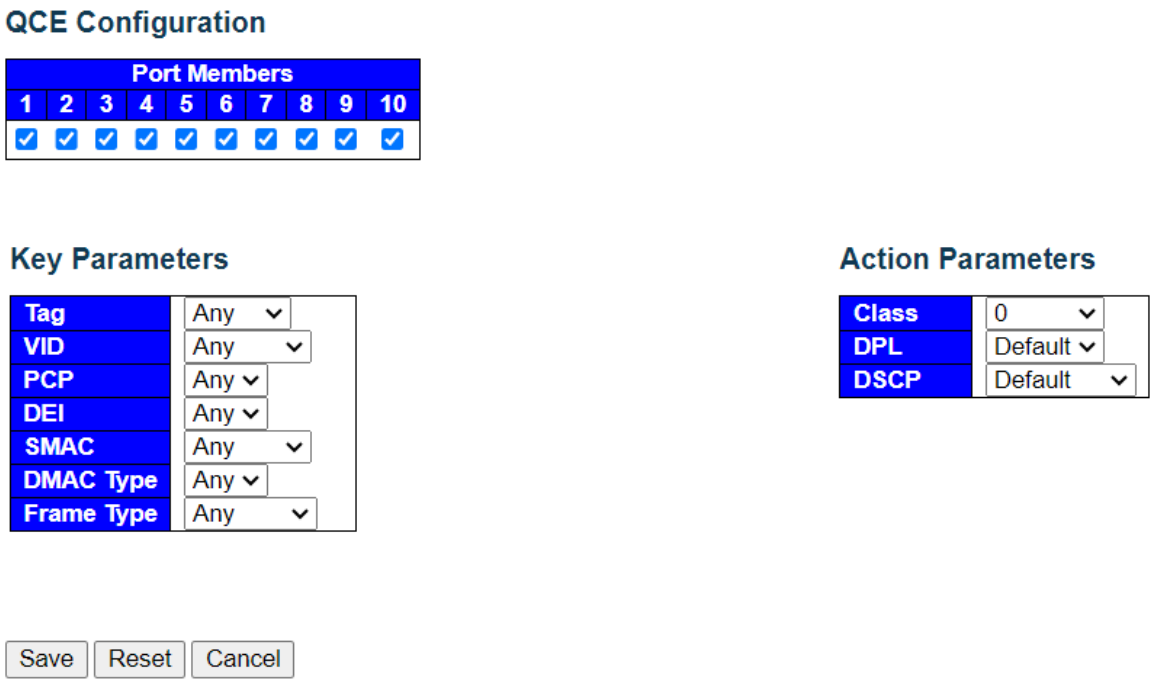
2.3.15.10 QoS コントロールリスト(QoS Control List)

[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。



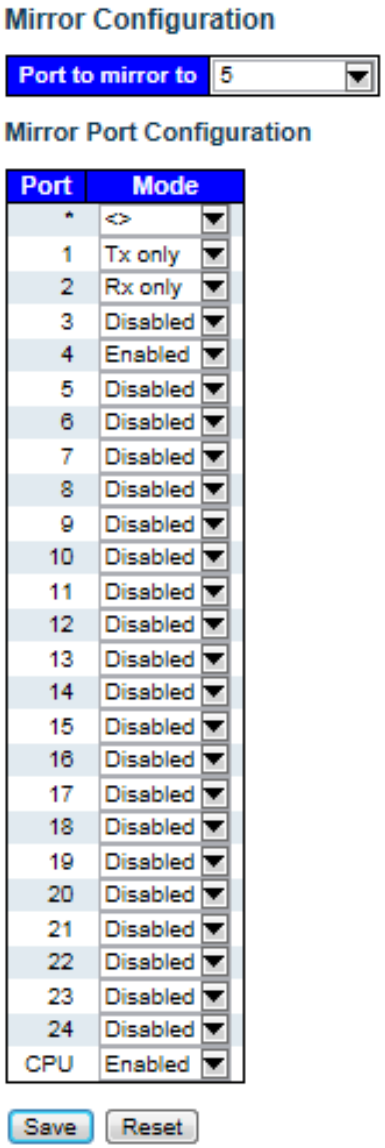
ここでは、QCL(QoS Control List)を設定します。それぞれの QCE は、パケットのパラメータおよび QoS アクションから構成されます。この機能により、特定のパケットのトラフィックは、設定されている QoS アクションで処理することが可能です。

(+)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。



2.3.16 ミラーリング(Mirroring)

[Configuration]→[Mirroring]をクリックすると、以下の情報が表示されます。

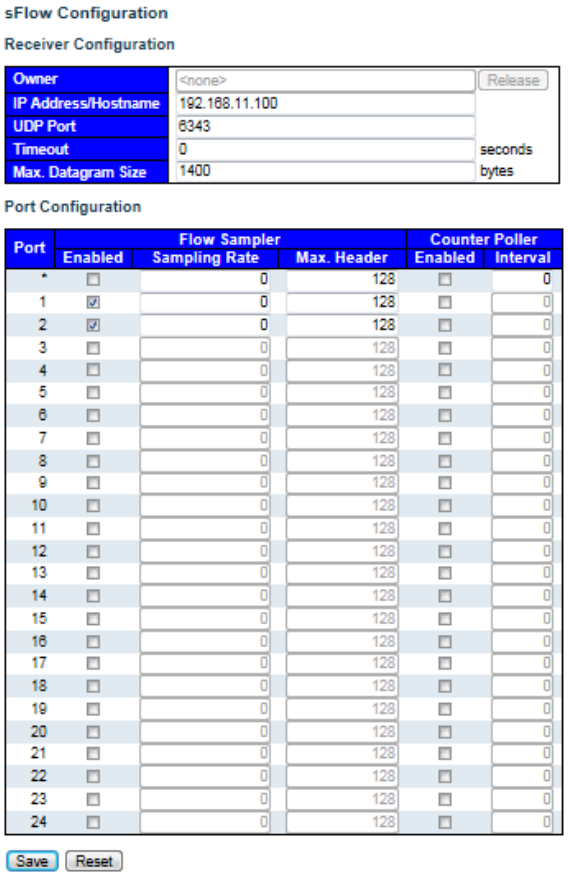


ここでは、本機のミラーリング機能を設定します。ネットワークの障害を解析するために、フレームフロー解析用に接続先のフレームアナライザーのミラーポートにトラフィックをコピーしたり、ミラーリングを行ったりすることが可能です。

ミラートラフィックは、パケットの送受信/送信/受信のフレームのミラーポートにミラーリングを行います。「Disabled」に設定すると、ミラーリング機能は無効になります。

2.3.17 sFlow設定(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 情報表示(Monitor)

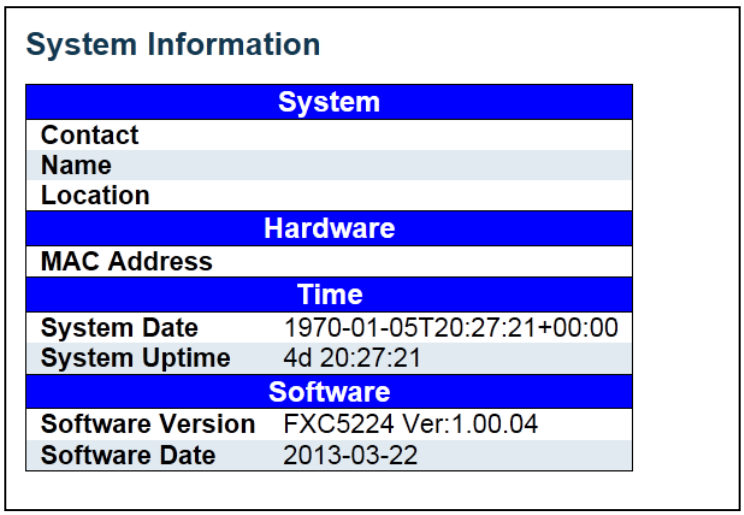
各種ステータス、情報を表示します。

2.4.1 システム情報(System)

システムに関する情報を表示します。

2.4.1.1 システム情報(information)

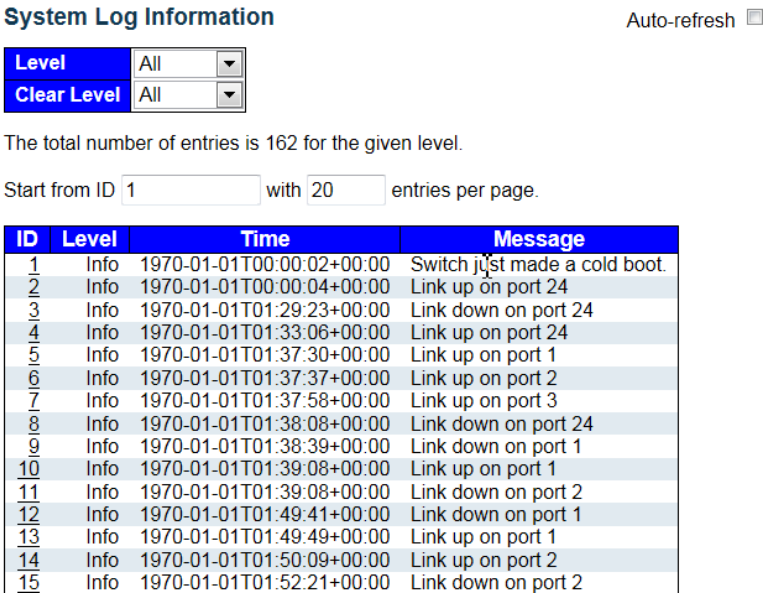
[Monitor]→[System]→[Information]をクリックすると、以下の画面が評されます。



ここでは、システム情報が表示されます。

2.4.1.2 システムログ情報(Log)

[Monitor]→[System]→[Log]をクリックすると、以下の画面が表示されます。

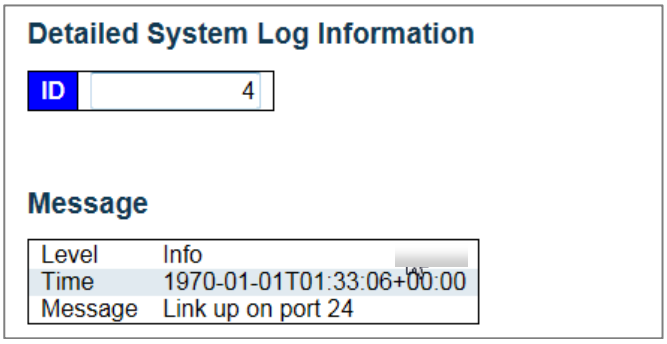


ここでは、本体のシステムログ情報が表示されます。

- 「Level」:選択したレベルのシステムログを表示します。
- 「Clear Level」:「Clear」ボタンをクリックすると、選択したレベルのログを削除します。
- 「ID」:ID 番号をクリックすると、ログの詳細が表示されます。

2.4.1.3 ログ情報の詳細(Detailed Log)

[Monitor]→[System]→[Detailed Log]をクリックすると、以下の画面が表示されます。



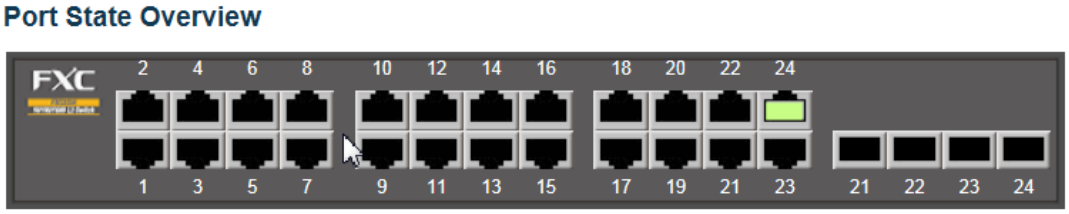
ここでは、ログの詳細が表示されます。
ID を入力すると、ログの詳細が表示されます。

2.4.2 ポート情報(Ports)

ポートに関する情報の表示します。

2.4.2.1 ポートの状態（State）

ポートの状態を設定するには、[Monitor]→[Ports]→[State]をクリックすると、以下の画面が表示されます。

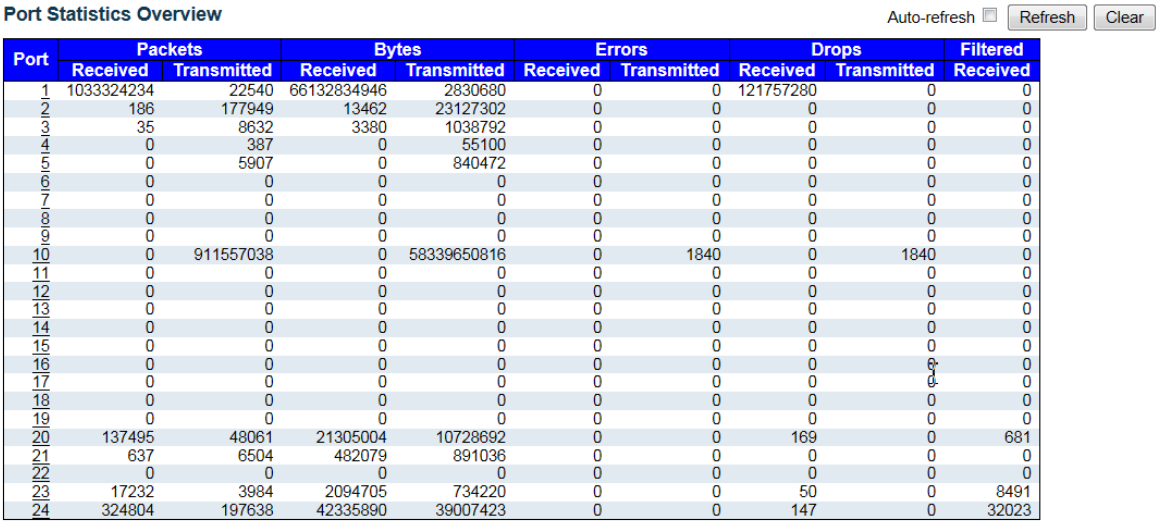


ここでは、ポートのリンク状態を表示します。
ポートにカーソルを合わせると速度、デュプレックスがポップアップされます。

ポートをクリックすると、統計情報が表示されます。
「Detailed Statistics」でも同じ統計情報が確認できます。

2.4.2.2 トラフィック統計概要(Traffic Overview)

[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

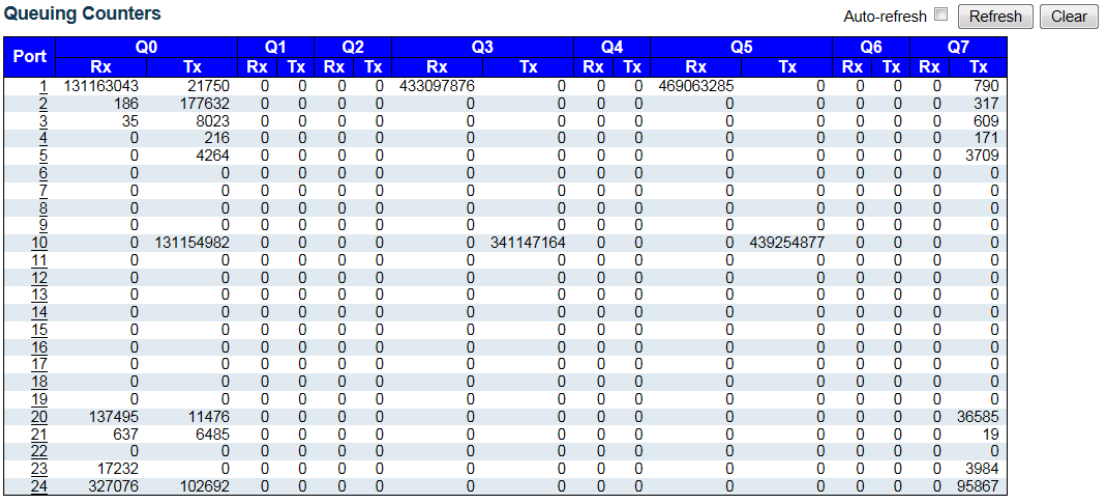
Auto-refresh Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	1033324234	22540	66132834946	2830680	0	0	121757280	0	0
2	186	177949	13462	23127302	0	0	0	0	0
3	35	8632	3380	1038792	0	0	0	0	0
4	0	387	0	55100	0	0	0	0	0
5	0	5907	0	840472	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	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	0	911557038	0	58339650816	0	1840	0	1840	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	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	137495	48061	21305004	10728692	0	0	169	0	681
21	637	6504	482079	891036	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	17232	3984	2094705	734220	0	0	50	0	8491
24	324804	197638	42335890	39007423	0	0	147	0	32023

ここでは、ポートごとのトラフィックの統計概要情報を表示します。

2.4.2.3 QoS 統計情報(QoS Statistics)

[Monitor]→[Ports]→[QoS Statistics]をクリックします。



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	131163043	21750	0	0	0	0	433097876	0	0	0	469063285	0	0	0	0	790
2	186	177632	0	0	0	0	0	0	0	0	0	0	0	0	0	317
3	35	8023	0	0	0	0	0	0	0	0	0	0	0	0	0	609
4	0	216	0	0	0	0	0	0	0	0	0	0	0	0	0	171
5	0	4264	0	0	0	0	0	0	0	0	0	0	0	0	0	3709
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	131154982	0	0	0	0	0	341147164	0	0	0	439254877	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	137495	11476	0	0	0	0	0	0	0	0	0	0	0	0	0	36585
21	637	6485	0	0	0	0	0	0	0	0	0	0	0	0	0	19
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	17232	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3984
24	327076	102692	0	0	0	0	0	0	0	0	0	0	0	0	0	95867

ここでは、ポートごとにキューのトラフィックの統計情報を表示します。ポートをクリックすると、統計情報が表示されます。

2.4.2.4 QCL ステータス(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。

QoS Control List Status

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
Static	1	Any	1-24	5	Default	Default	No

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 統計情報の詳細(Detailed Statistics)

統計情報を表示するには、[Monitor]→[Ports]→[Detailed Statistics]をクリックすると、以下の情報が表示されます。

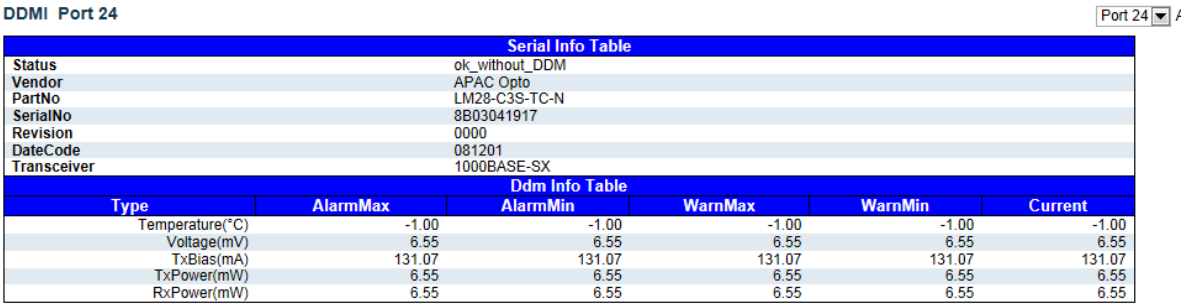
Detailed Port Statistics Port 1　　Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	1033324234	Tx Packets	22540
Rx Octets	66132834946	Tx Octets	2830680
Rx Unicast	1033323919	Tx Unicast	3808
Rx Multicast	177	Tx Multicast	4478
Rx Broadcast	147	Tx Broadcast	14254
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	1033321649	Tx 64 Bytes	8231
Rx 65-127 Bytes	2460	Tx 65-127 Bytes	7746
Rx 128-255 Bytes	89	Tx 128-255 Bytes	5503
Rx 256-511 Bytes	36	Tx 256-511 Bytes	406
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	562
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	92
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	131163043	Tx Q0	21750
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	433097876	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	469063285	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	790
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	121757280	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	0		

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、その統計情報の詳細が表示されます

2.4.2.6 DDMI

[Monitor]→[Port]→[DDMI]をクリックすると、以下の画面が表示されます。



DDMI Port 24

Port 24

Serial Info Table	
Status	ok_without_DDM
Vendor	APAC Opto
PartNo	LM28-C3S-TC-N
SerialNo	8B03041917
Revision	0000
DateCode	081201
Transceiver	1000BASE-SX

Ddm Info Table					
Type	AlarmMax	AlarmMin	WarnMax	WarnMin	Current
Temperature(°C)	-1.00	-1.00	-1.00	-1.00	-1.00
Voltage(mV)	6.55	6.55	6.55	6.55	6.55
TxBias(mA)	131.07	131.07	131.07	131.07	131.07
TxPower(mW)	6.55	6.55	6.55	6.55	6.55
RxPower(mW)	6.55	6.55	6.55	6.55	6.55

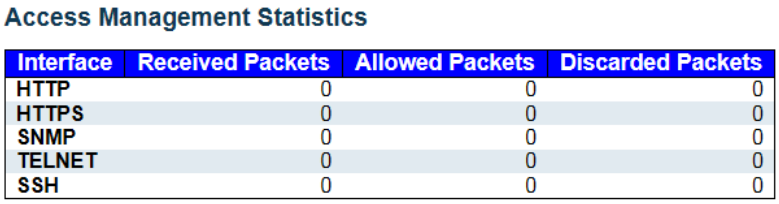
ここでは、トランシーバにより DDMI (Digital Diagnostics Monitoring Interface)機能がサポートされている場合は、SFP トランシーバ情報とステータスが表示されます。

2.4.3 セキュリティ情報(Security)

セキュリティに関する情報を表示します。

2.4.3.1 アクセス管理統計情報(Access Management Statistics)

[Monitor]→[Security]→[Access Management Statistics]をクリックすると、以下の情報が表示されます。



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、管理インターフェースのトラフィック統計情報が表示されます。

2.4.3.2 ネットワーク情報(Network)

ネットワークのセキュリティ情報を表示します。

1) ポートセキュリティのステータス情報(Port Security – 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

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	-	-
12	----	Disabled	-	-
13	----	Disabled	-	-
14	----	Disabled	-	-
15	----	Disabled	-	-
16	----	Disabled	-	-
17	----	Disabled	-	-
18	----	Disabled	-	-
19	----	Disabled	-	-
20	----	Disabled	-	-
21	----	Disabled	-	-
22	----	Disabled	-	-
23	----	Disabled	-	-
24	----	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。

- ポートの状態は以下のとおりです。

  - Disabled:
  現在ポートセキュリティ使用していません。
  - Ready:
  ポートセキュリティは使用中、未登録の 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は、ポートの MAC アドレス登録上限達し、これ以上の MAC アドレスは追加できなくなります。
  - Shutdown: ポートの MAC アドレス登録上限達し、これ以上の MAC アドレスは追加できなくなりポートが無効になります。
  管理画面から<Reopen>ボタンで復旧させるまで MAC アドレスの学習はできなくなります。

2)　ポートセキュリティの MAC アドレス情報(Port Security - Port)

[Monitor]→[Security] →[Network]→[Port Security]→[Port]をクリックすると、
以下の画面が表示されます。

Port Security Port Status　Port 1

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

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。
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。

2-1) ネットワークアクセスサーバのステータス情報(NAS - Switch)

ネットワークアクセスサーバのステータスを表示するには、
[Monitor]→[Security]→[Network]→[NAS]→[Switch]をクリックします。

Network Access Server Switch Status

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				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				

NAS (802.1x による) ポートの現在の状態を表示します。
NAS は、ネットワークアクセスサーバの略語です。NAS は、特定のソースへのアクセスを保護するゲートウェイとして動作します。クライアントは NAS への接続を行い、NAS は別のリソースに接続して、証明書をもつクライアントが有効かどうかを確認します。その応答を応じて、NAS は保護されているリソースへのアクセスを「許可/禁止」にします。本機は、IEEE 802.1X.により NAS を実行します。

ポートをクリックすると、802.1x のポート状態を表示します。

3) 各ポートの NAS の統計情報(NAS - Port)

[Monitor]→[Security]→[Network]→[NAS]→[Port]をクリックすると、
以下の情報が表示されます。

NAS Statistics Port 1　　Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

ここでは、NAS(802.1x)のポートの状態を表示します。
ポートを選択すると、802.1x のポートの状態が表示されます。

4) ACL ステータス情報 (ACL Status)

[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	101877	No
IP Management	All	IPv4/UDP 68 DHCP Server	Permit	Disabled	Disabled	Disabled	Yes	No	63	No
Static	1	IPv4/ICMP SIP:200.200.200.1/32	Deny	Disabled	Disabled	Disabled	No	No	0	No

ここでは、ACL ユーザごとに ACL ステータスを表示します。それぞれの行には、定義されている ACE が表示されます。

5) DHCP スヌーピング統計情報(DHCP - Snooping Statistics)

[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

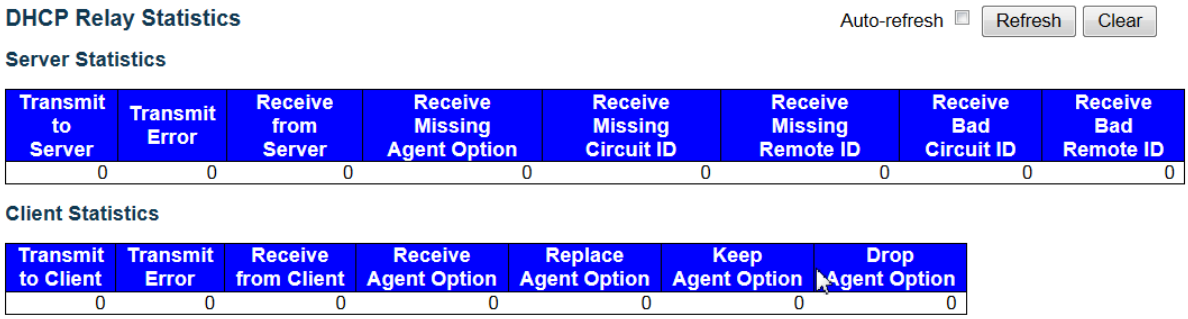
Port 1

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

ポートを選択すると、ポートの DHCP スヌーピングトラフィックの統計情報を表示します。

6) DHCP リレー統計情報(DHCP - Relay Statistics)

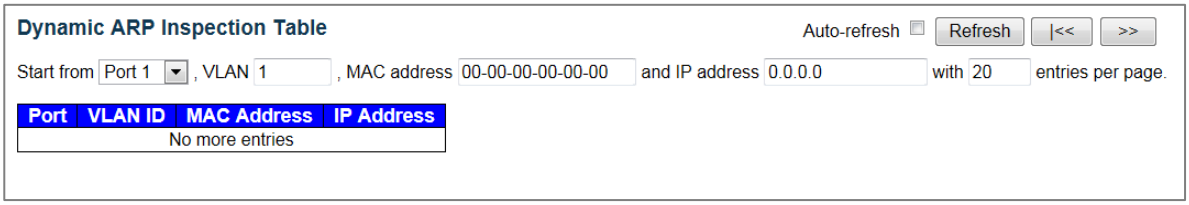
[Monitor]→[Security]→[Network]→[DHCP]→[Relay Statistics]をクリックすると、
以下の画面が表示されます。



ここでは、DHCP リレーの統計情報が表示されます。

7) ARP インスペクションテーブル情報(ARP Inspection)

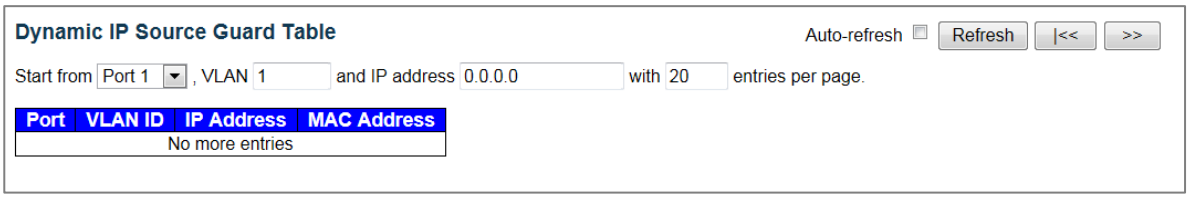
[Monitor]→[Security]→[Network]→[ARP Inspection]をクリックすると、
以下の画面が表示されます。



ここでは、ダイナミック ARP インスペクションテーブルのエントリが表示されます。ダイナミック ARP インスペクションテーブルには、エントリが 1024 まで含まれ、まずポートごとにソートされ、続いて MAC アドレス、IP アドレスごとにソートされます。

8) IP ソースガードテーブル情報(IP Source Guard)

[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。



ここでは、ダイナミック IP ソースガードテーブルが表示されます。ダイナミック IP ソースガードテーブルは、まずポートごとにソートされ、続いて VLAN ID、MAC アドレスごとにソートされます。

2.4.3.3 AAA 情報(AAA)

AAA の情報を表示します。

1) RADIUS 概要情報 (RADIUS Overview)

[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

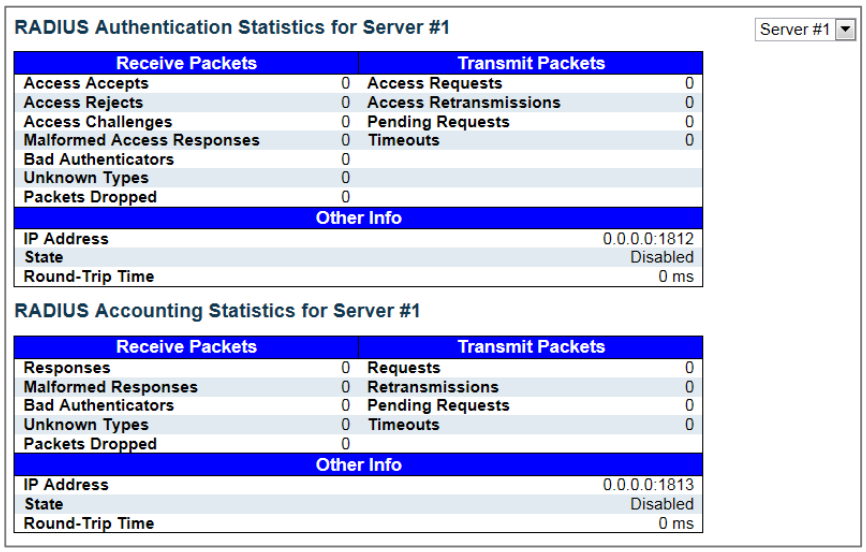
#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

ここでは、認証設定画面で 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 : サーバ設定は有効ですが、サーバと疎通ができません。
- Ready : サーバ設定は有効で、サーバは動作中であり、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 詳細情報(RADIUS Details)

[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。



ここでは、特定の RADIUS サーバの詳細な統計情報が表示されます。

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されます。
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。

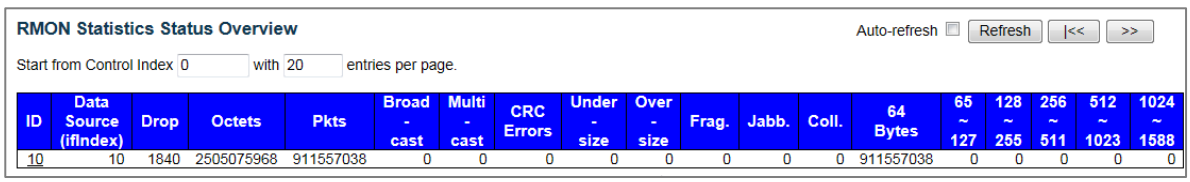
2.4.3.4 スイッチセキュリティ情報(Switch)

スイッチセキュリティ情報（RMON情報）を表示します。

1) RMON

1-1) 統計情報 Statistics

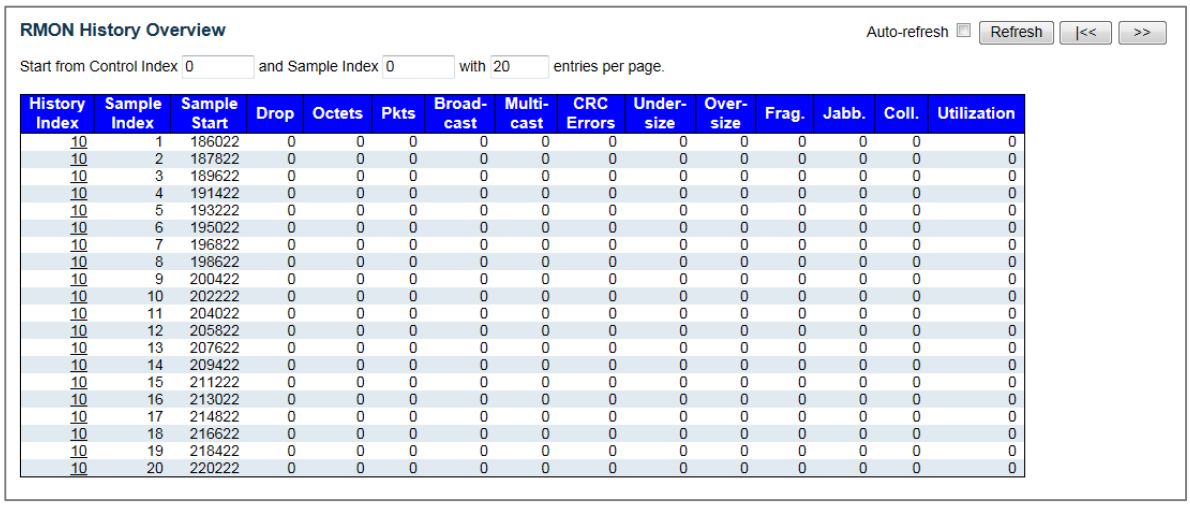
[Monitor]→[Security]→[Switch]→[RMON]→[Statistics]をクリックすると、
以下の画面が評されます。



ここでは、RMON 統計情報のエントリが表示されます。

1-2) 履歴(History)

[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。

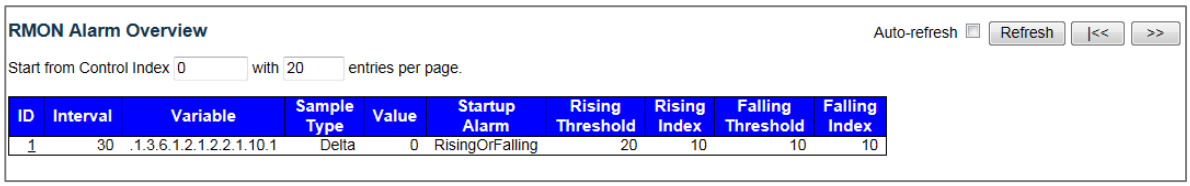


History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
10	1	186022	0	0	0	0	0	0	0	0	0	0	0	0
10	2	187822	0	0	0	0	0	0	0	0	0	0	0	0
10	3	189622	0	0	0	0	0	0	0	0	0	0	0	0
10	4	191422	0	0	0	0	0	0	0	0	0	0	0	0
10	5	193222	0	0	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

ここでは、RMON の履歴が表示されます。

1-3) RMON アラームの表示(Alarm)

[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。

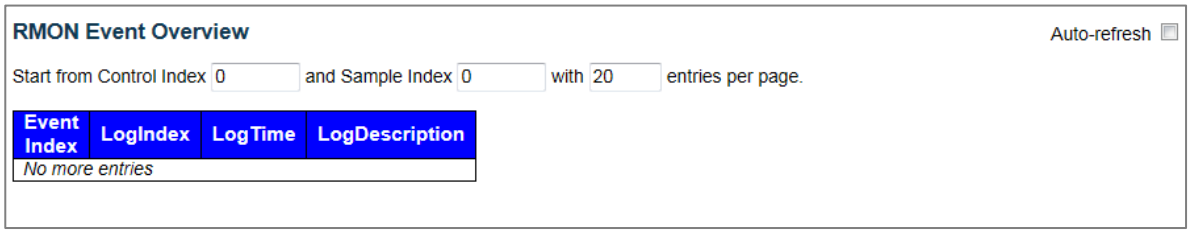


ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	30	.1.3.6.1.2.1.2.2.1.10.1	Delta	0	RisingOrFalling	20	10	10	10

ここでは、RMON のアラーム項目が表示されます。

1-4) イベント情報の表示(Event)

[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。



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 情報(LACP)

LACP の情報を表示します。。

2.4.4.1 システムステータス(System Status)

[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-c0-f6-63-17-4a	3	32768	0d 00:00:32	3,4

ここでは、LACP インスタンスすべてのステータスが表示されます。

2.4.4.2 ポートステータス(Port Status)

[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

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	Yes	3	LLAG1	00-c0-f6-63-17-4a	3	32768
4	Yes	3	LLAG1	00-c0-f6-63-17-4a	4	32768
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	-	-	-	-	-
19	No	-	-	-	-	-
20	No	-	-	-	-	-
21	No	-	-	-	-	-
22	No	-	-	-	-	-
23	No	-	-	-	-	-
24	No	-	-	-	-	-

ここでは、すべてのポートの LACP ステータスについて表示します。

2.4.4.3 ポートの統計情報(Port Statistics)

[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

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	131	134	0	0
4	118	115	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
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	7	0	0	0

ここでは、すべてのポートの LACP 統計情報を表示します。

2.4.5 ループ検知情報(Loop Protection)

[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

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Up	-	-
4	Shutdown	Enabled	0	Up	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-
13	Shutdown	Enabled	0	Down	-	-
14	Shutdown	Enabled	0	Down	-	-
15	Shutdown	Enabled	0	Down	-	-
16	Shutdown	Enabled	0	Down	-	-
17	Shutdown	Enabled	0	Down	-	-
18	Shutdown	Enabled	0	Down	-	-
19	Shutdown	Enabled	0	Down	-	-
20	Shutdown	Enabled	0	Down	-	-
21	Shutdown	Enabled	0	Down	-	-
22	Shutdown	Enabled	0	Down	-	-
23	Shutdown	Enabled	0	Down	-	-
24	Shutdown	Enabled	0	Up	-	-

ここでは、loop protection のポートステータスが表示されます。

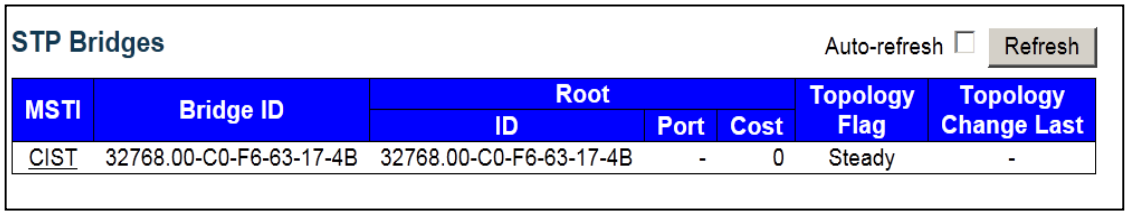
ループが発生すると、パケットストームが生成されます。これにより、ネットワーク障害が引き起こされる可能性がありますが、ループプロテクション機能により、ポート上で発生するこれらの障害を回避することができます。

2.4.6 スパニングツリー情報(Spanning Tree)

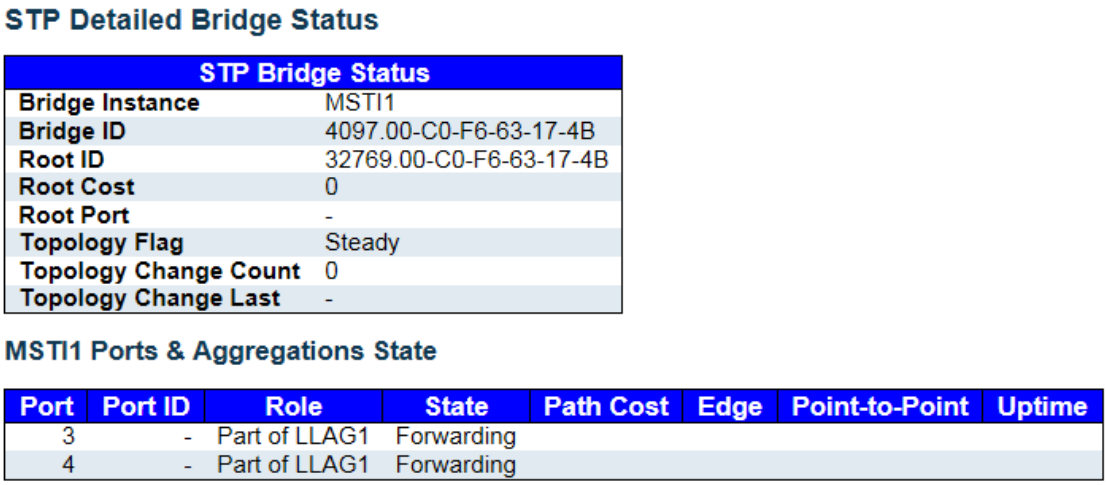
スパニングツリーの情報を表示します。

2.4.6.1 ブリッジステータス(Bridge Status)

[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。



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。
「CIST」、「MSTIx」をクリックすると、STP の詳細なブリッジステータスが表示されます。



2.4.6.2 ポートステータス情報(Port Status)

ポートステータスを表示するには、[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

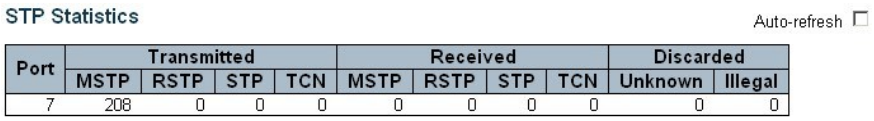
Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Port of LLAG1	Forwarding	-
4	Port of LLAG1	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
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	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	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 ロールは、代替ポート、バックアップポート、ルートポート、指定ポート、あるいは無効にします。
CIST 状態は、「Discarding」、「Learning」あるいは「Forwarding」のいずれかから設定可能です。

2.4.6.3 ポートの統計情報(Port Statistics)

[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 ☐

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
7	208	0	0	0	0	0	0	0	0	0

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。

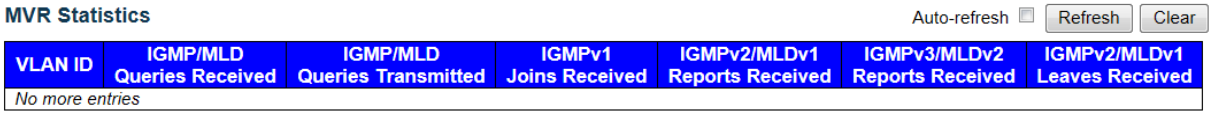
- MSTP: MSTP BPDU の送受信数
- RSTP: RSTP BPDU のによる送受信数.
- STP: legacy STP Configuration BPDU の送受信数.
- TCN(Topology Change Notification): BPDU の送受信数
- Discarded Unknown: アンノウンスパニングツリーBPDU の受信（破棄）数。
- Discarded Illegal: 不正のスパニングツリーの BPDU'の受信（破棄）数

2.4.7 MVR情報(MVR)

MVR の情報を表示します。

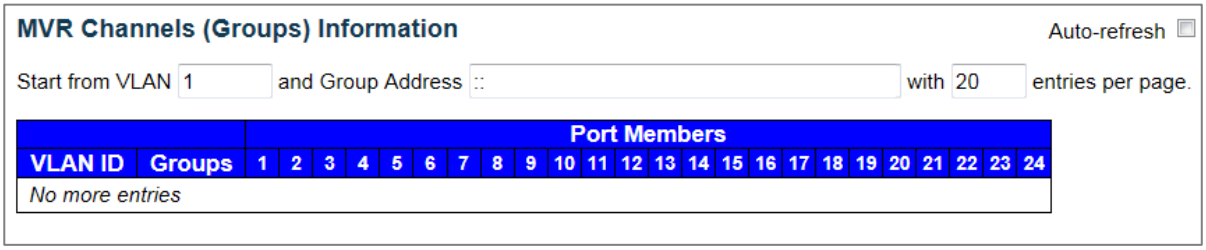
2.4.7.1 統計情報(Statistics)

[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 チャネルグループ情報(MVR Channel Groups)

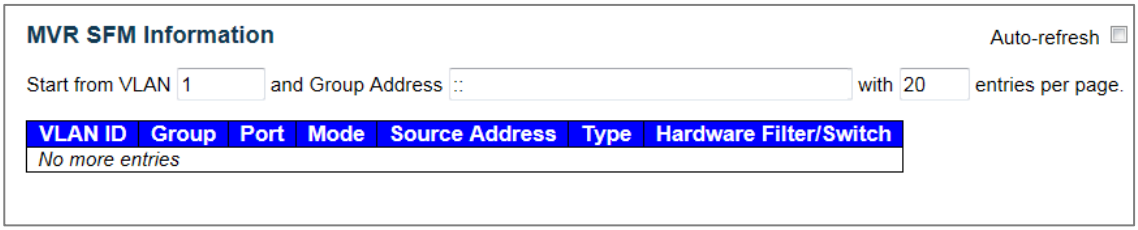
[Monitor]→[MVR]→[MVR Channel Groups]をクリックすると、
以下の画面が表示されます。



「MVR Channels (Groups) Information」表のエントリが表示されます。

2.4.7.3 MVR SFM 情報(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 IPマルチキャスト情報(IPMC)

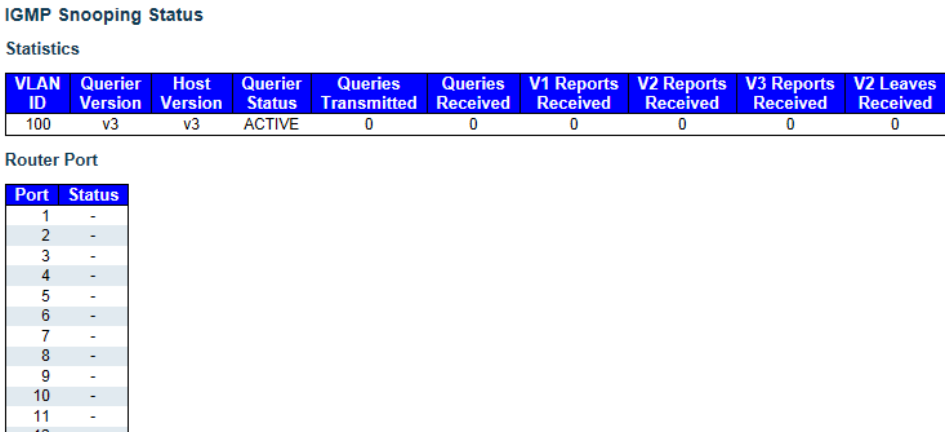
IPMC(IP マルチキャスト)に関する IGMP/MLD スヌーピング情報を表示します。

2.4.8.1 IGMP スヌーピング(IGMP Snooping)

IGMP スヌーピングに関する情報を表示します

1) IGMP スヌーピングのステータス(Status)

[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

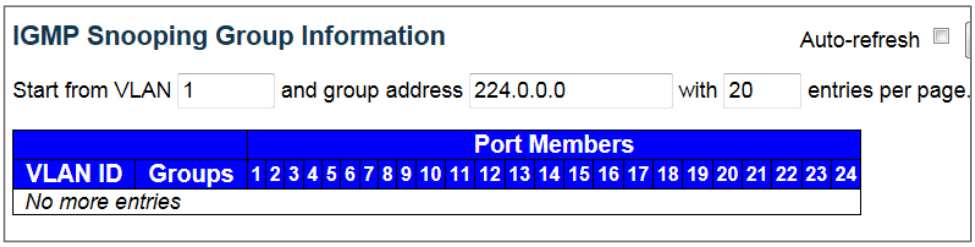
Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-

ここでは、IGMP Snooping のステータスを表示します。
プロトコルステータスおよび統計情報が評されます。
ルータのアクティブステータスが表示されます。

2) グループ情報（Groups Information）

[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。


IGMP Snooping Group Information　Auto-refresh

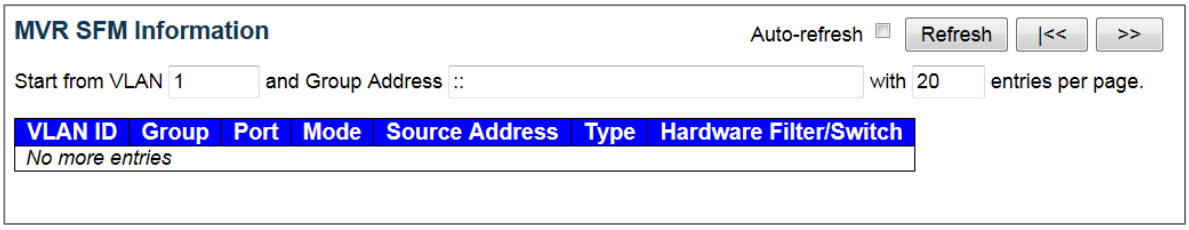
Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

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																									

「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 情報(IPv4 SFM Information)

[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。



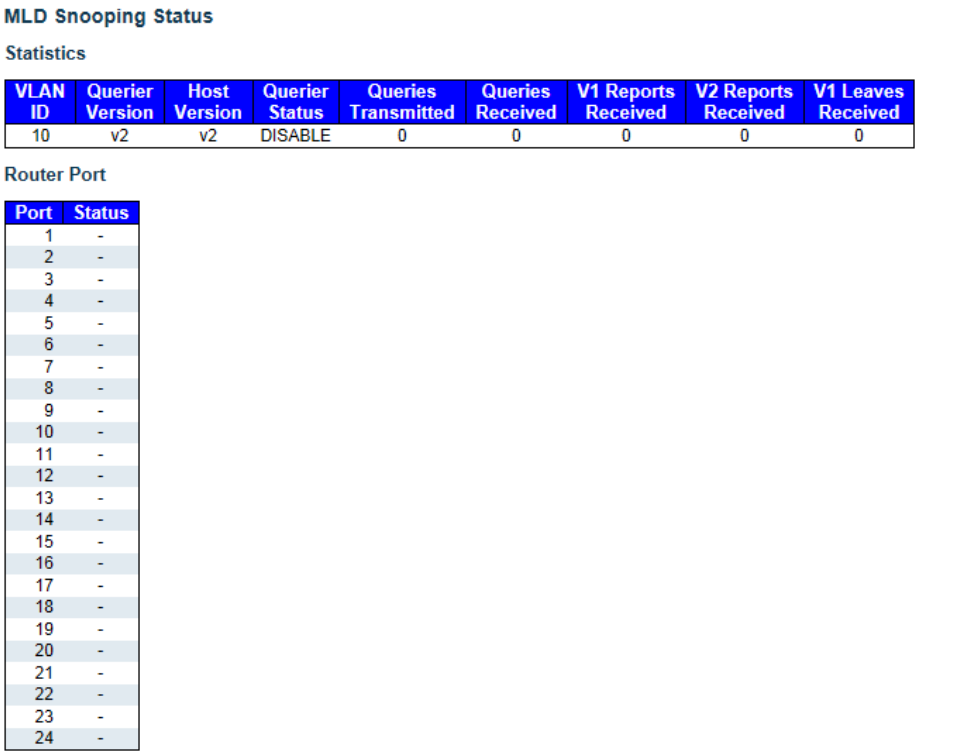
「IGMP SFM Information」テーブルのエントリが表示されます。「IGMP SFM (Source-Filtered Multicast) Information」テーブルには、SSM (Source-Specific Multicast) 情報も含まれます。この表は、まず VLAN ID ごとに、次にグループごと、ポートごとにソートされます。同じグループの異なるソースアドレスは、単一のエントリとして処理されます。

2.4.8.2 MLD Snooping

MLD スヌーピングに関する情報を表示します。

1) MLD Snooping のステータス(Status)

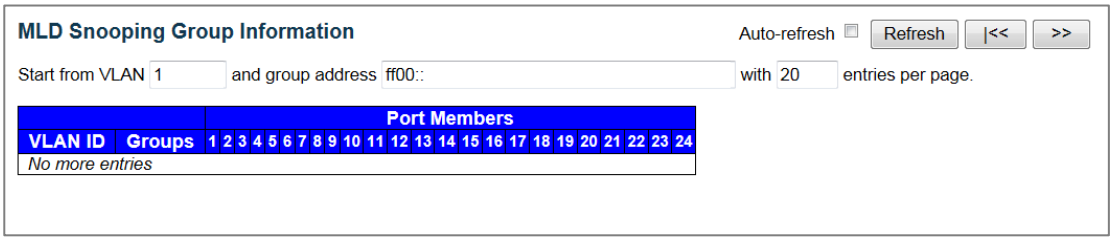
[Monitor]→[IPMC]→[MLD Snooping]→[Status]をクリックすると、以下の画面が表示されます。



ここでは、MLD Snooping のステータスプロトコルステータスおよび統計情報、
ルータポートの状態が表示されます。

2)　グループ情報の表示(Groups Information)

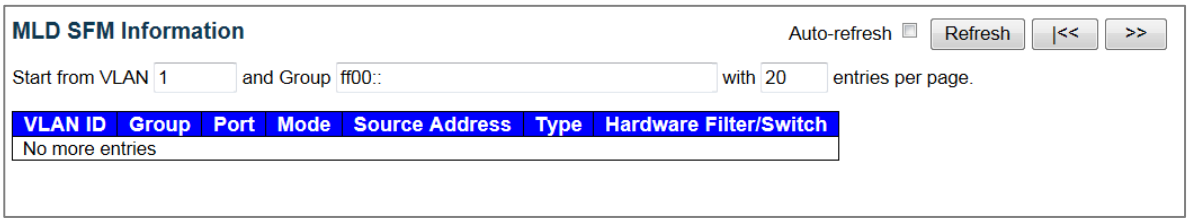
[Monitor]→[IPMC]→[MLD Snooping]→[Groups Information]をクリックすると、
以下の画面が表示されます。



MLD グループテーブルは、VLAN ID、次にグループごとにソートされます。

3)　IPv6 SFM 情報(IPv6 SFM Information)

[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。



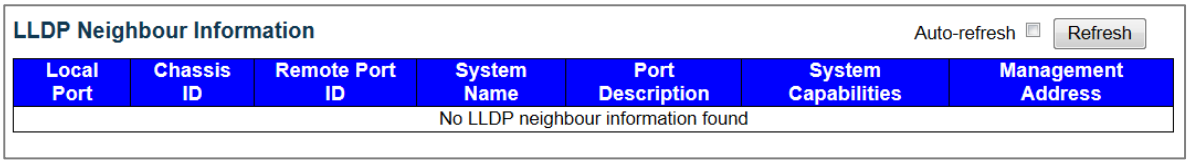
「MLD SFM Information」テーブルのエントリが表示されます。
「MLD SFM (Source-Filtered Multicast) Information」テーブルには、SSM (Source-Specific Multicast) 情報も含まれます。
この表は、まず VLAN ID ごと、次にグループごと、ポートごとにソートされます。
同じグループの異なるソースアドレスは、単一のエントリとして処理されます。

2.4.9 LLDPの情報(LLDP)

LLDP の情報を表示します。

2.4.9.1 LLDP ネイバー情報(Neighbours)

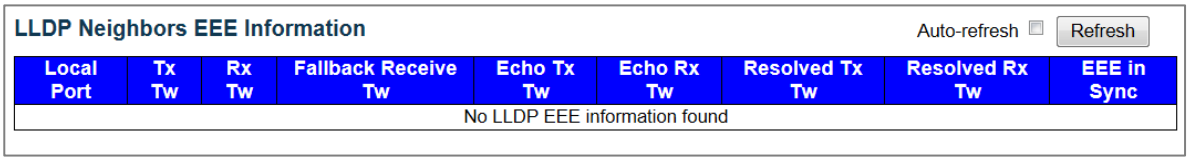
[Monitor]→[LLDP]→[Neighbours]をクリックすると、以下の画面が表示されます。



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、検出された LLDP ネイバー装置がポートごとに表示されます。

2.4.9.2 LLDP 省電力情報(EEE)

[Monitor]→[LLDP]→[EEE]をクリックすると、以下の画面が表示されます。

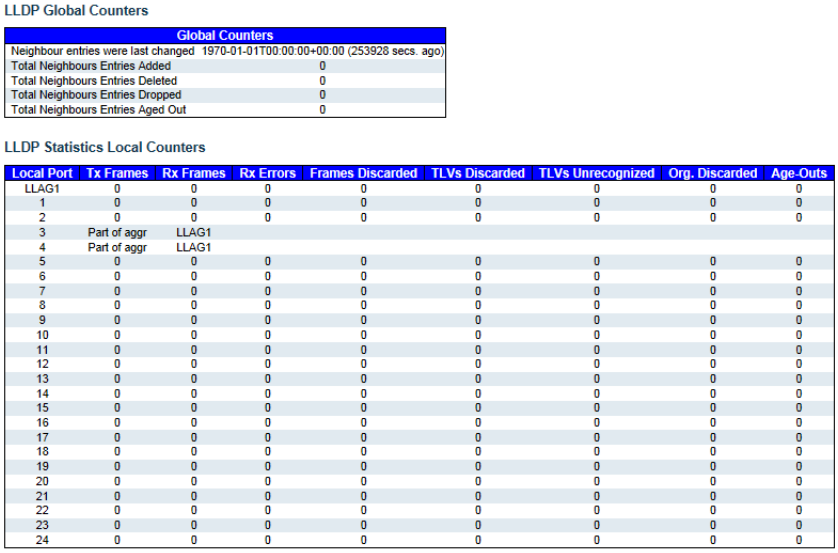


ここでは、LLDP によって交換される EEE 情報を表示します。
EEE の省電力モードにより、トラフィックの遅延を発生することがあります。
省電力モードは電力消費を抑えるために、必要な時だけ回路の電源を切るため、リンク上のトラフィックを再送信する際に回路が再起動する時間が必要となり、その結果遅延が生じます。この遅延時間は「wakeup time」と呼ばれます。

遅延を最小限に抑えるため、それぞれの送信（tx）および受信（rx）の「wakeup time」の情報を交換し、LLDP を使用して相互に必要な最小限の wakeup time を選択します。

2.4.9.3 ポート統計情報(Port Statistics)

[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

Global Counters	
Neighbour entries were last changed	1970-01-01T00:00:00+00:00 (253928 secs. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

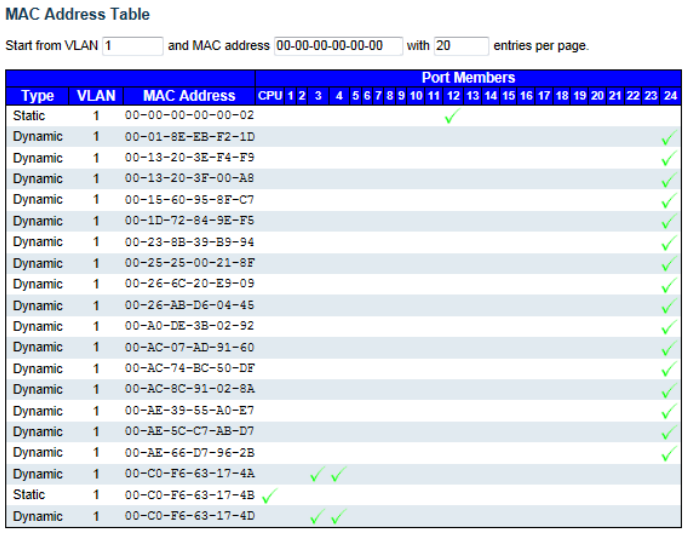
LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
LLAG1	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	Part of aggr	LLAG1						
4	Part of aggr	LLAG1						
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
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	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」はスイッチ全体のカウンタが表示され、
「LLDP Statistics local counters」にはポート単位で表示されます。

2.4.10 MACアドレステーブル情報(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 Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

Type	VLAN	MAC Address	Port Members: CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static	1	00-00-00-00-00-02													✓												
Dynamic	1	00-01-8E-EB-F2-1D																									✓
Dynamic	1	00-13-20-3E-F4-F9																									✓
Dynamic	1	00-13-20-3F-00-A8																									✓
Dynamic	1	00-15-60-95-8F-C7																									✓
Dynamic	1	00-1D-72-84-9E-F5																									✓
Dynamic	1	00-23-8B-39-B9-94																									✓
Dynamic	1	00-25-25-00-21-8F																									✓
Dynamic	1	00-26-6C-20-E9-09																									✓
Dynamic	1	00-26-AB-D6-04-45																									✓
Dynamic	1	00-A0-DE-3B-02-92																									✓
Dynamic	1	00-AC-07-AD-91-60																									✓
Dynamic	1	00-AC-74-BC-50-DF																									✓
Dynamic	1	00-AC-8C-91-02-8A																									✓
Dynamic	1	00-AE-39-55-A0-E7																									✓
Dynamic	1	00-AE-5C-C7-AB-D7																									✓
Dynamic	1	00-AE-66-D7-96-2B																									✓
Dynamic	1	00-C0-F6-63-17-4A				✓	✓																				
Static	1	00-C0-F6-63-17-4B	✓																								
Dynamic	1	00-C0-F6-63-17-4D				✓	✓																				

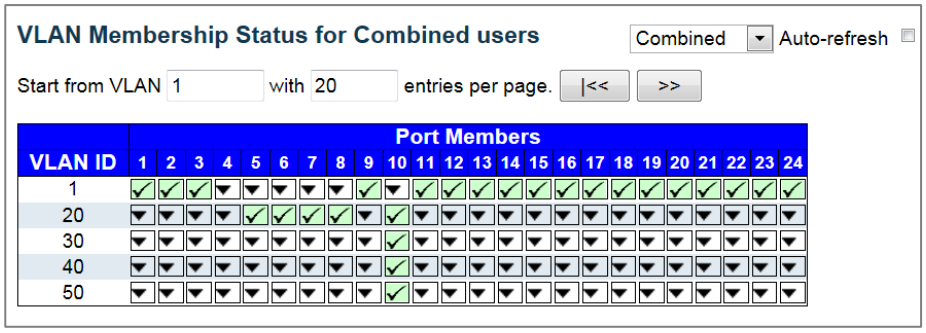
MAC テーブルのエントリが表示されます。MAC テーブルには、エントリは「8192 個」まで含まれ、まず VLAN ID、次に MAC アドレスごとにソートされます。

2.4.11 VLAN情報(VLANs)

VLAN 情報を表示します。

2.4.11.1 VLAN 割当て情報(VLAN Membership)

[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 メンバーのステータスが表示されます。

2.4.10.2 VLAN ポート情報(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　　Static

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	20	UnAware	Disabled	All	Untag_this	20	No
6	20	UnAware	Disabled	All	Untag_this	20	No
7	20	UnAware	Disabled	All	Untag_this	20	No
8	20	UnAware	Disabled	All	Untag_this	20	No
9	1	C-Port	Disabled	All	Tag_All	0	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
19	1	UnAware	Disabled	All	Untag_this	1	No
20	1	UnAware	Disabled	All	Untag_this	1	No
21	1	UnAware	Disabled	All	Untag_this	1	No
22	1	UnAware	Disabled	All	Untag_this	1	No
23	1	UnAware	Disabled	All	Untag_this	1	No
24	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。

2.4.12 sFlow情報(sFlow)

[Monitor]→[sFlow]をクリックすると、以下の画面が表示されます。

sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

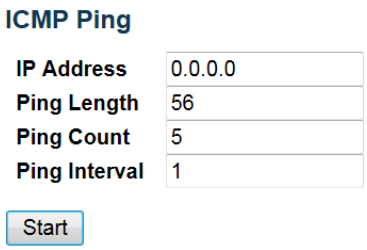
Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0	0	0
13	0	0	0
14	0	0	0
15	0	0	0
16	0	0	0
17	0	0	0
18	0	0	0
19	0	0	0
20	0	0	0
21	0	0	0
22	0	0	0
23	0	0	0
24	0	0	0

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 診断機能(Diagnostics)

2.5.1 IPv4 疎通確認(ping)

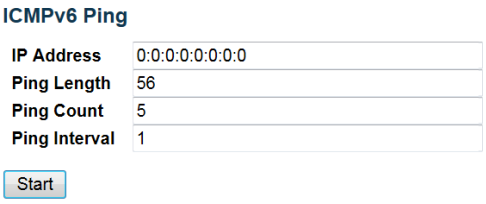
[Diagnostics]→[ping]をクリックすると、以下の画面が表示されます。



ICMP(PING)パケットを送信して、IPv4 の疎通確認を行います。
[Start]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ナンバ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 IPv6 疎通確認(ping6)

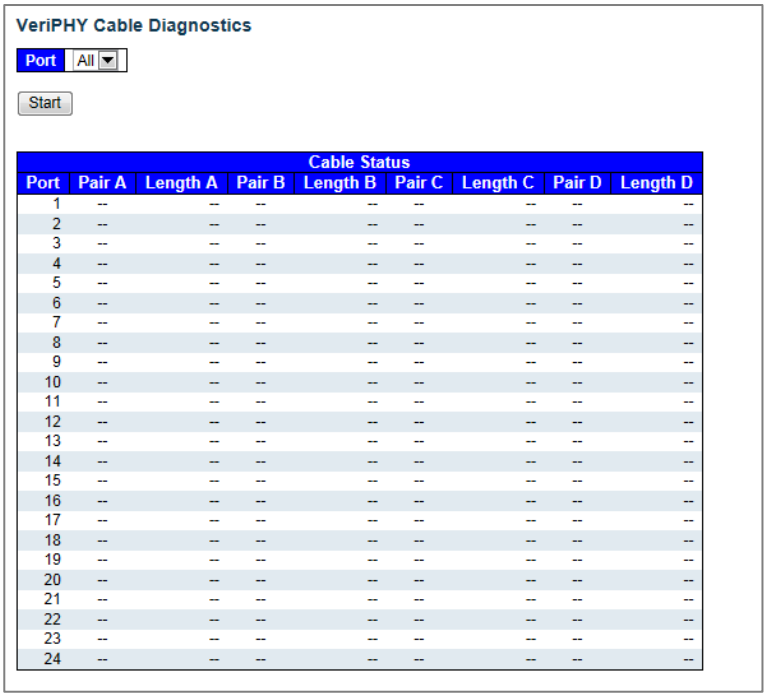
[Diagnostics]→[ping6]をクリックすると、下の画面が表示されます。



ICMPv6(PING)パケットを送信して、IPv6 の疎通確認を行います。[Start]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。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 ケーブル診断(VeriPHY)

[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、10M/100M および 1G ポートの VeriPHY ケーブル診断の設定を行います。
[Start]をクリックすると、診断が開始されます。1 ポートを選択した場合は、約 5 秒かかります。すべてのポートが選択されている場合は、約 15 秒かかります。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確に実行可能です。
10/100Mbps ポートは、VeriPHY が動作時ではリンクダウンするため、管理ポートで VeriPHY を行う場合は、VeriPHY が完了するまで応答しなくなります。

2.6 メンテナンス(Maintenance)

本項目では、再起動や再起動、Config の保存、ファームウェア更新等の機器のメンテナンスを行います。

2.6.1 リスタート(Restart Device）

[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、本機をリスタートします。リスタート後、本機は通常ブートします。

- [Yes] ：デバイスをリスタートします。
- [No] ：リスタートせずに、Port State 画面に戻ります。

2.6.2 工場出荷時設定(Factory Defaults)

工場出荷時に戻すには、[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、本機の設定をリセットします。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、リスタートする必要がありません。

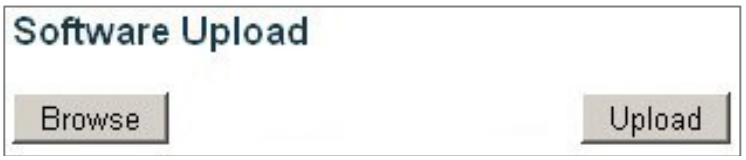
- [Yes] : 工場出荷時の値にリセットします。
- [No] : 設定をリセットせずに、ポートステータスの画面に戻ります。

2.6.3 ファームウェア(Software)

ファームウェアのアップロード、変更を行います。

2.6.3.1 アップロード(Upload)

[Maintenance]→[Software]→[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、ファームウェアのアップデートを行います。

[Browse]ボタンをクリックして、ソフトウェアの FW の保存場所を選択し、[Upload]ボタンをクリックします。

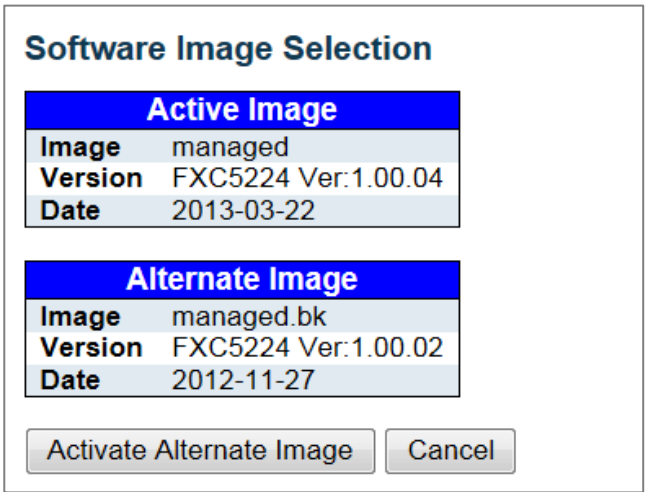
ソフトウェアのアップデートを行う場合、更新が開始されている旨のメッセージが表示されます。
約 1～2 分経過すると、ファームウェアの更新が完了し、本機は再起動します。

本機では、FW のバックアップ機能をサポートしています。古い FW は代替 FW に切り替わり、新規の FW がアクティブな FW になります。旧バージョンを使用したい場合は、
“Image Select”を選択することによりアクティブ FW に設定可能です。

【注記】:
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。障害が起きる可能性があります。

2.6.3.2 ソフトウェアの選択(Image Select)

ソフトウェアを選択するには、[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、デバイスのアクティブおよび代替（バックアップ）ファームウェアについての情報を表示します。
アクティブ FW と、代替 FW についての情報が表示されるため、使用したい FW を選択することが可能です。

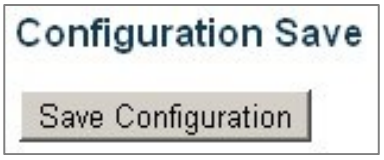
【注記】:
アクティブ FW が代替 FW の場合は。"Active Image"のみが表示されます。“Activate Alternate Image”ボタンは無効になります。
代替 FW を使用したい場合（オリジナル FW に問題が場合等）、新しいファームウェアの FW をアップロードすると、自動的にオリジナルの FW が選択されます。

2.6.4 configファイル操作(Configuration)

設定情報を保存/アップロードを行います。

2.6.4.1 設定情報保存(save)

[Maintenance]→[Configuration]→[Save]をクリックすると、
以下の画面が表示されます。設定情報はテキスト形式で保存されます。



2.6.4.2 設定情報アップロード(Upload)

[Maintenance]→[Configuration]→[Upload]をクリックすると、
以下の画面が表示されます。

[Browse]ボタンをクリックして、ソフトウェアの FW の保存場所を選択後、[Upload]をクリックします。
本機の設定のアップロードを行うことができます。config ファイルは CLI/テキスト形式です。

FXC5210/FXC5218/FXC5224 Management Guide（FXC13-DC-200007-R2.4）

初版	2013 年 3 月
第 2 版	2013 年 4 月
第 3 版	2016 年 6 月
第 4 版	2016 年 10 月
第 5 版	2017 年 2 月
第 6 版	2024 年 8 月

Management Guide
FXC5210/5218/5224

Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide
FXC5210/5218/5224
Management Guide

FXC株式会社