

	Future X Communicatio
Managem Managem	FXC5428 agement Guide
FXC5428	
Management Guide 2016年11月 Ver.1.0	



本マニュアルについて

■本マニュアルでは、FXC5428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。

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。



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。



・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。



はじめに	1
1 章コマンドインタフェース	2
1.1 コマンドラインインタフェースへのアクセス	2
1.1.1 コンソール接続	2
1.2 コマンドによる設定	7
121 基本コマンド	
1.2.2 config モードコマンド	
1.2.3 インタフェース設定コマンド	44
1.2.4 VLAN 設定コマンド	62
1.2.5 show コマンド	63
2章 WEB による設定	132
2.1 Telnet/SNMP 管理	132
2.1.1 Telnet によるマネジメント管理	
2.1.2 SNMP によるマネジメント管理	
2.2 初期設定	132
2.2.1 ログイン方法	
2.3 メインメニュー	135
2.3.1 メニューの構成	
2.4 Configuration(各機能の設定)	
2.4.1 System (システム)	138
2.4.2 Port (ポート設定)	
2.4.3 DHCP	
2.4.4 Security (セキュリティ設定)	145
2.4.5 Aggregation (アグリゲーション)	
2.4.6 Loop Protection (ループプロテクション)	
2.4.7 Spanning Tree (スパニングツリー)	
2.4.8 IPMC Profile (IP マルチキャストのプロファイル)	174
2.4.9 MVR (マルチキャスト VLAN レジストレーション)	
2.4.10 IPMC	
2.4.11 LLDP	
2.4.12 MAG TADIE (MAG $T - J \mu$)	
2.4.13 VLAN 2 & 14 Private VI AN(プライベート VI AN)	
	186
2.4.16 Voice VLAN(音声 VLAN)	
2.4.17 QoS	
2.4.18 Mirroring (ポートミラーリング)	
2.4.19 GVRP	
2.4.20 Stack (スタック接続)	
2.4.21 sFlow	

i

2.5 Monitor(モニタリング)	210
2.5.1 System (システム)	210
2.5.2 Green Ethernet	213
2.5.3 Port (ポート設定)	214
2.5.4 DHCP	217
2.5.5 Security (セキュリティ設定)	219
2.5.6 LACP	
2.5.7 Loop Protection (ループプロテクション)	
2.5.8 Spanning tree (スパニングツリー)	
2.5.9 MVR	
2.5.10 IPMC	
2.5.11 LLDP	
2.5.12 MAC Table	234
2.5.13 VLAN	
2.5.14 Stack (スタック設定)	237
2.5.15 sFlow	237
2.6 Diagnostics (診断機能)	238
2.6.1 Ping	
2.6.2 Ping6	
2.6.3 VeriPHY (ケーブル接続診断)	
2.7 Maintenance (メンテナンス)	240
2.7.1 Restart (システムリブート)	
2.7.2 Factory Defaults (初期設定に戻す)	241
2.7.3 Software (ソフトウェア)	241
2.7.4 Configuration (config ファイルの設定)	

ii

1

はじめに

この度は、弊社 FXC5428 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、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し、設定することも可能です。

1 章コマンドインタフェース

1.1 コマンドラインインタフェースへのアクセス

コンソールポート、又はネットワークからTelnet経由で管理インタ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フェース/CLI)により本機の設定を行います。

1.1.1 コンソール接続

コンソールポートへの接続は、以下の手順で行います。

接続方法:

機器前面の右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、もう片方を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。

	0
ボーレート	115200 Baud
データ	8 Bit
パリティ	なし
ストップビット	1 Bit
フロー制御	なし

- 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、及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。

Press ENTER to get started

Username:

■スタックモード設定時の注意事項:

システムをブートアップした後に、"% Error in file startup-config, line 22: % No such port: GigabitEthernet 6/1" のようなエラーメッセージが表示された場合は、スタック内の一部のスイッチ本体が検出されないことを意味します。 例として、上記のエラーメッセージは、スイッチ ID6 のスイッチが検出されないことを示しています。 この場合は、スイッチ本体の操作エラーではありません。 スタック設定から一部のスイッチ本体を削除する場合は、スタック内の該当メンバーを削除してください。

この設定については、基本コマンドの config モード内の「<u>38. switch コマンド</u>」を使って設定してください。

1.1.1.1 ユーザアカウント

ユーザのアクセスレベルは、1~15段階に分かれています。

デフォルト設定では、それぞれのアクセスレベルは以下のとおりです。

- 1. 管理者向けレベル (レベル 15): すべての機能にアクセス可能であり、デバイスのすべてを管理可能です。
- 2. <u>標準ユーザ向けレベル (レベル 10)</u>メンテナンス機能以外のステータスおよび設定内容を表示したり、 設定を変更したりすることが可能です。
- 3. <u>ゲスト向けレベル (レベル 5)</u>: 本機のステータスおよび設定内容を表示することのみ可能です。
- 【注記】: 1) ユーザの優先レベルは、アクセス先のグループの優先レベル以上の値に設定して下さい。
 2) システムメンテナンス(ソフトウェアのアップロード、工場出荷時設定など)を行う場合は「レベル 15 (管理者向けアカウント)」が必要となります。

1.1.1.2 ユーザのアクセスレベルの設定方法

以下に、コマンドによるユーザレベルの設定方法について説明します。

- 【注記】: この設定は、レベル 15 の管理者向けアカウントを持ったユーザのみ設定可能です。 初期設定時のユーザ名およびパスワードは "admin"/" admin"です。
- 1. 本機にログインすると、プロンプトは"#"と表示されます。

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

# 3		
	clear	Reset functions
	configure	Enter configuration mode
	сору	Copy from source to destination
	debug	Debugging functions
	delete	Delete one file in flash: file system
	dir	Directory of all files in flash: file system
	disable	Turn off privileged commands
	do	To run exec commands in config mode
	dot1x	IEEE Standard for port-based Network Access Control
	enable	Turn on privileged commands
	exit	Exit from EXEC mode
	firmware	Firmware upgrade/swap
	help	Description of the interactive help system
	ip	IPv4 commands
	logout	Exit from EXEC mode
	more	Display file
	no	Negate a command or set its defaults
	ping	Send ICMP echo messages
	reload	Reload system.
	send	Send a message to other tty lines
	show	Show running system information
	switch	Config commands for the switches in the stack
	terminal	Set terminal line parameters
#		

2. 続けて、config モードに移行します。

```
"configure terminal"コマンドを入力すると、以下の画面が表示されます。
システム設定はこの画面で行います。
```

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

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

4. ユーザ名、優先レベル、暗号化、パスワードをそれぞれ設定してください。

```
privilege Set user privilege level
(config) # username guest privilege ?
  <privilegeLevel : 0-15> User privilege level
(config) # username guest privilege 5 ?
  password Specify the password for the user
(config) # username guest privilege 5 password ?
                  Specifies an ENCRYPTED password will follow
  encrypted
                  NULL password
  none
  unencrypted Specifies an UNENCRYPTED password will follow
(config) # username guest privilege 5 password encrypted ?
  <Password : word4-44>The ENCRYPTED (hidden) user password. Notice the
                      ENCRYPTED password will be decoded by system
                      internally. You cannot directly use it as same as
                      the Plain Text and it is not human-readable text
                      normally.
(config) # username quest privilege 5 password encrypted quest ?
  <cr>
            _____
```

5. 以上で、アクセスレベルの設定は完了です。

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

```
Username: guest
Password:
#
```

1. 管理者向けレベル (レベル 15)

管理者レベルでは、本機の基本的 初期設定でのアクセスレベルは、" 本機にログインすると、プロンプトは コンソール用のコマンドラインをサポ	ちなシステム全般を設定することが可能です。 15"です。 "#"と表示されます。 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。
<pre># ? clear configure copy debug dolote</pre>	Reset functions Enter configuration mode Copy from source to destination Debugging functions Delate and file in flack: file system
delete dir disable do dot1x enable	Delete one file in flash: file system Directory of all files in flash: file system Turn off privileged commands To run exec commands in config mode IEEE Standard for port-based Network Access Control Turn on privileged commands
exit firmware help ip logout more	Exit from EXEC mode Firmware upgrade/swap Description of the interactive help system IPv4 commands Exit from EXEC mode Display file
no ping reload send	Negate a command or set its defaults Send ICMP echo messages Reload system. Send a message to other tty lines Show running system information
switch terminal #	Config commands for the switches in the stack Set terminal line parameters

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

2. 標準ユーザ向けレベル (レベル 10)

標準ユーザ向けレベルのユーザは、メンテナンス機能以外のステータスおよび設定内容を表示したり、設定を変更したりすることが可能です。初期設定でのアクセスレベルは、"10"です。

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

#	? ?	
	clear	Reset functions
	debug	Debugging functions
	disable	Turn off privileged commands
	do	To run exec commands in config mode
	enable	Turn on privileged commands
	exit	Exit from EXEC mode
	help	Description of the interactive help system
	logout	Exit from EXEC mode
	no	Negate a command or set its defaults
	ping	Send ICMP echo messages
	show	Show running system information
#		
	 -カぞわの表示 ⁻	

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

3. ゲスト向けレベル (レベル 5)

ゲスト向けレベルのユーザは、本機のステータスおよび設定内容を表示することのみ可能です。 初期設定でのアクセスレベルは、"5"です。

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

# 3	?	
	clear	Reset functions
	debug	Debugging functions
	disable	Turn off privileged commands
	do	To run exec commands in config mode
	enable	Turn on privileged commands
	exit	Exit from EXEC mode
	help	Description of the interactive help system
	logout	Exit from EXEC mode
	no	Negate a command or set its defaults
	ping	Send ICMP echo messages
	show	Show running system information
#		

ファンクションキー

ここでは、コンソール画面用のファンクションキーについて説明します。

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

1.2 コマンドによる設定

コンソール画面用のコマンドモードには、以下の4つがあります。

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、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。プロンプトは"#"と表示されます。 コマンドの詳細については、「1.2.1 基本コマンド」を参照してください。

2. config コマンド

"configure terminal"コマンドを使用すると、グローバル config モードに入ります。 グローバル config モードのコマンドは、本機の一般の設定を行います。 プロンプトは、"(config)#"と表示されます。 コマンドの詳細については、「1.2.2 config モードコマンド」を参照してください。

インタフェース設定(ポート/VLAN グループ設定)コマンド

ポートの設定を行う場合は、グローバル config モードで"interface GigabitEthernet x/y"コマンド、 または"interface 10GigabitEthernet x/y"を入力すると、プロンプトは"(config-if)#"と表示されます。 例えば、"interface GigabitEthernet 1/5"は、ID″1″のスイッチのポート″5″の設定を行います。

VLAN グループを設定する場合は、グローバル config モードにて"interface vlan x"コマンドを使用すると、 プロンプトは"(config-if-vlan)#"に切り替わります。 例えば、"interface vlan 100"は、「VLAN 100」の設定を行います。

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

コマンドの詳細については、「1.2.3 インタフェース設定コマンド」を参照してください。

4. VLAN 設定コマンド

一般的な VLAN 設定を行うには、グローバル config モードにて"vlan x"コマンドを入力します。 プロンプトは"(config-vlan)#"と表示されます。

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

コマンドの詳細については、「1.2.4 VLAN 設定コマンド」を参照してください。

■設定の保存

設定を保存する場合は、基本コマンドモードにて以下のコマンドを入力してください。

copy running-config startup-config

1.2.1 基本コマンド

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

"?"と入力すると、以下のとおりコマンドリストが表示されます。

# ?)	
	clear	Reset functions
	configure	Enter configuration mode
	сору	Copy from source to destination
	debug	Debugging functions
	delete	Delete one file in flash: file system
	dir	Directory of all files in flash: file system
	disable	Turn off privileged commands
	do	To run exec commands in config mode
	dot1x	IEEE Standard for port-based Network Access Control
	enable	Turn on privileged commands
	exit	Exit from EXEC mode
	firmware	Firmware upgrade/swap
	help	Description of the interactive help system
	ip	IPv4 commands
	logout	Exit from EXEC mode
	more	Display file
	no	Negate a command or set its defaults
	ping	Send ICMP echo messages
	reload	Reload system.
	send	Send a message to other tty lines
	show	Show running system information
	switch	Config commands for the switches in the stack
	terminal	Set terminal line parameters
#		

1. clear コマンド

統計情報や MAC アドレステーブルなどをリセットをします。

access	Access management
access-list	Access list
dot1x	IEEE Standard for port-based Network Access Control
ip	Interface Internet Protocol config commands
ipv6	IPv6 configuration commands
lacp	Clear LACP statistics
lldp	Clears LLDP statistics.
logging	Syslog
mac	MAC Address Table
mvr	Multicast VLAN Registration configuration
sflow	Statistics flow.
spanning-tree	STP Bridge
statistics	Clear statistics for one or more given interfaces

2. configure コマンド

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

```
# configure ?
terminal Configure from the terminal
```

3. copy コマンド

本機の内蔵メモリもしくは TFTP サーバを対象に、設定のコピーを行います。

```
# copy ?
flash:filename | tftp://server/path-and-filename File in FLASH or on TFTP
server
running-config Currently running configuration
startup-config Startup configuration
```

本コマンドの記述形式は"copy <コピー対象> <コピー先>"となっております。 <コピー対象>・<コピー先>の部分に、以下の1)~3)から任意に選択して入力します。

- flash:filename | tftp://server/path-and-filename 本機の内蔵メモリまたは TFTP サーバ内の設定データです。
- running-config 本機にて現在動作中の設定データです。 running-configの内容は、本機の再起動時に消去されます。 再起動後も同じ設定を使用したい場合は、本コマンドにて running-config を startup-config に コピーしてください。
- 3) startup-config 本機の起動時に読み出され、running-configへと自動適用される設定データです。

記述例:

- (1) copy running-config flash:test
 - この場合、本機の running-config の設定内容を、本機内蔵メモリ内へファイル名 "test"で コピーします。
- (2) copy flash:Test2 startup-config
 - この場合、本機内蔵メモリ内のファイル"Test2"の設定内容を、本機の startup-config へ コピーします。

4. debug コマンド

DHCP ヘルパーフレーム情報の表示やプロンプトの設定をします。

#	debug ? ip prompt show trace	Interface Internet Protocol config commands Set prompt for testing Show running system information Trace setting
1)	debug ip DHCP \J	dhcp helper frame information レパーフレーム情報を表示するためのコマンドです。
2)	debug pro ターミナルの	mpt <debug_prompt>)プロンプト名を設定するためのコマンドです。</debug_prompt>
3)	debug show secure-st 現在動作中	w ip http [secure-certificate secure-session atistics] Pのシステム情報を表示するためのコマンドです。
4)	debug tra トレースの	ce hunt <line64> 設定を行います。</line64>

5. delete コマンド

本機の内蔵メモリ内のファイルを削除します。

delete ? <Path : word> Name of file to delete

記述例:

delete flash:<ファイル名>

6. dir コマンド

本機の内蔵メモリ内のファイルを参照します。

r-: 読み込みのみ可能なコンフィグであることを示します。

rw: 読み書き可能なコンフィグであることを示します。

7. disable コマンド

特権モードを終了するか、もしくは現状より低いアクセスレベルへと変更ができます。

【注記】: このコマンドによって、現状より高いアクセスレベルには変更することはできません。

```
# disable ?
<0-15>
<cr>
```

8. do コマンド

″do″の後ろにコマンドを入力することで、そのコマンドを実行します。

do ? LINE Exec Command

9. dot1x コマンド

"dot1x initialize ?"と入力すると、サブコマンドを表示します。

```
# dot1x initialize ?
    interface Interface
    <cr>
```

 dot1x initialize [interface (<port_type> [<plist>])] dot1xの初期化を行います。 インタフェースを指定することで、そのインタフェースの dot1x を初期化します。

10. enable コマンド

特権モードに移行するか、もしくはアクセスレベルの変更ができます。

※ 特権モードへの移行、またはアクセスレベルを15に設定するためには、あらかじめ enable パスワードを設定しておく 必要があります。

```
# enable ?
     <0-15> Choose privileged level
     <cr>
```

11. exit コマンド

現在のオペレーションモードを終了し、前のモードに戻ります。

12. firmware コマンド

```
本機のファームウェアの切り替えやアップグレードを行います。

"firmware ?"と入力することで、サブコマンドを表示します。
```

- firmware swap
 現在動作中のファームウェアと代替えファームウェアを切り替えます。
- firmware upgrade <tftpserver_path_file>
 TFTP サーバを指定して、本機のファームウェア更新を行います。

13. help コマンド

help コマンドにより、ターミナルでの"?"コマンドの使用方法が表示されます。

14. IP コマンド

DHCP クエリのプロセスを再実行するためのコマンドです。

ip ? dhcp Dhcp commands

 ・ip dhcp retry interface vlan <vlan_id> 指定した VLAN インタフェースにて、DHCP クエリのプロセスを再実行します。

15. logout コマンド

ログアウト用のコマンドです。

16. more コマンド

本機の内蔵メモリ内または TFTP サーバ内に保存している config ファイルの設定内容を参照します。

```
# more ?
     <Path> File in FLASH or on TFTP server
```

17. no コマンド

設定コマンドの前に"no"をつけることで、その機能を無効にするか、工場出荷時の値に戻すことができます。 例として、"no ip address"コマンドを入力する場合の手順を以下に示します。

(1) グローバル config モードへと移行します。

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

(2) VLAN1 のインタフェース config モードに移行します。

```
(config)# interface vlan 1
(config-if-vlan)#
```

(3) ["]no ip address["]コマンドを入力します。

```
(config-if-vlan)# no ip address
(config-if-vlan)#
```

これにより、VLAN1のIPアドレスが未設定の状態になります。

18. ping コマンド

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

```
_____
# ping ip?
          IP (ICMP) echo
   ip
       IPv6 (ICMPv6) echo
   ipv6
_____
1) ping ip <v ip addr> [repeat <count> ] [size <size> ] [interval <seconds> ]
  - repeat : Ping 実行回数<範囲…1-60 回 デフォルト:5 回>
  - size
       : パケットサイズ<範囲…2-1452byte デフォルト:56byte>
  - interval: Ping 実行間隔<範囲…0-30 秒 デフォルト:0 秒>
  IPv4 アドレスを指定して、対象の端末へと ping を行います。
  Ping 実行回数・パケットサイズ・Ping 実行間隔をそれぞれ指定可能で、特に値を指定しない場合は、
  デフォルト値にて Ping が実行されます。
2) ping ipv6 <v_ipv6_addr> [ repeat <count> ] [ size <size> ] [ interval
    <seconds> ] [ interface vlan <v vlan id> ]
  - repeat : Ping 実行回数<範囲…1-60 回 デフォルト:5 回>
  - size : パケットサイズ<範囲…2-1452byte デフォルト:56byte>
  - interval: Ping 実行間隔<範囲…0-30 秒 デフォルト:0 秒>
  - interface vlan:VLAN インタフェース
```

※VLAN インタフェースは指定する必要があります。

IPv6 アドレス及び VLAN インタフェースを指定して、対象の端末へと ping を行います。 Ping 実行回数・パケットサイズ・Ping 実行間隔をそれぞれ指定可能で、特に値を指定しない場合は、 デフォルト値にて Ping が実行されます。

19. reload コマンド

本機の再起動または初期化する際に使用します。

```
# reload ?
    defaults Reload defaults without rebooting.
    system Reload system.
```

- reload defaults [keep-ip] 本機を初期化します。
 "reload defaults keep-ip"と入力した場合は、管理 IP アドレスを保持し、それ以外の設定の初期化を 行います。
- reload system
 本機をリセットする際に使用します。

20. send コマンド

メール送信システムを通してメッセージを送ります。 送信に失敗すると、send コマンドはエラー・メッセージを表示します。

- (1) *(All tty lines)本機のターミナルに接続している全ての端末へメッセージを送信します。
- (2) <0~16>

本機のターミナルに接続している端末の中から任意に選択して、その端末へメッセージを送信します。

- (3) console 本機のコンソールポートを用いてターミナルに接続している端末へメッセージを送信します。
- (4) vty

本機の vty ポートを用いてターミナルに接続している端末の中から任意に選択して、その端末へメッセージ を送信します。

21. show コマンド

システムの基本設定や情報が表示されます。

#	show ?	
	aaa	Login methods
	access	Access management
	access-list	Access list
	aggregation	Aggregation port configuration
	clock	Configure time-of-day clock
	ddmi	DDMI Serial Info Table
	dotlx	IEEE Standard for port-based Network Access Control
	green-ethernet	Shows green ethernet status for the switch.
	history	Display the session command history
	interface	Interface status and configuration
	ip	Internet Protocol
	ipmc	IPv4/IPv6 multicast configuration
	ipv6	IPv6 configuration commands
	lacp	LACP configuration/status
	line	TTY line information
	lldp	Display LLDP neighbors information.
	logging	Syslog
	loop-protect	Loop protection configuration
	mac	Mac Address Table information mac-auth-username
	mvr	Multicast VLAN Registration configuration
	ntp	Configure NTP
	port-security	Port Security status - Port Security is a module with
		no direct configuration.
	privilege	Display command privilege
	pvlan	PVLAN configuration
	qos	Quality of Service
	radius-server	RADIUS configuration
	rmon	RMON statistics
	running-config	Show running system information
	sflow	Statistics flow.
	snmp	Display SNMP configurations
	spanning-tree	STP Bridge
	switch	show information about the switch
	switchport	Display switching mode characteristics
	tacacs-server	TACACS+ configuration
	terminal	Display terminal configuration parameters
	users	Display information about terminal lines
	version	System hardware and software status
	vlan	VLAN status
	voice	Voice appliance attributes
	web	Web

(1) 各サブコマンドを入力すると、それぞれ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)と入力します。 以下に、"show port-security"コマンドでの help メッセージ表示例を示します。

show port-security ?
 port Show MAC Addresses learned by Port Security
 switch Show Port Security status.

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

```
# show port-security port ?
      Output modifiers
 interface
 <cr>
_____
```

(3) "show port-security port interface *"と入力すると、ポートセキュリティの設定が表示されます。

```
GigabitEthernet 2/1
MAC Address VID State Added Age/Hold Time
_____
<none>
GigabitEthernet 2/2
_____
MAC Address VID State Added Age/Hold Time
----- -----
                      _____
<none>
GigabitEthernet 2/3
 ------
MAC Address VID State Added Age/Hold Time
----- ----
<none>
GigabitEthernet 2/4
_____
MAC Address VID State Added Age/Hod Time
_____ ____
<none>
GigabitEthernet 2/5
_____
MAC Address VID State Added
                          Age/Hold Time
----- ----
                     _____
<none>
.
_____
```

このコマンドの詳細については、「<u>1.2.5 show コマンド</u>」を参照してください。

22. switch コマンド

スイッチがスタック接続されている場合に、このコマンドを入力することでマスタースイッチの再選が 自動的に行われます。

```
_____
# switch stack ?
 re-elect Force to re-elect master switch
   -----
                            _____

    switch stack re-elect
```

マスタースイッチを再選択します。

23. terminal コマンド

本機のターミナルの設定を行います。

<pre># terminal ?</pre>	
editing	Enable command line editing
exec-time	t Set the EXEC timeout
help	Description of the interactive help system
history	Control the command history function
length	Set number of lines on a screen
width	Set width of the display terminal

- editing 本機のコマンドラインのエディットを有効にします。
- exec-timeout <min> [<sec>] 本機のターミナルのタイムアウト時間を設定します。 タイムアウト時間経過後、ユーザは自動的にターミナルからログアウトされます。 単位は<min(分)>と<sec(秒)>にて設定します。

3) help

本機のターミナルについてのヘルプを表示します。

- history
 history コマンドを入力した場合に表示されるコマンド履歴の保存数を設定します。
- 5) length 本機が一度に最大何行まで文字を表示可能か設定します。 最大行数に達した後も表示する内容がある場合は、スペースキーまたは"G"キーを押すことで、 それらを継続して表示します。

6) width

"?"キーを入力した場合の1行ごとに表示可能な最大文字数を設定します。

1.2.2 configモードコマンド

コンソール画面の基本コマンドモードにて"configure terminal"と入力すると、プロンプトが"(config)#"に切り替わります。

本機の一般的な設定については、このモードで設定を行います。

config モードにて"?"と入力すると、以下のサブコマンドが表示されます。

(config)# ?	
aaa	Authentication, Authorization and Accounting
access	Access management
access-list	Access list
aggregation	Aggregation mode
banner	Define a login banner
clock	Configure time-of-day clock
default	Set a command to its defaults
do	To run exec commands in config mode
dot1x	IEEE Standard for port-based Network Access Control
enable	Modify enable password parameters
end	Go back to EXEC mode
exit	Exit from current mode
gvrp	Enable GVRP feature
help	Description of the interactive help system
hostname	Set system's network name
interface	Select an interface to configure
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
lacp	LACP settings
line	Configure a terminal line
lldp	LLDP configurations.
logging	Syslog
loop-protect	Loop protection configuration
mac	MAC table entries/configuration
mac-auth-usernam	e Mac auth username format
monitor	Set monitor configuration.
mvr	Multicast VLAN Registration configuration
no	Negate a command or set its defaults
ntp	Configure NTP
port-security	Enable/disable port security globally.
privilege	Command privilege parameters
qos	Quality of Service
radius-server	Configure RADIUS
rmon	Remote Monitoring
sflow	Statistics flow.
snmp-server	Set SNMP server's configurations
spanning-tree	Spanning Tree protocol
switch	Config commands for the switches in the stack
tacacs-server	Configure TACACS+
username	Establish User Name Authentication
v⊥an	VLAN commands
voice	Voice appliance attributes
web	dam

1. aaa コマンド

ユーザログイン時の認証方式を設定します。

この機能により、管理クライアントインタフェースを介してスイッチへログインする際のユーザ認証が可能になります。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config)# aaa ?
authentication Authentication
```

認証するインタフェースおよび認証方式の設定を行います。

- ・ 認証するインタフェースは、以下から選択可能です。
 - 1) console:コンソールの端末回線
 - 2) telnet:リモートコンソールアクセス(Telnet)用の仮想端末
 - 3) ssh: セキュリティで保護されたリモートコンソールアクセス(SSH) 用の仮想端末
 - 4) http:Web ブラウザと Web サーバの間で HTML などのコンテンツの送受信用の通信プロトコルを使用した 仮想端末

- 認証方式は以下から選択可能です。
 - 1) local:本機に設定されたユーザ名/パスワードにて認証を行います。
 - 2) radius: RADIUS 認証を行います。
 - 3) tacacs: TACACS+認証を行います。

2. access コマンド

管理用 IP フィルタの設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config) # access ?
    management Access management configuration
• access management <1-16> <1-4094> <ipv4_addr> [ to <ipv4_addr> ] { [ web ]
```

[snmp] [telnet] | all }
 管理セキュリティ機能を有効にします。
 本機へアクセスできる IP アドレス範囲や、その IP アドレス範囲内でのアクセス手段の制限を設定することが可能です。

3. access-list コマンド

ACL の設定情報およびステータスを設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

1) access-list ace[<AceId : 1-8192>|update] アクセスリストのエントリ(1-8192)を設定/更新します。 2) access-list rate-limiter[<RateLimiterList : 1~16>|pps] レートリミットの値(1-16)を設定します。

4. aggregation コマンド

このコマンドにより、アグリゲーションのモードを設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config)# aggregation ?
mode Traffic distribution mode
```

(config) # aggregation mode { [smac] [dmac] [ip] [port] }
 このコマンドにより、アグリゲーションの接続モードを設定します。
 設定した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。

5. banner コマンド

このコマンドにより、バナーの設定を行います。

```
(config)# banner ?
LINE c banner-text c, where 'c' is a delimiting character
exec Set EXEC process creation banner
login Set login banner
motd Set Message of the Day banner
```

 banner LINE バナーのテキストを入力します。
 ※ 'c'は区切り文字を示します。

2) banner exec

ルータやスイッチに接続した時点ではなく(banner motd)、パスワード認証が成功した時点でバナーが表示されます。

【注記】: banner exec の後にバナーの区切りの記号として、"\$"、または"#"など、バナーに含まれない 文字を使用して下さい。

3) banner login

ログインバナーを設定します。 本コマンドを実行すると入力待ちの状態になるので、バナーとして表示させたい文字列を入力(複数行可) し、完了したら Ctrl+D を入力してください。 ログインバナーは、リモートからの接続時にログインプロンプトの前に表示されます。

 4) banner motd 機器にログインした時に出力されるバナーメッセージです

6. clock コマンド

このコマンドにより、サマータイムの設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config)# clock ?
 summer-time Configure summer (daylight savings) time
 timezone Configure time zone

- clock summer-time <word16> date [<1-12> <1-31> <2000-2097> <hh:mm> <1-12> <1-31> <2000-2097> <hh:mm> [<1-1440>]]
 サマータイムの設定を行います。
 自動的に夏時間に切り替わるようにシステムを設定します。
- 2) clock timezone <word16> <-12-12> [<0-59>] タイムゾーンの設定を行います。

7. default コマンド

レートリミットの設定を工場出荷時状態にリストアします。

```
(config)# default ?
    access-list Access list
```

default access-list rate-limiter <RateLimiterId : 1-16>
 工場出荷時状態にリストアするレートリミットの ID(1~16までの値)を選択します。

8. do コマンド

このコマンドにより、config モードのまま、基本コマンドを実行できます。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config)# do ?
LINE Exec Command
```

9. dot1x コマンド

802.1x 機能の一般的な設定を行います。"dot1x?"と入力すると、以下の画面が表示されます。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config) # dot1x ?	Authentication
feature	Globally enables/disables a dotly feature
icacuic	functionality
guest-vlan	Guest VLAN
max-reauth-req	The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN
re-authentication system-auth-control timeout	Set Re-authentication state Set the global NAS state timeout

- dot1x authentication timer [inactivity <10-1000000> | re-authenticate <1-3600>]
 認証時のタイムを設定します。
- 2) dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] } dot1x 機能のグローバル設定を行います。
- 3) dot1x guest-vlan [<1-4095>| supplicant] ゲスト用 VLAN の ID を設定します。
 "x":「1~4095」の範囲内の値を持つ VLAN ID です。

この設定は以下のモードに適用されます(例えば、MACアドレスを取得する場合は、ポートセキュリティの機能を使用)。

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth

クライアントによるアクセスが拒否された場合: RADIUSサーバによりクライアントのアクセスが拒否された場合、あるいはRADIUSサーバによりリクエストが タイムアウトとなった場合のいずれかです。クライアントは非認証状態となります。 保持時間には、現在実行中の認証についてはカウントされません。

- dot1x max-reauth-req <1-255>
 再認証回数(1-255 回)を設定します。
- 5) dot1x re-authentication 802.1x 機能の再認証機能を有効にします。 "no dot1x reauthentication"コマンドにより、この機能を無効にします。

この機能が有効な場合は、再認証時間に指定した時間の経過後、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機能有効ポートの再認証により、本機に新しいデバイスが設定されり、サプリカントが接続されてないかどうかを検出します。

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

6) dot1x system-auth-control NASの設定を行います。

- 7) dot1x timeout [quiet-period <10-1000000> | tx-period <1-65535>] 802.1X 機能の認証時間を設定します。
- 10. enable コマンド

特権モードに移行する際のパスワードを設定します。 ※特権モードに移行するためには、本コマンドにてあらかじめ enable パスワードを設定しておく必要があります。

```
(config)# enable ?
  Password Assign the privileged level clear password
  secret Assign the privileged level secret
```

- 1) Enable password [WORD | level] enable パスワードを設定します。
- 2) Enable secret [0 | 5]
 パスワードの暗号化/非暗号化を設定します。
 -0:パスワードを非暗号しない
 -5:パスワードを暗号化する

11. end コマンド

グローバル config モードを終了します。

12. exit コマンド

現在のオペレーションモードを終了し、前のモードに戻ります。

13. gvrp コマンド

gvrp 機能を有効にします。

GVRP(GARP VLAN Registration Protocol)は、VLAN 情報をデバイス間で伝搬するために設計された業界 標準プロトコルです。 GVRP を使用すると、1 つのデバイスはネットワークに必要なすべての VLAN によって手動で設定 されます。また、ネットワーク上の他のすべてのデバイスは、これらの VLAN を動的に記憶します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config)# gvrp ?
max-vlans Number of simultaniously VLANs that GVRP can control
time Config GARP protocol timer parameters. IEEE 802.1D-2004,
clause 12.11.
<cr>
```

- 1) gvrp max-vlans <1-4095> GVRP により同時に制御可能な VLAN 数の上限(1~4095 までの値)を設定します。
- 2) gvrp time { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-5000>] } GARPプロトコルのタイムを設定します。 {join | leave | leaveall}:タイマの種類を示します。

14. help コマンド

help コマンドにより、ターミナルでの"?"コマンドの使用方法が表示されます。

15. hostname コマンド

ネットワーク上の本機の名前を設定します。 この名前は、本機の SNMP エージェント機能のホスト名としても使用します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config)# hostname ?
WORD This system's network name
```

hostname <word32>
 ホストネームはテキストベースでアルファベットにて入力します(32 文字以内)。
 使用可能な文字は A-Z,a-z,0-9 及び-(ハイフン)です。

16. interface コマンド

インタフェースの設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

このコマンドの詳細については、「1.2.3 インタフェース設定コマンド」を参照してください。

17. ip コマンド

このコマンドは、IP 依存機能の設定に使用します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

	(config)# ip ?	
	arp	Address Resolution Protocol
	dhcp	Dynamic Host Configuration Protocol
	dns	Domain Name System
	helper-address	DHCP relav server
	http	Hypertext Transfer Protocol
	iamp	Internet Group Management Protocol
	name-server	Domain Name System
	route	Add IP route
	routing	Enable routing for IPv4 and IPv6
	source	source command
	ssh	Secure Shell
	vorify	verify command
	verrry	
1)	ip arp inspectior	n [entry translate vlan]
	ARP インスペクション情	報の設定を行います。
2)	ip dhcp [relay	snooping database <kword255>]</kword255>
	リレーエージェントの情報	服を設定します。
3)	ip dns proxy	
	DNS(Domain Name	system)サーバの設定を行います。
4)	ip helper-address	s <ipv4_ucast></ipv4_ucast>
	DHCP リレーサーバの	没定を行います。
5)	ip http [secure	-certificate secure-redirect secure-server]
	HTTP セキュリティモー	ドの設定を行います。
6)	ip igmp [host-pr	coxy snooping ssm-range unknown-flooding]
	IGMP (Internet Grou	p Management Protocol)スヌーピングの設定の設定を行います。
	IGMP スヌーピングは	き的な VI AN でのみ有効にできます。 プライベート VI AN またはそのコミュニティ

7) ip name-server [<ipv4_ucast> | dhcp] DNSサーバ情報を設定します。

- 8) ip route <ipv4_addr> IPv4のルート情報を設定します。
- 9) ip routing IPv4/IPv6のルーティング機能を有効にします。
- 10) ip source binding IP ソースガードのバインディング情報を設定します。
- 11) ip ssh 本機への SSH 接続を有効にします。
- ip verify source translate
 IP ソースガードテーブルの動的エントリを静的エントリへと変換します。

18. ipmc コマンド

IPv4/IPv6 マルチキャストアドレスの設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
config)# ipmc ?
    profile IPMC profile configuration
    range A range of IPv4/IPv6 multicast addresses for the profile
```

- 1) ipmc profile <word16> IP マルチキャストの IPMC プロファイルを作成します。
- 2) ipmc range <word16> { <ipv4_mcast> [<ipv4_mcast>] | <ipv6_mcast>] [<ipv6_mcast>] } 作成した IPMC プロファイルの IP マルチキャストアドレス範囲を設定します。

19. ipv6 コマンド

VLAN 用の本機の IPv6 アドレスを設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config)# ipv6 ?
 mld Multicasat Listener Discovery
 route Configure static routes
1) ipv6 mld [host-proxy | snooping | ssm-range | unknown-flooding]
 IPv6 のマルチキャスト情報を設定します。

ipv6 route X:X:X:X::X/<0-128>
 IPv6で学習したルート情報を設定します。

20. lacp コマンド

ポート上で動作している LACP プロトコルを設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config) # lacp ?
   system-priority System priority
(config) # lacp system-priority ?
   <1-65535> Priority value, lower means higher priority
```

Lacp system-priority <1-65535>
 LACP プロトコルのプライオリティを設定します。

21. line コマンド

本機の管理用ターミナル画面の設定をします。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config) # line ?
 <0~16> List of line numbers
 console Console terminal line
 vty Virtual terminal

- line v<0~16> 指定した番号のターミナルを設定します。
 "line 0": コンソールポート接続時のターミナルを設定します。
 "line1~16": telnet 接続時のターミナルを設定します。
- 2) line console
 コンソールポートから接続した場合のターミナル画面を設定します。
- line vty <0~15> telnet 接続時のターミナル画面の設定をします。

22. lldp コマンド

ポートの LLDP 機能を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

holdtime	Sets LLDP hold time (The neighbor switch will
noracime	discarded the LLDP information after "hold time"
	multiplied with "timer" seconds)
reinit	LLDP tx reinitialization delay in seconds.
timer	Sets LLDP TX interval (The time between each LLDP
	frame transmitted in seconds)
transmission-delay	Sets LLDP transmision-delay. LLDP transmission
	delay(the amount of time that the transmission of
	LLDP Fram es will delayed after LLDP configuration
	has changed) in seconds.)

- 1) lldp holdtime <2-10>
 LLDP ホールドタイムを秒単位で設定します。
 この時間を経過すると、LLDP 情報は破棄されます。
- 2) lldp reinit <1-10> LLDPの送信時の遅延タイムを秒単位で設定します。
- 3) 11dp timer <5-32768>
 LLDPの送信間隔を秒単位で設定します。
- 4) lldp transmission-delay <1-8192> LLDPの送信遅延を秒単位で設定します。

23. logging コマンド

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

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
_____
(config) # logging ?
  host
       host
  level
        level
        Enable syslog server
  on
_____
1) logging host logging host <hostname>
   log サーバのドメイン名を設定します。
2) logging level { error | info | warning }
   Syslog サーバへと送信するログのレベルを設定します。

    error : エラーを送信します。

       :情報、警告、エラーを送信します。

    Info

    Warning:警告およびエラーを送信します。

3) logging on
    syslog サーバを有効にします。
```
24. loop-protect コマンド

本機全体でのループ検知機能の有効/無効、シャットダウン時間及びループプロテクションフレームの送信間隔の設定 をします。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

【注記】: ループ検知機能は、ポートごとに設定が必要です。 "(config-if)#"にて設定してください。

(config) # loop-protect ?
 shutdown-time Loop protection shutdown time interval
 transmit-time Loop protection transmit time interval
 <cr>

- loop-protect shutdown-time <0-604800> ループ検知時にポートがシャットダウンされる時間を設定します。 有効な値は、「0~604800秒(7日間)」、「0」の値は、ポートが無効な状態(次のデバイスが再起動する までの状態)を示します。
- loop-protect transmit-time <1-10>
 各ポートのループプロテクションのフレームの送信間隔を設定します。
 この場合の"x"は、送信間隔を表し、有効な値は「1~10 秒」です。

25. mac コマンド

本機全体の MAC アドレスの学習機能を設定します。 "no"をコマンドの前につけることにより、この機能は「無効」になります。

(config)# mac address-table ? aging-time Mac address aging time static Static MAC address

- mac address-table aging-time<0,10-1000000>
 本機のエージングタイムを設定します。
 有効な値(秒単位)は「0,10~1000000 秒」です。
 "0"と入力した場合は、本機の MAC アドレスエージングは無効となります。
- mac address-table static <mac_addr> vlan <vlan_id> interface <port_type_list>
 スタティック MAC アドレスを、指定したポートと VLAN ID 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。

26. monitor コマンド

ポートのミラーリング機能を行う際の宛先ポートと送信元ポートの設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config) # monitor	2
Destination	The destination port. That is the port that trafficed
	should be mirrored to.
source	The source port(s) That is the ports to be mirrored
	to the destination port.

- monitor Destination interface ポートのミラーリング機能の宛先ポートの設定を行います。
- monitor source interface ポートのミラーリング機能の送信元ポートを設定します。

27. mvr コマンド

ポートの MVR 機能を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

- 1) mvr name <MvrName : word16> MVRマルチキャスト名を設定します。
- 2) mvr vlan <vlan_list> 指定した VLAN ID での MVR 設定を行います。

28. no コマンド

機能を無効にするか、設定値を工場設定値に戻します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config)# no ?	
aaa	Authentication, Authorization and Accounting
access	Access management
access-list	Access list
aggregation	Aggregation mode
banner	Define a login banner
clock	Configure time-of-day clock
dotlx	IEEE Standard for port-based Network Access Control
enable	Modify enable password parameters
qvrp	Enable GVRP feature
hostname	Set system's network name
interface	Select an interface to configure
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
lacp	LACP settings
lldp	LLDP configurations.
logging	Syslog
loop-protect	Loop protection configuration
mac	MAC table entries/configuration
	mac-auth-username
monitor	Set monitor configuration.
mvr	Multicast VLAN Registration configuration
ntp	Configure NTP
port-security	Enable/disable port security globally.
privilege	Command privilege parameters
qos	Quality of Service
radius-server	Configure RADIUS
rmon	Remote Monitoring
sflow	Statistics flow.
snmp-server	Enable SNMP server
spanning-tree	STP Bridge
switch	Config commands for the switches in the stack
tacacs-server	Configure TACACS+
username	Establish User Name Authentication
vlan	Vlan commands
voice	Voice appliance attributes
web	Web

29. ntp コマンド

本機の NTP プロトコルを設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config) # ntp ?
  server Configure NTP server
  <cr>
```

ntp server <1-5> ip-address <hostname> <ipv4_ucast> <ipv6_ucast>
 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 つまでサポートされています。

30. port-security コマンド

スイッチ全体のポートセキュリティを設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config)# port-security ?
   aging Enable/disable port security aging.
   <cr>
```

 port-security aging time <10-10000000> ポートセキュリティのエージングタイムを設定します。

31. privilege コマンド

ネットワーク管理者(管理者向けレベル)は、どの特権レベルにどのコマンドが属するかを厳密に設定することができます。機能ごとに特権レベルを変更することが可能です(1~15 レベルまで)。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(co	<pre>onfig) # privilege config-vlan configure dhcp-pool exec if-vlan interface ipmc-profile line rfc2544-profile snmps-host stp-aggr</pre>	? VLAN Configuration Mode Global configuration mode DHCP Pool Configuration Mode Exec mode VLAN Interface Mode Port List Interface Mode IPMC Profile Mode Line configuration mode RFC2544 Profile Mode SNMP Server Host Mode STP Aggregation Mode
1)	privilege confic VLAN 設定モードの特	g-vlan level <0-15> <cmd> 特権レベルを設定します。</cmd>
2)	privilege config グローバル configモー	ıre level <0-15> <cmd> ドの特権レベルを設定します。</cmd>
3)	privilege dhcp-po DHCPプール設定モー	ool level <0-15> <cmd> -ドの特権レベルを設定します。</cmd>
4)	privilege exec le 基本コマンドモードの特	evel <0-15> <cmd> 特権レベルを設定します。</cmd>
5)	privilege if-vla VLAN インタフェースモ	n level <0-15> <cmd> ードの特権レベルを設定します。</cmd>
6)	privilege interfa ポートインタフェースモー	ace level <0-15> <cmd> ・ドの特権レベルを設定します。</cmd>
7)	privilege ipmc-p: IPMCプロファイルモー	rofile level <0-15> <cmd> ドの特権レベルを設定します。</cmd>
8)	privilege line le Line 設定モードの特権	evel <0-15> <cmd> 権レベルを設定します。</cmd>
9)	privilege rfc254 RFC2544 วินวะา่ม	4-profile level <0-15> <cmd> モードの特権レベルを設定します。</cmd>
10) privilege snmps [.] SNMPサーバホストモ	-host level <0-15> <cmd> ードの特権レベルを設定します。</cmd>

11) privilege stp-aggr level <0-15> <cmd> STP アグリゲーションモードの特権レベルを設定します。

32. qos コマンド

システムの QoS 機能を設定します。 Port-based QoS 設定は、"(config-if)#"の下のポート設定モードで設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config)# qos ? map Global QoS Map/Table qce QoS Control Entry wred Weighted Random Early Discard 1) qos map [cos-dscp | dscp-classify | dscp-cos | dscp-egress-translation | dscp-ingress-translation] 本機の QoS マップの情報を設定します。 2) qos qce [<Id : 1-4096> | refresh | update] 本機の QoS の QCE 情報を設定します。 3) qos wred queue <Queue : 0~5>

5) qos wred queue <Queue : 0~5> 本機の QoS のキューごとの設定を行います。

33. radius-server コマンド

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

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config) # radius-server ?
 attribute
 deadtime Time to stop using a RADIUS server that doesn't respond
 host Specify a RADIUS server
 key Set RADIUS encryption key
 retransmit Specify the number of retries to active server
 timeout Time to wait for a RADIUS server to reply

- 1) radius-server attribute [32 <id> | 4 <ipv4> | 95 <ipv6>] 使用する RADIUS サーバの NAS 識別子、IP アドレス(IPv4/IPv6)を設定します。
- radius-server deadtime <1-1440> RADIUS サーバのデッドタイム(1~1440 単位:秒)を設定します。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。 デッドタイムを「1」よりも大きい値に設定すると、この機能が有効になりますが、複数のサーバが設定されて いる場合のみ機能します。
- 3) radius-server host <HostName : word1-255> RADIUS 認証サーバに IP アドレス(1~225までの値)を割り当てます。
- radius-server key <line 1-63>
 RADIUS 認証サーバにシークレットキー(1~63)を割り当てます。
- 5) radius-server retransmit <1-1000> RADIUS 認証サーバへ再送する回数(1~1000 回までの値)を設定します。
- 6) radius-server timeout <1-1000>
 休止しているサーバを指定します。
 タイムアウトの値は、「1~1000」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。

サーバがタイムフレーム内に応答しない場合は、「休止」とみなして、次の有効なサーバに通信を行います (可能な場合)。

34. rmon コマンド

本機の RMON 機能を設定します。RMON グループはグループ 1(統計情報)、グループ 2(履歴)、グループ 3(アラーム)、 グループ 9(イベント)にそれぞれ分かれています。 RMON グループを設定するには、以下のコマンドを使用します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config) # rmon ? alarm Configure an RMON alarm event Configure an RMON event 1) rmon alarm <1-65535> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <uint> <1-2147483647> { absolute | delta } rising-threshold <-2147483648-2147483647> [<0-65535>] falling-threshold <-2147483648-2147483647> [<0-65535>] { [rising | falling | both] } RMON アラームを設定します。アラームエントリIDは、「1~65535」の範囲で設定可能です。 (1) rmon alarm x sample-type [absolute | delta]

- (1) Inion alarm x Sample-type [absolute | delta] 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"は「0~65535 秒」の範囲内のエントリの index になります。 サンプルのタイプは以下のとおりです。
 - absolute:サンプルを直接入手します。
 - delta : サンプル間の差異を算出します。

(2) rmon alarm x startup-alarm [falling | rising | both]
 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。Indexは、「1~65535 秒」
 の範囲内のエントリです。
 サンプルのタイプは以下のとおりです。

- falling : 最初の値が falling threshold に満たない場合は、アラームを出します。
- rising : 最初の値が rising threshold を超えた場合は、アラームを出します。
- both : 最初の値が falling threshold に満たない場合、または rising threshold を超えた場合 はアラームを出します。
- 2) rmon event <1-65535> [log] [trap <word127>] { [description <line127>] } RMON イベントを設定します。
 - event : イベントの ID を 1~65535 の範囲で指定します。
 - log : 各イベントのログテーブルにエントリが作成されます。
 - trap : SNMP トラップが1つまたは複数の管理ステーションに送信されます。
 - ・ description:このイベントを説明するコメントを指定します。(範囲:0~127 文字)

35. sflow コマンド

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 エージェントの 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。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

agent-ip The agent IP address used as agent-address i UDP datagrams. Defaults to IPv4 loopback address. collector-address collector-port Collector UDP port max-datagram-size timeout Receiver timeout measured in seconds. The switch decrements the timeout once per second and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0 the receiver and all its configuration is rese to defaults.	(config)# sflow ?	
collector-addressCollector addresscollector-portCollector UDP portmax-datagram-sizeMaximum datagram size.timeoutReceiver timeout measured in seconds. The switch decrements the timeout once per second and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0 the receiver and all its configuration is rese to defaults.	agent-ip	The agent IP address used as agent-address in UDP datagrams. Defaults to IPv4 loopback address.
timeout Receiver timeout measured in seconds. The switch decrements the timeout once per second and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0 the receiver and all its configuration is rese to defaults.	collector-address collector-port max-datagram-size	Collector address Collector UDP port Maximum datagram size.
	timeout	Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.

- 1) sflow agent-ip { ipv4 <ipv4_addr> | ipv6 <ipv6_addr> } sFlow コレクタごとに、sFlow エージェントの IP アドレスを設定します。
- 2) sflow collector-address[receiver <rcvr_idx_list>] [<ipv4_var> | < ipv6_var> | <domain_name>] sFlow コレクタごとに、sFlow コレクタの IP アドレスを設定します。IPv4 および IPv6 アドレスがサポートされています。
- 3) sflow collector-port <Collector Port : 1-65535> sFlow コレクタごとに、sFlow コレクタのポート番号を設定します。有効なポート番号は「1~65535」で す。
- sflow max-datagram-size <DatagramSize : 200-1468>
 sFlow コレクタごとに、sFlow コレクタのデータサイズの上限を設定します。設定可能な範囲の値は 「200-1468」です。
- sflow timeout [receiver <rcvr_idx_list>] <timeout>
 sFlow コレクタごとに、sFlow コレクタのタイムアウトを設定します。
 サンプリングを行うまでの残りの秒数です。タイムアウトすると、デフォルト設定値に戻ります。

sFlow 機能は、ポート単位で「有効」となります。その他のポートの sFlow 設定は "(config-if)#"モード ("interface ethernet x/y"コマンド)で行います。 詳細については、"sflow"コマンドを参照してください。

36. snmp-server コマンド

本機の SNMP 機能設定用に用います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config) # snmp-server ? accessaccess configurationcommunitySet the SNMP communitycontactSet the SNMP server's contact stringengine-idSet SNMP engine IDhostSet SNMP host's configurationslocationSet the SNMP server's location string security-to-group security-to-group configuration Set trap's configurations trap Set the SNMPv3 user's configurations user Set the SNMP server's version version view MIB view configuration <cr> 1) snmp-server access <GroupName : word32> SNMPv3でのアクセスの設定を行います。 2) snmp-server community [v2c <word127> | v3 <word127>] SNMP プロトコルへのアクセスを許可するためのコミュニティアクセス文字列を設定します。 3) snmp-server contact <line255> 担当者情報(本装置障害時の連絡先)などを設定します。 4) snmp-server engine-id local <word10-32> SNMP サーバのエンジン ID を設定します。 5) snmp-server host <word32> SNMP サーバのホストの設定を行います。 6) snmp-server location <line255> 本機の設置場所を設定します。 【注記】: テキスト文字列にはスペースを含めないでください。または、スペースを引用符で囲んだテキストを 入力してください。 7) snmp-server security-to-group model { v1 | v2c | v3 } name <word32> group <word32> 新しい SNMP (Simple Management Protocol)グループまたは SNMP ユーザを SNMP ビューにマップ するテーブルを設定します。 ・ v1:セキュリティモデルを SNMP バージョン 1 に設定します。 v2c:セキュリティモデルを SNMP バージョン 2c に設定します。 v3:セキュリティモデルを SNMP バージョン 3 に設定します。 8) snmp-server trap SNMP サーバのトラップを設定します。認証に失敗した場合にデバイスが SNMP トラップを送信できるよう にします

9) snmp-server user <word32> engine-id <word10-32> [{ md5 <word8-32> | sha <word8-40> } [priv { des | aes } <word8-32>]] SNMPv3ユーザの設定をします。

- auth-md5パスワード: HMAC-MD5-96 認証レベルを示します。機密用の DES キーの認証と生成のためのパスワードを入力してください。(範囲:8~32 文字)
- auth-sha パスワード: HMAC-SHA-96 認証レベルを示します。機密用の DES キーの認証と生成のためのパスワードを入力してください。(範囲:8~40 文字)
- 10) snmp-server version { v1 | v2c | v3 } SNMP のバージョンを選択します。 SNMP バージョンのオプションは、SNMP v1、SNMP v2c、SNMP v3 です。
- 11) snmp-server view <word32> <word255> { include | exclude } SNMP(Simple Network Management Protocol)サーバ ビュー エントリの作成または更新を行いま す。
 - view(ビュー名): 作成または更新されるビューレコードのラベルを指定します。名前はレコードの参照に使用されます。(範囲:1~30文字)
 - ・ included :指定したビューの種類が含まれていることを示します。
 - ・ excluded :指定したビューの種類が含まれていないことを示します。

37. spanning-tree コマンド

本機のスパニングツリープロトコルを設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(con	fig)# spanning-1	tree ?
	aggregation	Aggregation mode
	edge	Edge ports
	mode	STP protocol mode
	mst	STP bridge instance
	recovery	The error recovery timeout
	transmit	BPDUs to transmit
I) s	panning-tree ago	gregation
	スハニンクツリーのアクリ	ナーション機能を設定します。
"	spanning-tree aggrega	ation"と入力して"Enter"キーを押すと、以下の画面が表示されます。
	それぞれ設定を行ってく	ださい。
-		
(config-stp-aggr)# ?
	do	To run exec commands in config mode
	end	Go back to EXEC mode
	exit	Exit from current mode
	help	Description of the interactive help system
	no	Negate a command or set its defaults
	spanning-tree	Spanning Tree protocol
-		
<u>.</u>		
2) s	panning-tree edg	ge [bpdu-filter bpdu-guard]
	エッシボート上で有効に	こする機能を選択します。
	・ bpdu-guard : エッジ	ポートの BPDU ガードを有効にします。
	 bpdu-filter:エッジオ 	ペートの BPDU フィルタを有効にします。
	•	
3) s	panning-tree mod	de [mstp rstp stp]
•	゙スパニングッリーのオペレ	レーションモード(MSTP, RSTP, STP)を選択します。
	stn 7 パーンガ NU	

- ・ rstp : ラピッド スパニング ツリー プロトコル(RSTP)を有効にします。
- ・ mstp :マルチプル スパニング ツリー プロトコル(MSTP)を有効にします。

- 【解説】:MSTP モードでは、デバイスは隣接デバイスが RSTP を使用している場合に RSTP を使用し、 隣接デバイスが STP を使用している場合は STP を使用します。 RSTP モードでは、隣接デバイスが STP を使用している場合、デバイスは STP を使用します。
- 4) spanning-tree mst [<Instance: 0-7> | forward-time <4-30> | max-age <6-40> | max-hops <6-40> | name <word32> revision <0-65535>] システムの MSTP の設定情報を設定します。
 - 【注記】: MST リージョンのすべてのデバイスは、VLAN マッピング、設定リビジョン番号、およびリビジョン 名が同じである必要があります。
- spanning-tree recovery interval <30-86400>
 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。
- 6) spanning-tree transmit hold-count <1-10> 1秒間に発出する BPDU フレーム数を設定します。

38. switch コマンド

ここでは、スイッチのスタック機能を設定します。

スタック接続すると設定情報やルーティング情報などをスタック内の全スイッチで共有可能となり、物理的には複数のス イッチが1台の仮想的なスイッチとして動作します(スタック内の各スイッチごとに設定を行う必要がありません。) 同一のサブネット内(ブロードキャストドメイン)にあるスイッチを最大16台まで管理可能です。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
_____
(config) # switch ?
  stack Stack configuration
(config) # switch stack ?
  <1-16> Switch ID
  disable disable stacking
  enable enable stacking
  interface Configure stacking interface
  priority Configure master election priority
          Swap switch ID
  swap
                     _____
 switch stack [<1-16> | disable | enable | interface | priority | swap ]
   スタックの詳細設定を行います。
  1) switch stack <1-16> mac <mac-address>
     スイッチ ID (1-16 の範囲で指定)と mac アドレスを設定します。
     このコマンドはスタック機能無効時は設定できません。
  2) switch stack disable
     スタック機能を無効にします。
  3) switch stack enable
     スタック機能を有効にします。
  4) switch stack interface 10GigabitEthernet [ x/1,2 \mid x/1,3 \mid x/1,4 \mid
     x/2,3 \mid x/2,4 \mid x/3,4 \mid
     スタックに使用するポートを10Gigabit4ポートの中から2ポートの組み合わせで設定します。
     "x": スイッチ ID が入ります。
  5) switch stack priority [ <1-16> | local ] <1-4>
     スタックマスター選出のためのプライオリティー値(1-4の範囲で指定)を ID(1-16)または local を指定して
     設定します。
     プライオリティー値が一番小さい機器がスタックマスターとなります。
     このコマンドは、スタック機能無効時は設定できません。
```

 6) switch stack swap [<1-16> <1-16>] 指定したスイッチ ID を別のスイッチ ID へと変更します。 このコマンドは、スタック機能無効時は設定できません。

39. tacacs-server コマンド

TACACS+認証サーバを設定します(最大 5 つまで)。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config) # tacacs-server ?
 deadtime Time to stop using a TACACS+ server that doesn't respond
 host Specify a TACACS+ server
 key Set TACACS+ encryption key
 timeout Time to wait for a TACACS+ server to reply

1) tacacs-server deadtime <1-1440>

応答しない TACACS+サーバの使用を停止するまでの時間(デッドタイム)を設定します(範囲:1~1440 単位:秒)。

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。

【注記】:デッドタイムを「0」よりも大きい値に設定すると、この機能が有効になりますが、複数のサーバが 設定されている場合のみ機能します。

- 2) tacacs-server host{ <word1-255> | <ipv4_ucast> | <ipv6_ucast> } [port <0-65535>] [timeout <1-1000>] [key <line1-63>] TACACS+サーバを指定します。
- 3) tacacs-server key <line1-63> TACACS+の暗号キーを設定します(範囲:1~63文字)。 キー文字列:デバイスとTACACS+サーバの間のすべてのTACACS+通信の認証および暗号化キーを指 定します。このキーは、TACACS+デーモンで使用されている暗号化に一致している必要があ ります。
- 4) tacacs-server timeout <1-1000>

タイムアウトの値(1~1000)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。 サーバがタイムフレーム内に応答しない場合は、休止しているとみなして、次の有効なサーバへの通信を 行います(可能な場合)。

40. username コマンド

新規ユーザの作成を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

username <word31> privilege <0-15> password [encrypted <word4-44> | none | unencrypted <line31>]

```
新規ユーザのユーザ名・パスワード・権限の設定を行います。
```

デフォルト設定では、それぞれのアクセスレベルは以下のとおりです。

- 1. 管理者向けレベル(レベル 15):すべての機能にアクセス可能であり、デバイスのすべてを管理可能です。
- 標準ユーザ向けレベル(レベル 10):メンテナンス機能以外のステータスおよび設定内容を表示したり、設定 を変更したりすることが可能です。
- 3. <u>ゲスト向けレベル(レベル 5);</u>本機のステータスおよび設定内容を表示することのみ可能です。

このコマンドの使用方法の詳細については、「ユーザのアクセスレベルの設定方法」を参照してください。

41. vlan コマンド

VLAN 設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config)# vlan ?	
<vlan list=""></vlan>	ISL VLAN IDs 1~4095
ethertype	Ether type for Custom S-ports
protocol	Protocol-based VLAN commands

- 1) vlan <1-4095> VLAN ID を設定します(範囲:1~4095)。
- 2) vlan ethertype s-custom-port <0x0600-0xffff> Custom S-portsのethertypeを設定します。
- 3) vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id> プロトコルベース VLAN の情報を設定します。

VLAN の設定は、VLAN config モードで行います。 詳細については、「<u>1.2.4 VLAN 設定コマンド</u>」を参照してください。

42. voice コマンド

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。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(c	onfig)# voice ?			
	vlan	Vlan for voice traffic		
(c	onfig)# voice vla	n ?		
	aging-time	Set secure learning aging time		
	class	Set traffic class		
	oui vid	OUL CONFIGURATION		
	 voice vlan [aging-time <10-1000000> class <0-7> oui <oui (line32)<="" li=""> vlan < 1-4095>] Voice VLAN 機能を設定します。 </oui>			
	 voice vlan Voice VLAN se 設定可能な範囲 な場合に使用しま 実際のエージング 	aging-time <10-1000000> ecure learningのエージングタイムを設定します。]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」 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。 「タイムは[age_time; 2 * age_time]です。		
	(2) Voice vlan c Voice VLAN ^{k:} Voice VLAN 上	:lass <0-7> ラフィックのクラスを設定します(範囲:0-7)。 .のトラフィックはすべてこのクラスに適用されます。		
	(3) voice vlan (OUI 値およびその	oui <oui value=""> description <line32> D説明文(32文字以内)を設定します。</line32></oui>		
	(4) Voice vlan Voice VLANの VLAN IDの値は	vid < 1-4095> VLAN ID を設定します。 は、「1~4095」です。		
43. web コマン	۲ ۲			

WEB管理画面におけるユーザのアクセスレベルの設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config)# web ? privilege Web privilege

• (config) # web privilege group <cword> level { [cro <0-15>] [crw <0-15>]
 [sro <0-15>] [srw <0-15>] }

下記のレベルを設定します。

- <cword> : WEB の優先グループを設定します。
 - cro : ConfigurationRead-only <0-15>
 - crw : Configuration/Execute Read/write <0-15>
 - sro : Status/Statistics Read-only <0-15>
 - srw : Status/Statistics Read/write <0-15>

1.2.3 インタフェース設定コマンド

ポートの機能および VLAN グループ機能の設定を行うには、config モードにて"interface"コマンドを使用します。 config モードの"(config)#"プロンプトに続いて、"interface ?"と入力します。

- interface * すべてのスイッチ、あるいはポートに適用されます。
- interface GigabitEthernet x/y 1~24のギガビットイーサネットの"スイッチ ID x/ポート y"の設定を行います。 x/yの指定方法は"interface GigabitEthernet 1/5"は、スイッチ ID1のポート 5、 "interface GigabitEthernet 1/5、6、10-15"はスイッチ ID1のポート 5、6、10、11、12、13、14、15の 設定を行います。※ このコマンドにより、"(config)#"から"(config-if)#"プロンプトに移行します。

詳細については、本項「<u>1.2.3.1 インタフェース config コマンド」</u>を参照してください。

 3) interface 10GigabitEthernet x/y 25~28の10ギガビットイーサネットの"スイッチ ID x/ポート y"の設定を行います。 ※ このコマンドにより、"(config)#"から"(config-if)#"プロンプトに移行します。

詳細については、本項「<u>1.2.3.1 インタフェース config コマンド</u>」を参照してください。

4) interface vlan x <1-4095>

VLAN Group x インタフェース(この場合の"x"は、VLAN ID)を設定します。 VLAN インタフェースへの IP アドレスの割り当てを行う場合は、このコマンドを使用してください。 ※ このコマンドにより、"(config)#"から"(config-if-vlan)#"プロンプトに移行します。

【注記】:

一般的な VLAN の作成は"vlan"コマンドにて行います。 詳細については、「<u>1.2.4 VLAN 設定コマンド</u>」を参照してください。 interface vlan "x"コマンドにより、 VLAN インタフェースの設定ができます。 例えば、 VLAN インタフェースへの 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-vlan)# ip address 192.168.11.198 255.255.255.0

1.2.3.1 インタフェース config コマンド

インタフェース config モードの基本設定モードは、"(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、config モードで"interface GigabitEthernet x/y"コマンドを使用して設定を行います。 "x"にはスイッチIDが、"y"にはポート番号がそれぞれ入ります。

例えば、"interface GigabitEthernet 1/5"の場合は、ID″1″のスイッチのポート″5″の設定を行います。

ポート選択する場合には、以下の記述方法があります。

- interface GigabitEthernet x/y
 - "x":スイッチ ID "y":ポート番号
 - インタフェース config コマンドの設定はスイッチ ID"x"のポート"y"にのみ適用されます。
- interface GigabitEthernet x/y,z...
 - "x":スイッチ ID
 "y"および"z":ポート番号
 インタフェース config コマンドの設定はスイッチ ID["]x["]のポート["]y["],["]z["]…に適用されます。
 例えば、"interface GigabitEthernet 1/2,4"の場合は、スイッチ ID["]1"の Port["]2", Port["]4"に適用されます。
- interface GigabitEthernet x/y-z
 - "x":スイッチ ID
 "y"および"z":ポート番号
 インタフェース config コマンドの設定はスイッチ ID"x"のポート"y~z"に適用されます。
 例えば、"interface GigabitEthernet 1/4-7"の場合は、スイッチ ID"1"のポート"4~7"に適用されます。
- (1) 例として、"interface ethernet 1/5"と入力すると、以下のように表示されます。

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

(2) "?"と入力すると、以下のようにサブコマンドが表示されます。

(config-if)# ?	
access-list	Access list
aggregation	Create an aggregation
do	To run exec commands in config mode
dotlx	IEEE Standard for port-based Network Access Control
duplex	Interface duplex
end	Go back to EXEC mode
excessive-restar	t Restart backoff algorithm after 16 collisions
	(No excessive-restart means discard frame after 16
	collisions)
exit	Exit from current mode
flowcontrol	Traffic flow control
green-ethernet	Green ethernet (Power reduction)
gvrp	Enable GVRP on port(s)
help	Description of the interactive help system
ip	Internet Protocol
ipv6	IPv6 configuration commands
lacp	Enable LACP on this interface
lldp	LLDP configurations.
loop-protect	Loop protection configuration on port
mac	MAC keyword
mtu	Maximum transmission unit
mvr	Multicast VLAN Registration configuration

name	Port name
no	Negate a command or set its defaults
port-security	Enable/disable port security per interface.
pvlan	Private VLAN
qos	Quality of Service
rmon	Configure Remote Monitoring on an interface
sflow	Statistics flow.
shutdown	Shutdown of the interface.
snmp-server	Set SNMP server's configurations
spanning-tree	Spanning Tree protocol
speed	Configures interface speed. If you use 10, 100, or
	1000 keywords with the auto keyword the port will only
	advertise the specified speeds.
switchport	Switching mode characteristics

1. access-list コマンド

本コマンドはアクセスリストを設定するコマンドです。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

((config-if)# access	s-list ?
	action logging	Access list action Logging frame information. Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.
	policy port-state	Policy Re-enable shutdown port that was shutdown by access-list module
	rate-limiter redirect shutdown	Rate limiter Redirect frame to specific port Shutdown incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags)
1)	access-list actio フィルタ条件に一致した - denyを指定した場合 - permitを指定した場合	on { permit deny } E場合のフィルタ動作を指定します。 合 : アクセスを拒否します。 合 : アクセスを許可します。
2)	access-list logg: ログ情報を設定します ログ機能は、パケットサ ログレートが制限されて	ing 。 イズが 1518 未満の場合(VLAN タグなし)、かつシステムログのメモリサイズと こいる場合のみ有効です。
3)	access-list polic アクセスリストのポリシー	cy <0-255> -を設定します(0-255 文字以内)。
4)	access-list port アクセスリストのポート料	-state 犬態を設定します。
5)	access-list rate アクセスリストのレート制	-limiter <1-16> 制限を設定します。

6) access-list redirect interface { <port_type_id> | <port_type_list> } アクセスリストのリダイレクトインタフェースを設定します。 7) access-list shutdown アクセスリストのシャットダウンを設定します。

2. aggregation コマンド

アグリゲーションの設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if)# aggregation ?
  group Create an aggregation group
```

 aggregation group <uint> 指定した静的アグリゲーショングループのメンバーポートに設定します。

3. do コマンド

インタフェース config モードで基本コマンドを実行します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if)# do ?
LINE Exec Command
```

4. dot1x コマンド

ポートごとにネットワークアクセスコントロール機能を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if) # dot1x '	2
guest-vlan	Enables/disables guest VLAN
port-control	Sets the port security state.
radius-qos	doEnables/disables per-port state of RADIUS-assigned
	QoS.
radius-vlan	Enables/disables per-port state of RADIUS-assigned
	VLAN.
re-authenticate	Refresh (restart) 802.1X authentication process.

1) dot1x guest-vlan

ゲスト VLAN を有効/無効にします。 インタフェース上で承認されていないユーザがゲスト VLAN にアクセスできるようにします。

- 【注記】: ゲスト VLAN が定義済みで有効な場合、ポートが承認されていないとポートは自動的にゲスト VLAN に加入し、ポートが承認されるとゲスト VLAN から脱退します。ゲスト VLAN への加入と 脱退を可能にするには、ポートをゲスト VLAN の静的メンバにしないでください。
- 2) dot1x port-control

ポートの承認状態の手動制御を有効にします。

auto: インタフェースでの802.1x認証を有効にします。また、ポートとクライアント間の802.1x認証交換に基づいて、承認された状態または承認されていない状態にポートを遷移させます。

 force-authorized:インタフェースでの802.1x認証を無効にします。また、認証交換なしで、承認た 状態または承認されていない状態にポートを遷移させます。ポートは、クライアントの802.1xベースの認証なしで、通常のトラフィックの再送と受信をします。
 force-unauthorized:承認されていない状態にポートを遷移させ、クライアントによるすべての認証要 求を無視することで、このインタフェースを介したすべてのアクセスを拒否しま す。 デバイスは、このインタフェースを介してクライアントに認証サービスを提供できませ

3) dot1x radius-qos RADIUS 対応の QoS の各ポートの状態を有効/無効にします。

h.

- 4) dot1x radius-vlan RADIUS 対応 VLAN の各ポートの状態を有効/無効にします。
- 5) dot1x re-authenticate クライアントの定期的な再認証を有効にします。

5. duplex コマンド

ポートの duplex 設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if)# duplex ?
  auto Auto negotiation of duplex mode.
  full Forced full duplex.
  half Forced half duplex.
```

- duplex { auto | full |half } duplex を auto/full(全二重) /half(半二重)のいずれかに設定します。
- 【注記】duplex の設定ができるのは、ポートが「10M ポート」または「100M 固定ポート」の場合のみです。 「1000M/10G ポート」は全二重固定です。

6. end コマンド

基本コマンドモードに戻ります。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

7. excessive-restart コマンド

コリジョン発生時にバックオフアリゴリズムを再開します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
    excessive-restart
```

half duplex で接続時コリジョンの発生を連続 16 回検出した場合、バックオフアルゴリズムを 再スタートして該当送信フレームの再送を継続します。

8. exit コマンド

現行のオペレーションモードを終了し、元のモードに戻ります。

9. flowcontrol コマンド

指定したインタフェース上のフロー制御を有効/無効にします。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if)# flowcontrol ?
 off Disable flow control.
 on Enable flow control.

(config-if) # flowcontrol { on | off }
 フローコントロール機能を有効(on)または無効(off)に設定します。

10. gvrp コマンド

gvrp機能を有効に設定します。

GVRP(GARP VLAN Registration Protocol)は、VLAN 情報をデバイス間で伝搬するために設計された業界 標準プロトコルです。GVRP を使用すると、1 つのデバイスはネットワークに必要なすべての VLAN によって手動で設定 されます。また、ネットワーク上の他のすべてのデバイスは、これらの VLAN を動的に記憶します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

11. help コマンド

help コマンドにより、ターミナルでの"?"コマンドの使用方法が表示されます。

12. ip コマンド

インターネットプロトコル(arp/dhcp/igmp/verify)を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if)# ip ? arp Address Resolution Protocol	
arp Address Resolution Protocol	
dhcp Dynamic Host Configuration Protocol	
igmp Internet Group Management Protocol	
verity verity command	

- 1) ip arp inspection { check-vlan | logging | mode } ARP インスペクションの設定を行います。
- ip dhcp snooping trust
 DHCP スヌーピングのトラストポートに設定します。
- 3) ip igmp snooping [filter <word16> | immediate-leave | max-groups <1-10> | mrouter] IGMP スヌーピング設定を行います。
- ip verify source limit <0-2> IP ソースガードを設定します。

13. ipv6 コマンド

インタフェースの IPv6 の設定をします。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if)# ipv6 ?
mld Multicasat Listener Discovery
```

MLD(Multicast Listener Discovery)スヌーピング情報を設定します。

14. lacp コマンド

指定ポートで LACP 機能を有効にします。 この機能により、ポートの優先度を設定します

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if)# LACP ?
  key Key of the LACP aggregation
  role Active / Passive (speak if spoken to) role
  <cr>
1) lacp key { <1-65535> | auto }
```

LACP のポート管理キーを固定設定(1-65535 の範囲で指定)または"auto"に設定します。

2) lacp role { active | passive } LACPのロールを"active"または"passive"に設定します。

15. lldp コマンド

LLDP機能を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if) # llo	dp ?
cdp-aware	Configures if the interface shall be CDP aware
	(CDP discovery
	information is added to the LLDP neighbor table)
receive	Enable/Disable decoding of received LLDP frames.
tlv-select	Which optional TLVs to transmit.
transmit	Enable/Disabled transmision of LLDP frames.

1) lldp cdp-aware

CDP-Aware 機能を有効にします(CDP は"Cisco Discovery Protocol"を指します)。 "no lldp cdp-aware"コマンドにより、この機能を無効にします。

CDP オペレーションは受信した CDP フレームのデコード(復号化)に制限があります(本機から CDP フレー ム送信はできません)。CDP フレームは、ポートの LLDP が有効な場合のみデコーディングされます。 CDP TLVs は LLDP ネイバーテーブルに対応するフィールドにマッピングした場合のみデコード(復号化)さ れます。

それ以外の TLVs はすべて破棄されます(認識不可能な CDP TLVs および破棄された CDP フレームは LLDP 統計情報には表示されません)。

【注記】:

すべてのポートで CDP-Aware が無効な場合、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。一つのポートで CDP-Aware が有効な場合、CDP フレームは本機で終端します。

- 2) lldp receive
 LLDP 機能のフレーム受信を有効に設定します。
- 3) lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name } 指定した情報要素(TLV)を対象スイッチポートからLLDPで送信するよう設定します。
- 11dp transmit
 LLDP 機能のフレーム送信を有効に設定します。

16. loop-protect コマンド

ポートのループプロテクション機能を有効に設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if) # loop-protect ?
    action Action if loop detected
    tx-mode Actively generate PDUs
    <cr>
```

- loop-protect action { [shutdown] [log] } ループ検出時の処理(ポートのシャットダウンまたはログ出力)を設定します。
 "loop-protect action log shutdown"または"loop-protect action shutdown log"と入力した場 合、シャットダウンとログ出力両方が有効になります。
- loop-protect tx-mode ループプロテクション機能の PDU 送信を有効に設定します。

17. mac コマンド

MAC アドレスの学習機能を有効に設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if) # mac ? address-table MAC table configuration

mac address-table learning secure
 MAC アドレスの学習機能を設定します。

18. mtu コマンド

ネットワークにおいて送信可能なデータの最大値をバイト単位で設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if)# mtu ? 1518-10056 Maximum frame size in bytes.

- mtu <1518-10056>
 - MTU(Maximum Transmission Unit)とは、通信機器などが一度に送信できる最大データ量を示します。MTUの値を(1518-10056の範囲で指定)設定します。
 - 【注記】: MTU が大きいほど効率的にデータを送ることができ、実質的な転送速度を向上させることができま すが、雑音等による通信品質が低い環境では、値が小さいほうがエラーなどによる再送が減って 転送効率が高まることがあります。

19. mvr コマンド

ポートの MVR 機能を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

_____ (config-if) # mvr ? immediate-leave Immediate leave configuration MVR multicast name name vlan MVR multicast vlan _____ _____ 1) mvr Immediate Leave MVR の即時脱退機能を有効に設定します。 2) mvr name <word16> type { source | receiver } mvr name <word16>に対する MVR ポートタイプを source または receiver に設定します。 3) mvr vlan <vlan list> type { source | receiver } vlan <vlan list>に対する MVR ポートタイプを"source"または"receiver"に設定します。 - receiver-port : 加入者ポート、かつマルチキャストデータの受信のみを行う場合は、ポートをレシーバ ーポートとして設定します。IGMP/MLD メッセージを発行することにより、マルチキャス トグループのメンバになる場合以外は、データの受信は行いません。 - source-port : ソースポートとしてマルチキャストデータの送受信を行うアップリンクポートを設定しま

す。加入者は直接ソースポートに接続することはできません。

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

20. name コマンド

ポート名を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if)# name ?
    <line32> Maximum length: 32
```

name name 32>

ポート名を32文字以内で設定します。

21. no コマンド

機能を無効にするか、設定値を工場設定値に戻します。

(config-if)# no ?	
access-list	Access list
aggregation	Aggregation keyword
dotlx	IEEE Standard for port-based Network Access
	Control
duplex	Set duplex to default.
excessive-restart	Restart backoff algorithm after 16 collisions
	(No excessive-restart means discard frame
	after 16 collisions)
flowcontrol	Configure flow control.
green-ethernet	Green ethernet (Power reduction)
gvrp	Enable GVRP on port(s)
ip	Internet Protocol
ipv6	IPv6 configuration commands
lacp	Enable LACP on this interface
lldp	LLDP configurations.
loop-protect	Loop protection configuration on port
mac	MAC keyword
mtu	Maximum transmission unit
mvr	Multicast VLAN Registration configuration
name	Port name
port-security	Enable/disable port security per interface.
pvlan	Private VLAN
qos	Quality of Service
rmon	Configure Remote Monitoring on an interface
sflow	Statistics flow.
shutdown	Shutdown of the interface.
snmp-server	Set SNMP server's configurations
spanning-tree	Enable/disable STP on this interface
speed	Configure speed to default.
switchport	Switching mode characteristics

22. port-security コマンド

ポートセキュリティを有効に設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if)#	port-security ?
maximum	Miximum number of MAC addresses that can be learned on this
	set of interfaces.
violation	The action involved with exceeding the limit.
<cr></cr>	

- 1) port-security maximum [<1-1024>] ポートで学習できる MAC アドレス最大数(1-1024 の範囲で指定)を設定します。
- 2) port-security violation { none | trap | trap-shutdown | shutdown } ポートセキュリティー動作時の処理(none/trap/trap-shutdown/shutdown から選択)を設定します。
 - none: 登録されている MAC アドレス以外で接続してきた場合、パケットは破棄されます。
 ただし、セキュリティ違反が発生した場合でも SNMP トラップや Syslog メッセージは送信される事はなく、また、違反カウンターが増加することもありません。trunk ポートにこのモードは
 設定できません。
 - trap: セキュリティ違反が発生した場合に、トラップを送信します。
 - ・ trap-shutdown:セキュリティ違反が発生した場合に、トラップを送信し、ポートをシャットダウンします。
 - shutdown:登録されている MAC アドレス以外で接続してきた場合、ポートは errdisable となり、 シャットダウンされます。また、SNMP トラップや Syslog メッセージが送信されます。

23. pvlan コマンド

プライベート VLAN を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if)# pvlan ?
    isolation Port isolation
```

pvlan isolation
 ポートをアイソレーションポートに設定します。

24. qos コマンド

QoS 機能を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(onfig-if) # gos ?	
(0	, oning in) # 403 :	Class of sorvice configuration
		Class of service configuration
		Diop precedence rever configuration
	dscp-classify	DSCP ingress classification
	dscp-remark	DSCP egress remarking
	dscp-translate	DSCP ingress translation
	map	QoS Map/Table configuration
	policer	Policer configuration
	queue-shaper	Queue shaper configuration
	shaper	Shaper configuration
	storm	Storm policer
	tag-remark	Tag remarking configuration
	trust	Trust configuration
	Wrr	Weighted round robin configuration
	wii	
1)	qos cos <0-7> CoSのクラス値(0-7の ポートが信頼されている CoS値の割り当てに何	〕範囲で指定)を設定します。 5場合、ポートのデフォルト CoS 値は、ポートで受信するタグなしのパケットへの を用されます。
2)	qos dpl <0-3> ポートの DPL(Drop P	recedence Level :0-3 の範囲で指定)を設定します。
3)	qos dscp-classify ポート入力 DSCP 機	- { zero selected any } 能のクラス分け種類(zero/selected/any から選択)を設定します。
4)	qos dscp-remark 入力 DSCP リライト機	: rewrite remap } 能の種類(rewrite/remap から選択)を設定します。
5)	qos dscp-translat ポート入力 DSCP 変	_{こe} 換機能を有効に設定します。
6)	qos map cos-tag o ポート出力タグリマーク ~7」で指定)、DEI 値	cos <0~7> dpl <0~1> pcp <0-7> dei <0-1> 機能の Map の CoS 値(「0~7」で指定)、DPL 値(「0~1」で指定)、PCP 値(「0 (「0~1」で指定)を設定します。
7)	qos policer <100- ポート入力ポリシャーの	-13200000> レート値(100-13200000 kbps の範囲で指定)を設定します。
8)	qos queue-shaper <0~7>で指定したキュ す。	_{queue} <0~7> <100–13200000> ーの出力シェーパーのレート値(100-13200000 kbps の範囲で指定)を設定しま
9)	qos storm { unica ストームコントロール機 レート値(100-132000	ast broadcast unknown } <100-13200000> 能のフレーム種別(unicast/broadcast/unknownから選択)と)00 kbps の範囲で指定)を設定します。
10)	qos tag-remark ポート出力タグリマーク ポート出力タグリマーク	(mapped pcp <0-7> dei <0-1> } 機能を Mapped モードに設定します。 機能の PCP 値(0-7 で指定)と DEI 値(0-1 で指定)を設定します。

- 11) qos trust dscp DSCP 機能を有効に設定します。
- 12) qos wrr <1-100> <1-100> <1-100> <1-100> <1-100> <1-100> キューの閾値(0~5まで)のWRR 値を(1~100の範囲で指定)設定します。

25. rmon コマンド

RMON 機能の設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if)# rmon ?
 collection Configure Remote Monitoring Collection on an interface

- rmon collection history <1-65535> [buckets <1-65535>] [interval <1-3600>]rmon collection stats <1-65535>
 RMONの履歴収集の設定を行います。
- rmon collection history <1-65535> buckets <1-65535> 統計の RMON 収集履歴グループに指定したパケット数を設定します。 指定しない場合、デフォルトの「50」になります(範囲:1~65535)。
- rmon collection history <1-65535> interval <1-3600>
 RMON 収集間隔を設定します(範囲:1~3600 秒)。
 デフォルトでは 1800 秒に設定されています。
- 3) rmon collection stats <1-65535> RMON 統計情報収集の設定をします(範囲:1~65535)。

26. sflow コマンド

sFlow コレクタの設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if)# sflow ?	
counter-poll-interval	The interval - in seconds - between counter poller
	samples.
max-sampling-size	Specifies the maximum number of bytes to transmit
	per flow sample.
sampling-rate	Specifies the statistical sampling rate. The
	sample rate is specified as N to sample 1/Nth of
	the packets n the monitored flows. There are no
	restrictions on the value, but the switch will
	adjust it to the closest possible sampling rate.
<cr></cr>	
<cr></cr>	the packets n the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate.

1) sflow counter-poll-interval <1-3600> 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(「1~3600 秒」までの値)。

- sflow max-sampling-size <14-200> 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(「14~200 bytes」 までの値)。最大データサイズがヘッダーの最大サイズに収まらない場合、サンプリングデータは破棄されま す。
- 3) sflow sampling-rate <1-4294967295> 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(サンプリングレート「1~4294967295の 値」)。サンプルレートを"N"と設定し、ポートで送受信されたパケットの"1/N"番目で平均を算出します。サ ンプリングしたすべてのデータが算出されるわけではありません。 サポートされていないサンプリングレートを要求された場合は、一番近いサンプリングレートに自動的に調 整します。

27. shutdown コマンド

ポートをシャットダウンします。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

28. snmp-server コマンド

SNMP サーバを設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

```
(config-if) # snmp-server ?
```

host Set SNMP host's configurations

snmp-server host <word32>
 SNMP サーバのホスト名を設定します(32 文字以内)。

29. spanning-tree コマンド

ポートのスパニングツリー機能を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if) # spanning-tree ?
 auto-edge Auto detect edge status
 bpdu-guard Enable/disable BPDU guard
 edge Edge port
 link-type Port link-type
 mst STP bridge instance
 restricted-role Port role is restricted (never root port)
 restricted-tcn Restrict topology change notifications
 <cr>

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

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

3) spanning-tree edge

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

- spanning-tree link-type { point-to-point | shared | auto } ポートの接続方法(「ポイントツーポイント」、「共有」、「自動」のいずれか)を設定します。
- 5) spanning-tree mst <instance> cost { <cost> | auto } spanning-tree mst <instance> port-priority <prio> スパニングツリーの MST(Multiple Spanning Tree)の設定をします。
 - 5-1) spanning-tree mst <instance> cost { < 1-20000000> | auto } ポートのパスコストを設定します。(1-20000000 または自動)auto に設定した場合は、パスコストが 自動で決定されます。
 - 5-2) spanning-tree mst <instance> port-priority <0-240> ポートのプライオリティを設定します。(0~240までの値)
- spanning-tree restricted-role MSTP での動作を制限します。この機能が有効な場合は、スパニングツリーのプライオリティが高い場合で も、CIST、MSTI などのルートポートとして選択することはできません。 このポートはルートポートが選択された後に、代替ポートとして選択されます。 代替ポートを設定すると、スパニングツリーの接続が切れる場合があります。

すべてのブリッジが管理者の制御下にない可能性があるので、ネットワーク管理者によりネットワークの中 核領域外のブリッジがスパニングツリーのアクティブトポロジーに影響を与えないように設定を行うことができ ます。

この機能は、"ルートガード"と呼ばれます。 "no spanning-tree restrictedrole "コマンドにより、この機能を無効にします。

7) spanning-tree restricted-tcn

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。

30. speed コマンド

ポートの通信速度を設定します。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if)# speed ?
 10 10Mbps
 100 100Mbps
 1000 1Gbps
 10g 10Gbps
 auto Auto negotiation

- 1) speed 10 :10M の通信速度に設定します。
- 2) speed 100 :100M の通信速度に設定します。
- 3) speed 1000 :1000M(1G)通信速度、全二重モードに設定します。

4) speed 10G :10G の通信速度、全二重モードに設定します。

5) speed auto :auto-negotiation モードに設定します。

【注記】

このコマンドでは duplex の設定ができません。10M または 100M 固定ポートの duplex を設定する場合は、インタフェース設定コマンドの「5. duplex コマンド」を使って設定してください。 なお、1000M/10G のポートは duplex は全二重固定です。

31. switchport コマンド

ポートの VLAN の設定を行います。

"no"をコマンドの前につけることにより、この機能は「無効」になります。

(config-if)#	switchport ?
access	set access mode characteristics of the interface
forbidden	Adds or removes forbidden VLANs from the current list of
	forbidden VLANs
hybrid	Change PVID for hybrid port
mode	Set mode of the interface
trunk	Change PVID for trunk port
vlan	VLAN commands
voice	Voice appliance attributes

- 1) switchport access vlan <vlan_id> Access モード時のポート VLAN ID を設定します。
- 2) switchport forbidden { add | remove } { { vid <vlan_id> } | { name <word> } } 指定した VLAN IDを forbidden VLAN へ追加するか、または forbidden VLAN から削除します。
- 3) switchport hybrid { acceptable-frame-type | allowed | egress-tag | ingress-filtering | native | port-type } ハイブリッドモードのポートの設定を行います。
- 4) switchport mode { access | trunk | hybrid } ポートの VLAN に関するモード(access/trunk/hybrid から選択)を設定します。
- 5) switchport trunk { allowed | native | vlan } トランクモード時の VLAN の設定を行います。
- 6) switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid> switchport vlan mac <mac_addr> vlan <vid> switchport vlan protocol group <grp_id> vlan <vid>

```
VLAN の設定(IP サブネットベース/MAC アドレスベース/プロトコルベース)を行います。
```

- 6-1) switchport vlan ip-subnet id <1-128> <ipv4> vlan <vlan_id> IP サブネットベース VLAN の設定を行います。
- 6-2) switchport vlan mac <mac_addr> vlan <vlan_id> MAC アドレスベース VLAN の設定を行います。
- 6-3) switchport vlan protocol group <grp_id> vlan <vlan_id> プロトコルベース VLAN の設定を行います。
- 7) switchport voice vlan { discovery-protocol | mode | security } 音声 VLAN の属性を設定します。

1.2.4 VLAN設定コマンド

VLAN インタフェースの設定を行うには、config モードにて"interface vlan x" コマンドを使用します。 config モードの "(config)#"プロンプトに続いて、"interface vlan x"と入力します。 "x"には VLAN ID を入力します。

例えば、"interface vlan 100"は、VLAN100の設定を行います。 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。

【注記】:

VLAN グループの作成/追加は、config モードの"vlan"コマンドで行ってください。 詳細については、「VLAN 設定コマンド」を参照してください。

例として、VLAN100の VLAN インタフェース config モードに入る場合の入力例を以下に示します。

(1) config モードの "(config)#"プロンプトに続いて、"interface vlan 100"と入力します。

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

(2) "?"と入力すると、以下のようにサブコマンドが表示されます。

<pre>(config-if-vlan)# ?</pre>	
do	To run exec commands in config mode
ena evit	GO DACK TO EXEC MODE
help	Description of the interactive help system
ip	IPv4 configuration
ipv6	IPv6 configuration commands
no	Set a command to its defaults
1) do コマンド	config モードで基本コマンドを実行します。
2) end コマンド	基本コマンドモードまで戻ります。
3) exit コマンド	現在のオペレーションモードを終了し、前のモードに戻ります。
4) help コマンド	help コマンドにより、ターミナルでの"?"コマンドの使用方法が表示されます。
5) ip コマンド	IPv4 を設定します。
6) ipv6 コマンド	IPv6 を設定します。
7) no コマンド	デフォルト設定値(ip/ipv6)に戻ります。

1.2.5 showコマンド

show コマンドにより、システムの基本設定や情報が表示されます。

"show ?"と入力すると、以下のサブコマンドが表示されます。

#	show ?	
	aaa	Login methods
	access	Access management
	access-list	Access list
	aggregation	Aggregation port configuration
	clock	Configure time-of-day clock
	ddmi	DDMI Serial Info Table
	dot1x	IEEE Standard for port-based Network Access Control
	green-ethernet	Shows green ethernet status for the switch.
	history	Display the session command history
	interface	Interface status and configuration
	ip	Internet Protocol
	ipmc	IPv4/IPv6 multicast configuration
	ipv6	IPv6 configuration commands
	lacp	LACP configuration/status
	line	TTY line information
	lldp	Display LLDP neighbors information.
	logging	Syslog
	loop-protect	Loop protection configuration
	mac	Mac Address Table information
	mac-auth-usernam	le
	mvr	Multicast VLAN Registration configuration
	ntp	Configure NTP
	port-security	Port Security status - Port Security is a module with
		no direct configuration.
	privilege	Display command privilege
	pvlan	PVLAN configuration
	qos	Quality of Service
	radius-server	RADIUS configuration
	rmon	RMON statistics
	running-config	Show running system information
	sflow	Statistics flow.
	snmp	Display SNMP configurations
	spanning-tree	STP Bridge
	switch	show information about the switch
	switchport	Display switching mode characteristics
	tacacs-server	TACACS+ configuration
	terminal	Display terminal configuration parameters
	users	Display information about terminal lines
	version	System hardware and software status
	vlan	VLAN status
	voice	Voice appliance attributes
	web	Web

ここでは、すべてのコマンドで表示される" | "について説明します。

show コマンドでは、下記の例示のように "?" コマンドを入力することで、入力可能なコマンドが表示されます。 例: (1) "show aaa ?"を入力します

全てのコマンドで" | "が表示されます。

(2) 次に、"show aaa | ?"と入力します

# show aaa ?	
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match

″ | ″以降のコマンドは必ず上記3コマンドになります。

以下に、"show aaa"コマンドにおける表示例を示します。

■ show aaa | begin <line>コマンド

line>:任意の文字列

"show aaa"コマンドを実行した場合に表示される情報のうち、<line>に入力した文字列と一致する文字を含む行から情報の表示を開始します。

例:

```
# show aaa | begin l
Console : local
telnet : local
ssh : local
http : local
```

■ show aaa | exclude <line>コマンド

line>:任意の文字列

´´show aaa´´コマンドを実行した場合に表示される情報のうち、<line>に入力した文字列と一致する文字を含む行を 除いて表示します。

```
例:
```

```
# show aaa | exclude t
    console : local
    ssh : local
```

■ show aaa | include <line>コマンド

line>:任意の文字列

"show aaa"コマンドを実行した場合に表示される情報のうち、<line>に入力した文字列と一致する文字を含む 行のみを表示します。

例:

```
# show aaa | include ssh
    ssh : local
```
1. show aaa コマンド

AAA 認証のステータス情報を表示します。

_____ # show aaa Console : local telnet : local ssh : local : local http _____ _____ 2. show access management { * }コマンド 管理用 IP フィルタの設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。 "show access management ?"と入力すると、以下のサブコマンドが表示されます。 -----# show access management ? <AccessIdList : 1~16> ID of access management entry Output modifiers statistics Statistics data <cr> _____ 例: _____ # show access management 2 Switch access management mode is disabled W: WEB/HTTPS S: SNMP T: TELNET/SSH WST Idx VID Start IP Address End IP Address ____ ____ 2 100 192.168.1.2 192.168.1.2 ΝΥΥ _____

3. show access management statistics コマンド

管理用 IP パケットの統計情報を表示します。

_____ # show access management statistics Access Management Statistics: Receive: _____ 0 Allow: 0 Discard: 0 Allow: 0 Discard: HTTP 0 HTTPS Receive: 0 0 Allow: SNMP Receive: 0 Allow: 0 Discard: 0 TELNET Receive: 0 Discard: 0 SSH Receive: 0 Discard: 0 _____

4. show access-list{*}コマンド

```
ACLの設定情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

″show access-list ?″と入力すると、以下のサブコマンドが表示されます。

```
_____
# show access-list ?
            Output modifiers
Access list entry
  ace
             The local ACEs status
Select an interface to configure
  ace-status
  interface
  rate-limiter Rate limiter
   <cr>>
          _____
例)
_____
# show access-list
Switch access-list ace number: 0
Switch access-list rate limiter ID 1 is 1 pps
Switch access-list rate limiter ID 2 is 1 pps
Switch access-list rate limiter ID 15 is 1 pps
Switch access-list rate limiter ID 16 is 1 pps
GigabitEthernet 1/1 :
GigabitEthernet 1/1 access-list action is permit
GigabitEthernet 1/1 access-list policy ID is 0
GigabitEthernet 1/1 access-list rate limiter ID is disabled
GigabitEthernet 1/1 access-list redirect is disabled
GigabitEthernet 1/1 access-list logging is disabled
GigabitEthernet 1/1 access-list shutdown is disabled
GigabitEthernet 1/1 access-list port-state is enabled
GigabitEthernet 1/1 access-list counter is 0
GigabitEthernet 1/2 :
_____
GigabitEthernet 1/2 access-list action is permit
GigabitEthernet 1/2 access-list policy ID is 0
GigabitEthernet 1/2 access-list rate limiter ID is disabled
GigabitEthernet 1/2 access-list redirect is disabled
GigabitEthernet 1/2 access-list logging is disabled
GigabitEthernet 1/2 access-list shutdown is disabled
GigabitEthernet 1/2 access-list port-state is enabled
GigabitEthernet 1/2 access-list counter is 0
GigabitEthernet 1/24 :
_____
GigabitEthernet 1/24 access-list action is permit
GigabitEthernet 1/24 access-list policy ID is 0
GigabitEthernet 1/24 access-list rate limiter ID is disabled
GigabitEthernet 1/24 access-list redirect is disabled
GigabitEthernet 1/24 access-list logging is disabled
GigabitEthernet 1/24 access-list shutdown is disabled
GigabitEthernet 1/24 access-list port-state is enabled
GigabitEthernet 1/24 access-list counter is 0
10GigabitEthernet 1/1 :
_____
10GigabitEthernet 1/1 access-list action is permit
```

```
10GigabitEthernet 1/1 access-list policy ID is 0
10GigabitEthernet 1/1 access-list rate limiter ID is disabled
10GigabitEthernet 1/1 access-list redirect is disabled
10GigabitEthernet 1/1 access-list logging is disabled
10GigabitEthernet 1/1 access-list shutdown is disabled
10GigabitEthernet 1/1 access-list port-state is enabled
10GigabitEthernet 1/1 access-list counter is 0
10GigabitEthernet 1/2 :
_____
10GigabitEthernet 1/2 access-list action is permit
10GigabitEthernet 1/2 access-list policy ID is 0
10GigabitEthernet 1/2 access-list rate limiter ID is disabled
10GigabitEthernet 1/2 access-list redirect is disabled
10GigabitEthernet 1/2 access-list logging is disabled
10GigabitEthernet 1/2 access-list shutdown is disabled
10GigabitEthernet 1/2 access-list port-state is enabled
10GigabitEthernet 1/2 access-list counter is 0
                            -----
```

5. show access-list ace statistic {*}コマンド

ACL のエントリー情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show access-list ace statistics ?"と入力すると、以下のサブコマンドが表示されます。

```
_____
# show access-list ace statistics ?
  <AceId : 1~8192>
                 ACE ID
                   Output modifiers
                   Select an interface to configure
  interface
  rate-limiter
                   Rate limiter
  <cr>>
          _____
例:
       # show access-list ace statistics
ID SID Policy Frame Action Rate L. Counter
   ___
        ----- ----- ------
       Any Any Permit Disabled 85018
Any Any Permit Disabled 0
10 Any
20 1
```

6. show access-list ace statistics interface {*}コマンド

インタフェースに設定された ACL 設定情報を示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

" show access-list ace statistics interface ?"と入力すると、以下のサブコマンドが表示されます。

#	show access-list a	ce statistics interface ?
		Output modifiers
	*	All switches or All ports
	GigabitEthernet	1 Gigabit Ethernet Port
	10GigabitEthernet	10 Gigabit Ethernet Port
	rate-limiter	Rate limiter
	<cr></cr>	

例: _____ # show access-list ace statistics interface GigabitEthernet 1/1 ID SID Policy Frame Action Rate L. Counter ----- ----- ----- -----___ ___ 2 Any Any Any Permit Disabled 270 Switch access-list ace number: 1 GigabitEthernet 1/1 : _____ GigabitEthernet 1/1 access-list action is permit GigabitEthernet 1/1 access-list policy ID is 0 GigabitEthernet 1/1 access-list rate limiter ID is disabled GigabitEthernet 1/1 access-list redirect is disabled GigabitEthernet 1/1 access-list logging is disabled GigabitEthernet 1/1 access-list shutdown is disabled GigabitEthernet 1/1 access-list port-state is enabled GigabitEthernet 1/1 access-list counter is 0 GigabitEthernet 1/2 : _____ GigabitEthernet 1/2 access-list action is permit GigabitEthernet 1/2 access-list policy ID is 0 GigabitEthernet 1/2 access-list rate limiter ID is disabled GigabitEthernet 1/2 access-list redirect is disabled GigabitEthernet 1/2 access-list logging is disabled GigabitEthernet 1/2 access-list shutdown is disabled GigabitEthernet 1/2 access-list port-state is enabled GigabitEthernet 1/2 access-list counter is 0 GigabitEthernet 1/24 : _____ GigabitEthernet 1/24 access-list action is permit GigabitEthernet 1/24 access-list policy ID is 0 GigabitEthernet 1/24 access-list rate limiter ID is disabled GigabitEthernet 1/24 access-list redirect is disabled GigabitEthernet 1/24 access-list logging is disabled GigabitEthernet 1/24 access-list shutdown is disabled GigabitEthernet 1/24 access-list port-state is enabled GigabitEthernet 1/24 access-list counter is 0 10GigabitEthernet 1/1 : _____ 10GigabitEthernet 1/1 access-list action is permit 10GigabitEthernet 1/1 access-list policy ID is 0 10GigabitEthernet 1/1 access-list rate limiter ID is disabled 10GigabitEthernet 1/1 access-list redirect is disabled 10GigabitEthernet 1/1 access-list logging is disabled 10GigabitEthernet 1/1 access-list shutdown is disabled 10GigabitEthernet 1/1 access-list port-state is enabled 10GigabitEthernet 1/1 access-list counter is 0 10GigabitEthernet 1/2 : _____ 10GigabitEthernet 1/2 access-list action is permit 10GigabitEthernet 1/2 access-list policy ID is 0 10GigabitEthernet 1/2 access-list rate limiter ID is disabled 10GigabitEthernet 1/2 access-list redirect is disabled 10GigabitEthernet 1/2 access-list logging is disabled 10GigabitEthernet 1/2 access-list shutdown is disabled 10GigabitEthernet 1/2 access-list port-state is enabled 10GigabitEthernet 1/2 access-list counter is 0

```
7. show access-list ace statistics rate-limiter {*}コマンド
```

ACL のエントリー情報とレートリミット設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show access-list ace statistics rate-limiter ?"と入力すると、以下のサブコマンドが表示されます。

```
# show access-list ace statistics rate-limiter ?
                       Rate limiter ID
  <RateLimiterList : 1~16>
  Output modifiers
                          Select an interface to configure
  interface
  <cr>
       _____
例:
_____
# show access-list ace statistics rate-limiter
ID SID Policy Frame Action Rate L. Counter
  ___
         ----- ----- ------ ------
        Any Any Permit Disabled
2
  Any
                                  150
Switch access-list ace number: 1
Switch access-list rate limiter ID 1 is 1 pps
Switch access-list rate limiter ID 2 is 1 pps
.
Switch access-list rate limiter ID 14 is 1 pps
Switch access-list rate limiter ID 15 is 1 pps
Switch access-list rate limiter ID 16 is 1 pps
                                   _____
_____
```

8. show access-list ace-status {*}コマンド

プロトコル毎に ACL エントリーのステータス情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

```
"show access-list ace-status ?"と入力すると、以下のサブコマンドが表示されます。
```

```
# show access-list ace-status ?
                  Output modifiers
   arp-inspection The ACEs that are configured by ARP Inspection module
                 The ACEs that did not get applied to the hardware
   conflicts
                   due to hardware limitations
                   The ACEs that are configured by DHCP module
   dhcp
   ip-source-guard The ACEs that are configured by IP Source Guard module
ipmc The ACEs that are configured by IPMC module
   Icop-protectThe ACEs that are configured by Loop Protect modulestaticThe ACEs that are configured by users manually
   switch
                   Switch
   <cr>
_____
例·
    _____
# show access-list ace-status
User
S : Static
IPSG: IP Source Guard
IPMC: IPMC
ARPI: ARP Inspection
DHCP: DHCP
LOOP: Loop Protect
```

User II	D	Frame	Actic	n Rate L.	CPU	Counte	er Conflict
	-						
DHCP 1		UDP	Deny	Disabled	Yes	0	No
DHCP 2		UDP	Deny	Disabled	Yes	0	No
Switch	1	access	-list	ace number	: 2		

9. show access-list interface {*}コマンド

インタフェースに設定された ACL の action 情報のみを表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show access-list interface ?"と入力すると、以下のサブコマンドが表示されます。

```
_____
# show access-list interface ?
                        Output modifiers
   All switches or All ports
   GigabitEthernet 1 Gigabit Ethernet Port
                        10 Gigabit Ethernet Port
   10GigabitEthernet
                        Access list entry
   ace
                 Rate limiter
  rate-limiter
   <cr>
                     _____
例:
# show access-list interface
GigabitEthernet 1/1 :
_____
GigabitEthernet 1/1 access-list action is permit
GigabitEthernet 1/1 access-list policy ID is 0
GigabitEthernet 1/1 access-list rate limiter ID is disabled
GigabitEthernet 1/1 access-list redirect is disabled
GigabitEthernet 1/1 access-list logging is disabled
GigabitEthernet 1/1 access-list shutdown is disabled
GigabitEthernet 1/1 access-list port-state is enabled
GigabitEthernet 1/1 access-list counter is 0
GigabitEthernet 1/2 :
_____
GigabitEthernet 1/2 access-list action is permit
GigabitEthernet 1/2 access-list policy ID is 0
GigabitEthernet 1/2 access-list rate limiter ID is disabled
GigabitEthernet 1/2 access-list redirect is disabled
GigabitEthernet 1/2 access-list logging is disabled
GigabitEthernet 1/2 access-list shutdown is disabled
GigabitEthernet 1/2 access-list port-state is enabled
GigabitEthernet 1/2 access-list counter is 0
GigabitEthernet 1/24 :
_____
GigabitEthernet 1/24 access-list action is permit
GigabitEthernet 1/24 access-list policy ID is 0
GigabitEthernet 1/24 access-list rate limiter ID is disabled
GigabitEthernet 1/24 access-list redirect is disabled
GigabitEthernet 1/24 access-list logging is disabled
GigabitEthernet 1/24 access-list shutdown is disabled
GigabitEthernet 1/24 access-list port-state is enabled
GigabitEthernet 1/24 access-list counter is 0
10GigabitEthernet 1/1 :
_____
10GigabitEthernet 1/1 access-list action is permit
```

```
10GigabitEthernet 1/1 access-list policy ID is 0
10GigabitEthernet 1/1 access-list rate limiter ID is disabled
10GigabitEthernet 1/1 access-list redirect is disabled
10GigabitEthernet 1/1 access-list logging is disabled
10GigabitEthernet 1/1 access-list shutdown is disabled
10GigabitEthernet 1/1 access-list port-state is enabled
10GigabitEthernet 1/1 access-list counter is 0
10GigabitEthernet 1/2 :
_____
10GigabitEthernet 1/2 access-list action is permit
10GigabitEthernet 1/2 access-list policy ID is 0
10GigabitEthernet 1/2 access-list rate limiter ID is disabled
10GigabitEthernet 1/2 access-list redirect is disabled
10GigabitEthernet 1/2 access-list logging is disabled
10GigabitEthernet 1/2 access-list shutdown is disabled
10GigabitEthernet 1/2 access-list port-state is enabled
10GigabitEthernet 1/2 access-list counter is 0
                     _____
```

10. show access-list rate-limiter {*}コマンド

ACL のレートリミット設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

```
<sup>"</sup>show access-list rate-limiter ?"と入力すると、以下のサブコマンドが表示されます。
```

```
_____
# show access-list rate-limiter ?
  <RateLimiterList : 1~16> Rate limiter ID
                  Output modifiers
  ace
                   Access list entry
  interface
                        Select an interface to configure
  <cr>
      _____
例:
   _____
# show access-list rate-limiter
Switch access-list rate limiter ID 1 is 1 pps
Switch access-list rate limiter ID 2 is 1 pps
•
Switch access-list rate limiter ID 14 is 1 pps
Switch access-list rate limiter ID 15 is 1 pps
Switch access-list rate limiter ID 16 is 1 pps
_____
                                -----
```

11. show aggregation { * }コマンド

```
ポートアグリゲーションの設定情報を表示します。
```

```
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

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

```
_____
# show aggregation ?
 | Output modifiers
     Traffic distribution mode
 mode
 <cr>
_____
例:
 _____
# show aggregation
Aggr ID Name Type Speed Configured Ports
                         Aggregated
Ports
_____ ____
_____
  GLAG2 Static Undefined GigabitEthernet 1/4-5 none
2
```

12. show aggregation mode コマンド

ポートアグリゲーションのモード情報を表示します。

```
# show aggregation mode
Aggregation Mode:
SMAC : Enabled
DMAC : Disabled
IP : Enabled
Port : Enabled
```

13. show clock コマンド

現行のシステムタイム情報を表示します。

```
<sup>″</sup>show clock ?と入力すると、以下のサブコマンドが表示されます。
```

```
# show clock ?
    detail Display detailed information
    <cr>
Ø:
# show clock
System Time : 1970-01-01T02:04:18+00:00
```

14. show clock detail コマンド

システムタイム情報の詳細を表示します。

```
_____
# show clock detail
System Time : 1970-01-01T02:04:22+00:00
Timezone : Timezone Offset : 0 ( 0 minutes)
Timezone Acronym :
Daylight Saving Time Mode : Disabled.
Daylight Saving Time Start Time Settings :
           0
     Week:
     Day:
               0
             0
0
     Month:
     Date:
               0
     Year:
     Hour:
               0
     Minute: 0
Daylight Saving Time End Time Settings :
     Week: 0
     Day:
               0
            0
     Month:
     Date:
               0
               0
     Year:
     Hour:
               0
    Minute: 0
Daylight Saving Time Offset : 1 (minutes)
_____
```

```
15. show ddmi {interface} { * }コマンド
```

DDMI のステータス情報を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

```
″show ddmi ?と入力すると、以下のサブコマンドが表示されます。
```

```
_____
# show ddmi
Serial Info Table
_____
10GigabitEthernet 1/1
_____
Serial Info Table
Status : N/A
Vendor
PartNo
SerialNo
Revision
DateCode
       •
Transceiver: N/A
Ddm Info Table
Туре
          AlarmMax AlarmMin WarnMax WarnMin Current
N/A
         0.00 0.00 0.00 0.00 0.00
         0.000.000.000.000.000.000.000.00
N/A
                                 0.00
N/A
                                 0.00
         0.00
N/A
                                 0.00
N/A
10GigabitEthernet 1/2
_____
                   _____
Serial Info Table
Status : N/A
Vendor
       :
PartNo
       :
SerialNo :
Revision
       :
DateCode
       :
Transceiver: N/A
Ddm Info Table
          AlarmMax AlarmMin WarnMax WarnMin Current
Type
N/A
          0.00 0.00 0.00 0.00 0.00
                           0.00
0.00
0.00
               0.00
                     0.00
                                  0.00
N/A
         0.00
              0.00
0.00
0.00
                    0.00
                                 0.00
N/A
         0.00
N/A
         0.00
                                  0.00
N/A
         0.00
                     0.00
                           0.00
                                  0.00
10GigabitEthernet 1/3
_____
Serial Info Table
Status : N/A
Vendor
       :
PartNo
       :
SerialNo
       :
Revision
       :
DateCode
       :
Transceiver: N/A
Ddm Info Table
          AlarmMax AlarmMin WarnMax WarnMin Current
Туре
N/A
         0.00 0.00 0.00 0.00 0.00
               0.00
                           0.00
                                 0.00
                     0.00
N/A
         0.00
                                 0.00
N/A
         0.00 0.00 0.00 0.00
         0.000.000.000.000.000.000.000.000.000.00
N/A
N/A
10GigabitEthernet 1/4
_____
Serial Info Table
```

```
: N/A
Status
Vendor
          :
PartNo
          :
SerialNo
          :
Revision
          :
DateCode
          :
Transceiver: N/A
Ddm Info Table
             AlarmMax AlarmMin WarnMax WarnMin Current
Туре
             0.000.000.000.000.000.000.000.000.000.000.000.00
N/A
                                            0.00
N/A
             0.00
                                              0.00
                                             0.00
N/A
                   0.00
                                    0.00
                           0.00
N/A
             0.00
                                              0.00
                     0.00
                                     0.00
N/A
             0.00
                                             0.00
```

16. show dot1x statistics all {*}コマンド

802.1xの EAP パケットおよび認証パケット情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show dot1x statistics all ?"と入力すると、以下のサブコマンドが表示されます。

<pre># show dot1x statistics all ?</pre>			
例:			
# show dot1x statistics all			
GigabitEthernet 1/1 EAPOL Statistic	cs:		
Rx Total:	0	Tx Total: ()
Rx Response/Id:	0	Tx Request/Id: ()
Rx Response:	0	Tx Request: ()
Rx Start:	0		
Rx Logoff:	0		
Rx Invalid Type:	0		
Rx Invalid Length:	0		
GigabitEthernet 1/1 Backend Server	Sta	tistics:	
Rx Access Challenges: 0	0	Tx Responses:	
Rx Other Requests:	0		
Rx Auth. Successes:	0		
Rx Auth. Failures:	0		
GigabitEthernet 1/2 EAPOL Statistic	cs:		
Rx Total:	0	Tx Total:)
Rx Response/Id:	0	Tx Request/Id: ()
Rx Response:	0	Tx Request: ()
Rx Start:	0		
Rx Logoff:	0		
Rx Invalid Type:	0		
Rx Invalid Length:	0		
GigabitEthernet 1/2 Backend Server	Stat	tistics:	
Rx Access Challenges:	0	Tx Responses: ()
Rx Other Requests:	0		
Rx Auth. Successes:	0		
Rx Auth. Failures:	0		

FXC5428

•

•				
GigabitEthernet 1/24 EAPOL Statist.	ics:			
Rx Total:	0	Тx	Total:	0
Rx Response/Id:	0	Тx	Request/Id:	0
Rx Response:	0	Тx	Request:	0
Rx Start:	0			
Rx Logoff:	0			
Rx Invalid Type:	0			
Rx Invalid Length:	0			
GigabitEthernet 1/24 Backend Serve	r St	ati	stics:	
Rx Access Challenges:	0	Τx	Responses:	0
Rx Other Requests:	0			
Rx Auth. Successes:	0			
Rx Auth. Failures:	0			
10GigabitEthernet 1/1 EAPOL Statis	tics	:		
Rx Total:	0	Тx	Total:	0
Rx Response/Id:	0	Тx	Request/Id:	0
Rx Response:	0	Тx	Request:	0
Rx Start:	0			
Rx Logoff:	0			
Rx Invalid Type:	0			
Rx Invalid Length:	0			
10GigabitEthernet 1/1 Backend Serve	er S	tat	istics:	
Rx Access Challenges:	0	Τx	Responses:	0
Rx Other Requests:	0			
Rx Auth. Successes:	0			
Rx Auth. Failures:	0			
10GigabitEthernet 1/2 EAPOL Statis	tics	:		
Rx Total:	0	Τx	Total:	0
Rx Response/Id:	0	Τx	Request/Id:	0
Rx Response:	0	Τx	Request:	0
Rx Start:	0			
Rx Logoff:	0			
Rx Invalid Type:	0			
Rx Invalid Length:	0			
10GigabitEthernet 1/2 Backend Serve	er S	tat	istics:	
Rx Access Challenges:	0	Τx	Responses:	0
Rx Other Requests:	0			
Rx Auth. Successes:	0			
Rx Auth. Failures:				

17. show dot1x statistics eapol {*}コマンド

.P パケットの情報を表示します。 以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。 show dot1x statistics eapol ?″と入力すると、以下のサブコマンドが表示されます。								
<pre># show dot1x stati</pre>	stics Outr Inte	eapol ? out modif erface	liers					
 例:								
# show dot1x stati	stics Rx	eapol Tx	Rx !			 Tx	Rx	Rx
Rx Interface Logoff Error	Total	Total	RespId	ReqId	Resp	Req	Sta	irt -
GigabitEthernet 1/	 1 0	0	0	0	0	0	0	0
GigabitEthernet 1/. 0	2 0	0	0	0	0	0	0	0
GigabitEthernet 1/.	24 0	0	0	0	0	0	0	0
10GigabitEthernet 0	1/1 0	0	0	0	0	0	0	0
10GigabitEthernet 0	1/2 0	0	0	0	0	0	0	0

18. show dot1x statistics radius { * }コマンド

認証パケットの情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

_____ # show dot1x statistics radius ? Output modifiers Interface interface <cr> _____ _____ # show dot1x statistics radius Rx Access Rx Other Rx Auth. Rx Auth. Tx MAC Challenges Requests Successes Failures Responses Interface Address _____ _____ _____ ____ GigabitEthernet 1/1 0 0 0 0 0 GigabitEthernet 1/2 0 0 0 0 0

.

-					
- 10GigabitEthernet 1/2	0	0	0	0	0
- 10GigabitEthernet 1/1	0	0	0	0	0
GigabitEthernet 1/24	0	0	0	0	0

19. show dot1x status { * }コマンド

現行の 802.1x ネットワークアクセスサーバのステータス情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show dot1x status ?"と入力すると、以下のサブコマンドが表示されます。

```
_____
# show dot1x status ?
 | Output modifiers
brief Show attained
 brief Show status in a brief format
interface Interface
 <cr>
    _____
例:
    _____
# show dot1x status interface *
GigabitEthernet 1/1 :
_____
Admin State Port State
                  Last Source Last ID
----- -----
_____
Force Authorized Globally Disabled
Current Radius QOS Current Radius VLAN Current Guest VLAN
_____ ____
GigabitEthernet 1/2 :
_____
       Port State Last Source
Admin State
                                Last ID
_____ ____
Force Authorized Globally Disabled
Current Radius QOS Current Radius VLAN Current Guest VLAN
 _____
GigabitEthernet 1/24 :
_____
Admin State Port State Last Source Last ID
_____
Force Authorized Globally Disabled - - Current Radius QOS Current Radius VLAN Current Guest VLAN
-----
                         _____
10GigabitEthernet 1/1 :
_____
Admin State Port State Last Source Last ID
_____ ____
_____
Force Authorized Globally Disabled
                         _
Current Radius QOS Current Radius VLAN Current Guest VLAN
_____ ____
```

_

20. show dot1x status brief{*}コマンド

現行の 802.1x ネットワークアクセスサーバのステータス情報を簡易的に表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

_

"show dot1x status brief?"と入力すると、以下のサブコマンドが表示されます。

<pre># show do inter: <cr></cr></pre>	otlx sta face	atus brief 3 Output Interf	? modifiers ace			
例: 						
# show do Inf Guest	Admin	atus brief Port State	Last Src	Last ID	QOS	VLAN
Gi 1/1 Gi 1/2	 Auth Auth	Disabled Disabled	-	- -		-
Gi 1/24 10G 1/1 10G 1/2	Auth Auth Auth	Disabled Disabled Disabled	- -	- - -		-

21. show history コマンド

入力したコマンドの履歴を表示します。

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

```
_____
                                  _____
# show history ?
  Output modifiers
  <cr>
     _____
 例:
_____
# show history
 show access-list ace-status
 show access-list ace-status arp-inspection
 show access-list ace-status arp-inspection conflicts dhcp
 show access-list interface GigabitEthernet 1/5
 show access-list interface
 show access-list rate-limiter
 show access-list rate-limiter ace statistics
 show access-list rate-limiter ace statistics interface GigabitEthernet 1/3
 show aggregation
 show aggregation mode
 show clock
 show clock detail
 show history
                _____
```

22. show interface [[GigabitEthernet | 10GigabitEthernet]〈Port list in x/y〉]capabilities コ マンド

ポートのトランシーバの情報を表示します。

23. show interface [[GigabitEthernet | 10GigabitEthernet] 〈Port list in x/y〉] name コマンド ポートに設定された名前を表示します。

```
# show interface GigabitEthernet 1/1 name
Interface Name
GigabitEthernet 1/1 Port 1
```

24. show interface [[GigabitEthernet | 10GigabitEthernet]〈Port list in x/y〉] statistics {*]コマンド

```
ポートの統計情報を表示します。
```

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

例として"show interface GigabitEthernet 1/1 switchport ?"と入力すると、以下のサブコマンドが表示されます。

```
# show interface 10GigabitEthernet 1/1 statistics ?
  Under Dutput modifiers
  bytes Show byte statistics.
discards Show discard statistics.
                Show ports which are down
  down
                Show error statistics.
Show filtered statistics.
   errors
   filtered
                Show packet statistics.
  packets
                Queue number
  priority
                  Show ports which are up
  up
   <cr>
      _____
 例:
_____
# show interface 10GigabitEthernet 1/1 statistics
10GigabitEthernet 1/1 Statistics:
Rx Packets:
                        0 Tx Packets:
                                                   0
Rx Octets:
                         0 Tx Octets:
                                                   0
Rx Unicast:
                        0 Tx Unicast:
                                                   0
                        0 Tx Multicast:
                                                   0
Rx Multicast:
                        0 Tx Broadcast:
Rx Broadcast:
                                                   0
                        0 Tx Pause:
                                                   0
Rx Pause:
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
                        0 Tx 1527- :
Rx 1527- :
                                                   0
                        0 Tx Priority 0:
Rx Priority 0:
                                                   0
                        0 Tx Priority 1:
Rx Priority 1:
                                                   0
                        0 Tx Priority 2:
Rx Priority 2:
                                                   0
Rx Priority 3:
                        0
                           Tx Priority 3:
                                                   0
Rx Priority 4:
                        0
                            Tx Priority 4:
                                                   0
Rx Priority 5:
                        0
                            Tx Priority 5:
                                                   0
Rx Priority 6:
                        0
                            Tx Priority 6:
                                                   0
Rx Priority 7:
                        0
                            Tx Priority 7:
                                                   0
                        0
                            Tx Drops:
Rx Drops:
                                                   0
                     0
Rx CRC/Alignment:
                            Tx Late/Exc. Coll.:
                                                   0
Rx Undersize:
                        0
Rx Oversize:
                         0
```

Rx	Fragments:	0		
		-		
Rx	Jabbers:	0		
Rx	Filtered.	0		
1 (21	11100104.	•		

- 25. show interface [[GigabitEthernet | 10GigabitEthernet]〈Port list in x/y〉] status コマン ド
 - ポートのステータス情報を表示します。

26. show interface [[GigabitEthernet | 10GigabitEthernet] 〈Port list in x/y〉] switchport {*}コマンド

ポートの vlan 設定情報およびステータスを表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show interface GigabitEthernet x/y switchport ?"と入力すると、以下のサブコマンドが表示されます。 (以下は、"show interface GigabitEthernet 1/1 switchport ?"と入力した場合の表示例です。)

```
# show interface GigabitEthernet 1/1 switchport
Name: GigabitEthernet 1/1
Administrative mode: access
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Native VLAN tagging: disabled
Allowed VLANs: 1-4095
Hybrid port configuration
_____
Port Type: C-Port
Acceptable Frame Type: All
Ingress filter: Disabled
Egress tagging: All except-native
Hybrid Native Mode VLAN: 1
Hybrid VLANs Enabled: 1-4095
```

27. show interface [[GigabitEthernet | 10GigabitEthernet] 〈Port list in x/y〉] veriphy コマン ド

```
ケーブル診断を実行します。
```

```
# show interface GigabitEthernet 1/1 veriphy
Starting VeriPHY - Please wait
Interface Pair A Length Pair B, Length Pair C Length Pair D
Length
_______
GigabitEthernet 1/1 OK 0 OK 0 OK 0 OK
```

28. show interface vlan (vlan-list)コマンド

Vlan の設定情報を表示します。

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

29. show ip arp コマンド

Arp テーブル情報を表示します。

30. show ip arp inspection {*}コマンド

```
Arp インスペクションのステータス情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

```
"show ip arp inspection ?"と入力すると、以下のサブコマンドが表示されます。
```

```
# show ip arp inspection ?
entry arp inspection entries
interface arp inspection entry interface config
vlan VLAN configuration
<cr>
```

```
_____
```

```
# show ip arp inspection
ARP Inspection Mode : disabled
Port Port Mode Check VLAN Log Type
---- GigabitEthernet 1/1 disabled disabled NONE
GigabitEthernet 1/2 disabled disabled NONE
.
.
GigabitEthernet 1/24 disabled disabled NONE
10GigabitEthernet 1/1 disabled disabled NONE
10GigabitEthernet 1/2 disabled disabled NONE
```

31. show ip arp inspection entry { * }コマンド

Arp インスペクションのエントリー情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

```
"show ip arp inspection entry ?"と入力すると、以下のサブコマンドが表示されます。
  _____
 # show ip arp inspection entry ?
   dhcp-snooping learn from dhcp snooping
interface arp inspection entry interface config
   interface
               setting from static entries
   static
   <cr>
           _____
  例:
         _____
 # show ip arp inspection entry
 Type Port
           VLAN MAC Address IP Address
                      ----
 ____
 Static GigabitEthernet 1/1 1 00-00-00-00-01 192.168.1.1
```

32. show ip arp inspection vlan 〈vlan-list〉コマンド

Vlan ごとに Arp インスペクションのステータス情報を表示します。

```
# show ip arp inspection vlan 1
VLAN VLAN mode VLAN Log Type
1 disabled NONE
```

33. show ip dhcp detailed statistics {*}コマンド

```
DHCP クライアントの統計情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
(1) "show ip dhcp detailed statistics?"と入力すると、以下のサブコマンドが表示されます。
  _____
  # show ip dhcp detailed statistics ?
    client DHCP client
combined Show all DHCP related statistics
    normal-forward DHCP normal L2 or L3 forward
    relay DHCP relay
snooping DHCP snooping
  _____
  例:
  _____
  # show ip dhcp detailed statistics client
   GigabitEthernet 1/1 Statistics:
  _____
  Rx Discover:
                        0 Tx Discover:
                                                       0
  Rx Offer:
                              0 Tx Offer:
                                                       0
                               0 Tx Request:
  Rx Request:
                                                       0
                                 Tx Decline:
  Rx Decline:
                               0
                                                       0
                                 Tx ACK:
  Rx ACK:
                               0
                                                       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
                                 Tx Lease Unassigned:
                              0
  Rx Lease Unassigned:
                                                       0
                             0
  Rx Lease Unknown:
                                 Tx Lease Unknown:
                                                       Ο
                             0
  Rx Lease Active:
                                 Tx Lease Active:
                                                       Ο
  Rx Lease Active:
                              0
                                 Tx Lease Active:
                                                       Ο
  Rx Discarded checksum error:
                              0
  GigabitEthernet 1/2 Statistics:
  -----
 Rx Discover:
                               0 Tx Discover:
                                                       0
 Rx Offer:
                               0 Tx Offer:
                                                       0
                              0 Tx Request:
                                                       0
 Rx Request:
                              0 Tx Decline:
 Rx Decline:
                                                       0
                               0 Tx ACK:
 Rx ACK:
                                                       0
                              0 Tx NAK:
 Rx NAK:
                                                       0
                              0 Tx Release:
 Rx Release:
                                                       0
                              0 Tx Inform:
 Rx Inform:
                                                       0
 Rx Lease Query:
                             0 Tx Lease Query:
                                                       0
                             0 Tx Lease Unassigned:
 Rx Lease Unassigned:
                                                      0
 Rx Lease Unknown:
                             0 Tx Lease Unknown:
                                                      0
 Rx Lease Active:
                             0 Tx Lease Active:
                                                      0
  Rx Lease Active:
                              0 Tx Lease Active:
                                                      0
  Rx Discarded checksum error:
                             0
  .
  GigabitEthernet 1/24 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
                                                     85
```

Rx	Lease Query:	0	Τx	Lease Query:	0
Rx	Lease Unassigned:	0	Тx	Lease Unassigned:	0
Rx	Lease Unknown:	0	Тx	Lease Unknown:	0
Rx	Lease Active:	0	Тx	Lease Active:	0
Rx	Lease Active:	0	Тx	Lease Active:	0
Rx	Discarded checksum error:	0			
Rx	Discover:	0	Τx	Discover:	0
Rx	Offer:	0	Τx	Offer:	0
Rx	Request:	0	Τx	Request:	0
Rx	Decline:	0	Τx	Decline:	0
Rx	ACK:	0	Тx	ACK:	0
Rx	NAK:	0	Тx	NAK:	0
Rx	Release:	0	Тx	Release:	0
Rx	Inform:	0	Тx	Inform:	0
Rx	Lease Query:	0	Τx	Lease Query:	0
Rx	Lease Unassigned:	0	Тx	Lease Unassigned:	0
Rx	Lease Unknown:	0	Тx	Lease Unknown:	0
Rx	Lease Active:	0	Тx	Lease Active:	0
Rx	Lease Active:	0	Тx	Lease Active:	0
Rx	Discarded checksum error:	0			
100	GigabitEthernet 1/2 Statistics:				
Rx	Discover:	0	Τx	Discover:	0
Rx	Offer:	0	Τx	Offer:	0
Rx	Request:	0	Τx	Request:	0
Rx	Decline:	0	Τx	Decline:	0
Rx	ACK:	0	Τx	ACK:	0
Rx	NAK:	0	Τx	NAK:	0
Rx	Release:	0	Τx	Release:	0
Rx	Inform:	0	Τx	Inform:	0
Rx	Lease Query:	0	Τx	Lease Query:	0
Rx	Lease Unassigned:	0	Τx	Lease Unassigned:	0
Rx	Lease Unknown:	0	Τx	Lease Unknown:	0
Rx	Lease Active:	0	Τx	Lease Active:	0
Rx	Lease Active:	0	Τx	Lease Active:	0
Rx	Discarded checksum error:	0			

各統計情報はさらに絞込みを行えます。

(2) "show ip dhcp detailed statistics client ?"と入力すると、以下のサブコマンドが表示されます。

# :	<pre># show ip dhcp detailed statistics client ?</pre>					
侈	———————————————————— 例					
# s 100	show ip dhcp detail GigabitEthernet 3/	ed statisti 1 Statistic	.cs s:	client interface	10GigabitEthernet 3/1	
Rx	Discover:	0	Тх	Discover:	0	
Rx	Offer:	0	Тx	Offer:	0	
Rx	Request:	0	Тx	Request:	0	
Rx	Decline:	0	Тx	Decline:	0	
Rx	ACK:	0	Тx	ACK:	0	
Rx	NAK:	0	Тx	NAK:	0	
Rx	Release:	0	Тx	Release:	0	
Rx	Inform:	0	Тx	Inform:	0	
Rx	Lease Query:	0	Тx	Lease Query:	0	
Rx	Lease Unassigned:	0	Тx	Lease Unassigned:	0	

0

0

0

0

34. show ip dhcp relay { * }コマンド

リレーエージェントの設定情報を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

35. show ip dhcp relay statistics コマンド

DHCP メッセージの統計情報を表示します。

```
_____
# show ip dhcp relay statistics
Switch DHCP relay mode is disabled
Switch DHCP relay server address is 0.0.0.0
Switch DHCP relay information option is disabled
Switch DHCP relay information policy is keep
Server Statistics:
_____
Transmit to Server: 0Transmit Error: 0Receive from Server: 0Receive Missing Agent Option: 0Receive Missing Circuit ID: 0Receive Missing Remote ID: 0Receive Bad Circuit ID: 0Receive Bad Remote ID: 0Chient Chatistic: 0Receive Bad Remote ID: 0
Client Statistics:
_____
Transmit to Client: 0Transmit ErrorReceive from Client: 0Receive Agent OptionReplace Agent Option: 0Keep Agent OptionDrop Agent Option: 0. 0
                                                                             : 0
                                                                             : 0
                                                                               : 0
_____
```

36. show ip dhcp snooping { * }コマンド

```
DHCP スヌーピングのポート設定およびパラメータ設定を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

```
"show ip dhcp snooping ?"と入力すると、以下のサブコマンドが表示されます。
 _____
  # show ip dhcp snooping ?
        Output modifiers
   interface Select an interface to configure
   table
              show ip dhcp snooping table
   <cr>
 _____
  例·
          _____
 # show ip dhcp snooping
 Agent URL is
 Timeout interval is 300
 Write delay interval is 300
 DHCP snooping is configured on following
 GigabitEthernet 1/1 trusted
 GigabitEthernet 1/2 trusted
 GigabitEthernet 1/24 trusted
 10GigabitEthernet 1/1 trusted
 10GigabitEthernet 1/2 trusted
 _____
```

37. show ip dhcp snooping table コマンド

DHCP バインディングテーブルの情報を表示します。

```
# show ip dhcp snooping table
Entry ID : 1
MAC Address : 00-12-2e-bd-fb-9a
VLAN ID : 1
Expired Lease Time : 2d23h59m48s
Source Port : GigabitEthernet 1/22
IP Address : 192.168.11.59
IP Subnet Mask : 255.255.255.0
DHCP Server Address : 192.168.11.1
Total Entries Number : 1
```

38. show ip http server secure status コマンド

現行の HTTP セキュリティモードのステータスを表示します。

show ip http server secure status Switch secure HTTP web server is disabled Switch secure HTTP web redirection is disabled Switch secure HTTP certificate is presented

39. show ip igmp snooping {*}コマンド

```
IGMP スヌーピングの設定情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

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

<pre># show ip igmp snoo</pre>	 ping ?
 detail group-database mrouter vlan <cr></cr>	Output modifiers Detail running information/statistics of IGMP snooping Multicast group database from IGMP Multicast router port status in IGMP Search by VLAN
例: 	
<pre># show ip igmp snoo IGMP Snooping is di</pre>	ping sabled to stop snooping IGMP control plane.

40. show ip interface brief コマンド

VLAN インタフェースごとの IP 情報を表示します。

show ip interface brief Vlan Address Method Status 1 192.168.1.1/24 Manual UP

41. show ip name-server コマンド

DNS サーバ情報を表示します。

```
# show ip name-server
Current DNS server is not set.
```

42. show ip route コマンド

学習したルート情報を表示します。

show ip route
127.0.0.1/32 via 127.0.0.1 <UP HOST>
192.168.1.0/24 via VLAN1 <UP HW_RT>
224.0.0.0/4 via 127.0.0.1 <UP>

43. show ip source binding {*}コマンド

```
IP ソースガードのバインディング情報を表示します。
```

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

```
"show ip source binding?"と入力すると、以下のサブコマンドが表示されます。
```

44. show ip ssh コマンド

現行の SSH 設定情報を表示します。

show ip ssh Switch SSH is enabled

45. show ip statistics { * }コマンド

```
IPv4 パケットの統計情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

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

```
# show ip statistics ?
  | Output modifiers
  icmp
           IPv4 ICMP traffic
  icmp-msg IPv4 ICMP traffic for designated message type
  interface Select an interface to configure
  system IPv4 system traffic
  <cr>
 例:
   _____
# show ip statistics
IPv4 statistics:
 Rcvd: 3335 total in 502767 bytes
      2698 local destination, 0 forwarding
      0 header error, 2 address error, 0 unknown protocol
      0 no route, 0 truncated, 637 discarded
 Sent: 1383 total in 1007320 bytes
      1383 generated, 0 forwarded
      14 no route, 0 discarded
 Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
      0 fragment (0 fragmented, 0 couldn't fragment)
      0 fragment created
 Mcast: 2110 received in 276601 bytes
      0 sent in 0 byte
```

```
Bcast: 1464 received, 0 sent
IP interface statistics:
IPv4 Statistics on Interface VLAN: 1
Rcvd: 3335 total in 502767 bytes
       2698 local destination, 0 forwarding
       0 header error, 2 address error, 0 unknown protocol
      0 no route, 0 truncated, 637 discarded
Sent: 1383 total in 1007320 bytes
       1383 generated, 0 forwarded
       0 discarded
Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
       0 fragment (0 fragmented, 0 couldn't fragment)
       0 fragment created
Mcast: 2110 received in 276601 bytes
      0 sent in 0 byte
Bcast: 1464 received, 0 sent
IPv4 Statistics on Interface VLAN: 10
Rcvd: 0 total in 0 byte
      0 local destination, 0 forwarding
      0 header error, 0 address error, 0 unknown protocol
      0 no route, 0 truncated, 0 discarded
Sent: 0 total in 0 byte
      0 generated, 0 forwarded
      0 discarded
Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
      0 fragment (0 fragmented, 0 couldn't fragment)
      0 fragment created
Mcast: 0 received in 0 byte
      0 sent in 0 byte
Bcast: 0 received, 0 sent
IPv4 ICMP statistics:
Rcvd: 1 Message, 0 Error
Sent: 14 Messages, 13 Errors
ICMP message statistics:
IPv4 ICMP Message: Echo Reply
Rcvd: 0 Packet
Sent: 1 Packet
IPv4 ICMP Message: Destination Unreachable
Rcvd: 0 Packet
Sent: 13 Packets
IPv4 ICMP Message: Echo
Rcvd: 1 Packet
Sent: 0 Packet
```

46. show ip verify source { * }コマンド

```
IP ソースガードの設定情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
"show ip verify source ?"と入力すると、以下のサブコマンドが表示されます。
 _____
 # show ip verify source ?
  interface ip verify source interface config
   <cr>
 _____
  例:
          _____
                   _____
 # show ip verify source
 IP Source Guard Mode : disabled
               Port Mode
                      Dynamic Entry Limit
 Port
               _____
 ____
                       _____
```

GigabitEthernet 1/1 GigabitEthernet 1/2 •	disabled disabled	unlimited unlimited
GigabitEthernet 1/24 10GigabitEthernet 1/1 10GigabitEthernet 1/2	disabled disabled disabled	unlimited unlimited unlimited

47. show ipmc profile { * }コマンド

IP マルチキャストの IPMC プロファイル情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

48. show ipmc range { * }コマンド

設定した IP マルチキャストアドレスの範囲を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

49. show ipv6 interface { * }コマンド

インタフェースの IPv6 ステータス情報および統計情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

["]show ipv6 interface ?"と入力すると、以下のサブコマンドが表示されます。

```
_____
_____
# show ipv6 interface ?
 | Output modifiers
  vlan
         VLAN of IPv6 interface
  <cr>
            _____
  例:
_____
# show ipv6 interface
IPv6 Vlan1 interface is down.
 Internet address is fe80::217:2eff:fe1b:b7ff
 Static address is not set
 IP stack index (IFID) is 2
 Routing is disabled on this interface
 MTU is 1500 bytes
 IPv6 Statistics on Interface VLAN: 1
 Rcvd: 0 total in 0 byte
      0 local destination, 0 forwarding
      0 header error, 0 address error, 0 unknown protocol
      0 no route, 0 truncated, 0 discarded
 Sent: 4 total in 288 bytes
      4 generated, 0 forwarded
      0 discarded
 Frags:0 reassemble (0 reassembled, 0 couldn't reassemble)
      0 fragment (0 fragmented, 0 couldn't fragment)
      0 fragment created
 Mcast:0 received in 0 byte
     4 sent in 288 bytes
 Bcast:0 received, 0 sent
```

50. show ipv6 mld snooping {*}コマンド

IPv6のマルチキャスト情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show ipv6 mld snooping ?"と入力すると、以下のサブコマンドが表示されます。

# show ipv6 mld snoc	pping ?
 detail group-database mrouter vlan <cr></cr>	Output modifiers Detail running information/statistics of MLD snooping Multicast group database from MLD Multicast router port status in MLD Search by VLAN
例:	
# show ipv6 mld snoc MLD Snooping is disa	pping bled to stop snooping MLD control plane.

51. show ipv6 neighbor{*]コマンド

```
IPv6のネイバー情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

```
"show ipv6 neighbor ?"と入力すると、以下のサブコマンドが表示されます。
```

52. show ipv6 route {*}コマンド

IPv6 で学習したルート情報を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show ipv6 route ?"と入力すると、以下のサブコマンドが表示されます。

53. show ipv6 statistics {*} コマンド

IPv6 パケットの統計情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

["]show ipv6 statistics ?"と入力すると、以下のサブコマンドが表示されます。

```
# show ipv6 statistics ?
          Output modifiers
  IPv6 ICMP traffic
  icmp
              IPv6 ICMP traffic for designated message type
Select an interface to configure
  icmp-msg
  interface
                IPv6 system traffic
  system
  <cr>
          _____
 例:
     _____
# show ipv6 statistics
IPv6 statistics:
 Rcvd:
          32 total in 1840 bytes
          32 local destination, 0 forwarding
          O header error, O address error, O unknown protocol
          0 no route, 0 truncated, 0 discarded
          25 total in 1568 bytes
 Sent:
          29 generated, 0 forwarded
```

```
0 no route, 0 discarded
           0 reassemble (0 reassembled, 0 couldn't reassemble)
Frags:
           0 fragment (0 fragmented, 0 couldn't fragment)
           0 fragment created
Mcast:
          32 received in 1840 bytes
           25 sent in 1568 bytes
        0 received, 0 sent
Bcast:
IP interface statistics:
IPv6 Statistics on Interface VLAN: 1
Rcvd: 32 total in 1840 bytes
      32 local destination, 0 forwarding
       0 header error, 0 address error, 0 unknown protocol
       0 no route, 0 truncated, 0 discarded
Sent: 25 total in 1568 bytes
      25 generated, 0 forwarded
       0 discarded
Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
       0 fragment (0 fragmented, 0 couldn't fragment)
       0 fragment created
Mcast: 32 received in 1840 bytes
      25 sent in 1568 bytes
Bcast: 0 received, 0 sent
IPv6 ICMP statistics:
Rcvd: 32 Messages, 0 Error
Sent: 27 Messages, 0 Error
ICMP message statistics:
IPv6 ICMP Message: Multicast Listener Report
Rcvd: 0 Packet
Sent: 10 Packets
IPv6 ICMP Message: Router Solicitation (NDP)
Rcvd: 26 Packets
Sent: 12 Packets
IPv6 ICMP Message: Neighbor Solicitation (NDP)
Rcvd: 0 Packet
Sent: 5 Packets
IPv6 ICMP Message: Neighbor Advertisement (NDP)
Rcvd: 3 Packets
Sent: 0 Packet
_____
```

54. show lacp internal コマンド

55. show lacp neighbor コマンド

本機とLACP で接続しているネイバー情報を表示します。

_____ # show lacp neighbour Aggr ID Partner System ID Partner Prio Partner Key Last Changed _____ _____ _____ 00:17:2e:21:84:82 32768 3 00:00:58 1 State Key Aggr ID Partner Port Partner Port Prio Port _____ _____ Partner Key Last Changed _____ ____ 00:17:2e:21:84:82 32768 3 1 00:00:58 Port State Key Aggr ID Partner Port Partner Port Prio _____ ____ _____ _____ Enabled 3 1 Enabled 3 1 3 Gi 1/3 32768 Gi 1/4 4 32768 _____ _____

56. show lacp statistics コマンド

LACP 設定したポートのパケット統計情報を表示します。

show lacp statistics Rx Frames Tx Frames Rx Unknown Rx Illegal Port ----- ------ ------ ------0 0 0 5 0 0 0 Gi 1/22 0 0 Gi 1/23

57. show lacp system-id コマンド

現行の LACP システム ID 情報を表示します。

_____ # show lacp system-id System Priority: 32768 _____

58. show line { * }コマンド

管理アクセスモードの情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show line ?"と入力すると、以下のサブコマンドが表示されます。

```
_____
# show line ?
 | Output modifiers
 alive Display information about alive lines
 <cr>
_____
例:
_____
# show line
Line is con 0.
 * You are at this line now.
```

```
Alive from Console.
Default privileged level is 2.
Command line editing is enabled
Display EXEC banner is enabled.
Display Day banner is enabled.
Terminal width is 80.
         length is 24.
         history size is 32.
         exec-timeout is 10 min 0 second.
Current session privilege is 15.
Elapsed time is 0 day 0 hour 25 min 2 sec.
Idle time is 0 day 0 hour 0 min 0 sec.
Line is vtv 0.
Not alive.
Default privileged level is 2.
Command line editing is enabled
Display EXEC banner is enabled.
Display Day banner is enabled.
Terminal width is 80.
       length is 24.
       history size is 32.
       exec-timeout is 10 min 0 second.
Current session privilege is 0.
Elapsed time is 0 day 0 hour 0 min 0 sec.
Idle time is 0 day 0 hour 0 min 0 sec.
Line is vty 1.
Not alive.
Default privileged level is 2.
Command line editing is enabled
Display EXEC banner is enabled.
Display Day banner is enabled.
Terminal width is 80.
        length is 24.
        history size is 32.
         exec-timeout is 10 min 0 second.
Current session privilege is 0.
Elapsed time is 0 day 0 hour 0 min 0 sec.
Idle time is 0 day 0 hour 0 min 0 sec.
                                        _____
```

59. show lldp neighbors { * }コマンド

LLDP で取得したネイバー情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

60. show lldp statistics { * }コマンド

```
LLDP で取得したネイバーのエントリー情報およびパケット統計情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

"show lldp lldp statistics ?"と入力すると、以下のサブコマンドが表示されます。 _____ # show lldp statistics ? | Output modifiers interface Interface to display. <cr> _____ 例: _____ _____ # show lldp statistics LLDP global counters Neighbor entries was last changed at 1970-01-01T00:00:00+00:00 (12490 secs. 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 Frames Frames Errors Discards Errors Interface Unknown Organiz. Aged _____ _____ _____ ____ _____ _____ ____ GigabitEthernet 1/1 0 0 0 0 0 0 0 0 GigabitEthernet 1/2 0 0 0 0 0 0 0 0 . . GigabitEthernet 1/24 0 0 0 0 0 0 0 0 10GigabitEthernet 1/1 0 0 0 0 0 0 0 0 10GigabitEthernet 1/2 0 0 0 0 0 0 0 0 _____

61. show logging {*}コマンド

現在の system log および system log 設定を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

# shc <: e: in st wa <c< th=""><th>ow logging_ logging_ nror nfo witch arning cr></th><th>ng ? id: 1-4294967295</th><th>> Logging I Outpu Error Infor Switc Warni</th><th>D t modi mation h ng</th><th>fiers</th><th></th></c<>	ow logging_ logging_ nror nfo witch arning cr>	ng ? id: 1-4294967295	> Logging I Outpu Error Infor Switc Warni	D t modi mation h ng	fiers	
例:						
<pre># sho Switc Switc Switc Numbe Info Warn: Erron All ID </pre>	ow loggi ch loggi ch loggi ch loggi er of en : 4 ing: 0 r : 0 : 4 Level	ng ng host mode is ng host address ng level is inf tries on Switch Time	enabled is null ormation 1: Me	ssage		
1 2 3 4	Info Info Info Info	1970-01-01T04:4 1970-01-01T04:4 1970-01-01T04:4 1970-01-01T04:4	17:26+00:00 17:29+00:00 17:30+00:00 17:34+00:00	Link Link Link Link	down on switch 1, port up on switch 1, port 3 down on switch 1, port up on switch 1, port 4	3 4

```
62. show loop-protect {*}コマンド
  ループバック検知の設定およびステータスを表示します。
  *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
  "show loop-protect ?"と入力すると、以下のサブコマンドが表示されます。
    ------
                                         _____
    # show loop-protect ?
      interface Interface status and configuration
      <cr>
    _____
     例:
                      _____
    # show loop-protect
    Loop Protection Configuration
    _____
    Loop Protection : Disable
    Transmission Time : 5 sec
    Shutdown Time : 180 sec
    GigabitEthernet 1/1
    _____
       Loop protect mode is enabled.
      Action is shutdown.
      Transmit mode is enabled.
      No loop.
       The number of loops is 0.
       Status is down.
    GigabitEthernet 1/2
    _____
      Loop protect mode is enabled.
      Action is shutdown.
      Transmit mode is enabled.
      No loop.
      The number of loops is 0.
       Status is down.
    GigabitEthernet 1/24
      Loop protect mode is enabled.
      Action is shutdown.
      Transmit mode is enabled.
      No loop.
      The number of loops is 0.
       Status is down.
    10GigabitEthernet 1/1
    -----
      Loop protect mode is enabled.
      Action is shutdown.
      Transmit mode is enabled.
      No loop.
       The number of loops is 0.
       Status is down.
    10GigabitEthernet 1/2
    _____
      Loop protect mode is enabled.
      Action is shutdown.
      Transmit mode is enabled.
      No loop.
      The number of loops is 0.
       Status is down.
                        _____
```
63. show mac address-table { * }コマンド

MAC アドレステーブルおよびその他の機能の情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

["]show mac address-table ?"と入力すると、以下のサブコマンドが表示されます。

```
# show mac address-table ?
        Output modifiers
  address MAC address lookup
aging-time Aging time
             User added static mac addresses
  conf
             Total number of mac addresses
  count
             Select an interface to configure
  interface
  learning
             Learn/disable/secure state
  static
             All static mac addresses
  vlan
              Addresses in this VLAN
  <cr>
     _____
```

例:

```
# show mac address-table
Type VID MAC Address Ports
Static 1 ff:ff:ff:ff:ff GigabitEthernet 1/1-24 10GigabitEthernet
1/1-4 CPU
```

64. show mac address-table aging-time コマンド

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
```

65. show mac address-table count { * }コマンド

MAC アドレステーブルの学習数を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show mac address-table count ?"と入力すると、以下のサブコマンドが表示されます。

```
_____
# show mac address-table count ?
                 Output modifiers
  interface Select an interface to configure
  <cr>
 例:
_____
# show mac address-table count
Port Dynamic addresses
1
  0
2
  0
3
  2
  0
24
  0
25
```

```
26 0
27 0
28 0
Total learned dynamic addresses for the switch: 2
Total static addresses in table: 4
```

66. show mac address-table learning { * }コマンド

```
MAC アドレステーブルの学習モードを表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

"show mac address-table learning?"と入力すると、以下のサブコマンドが表示されます。

```
_____
# show mac address-table learning ?
             Output modifiers
  interface
           Select an interface to configure
  <cr>
 例:
      _____
# show mac address-table learning
Port
           Learning
GigabitEthernet 3/1 Auto
GigabitEthernet 3/2 Auto
GigabitEthernet 3/3 Auto
10GigabitEthernet 3/1 Auto
10GigabitEthernet 3/2 Auto
                  _____
```

67. show mac-auth-username コマンド

MAC アドレス認証ユーザ情報を表示します。

```
# show mac-auth-username
mac auth username format:with-hyphen lower-case
```

68. show mvr {*}コマンド

MVR 設定およびステータスを表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

[″]show mvr ?[″]と入力すると、以下のサブコマンドが表示されます。

# snow mvr ? detail group-database	Output modifiers Detail information/statistics of MVR group database Multicast group database from MVR
vlan <cr></cr>	Search by VLAN
例:	
# show mvr	

MVR is currently disabled, please enable MVR to start group registration.

69. show ntp status コマンド

本機の NTP 機能の設定情報を表示します。

70. show port-security port {*}コマンド

本機の各ポートのポートセキュリティの情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
# show port-security port ?
 Output modifiers
 interface
 <cr>
例:
  _____
            _____
# show port-security port
GigabitEthernet 2/1
_____
MAC Address VID State Added
                             Age/Hold Time
_____ ____
_____
<none>
GigabitEthernet 2/2
_____
MAC Address VID State Added
                             Age/Hold Time
_____ ____
_____
<none>
•
•
GigabitEthernet 2/24
_____
        VID State Added
MAC Address
                             Age/Hold Time
_____ ____
_____
<none>
10GigabitEthernet 2/1
_____
MAC Address
        VID State Added
                              Age/Hold Time
_____ ____
_____
<none>
10GigabitEthernet 2/2
```

MAC Address	VID	State	Added	Age/Hold	Time
<none></none>					

71. show port-security switch {*}コマンド

スイッチ全体のポートセキュリティ情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show port-security switch ?"と入力すると、以下のサブコマンドが表示されます。

<pre># show port-security</pre>	switch ? modifiers	
<pre># show port-security Users: L = Limit Control 8 = 802.1X D = DHCP Snooping V = Voice VLAN Interface</pre>	switch Users State	MAC Cnt
GigabitEthernet 2/1 GigabitEthernet 2/2 GigabitEthernet 2/3 • •	No users No users No users	0 0 0 0
GigabitEthernet 2/22 GigabitEthernet 2/23 GigabitEthernet 2/24	No users No users No users	0 0 0

72. show privilege コマンド

本機の各機能の特権レベルについての設定情報を表示します。

show privilege The order is as the input sequence and | the last one has the highest priority. | privilege configure level 15 interface privilege configure level 15 default privilege configure level 15 vlan privilege interface level 10 switchport privilege interface level 10 speed

73. show pvlan { * }コマンド

本機のプライベート VLAN の設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。 "show pvlan ?"と入力すると、以下のサブコマンドが表示されます。 _____ _____ # show pvlan ? interface List of port type and port ID, ex, Fast 1/1 Gigabit 2/3-5 Gigabit 3/2-4 Tengigabit 4/6 <cr> _____ _____ # show pvlan interface * Port Isolation _____ GigabitEthernet 1/1 Disabled GigabitEthernet 1/2 Disabled GigabitEthernet 1/3 Disabled GigabitEthernet 1/24 Disabled 10GigabitEthernet 1/1 Disabled IOGIGADICECTIETTIEIIIDisabled10GigaDitEthernet1/2Disabled _____

74. show qos {*}コマンド

本機の QoS 設定を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

″show qos ?″と入力すると、以下のサブコマンドが表示されます。

```
_____
                                        _____
# show qos ?
           Output modifiers
  interface Interface
  InterfaceInterfacemapsGlobal QoS Maps/TablesqceQoS Control EntrywredWeighted Random Early Discard
  <cr>
_____
 例:
        _____
# show qos
interface GigabitEthernet 1/1
qos cos O
qos dpl 0
qos trust dscp disabled
qos policer mode: disabled, rate: 500 kbps
qos shaper mode: disabled, rate: 500 kbps
qos queue-shaper queue 0 mode: disabled, rate: 500 kbps, excess: disabled
gos wrr mode: disabled, weight: q0:17 q1:17 q2:17 q3:17 q4:17 q5:17
qos tag-remark classified
qos map cos-tag cos 0 dpl 0 pcp 1 dei 0
```

•

```
.
qos dscp-translate disabled
qos dscp-classify disabled
qos dscp-remark disabled
qos storm unicast mode: disabled, rate: 500 kbps
qos storm broadcast mode: disabled, rate: 500 kbps
qos storm unknown mode: disabled, rate: 500 kbps
.
qos wred:
_____

        Queue
        Mode
        Min
        Th
        Mdp
        1
        Mdp
        2
        Mdp
        3

        -----
        -----
        -----
        -----
        -----
        -----
        -----

0 disabled 0 1 5 10
.
qos map dscp-cos:
_____
DSCP Trust Cos Dpl
----- ---- ---
0 (BE) disabled 0 0
   disabled 0 0
1
.
qos map dscp-ingress-translation:
_____
DSCP Translated DSCP
_____
0 (BE) 0 (BE)
.
•
qos map dscp-classify:
_____
DSCP Classify
-----
0 (BE) disabled
•
.
qos map cos-dscp:
_____
Cos DSCP
--- -----
0 0 (BE)
•
qos map dscp-egress-translation:
_____
DSCP Remap
_____
0 (BE) 0 (BE)
•
_____
```

75. show qos maps {*}コマンド

本機の QoS マップの情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
# show qos maps ?
 Output modifiers
  cos-dscp
                Map for cos to dscp
  dscp-classify
                Map for dscp classify enable
                Map for dscp to cos
  dscp-cos
  dscp-egress-translation Map for dscp egress translation
  dscp-ingress-translation Map for dscp ingress translation
  <cr>
_____
          _____
 例:
_____
# show qos maps
qos map dscp-cos:
_____
DSCP Trust Cos Dpl
0 (BE) disabled 0 0
  disabled 0 0
1
qos map dscp-ingress-translation:
_____
DSCP Translated DSCP
_____
0 (BE) 0 (BE)
.
•
qos map dscp-classify:
_____
DSCP Classify
_____
0 (BE) disabled
qos map cos-dscp:
_____
Cos DSCP
--- ------
0
 0 (BE)
•
qos map dscp-egress-translation:
_____
DSCP Remap
_____ ___
0 (BE) 0 (BE)
•
_____
```

76. show qos qce {*}コマンド

```
本機の QoS の QCE 情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
"show qos qce ?"と入力すると、以下のサブコマンドが表示されます。
 _____
 # show qos qce ?
   <Id : 1-4096> QCE ID
           Output modifiers
   <cr>
 _____
 例:
 _____
 # show qos qce 1
 static qce 1:
 _____
 port: 1-28
  key parameters:
  tag:
  type:any
  vid: any
  pcp: any
  dei: any
  smac:any
  dmac:any
  frametype: etype any
  action parameters:
  cos: 6
 dpl: default
 dscp: default
            -----
```

77. show qos wred コマンド

本機の QoS のキューごとの設定を表示します。

# show qos wi	w qos wred red:	1			
	====				
Queue	Mode	Min Th	Mdp 1	Mdp 2	Mdp
0	disabled	0	1	5	10
1	disabled	0	1	5	10
2	disabled	0	1	5	10
3	disabled	0	1	5	10
4	disabled	0	1	5	10
5	disabled	0	1	5	10

78. show radius-server { * }コマンド

本機の RADIUS サーバ設定情報を表示します。

```
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

```
″show radius-server ?″と入力すると、以下のサブコマンドが表示されます。
```

show radius-server

```
Global RADIUS Server Timeout : 5 seconds

Global RADIUS Server Retransmit : 3 times

Global RADIUS Server Deadtime : 0 minutes

Global RADIUS Server Key :

Global RADIUS Server Attribute 4 :

Global RADIUS Server Attribute 95 :

Global RADIUS Server Attribute 32 :

No hosts configured!
```

79. show rmon alarm {*}コマンド

本機の RMON アラームの設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
                                         _____
# show rmon alarm ?
  <1~65535> Alarm entry list
  Output modifiers
   <cr>
          _____
例:
_____
# show rmon alarm 1
Alarm ID : 1
_____
    Interval : 2000
Variable : .1.3.6.1.2.1.2.2.1.13.1
SampleType : absoluteValue
Value : 0
Startup : risingOrFallingAlarm
RisingThrld : 2000000
FallingThrld : 200000
    RisingEventIndex : 0
    FallingEventIndex : 0
```

80. show rmon event {*}コマンド

本機の RMON イベントの設定情報を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

81. show rmon history {*}コマンド

本機のRMON ヒストリーの設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
                               _____
# show rmon history ?
  <1~65535> History entry list
            Output modifiers
  <cr>
 例:
         _____
# show rmon history
History ID : 1
  Data Bucket Request : 50
Data Interval
_____
  History ID
                  : 2
_____
 Data Source : .1.3.6.1.2.1.2.2.1.1.11
Data Bucket Request : 50
Data Bucket Granted : 50
                 : 1800
  Data Interval
      _____
```

82. show rmon statistics {*}コマンド

本機の RMON 統計情報を表示し * 以下の一覧から特定の項目を通 ["] show rmon statistics ?"と入力で	ます。 選択した場合、該当した情 すると、以下のサブコマンド	報のみを表示します。
# show rmon statisti <1~65535> <cr></cr>	cs ? Statistics entry Output modifiers	list
# show rmon statisti Statistics ID :	lcs 1 1	
Data Source etherStatsDropE etherStatsOctets etherStatsPkts etherStatsBroad etherStatsMultic etherStatsCRCAL etherStatsOvers etherStatsOvers etherStatsJabbes etherStatsJabbes etherStatsPkts6 etherStatsPkts6 etherStatsPkts1 etherStatsPkts5 etherStatsPkts5	vents : s : castPkts : castPkts : ignErrors : sizePkts : izePkts : rs : sions : 40ctets : 5to1270ctets : 28to2550ctets : 56to5110ctets : 12to10230ctets :	.1.3.6.1.2.1.2.2.1.1.12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

83. show running-config {*}コマンド

本機で現在動作している設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

<pre># show running-conf</pre>	ig ?
	Output modifiers
all-defaults	Include most/all default values
feature	Show configuration for specific feature
interface	Show specific interface(s)
line	Show line settings
vlan	VLAN
<cr></cr>	
例:	
<pre># show running-confi</pre>	-g
Building configurati	.on
username admin privi	lege 15 password encrypted YWRtaW4=
!	
vlan 1	
!	
vlan 3	
!	

```
vlan 10
vlan 20
ip route 0.0.0.0 255.255.255.0 192.168.1.1
spanning-tree mst name 00-ff-ff-ff-ff revision 0
voice vlan oui 00-03-6B description Cisco phones
.
interface GigabitEthernet 1/1
no spanning-tree
1
interface GigabitEthernet 1/2
no spanning-tree
!
interface GigabitEthernet 1/3
no spanning-tree
.
interface vlan 1
ip address 192.168.1.1 255.255.255.
line vty 14
!
line vty 15
!
end
            -----
```

84. show running-config all-defaults コマンド

全ての設定の初期値を表示します。

```
# show running-config all-defaults
Building configuration...
no logging
no logging on
no logging host
logging level info
username admin privilege 15 password encrypted YWRtaW4=
no access management
no loop-protect
loop-protect transmit-time 5
loop-protect shutdown-time 180
.
.
.
```

85. show sflow コマンド

本機の sflow の情報を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
_____
# show sflow ?
 Output modifiers
  statistics sFlow statistics.
  <cr>
        _____
 例:
           _____
_____
# show sflow
Agent Configuration:
_____
Agent Address: 127.0.0.1
Receiver Configuration:
_____
Owner
        : <none>
Receiver : 0.0.0.0
UDP Port : 6343
Max. Datagram
           : 1400 bytes
Time left : 0 seconds
No enabled collectors (receivers) Skipping displaying per-port info.
```

86. show sflow statistics receiver コマンド

本機の sflow のレシーバの統計情報を表示します。

# show sflow statistics receiver	
Tx Successes Tx Errors Flow Samples Counter Sample	S
0 0 0 0	

87. show sflow statistics samplers コマンド

本機の sflow のサンプラーの統計情報を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。 ["]show sflow statistics samplers ?"と入力すると、以下のサブコマンドが表示されます。

```
# show sflow statistics samplers ?
                   Output modifiers
  All switches or All ports
  GigabitEthernet 1 Gigabit Ethernet Port
  10GigabitEthernet 10 Gigabit Ethernet Port
  <range list>
                   runtime, see sflow icli functions.c
  <cr>
         _____
 例:
    _____
# show sflow statistics samplers
Per-Port Statistics:
_____
Interface Flow Samples Counter Samples
_____ ____
GigabitEthernet 2/1 0 0
GigabitEthernet 2/2 0 0
```

```
GigabitEthernet 2/3 0 0

.

.

GigabitEthernet 2/24 0 0

10GigabitEthernet 2/1 0 0

10GigabitEthernet 2/2 0 0
```

88. show snmp {*}コマンド

```
本機の SNMP 設定情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
```

"show snmp?"と入力すると、以下のサブコマンドが表示されます。

<pre># show snmp ? access community host mib security-to-group user view <cr></cr></pre>	Output modifiers access configuration Community Set SNMP host's configurations MIB(Management Information Base) security-to-group configuration User MIB view configuration
<pre># show snmp SNMP Configuration SNMP Mode SNMP Version Read Community Write Community Trap Mode SNMPv3 Communities T Community Source IP Source Mask Community Source IP Source Mask SNMPv3 Users Table: User Name Engine ID Security Level Authentication Proto Privacy Protocol</pre>	<pre>: enabled : 2c : public : private : disabled able: : public : 0.0.0.0 : 0.0.0.0 : private : 0.0.0.0 : 0.0.0.0.0 : 0.0.0.0.0 : 0.0.0.0 : 0.0.0.0 : 0.0.0.0 : 0.0.0.0 : 0.0.0.0.0 : 0.0</pre>
SNMPv3 Groups Table; Security Model Security Name Group Name Security Model Security Name Group Name Security Model Security Name Group Name Security Model Security Name Group Name	<pre>: v1 : public : default_ro_group : v1 : private : default_rw_group : v2c : public : default_ro_group : v2c : private : default_rw group</pre>

Security Model : v3 Security Name : default_user Group Name : default_rw_group SNMPv3 Accesses Table: SNMPv3 Accesses Table: Group Name : default_ro_group Security Model : any Security Level : NoAuth, NoPriv Read View Name : default_view Write View Name : default_rw_group Security Model : any Security Level : NoAuth, NoPriv Read View Name : default_view Write View Name : default_view Write View Name : default_view SNMPv3 Views Table : SNMPv3 Views Table : View Name : default_view OID Subtree : .1 View Type : included _____

89. show snmp access {*}コマンド

SNMP アクセスエントリを表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

<pre># show snmp access ? <groupname :="" word32=""> <cr></cr></groupname></pre>	Output modifiers group name
<pre># show snmp access Group Name : defa Security Model : any Security Level : NoAu Read View Name : defa Write View Name: <no :="" any="" defa="" default_v<="" group="" level="" model="" name="" name:="" noau="" pre="" read="" security="" view="" write=""></no></pre>	ault_ro_group ath, NoPriv ault_view view specified> ault_rw_group ath, NoPriv ault_view iew

90. show snmp community v3 {*}コマンド

本機の SNMPv3 コミュニティ名及び IP 設定を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show snmp community v3 ?"と入力すると、以下のサブコマンドが表示されます。

<pre># show snmp community v3 ? <community :="" word32=""> <cr></cr></community></pre>	Output modifiers Specify community na:	me
例:		
# show snmp community v3		115

Community	: public
Source IP	: 0.0.0.0
Source Mask	: 0.0.0.0
Community	: private
Source IP	: 0.0.0.0
Source Mask	: 0.0.0.0

91. show snmp host {*}コマンド

SNMP ホストの設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
_____
# show snmp host ?
  Output modifiers
  <ConfName : word32>Name of the host configuration
                    AAA event group
  aaa
  interface
                    Interface event group
                    Switch event group
  switch
  system
                    System event group
  <cr>
            _____
```

例:

# show shinp host	
Trap Global Mode	: Enabled
Trap test (ID:0) i	Disabled
Community	: Public
Destination Host	: 0.0.0.0
UDP Port	: 162
Version	: V2C
Inform Mode	: Disabled
Inform Timeout	: 3
Inform Retry	: 5

92. show snmp mib context コマンド

アクセス可能な本機の MIB 情報を表示します。

```
_____
# show snmp mib context
BRIDGE-MIB :
   - dot1dBase (.1.3.6.1.2.1.17.1)
   - dot1dTp (.1.3.6.1.2.1.17.4)
ENTITY-MIB :
   - entityMIBObjects (.1.3.6.1.2.1.47.1)
EtherLike-MIB :
   - transmission (.1.3.6.1.2.1.10)
IEEE8021-BRIDGE-MIB :
   - ieee8021BridgeBasePortTable (.1.3.111.2.802.1.1.2.1.1.4)
IEEE8021-MSTP-MIB :
   - ieee8021MstpMib (.1.3.111.2.802.1.1.6)
IEEE8021-PAE-MIB :
  - ieee8021paeMIB (.1.0.8802.1.1.1.1)
IEEE8021-Q-BRIDGE-MIB :
  - ieee8021QBridgeMib (.1.3.111.2.802.1.1.4)
IEEE8023-LAG-MIB :
  - lagMIBObjects (.1.2.840.10006.300.43.1)
```

```
SFLOW-MIB :
  - sFlowAgent (.1.3.6.1.4.1.14706.1.1)
SMON-MIB :
  - switchRMON (.1.3.6.1.2.1.16.22)
SNMP-FRAMEWORK-MIB :
  - snmpEngine (.1.3.6.1.6.3.10.2.1)
SNMP-MPD-MIB :
  - dot1dTpHCPortTable (.1.3.6.1.2.1.17.4.5)
   - snmpMPDStats (.1.3.6.1.6.3.11.2.1)
SNMP-USER-BASED-SM-MIB :
   - usmStats (.1.3.6.1.6.3.15.1.1)
   - usmUserTable (.1.3.6.1.6.3.15.1.2)
SNMP-VIEW-BASED-ACM-MIB :
   - vacmContextTable (.1.3.6.1.6.3.16.1.1)
   - vacmSecurityToGroupTable (.1.3.6.1.6.3.16.1.2)
   - vacmAccessTable (.1.3.6.1.6.3.16.1.4)
   - vacmMIBViews (.1.3.6.1.6.3.16.1.5)
                                        _ -----
_____
```

93. show snmp mib ifmib ifIndex コマンド

本機の Ifmib の情報を表示します。

# show sr ifIndex	nmp mib ifmib ifIndex ifDescr	Interface
1 2 3 •	Switch 1 - Port 1 Switch 1 - Port 2 Switch 1 - Port 3	GigabitEthernet 1/1 GigabitEthernet 1/2 GigabitEthernet 1/3
24 25 26 27 28 50001 60001	Switch 1 - Port 24 Switch 1 - Port 25 Switch 1 - Port 26 Switch 1 - Port 27 Switch 1 - Port 28 VLAN 1 IP Interface 1	GigabitEthernet 1/24 10GigabitEthernet 1/1 10GigabitEthernet 1/2 10GigabitEthernet 1/3 10GigabitEthernet 1/4 vlan 1 vlan 1

94. show snmp security-to-group {*}コマンド

SNMP セキュリティグループエントリを表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show snmp security-to-group ?"と入力すると、以下のサブコマンドが表示されます。

Security Name	:	public
Group Name	:	default_ro_group
Security Model	:	vl
Security Name	:	private
Group Name	:	default_rw_group
Security Model	:	v2c
Security Name	:	public
Group Name	:	default_ro_group
Security Model	:	v2c
Security Name	:	private
Group Name	:	default_rw_group
Security Model	:	v3
Security Name	:	default_user
Group Name	:	default_rw_group

```
95. show snmp user {*}コマンド
```

SNMP ユーザの情報を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

<pre># show snmp user ? <username :="" word32=""> <cr></cr></username></pre>	Output modifiers Security user name
<pre># show snmp user User Name : def Engine ID Security Level Authentication Protocol Privacy Protocol</pre>	ault_user : 800007e5017f000001 : NoAuth, NoPriv : None : None

96. show snmp view {*}コマンド

SNMP ビューの情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
------
                        _____
           _____
# show snmp view ?
             Output modifiers
 <ViewName : word32> MIB view name
 <cr>
_____
例:
_____
# show snmp view
View Name : default_view
OID Subtree : .1
View Type : included
             _____
```

97. show spanning-tree {*}コマンド

本機のスパニングツリーの設定を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

<pre># show spanning-tree</pre>	2 ?
	Output modifiers
active	STP active interfaces
detailed	STP statistics
interface	Choose port
mst	Configuration
summary	STP summary
<cr></cr>	1
例:	
<pre># show spanning-tree</pre>	j
CIST Bridge STP Stat	
Bridge ID	· 32768 00-17-2E-FF-FF
Root ID	• 32768 00-17-2E-FF-FF
Boot Port	• -
Root PathCost	• 0
Regional Root	• • • • • • • • • • • • • • • • • • •
Int PathCost	• 0
May Hope	. 0
Max nops	· 20
TC Flag	· o
	. 0
TC Last	
Port Port Role	State Pri PathCost Edge P2P Uptime

98. show spanning-tree active コマンド

アクティブなスパニングツリーの情報を表示します。

```
_____
# show spanning-tree active
CIST Bridge STP Status
Bridge ID : 32768.00-17-2E-FF-FF
Root ID
              : 32768.00-17-2E-FF-FF
Root Port
              : -
Root PathCost : 0
Regional Root : 32768.00-17-2E-FF-FF
Int. PathCost
              : 0
        . 20
: Steady
: 0
Max Hops
TC Flag
TC Count
TC Last
Port Port Role State Pri PathCost Edge P2P Uptime
        _____ __ ___ ___ ___ ___ ___ ___ ___
_____
```

99. show spanning-tree detailed {*}コマンド

```
スパニングツリーの詳細について情報を表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
"show spanning-tree detailed ?"と入力すると、以下のサブコマンドが表示されます。
 _____
 # show spanning-tree detailed ?
  | Output modifiers
   interface List of port type and port ID, ex, Fast 1/1 Gigabit 2/3-5
        Gigabit 3/2-4 Tengigabit 4/6
   <cr>
 _____
  例:
         _____
 # show spanning-tree detailed
 Port Rx MSTP Tx MSTP Rx RSTP Tx RSTP Rx STP Tx STP Rx TCN Tx
 TCN Rx Ill. Rx Unk.
```

100. show spanning-tree mst {*}コマンド

本機の MSTP ブリッジのステータスを表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show spanning-tree mst?"と入力すると、以下のサブコマンドが表示されます。

```
_____
# show spanning-tree mst ?
  <Instance : 0-7> Choose port
             Output modifiers
  configuration
              STP bridge instance no (0-7, CIST=0, MST2=1...)
  <cr>>
           _____
 例:
_____
# show spanning-tree mst
CIST Bridge STP Status
Bridge ID : 32768.00-17-2E-FF-FF
Root ID : 32768.00-17-2E-FF-FF
Root Port : -
Root PathCost: 0
Regional Root: 32768.00-17-2E-FF-FF
Int. PathCost: 0
Max Hops : 20
TC Flag : Steady
TC Count : 0
TC Last
        : -
Mst Port PortRole State Pri PathCost Edge P2P Uptime
    _____ ___ ____
```

101. show spanning-tree mst configuration コマンド

本機の MST の VLAN マッピング設定情報を表示します。

# show	sp	anning	-tree mst	configuration	
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		

102. show spanning-tree summary コマンド

スパニングツリー情報の概要を表示します。

```
# show spanning-tree summary
Protocol Version: RSTP
Max Age : 20
Forward Delay : 15
Tx Hold Count : 6
Max Hop Count : 20
BPDU Filtering : Disabled
BPDU Guard : Disabled
Error Recovery : Disabled
CIST Bridge is active
```

103. show switch stack コマンド

スイッチのスタック状態についての情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
# show switch stack ?
  details Detail information
  <cr>
      _____
例:
_____
# show switch stack
Stack Interface A : 10GigabitEthernet 2/1
Stack Interface B : 10GigabitEthernet 2/2
           Forwarding Master
          SID Intf A Intf B Prio Time
Stack Member
----- ---- ---- ----- -----
*00-17-2e-FF-FF-F2 2 Local Local 1 01:27:44
00-17-2e-FF-FF-F1 1 Currently not present in stack
00-17-2e-FF-FF-F3 3 Currently not present in stack
_____
```

104. show switch stack details コマンド

スイッチのスタック状態について詳細な情報を表示します。

<pre># show switch stack det Stack topology : S Stack Member Count : 1 Last Topology Change: 1 Master Switch : C Last Master Change : 1 Stack Interface A : 1 Stack Interface B : 1 Fo: Stack Member SID</pre>	ails Standalone .970-01-01T0 00-17-2e-FF- .970-01-01T0 .0GigabitEth .0GigabitEth rwarding Intf A Int	0:00:00+00: FF-F2 0:00:00+00: ernet 2/1 ernet 2/2 Master :f B Prio	00 00 Time	Reelect
*00-17-2e-FF-FF-F2 2	Local Lo	cal 1	01:28:30	0
00-17-2e-FF-FF-F1 1	Currently r	not present	in stack	
00-17-2e-FF-FF-F3 3	Currently r	not present	in stack	
In	tf A Int	f B		
Link State:	Up	Down		
SPROUT State:	Down	Down		
SPROUT Update Counters:				
Rx PDUs:	1608	0		
Tx Periodic PDUs:	1607	0		
Tx Triggered PDUs:	1	0		
Tx Policer Drops:	0	0		
Rx Errors:	0	0		
Tx Errors:	0	0		
SPROUT Alert Counters:				
Rx PDUs:	0	0		
Tx PDUs:	0	0		
Tx Policer Drops:	0	0		
Rx Errors:	0	0		
Tx Errors:	0	0		

105. show switchport forbidden {*}コマンド

```
VLAN ID の禁止ポートのエントリーを表示します。
*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
"show switchport forbidden ?"と入力すると、以下のサブコマンドが表示されます。
 _____
 # show switchport forbidden ?
   | Output modifiers
   name - Show forbidden access for specific VLAN name.
   vlan vid - Show forbidden access for specific VLAN id.
   <cr>
 _____
        _____
  例:
 _____
 # show switchport forbidden
 VID Interfaces
 ____
    _____
 100 2
 _____
```

106. show switchport forbidden name <name>コマンド

指定した VLAN 名のアクセス禁止ポートの情報を表示します。

# shc VID	w switchport VLAN Name	forbidden n	ame V100eigyou Interfaces	
100	V100eigyou		25,26	

107. show switchport forbidden vlan <vlan_id>コマンド

指定した VLAN ID のアクセス禁止ポートの情報を表示します。

```
# show switchport forbidden vlan 100
VID Interfaces
100 2
```

108. show tacacs-server コマンド

本機に設定されている TACACS サーバの情報を表示します。

```
# show tacacs-server
Global TACACS+ Server Timeout : 5 seconds
Global TACACS+ Server Deadtime : 0 minutes
Global TACACS+ Server Key :
No hosts configured!
```

109. show terminal コマンド

ターミナルの情報を表示します。

```
_____
# show terminal
Line is con 0.
  * You are at this line now.
  Alive from Console.
  Default privileged level is 2.
  Command line editing is enabled
  Display EXEC banner is enabled.
  Display Day banner is enabled.
  Terminal width is 80.
          length is 24.
          history size is 32.
          exec-timeout is 10 min 0 second.
  Current session privilege is 15.
  Elapsed time is 0 day 0 hour 28 min 49 sec.
  Idle time is 0 day 0 hour 0 min 0 sec.
_____
```

110. show users {*}コマンド

本機に現在ログインしているユーザの情報を表示します。

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

```
_____
# show users ?
  | Output modifiers
  myself Display information about mine
  <cr>
     _____
 例:
_____
# show users
 Line is con 0.
  * You are at this line now.
  Connection is from Console.
  User name is admin.
  Privilege is 15.
  Elapsed time is 0 day 0 hour 1 min 53 sec.
  Idle time is 0 day 0 hour 0 min 0 sec.
 Line is vty 0.
  Connection is from 192.168.11.100:49166 by Telnet.
  User name is test.
  Privilege is 0.
  Elapsed time is 0 day 0 hour 0 min 5 sec.
  Idle time is 0 day 0 hour 0 min 3 sec.
```

111. show version コマンド

本機の MAC アドレスやシステム情報、ファームウェアバージョンなどの情報を表示します。

<pre># show version MAC Address Previous Restart System Contact System Name System Location System Time</pre>	: 00-17-2e-FF-FF : Cold : : : : 1970-01-01T07:14:39+00:00
System Uptime Active Image	: 07:14:39
 Image Version Date Alternate Image	: managed : FXC5428 Ver:1.00.01 : 2015-05-13
Image Version Date	: managed.bk : FXC5428 Ver:1.00.01 : 2015-05-13
SID : 2	
Port Count Product Software Version	: 28 : FXC5428 Switch : FXC5428 Ver:1.00.01

112. show vlan {*}コマンド

本機の VLAN 設定情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show vlan ?"と入力すると、以下のサブコマンドが表示されます。

<pre># sho a b i i n r r s s <</pre>	ow vlan ? ll prief d p-subnet ac ame protocol status Ccr>	Show all VLANs (If left out only static VLANs are shown) VLAN summary information VLAN status by VLAN id Show VLAN ip-subnet entries. Show VLAN MAC entries. VLAN status by VLAN name Protocol-based VLAN status Show the VLANs configured for each interface.
例:		
# sho VLAN	ow vlan Name	Interfaces
1	default	Gi 1/1-2,4-24 Gi 2/1-24 Gi 3/1-24
100	V100eigyo	u

113. show vlan brief コマンド

本機の VLAN 情報の概要を表示します。

# shc	w vlan brief Name	Interfaces
1	default	Gi 1/1,6-24 Gi 2/1-24 Gi 3/1-24
2	VLAN0002	Gi 1/2
3	VLAN0003	Gi 1/3
4	VLAN0004	Gi 1/4

114. show vlan id <vlan_list>コマンド

指定した VLAN ID の情報を表示します。

# sh VLAN	ow vlan id 1-3 Name	Interfaces
1	default	Gi 1/1,6-24 Gi 2/1-24 Gi 3/1-24
2 3	VLAN0002 VLAN0003	Gi 1/2 Gi 1/3

115. show vlan ip-subnet id {*}コマンド

VLANのIPサブネット設定の情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

"show vlan ip-subnet ?"と入力すると、以下のサブコマンドが表示されます。

```
116. show vlan mac {*}コマンド
```

MAC アドレスごとの VID 及び接続ポートの情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
# show vlan mac ?
address Show a specific MAC entry.
<cr>
例:
FXC5428# show vlan mac
MAC Address VID Interfaces
```

117. show vlan name <vword32>コマンド

指定した VLAN 名が設定されている VLAN ID の情報を表示します。

```
# show vlan name test
VLAN Name Interfaces
3 test Gi 1/3-4
```

118. show vlan protocol { * }コマンド

プロトコルベース VLAN の情報を表示します。 *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
    _____
# show vlan protocol ?
 eth2 Ethernet protocol based VLAN status
     LLC-based VLAN status
 llc
    SNAP-based VLAN status
 snap
 <cr>
_____
例·
   ------
            ______
# show vlan protocol
Protocol Type Protocol (Value) Group ID
_____
               1
EthernetII ETYPE:0x800
Switch 1
_____
Group ID
        VID Ports
----- ----
1
       1
          GigabitEthernet 1/4
_____
                     _____
```

119. show vlan status {*}コマンド

インタフェースごとの VLAN 設定を表示します。

*以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。

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

```
_____
# show vlan status ?
  admin Show the VLANs configured by administrator.
  all
              Show all VLANs configured.
  all
combined
conflicts
             Show the VLANs configured by a combination.
             Show VLANs configurations that has conflicts.
             Show the VLANs configured by GVRP.
  avrp
  interface Show the VLANs configured for a specific interface(s)
              Show the VLANs configured by MSTP.
  mstp
              Show the VLANs configured by MVR.
  mvr
              Show the VLANs configured by NAS.
  nas
       Show the VLANs configured by VCL.
  vcl
  voice-vlan Show the VLANs configured by Voice VLAN.
  <cr>
_____
例:
         _____
____
# show vlan status
GigabitEthernet 1/1 :
------
              PVID Frame Type Ing Filter Tx Tag
VLAN User PortType
UVID Conflicts
----- ------ ---- -----
_____
      C-Port 1 All Enabled All except-native 1
Admin
NAS
   No
GVRP
   No
MVR
   No
Voice VLAN
   No
MSTP
   No
VCL
   No
Combined C-Port 1 All Enabled All except-native
1 No
GigabitEthernet 1/2 :
_____
VLAN User PortType PVID Frame Type Ing Filter Tx Tag
UVID Conflicts
----- ----- ---- ----- ----- ------
      C-Port 1 All Enabled All except-native 1
Admin
NAS
   No
GVRP
   No
MVR
   No
Voice VLAN
    No
MSTP
   No
VCL
   No
```

1章 コマンドインタフェース

```
Combined C-Port
               1
                                  All except-native
                   All
                           Enabled
1 No
.
.
10GigabitEthernet 1/1 :
_____
VLAN User PortType PVID Frame Type Ing Filter Tx Tag
UVID Conflicts
----- ----- ---- -----
----- ----
              1
                 All
                      Enabled All except-native 1
Admin C-Port
NAS
   No
GVRP
   No
MVR
   No
Voice VLAN
   No
MSTP
   No
VCL
   No
Combined C-Port 1 All Enabled All except-native
1 No
10GigabitEthernet 1/2 :
_____
VLAN User PortType PVID Frame Type Ing Filter Tx Tag
UVID Conflicts
----- ----- ---- ----- -----
----- ----
            1 All
Admin C-Port
                          Enabled All except-native 1
NAS
  No
GVRP
  No
MVR
  No
Voice VLAN
   No
MSTP
  No
VCL
   No
Combined C-Port 1 All Enabled All except-native
1 No
_____
```

```
120. show voice vlan {*}コマンド
   音声 VLAN の情報を表示します。
   *以下の一覧から特定の項目を選択した場合、該当した情報のみを表示します。
   "show voice vlan ?"と入力すると、以下のサブコマンドが表示されます。
     _____
     # show voice vlan ?
        Output modifiers
                   Select an interface to configure
        interface
                      OUI configuration
        oui
        <cr>
     _____
     例:
         _____
     # show voice vlan
     Switch voice vlan is disabled
     Switch voice vlan ID is 1000
     Switch voice vlan aging-time is 86400 seconds
     Switch voice vlan traffic class is 7
     Telephony OUI Description
     -----
    00-01-E3Siemens AG phones00-03-6BCisco phones00-0F-E2H3C phones00-60-B9Philips and NEC AG phones00-D0-1EPingtel phones00-E0-75Polycom phones00-E0-BB3Com phones
     Voice VLAN switchport is configured on following:
     GigabitEthernet 1/1 :
     _____
     GigabitEthernet 1/1 switchport voice vlan mode is disabled
     GigabitEthernet 1/1 switchport voice security is disabled
     GigabitEthernet 1/1 switchport voice discovery protocol is oui
     GigabitEthernet 1/2 :
     _____
     GigabitEthernet 1/2 switchport voice vlan mode is disabled
     GigabitEthernet 1/2 switchport voice security is disabled
     GigabitEthernet 1/2 switchport voice discovery protocol is oui
     GigabitEthernet 1/24 :
     _____
     GigabitEthernet 1/24 switchport voice vlan mode is disabled
     GigabitEthernet 1/24 switchport voice security is disabled
     GigabitEthernet 1/24 switchport voice discovery protocol is oui
     10GigabitEthernet 1/1 :
     10GigabitEthernet 1/1 switchport voice vlan mode is disabled
     10GigabitEthernet 1/1 switchport voice security is disabled
     10GigabitEthernet 1/1 switchport voice discovery protocol is oui
     10GigabitEthernet 1/2 :
     _____
     10GigabitEthernet 1/2 switchport voice vlan mode is disabled
     10GigabitEthernet 1/2 switchport voice security is disabled
     10GigabitEthernet 1/2 switchport voice discovery protocol is oui
```

121. show web privilege group $\langle group_name \rangle$ level $\exists \forall \forall \flat k$

それぞれの機能グループの特権レベルを表示します。

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

#	show web	privilege group ?
	CWORD	Valid words are 'Aggregation' 'DHCP' 'Debug' 'Dhcp_Client'
		'Diagnostics' 'EEE' 'Fan Control' 'Green Ethernet' 'IP2'
		'IPMC Snooping' 'LACP' 'LLDP' 'Loop Protect' 'MAC Table'
		'MVR' 'Maintenance' 'Mirroring' 'NTP' 'Ports'
		'Private VLANs' 'QoS' 'RPC' 'Security' 'Spanning Tree'
		'Stack' 'System' 'Timer' 'VCL'
		'VLANs' 'Voice VLAN' 'XXRP' 'sFlow'
	level	Web privilege group level

<proup_name>を指定して入力した場合はそのグループの特権レベルを、<proup_name>を指定せず "show web privilege group level"と入力した場合は全てのグループの特権レベルを表示します。 例:

gr Pr CR	oup ivil O CRI	leve ege W SF	el Level RO SRW		
.5	10	.5	- - 10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
15	15	15	15		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	1	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	1	10		
5	10	1	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
5	10	5	10		
	gPC 555555555555555555555555555555555555	group 7 Privile CRO CRU 5 10 5 10 5 10 5 10 5 10 5 10 5 10 5 10	group leve Privilege CRO CRW SF 5 10 5 5 10 5 5 5 10 5 5 1	group level Privilege Level CRO CRW SRO SRW 5 10 5 10 5 10 5 10 5 10 5 1	group level Privilege Level CRO CRW SRO SRW 5 10 5 10 5 10 5 10 5 10 5 10 5 10 5 10 5 10 5 10 5 10 5 10 5 10



2.1 Telnet/SNMP 管理

2.1.1 Telnetによるマネジメント管理

Telnet を介して本機のリモート管理を行う場合は、まず IP/NetMask/Gateway(任意)アドレスを設定し、コンソール 画面を使って、操作を行ってください。

2.1.2 SNMPによるマネジメント管理

NMS を介して本機のリモート管理を行う場合は、IP/NetMask/Gateway アドレスを設定して、SNMP の設定を 行ってください。

本機では、SNMP v1, v2c, v3 のエージェント機能および MIB II(Interface)、Bridge MIB、802.1Q MIB および Private MIB をサポートしています。 初期設定の GET コミュニティ名は"public"、および SET コミュニティ名は"private"です。

2.2 初期設定

ここでは、WEB ブラウザを用いて本製品のWEB マネジメント画面にログインする手順を説明いたします。

2.2.1 ログイン方法

WEB ブラウザを使用してログインするには以下の手順に従ってください。

Step 1. WEB ブラウザを起動します。

- Step 2. WEB ブラウザの「アドレス」に本製品の IP アドレスを入力し、Enter キーを入力します。 (初期設定時は、IP アドレス、"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「ユーザー名」と「パスワード」を入力します。 (初期設定時は、「ユーザー名」と「パスワード」ともに"admin"となります。)
- IP アドレスを変更する場合は、以下の手順に従ってください。
 - 1) "config"コマンドを入力すると、"(config)#"がプロンプト表示されます。
 - 2) "interface vlan 1"コマンドを入力すると、"(config-if-vlan)#"のプロンプト表示に切り替わります。
 - 3) "ip xxx.xxx.xxx yyy.yyy.yyy.yyy.yyy"コマンド(xxx.xxx.xxx は IP アドレス、yyy.yyy.yyy.yyy はネットマ スク)を入力して、本体の IP アドレスを変更します。
 - 4) "exit"コマンドを入力し、"(config)#"に戻ります。
 - 5) IP ゲートウェイを設定する場合は、"ip route 0.0.0.0 0.0.0.0 zzz.zzz.zzz.zzz"コマンドを入力して、 IP ルートエントリを設定します(zzz.zzz.zzz.zzz はゲートウェイの IP アドレスです)。
 - 6) "exit"コマンドを入力すると、"#"のプロンプト表示に切り替わります。
 - 7) "show ip interface brief"コマンドを入力して、IP が正しく設定されているかどうか確認してください。
 - 8) "copy running-config startup-config"コマンドを入力して、設定値を保存します。

HTTP 接続を開始するには、IP を設定した後ネットワークに接続後、本機の IP アドレスを WEB ブラウザの WEB アド レスに入力すると、以下のユーザ名とパスワードのログイン画面が表示されます(デフォルトのユーザ名とパスワードは *admin* / *admin* です)。

初期設定値

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

認証用アクセス画面

Windows セキュリ	71	×			
iexplore.exe サーバー 192.168がユーザー名とパスワードを要求しています。サーバーの報告 によると、これは FXC5428 からの要求です。					
警告: ユーザー名とパスワードは、セキュリティで保護されていない接続で基本認証を 使用して送信されます。 					
8	 □ 資格情報を記憶する 				
	OK キャンセル				

【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 4 人までのユーザのみが同時にログインすることが可能です。

【注意】:

WEB ブラウザは"Microsoft IE 6.0"以上、"Netscape V7.1"以上、あるいは"Fire Fox V1.00"以上、 またモニターは解像度を"1024x768"以上でご使用になることを推奨します。

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。

Future X Communications	2 4 6 8 10 12 14 16 18 20 22 24 Image: Contract of the state of the sta	
 Configuration Bystem Information IP NTP Time Log Ports DHCP Security Aggregation Loop Protection Spanning Tree IPMC Profile MVR IPMC Profile MVR ILDP MAC Table VLANs Private VLANs VCL Voice VLAN QoS Mirroring GVRP Stack sFlow Monitor Diagnostics Maintenance 	stem Information Configuration ystem Contact ystem Name ystem Location Nave Reset	
• ① メニューウィンドウ	② メインウィンドウ	■ ③ トップメニューウィンドウ

設定/表示項目:

① メニューウィンドウ

メニューウィンドウでは、本製品でサポートされる各メニューがツリー状に表示されます。 それぞれ、「Configuration(設定)」メニュー、「Monitor(モニタリング)」メニュー、「Dignostics(診断)」 メニュー、「Maintenance(メンテナンス)」メニューの4つメニューから構成されています。

- ② メインウィンドウ
 メニューウィンドウで選択したメニューの設定項目、およびステータス情報を表示します。
- ③ トップメニューウィンドウ

本製品のインターフェイスが表示されており、10/100M、1000M、10G でリンクアップしている場合は それぞれ「緑色」で表します。 また各ポートをクリックすることにより、カウンターのメニューが表示されます。 「Logout」ボタンをクリックすることにより本製品からログアウトします。 「Show help」からは表示メニューの Help を別ウィンドウで表示することが可能です。

画面の右上に以下のアイコンが表示されます。



ログアウト用のボタンです。



ヘルプ情報を入手することができます。

HTTP 接続によるマネジメント方法の詳細は、以降の項で説明します。

2.3 メインメニュー

2.3.1 メニューの構成

ここでは、それぞれ以下のメニューから構成されています。

- 1. System (システム)
 - (1) システム名、問い合わせ先、ロケーション、Mac ID、ファームウェアバージョン、稼働時間
 - (2) IP 設定
 - (3) NTP 設定
 - (4) タイム設定
 - (5) log 設定
- 2. Port (ポート)
 - ポートネーム、通信速度、通信モード、ステータス、フローコントロール、最大パケットサイズ、Excessive Collision 設定
- 3. DHCP
 - (1) DHCP スヌーピング
 - (2) DHCP リレー
- 4. Security (セキュリティ)
 - (1)セキュリティ管理
 - a)管理パスワード、管理者および優先レベルの設定
 - b) コンソール、telnet, ssh, http インタフェースの認証方式
 - c)管理アクセスの制限
 - d) SSH, HTTPS 設定
 - e) SNMP 設定
 - f) RMON 設定
 - (2) ネットワークアクセスのセキュリティ
 - a)ポートのネットワーク接続数の制限
 - b) 802.1x ネットワークアクセスの設定
 - c) ACL 設定
 - d) IP ソースガードの設定
 - e) ARP インスペクションの設定
 - (3) AAA
- a) RADIUS および TACACS+サーバの設定
- 5. Aggregation (アグリゲーション)
 - (1) スタティックトランク設定
 - (2) LACP 設定
- Loop Protection (ループプロテクション)

 ループプロテクションの設定
- 7. Spanning Tree (スパニングツリー)
 - (1) グローバル設定
 - a)プロトコル、プライオリティ設定
 - b) Forward Delay、Max Age、Hop Count、Hold Count 設定
 - c) BPDU フィルター、BPDU ガード設定
 - (2) MSTI マッピング設定
 - (3) MSTI プライオリティ設定
 - (4) CIST ポート設定
 - (5) MSTIポート設定

```
    8. IPMC Profile (IP マルチキャスト)
    (1) IP マルチキャストプロファイル
```

9. MVR

(1) MVR 設定

10. IPMC

(1) IGMP スヌーピング設定(2) MLD スヌーピング設定

11. LLDP

(1) LLDP 設定

- MAC Table (MAC テーブル)

 エージングタイム、ラーニング、安全設定
 スタティック Mac ID の割り当て
- 13. VLAN (1) 802.1Q VLAN 設定
- 14. プライベート Vlan (1) Isolation 設定

15. VCL

- (1) Mac-based Vlan 設定
- (2) Protocol-based Vlan 設定
- (3) IP Subnet-based Vlan 設定
- 16. Voice Vlan
 - (1) コンフィグレーション設定
 - (2) OUI エントリー設定

17. QoS

(1) ポートのデフォルト QoS 設定
(2) ポート入力ポリシング設定
(3) ポート出力スケジューリング設定
(4) 出力シェイピング設定
(5) ポートタグリマーキング設定
(6) ポート DSCP 設定
(7) DSCP クラス設定
(8) DSCP トランスレーション設定
(9) DSCP マッピング設定
(10) QoS コントロールリスト設定
(11) QoS ストームコントロール設定
(12) WRED 設定

- 18. Mirroring (ポートミラーリング)
 (1) ポートミラーリング設定
- 19. GVRP
 - (1) Enable 設定 Join-time、Leave-time、LeaveAll-time、Max Vlan 設定
 (2) ポート Enable 設定
- 20. Stack(スタックモジュール用)
 - (1) スタック設定
21. sFlow

(1) sFlow 設定

- 22. モニタリング (1) コンフィグレーションで設定した機能結果を表示
- 23. 診断機能
 - (1) Ping 機能
 - (2) VeriPHY 機能
- 24. メンテナンス
 - (1) リスタート
 - (2) 初期設定のリストア
 - (3) ソフトウェアのアップデート
 - (4) アップロード/リストア

2.4 Configuration(各機能の設定)

ここでは、各機能の設定方法について説明します。



2.4.1 System (システム)

システム情報について表示します。

Save Reset

2.4.1.1 Information (システム情報の設定)

ここでは、システム名、設置場所、システム担当者名の設定を行うことができます。

「Configuration」→「System」→「Information」をクリックすると、以下の画面が表示されます。

System Information Configuration

System Contact	
System Name	
System Location	

2.4.1.2 IP (IP 設定)

ここでは DNS サーバと管理 IP アドレスの設定を行います。 IP 設定メニューは、「Host」モードと「Router」モードから選択することが可能です。

(1)「System」→「IP」をクリックすると、以下の画面が表示されます。

IP Confi	IP Configuration Host/Router モード							
Mode DNS Ser DNS Pro	Mode From any DHCP interfaces DNS Server No DNS server DNS Proxy Configured From this DHCP interface							
IP Interf	aces			n			ID.C	
Delete	VLAN	Enable	Fallback	HCP IPv4 IPv6 Current Address Mask Address Lease		Mask Length		
	1		0		192.168.11.206	24		
Add Inte	Add Interface							
IP Route	IP Routes							
Delete	Delete Network Mask Length Gateway Next Hop VLAN							
Add Rou	Add Route							
Save	Save Reset							
Note: the r	Note: the next hop VLAN can be set only in IPv6.							

DNS サーバを使用する場合は、サーバ IP を入力してください。 DHCP クライアント機能を有効にすると、DHCP サーバから自動的に IP が設定されます。 DHCP クライアント機能を無効にすると、手動にて IP の設定を行うことができます。

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.4.1.3 NTP (NTP 設定)

ここでは本機の NTP の設定を行うことができます。 「Configuration」→「System」→「NTP」をクリックすると、次の画面が表示されます。

NTP Configuration

Disabled	~
	Disabled

Save Reset

本機は、NTP プロトコルをサポートしているため、NTP サーバから時刻情報を入手することができます。

この機能を有効にしてから、NTP サーバの IP を入力してください。 【注記】:機能を有効にするには、ネットワーク管理者によって、まず NTP サーバの IP を入手する必要があります。

2.4.1.4 Time (タイム設定)

```
ここでは時刻の設定を行うことができます。
```

```
サマータイムの設定を行うには、「Configuration」→「System」→「Time」をクリックすると、以下の画面が表示されます。
```

Time Zone Configuration

	Time	Zone Configuration	
Time Zone	None		`
Acronym		(0 - 16 characters)	
Daylight Savin	g Time Configura	tion	
Da	ylight Saving Time	Mode	
Daylight Saving	Time Disabled	\sim	
	Start Time cottin	ac.	
Month	Jan	gs v	
Dato	1		
Voar	2000		
Houre	0		
Minutes	0	~	
minutos	End Time setting	ns.	
Month	Jan	~	
Date	1	~	
Year	2000	~	
Hours	0	\sim	
Minutes	0	\sim	
	Offset settings		
Offset	1	(1 - 1440) Minutes	

Save Reset

NTP を使って、タイムゾーンを設定することができます。NTP では、英国のグリニッジを通る地球の本初子午線(経度 0)を基準とする協定世界時が使用されます(協定世界時は、UTC と呼ばれるものであり、正式名称はグリニッジ標 準時間(GMT))。デバイスの正確な時間を保持することにより、システムログはイベントエントリの日時を正確に記録 します。

ローカルタイムに応じて現在の時刻を表示するには、お使いのタイムゾーンの設定を行ってください。

「サマータイム」機能により、通常の時刻より1時間早くシステムタイムを設定することが可能です。 開始時間と終了時間を設定することで、その期間サマータイム機能を有効化できます。

2.4.1.5 Log

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 サーバヘイベントが記録されます。 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)。

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。 「Configuration」→「System」→「Log」をクリックすると、以下の画面が表示されます。

System Log Configuration

Syslog Mode)isabled 🗸
Server Mode	Disabled V
Server Address	
Syslog Level	Info
Save Reset	Warning Error

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。

2.4.2 Port (ポート設定)

ここでは、ポートネーム、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。

ここでは、各ポートの設定を行うことができます。

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

Port Configuration for Switch 1

Port C	onfiguration for Switch 1									Refresh
				Speed			Flow Contro	bl	Maximum	Excessive
Port	Name	Link	Current	Configured		Current Rx	Current Tx	Configured	Frame Size	Collision Mode
*				\diamond	<				10056	◇ ∨
1	Port 1		1Gfdx	Auto	\sim	×	×		10056	Discard 🗸
2	Port 2		Down	Auto	\checkmark	×	×		10056	Discard 🗸
3	Port 3	۲	Down	Auto	\sim	×	×		10056	Discard 🗸
4	Port 4		Down	Auto	\sim	×	×		10056	Discard 🗸
5	Port 5		Down	Auto	\sim	×	×		10056	Discard 🗸
6	Port 6		Down	Auto	\checkmark	×	×		10056	Discard 🗸
7	Port 7		Down	Auto	\sim	×	×		10056	Discard 🗸
8	Port 8		Down	Auto	\checkmark	×	×		10056	Discard 🗸
9	Port 9		Down	Auto	$\mathbf{\sim}$	×	x		10056	Discard 🗸
10	Port 10	٠	Down	Auto	\sim	×	×		10056	Discard 🗸
11	Port 11	۲	Down	Auto	~	×	×		10056	Discard 🗸
12	Port 12	٠	Down	Auto	~	×	×		10056	Discard 🗸

ポートの設定	
Name:	各インタフェース管理用の名前を作成します。
Speed:	通信速度および通信方式の設定を行います。
Flow Control:	全二重通信時のフロー制御を設定します。
Maximum Frame Size:	最大フレームサイズを設定します。範囲は「1518-10056」バイトで す。尚、設定する場合は、本機に接続する他のネットワーク機器が ジャンボフレーム機能に対応しているか確認してください。
Excessive Collision Mode:	半二重通信時のコリジョン機能の設定をします。

2.4.3 DHCP

この機能は、DHCP 機能について以下のメニューをサポートしています。

2.4.3.1 Snooping (DHCP スヌーピング)

DHCP スヌーピングは、DHCP クライアント/サーバ間での DHCP メッセージ情報を監視する機能です。 これにより、不正な DHCP サーバの侵入を防ぐことができます。

DHCPの設定メニューは、以下のとおりです。

- ・ 有効/無効の設定
- ・ DHCP セキュリティデータベースの設定
- Trusted/Untrustedの設定
- DHCPの設定を行うには、「Configuration」 -> 「DHCP」 -> 「Snooping」をクリックすると、以下の画面が表示 されます。

DHCP Snooping Configuration

Snooping Mode Disabled ✓

Database

Agent URL		
Timeout interval	300	seconds
Write delay interval	300	seconds

Renew DHCP Snooping URL

Renew

Port Mode Configuration for Switch 1

Port	Mode		
*	<>	<	
1	Trusted	<	
2	Trusted	~	
3	Trusted	<	
4	Trusted	~	
5	Trusted	<	
6	Trusted	<	
7	Trusted	<	
8	Trusted	~	

2.4.3.2 Relay (DHCP リレーエージェント)

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 リレーは、異なるサブネットドメインのクライアントおよびサーバ間で DHCP メッセージの送受信を行うために使用 します。

クライアントの DHCP パケットを DHCP サーバに送信する際、「DHCP オプション 82」により DHCP リレーエージェントは、 DHCP リクエストパケットに特定情報を取り込み、サーバの DHCP パケットを DHCP クライアントに送信する際に DHCP リレーパケットから特定の情報を取り除きます。

DHCP サーバはこの情報を用いて、IP アドレス、またはその他の割り当てポリシーを実行します。特にこのオプションは、 回線 ID(オプション(1)およびリモート ID(オプション(2)の 2 つのサブオプションを設定することによって機能します。 回線 ID のサブオプションにはリクエストを受信した回線に関する情報が含まれるように設定され、リモート ID のサブオプ ションには回線のリモート側のホストに関連のある情報を送信するように設定されています。

本機の回線 ID の定義は「4 バイト」であり、フォーマットは"vlan_id","module_id","port_no"となります。 "vlan_id"パラメータは、先頭の2 バイトは「VLAN ID」を表します。"module_id"パラメータは、モジュール ID の3 番目の バイト(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)。 "port_no"パラメータは 4 番目のバイトであり、「ポート番号」を表します。

リモート ID は 6 バイトであり、かつその値は DHCP リレーエージェントの MAC アドレスの値と同じです。

ここでは、DHCP の有効/無効、VLAN のレンジを設定します。

DHCP 設定を行うには、「Configuration」 -> 「DHCP」 -> 「Relay」をクリックすると、以下の画面が表示されます。

DHCP Relay Configuration

Relay Mode	Disabled	<
Relay Server	0.0.0.0	
Relay Information Mode	Disabled	~
Relay Information Policy	Кеер	~

Save Reset

2.4.4 Security (セキュリティ設定)

ここでは、セキュリティに関する設定について説明します。

2.4.4.1 Switch (スイッチ管理上のセキュリティ)

ユーザの優先レベルは、1~15 段階に分かれています。レベル 15 は、どのグループにもアクセス可能であり、デバイス のすべてを管理することができます。それ以外の優先レベルについては、各グループの優先レベルを参照してください。 ユーザの優先レベルは、アクセス先のグループの優先レベル以上の値に設定して下さい。 デフォルト設定では、グループの「レベル 5」は読取り用アクセス、「レベル 10」は読書き用アクセスです。 システムメンテナンス(ソフトウェアのアップロード、工場出荷時設定など)を行う場合は「レベル 15」が必要となります。 通常、「レベル 15」は管理者向けアカウント、「レベル 10」は標準ユーザ向けアカウント、「レベル 5」はゲスト向けアカウ ントとなります。

1. User (管理者およびユーザアクセスレベルの設定)

 ユーザ設定を行うには、「Configuration」->「Security」->「Switch」->「Users」をクリックすると、 以下の画面が表示されます。

Users Configuration			
User Name	Privilege Level		
admin	15		

Add New User

(2) <Add Ner User>ボタンをクリックすると、以下の画面が表示れます。

Add User

User Settings				
User Name				
Password				
Password (again)				
Privilege Level	1 ~			

Save Reset Cancel

それぞれ設定したいレベルに応じて、ユーザ名、パスワード、優先レベル(1~15)を割り当ててください。

2. Privilege Level (ユーザの優先レベルについて)

- (1) ユーザのアクセスレベルの設定を行うには、「Configuration」->「Security」->「Switch」->「Privilege Levels」をクリックすると、以下の画面が表示されます。
 - 【注記】:本機能は、WEB専用機能となります。そのため、本機能はCLIでは動作しません。

Privilege Level Configuration

		Levels		
Group Name	Configuration	Configuration/Execute	Status/Statistics	Status/Statistics
	Read-only	Read/write	Read-only	Read/write
Aggregation	5 🗸	10 🗸	5 🗸	10 🗸
DHCP	5 🗸	10 🗸	5 🗸	10 🗸
Dhcp_Client	5 🗸	10 🗸	5 🗸	10 🗸
Diagnostics	5 🗸	10 🗸	5 🗸	10 🗸
Fan_Control	5 🗸	10 🗸	5 🗸	10 🗸
Green_Ethernet	5 🗸	10 🗸	5 🗸	10 🗸
IP2	5 🗸	10 🗸	5 🗸	10 🗸
IPMC_Snooping	5 🗸	10 🗸	5 🗸	10 🗸
LACP	5 🗸	10 🗸	5 🗸	10 🗸
LLDP	5 🗸	10 🗸	5 🗸	10 🗸
Loop_Protect	5 🗸	10 🗸	5 🗸	10 🗸
MAC_Table	5 🗸	10 🗸	5 🗸	10 🗸
Maintenance	15 🗸	15 🗸	15 🗸	15 🗸
Mirroring	5 🗸	10 🗸	5 🗸	10 🗸

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

3. Auth Method (認証方式の設定)

ここでは、認証方式の設定(Console、Telnet、SSH、Http インタフェース)を行います。

- この機能により、管理クライアントインタフェースを介してスイッチへログインする際のユーザ認証が可能になります。
- console:コンソールの端末回線
- ・ telnet:リモートコンソールアクセス(Telnet)用の仮想端末
- ・ ssh:セキュリティで保護されたリモートコンソールアクセス(SSH)用の仮想端末
- ・ http:Web ブラウザと Web サーバの間で HTML などのコンテンツの送受信用の通信プロトコルを使用した仮想端末
- 認証方式を設定するには、「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。

Authentication Method Configuration

Client	no	Meth	nods		
console	local	no	~	no	<
telnet	radius	no	\sim	no	\sim
ssh	tacacs	no	\sim	no	\sim
http	local 🗸	no	\sim	no	\sim

Save Reset

4. SSH

この機能により、SSHのセキュリティ機能を有効/無効に設定します。.

 SSHの設定を行うには、「Configuration」->「Security」->「Switch」->「SSH」をクリックすると、 以下の画面が表示されます。



(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

5. HTTPS の設定

この機能により、HTTPSのセキュリティ機能を有効/無効に設定します。.

 HTTPSの設定を行うには、「Configuration」->「Security」->「Switch」->「HTTPS」をクリックすると、 以下の画面が表示されます。

HTTPS Configuration

Mode	Disabled	<
Automatic Redirect	Disabled	\sim
Certificate Maintain	None	\sim
Certificate Status	Switch secure HTTP certificate is preser	nted

Save Reset

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

6. Access Management (管理アクセスの制限)

ここでは、管理ソースインタフェースのアクセス制限を行います。

 アクセス管理の設定を行うには、「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。

Access Management Configuration

Mode Disabled Enabled	Ρ				
Delete VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Add New Entry					
Save Reset					

7. SNMP

SNMP は、「Simple Network Management Protocol」の略であり、ネットワーク管理の TCP/IP の一部です。 SNMP より、多様なネットワークオブジェクトのネットワーク管理構造への参入が可能になります。 ネットワーク管理システムは、SNMP を実装しているネットワーク機器からのトラップ、または変更通知を受信することに より、ネットワークの問題を学習することが可能になります。

1) System(システムの設定)

システム設定のメニューを設定するには、「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。

SNMP System Configuration

Mode	SNMP v1
Version	SNMP v2c
Read Community	SNMP v3
Write Community	private
Engine ID	800007e5017f000001

Save Reset

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2) Trap (トラップ設定)

 トラップを設定するには、「Configuration」->「Security」->「Switch」->「SNMP」->「Trap」をクリック すると、以下の画面が表示されます。

Trap Configuration

Global Settings

Mode	Disabled					
	Enabled	ſ				
Trap Destination Configurations						

Delete Name Enable Version Destination Address Destination Port

Add New Entry

Save Reset

(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されます。

SNMP Trap Configuration

Trap Config Name		
Trap Mode	Disabled	~
Trap Version	SNMP v2c	~
Trap Community	Public	
Trap Destination Address		
Trap Destination Port	162	
Trap Inform Mode	Disabled	~
Trap Inform Timeout (seconds)	3	
Trap Inform Retry Times	5	
Trap Probe Security Engine ID	Enabled	\sim
Trap Security Engine ID		
Trap Security Name	None	\sim

SNMP Trap Event for Switch 1

System	□ * □ Warm Start	Cold Start
Interface	Link up ● none ○ specific ○ all switches □*Link down ● none ○ specific ○ all switches LLDP ● none ○ specific ○ all switches	
AAA	* Authentication Fail	
Switch	□ * □ STP	

Save Reset

(3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

3) Communities (SNMPv3 コミュニティ設定)

SNMPv3 アクセス情報を設定するには、「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 Community Configuration

Delete	Community	Source IP	Source Mask		
	public	0.0.0.0	0.0.0.0		
	private	0.0.00	0.0.0.0		
Add New Entry Save Reset					

4) User (SNMPv3 ユーザ設定)

 SNMPv3ユーザ情報を設定するには、「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 Nev	v Entry Save F	Reset					

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

5) Groups (SNMPv3 グループの設定)

SNMPv3 アクセス情報を設定するには、「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

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

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
Delete	v1 🗸	public 🗸	

Add New Entry

Save Reset

6) Views (SNMPv3 ビューの設定)

 (1) SNMPv3ビュー情報を設定するには、「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 I	Name	Vie	ew Type	OID Subtree
	defaul	t_view	inc	luded	.1
			exc	cluded	_
Add Nev	v Entry	Sa	ve	Reset	

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

7) Access (SNMPv3 アクセス設定)

(1) SNMPv3 アクセス設定情報を行うには、「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 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
	default_ro_group	any	NoAuth, NoPriv	default_view 🗸	None 🗸
	default_rw_group	any	NoAuth, NoPriv	default_view 🗸	default_view 🗸
Add Nev	v Entry Save	Reset			

8. RMON

RMON (Remote Network Monitor)により、ネットワーク管理者は、中央(管理センター)から接続先の LAN 側の通信 情報のモニタリング、解析、およびトラブルシューティングを行うための通信情報を入手することができます。また、ネット ワークモニタリングシステムにより提供可能な情報を定義します。RMON は、デバイス("probes"ともいう)をモニタリング することによりサポートします。

例えば、LAN スイッチには、MIB を介してトラフィックフローとして情報をトラップ可能なソフトウェアが含まれ、その MIB に 記録されます。ソフトウェアエージェントは情報を収集し、グラフィカルユーザインタフェースを介しその情報をネットワーク 管理者に提供することが可能です。

1) Statistics (RMON 統計情報の設定)

ここでは、RMON 統計情報のエントリの追加/削除を行うことができます。

 RMON 統計情報を設定するには、「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 Statistics Configuration

Delete ID	Data		
Add New Entr	У	Save	Reset

(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されるため、新規の ID を設定してください。

RMON Statistics Configuration

Delete	ID	Data Source			
Delete		.1.3.6.1.2.1.2.2.1.1. 0			
Add New	Entry S	ave Reset			

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2) History (RMON の履歴の設定)

ここでは、RMON 履歴のエントリの追加/削除を行うことができます。

 「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 History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Add Nev	v Ent	Save	Reset		

(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されるため、新規の ID を設定してください。

RMON History Configuration

Delete	ID	Data Source		Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1.	0	1800	50	
Add New I	Entry S	ave Reset				

(3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

3) Alarm (アラームの設定)

ここでは、RMON アラームのエントリの追加/削除を行うことができます。

 アラーム設定を行うには、「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 Alarm Configuration

Delete	ID	Inte	rval	Va	riable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Add Nev	v Ent	ry	Sav	/e	Reset							

(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されるため、新規の ID を設定してください。

RMON Alarm Configuration											
Delete	ID		Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete			30	.1.3.6.1.2.1.2.2.1. 0.0	Delta 🗸	0	RisingOrFalling ∨	0	0	0	0
Add New	Entry	Save	Reset								

(3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

4) Event (イベントの設定)

ここでは、RMON イベントのエントリの追加/削除を行うことができます。

 (1)「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 Event Configuration

Delete	ID	Desc	Туре	Community	Event Last Time
Add Nev	v Enti	У	Save	Reset	

(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されるため、新規の ID を設定してください。

RMON Ev	ent Config	guration			
Delete	ID	Desc	Туре	Community	Event Last Time
Delete			none 🗸	public	0
Add New I	Entry S	Save Reset			

2.4.4.2 Network(ネットワーク管理のセキュリティ)

ここでは、ネットワーク管理上のセキュリティ機能について説明します。

1. Limit Control (リミットコントロールの設定)

Disabled V

6

リミットコントロール機能により、指定したポートのユーザ数の制限を行うことができます。MAC アドレスおよび VLAN ID により、ユーザを識別します。リミットコントロールを有効にすると、ポートのユーザによるアクセス数の上限を設定可能です。その上限を超えると、一定の処理が実行されます。

リミットコントロール機能を設定するには、「Configuration」 -> 「Security」 -> 「Network」 -> 「Limit Control」をクリックすると、以下の画面が表示されます。

ort Security Limit Control Configuration											
ystem	n Configu	ratio	n								
Mode Aging Aging	Enabled Period	Disa	abled 0 see	✓ conds							
Port Configuration for Switch 1											
Port	Mode		Limit	Actio	on	State	Re-open				
Port *	Mode	~	Limit 4	Actio	on V	State	Re-open				
Port * 1	Mode <> Disabled	>	Limit 4	Actio	on V	State Disabled	Re-open Reopen				
Port * 1 2	Mode <> Disabled Disabled	> >	Limit 4 4	Actional Act	on V V V V V	State Disabled Disabled	Re-open Reopen Reopen				
Port * 1 2 3	Mode <> Disabled Disabled Disabled	> $>$ $>$ $>$	Limit 4 4 4	Actional Act	on V V V V V V V V	State Disabled Disabled Disabled	Reopen Reopen Reopen Reopen				
* 1 2 3 4	Mode <> Disabled Disabled Disabled Disabled	$\mathbf{>}\mathbf{>}\mathbf{>}\mathbf{>}\mathbf{>}\mathbf{>}\mathbf{>}\mathbf{>}\mathbf{>}\mathbf{>}$	Limit 4 4 4 4 4	Actio	on > > > > > >	State Disabled Disabled Disabled Disabled	Reopen Reopen Reopen Reopen Reopen				

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

Disabled

Reopen

 \sim

None

4

2. NAS (802.1x ネットワークアクセスの設定)

IEEE 802.1X 規格では、ポートベースのアクセスコントロールの手順を定義しており、ユーザに認証用の許可書を提出 させることにより、ネットワークへの不正なアクセスを防止します。1つ以上の中央サーバ、バックエンドサーバ(RADIUS) によって、ネットワークへのアクセスが許可されたユーザかどうかを判断します。これらの RADIUS(バックエンド)サーバの設 定は、「Configuration」→「Security」→「AAA」の手順で設定可能です。

IEEE802.1X 規格では、ポートベースのオペレーションを定義していますが、非標準変数は以下に検討すべくセキュリテ 上の制限事項があります。

MAC ベース認証により、同じポート上で複数のユーザの認証が可能となり、ユーザは個々のシステムに特殊な 802.1X サプリカントソフトウェアをインストールする必要はありません。

本機は、ユーザの MAC アドレスを使って、バックエンドサーバへの認証を行います。

侵入者による不正な MAC アドレスが使用される可能性があるため、MAC ベース認証は、802.1X 認証よりも セキュリティが低くなります。

 本機のネットワークアクセスサーバの設定を行うには、「Configuration」->「Security」->「Network」-> 「NAS」をクリックすると、以下の画面が表示されます。

Network Access Server Configuration

System Configuration

Mode	Disabled	~		
Reauthentication Enabled				
Reauthentication Period	3600	second	s	
EAPOL Timeout	30	second	S	
Aging Period	300	second	S	
Hold Time	10	second	S	
RADIUS-Assigned QoS Enabled				
RADIUS-Assigned VLAN Enabled				
Guest VLAN Enabled		_		
Guest VLAN ID	1			
Max. Reauth. Count	2]		
Allow Guest VLAN if EAPOL Seen				
Mac Auth Username Format	with-hyphe	n 🗸	Lower-case	~

Port Configuration for Switch 1

Port	Admin State	RADIUS- Assigned QoS Enabled	RADIUS- Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Resta	rt
*	◇ V						
1	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized 🗸				Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize

Refresh

3. ACL 設定

ACL は、「Access Control List(アクセスコントロールリスト)」の略です。これは、ACE のリストテーブルであり、このリスト テーブルには、アクセスコントロールのエントリが含まれ、プロセス、またはプログラムなどの特定のトラフィックのオブジェクト に許可/拒否された個々のユーザをそれぞれ指定します(ACE は、「Access Control Entry」の略であり、特定の ACE ID に関連付けられるアクセス許可について記述されています)。

ACE は、3つのフレームタイプ(イーサネットタイプ、ARP、IPv(4)と、2つの ACE アクション(許可/拒否)で構成されています。ACE には、個々のアプリケーションで利用可能な各パラメータのオプションの詳細が含まれています。

各アクセス可能なトラフィックオブジェクトには、その ACL の識別子が含まれます。優先レベルにより、特定オブジェクトのアクセス権の有無が判別されます。

ACLの実装は、それぞれの状況に応じてACEの優先付けを行うため、非常に複雑になる場合があります。ネットワークでは、ACLは、ホスト/サーバー上で有効なサービスポートのリスト、またはネットワークサービスを指し、それぞれサービスの使用を許可/拒否されたホスト/サーバのリストを保有しています。 ACLは、通常ファイアーオールと同様に受信トラフィックを制御するように設定されます。

ACL 設定に関連付けられる WEB 画面は以下の3つです。

1) Ports (ポート)

ACLポートの設定を用いて、入力ポートへポリシーIDの割り当てを行います。これは、同一のトラフィックルールに従うた めに、ポートをグループ化する際に有用です。トラフィックポリシーは、"Access Control List"に設定します。また各入 力それぞれのポートごとに特定のトラフィックの特性(Action/Rate Limiter /Port copy、その他)を設定することも可能 です。ACE マッチングと一致した場合にのみ適用されます。 この場合、そのポートに関連のある値が大きくなります。 詳細については、WEB 画面の「help 情報」を参照してください。

ポートのデフォルト設定

 「Configuration」->「Security」->「Network」->「ACL」->「Ports」をクリックすると、以下の画面が 表示されます。

ACL P	ACL Ports Configuration for Switch 1				Refres	h Clear		
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*	0	◇ ∨	◇ ∨	◇ ∨	◇ ∨	<> v	<> ∨	*
1	0	Permit 🗸	Disabled 🗸	Disabled V	Disabled V	Disabled V	Enabled V	4379300
2	0	Permit 🗸	Disabled 🗸	Disabled V	Disabled V	Disabled 🗸	Enabled V	0
3	0	Permit 🗸	Disabled 🗸	Disabled 🗸	Disabled 🗸	Disabled 🗸	Enabled 🗸	0
4	0	Permit 🗸	Disabled V	Disabled V	Disabled V	Disabled V	Enabled V	0
5	0	Permit 🗸	Disabled 🗸	Disabled V	Disabled 🗸	Disabled 🗸	Enabled V	0
6	0	Permit 🗸	Disabled 🗸	Disabled V	Disabled V	Disabled 🗸	Enabled V	0
7	0	Permit 🗸	Disabled 🗸	Disabled 🗸	Disabled 🗸	Disabled 🗸	Enabled 🗸	0
8	0	Permit 🗸	Disabled V	Disabled V	Disabled V	Disabled V	Enabled V	0
9	0	Permit 🗸	Disabled V	Disabled V	Disabled V	Disabled V	Enabled V	0
10	0	Permit 🗸	Disabled 🗸	Disabled 🗸	Disabled 🗸	Disabled 🗸	Enabled V	0
11	0	Permit 🗸	Disabled 🗸	Disabled 🗸	Disabled 🗸	Disabled 🗸	Enabled 🗸	0
12	0	Permit 🗸	Disabled 🗸	Disabled V	Disabled V	Disabled V	Enabled V	0
13	0	Permit 🗸	Disabled 🗸	Disabled V	Disabled V	Disabled V	Enabled V	0
14	0	Permit 🗸	Disabled 🗸	Disabled 🗸	Disabled V	Disabled 🗸	Enabled V	0

2) Rate Limiters(レートリミッター)

ここでは、レートリミッタ—を設定することが可能です。レートリミッターは 15 段階に分かれています(毎秒 1-1024 パケット/毎秒)。"Ports"および"Access Control List"メニューの ACE または入力ポートにレートリミッタ ID を割り当てることができます。

レートリミットの設定:

 「Configuration」->「Security」->「Network」->「ACL」->「Rate Limiters」をクリックすると、以下の 画面が表示されます。

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1
Save Reset	

3) Access Control List (アクセスコントロールリスト)

ここでは、ACEの優先付けの方法(最上位から最下位まで)を示しています。

デフォルトでは、このテーブルは空欄です。入力フレームは ACE と一致する複数の ACE が存在した場合でも、その中からACEを 1 つのみ取得します。ACE に一致すると、フレームに対してアクション(許可/拒否)を行い、その ACE に関連のある値が増えます。

ACE ポリシーが設定されると、ポリシー、入力ポートのいずれか、あるいは任意の入力ポート(スイッチ全体)関連付けが可能です。

ACEポリシーが設定されると、WEB画面の"Ports"のポートのグループと関連付けが可能です。ACEで設定可能なパ ラメーターはたくさんあります。詳細については、WEB画面の「help 情報」を参照してください。 ACE の上限は「64」です。

ACL エントリ設定:

 ACLを設定するには、「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。

Access Control List Configuration				to-refresh	Refresh	Clear	Remove All	
ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Counter	
								Ð

(2) "(+)"をクリックすると、以下の画面が表示されます。

ACE Configuration

Ingress Port	All	~
Policy Filter	Any	~
Frame Type	Any	~

Action	Permit 🗸
Rate Limiter	Disabled 🗸
Logging	Disabled 🗸
Shutdown	Disabled 🗸
Counter	0



Save	Reset	Cancel
------	-------	--------

VI AN	Parameters
	i alameters

VLAN ID Filter	Any	<
Tag Priority	Any	~

2.4.4.3 IP Source Guard (IP ソースガード)

IP ソースガードは、DHCP スヌーピングテーブルに応じて、トラフィックのフィルタリングを行なったり、IP ソースブリッジを手動でバインドすることにより、DHCP スヌーピングのアントラストポートの IP トラフィックを制限することができます。 これにより、別のホストによる IP アドレスが不正に使用されることから防ぐことができます。

1. Configuration (IP ソースガードの設定)

(1) 有効/無効の設定、ダイナミッククライアント数を設定するには、「Configuration」->「Security」->
 「Network」->「IP Source Guard」->「Configuration」をクリックすると、以下の画面が表示されます。

IP Source Guard Configuration

Mode	Disabled			
	Enabled			
Translate dynamic to static				

Port Mode Configuration for Switch 1

Port	Mode	Max Dynamic Clients
*	 V 	◇ ∨
1	Disabled \checkmark	Unlimited 🗸
2	Disabled 🗸	Unlimited 🗸
3	Disabled \checkmark	Unlimited 🗸
4	Disabled 🗸	Unlimited 🗸
5	Disabled \checkmark	Unlimited 🗸
6	Disabled 🗸	Unlimited 🗸
7	Disabled \checkmark	Unlimited 🗸
8	Disabled \checkmark	Unlimited 🗸
9	Disabled \checkmark	Unlimited 🗸
10	Disabled 🗸	Unlimited 🗸

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2. Static Table (スタティック IP ソースガードテーブルの設定)

(1)「Configuration」->「Security」->「Network」->「IP Source Guard」->「Static Table」をクリックすると、
 以下の画面が表示されます。



(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されるため、新規の ID を設定してください。

Static IP Source Guard Table for Switch 1

Delete	Port	VLAN ID	IP Address	IP Mask
Delete	1 🗸			
Add New	Entry			
Save	Reset			

(3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.4.4.4 ARP Inspection (ARP インスペクション)

ここでは、ARP インスペクション機能の設定を行います。ARP インスペクションは、セキュリティのための機能です。ARP キャッシュをポイズニングすることによって、レイヤ 2 ネットワークに接続されているホスト、またはデバイスが攻撃を受けた場合それらの攻撃をブロックします。有効な ARP リクエストとその応答のみ通過することが可能です。

1. Port Configuration(ポートの設定を有効/無効にする)

 「Configuration」->「Security」->「Network」->「ARP Inspection」->「Port Configuration」を クリックすると、以下の画面が表示されます。

ARP Inspection Configuration

Mode Disabled V

Translate dynamic to static

Port Mode Configuration for Switch 1

Port	Mode	Check VLAN	Log Type
*	~ v	◇ ∨	0
1	Disabled 🗸	Disabled 🗸	None
2	Disabled 🗸	Disabled 🗸	Permit
3	Disabled 🗸	Disabled 🗸	All
4	Disabled 🗸	Disabled 🗸	None 🗸
5	Disabled 🗸	Disabled 🗸	None 🗸
6	Disabled 🗸	Disabled 🗸	None 🗸
7	Disabled 🗸	Disabled 🗸	None 🗸
8	Disabled 🗸	Disabled 🗸	None 🗸
9	Disabled 🗸	Disabled 🗸	None 🗸
10	Disabled 🗸	Disabled 🗸	None 🗸
11	Disabled 🗸	Disabled 🗸	None 🗸

2. VLAN Configuration(VLAN 設定)

 「Configuration」->「Security」->「Network」->「ARP Inspection」->「VLAN Configuration」を クリックすると、以下の画面が表示されます。

VLAN Mode Configuration	Refresh << >>	
Start from VLAN 1 with 20	entries per page.	
Delete VLAN ID Log Type		
Add New Entry		
Save Reset		

(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されるため、新規の ID を設定してください。

VLAN Mode Configu	ration	Refresh << >>
Start from VLAN 1	with 20	entries per page.
Delete VLAN ID	Log Type	
Delete	None	
Add New Entry	Permit All	
Save Reset		

(3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

3. Static Table (スタティック ARP インスペクションのエントリを指定する)

 「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。

Static ARP Inspection Table for Switch 1

Delete Port VLAN ID MAC Address IP Address

Add New Entry

Save Reset

(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されるため、新規の ID を設定してください。

Static ARP Inspection Table for Switch 1

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1 🗸			
Add New	Entry			

Save Reset

(3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

4. Dynamic Table (ダイナミック ARP インスペクションテーブルを表示する)

 「Configuration」->「Security」->「Network」->「ARP Inspection」->「Dynamic Table」をクリック すると、以下の画面が表示されます。

Dynamic ARP Ir	spection Table	for Switch 1	Auto-refresh 🗌 🛛	tefresh << >>
Start from Port 1	, VLAN 1	, MAC address	00-00-00-00-00	and IP address
0.0.0.0	with 20 entri	es per page.		
Port VLAN ID	MAC Address	IP Address	Translate to static	1
	No more	e entries		

2.4.4.5 AAA(AAA サーバのセキュリティ)

ここでは、AAA の設定を行います。

1. RADIUS (RADIUS サーバの設定)

RADIUS は、「Remote Authentication Dial In User Service」の略です。 このネットワークプロトコルにより、ユーザが個々にコンピュータを接続したり、ネットワークサービスを介して集 中アクセス、認証、アカウント管理を行うことが可能です。 RADIUS サーバは、これらのサービスを提供するサーバです。

 RADIUS サーバの設定を行うには、「Configuration」 -> 「Security」 -> 「AAA」 -> 「RADIUS」をクリッ クすると、以下の画面が表示されます。

RADIUS Server Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NA S-Identifier		

Global Configuration

Server Configuration

Delete Hostname Auth Port Acct Port Timeout Retransmit Key

Add New Server

(2) <Add New Server>ボタンをクリックすると、次の画面が表示されるため、それぞれ値を入力してください。

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NA S-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete		1812	1813			
Add New	/ Server					
Save	Reset					

FXC5428

2. TACACS+(TACACS+サーバの設定)

TACACS+は、「Terminal Acess Controller Access Control System Plus」の略です。 このプロトコルは、ルーター、ネットワークアクセスサーバ、1つ以上の集中型サーバを介して他のネットワークコンピュータ 装置のアクセス制御を行うネットワークプロトコルです。 TACACS+サーバにより、認証、許可、アカウントサービスを個々に行うことが可能です。

「Configuration」->「Security」->「AAA」->「TACACS+」をクリックすると、以下の画面が表示されます。

TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

Server Configuration

|--|

Add Ne	ew Server
Save	Reset

(2) <Add New Server>ボタンをクリックすると、次の画面が表示されるため、それぞれ値を入力してください。

TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

Server Configuration

Delete	Hostname	Port	Timeout	Key
Delete		49		
Add New	Server			

Save Reset

2.4.5 Aggregation (アグリゲーション)

ポートアグリゲーション(Link Aggregation)は、複数ポートを束ねて用いることにより、ポートの制限を超えてリンク速度を向上させ、可用性のより高い冗長性の高めます。

2.4.5.1 Static (スタティック設定)

ここでは、アグリゲーション機能を固定で設定することができます。

(1) 「Configuration」->「Aggregation」->「Static」をクリックすると、以下の画面が表示されます。

Aggregation Mode Configuration

 Hash Code Contributors

 Source MAC Address
 Image: Contributors

 Destination MAC Address
 Image: Contributors

 IP Address
 Image: Contributors

 TCP/UDP Port Number
 Image: Contributors

Aggregation Group Configuration for Switch 1

												- F	Port	t Me	emt	pers	5											
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Normal	\odot	\odot	۲	۲	۲	۲	۲	۲	۲	۲	\odot	۲	۲	۲	\odot	۲	\odot	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
1	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc
2	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	$^{\circ}$
3	$^{\circ}$	$^{\circ}$	0	$^{\circ}$	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc
4	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	$^{\circ}$																
5	$^{\circ}$	$^{\circ}$	0	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	0	\bigcirc
6	Ο	\bigcirc	Ο	\bigcirc	Ο	\bigcirc	0	\bigcirc	0	0																		
7	$^{\circ}$	$^{\circ}$	$^{\circ}$	0	$^{\circ}$	0	0	\bigcirc	Ο	0	$^{\circ}$	0	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	0	$^{\circ}$	0	\bigcirc	0	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	0	$^{\circ}$
8	\bigcirc	Ο	Ο	Ο	\bigcirc	\bigcirc	Ο	\bigcirc	Ο	\bigcirc	\bigcirc	\bigcirc	Ο	0	\bigcirc	Ο	0											
9	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	$^{\circ}$	\bigcirc	\bigcirc	\bigcirc	\bigcirc	$^{\circ}$	\bigcirc	$^{\circ}$	$^{\circ}$	$^{\circ}$	\bigcirc	$^{\circ}$	0	$^{\circ}$	0	\bigcirc	\bigcirc	$^{\circ}$	$^{\circ}$	0	\bigcirc	0	\bigcirc
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

「Aggregation Hash」モードでは、「Hash Code Contributors」のメニューの中から選択して、フレームの 宛先ポートを算出します。アグリゲーショングループは、最大8ポートまで固定設定が可能です。 「Aggregation Mode Configuration」のメニューの中から、お使いのユーザ環境に合わせてポートの設定を 行ってください

2.4.5.2 LACP

LACP とは、複数の物理的なポートを束ねてひとつの論理的チャネルとして扱うためのプロトコルのことです。IETF による標準規格のひとつである IEEE 802.3ad の中で規定されています。

 LACP の設定を行うには、「Configuration」 -> 「Aggregation」 -> 「LACP」をクリックすると、以下の画面が 表示されます。

Port	LACP Enabled	Ke	ey 🛛	Role	•
*		<> ∨		\sim	\sim
1		Auto 🗸		Active	\sim
2		Auto 🗸		Active	\sim
3		Auto 🗸		Active	\sim
4		Auto 🗸		Active	\checkmark
5		Auto 🗸		Active	\sim
6		Auto 🗸		Active	\checkmark
7		Auto 🗸		Active	\sim
8		Auto 🗸		Active	\checkmark

LACP Port Configuration for Switch 1

2.4.6 Loop Protection (ループプロテクション)

ここでは、ループプロテクション機能の設定方法について説明します。

ループが発生すると、パケットストームが生成されることにより、ネットワーク障害が引き起こされる可能性があります。 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。

ループプロテクションを有効にすると、Tx(送信)モードが有効になっている場合、ポートはループプロテクションの PDU を 設定します。ループバックを検出すると、ポートはシャットダウンされるか、またはその情報を記録します。 シャットダウン時間は、一定の間隔で設定可能です。

(1) ループプロテクションの設定を行うには、「Configuration」->「Loop Protection」をクリックすると、 以下の画面が表示されます。

Loop Protection Configuration

General Settings								
Global Configuration								
Enable Loop Protection	Disable 🗸							
Transmission Time	5	seconds						
Shutdown Time	180	seconds						
Shutdown Time	180	seconds						

Port Configuration for Switch 1									
Port	Enable	Action	Tx Mo	de					
*	\checkmark	\diamond	~	<>	\mathbf{v}				
1	\checkmark	Shutdown Port	~	Enable	~				
2	\checkmark	Shutdown Port	~	Enable	~				
3	\checkmark	Shutdown Port	~	Enable	~				
4	\checkmark	Shutdown Port	~	Enable	~				
5	\checkmark	Shutdown Port	~	Enable	~				
6	\checkmark	Shutdown Port	~	Enable	~				
7	\checkmark	Shutdown Port	~	Enable	~				
8	~	Shutdown Port	~	Enable	~				

2.4.7 Spanning Tree (スパニングツリー)

スパニングツリーは、ネットワークトポロジ内のネットワークのループを防止するためのプロトコルです。

ネットワークのループが発生すると、トラフィックが多くなればなるほど、ネットワークのループによりネットワークが不安定に なります。そのため、ネットワークのループが生じると、スパニングツリープロトコルにより、ループした接続を自動的にブロッ クします。ネットワークトロポジ—の検出によりネットワーク接続が変更されると、遅延(STPの場合は「30秒」、RSTP の場合は「30秒以下」)が生じます。

本機では、MSTP/RSTP/STP 機能をサポートしているため、ここでは、スパニングツリーの設定方法について説明します。

2.4.7.1 Bridge Setting (STP ブリッジの設定方法)

ここでは、スパニングツリーのブリッジについての設定方法について説明します。

 STP ブリッジの設定を行うには、「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。

S	TP Bridge Configura	ition
Ч	Basic Settings	
	Protocol Version	MSTP V
	Bridge Priority	32768 🗸
	Forward Delay	15
	Max Age	20
	Maximum Hop Count	20
	Transmit Hold Count	6
	Advanced Settings	
	Edge Port BPDU Filteri	ing
	Edge Port BPDU Guard	
	Port Error Recovery	
	Port Error Recovery Ti	meout
L		
	Save Reset	

2.4.7.2 MSTI Mapping

ここでは、MSTIマッピングの設定を行います。

 MSTIマッピング設定を行うには、「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。

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configurat	ion Identification	
Configure Configure	ation Name00-17-2e-1b-b8-00ation Revision0	
MSTI Map	ping	
MSTI	VLANs Mapped	
MSTI1		$\langle \rangle$
MSTI2		\sim
MSTI3		$\langle \rangle$
MSTI4		\bigcirc
MSTI5		$\langle \rangle$
MSTI6		$\widehat{}$
MSTI7		\sim

Save Reset

ID は、VLAN から MSTI のマッピングを識別するために名前とリビジョンで構成されます。 ブリッジは、名前とリビジョンを共有し、同様に複数の MSTI 内のスパニングツリーの VLAN-to-MSTI mapping 設定を共有する必要があります。

2.4.7.3 MSTI Priorities

ここでは、MSTI プライオリティの設定を行います。

 MSTI プライオリティの設定を行うには、「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。

MSTI Configuration

MSTI Pri	iority Config	guration
MSTI	Priority	<u>/</u>
*	< V	I
CIST	32768 🗸	-
MSTI1	32768 🗸	1
MSTI2	32768 🗸	7
MSTI3	32768 🗸	1
MSTI4	32768 ¥	1
MSTI5	32768 V	
W3115	J2100 ¥	4
MSTI6	32768 🗸	<
MSTI7	32768 🗸	<u> </u>

Save Reset

ここでは、MSTI プライオリティを設定します。値が低い方が、プライオリティが高くなります。 ブリッジのプライオリティと MST インスタンス番号は、6 バイトの MAC アドレスで連結され、ブリッジの識別子を 構成します。

2.4.7.4 CIST Port (CIST ポート)

ここでは、CIST ポートの設定を行うことができます。

(1) 「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。

CIST A	agregated Do	t Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role TCN	BPDU Guard	Point-to- point				
-		Auto 🗸	128 🗸	Non-Edge 🗸	V			Forced True 🗸				
CIST Normal Port Configuration for Switch 1												
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role TCN	BPDU Guard	Point-to- point				
*		 V 	 V 		V			<> V				
1		Auto 🗸	128 🗸	Non-Edge 🗸	\checkmark			Auto 🗸				
2		Auto 🗸	128 🗸	Non-Edge 🗸	\checkmark			Auto 🗸				
3		Auto 🗸	128 🗸	Non-Edge 🗸	\checkmark			Auto 🗸				
4		Auto 🗸	128 🗸	Non-Edge 🗸	\checkmark			Auto 🗸				
5		Auto 🗸	128 🗸	Non-Edge 🗸	\checkmark			Auto 🗸				
6		Auto 🗸	128 🗸	Non-Edge 🗸	\checkmark			Auto 🗸				
7		Auto 🗸	128 🗸	Non-Edge 🗸	\checkmark			Auto 🗸				

STP CIST Port Configuration
2.4.7.5 MSTI Port (MSTI ポートの設定)

ここでは、MSTI ポートの設定を行います。

 MSTI ポートの設定を表示するには、「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 Port Configuration

Select MSTI	
MST1 V	Set

(2)「MSTI」を選択して、<Get>ボタンをクリックすると、MSTIのポート設定画面が表示されます。

MSTI Aggregated Ports Configuration (Stack Glob					
Port		Path	Cost	Prio	rity
-	Auto	~		128	<
MSTI N	ormal Por	rts Con	figuration for Sv	vitch 2	
Port		Path	Cost	Prio	rity
*	\diamond	~		\diamond	~
1	Auto	~		128	✓
2	Auto	\checkmark		128	~
3	Auto	~		128	✓
4	Auto	~		128	<
5	Auto	~		128	~

MST1 MSTI Port Configuration

2.4.8 IPMC Profile (IPマルチキャストのプロファイル)

IP マルチキャストとは、特定の複数の受信者に対して一回で IP データを送信するための方式です。 インターネットおよびプライベートネットワーク上ではストリーミング・メディアアプリケーションが多く採用されます。

2.4.8.1 Profile Table (プロファイルテーブル)

IPMC プロファイルは、「IP MultiCast Profile」の略です。 IPMC プロファイルは、IP マルチキャストストリーム上のアクセスコントロールに使用されます。

 プロファイルテーブルの設定を行うには、「Configuration」 -> 「IPMC Profile」 -> 「Profile Table」を クリックすると、以下の画面が表示されます。

IPMC Profile Configurations

Global Profile Mode	Disabled	Π
	Enabled	Г

IPMC Profile Table Setting

Delete Profile Name Profile Description Rule

Add New IPMC Profile

Save Reset

- (2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。
- (3) プロファイル名とその記述を設定して、"Rule"をチェックします。 <Add New IPMC Profile>ボタンをクリックすると、 次の画面が表示されるので、新しいエントリを追加してください(エントリの設定方法については、 "「Configuration」 -> 「IPMC Profile」 -> 「Address Entry」"を参照してください)。

IPMC Profile Configurations

IPMC Profile Global Setting

Global Profile Mode Disabled V

IPMC Profile Table Setting



2.4.8.2 Address Entry (アドレスのエントリ)

 アドレスのエントリ設定を行うには、「Configuration」 -> 「IPMC Profile」 -> 「Address Entry」をクリックすると、 以下の画面が表示されます。

IPMC Profile Address Configuration	Refresh	<<	>>
Navigate Address Entry Setting in IPMC Profile by 20 entries per page.			
Delete Entry Name Start Address End Address			
Add New Address (Range) Entry			
Save Reset			

2.4.9 MVR (マルチキャストVLANレジストレーション)

MVR 機能により、マルチキャスト VLAN 上でマルチキャストトラフィックの送信を可能にします。 マルチキャストテレビアプリケーションでは、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、あるいは PC を1つの加入者ポート(MVR 受信側ポートと して設定されているポート)に接続可能です。加入者はチャンネルを選択すると、セットトップボックス、あるいは PC は 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設定します。 マルチキャスト VLAN に対するマルチキャストデータの送受信先のアップリンクポートは"MVR 送信元ポート"と言います。 これにより、各マルチキャスト VLAN ごとに対応するチャンネルのプロファイルをもつ MVR を最大 4 つまで設定可能で す。チャンネルのプロファイルは、フィルタリング条件をもつ IPMC プロファイルによって定義されます。

ここでは、MVR機能の設定を行います。MVR機能により、マルチキャストトラフィックをマルチキャスト VLAN に伝送を 行うことが可能になります。

(1) MVR の設定を行うには、「Configuration」 -> 「MVR」をクリックすると、以下の画面が表示されます。



VLAN Interface Setting for Switch 1 (Role [I:Inactive / S:Source / R:Receiver])

	Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
--	--------	------------	-------------	-----------------	------	---------	----------	------	---------------------------------

Add New MVR VLAN

Immediate Leave Setting for Switch 1

Port	Immedia	ite Leave
×	0	<
1	Disab	oled 🗸
2	Disab	oled 🗸
3	Disab	oled 🗸
4	Disab	oled 🗸
5	Disab	oled 🗸
6	Disab	oled 🗸
7	Disab	oled 🗸

MVR Con	figurations						
MVR Mod	e Disabled ✓						
VLAN Inte	erface Setting for	Switch 1 (Role [I:Ina	ctive / S:Source / R:I	Receiver])			
Delete	MVR VID	MVR Name	IGMP Address	Mode	ragging Priority	LLQI	Interface Channel Profile
Delete			0.0.0.0	Dynamic 🗸 Ta	igged ∨ 0	5 🐟 - 🗸	
Port	12345	6 7 8 9 10 11 12	13 14 15 16 17 18 1	19 20 21 22 23 24 2	25 26 27 28		
Role							
Add New	MVR VLAN						
Immediate	e Leave Setting f	for Switch 1					
Port In	mediate Leave						
•	◇						
1	Disabled V						
2	Disabled V						
3	Disabled V						
4	Disabled V						
0	Disabled V						
7	Disabled V						
8	Disabled V						
9	Disabled V						
-							

2.4.10 IPMC

ここでは、IGMP スヌーピングおよび MLD スヌーピング機能を設定します。

2.4.10.1 IGMP (IGMP スヌーピング)

IGMP とは、「Internet Group Management Protocol」の略です。

このプロトコルは、インターネットプロトコルマルチキャストグループのメンバーを管理する通信プロトコルです。 IGMPは、IPホストおよび近隣のマルチキャストルータにより使用され、マルチキャストグループのメンバーを設定します。 これは、ユニキャスト向けのICMPと同様に、IPマルチキャスト仕様上不可欠な部分です。IGMPは、オンラインビデオ およびゲームに使用され、リソースをより効率的に使用することができます。

IGMP スヌーピングは、IGMP ネットワークトラフィックを受信するための手順です。この機能により、ネットワークスイッチは、 ホスト/ルータ間の IGMP 通信を受信できるようになります。これらの通信を受信することにより、IP マルチキャストストリ ームに必要なリンクのマップを保持することが可能です。

リンクから不要なマルチキャストをフィルタリングすることにより、ポートで受信した特定のマルチキャストのトラフィックを制御することができます。

1. Basic Configuration (グローバルによる基本設定およびポート関連の設定)

 グローバルによる基本設定およびポート関連の設定を行うには、「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。

IGMP Snooping Configuration

Stack Global Settings

Global Configuration						
Snooping Enabled						
Unregistered IPMCv4 Flooding Enabled	\checkmark					
IGMP SSM Range	232.0.0.0 / 8					
Leave Proxy Enabled						
Proxy Enabled						

Port Related Configuration for Switch 2

Port	Router Port	Fast Leave	Throttling
*			<>
1			unlimited V
2			unlimited V
3			unlimited V
4			unlimited V
5			unlimited \checkmark

2. VLAN Configuration(IGMP スヌーピング VLAN 設定)

ここでは、IGMP スヌーピングの VLAN テーブルのメンテナンスを行います。

 IGMP スヌーピング VLAN 設定を行うには、「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。

IGMP Snooping VLAN Configuration Refresh << >>											
Start from	Start from VLAN 1 with 20 entries per page.										
Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Add Nev	Add New IGMP VLAN										
Save	Save Reset										
い下の	い下の機能をサポートしています										

以下の機能をサポートしています。

- 新規 IGMP VLAN の追加/設定/保存
- IGMP VLAN の編集
- IGMP VLAN の削除
- (2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

3. Port Filtering Profile (IGMP スヌーピングポートフィルタリングのプロファイル):

IGMP スヌーピングポートフィルタリングのプロファイルを設定するには、「Configuration」 -> 「IPMC」 -> 「IGMP Snooping」 -> 「Port Filtering Profile」をクリックすると、以下の画面が表示されます。

IGMP Snooping Port Filtering Profile Configuration for Switch 1



(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

【注記】: プロファイルを選択した後、" 🗢 "アイコンをクリックすると、プロファイルの内容が表示されます。

2.4.10.2 MLD Snooping (MLD スヌーピング)

MLDとは、IPv6 向けの「Multicast Listener Discovery」の略です。

このプロトコルは、IGMP が IPv4 で使用されるのと同じように、接続先のマルチキャストリスナーを検出するために、IPv6 ルータで使用されます。このプロトコルは、他のプロトコルを用いず、ICMPv6 に組み込まれています。

MLD スヌーピングにより、MLD パケットを受信し、その内容に応じて伝送を行います。

本機では、MLD、または MLD スヌーピングクエリアから MLD クエリを受信するサブネット内の MLD スヌーピングを使用 するように設定することが可能です。

MLD スヌーピングは、レイヤ2のLAN ポートを動的に設定することにより、レイヤ2のIPv6マルチキャストトラフィックを 抑制して、受信を要求するポートにのみIPv6マルチキャストトラフィックを伝送します。

1. Basic Configuration(グローバル基本設定およびポート関連の設定)

ここでは、MLD スヌーピング機能の基本設定を行います。

(1) グローバル基本設定およびポート関連の設定を行うには、「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。

MLD Snooping Configuration

Global Configuration						
Snooping Enabled						
Unregistered IPMCv6 Flooding Enabled	\checkmark					
MLD SSM Range	ff3e::	/ 96				
Leave Proxy Enabled						
Proxy Enabled						

Port Related Configuration for Switch 1

Port	Router Port	Fast Leave	Throttling
*			◇ ∨
1			unlimited \checkmark
2			unlimited 🗸
3			unlimited \checkmark
4			unlimited 🗸
5			unlimited 🗸
6			unlimited 🗸
7			unlimited 🗸
8			unlimited 🗸
9			unlimited \checkmark

2. VLAN Configuration(MLD スヌーピングの VLAN 設定)

 「Configuration」->「IPMC」->「MLD Snooping」->「VLAN Configuration」をクリックすると、 以下の画面が表示されます。

MLD Sn	MLD Snooping VLAN Configuration Refresh << >>												
Start from VLAN 1 with 20 entries per page.													
Delete	Delete VLAN Snooping Querier Election Compatibility PRI RV QI QRI LLQI URI (0.1 (0.1 (0.1 (sec) sec) sec) (sec) (sec) sec) (sec) (se												
Add Nev	Add New MLD VLAN												
Save	Save Reset												

以下の機能がサポートされています。 - 新規 MLD VLAN の追加/設定/保存

- MLD VLAN の編集
- MLD VLAN の削除
- (2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

3. Port Filtering Profile (MLD スヌーピングポートのフィルタリングプロファイル)

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。

MLD スヌーピングポートのフィルタリングプロファイルを設定するには、「Configuration」 -> 「IPMC」 -> 「MLD Snooping」 -> 「Port Filtering Profile」をクリックすると、以下の画面が表示されます。

MLD Snooping Port Filtering Profile Configuration for Switch 1

Port	Filtering Pr	rofile
1	٠	Ś
2	۰.	- 🗸
3	۰.	- ~
4	۰.	- ~
5	۰.	- ~
6	۰.	- ~
7	۰.	- 🗸
8	۰.	- 🗸
9	۰.	- 🗸
10	۰.	- ~
11	۰.	- 🗸
12	•	

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

【注記】: プロファイルを選択した後、" 🗢 "アイコンをクリックすると、プロファイルの内容が表示されます。

2.4.11 LLDP

LLDP とは、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。

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。

 ネイバー情報を設定するには、「Configuration」 ->「LLDP」 ->「LLDP」をクリックすると、以下の画面が 表示されます。

LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration for Switch 1

					Optional TLV:	8	
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	◇ ∨		V	✓		✓	×
1	Disabled 🗸		\mathbf{V}	\checkmark	\mathbf{v}	\checkmark	\checkmark
2	Disabled 🗸			\checkmark		\checkmark	✓
3	Disabled 🗸		\mathbf{V}	\checkmark	\mathbf{Y}	\checkmark	\checkmark
4	Disabled 🗸			\checkmark		\checkmark	✓
5	Disabled 🗸		\mathbf{V}	\checkmark	\mathbf{v}	\checkmark	V
6	Disabled 🗸			~	\checkmark	\checkmark	✓
7	Disabled 🗸		V	\checkmark	\mathbf{Y}	\checkmark	\checkmark
8	Disabled 🗸			\checkmark		\checkmark	\checkmark
-		_	_				_

表には、検出した LLDP ネイバー装置がポートごとに表示されます。

2.4.12 MAC Table (MACテーブル)

フレームの切り替えは、フレーム内の DMAC アドレスに応じて異なります。

スイッチは、フレームの送信先のポート情報(フレーム内の DMAC アドレスに基づいて)を認識して、MAC アドレスをポ ートにマッピングするためのテーブルを構成します。このテーブルには、スタティックおよびダイナミックエントリが含まれます。 スタティックエントリは、DMAC アドレスとポート間のマッピングを固定したい場合にネットワーク管理者により設定可能 です。

フレームには MAC アドレス(SMAC アドレス)が含まれ、この MAC アドレスは、フレームの送信元の機器の MAC ア ドレスです。 SMAC アドレスはスイッチ本体で用いられ、 MAC テーブルはダイナミック MAC アドレスにより自動的に更 新されます。

ダイナミックエントリは、対応する SMAC アドレスをもつフレームがエージングタイム後に表示されない場合は、MACテ ーブルから削除されます。

ここでは、ダイナミック MAC テーブル内のエントリのタイムアウトを設定し、スタティック MAC テーブルを設定します。

(1) MAC テーブルの設定を行うには、「Configuration」 -> 「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 Configuration

Aging Configuration

MAC Table Learning for Switch 1

		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	25	26	27	28
Auto	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
Disable	0	$^{\circ}$	$^{\circ}$	0	Ο	0	0	0	0	0	0	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	0	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	0	0	Ο	0	0	0	0	0
Secure	0	0	0	Ο	0	Ο	Ο	0	Ο	Ο	Ο	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	0	$^{\circ}$	$^{\circ}$	$^{\circ}$	$^{\circ}$	Ο	Ο	Ο	Ο	Ο	Ο	Ο	0

Static MAC Table Configuration for Switch 1

Port Members Delete VLAN ID MAC Address 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

Add New Static Entry

Save Reset

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。

2.4.13 VLAN

VLAN(仮想LAN)は、スイッチポート間の通信を制限する方法です。レイヤ2では、ネットワークは、複数の異なる分離したブロードキャストドメインに分かれています。

本機では、各 VLAN のアプリケーションに応じて、802.1Q VLAN、プライベート VLAN、MAC ベース VLAN、プロト コルベース VLAN、IP サブネットベース VLAN、および音声 VLAN をサポートしています。

2.4.13.1 802.1Q VLAN

IEEE 802.1Q は、イーサネットネットワーク上の仮想 LAN のサポートネットワーク規格(VLAN)です。

この規格では、フレームを処理するブリッジおよびスイッチで用いる手順、イーサネットフレームの VLAN タグ付けのシステムを定義します。

VLAN に対応しているネットワーク部分(すなわち、IEEE802.1Q 準拠)には、VLAN タグが含まれます。

ネットワーク上の VLAN に対応していないトラフィック(すなわち、IEEE802.1D 準拠)には VLAN タグは含まれません。 フレームがネットワークの VLAN 対応装置で受信されると、ポートベース、またはポート/プロトコルベース VLAN のクラス かどうかに応じてタグが付加され、フレームのポート、ポート/プロトコルを組み合わせたいずれかの VLAN メンバーが表 示されます。

各フレームは、VLANごとに区別されなければなければなりません。

ネットワーク VLAN に対応したフレーム(VLAN タグを含まない)は、ネイティブ VLAN(あるいはデフォルト VLAN)上で伝送されることを前提としています。

ここでは、ポートの 802.1Q VLAN および Q-in-Q 機能の設定を行います。

(1)「Configuration」->「VLANs」をクリックすると、以下の画面が表示されます。

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration for Switch 1

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
-	○ ∨	1	0	< <	◇ ∨	 	1	
1	Access 🗸	1	C-Port	\sim	Tagged and Untagged \vee	Untag Port VLAN 🗸	1	
2	Access ∨	1	C-Port	~	Tagged and Untagged \lor	Untag Port VLAN 🗸	1	
3	Access ∨	1	C-Port	\sim	Tagged and Untagged ∨	Untag Port VLAN 🗸	1	
4	Access ∨	1	C-Port	~ ~	Tagged and Untagged V	Untag Port VLAN V	1	
5	Access ∨	1	C-Port	\checkmark	Tagged and Untagged \checkmark	Untag Port VLAN 🗸	1	
6	Access ∨	1	C-Port	~	Tagged and Untagged ∨	Untag Port VLAN 🗸	1	
7	Access ∨	1	C-Port	\checkmark	Tagged and Untagged \lor	Untag Port VLAN 🗸	1	
8	Access ∨	1	C-Port	~	Tagged and Untagged ∨	Untag Port VLAN 🗸	1	
9	Access 🗸	1	C-Port	~	Tagged and Untagged \lor	Untag Port VLAN 🗸	1	
10	Access ∨	1	C-Port	× ×	Tagged and Untagged V	Untag Port VLAN 🗸	1	

(2)	画面右上の"?"アイコンをクリックすると、	、画面内の項目についての説明を記載したポップアップが表示され
	ます。	

ポートタイプ	
Unaware:	ポートは"Unaware"に設定されると、受信フレームは"タグなしフレーム"として 処理されます。受信フレームがタグ付きの場合でも、タグはペイロードとして処 理されます。フレームはポートベースVLANPVIDにクラス分けされます。これ は、802.1Qアクセス接続用、またはQ-in-Qダウンリンク接続用です。ポートベ ースVLANを使用する場合、同じPVIDの場合は「Unaware」に設定してくださ い。
C-port:	ポートがC-port,タグ付きフレームに設定されている場合は、タグ付きフレーム はフレームのタグに応じてVLANにクラス分けされます。これは、802.1Q VLAN トランクです。
S-port:	S-portに設定されている場合は、出力フレームのタグのTPIDは通常サービス VLANとして「0x88A8」です。これは、Q-in-Qアップリンク接続用です。
S-custom-port:	S-custom-portに設定されている場合は、出力フレームのタグのTPIDはサー ビスVLANとしてカスタマイズされます。
ポートVLAN	
None:	PVIDは無視されます。クラス分けされたVLAN IDをもつタグがポート上で送信 されたフレームに挿入されます。 このモードは、通常802.1Q VLANトランク接続としてVLAN認識スイッチに接 続されているポートに使用されます。このモードを使用時には、"Tx Tag"は 「Untag_pvid」に設定してください。
Specific:	ポートのVLAN IDを設定可能です。ポートで受信したタグなしフレームは、ポ ートのVLAN IDにクラス分けされます。VLANの認識ができない場合(ポートタ イプが非対応の場合)は、ポートで受信したフレームはすべてそのポートの VLAN IDにクラス分けされます。ポート上で送信されたフレーム内の"クラス分 けされたVLAN ID"が"ポートVLAN ID"と異なる場合は、"クラス分けされた VLAN ID"と"VLANタグ"がフレームに挿入されます。

"Tx_Tag"により、ポートからのフレームの送信時のタグ付け方法が設定されます。

1) 802.1Q VLAN 設定において、各ポートの設定は下記のとおりです。

Access: [Port Type]-"Unaware", [Port VLAN Mode]-"Specific(set PVID)", [Tx Tag]-"Untag_all" Trunk: [Port Type]-"C-port", [Port VLAN Mode]-"None", [Tx Tag]-"Untag_pvid" Hybrid: [Port Type]-"Unaware", [Port VLAN Mode]-"Specific(set PVID)", [Tx Tag]-"Untag_pvid"

 Q-in-Q 設定において、各ポートの設定は下記のとおりです。 Uplink: [Port Type]-"S-port"(あるいは、custom TPID をもつ"S-custom-port"), [Port VLAN Mode]-"None", [Tx Tag]-"Untag_pvid" Downlink: [Port Type]-"Unaware"、[Port VLAN Mode]-"Specific"(サービス VLAN ID を"PVID"に設定し ます。事前にサービス VLAN ID を作成し、その VLAN 内でのアップリンク/ダウンリンクポートの設定をしてくださ い。)、[Tx Tag]-"Untag_all"

2.4.14 Private VLAN(プライベートVLAN)

プライベート VLAN、PVLAN では、同一ブロードキャストドメインのポート間のレイヤ 2 の分割を行います。 PVLAN 部分として分割されたポートは相互に通信を行うことができません。PVLAN のメンバーポートは相互に通信 可能です。

2.4.14.1 Port Isolation (ポートアイソレーションの設定)

ここでは、ポートのアイソレーション機能を設定します。設定されたポートは、同じ VLAN 上でも互いに通信を行うことができなくなります。

(1) ポートアイソレーションの設定を行うには、「Configuration」 -> 「Private VLANs」 -> 「Port Isolation」を クリックすると、以下の画面が表示されます。

Port I	Port Isolation Configuration for Switch 1											Auto-refresh 🗌 Refresh						sh								
											Por	t N	um	ber												
1 2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Save		Res	et]																						

2.4.15 VCL

この章は、MAC ベース VLAN、プロトコルベース VLAN、IP サブネットベース VLAN より構成されます。

2.4.15.1 MAC-based VLAN (MAC ベース VLAN)

VLAN メンバーをグループ化する方法として、MAC アドレスベース VLAN (MAC-based VLAN) により、フレームの送信元 MAC アドレスに応じて、タグなしフレームの転送先の VLAN を決定します。

 MAC ベース VLAN を設定するには、「Configuration」 -> 「VCL」 -> 「MAC-based VLAN」をクリックすると、 以下の画面が表示されます。

MAC-b	ased VLAN Men	nbership C	Configuration for Switch 1	Auto-refresh 🗌 Refresh	<< >>
			Por	t Members	
Delete	MAC Address	VLAN ID	1 2 3 4 5 6 7 8 9 10 11 12 13 14 1	5 16 17 18 19 20 21 22 23 24 25 26 27 28	
			Currently no entries present		
Add Ne	ew Entry				
Save	Reset				

2.4.15.2 Protocol-based VLAN (プロトコルベース VLAN)

プロトコルベース VLAN メンバーに応じて、お使いのプロトコルにより接続先の PC は VLAN に割り当てられます。 例えば、IPX(Internetwork Packet Exchange)、または IP(Internet Protocol)は固有の VLAN に設定することが可能 です。

1. Protocol to Group (プロトコルのグループへのマッピングの設定/削除)

 プロトコルのグループへのマッピングの設定/削除を行うには、「Configuration」->「VCL」-> 「Protocol-based VLAN」->「Protocol to Group」をクリックすると、以下の画面が表示されます。

Protoco	I to Group Mappin	g Table	Auto-re	efresh 🗆	Refresh
Delete	Frame Type	Value	Group Name	e	
	No Group entry found!				
Add Nev	v Entry				
Save	Reset				

2. Group to VLAN (VLAN マッピンググループの設定/削除)

(1) VLAN マッピンググループの設定/削除を行うには、「Configuration」 -> 「VCL」 -> 「Protocol-based VLAN」
 -> 「Group to VLAN」をクリックすると、以下の画面が表示されます。

Group Name to VLAN mappin	g Table for Switch 1	Auto-refresh 🗌 Refresh
	Port Membe	rs
Delete Group Name VLAN I	D 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 1	8 19 20 21 22 23 24 25 26 27 28
	No Group entries	
Add New Entry		
Save Reset		

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.4.15.3 IP Subnet-based VLAN(IP サブネットベース VLAN)

IP サブネットベース VLAN では、IP サブネットのエンドワークステーションはすべて同じ VLAN に割り当てられます。 この VLAN では、ネットワークアドレスの再構成を行うことなく、ワークステーションを移行することができます。

IP サブネット VLAN は、パケットのヘッダのレイヤ 3 情報に応じて異なります。 VLAN メンバーを決定する上で、ネットワーク層アドレス(例えば、TCP/ IP ネットワークのサブネットアドレス)を使用しま す。パケットがタグなし/タグ付きの場合は、これに応じて一致する IP サブネットクラスにパケットを関連付けます。 IP サブネットのクラス分けが行われない場合は、スイッチの標準 VLAN クラス分けルールが適用されます。 この IP サブネット機能は、ルーティング機能でも、VLAN をルーティングするものでもありません。 IP サブネットのクラス分けの機能は、パケットの VLAN 設定時にのみ適用されます。パケットを切り替えるには、適切な 802.1Q VLAN 設定が必要です。

 IP Subnet-based VLAN を設定するには、「Configuration」->「VCL」->「IP Subnet-based VLAN」を クリックすると、以下の画面が表示されます。

IP Subn	et-base	Auto-refresh 🗌 Refresh										
					Port Members							
Delete	VCE ID	IP Address	Mask Length	VLAN ID	1 2 3 4 5 6 7 8 9 10 11 12 13	14 15 16 17 18 19 20 21 22 23 24 3						
	Currently no entries present											
Add Nev	v Entry											
Save	Reset											

(2) <Add New Entry>ボタンをクリックすると、以下の画面が表示されるので、各項目にそれぞれ値を入力して ください。

IP Subne	IP Subnet-based VLAN Membership Configuration fo						1											Auto	o-ref	resh		Re	fresh	
														P	ort N	lem	ber	s						
Delete	VCE ID	IP Address	Mask Length	VLAN ID	1	2 3	3 4	5	6	7 8	3 9	10	11	12	13 14	15	16	17	18	19 2	0 21	22	23	24
Delete	0	0.0.0.0	24	1																				
Add New	Entry																							
Save	Reset																							

2.4.16 Voice VLAN(音声VLAN)

Voice VLAN は、音声トラフィック用の特別な VLAN 設定です。Voice VLAN 用の音声機器をポートに設定して、 音声データの QoS 関連の設定を行うことにより、音声トラフィックの通信上の優先順位および安定した音声品質を 確保することが可能です。

2.4.16.1 Configuration (Voice VLAN 設定方法)

 Voice VLAN の設定を行うには、「Configuration」 -> 「Voice VLAN」 -> 「Configuration」をクリックすると、 以下の画面が表示されます。

Voice VLAN Configuration

Mode	Disabled	<
VLAN ID	1000	
Aging Time	86400	seconds
Traffic Class	7 (High)	~

Port Configuration for Switch 1

Port	Mode	Security	Discovery Protocol
*	 	○ ∨	
1	Disabled \checkmark	Disabled \checkmark	oui 🗸
2	Disabled 🗸	Disabled \checkmark	oui 🗸
3	Disabled 🗸	Disabled \checkmark	oui 🗸
4	Disabled 🗸	Disabled \checkmark	oui 🗸
5	Disabled 🗸	Disabled \checkmark	oui 🗸
6	Disabled 🗸	Disabled \checkmark	oui 🗸
7	Disabled \checkmark	Disabled \checkmark	oui 🗸
8	Disabled 🗸	Disabled \vee	OUI 🗸
9	Disabled 🗸	Disabled \checkmark	oui 🗸
10	Disabled 🗸	Disabled 🗸	OUI 🗸
11	Disabled 🗸	Disabled \checkmark	oui 🗸
12	Disabled ∨	Disabled V	OUI 🗸

ここでは本機の音声 VLAN を設定します。

この機能を有効にすると、VoIP トラフィックを自動検知し、特定のプライオリティに応じて音声 VLAN トラフィック の伝送を行います。音声 VLAN ポート検出プロトコルは、OUI または LLDP により有効です(OUI は、 MAC アドレスの最初の3バイトのベンダコードです)。

2.4.16.2 OUI

ここでは、音声 VLAN(Voice VLAN)の設定について説明します。

ここでは、Voice IP トラフィックの OUI テーブルのメンテナンスを行います。OUI は、MAC アドレスの最初の3バイトです。 OUI をもつパケットは、音声トラフィックとして処理されます。

(1) OUI を設定するには、「Configuration」 -> 「Voice VLAN」 -> 「OUI」をクリックすると、以下の画面が表示されます。

Delete	Telephony OUI	Description							
	00-01-e3	Siemens AG phones							
	00-03-6b	Cisco phones							
	00-0f-e2	H3C phones							
	00-60-b9	Philips and NEC AG phones							
	00-d0-1e	Pingtel phones							
	00-e0-75	Polycom phones							
	00-e0-bb	3Com phones							
Add Nev	Add New Entry								

Voice VLAN OUI Table

Save Reset

ここでは、Voice IP トラフィックの OUI テーブルのメンテナンスを行います。 OUI は、MAC アドレスの最初の3バ イトです。 OUI をもつパケットは音声トラフィックとして処理されます。

(2) 画面下の<Add New Entry>ボタンをクリックすると、以下の画面が表示されるため、新規に入力してください。

Voice VLAN OUI Table									
Delete	Telephony OUI	Description							
	00-01-e3	Siemens AG phones							
	00-03-6b	Cisco phones							
	00-0f-e2	H3C phones							
	00-60-b9	Philips and NEC AG phones							
	00-d0-1e	Pingtel phones							
	00-e0-75	Polycom phones							
	00-e0-bb	3Com phones							
Delete									

Add New Entry

Save Reset

2.4.17 QoS

QoS は、" Quality of Service(サービス品質)"の略です。 この機能は、個々のアプリケーションまたはプロトコル間の帯域幅を保証します。

通信ネットワークは、リアルタイム音声のような高品質のビデオおよび遅延に対して負荷の大きいデータを含む多様な アプリケーションデータを伝送します。

ネットワークは、安全性が高く、予測および測定可能な保証サービスを提供する必要があります。 この QoS 機能は、エンドツーエンドのビジネス・ソリューションとなり、ネットワークリソースを管理するための技術の 1 つです。

受信フレームすべては QoS クラスに分類され、その特定の QoS クラスに応じて、フレームに対するキューイング、スケジ ューリングおよび輻輳制御の保証を行うために装置全体で使用されます。 QoS クラス、キューおよび優先度との間のマッピングを行います。QoS クラスが「0(ゼロ)」の場合は、優先度が最も低 くなります。

2.4.17.1 Port Classification (ポート入力のクラス分け)

すべてのポートに対して、基本的な QoS 入力クラス分けの設定を行います。 「DSCP Based」を使って、IP ヘッダの DSCP を用いて QoS を有効/無効にします。

DSCP クラス分けについて

入力 DSCP クラス分けの設定については、「<u>DSCP-Based QoS</u>」画面を参照してください。この画面の「Trust」を選択すると、DSCP 値が有効になります。

入力 DSCP クラス分け変換の設定に関する詳細については、「<u>DSCP Translation</u>」および「<u>Port DSCP</u>」を参照してく ださい。

 ポート入力のクラス分けの設定を行うには、「Configuration」->「QoS」->「Port Classification」をクリック すると、以下の画面が表示されます。

QoS Ingress Port Classification for Switch 1
Port CoS DPL DSCP Based

Port	COS	DPL	DSCP Based
*	$\diamond \lor$	\diamond	
1	0 🗸	0 🗸	
2	0 🗸	0 🗸	
3	0 🗸	0 🗸	
4	0 🗸	0 🗸	
5	0 🗸	0 🗸	
6	0 🗸	0 🗸	
7	0 🗸	0 🗸	
8	0 🗸	0 🗸	
9	0 🗸	0 🗸	
10	0 🗸	0 🗸	
11	0 🗸	0 🗸	
12	0 🗸	0 🗸	
13	0 ~	0 ~	

2.4.17.2 Port Policing (ポート入力ポリシング)

この設定を用いて、ポートの入力レートの制限を行います。フロー制御を有効、かつフロー制御モードの場合は、上限のレートに達すると、フレームを破棄せずに、ポーズフレームを送信します。

 ポート入力ポリシャーの設定を行うには、「Configuration」->「QoS」->「Port Policing」をクリックすると、 以下の画面が表示されます。

Port	Enabled	Rate	Unit
*		500	° <
1		500	kbps 🗸
2		500	kbps 🗸
3		500	kbps 🗸
4		500	kbps 🗸
5		500	kbps 🗸
6		500	kbps 🗸
7		500	kbps 🗸
8		500	kbps 🗸
9		500	kbps 🗸
10		500	kbps 🗸
11		500	kbps 🗸
12		500	kbps 🗸
13		500	kbps 🗸
14		500	kbps 🗸
15		500	kbps 🗸
			· · ·

QoS Ingress Port Policers for Switch 1

2.4.17.3 Port Scheduler(ポート出力スケジューラ)

ここでは、ポートの出力スケジューラおよび各キューの重みづけが表示されます。

(1) ポート出力スケジューラーの設定を行うには、「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 for Switch 1

Dort	Mada	Weight					
FUIL	mode	Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
<u>11</u>	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-

(2) ポート番号をクリックすると、キューの出カスケジューラーおよびシェイパー画面が表示されます。



(3) トラフィックスケジューラは、「Strict Priority」モード、あるいは「Weighted」モードのいずれに設定します。 「Weighted」モードの場合は、それぞれのキューの重みづけが設定されます。



- (4) トラフィックシェイパーは、キュー単位、またはポート単位で設定します。 いずれかを選択すると、それぞれ制限値が設定されます。
- (5) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.4.17.4 Port Shaping(ポートおよびキュー出力シェイパー)

この設定は、各ポートとおよびキューの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して、出力シェイパーの設定を行ってください。

(1)「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 for Switch 1

Dort					Shapers				
POIL	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
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								

(2) ポート番号をクリックすると、以下のように、ポートおよびキュー出力スケジューラおよびシェイパーの設定画面が 表示されます。



- トラフィックスケジューラは、「Strict Priority」モード、あるいは「Weighted」モードのいずれに設定します。
 「Weighted」モードの場合は、それぞれのキューの重みづけが設定されます。
- トラフィックシェイパーは、キュー単位、またはポート単位で設定します。いずれかを選択すると、それぞれ制限値が 設定されます。
- ・ 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.4.17.5 Port Tag Remarking(ポート出力タグのリマーキング)

このメニューでは、各ポートの出力タグのリマーキングモードを表示します。

- このモードは、それぞれ以下のメニューから構成されます。 - Classified: クラス分けされた 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したバージョンを使用。 ポート番号をクリックして、その出力タグのリマーキングモードを設定します。
- ポート出力タグのリマーキングの設定を行うには、「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。

QoS Egress Port Tag Remarking for Switch 1

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
<u>11</u>	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified

(2) ポート番号をクリックすると、ポートの出力タグのリマーキング設定の画面が表示されます。

•「Classified」モードの場合:

QoS Egress Port Tag Remarking for Switch 1 Port 1	Port 1 🗸
Tag Remarking Mode Classified V	
Save Reset Cancel	
「Default Iモードの場合・	
QoS Egress Port Tag Remarking for Switch 1 Port 1	Port 1 V
Tag Remarking Mode Default V	
PCP/DEI Configuration	
Default PCP0Default DEI0	
Save Reset Cancel	

「Mapped」モードの場合:

QoS Egress Port Tag Remarking for Switch 1 Port 1

Tag Remarking Mode Mapped 🗸

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PC	P	DEI		
-	•	\diamond	~	\diamond	<	
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	<	

(3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

Port 1 🗸

2.4.17.6 Port DSCP(DSCP の設定)

ポートの QoS ポートの DSCP の基本設定を行うことが可能です。IP の優先度と同様に、パケットに優先度を付ける 場合に使用します。

(1)「Configuration」->「QoS」->「Port DSCP」をクリックすると、以下の画面が表示されます。

		-				
Port	Ingr	Egress				
1011	Translate	Classify	Rewrite			
*		<>	\$ <			
1		Disable DSCP-0	Disable 🗸			
2		Selected	Disable 🗸			
3		All	Disable 🗸			
4		Disable 🗸	Disable 🗸			
5		Disable 🗸	Disable 🗸			
6		Disable 🗸	Disable 🗸			
7		Disable 🗸	Disable 🗸			
8		Disable 🗸	Disable 🗸			
9		Disable 🗸	Disable 🗸			
10		Disable 🗸	Disable 🗸			

QoS Port DSCP Configuration for Switch 1

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

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と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、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「<u>DSCP Translation</u>」画面で設定してください。変換した DSCP 値は、入力 DSCP のQoS 設定に使用します。
- 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なく(DSCP から QoS へのマッピ ングは「DSCP-Based QoS」画面で設定可能)、「Port DSCP」画面の"Ingress Classify(入力クラス分 け)"は、QoS から内部 DSCP へのマッピングを行います。

「port default」、「VLAN タグ」、「DSCP」のいずれかから QoS クラスを入手すると、Ingress Classify(入力 クラス分け)により、この QoS クラスを内部 DSCP にマッピングします。

内部 DSCP はフレーム送信時の DSCP 値を変更するために、別の入力マップを行うことが可能です。

内部 DSCP への QoS マッピングは、「DSCP Classification」画面で設定します。

「Port DSCP」の Egress Rewrite(出力リライト)"が"enable"/"Remap"の場合は、出力パケットにマッピン グを行います。この場合元の DSCP 値は消去されます。

- 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)。
 - Selected: 「<u>DSCP Translation</u>」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(出カリライト):出カパケットの DSCP リライトを設定します。
 - Disable: Egress rewrite(出力リライト)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「<u>DSCP Translation</u>」画面の"Remap DP0"、または "Remap DP1"の設定をリマッピングします。

2.4.17.7 DSCP-Based QoS

DSCP への内部プライオリティのマッピング(入力)

ここでは、それぞれの DSCP 値ごとに QoS 入力のクラス分けを行います。 トラスト DSCP の値をもつフレームのみ、特定の QoS クラスおよび破棄優先レベルへのマッピングを行います。 アントラスト DSCP 値を持つフレームは適用されません。

 DSCP ベース QoS の設定を行うには、「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。

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
ż		\diamond V	◇∨
0 (BE)		0 🗸	0 🗸
1		0 🗸	0 🗸
2		0 🗸	0 🗸
3		0 🗸	0 🗸
4		0 🗸	0 🗸
5		0 🗸	0 🗸
6		0 🗸	0 🗸
7		0 🗸	0 🗸
8 (CS1)		0 🗸	0 🗸
9		0 🗸	0 🗸
		[a]	A · · ·

2.4.17.8 DSCP Translation (DSCP 変換の設定方法)

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。

「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

DSCD	In	Egress					
Dack	Translat	te	Classify	Remap			
ż	\diamond	~		\diamond	~		
0 (BE)	0 (BE)	\sim		0 (BE)	\checkmark		
1	1	\sim		1	$\mathbf{\sim}$		
2	2	\sim		2	\sim		
3	3	\sim		3	$\mathbf{\sim}$		
4	4	\sim		4	\sim		
5	5	\sim		5	$\mathbf{\sim}$		
6	6	~		6	$\mathbf{\sim}$		
7	7	\sim		7	\checkmark		
8 (CS1)	8 (CS1)	~		8 (CS1)	$\mathbf{\sim}$		
9	9	\sim		9	\checkmark		
10 (AF11)	10 (AF11)	\sim		10 (AF11)	\sim		
11	11	\sim		11	\checkmark		
12 (AF12)	12 (AF12)	\sim		12 (AF12)	\sim		

QoS クラスおよび DPL マップ用の DSCP を使用する前に、入力側の DSCP をまず新しい DSCP に変換します。

DSCP 変換方法には、以下の2つの設定方法があります。

- Translate : 入力側の DSCP は、DSCP 値(0~63 のいずれかの値)に変換可能です。
- Classify :「Port DSCP」メニューで「Ingess Classify」が選択されている場合に、DSCP 値を選択すると、 内部 DSCP への QoS クラスのマッピングが有効にします。

出力を行う場合に出力側で設定可能なパラメータは以下のとおりです。

- Remap DP0 により、「DP level 0」のフレームのリマッピングを制御します。
- Remap DP1 により、「DP level 1」のフレームのリマッピングを制御します。

この設定は、「Port DSCP」メニューの Egress Rewrite(出力リライト)に適用されます。 詳細については、「<u>Port DSCP</u>」メニューの「Egress Rewrite(出力リライト)」を参照してください。

2.4.17.9 DSCP Classification (DSCP クラス分け)

DSCP への内部プライオリティのマッピング(出力)

ここでは、QoS クラスの内部 DSCP 値へのマッピングを設定します。

フレームは、デフォルトポート、または VLAN タグ、または DSCP のいずれから QoS クラスを入手して、この QoS を内部 DSCP にマッピングすることができます。

これにより、内部 DSCP は、別の出力マップにより、フレームを送信時の DSCP 値に影響を与える可能性があります。 「Port DSCP」画面の出力リライトが有効な場合は、出力 DSCP 値をリライトすることができます。 詳細については、「<u>Port DSCP</u>」画面の「Egress Rewrite(出力リライト)」を参照して下さい。

 DSCP クラス分けの設定を行うには、「Configuration」->「QoS」->「DSCP Classification」をクリックすると、 以下の画面を表示します。

DSCP Classification

QoS Class	DSC	P
ż	\diamond	×
0	0 (BE)	~
1	0 (BE)	\sim
2	0 (BE)	~
3	0 (BE)	\sim
4	0 (BE)	\sim
5	0 (BE)	\sim
6	0 (BE)	~
7	0 (BE)	~

Save Reset

2.4.17.10 QoS Control list (QoS コントロールリスト)

QCL は QoS コントロールリストの略であり、QCE のテストテーブルです。 このテストテーブルは、特定のトラフィックオブジェクト上の特定の QoS クラスごとに、分類する QoS コントロールエントリ が含まれます。 それぞれのアクセス可能なトラフィックには、その OCL の識別子が含まれます。優先順位によって、特定の QoS クラス の特定のトラフィックオブジェクトが決まります。 QCE は、QoS クラスコントロールエントリの略であり、特定の QCE の ID に関連のある QoS クラスについて記述していま す。

 QoSコントロールリストの設定するには、「Configuration」 -> 「QoS」 -> 「QoS Control List」をクリックすると、 以下の画面が表示されます。

QoS Control List Configuration

QCE	Switch	Port	DMAC	SMAC	C Tag Type	VID	PCP	DEI	Frame	Action			
			DIMAC						Туре	CoS	DPL	DSCP	
													Ð

(2) "(+)"をクリックすると、QoSコントロールエントリを設定します。

QCE Configuration

	Port Members																										
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
✓	<	<	~	<	~	>	~	<	>	>	>	>	>	>	>	<	>	>	\checkmark	>	>	>	>	~	>	~	<

Key Parameters

DMAC	Any 🗸
SMAC	Any 🗸
Tag	Any 🗸
VID	Any 🗸
РСР	Any 🗸
DEI	Any 🗸
Frame Type	Any 🗸

Action Parameters

CoS	0 🗸
DPL	Default 🗸
DSCP	Default 🗸

Save Reset Cancel

2.4.17.11 Storm Control (ストームコントロール)

すべてのポートにストームコントロール機能を設定可能です。

ここでは、ユニキャストフレーム、ブロードキャストフレーム、宛先不明(フラッディングされた)フレームのストームレートコントロールで設定可能です。

(1) ストームコントロールの設定を行うには、「Configuration」->「QoS」->「Storm Control」をクリックすると、 以下の画面が表示されます。

Dest	Un	icast Frame	s	Bro	adcast Fram	ies	Unknown Frames					
Port	Enabled	Rate	Unit	Enabled	Rate	Unit	Enabled	Rate	Unit			
*		500	◇ ∨		500	◇ ∨		500	 			
1		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
2		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
3		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
4		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
5		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
6		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
7		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
8		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
9		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
10		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			
11		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸			

QoS Port Storm Control for Switch 1

2.4.17.12 WRED(Weighted Random Early Detection) 設定

WRED(Weighted random early detection)は、輻輳を回避させる為に、キュー処理を制御して、インタフェースのキュ ー内のパケットを破棄します。このWREDは、RED(random early detection)を拡張したものであり、シングルキューはそ れぞれキューの閾値を持っています。

各キューのしきい値は、特定のトラフィッククラスに関連付けられています。

例えば、キューは、優先度の低いパケットよりも更に低い閾値を保持することができます。そのため、キューの蓄積は、 優先順位の高いパケットを保護し、優先順位の低いパケットを破棄します。

このように、同じバッファーを用いてパケットのプールから重要なパケットに対して QoS の優先順位付けを行うことができます。同様に、標準のトラフィックはプライオリティの高いトラフィックよりも破棄される可能性が高くなります。

WRED の設定を行うには、「Configuration」->「QoS」->「WRED」をクリックすると、以下の画面が表示されます。

Weighted Random Early Detection Configuration

Queue	Enable	Min. Th	reshold	Max. DP 1		Ma	Max. DP 2		Max. DP 3	
0			0		1		5		10	
1			0		1		5		10	
2			0		1		5		10	
3			0		1		5		10	
4			0		1		5		10	
5			0		1		5		10	

Save Reset

2.4.18 Mirroring (ポートミラーリング)

ネットワークの問題のデバッグ、またはネットワークトラフィックのモニタリングを行うには、複数のポートからミラーリングポートにフレームのミラーリングを行なうようにシステムを設定することが可能です(この場合のフレームのミラーリングとは、フレ ームをコピーすることと同じです)。送受信フレームをミラーポートにミラーリングすることができます。

(1) ポートミラーリングの設定を行うには、「Configuration」->「Mirroring」をクリックすると、以下の画面が表示 されます。

Mirror Configuration



Mirror Port Configurationfor Switch 1

Port	Mode
ż	◇ ∨
1	Disabled V
2	Disabled V
3	Disabled V
4	Disabled V
5	Disabled V
6	Disabled V
7	Disabled V
8	Disabled V
9	Disabled V
10	Disabled V
11	Disabled V
12	Disabled V
13	Disabled V
14	Disabled V
15	Disabled V

ミラートラフィックは、パケットの送信/受信、あるいはその両方のフレームでミラーポートにミラーリングを行います。 モードを"Disabled"設定すると、ミラーリング機能は無効になります。

2.4.19 GVRP

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) は、大規模ネットワーク内の VLAN を制御するプロトコルです。GVRP は IEEE 802.1Q に準拠し、VLAN 設定データのフレームのタグ付け方法を定義します。これにより、ネットワーク機器は他の機器との間で VLAN 設定情報を自動的に交換できるようになります。

GVRP は、GARP (Generic Attribute Registration Protocol)に応じて異なります。

GARP は、LAN 内のエンドステーション/スイッチが他の機器との間で識別子やアドレスなどの属性を登録したり、登録解除する手順を定義するためのプロトコルです。

そのため、エンドステーションおよびスイッチはすべて、個々にアクセス可能なデータを保有することができます。GVRP は、GARPと同様に、登録されていないユーザへの情報の送信を回避することにより、不要なネットワークのトラフィッ クを削除します。また、スイッチは1台のみ固定で設定する必要がありますが、それ以外のスイッチはすべて状況に応じ て設定されます。

2.4.19.1 Global config (GVRPの基本設定):

 グローバル設定を行うには、「Configuration」->「GVRP」->「Global config」をクリックすると、以下の画面が 表示されます。

GVRP Configuration

Enable GVRP						
Parameter	Value					
Join-time:	20					
Leave-time:	60					
LeaveAll-time:	1000					
Max VLANs:	20					

Save

2.4.19.2 Port config (ポートの GVRP 設定)

GVRP を使用することで、スイッチは他の GVRP スイッチと VLAN 設定情報を交換し、不要なブロードキャストや不明のユニキャスト・トラフィックを取り除きます。 VLAN 設定情報の登録、または削除は GARP に基づき実行されます。

 ポートの GVRP 設定を行うには、「Configuration」 -> 「GVRP」 -> 「Port config」をクリックすると、 以下の画面が表示されます。

GVRP Port Configuration for Switch 1

Port	Mode	
×	\diamond	<
1	Disabled	~
2	Disabled	\sim
3	Disabled	\sim
4	Disabled	\sim
5	Disabled	~
6	Disabled	\sim
7	Disabled	~
8	Disabled	\sim
9	Disabled	~
10	Disabled	\sim
11	Disabled	~
12	Disabled	\sim

2.4.20 Stack (スタック接続)

ここでは、スタック接続方法について説明します。

スタック接続すると設定情報やルーティング情報などをスタック内の全スイッチで共有可能となり、物理的には複数の スイッチが1台の仮想的なスイッチとして動作します(スタック内の各スイッチごとに設定を行う必要がありません。) 同一のサブネット内(ブロードキャストドメイン)にあるスイッチを最大16台まで管理可能です。

スタック機能の設定については、まず機能の設定を行ってからスタックにケーブルを接続してください。

(1) スタック接続を行うには、「Configuration」 -> 「Stack」をクリックすると、以下の画面が表示されます。

Stack Configuration								
Stacking StateDisabledStacking Enabled								
Delete	Stack Member	Switch ID	Master Capable P	r riority	S 25,26 25,27	3	Switch Status	Switch Type
	00-17-2e-1b-b8-0e	1	Yes	-	25,28		Active	FXC5428 Switch
Start Master Election 26,27 26,28 27,28								
Save Reset								
2.4.21 sFlow

sFlow は、ポートカウンタのランダム、または一定時間のサンプリングによってネットワークのモニタリングを行う業界標準の技術です。サンプリングを行ったパケットおよびカウンタ(それぞれ、"フローサンプル"、"カウンターサンプル"と呼ぶ)は、 中央ネットワークのトラフィックモニタリングサーバに対して、sFlow の UDP データとして送信されます。 この中央サーバは、"sFlow のレシーバ"、または"sFlow コレクタ"と呼びます。 sFlow の詳細については、「http://sflow.org」を参照してください。

(1) sFlow の設定を行うには、「Configuration」->「sFlow」をクリックすると、以下の画面が表示されます。

sFlow Configuration					
Agent Configuration					
IP Address 127.0.0.1					
Receiver Configuration	1				
Owner	<none></none>	Release			
ID Address/Hestnems	0.0.0.0				

IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

Port Configuration for Switch 1

Dort		Flow Sampler		Counter	Poller
FOIL	Enabled	Sampling Rate	Max. Header	Enabled	Interval
ż		0	128		0
1		0	128		0
2		0	128		0
3		0	128		0
4		0	128		0
5		0	128		0
6		0	128		0
7		0	128		0

(2) 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。

【注記】:

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。

2.5 Monitor(モニタリング)

各機能の現在のステータスを表示します。

Configuration Monitor Sustame	System Informat	Auto-refresh C Refresh
► System ► Green Ethernet		System
Green Ethernet Norte	Contact	
	Name	
Security	Location	
	le l	lardware
Loop Protection	MAC Address	00-17-2e-1b-b8-05
Spanning Tree	Model Name	FXC5428
MVR		Time
▶ IPMC	System Date	1970-01-01T00:09:03+00:00
► LL DP	System Uptime	0d 00:09:03
MAC Table	5	Software
▶ VLANs	Software Version	1.00.02
 Stack 	Software Date	2016-06-07
• sFlow		

2.5.1 System (システム)

ここでは、システム情報を確認することができます。

2.5.1.1 Information (システム情報の設定)

システム情報を表示するには、「Monitor」→「System」→「Information」をクリックすると、以下の画面が表示されます。

System Information

	System
Contact	
Name	
Location	
	Hardware
MAC Address	00-17-2e-1b-b8-0e
Model Name	FXC5428
	Time
System Date	1970-01-01T23:08:49+00:00
System Uptime	0d 23:08:49
	Software
Software Version	1.00.01
Software Date	2016-01-25

2.5.1.2 CPU Load (CPU 負荷)

CPU の負荷ステータスに関する情報を表示するには、「Monitor」→「System」→「CPU Load」をクリックすると、以下の画面が表示されます。

CPU Load 100ms 0%	1sec 0%	10sec 0%	Auto-refresh ⊠ (all numbers running average)
			75%
			50%
			25%

2.5.1.3 Temperature (温度)

本体内部のチップの温度を測定するには、「Monitor」→「System」→「Temperature」をクリックすると、以下の画面 が表示されます。

Auto-refresh 🗌 R						
Status						
FAN Status	Normal	Wor	k			
Main Chip Temperature	52	°C				

2.5.1.4 IP Status (IP 設定)

IP ステータスを表示するには、「Monitor」→「System」→「IP Status」をクリックすると、以下の画面が表示されます。

IP Interfac	es		Auto-refresh 🗌 Refr
Interface	Туре	Address	Status
OS:lo	LINK	00-00-00-00-00	<up loopback="" multicast="" running=""></up>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-17-2e-1b-b8-0e	<up broadcast="" multicast="" running=""></up>
VLAN1	IPv4	192.168.11.206/24	
VLAN1	IPv6	fe80::217:2eff:fe1b:b80e/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<up host=""></up>
192.168.11.0/24	VLAN1	<up hw_rt=""></up>
224.0.0.0/4	127.0.0.1	<up></up>
::1/128	::1	<up host=""></up>

Neighbour cache

IP Address	Link Address
192.168.11.1	VLAN1:00-a0-de-ab-19-0d
192.168.11.17	VLAN1:00-ac-b5-ee-53-6a
192.168.11.23	VLAN1:34-17-eb-8f-61-a2
192.168.11.31	VLAN1:00-ac-4d-33-f4-67
192.168.11.32	VLAN1:00-ac-bd-fb-3f-7b
192.168.11.155	VLAN1:40-61-86-b6-68-9a
fe80::217:2eff:fe1b:b80e	VLAN1:00-17-2e-1b-b8-0e

2.5.1.5 Log

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記録されます。 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 情報を表示するには、「Monitor」→「System」→「Log」をクリックすると、以下の画面が表示されます。

System Log	Inform	natio	n for Sw	itch 1	Auto-refresh	Refresh	Clear	<<	<<	>>	>>
Level	All	\checkmark									
Clear Level	All	\sim									
The total numb	er of ent	ries is	0 for the gi	iven leve	I.						
Start from ID 1			with 20	entri	es per page.						

ID Level Time Message No entry exists

ここでは、本体のシステムログ情報が表示されます。

システムのログ情報				
Level	選択したレベルのシステムログを表示します。			
Clear Level	レベルを選択した後、 <clear>ボタンを押すと、選択したレベルのログを消去します。</clear>			
ID	ID をクリックすると、ログの詳細(時刻とそのメッセージ)が表示されます。			

2.5.1.6 Detailed Log (ログ情報の詳細)

1) ログ情報の詳細を表示するには、「Monitor」→「System」→「Detailed Log」をクリックすると、 以下の画面が表示されます。

Detailed System Log Information for Switch 1	Refresh	<<	<<	>>	>>
1D 1					

Message

No system log entry

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

2.5.2 Green Ethernet

Green Ethernetとは、EEE 機能(省電力 Ethernet)とも呼ばれており、ネットワークのトラフィックが少ないときに機器の消費電力を抑える機能です。

Green Ethernet 機能に対応したスイッチ間では、省電力設定が相互に自動調整されます。

2.5.2.1 Port Power Savings

Port P	ower	Savings \$	Status fo	Auto-refresh 🗌 Refresh			
Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1		\checkmark	×	×	×	×	×
2		\sim	×	×	×	×	×
3		\checkmark	×	×	×	×	×
4		\sim	×	×	×	×	×
5		\checkmark	×	×	×	×	×
6		\sim	×	×	×	×	×
7		\checkmark	×	×	×	×	×
8		\sim	×	×	×	×	×
9		\checkmark	×	×	×	×	×
10		\sim	×	×	×	×	×
11		\checkmark	×	×	×	×	×
12		\checkmark	×	×	×	×	×

Link: ポートのリンク状態を表示します。EEE cap: ポートが EEE に対応しているかどうかを表示します。EEE cap: ポートでEEEが有効かどうかを表示します(「Port Power Savings」画面の設定が反映されます。)LP EEE cap: リンク先が EEE に対応しているかどうかを表示します。EEE in power save:現在の省電力状態(on/off)を表示します。EEE in power save:: ActiPhy 方式による省電力モードになっていることを表示します。PerfectReach Savings:PerfectReach 方式による省電力モードになっていることを表示します。

2.5.3 Port (ポート設定)

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。

2.5.3.1 State (ポートの状態)

ここでは、ポートのリンク状態を表示します。ポートをクリックすると、選択したポートの統計情報が表示されます。 「Monitor」→「Ports」→「State」をクリックすると、以下の画面が表示されます。

Port Sta	ate O	/ervi	ew										Auto-re	fresh		Refresh
FXC	2	4	6	8	10	12	14	16	18	20	22	24				
Sector Sector																
	1	3	5	7	9	11	13	15	17	19	21	23	25	26	27	28

2.5.3.2 Traffic Overview (トラフィックの概要)

ここでは、ポートごとの統計情報を表示します。

「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 S	tatistics Ov	verview for S		Auto-ref	fresh 🗌 Refre	sh Clear			
	Pa	ckets	B	vtes	E	rrors	D	Filtered	
Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	769489	78221	97886122	16694168	0	0	119506	0	119506
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
<u>6</u>	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
<u>9</u>	0	0	0	0	0	0	0	0	0
<u>10</u>	0	0	0	0	0	0	0	0	0
<u>11</u>	0	0	0	0	0	0	0	0	0
<u>12</u>	0	0	0	0	0	0	0	0	0
<u>13</u>	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
<u>15</u>	0	0	0	0	0	0	0	0	0
<u>16</u>	0	0	0	0	0	0	0	0	0
<u>17</u>	0	0	0	0	0	0	0	0	0
<u>18</u>	0	0	0	0	0	0	0	0	0
<u>19</u>	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
<u>21</u>	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
<u>23</u>	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
<u>26</u>	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0

2.5.3.3 QoS Statistics (QoS 統計情報)

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

「Monitor」→「Ports」→「QoS Statistics」をクリックすると、以下の画面が表示されます。

Queui	ng Cour	Auto-refresh 🗌 Refresh Clear							Clear							
Dert	Q0	Q0 (1	Q	2	Q	3	Q	4	Q	5	G	6		Q7
Port	Rx	Тх	Rx	Тх	Rx	Тх	Rx	Тх	Rx	Tx	Rx	Тх	Rx	Тх	Rx	Tx
1	650639	0	0	0	0	0	0	0	0	0	0	0	0	0	0	78342
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<u>5</u>	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<u><u>7</u></u>	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

2.5.3.4 QCL Status (QCL ステータス)

ここでは、QCL ユーザごとに QCL ステータスを表示します。

それぞれの行では、設定されている QCE について表示します。特定の QCE がハードウェアに適用されない場合はハードウェア制限によりコンフリクトが生じます。

「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 for Switch 1						Combin	ed 🗸 Aut	o-refresh 🗌	Resolve Conflict	Refresh
User	QCE	Port	Frame Type	CoS	Action DPL	n DSCP	Conflict			
No ent	ries									

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リソースは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 を追加するために必要なリソースは利用できません。

<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。

2.5.3.5 Detailed Statistics (統計情報の詳細)

ここでは、ポートの統計情報の詳細を表示します。 ポートを選択すると、そのポートの統計情報の詳細が表示されます。

「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 for Switch 1 P	ort 1	Port	1 ∨ Auto-refresh □ Refres	h Clear
Receive Total		Trar	nsmit Total	
Rx Packets	772462	Tx Packets	7859	6
Rx Octets	98196727	Tx Octets	1684321	2
Rx Unicast	82781	Tx Unicast	7858	8
Rx Multicast	188365	Tx Multicast		6
Rx Broadcast	501316	Tx Broadcast		2
Rx Pause	0	Tx Pause		0
Receive Size Counters	Transmit	t Size Counters		
Rx 64 Bytes	432989	Tx 64 Bytes	5623	1
Rx 65-127 Bytes	126663	Tx 65-127 Bytes	456	0
Rx 128-255 Bytes	137660	Tx 128-255 Bytes	645	7
Rx 256-511 Bytes	44308	Tx 256-511 Bytes	557	2
Rx 512-1023 Bytes	30276	Tx 512-1023 Bytes	4	7
Rx 1024-1526 Bytes	566	Tx 1024-1526 Bytes	572	9
Rx 1527- Bytes	0	Tx 1527- Bytes		0
Receive Queue Counters		Transmit	Queue Counters	
Rx O0	652662	Tx Q0		0
114 40				0
Rx Q1	0	Tx Q1		0
Rx Q1 Rx Q2	0	Tx Q1 Tx Q2		0
Rx Q1 Rx Q2 Rx Q3	0 0 0	Tx Q1 Tx Q2 Tx Q3		0
Rx Q1 Rx Q2 Rx Q3 Rx Q4	0 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4		0 0 0 0
Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5	0 0 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5		000000000000000000000000000000000000000
Rx Q1 Rx Q2 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6	0 0 0 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6		0 0 0 0 0
Rx Q1 Rx Q2 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q6 Rx Q7	0 0 0 0 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7	7859	0 0 0 0 0 0 6
Rx Q1 Rx Q2 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Receive Error Counters	0 0 0 0 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Transmit	7859 Error Counters	0 0 0 0 0 0 0 6
Rx Q1 Rx Q2 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx Q7 Rx Drops	0 0 0 0 0 0 119800	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Transmit Tx Drops	7859 : Error Counters	0 0 0 0 0 0 0 6 0
Rx Q1 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx C7 Rx Drops Rx CRC/Alignment	0 0 0 0 0 0 0 119800 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Tx Drops Tx Late/Exc. Coll.	7859 Error Counters	
Rx Q1 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx Drops Rx CRC/Alignment Rx Undersize	0 0 0 0 0 0 0 119800 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q4 Tx Q6 Tx Q6 Tx Q7 Transmit Tx Drops Tx Late/Exc. Coll.	7859 Error Counters	000000000000000000000000000000000000000
Rx Q1 Rx Q2 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q6 Rx Q7 Receive Error Counters Rx Drops Rx CRC/Alignment Rx Undersize Rx Oversize	0 0 0 0 0 0 0 119800 0 0 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Tx Drops Tx Late/Exc. Coll.	7859 Error Counters	
Rx Q1 Rx Q2 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q5 Rx Q7 Receive Error Counters Rx Drops Rx CRC/Alignment Rx Undersize Rx Oversize Rx Oversize Rx Fragments	0 0 0 0 0 0 0 119800 0 0 0 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Tx Drops Tx Late/Exc. Coll.	7859 Error Counters	
Rx Q1 Rx Q2 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx Drops Rx CRC/Alignment Rx Undersize Rx Oversize Rx Oversize Rx Fragments Rx Fragments Rx Jabber	0 0 0 0 0 0 119800 0 0 0 0 0 0 0 0 0	Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Tx Drops Tx Late/Exc. Coll.	7859 : Error Counters	

2.5.3.6 DDMI

ここでは、DDMI(Digital Diagnostics Monitor Interface)機能がサポートされている SFP トランシーバが本機に挿入されている場合に、その SFP トランシーバの情報とステータスが表示されます。

(1)「Monitor」→「Ports」→「DDMI」をクリックすると、以下の画面が表示されます。

DDMI for Switch 1	Port 25			Port 25	✓ Auto-refres	sh 🗆
		Serial Info Ta	ble			
Status		N/A				
Vendor						
PartNo						
SerialNo						
Revision						
DateCode						
Transceiver		N/A				
		Ddm Info Tal	ole			
Туре	AlarmMax	AlarmMin	WarnMax	WarnMin	Current	
Temperature(°C)	0.00	0.00	0.00	0.00	0.00	
Voltage(V)	0.00	0.00	0.00	0.00	0.00	
TxBias(mA)	0.00	0.00	0.00	0.00	0.00	
TxPower(mW)	0.00	0.00	0.00	0.00	0.00	
RxPower(mW)	0.00	0.00	0.00	0.00	0.00	

(2) この WEB 画面で"?"をクリックすると、設定の詳細が表示されます。

2.5.4 DHCP

この機能は、DHCP 機能について以下のメニューをサポートしています。

2.5.4.1 Snooping Table

 DHCP ステータスを表示するには、「Monitor」 -> 「DHCP」 -> 「Snooping Table」をクリックすると、 以下の画面が表示されます。

Dynamic DHC	P Snoopin	ıg Table		Auto-refres	n 🗌 Refresh	<< >>			
Start from MAC address 00-00-00-00-00 , VLAN 0 with 20 entries per page.									
MAC Address	VLAN ID	Expired Lease Time	Source Port	IP Address	IP Subnet Mask	DHCP Server			
	No	more entries							

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.5.4.2 Relay Statistics(DHCP リレー統計情報)

 DHCP リレー統計情報を表示するには、「Monitor」->「DHCP」->「Relay Statistics」をクリックすると、 以下の画面が表示されます。

DHCP Relay Statistics Auto-refresh Clear									Clear		
Server Stati	istics										
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive M Circuit	issing ID	Receive Rem	e Missing ote ID	Recei Circ	ive Bad :uit ID	Receiv Remo	e Bad te ID
0	0	0		D	0		0		0		0
Client Statis	stics										
Transmit	Transmit	Receive	Receive	Replace	Ke	ер	Drop				
to Client	Error	from Client	Agent Option A	gent Option	Agent	Option	Agent Op	otion			
0	0	0	0	0		0		0			

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.5.4.3 Detailed Statistics(統計情報の詳細)

ここでは、ポートの統計情報の詳細を表示します。

「Monitor」→「Monitor」→「DHCP」→「Detailed Statistics」をクリックすると、以下の情報が表示されます。

ポートを選択すると、そのポートの統計情報の詳細が表示されます

DHCP Detailed Statistics for S	witch 1 Port	1 Combined	Port 1	✓ Auto-refresh □	Refresh Clear
Receive Packets	Т	Normal Forward			
Rx Discover	0 Tx Disc	oveSnooping	П		
Rx Offer	0 Tx Offe	r Relay			
Rx Request	0 Tx Req	uest	0		
Rx Decline	0 Tx Dec	line	0		
Rx ACK	0 Tx AC	(0		
Rx NAK	0 Tx NA	(0		
Rx Release	0 Tx Rele	ease	0		
Rx Inform	0 Tx Info	rm	0		
Rx Lease Query	0 TxLea	se Query	0		
Rx Lease Unassigned	0 Tx Lea	se Unassigned	0		
Rx Lease Unknown	0 Tx Lea	se Unknown	0		
Rx Lease Active	0 Tx Lea	se Active	0		
Rx Discarded Checksum Error	0				
Rx Discarded from Untrusted	0				

2.5.5 Security (セキュリティ設定)

ここでは、セキュリティに関する設定情報について確認することができます。

2.5.5.1 Access Management (管理アクセスの制限)

管理ソースインタフェースのアクセス制限のステータスを表示するには、「Monitor」→「Security」→「Access Management」をクリックすると、以下の画面が表示されます。

Access Ma	anagement Statisti	cs Auto-refresh	Refresh Clear
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

2.5.5.2 Network

1. Port Security

ここでは、本機全体のポートセキュリティ、およびポート単位のポートセキュリティのステータスを表示します。

1) Switch

本機全体のポートセキュリティのステータスを表示するには、「Monitor」→「Security」→「Network」→「Switch」をクリックすると、以下の画面が表示されます。

Auto-refresh 🗌 Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status for Switch 1

Dort	Heare	State	MAC Cour	nt
Port	Users	State	Current Li	mit
1		Disabled	-	
2		Disabled	-	-
3		Disabled	-	-
4		Disabled	-	-
<u>5</u>		Disabled	-	-
<u>6</u>		Disabled	-	-
7		Disabled	-	-
<u>8</u>		Disabled	-	-
9		Disabled	-	-
<u>10</u>		Disabled	-	-

2) Port

ポートごとのポートセキュリティのステータスを表示するには、「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。



MAC AddressVLAN IDStateTime of AdditionAge/HoldNo MAC addresses attached

2. NAS

ここでは、ユーザの MAC アドレスを使って、バックエンドサーバへの認証を行います。 侵入者による不正な MAC アドレスが使用される可能性があるため、MAC ベース認証は、802.1X 認証よりもセキュリ ティが低くなります。

1) Switch

本機全体のポートの NAS 機能のステータスを表示するには、「Monitor」→「Security」→「NAS」→「Switch」をクリッ クすると、以下の画面が表示されます。

Network Access	Server	Switch	Status	for	Switch	5
----------------	--------	--------	--------	-----	--------	---

Auto-refresh 🗌 Refresh

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
<u>6</u>	Force Authorized	Globally Disabled			-	
<u>7</u>	Force Authorized	Globally Disabled			-	
<u>8</u>	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	
<u>10</u>	Force Authorized	Globally Disabled			-	
<u>11</u>	Force Authorized	Globally Disabled			-	
<u>12</u>	Force Authorized	Globally Disabled			-	
<u>13</u>	Force Authorized	Globally Disabled			-	
<u>14</u>	Force Authorized	Globally Disabled			-	
<u>15</u>	Force Authorized	Globally Disabled			-	

2) Port

ポートごとの NAS 機能のステータスを表示するには、「Monitor」→「Security」→「NAS」→「Port Security」→「port」 をクリックすると、以下の画面が表示されます。

NAS Statistics for Switch 5 Port 1 Port 1 V Auto-refresh C Refresh

Port State



3. ACL Status (ACL ステータス)

ACL ステータスを確認するには、「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 S	tatus f	or Switch 1	[combined	✓ Auto	o-refresh 🗌	Refresh	
	User	ACE	Frame Type	Action	Rate Limiter	CPU	Counter	Conflict	
No entries									

4. ARP Status (ARP ステータス)

ARP ステータスを表示するには、「Monitor」→「Security」→「Network」→「ARP Status」をクリックすると、以下の画 面が表示されます。

Dynamic ARP	nspection Table	e for Switch 1	Auto-refresh 🗌 🛛	Refresh << >>
Start from Port 1 0.0.0.0	✓ , VLAN 1 with 20 entr	, MAC address ies per page.	00-00-00-00-00	and IP address
Port VLAN ID	MAC Address No more entries	IP Address		

5. IP Source Guard (IP ソースガード)

IP ソースガードの情報を表示するには、「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。

Dynar	nic IP So	urce Guard Ta	able for Switch	Auto-refresh	Refresh	<<	>>
Start fro page.	m Port 1	V, VLAN 1	and IP address	0.0.0.0	with 20	entri	es per
Port	VLAN ID	IP Address	MAC Address				
		No more entries					

2.5.5.3 AAA

1) RADIUS Overview (RADIUS の概要)

ここでは、認証設定画面で設定可能な RADIUS サーバのステータス情報を表示します。

(1) 「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。

RA	DIUS Serve	r Status Overview	Auto-refresh 🗌 Refresh				
#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status		
1	0.0.0.0	0	Disabled	0	Disabled		
2	0.0.0.0	0	Disabled	0	Disabled		
3	0.0.0.0	0	Disabled	0	Disabled		
4	0.0.0.0	0	Disabled	0	Disabled		
<u>5</u>	0.0.0.0	0	Disabled	0	Disabled		

【注記】:

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。この状態になるまでの秒数 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) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2) RADIUS Details (RADIUS の概要)

「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。

RADIUS Authentication Statist	tics for	Server #1 Server #1 ∨ Au	to-refresh 🗌	Refresh	Cle
Receive Packets		Transmit Packets	S		
Access Accepts	0	Access Requests	0		
Access Rejects	0	Access Retransmissions	0		
Access Challenges	0	Pending Requests	0		
Malformed Access Responses	0	Timeouts	0		
Bad Authenticators	0				
Unknown Types	0				
Packets Dropped	0				
	Othe	r Info			
IP Address			0.0.0.0:0		
State			Disabled		
Round-Trip Time			0 ms		

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets			
Responses	0	Requests	0		
Malformed Responses	0	Retransmissions	0		
Bad Authenticators	0	Pending Requests	0		
Unknown Types	0	Timeouts	0		
Packets Dropped	0				
	Othe	r Info			
IP Address			0.0.0.0:0		
State			Disabled		
Round-Trip Time			0 ms		

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.5.5.4 Switch

RMON

ここでは、RMON 統計情報を表示することができます。

1) Statistics (RMON 統計情報の設定)

RMON 統計情報を設定するには、「Monitoring」->「Security」->「Switch」->「RMON」->「Statistics」を クリックすると、以下の画面が表示されます。

R	Auto-refresh Refresh I< >>																	
St	Start from Control Index 0 with 20 entries per page.																	
I	Data D Source (ifIndex)	Drop	Octets	Pkts	Broad- cast	Multi- cast	CRC Errors	Under- size	Over- size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
Λ	Vo more entries	;																

2) History (履歴)

RMON の履歴情報を表示するには、「Monitoring」->「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 H	istory Ov	erview			Auto-refresh Refresh I<->>									
Start from Control Index 0 and Sample Index 0 with 20 entries per page.														
History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad- cast	Multi- cast	CRC Errors	Under- size	Over- size	Frag.	Jabb.	Coll.	Utilization
No more	No more entries													

3) Alarm (アラーム)

RMON アラーム情報を表示するには、「Monitoring」->「Security」->「Switch」->「RMON」->「Alarm」を クリックすると、以下の画面が表示されます。

RMO	ON Alarm	Overview			Auto-refresh Refresh						
Start	from Contro	ol Index 0	with	20	entries per	page.					
ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index		

4) Event (イベント)

RMON イベント情報を表示するには、「Monitoring」 -> 「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 I	Event Over	view	Au	to-refresh CRefresh I<< >>
Start from	Control Inde>	0	and Sample Index 0	with 20 entries per page.
Event Index	LogIndex	LogTime	LogDescription	
No more	entries			

2.5.6 LACP

LACP とは、複数の物理的なポートを束ねてひとつの論理的チャネルとして扱うためのプロトコルのことです。 IETF による標準規格のひとつである IEEE 802.3ad の中で規定されています。

2.5.6.1 System status (システムステータス)

LACP のシステムステータスを表示するには、「Monitoring」->「LACP」->「System status」をクリックすると、以下の画面が表示されます。

LACP Sy	stem Status	;	Auto-refresh 🗌 Refresh									
Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports							
No ports e	No ports enabled or no existing partners											

2.5.6.2 Port Status (ポートステータス)

LACP のポートステータスを表示するには、「Monitoring」->「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	for Sv	vitch 5	Auto-refresh 🗌 Refresh						
Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio				
1	No	-	-	-	-	-				
2	No	-	-	-	-	-				
3	No	-	-	-	-	-				
4	No	-	-	-	-	-				
5	No	-	-	-	-	-				
6	No	-	-	-	-	-				
7	No	-	-	-	-	-				
8	No	-	-	-	-	-				
9	No	-	-	-	-	-				
10	No	-	-	-	-	-				

2.5.6.3 Port Statistics (ポートの統計情報)

LACP のシステムステータスを表示するには、「Monitoring」 -> 「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	for Switch 1	Auto-refr	esh 🗆	Refresh	Clear
Port	LACP	LACP	Discar	ded		
	Received	fransmitteu	Unknown	megai		
1	0	0	0	0		
2	0	0	0	0		
3	0	0	0	0		
4	0	0	0	0		
5	0	0	0	0		
6	0	0	0	0		
7	0	0	0	0		
8	0	0	0	0		
9	0	0	0	0		
10	0	0	0	0		
11	0	0	0	0		
12	0	0	0	0		
13	0	0	0	0		
14	0	0	0	0		
15	0	0	0	0		
16	0	0	0	0		

2.5.7 Loop Protection (ループプロテクション)

ここでは、ループプロテクション機能の設定方法について説明します。 ループが発生すると、パケットストームが生成されることにより、ネットワーク障害が引き起こされる可能性があります。 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。

ループプロテクションを有効にすると、Tx(送信)モードが有効になっている場合、ポートはループプロテクションの PDU を 設定します。ループバックを検出すると、ポートはシャットダウンされるか、またはその情報を記録します。 シャットダウン時間は、一定の間隔で設定可能です。

(1) ループプロテクションのステータスを表示するには、「Monitoring」 -> 「LACP」 -> 「Port Statistics」をクリック すると、以下の画面が表示されます。

Loop	Protectio	on Status f	or Swite	ch 5	Auto-refresh 🗌 Refresh					
Port	Action	Transmit	Status	Loop	Time of Last Loop					
No po	rts enabled	1								

2.5.8 Spanning tree (スパニングツリー)

スパニングツリーは、ネットワークトポロジ内のネットワークのループを防止するためのプロトコルです。

ネットワークのループが発生すると、トラフィックが多くなればなるほど、ネットワークのループによりネットワークが不安定に なります。そのため、ネットワークのループが生じると、スパニングツリープロトコルにより、ループした接続を自動的にブロッ クします。ネットワークトロポジ—の検出によりネットワーク接続が変更されると、遅延(STPの場合は「30秒」、RSTP の場合は「30秒以下」)が生じます。

本機では、MSTP/RSTP/STP 機能をサポートしているため、ここでは、スパニングツリーの設定方法について説明します。

2.5.8.1 Bridge Status (ブリッジステータス)

STP ブリッジの設定情報を表示するには、「Monitoring」->「Spanning Tree」->「Bridge Status」をクリックすると、 以下の画面が表示されます。

STP Bridges Auto-refresh 🗌 Refresh												
меті	Bridge ID	Root			Topology	Topology						
IN STI	Bridge ib	ID	Port	Cost	Flag	Last						
CIST	32768.00-17-2E-1B- B8-0E	32768.00-17-2E-1B- B8-0E	-	0	Steady	-						

2.5.8.2 Port Status (ポートステータス)

STP ブリッジのステータスを確認するには、「Monitoring」->「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 P	ort Status f	or Switch 5	Auto-refres	sh 🗌 Refresh
Port	CIST Role	CIST State	Uptime	
5:1	Non-STP	Forwarding	-	
5:2	Non-STP	Forwarding	-	
5:3	Non-STP	Forwarding	-	
5:4	Non-STP	Forwarding	-	
5:5	Non-STP	Forwarding	-	
5:6	Non-STP	Forwarding	-	
5:7	Non-STP	Forwarding	-	
5:8	Non-STP	Forwarding	-	
5·0	Non-STP	Fonwarding	_	

2.5.8.3 Port Statistics (ポートの統計情報)

STP ブリッジの統計情報を確認するには、「Monitoring」->「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 S	tatistics	s for Sw	itch 1			Clear						
Dort		Transm	itted			Receiv	ved		Discarded			
Port	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal		
No po	rts enable	d										

2.5.9 MVR

MVR 機能により、マルチキャスト VLAN 上でマルチキャストトラフィックの送信を可能にします。 マルチキャストテレビアプリケーションでは、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、あるいは PC を1つの加入者ポート(MVR 受信側ポートと して設定されているポート)に接続可能です。加入者はチャンネルを選択すると、セットトップボックス、あるいは PC は 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設定します。 マルチキャスト VLAN に対するマルチキャストデータの送受信先のアップリンクポートは"MVR 送信元ポート"と言います。 これにより、各マルチキャスト VLAN ごとに対応するチャンネルのプロファイルをもつ MVR を最大 4 つまで設定可能で す。チャンネルのプロファイルは、フィルタリング条件をもつ IPMC プロファイルによって定義されます。

2.5.9.1 Statistics (MVR 統計情報)

MVRの統計情報を表示するには、「Monitoring」->「MVR」->「Statistics」をクリックすると、以下の画面が表示されます。

MVR Statistics for Switch 1 Auto-refresh Clear												
VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received						
No more e	entries											

2.5.9.2 MVR Channel Groups (MVR チャネルグループ)

MVR のチャネルグループを表示するには、「Monitoring」 -> 「MVR」 -> 「MVR Channel Groups」クリックすると、 以下の画面が表示されます。

IVR Channels (Groups) Information for Switch 1 Auto-refresh														efre	esh		<<		>>	•								
itart from VLAN 1 and Group Address ::																v	vith	20		er	ntrie	s pe	r pa	ige.				
			Port Members																									
													F	or	t Mi	emt	pers											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	F 12	Port 13	t Mo 14	emi 15	oers 16	; 17 18	19	20	21	22	23	24	25	26	27	28

2.5.9.3 MVR SFM Information (MVR SFM 情報)

MVRの SFM 情報を表示するには、「Monitoring」->「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	Informa	tion fo	or Swite	:h1 ,	Auto-refr	esh 🗌 Refresh	<<	>>
Start from VL entries per pa	AN 1 age.	and	d Group A	Address ::			with	20
VLAN ID Group Port Mode Source Address Type Hardware Filter/Switch								
No more entries								

2.5.10 IPMC

2.5.10.1 IGMP Snooping

IGMP とは、「Internet Group Management Protocol」の略です。

このプロトコルは、インターネットプロトコルマルチキャストグループのメンバーを管理する通信プロトコルです。 IGMP は、IP ホストおよび近隣のマルチキャストルータにより使用され、マルチキャストグループのメンバーを設定します。 これは、ユニキャスト向けの ICMP と同様に、IP マルチキャスト仕様上不可欠な部分です。IGMP は、オンラインビデオ およびゲームに使用され、リソースをより効率的に使用することができます。

IGMP スヌーピングは、IGMP ネットワークトラフィックを受信するための手順です。この機能により、ネットワークスイッチは、 ホスト/ルータ間の IGMP 通信を受信できるようになります。これらの通信を受信することにより、IP マルチキャストストリ ームに必要なリンクのマップを保持することが可能です。

リンクから不要なマルチキャストをフィルタリングすることにより、ポートで受信した特定のマルチキャストのトラフィックを制御することができます。

1. Status (ステータス)

IGMP スヌーピングのステータスを表示するには、「Monitoring」 -> 「IPMC」 -> 「IGMP Snooping」 -> 「Status」を クリックすると、以下の画面が表示されます。

IGN	MP Snooping Status for Switch 1 Auto-refresh Clear									
Stat	isti	cs								
VL I	AN D	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
Rou	iter	Port								
Po	rt	Status								
	2	-								
	3	-								
	4	-								
	5	-								
	6	-								
	7	-								
	8	-								
	9	-								
	10	-								

2. Group Information (グループ情報)

グループ情報を表示するには、「Monitoring」->「IPMC」->「IGMP Snooping」->「Group Information」をクリックすると、以下の画面が表示されます。

IGMP Snooping Group Information for Switch 1 Auto-refresh							Refre	sh	<<		>>			
Start from VL	AN 1	and g	group add	ress 2	24.0.0.0		w	ith 20)	entries	s per	page.		
Port Members														
VLAN ID	Groups	1234	56789	10 11	12 13 14	15 16	5 17 18	19 20	21 22	2 23 24	25 2	26 27 2	28	
No more en	ntries													

3. IPv4 SFM information (IPv4 SFM 情報)

IPv4 SFM 情報を表示するには、「Monitoring」 -> 「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	or Swit	ch 1	Auto-refres	h 🗆 [Refresh	<<	>>		
Start from VL	AN 1	and	d Group	224.0.0.0	w	ith 20	entrie	s per pag	e.
VLAN ID	Group	Port	Mode	Source	Address	Туре	Hardwa	are Filte	r/Switch
No more en	tries								

2.5.10.2 MLD Snooping

MLD とは、IPv6 向けの「Multicast Listener Discovery」の略です。 このプロトコルは、IGMP が IPv4 で使用されるのと同じように、接続先のマルチキャストリスナーを検出するために、IPv6 ルータで使用されます。このプロトコルは、他のプロトコルを用いず、ICMPv6 に組み込まれています。 MLD スヌーピングにより、MLD パケットを受信し、その内容に応じて伝送を行います。 本機では、MLD、または MLD スヌーピングクエリアから MLD クエリを受信するサブネット内の MLD スヌーピングを使用 するように設定することが可能です。 MLD スヌーピングは、レイヤ 2 の LAN ポートを動的に設定することにより、レイヤ 2 の IPv6 マルチキャストトラフィックを 抑制して、受信を要求するポートにのみ IPv6 マルチキャストトラフィックを伝送します。

1) Status (MLD Snooping のステータス)

MLD スヌーピングのステータスを表示するには、「Monitoring」->「IPMC」->「MLD Snooping」->「Status」をク リックすると、以下の画面が表示されます。

MLD Snooping Status for Switch 1

Auto-refresh Clear

Statistics

VLAN	Querier	Host	Querier	Queries	Queries	V1 Reports	V2 Reports	V1 Leaves
ID	Version	Version	Status	Transmitted	Received	Received	Received	Received

Router Port

Port	Status	
1	-	
2	-	
3	-	
4	-	
5	-	
6	-	
7	-	
8	-	
9	-	

2) Groups Information (グループ情報)

MLD スヌーピングのグループ情報を表示するには、「Monitoring」 -> 「IPMC」 -> 「MLD Snooping」 -> 「Groups Information」をクリックすると、以下の画面が表示されます。

MLD Snooping Group Information for Switch 1 Auto-refresh Careford Refresh I							
Start from VLAN 1 entries per page.	and group address ff00::	with 20					
	Port Members						
VLAN ID Groups	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 2	6 27 28					
No more entries							

3) IPv6 SFM Information

IPv6 SFM 情報を表示するには、「Monitoring」 -> 「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 Informa	tion for Swite	Auto-re	fresh 🗌 Refresh 🛛 I<< >>	
Start from VLAN 1 page.	and Group		with 20 entries per	
VLAN ID Group No more entries	Port Mode	Source Address	Туре	Hardware Filter/Switch

2.5.11 LLDP

LLDPとは、IEEE802.1AB 標準プロトコルです。 データリンク層の接続を検出/管理するプロトコルで IEEE802.1ab により標準化されています。 当機能で LAN に接続された機器を検出して各種の設定や管理を行うことができます。

LLDP は、IEEE802 の LAN の接続先のステーションが、同じ IEEE802 の LAN に接続されている他のステーション に、これらの機能の管理を行う本体の管理アドレス、管理用の本体に必要な IEEE802 への接続のステーション ポイントの情報を取り込むシステムによって提供される主な機能を通知します。

プロトコルを介して送信されている情報は、MIBの受信側によってストアされ、SNMP などの管理プロトコルを使用して NMS による情報へのアクセスが可能になります。

2.5.11.1 Neighbors (ネイバー情報)

ネイバー情報を表示するには、「Monitoring」-> 「LLDP」-> 「Neighbors」をクリックすると、以下の画面が表示されます。

LLDP Ne	LDP Neighbor Information for Switch 1 Auto-refresh C Refresh								
	LLDP Remote Device Summary								
Local Port	Local Chassis Port Port System System Management Port ID ID Description Name Capabilities Address								
	No neighbor information found								

2.5.11.2 EEE

EEE 情報を表示するには、「Monitoring」-> 「LLDP」->「EEE」をクリックすると、以下の画面が表示されます。

LLDP Nei	ghbor	s EEE	Information for	Switch 5		Au	to-refresh 🗌 R	efresh	
Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync	
	No LLDP EEE information found								

2.5.11.3 Port Statistics (ポート統計情報)

ポートの統計情報を表示するには、「Monitoring」 ->「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 for Switch 1

Auto-refresh	Refresh	Clear
--------------	---------	-------

Global Counters								
Neighbor entries were last changed	1970-01-01T00:00:00+00:00 (99305 secs. ago)							
Total Neighbors Entries Added	0							
Total Neighbors Entries Deleted	0							
Total Neighbors Entries Dropped	0							
Total Neighbors Entries Aged Out	0							

LLDP Statistics Local Counters for Switch 1

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age- Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0

2.5.12 MAC Table

フレームの切り替えは、フレーム内の DMAC アドレスに応じて異なります。

スイッチは、フレームの送信先のポート情報(フレーム内の DMAC アドレスに基づいて)を認識して、MAC アドレスをポ ートにマッピングするためのテーブルを構成します。このテーブルには、スタティックおよびダイナミックエントリが含まれます。 スタティックエントリは、DMAC アドレスとポート間のマッピングを固定したい場合にネットワーク管理者により設定可能 です。

フレームには MAC アドレス(SMAC アドレス)が含まれ、この MAC アドレスは、フレームの送信元の機器の MAC アドレスです。SMAC アドレスはスイッチ本体で用いられ、MAC テーブルはダイナミック MAC アドレスにより自動的に更新されます。

ダイナミックエントリは、対応する SMAC アドレスをもつフレームがエージングタイム後に表示されない場合は、MACテ ーブルから削除されます。

(1) MAC テーブルを表示するには、「Monitoring」 -> 「MAC Table」をクリックすると、以下の画面が表示されます。

MAC Add	dress T	able for Switch 1		Auto-refresh Clear I<< >>
Start from \	/LAN 1	and MAC addre	ss 00-00	0-00-00-00 with 20 entries per page.
				Port Members
Туре	VLAN	MAC Address	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 25 26 27 28
Dynamic	1	00-01-8E-7B-84-50	\sim	
Dynamic	1	00-08-CA-F0-AF-1D	~ ~	
Dynamic	1	00-0C-29-3B-CB-3A	\checkmark	
Dynamic	1	00-0C-29-C1-92-A5	\sim	
Dynamic	1	00-0C-29-C1-92-AF	\checkmark	
Dynamic	1	00-0с-29-с1-92-в9	\checkmark	
Dynamic	1	00-0C-29-C1-92-C3	\checkmark	
Dynamic	1	00-0C-29-C1-92-CD	\checkmark	
Dynamic	1	00-0C-29-C1-92-D7	\checkmark	
Dynamic	1	00-0C-29-C1-92-E1	1	

2.5.13 VLAN

VLAN(仮想LAN)は、スイッチポート間の通信を制限する方法です。レイヤ2では、ネットワークは、複数の異なる分離したブロードキャストドメインに分かれています。

本機では、各 VLAN のアプリケーションに応じて、802.1Q VLAN、プライベート VLAN、MAC ベース VLAN、プロト コルベース VLAN、IP サブネットベース VLAN、および音声 VLAN をサポートしています。

2.5.13.1 Membership (VLAN メンバー)

 VLAN のメンバーを表示するには、「Monitoring」 -> 「Membership」 -> 「vlans」をクリックすると、以下の画面が 表示されます。

??																																	
VLAN Mei	mb	er	sh	ip	Sta	itu	s f	or	Co	mb	in	ed	us	ser	rs f	or	Sv	vite	ch	1	[Со	mb	inec	ł	V	Au	to-r	efre	esh		Refr	esh
Start from VI	LAN	1				witl	n 2	0		e	ntri	es	per	pa	ige.		<<		>	>													
												P	ort	M	em	be	rs																
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28					
1	\checkmark																																

2.5.13.2 Ports (ポート設定)

(1) VLAN のメンバーを表示するには、「Monitoring」 -> 「Ports」-> 「vlans」をクリックすると、以下の画面が表示されます。

VLAN	Port Status	for Combined us	sers for Swite	:h 1	Combin	ned V Auto-refresh	Refresh
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	\checkmark	All	1	Untag PVID		No
2	C-Port	\checkmark	All	1	Untag PVID		No
3	C-Port	\checkmark	All	1	Untag PVID		No
4	C-Port	\checkmark	All	1	Untag PVID		No
5	C-Port	\checkmark	All	1	Untag PVID		No
6	C-Port	\checkmark	All	1	Untag PVID		No
7	C-Port	\checkmark	All	1	Untag PVID		No
8	C-Port	\checkmark	All	1	Untag PVID		No
9	C-Port	\checkmark	All	1	Untag PVID		No
10	C-Port	\checkmark	All	1	Untag PVID		No

2.5.14 Stack (スタック設定)

スタック機能によって 設定情報やルーティング情報等をスタック内の全スイッチで共有することになるため、 物理的には複数のスイッチが1台の仮想的なスイッチとして動作します。 スタック内の各スイッチごとの設定が不要です。

(1) VLAN のメンバーを表示するには、「Monitoring」 -> 「Stack」をクリックすると、以下の画面が表示されます。

Stack Status

Refresh

State Stacking Disabled

2.5.15 sFlow

sFlowは、ポートカウンタのランダム、または一定時間のサンプリングによってネットワークのモニタリングを行う業界標準の技術です。サンプリングを行ったパケットおよびカウンタ(それぞれ、"フローサンプル"、"カウンターサンプル"と呼ぶ)は、 中央ネットワークのトラフィックモニタリングサーバに対して、sFlowのUDPデータとして送信されます。 この中央サーバは、"sFlowのレシーバ"、または"sFlowコレクタ"と呼びます。 sFlowの詳細については、「http://sflow.org」を参照してください。

(1) VLAN のメンバーを表示するには、「Monitoring」 ->「sFlow」をクリックすると、以下の画面が表示されます。

sFlow Statistics	Auto-refresh	Refresh	Clear Receiver	Clear Ports
------------------	--------------	---------	----------------	-------------

Receiver Statistics

Owner	<none></none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics for Switch 1

Port	Flow Samples	Counter Samples
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0

2.6 Diagnostics (診断機能)

本機では、ping テスト、および TX ポートのケーブル接続によりネットワーク接続診断を行います。

Configuration Monitor	ICMP Ping	
 Diagnostics Ping 	IP Address	0.0.0.0
• Ping6	Ping Length	56
 VeriPHY 	Ping Count	5
 Maintenance Restart Devic 	e Ping Interval	1
 Factory Defau Software Configuration 	Start	

2.6.1 Ping

ここでは、IP 接続の問題解決のために、ICMP の PING パケットを送信することができます。

(1)「Diagnostics」->「Ping」をクリックすると、以下の画面が表示されます。

ICMP Ping	
IP Address	0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1
Start	

<Start>ボタンをクリックすると、ICMPパケットが送信され、応答を受信次第シーケンス番号および往復時間が表示されます。

ICMP ECHO_REPLYのIPパケットを受信したデータ量は常に要求したデータスペース(ICMP header)より も大きく、「8バイト」になります。

この画面は、すべてのパケットからの応答を受信するまで、またはタイムアウトまで自動的に更新されます。

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.6.2 Ping6

ここでは、ICMPv6 接続の問題解決のために、ICMPv6 PING パケットを送信することができます。

(1)「Diagnostics」->「Ping6」をクリックすると、以下の画面が表示されます。

ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	

Start

<Start>ボタンをクリックすると、ICMPv6パケットが送信され、応答を受信次第シーケンス番号および往復時間が 表示されます。

この画面は、すべてのパケットからの応答が受信されるまで、またはタイムアウトまで自動的に更新されます。

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.6.3 VeriPHY (ケーブル接続診断)

ここでは、10/100/1000M ポートの VeriPHY(ケーブル診断)の設定を行います。

(1) ケーブル診断を行うには、「Diagnostics」 -> 「VeriPHY」をクリックすると、以下の画面が表示されます。

VeriPHY Cable Diagnostics for Switch 1

Port	All 1								
Start	2								
	4								
	6				Cable Sta	tus			
Port	7	4	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	8	Г					-		
2	9								
3	10						-		
4	12								
5	13								
6	14								
7	15								
8	16								
9	17						-		
10	18								

ポートを指定して<Start>をクリックすると、そのポートの診断が開始されます。診断には「約5秒」ほどかかります。 すべてのポートが選択されている場合は、診断に「約15秒」ほど要します。完了すると、画面が自動的に更新さ れ、ケーブルステータス表にケーブル診断の結果が表示されます。

【注記】:

VeriPHY は、「7~140m」の長さのケーブルについては正確に実行することができます。

10/100Mbps ポートは、VeriPHY の動作時にリンクダウンするため、10Mbps または 100Mbps の管理ポートで VeriPHY を起動する場合は、VeriPHY が完了するまで応答しなくなります。

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.7 Maintenance (メンテナンス)

ここでは、メンテナンス(システムのリブート、ソフトウェアの更新/選択、バックアップの設定/リストア、工場設定値を含む) について説明します。



2.7.1 Restart (システムリブート)

ここでは、本機の再起動を行います。

(1) システムのリブートを行うには、「Maintenance」 -> 「Restart Device」をクリックすると、以下の画面が表示されます。

Restart Device

Are you sure you want to perform a Restart?	
Yes No	
Yes :本機を再起動します。	

- No : 再起動を行わずに、「Port State Overview」画面に戻ります。
- (2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.7.2 Factory Defaults (初期設定に戻す)

(1) 初期設定に戻すには、「Maintenance」->「Factory Defaults」をクリックすると、以下の画面が表示されます。

Factory Defaults



ここでは、本機の設定を工場出荷時状態に戻すことができます(IP 設定のみ保持されます。)。 新しい設定はすぐに適用されるため、再起動する必要がありません。

- Yes :本機の設定を工場出荷時の状態に戻します。
- No : 設定をリセットせずに、「Port State Overview」画面に戻ります。
- (2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.7.3 Software (ソフトウェア)

ここでは、ソフトウェアのアップロードとソフトウェアの設定方法について説明します。

2.7.3.1 Upload (ソフトウェアのアップロード)

 ソフトウェアをアップロードするには、「Maintenance」 -> 「Software」 -> 「Upload」をクリックすると、以下の画面 が表示されます。

Software Upload



ソフトウェアのアップロードを行うには、<参照>ボタンをクリックして、ソフトウェアの保存場所を選択し、 <Upload>ボタンをクリックします。

ソフトウェアの更新を行う場合、更新が開始されている旨のメッセージが表示されます。

約1~2分経過すると、ソフトウェアの更新が完了し、再起動します。

本機では、ソフトウェアのバックアップ機能をサポートしています。ソフトウェアの更新後、古いソフトウェアは代替 ソフトウェアに切り替わり、新規のソフトウェアを有効にします。古いバージョンのソフトウェアを使用したい場合は 「Image Select」画面の〈Activate Alternate Image〉ボタンをクリックすることによって有効にすることが可能で す。

【警告】:

更新中は、Web へのアクセスが中断しているように見えますが、電源を再起動したり、電源を落としたりしないで ください。万が一更新中に電源を切った場合は、何らかの障害が起きる可能性があります。

2.7.3.2 Image Select (ソフトウェアを書き換え)

ここでは、本機で現在有効となっているソフトウェア(Active Image)と、代替ソフトウェア(Alternate Image)についての情報が表示され、使用するソフトウェアを選択することが可能です。

(1) 現在使用しているソフトウェアを書き換えるには、「Maintenance」 -> 「Software」 -> 「Image Select」を クリックすると、以下の画面が表示されます。

Active Image			
Image	managed		
Version	1.00.01		
Date	2016-01-25		
Altern	ate Image		
Image	managed.bk		
Version	1.00.01		
Date	2016-01-25		
Activate Alternate Image		Cance	

Software Image Selection

【注記】:

- 1. 現在実行中のソフトウェアが代替のソフトウェアの場合は、起動中のソフトウェアのみが表示され、 < Activate Alternate Image > ボタンは無効になります。
- 2. 代替ソフトウェアを使用している場合(元々有効な状態だったソフトウェアに問題がある場合や、手動でソフトウェアを切り替えた等の理由で)、新しいソフトウェアをアップロードすると、"Active Image"のスロットに新し いソフトウェアがインストールされ、これが有効となります。

2.7.4 Configuration(configファイルの設定)

ここでは、config ファイルの設定方法(ファイルの保存、ダウンロード/アップロード、有効化、削除方法)について説明します。

2.7.4.1 Save startup-config (起動用 config ファイルとして保存する)

 記動用 config ファイルとして保存するには、「Maintenance」 -> 「Configuration」 -> 「Save startup-config」 をクリックすると、以下の画面が表示されます。

<Save Configuration>ボタンをクリックすることで、現在の Config ファイルを起動用 Config ファイルとして保存します。

Save Running Configuration to startup-config
Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.
Save Configuration

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.7.4.2 Download (config ファイルのダウンロード)

 config ファイルをダウンロードするには、「Maintenance」 -> 「Configuration」 -> 「Download」をクリックすると、 以下の画面が表示されます。

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
○ running-config
○ default-config
⊖ startup-config
○ backup-config
Obackup-config_20160314
⊖test
Download Configuration

- (2) この画面にてダウンロードしたい Config ファイルを選択し、<Download Configuration>ボタンをクリックすることで、 選択した Config ファイルをダウンロードします。
- (3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

2.7.4.3 Upload (config ファイルのアップロード)

config ファイルのアップロードを行うには、「Maintenance」 -> 「Configuration」 -> 「Upload」をクリックすると、以下の 画面が表示されます。

Upload Configuration

File To Upload

	参照					
Destination File						
File Name	Parameters					
○ running-config	Replace	Merge				
⊖ startup-config						
O backup-config						
Obackup-config_20160314						
Otest						

Note: File system is full; either delete a file to make room, or select an existing file.

Upload Configuration

(1) config ファイルのアップロードを行うには、<参照>ボタンをクリックしてアップロードするファイルを選択します。

- (2) "Destination File"メニューより、保存先とパラメータ(Replace(リプレース)/Merge(ファイルを統合する)を選択して、<Upload Configuration>ボタンをクリックします。
- (3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。
2.7.4.4 Activate (config ファイルを有効にする)

config ファイルを有効にするには、「Maintenance」->「Configuration」->「Activate」をクリックすると、以下の画 面が表示されます。

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will <u>not</u> be saved to startup-config automatically.

File Name
O default-config
○ startup-config
○ backup-config
Obackup-config_20160314
⊖test

Activate Configuration

"File Name"メニューより、使用したい Config ファイル名を選択して、〈Activate Configuration〉ボタンをクリックすることで、選択した Config ファイルを有効にします。

Config ファイルを有効にすることによりそれまで使用していたファイルが上書きされるため、管理上接続が切れてしまう可能性があります。

【注記】:

ここで config ファイルを有効にしても、そのファイルは自動的に起動用 config ファイルとして保存されないため注意してく ださい。

有効化した config ファイルを起動用 config ファイルとして保存する場合は、「Save startup-config」画面にて"Save Configuration"ボタンをクリックしてください。

2.7.4.5 Delete (config ファイルを削除する)

 config ファイルを削除するには、「Maintenance」 -> 「Configuration」 -> 「Delete」をクリックすると、 以下の画面が表示されます。

Delete Configuration File

Select configuration file to delete.

File Name
⊖ startup-config
○ backup-config
O backup-config_20160314
Otest
Delete Configuration File

(2) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。 削除するファイル名を選択して、<Delete Configuration File>ボタンをクリックしてください。

(3) 画面右上の"?"アイコンをクリックすると、画面内の項目についての説明を記載したポップアップが表示されます。

FXC5428 Management Guide (FXC16-DC-200005-R1.0)

初版 2016年11月

- ・本ユーザマニュアルは、FXC株式会社が制作したもので、全ての権利を 弊社が所有します。弊社に無断で本書の一部、または全部を複製/転載 することを禁じます。
- ・改良のため製品の仕様を予告なく変更することがありますが、ご了承く ださい。
- 予告なく本書の一部または全体を修正、変更することがありますが、ご 了承ください。
- ユーザマニュアルの内容に関しましては、万全を期しておりますが、万 ーご不明な点がございましたら、弊社サポートセンターまでご相談くだ さい。

FXC5428 Management Guide



