

Management Guide
FXC3008

Management Guide
FXC3008
Management Guide

Management Guide
FXC3008

本マニュアルについて

- 本マニュアルでは、FXC3008 の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末接続して、CLI（コマンドラインインタフェース）または Web ブラウザで行います。
- このマニュアルには、事故を防ぐための重要な注意事項と本製品を使う前の必要な準備について説明しています。まず、この取扱説明書をよくお読みのうえ、安全に製品をご使用ください。お読みになったあとは、いつでも見られるところに必ず保管してください。



製品取り扱い時のご注意

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

◆ 下記事項は、安全のために必ずお守りください。



-
- 安全のための注意事項を守る
注意事項をよくお読みください。製品全般の注意事項が記載されています。
 - 故障したら使わない
すぐに販売店まで修理をご依頼ください。
 - 万一異常が起きたら
 - ◆ 煙が出たら
 - ◆ 異常な音、においがしたら
 - ◆ 内部に水・異物が入ったら
 - ◆ 製品を高所から落としたり、破損したとき

電源を切る（電源コードを抜く）
接続ケーブルを抜く
販売店に修理を依頼する

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



- 電源ケーブルや接続ケーブルを傷つけない
 - ◆ 電源ケーブルを傷つけると火災や感電の原因となります。
 - ◆ 重いものをのせたり、引っ張ったりしない。
 - ◆ 加工したり、傷つけたりしない。
 - ◆ 熱器具の近くに配線したり、加熱したりしない。
 - ◆ 電源ケーブルを抜くときは、必ずプラグを持って抜く。
- 内部に水や異物を入れない
 - ◆ 火災や感電の原因となります。
 - ◆ 万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。
- 内部をむやみに開けない
 - ◆ 本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。
- 落雷が発生したらさわらない
 - ◆ 感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。
- 油煙、湯気、湿気、ほこりの多い場所には設置しない
 - ◆ 本書に記載されている使用条件以外の環境でのご使用は、火災や感電の原因となります。

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



- ぬれた手で電源プラグやコネクタに触らない
感電の原因となります。
 - 指定された電源コードや接続ケーブルを使う
マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。
 - 指定の電圧で使う
マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。
 - コンセントや配線器具の定格を超えるような接続はしない
発熱による火災の原因となります。
 - 通風孔をふさがない
 - ◆ 通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。
 - ◆ 毛足の長いジュウタンなどの上に直接設置しない。
 - ◆ 布などでくるまない。
 - 移動させるときは、電源ケーブルや接続ケーブルを抜く
接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。
-

目次

1.	コマンドラインインタフェース	3
1.1	CLI へのアクセス	3
1.2	コマンド	5
1.2.1	基本コマンド	5
	backup - バックアップ	5
	logout (exit) - ログアウトコマンド	5
	Ping コマンド	6
	Reset	6
1.2.2	各種コマンド	7
	admin - 管理ユーザ設定	7
	arl - ARL テーブル	8
	eth0 - IP 設定	9
	idle - アイドルタイム	10
	igmp - IGMP snooping	10
	mirror - ポートミラーリング	11
	mvr - MVR (Multicast VLAN Registration)	13
	age - エージングタイム	15
	automode - オートモード	15
	loopback - ループバック検出機能	16
	mgr - 管理者グループのアクセス権	17
	port - ポート設定	18
	qos - Quality of Service	19
	snmp - SNMP (Simple Network Management Protocol)	22
	trunk - トランク	23
	sta - スパニングツリープロトコル	24
	http - HTTP アクセス	26
	gvrp - GVRP (GARP VLAN Registration Protocol)	27
	1qvlan - 802.1QVLAN	28
	dot1x - 802.1X	30
	security - セキュリティ	32
	ratecontrol - レートコントロール	34
	stormcontrol - ストームコントロール	36
	telnet - Telnet	37
	show dynamic - 動的 MAC アドレステーブルの表示	37
	show cfg - 機器情報の表示	38
	show statistics - 統計情報の表示	38
2.	Web インタフェースからの設定	39
2.1	Web インターフェースへの接続	39
2.2	Web インターフェースの操作方法	40

2.2.1	パネルの表示	40
2.2.2	設定	40
2.3	システム設定	41
2.4	Admin 設定	43
2.5	ポート設定	44
2.6	スパニングツリー	45
2.7	MAC アドレステーブル	46
2.7.1	Dynamic MAC Address Table	46
2.7.2	静的 MAC アドレステーブル	47
2.7.3	Mac セキュリティ	48
2.8	VLAN	49
2.8.1	VLAN 設定	49
2.8.2	Static 802.1Q VLAN	51
2.8.3	VLAN テーブル	52
2.9	802.1x 設定	53
2.10	トランク	55
2.11	ポートミラーリング	56
2.12	QoS	57
2.13	レートコントロール	60
2.14	ストームコントロール	61
2.15	Telnet	62
2.16	SNMP	62
2.17	IGMP	62
2.18	MVR	63
2.18.1	MVR VLAN	63
2.18.2	MVR グループ	65
2.19	ポート統計情報	66
2.20	システム管理	67

1. コマンドラインインタフェース

1.1 CLI へのアクセス

コンソールポートへの接続は以下の手順で行います。

- (1) 本機のコンソールポートと、PC のシリアルポートを、コンソールケーブルで繋ぎます。
- (2) ターミナルソフトウェアを起動します。設定を以下の通り行ってください。

```
通信ポート ----- RS-232C ケーブルが接続されているポート  
                    ( COM ポート 1 又は COM ポート 2 )  
通信速度 ----- 38400 ボー ( baud )  
データビット ----- 8bit  
ストップビット ----- 1bit  
パリティ ----- なし
```

- (3) 本機の電源を入れます。
接続が確立されると初期化が行われた後、以下の画面が表示されます。

```
Booting Program Version 1.02.00, built at 08:42:45, Mar 30 2004  
  
RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available  
FLASH: 0x05800000 - 0x05900000, 16 blocks of 0x00010000 bytes each.  
==> enter ^C to abort booting within 3 seconds .....
```

Start to run system initialization task

```
[System Configuration]  
Company Name      :  
Model Name       : 8-Port Switch  
MAC Address      : 00:C0:F6:64:22:29  
Firmware Version : 2.10.14 < Mar 1 2005 16:44:22 >
```

Press <ENTER> key to start.
UCD-SNMP version 4.1.2

```
Username:  
Password:
```

- (4) “Enter” キーを押すと、ユーザー名とパスワードが要求されます。
ユーザー名、パスワードの変更を行っていない場合には以下の値を入力してください。

```
Username:admin / Password:123456
```

[注意] 安全のために CLI へログイン後 P7 「admin - 管理ユーザ設定」コマンドを使用してパスワードの変更を行ってください。

- (5) スイッチにログイン後、プロンプトが表示されます。
“?” または “help” コマンドで、本機で使用可能なコマンドリストを確認することができます。

例

```
8-Port Switch>help
[Command List]
?..... Help commands
backup..... backup run-time firmware or configuration file
del..... Del commands
find..... Find commands
exit..... Logout
help..... Help commands
logout..... Logout
ping..... Ping a specified host with IP address
reset..... Reset system or reset factory default setting
set..... Set commands
show..... Show commands
upgrade..... Upgrade run-time firmware or configuration file
```

Telnet 接続経由での管理も、コンソール接続と同じインタフェースを使用します。

1.2 コマンド

1.2.1 基本コマンド

backup - バックアップ

本機は TFTP プロトコルによる、ファームウェア及び設定ファイルのダウンロード・アップロードをサポートしています。

まずファームウェアまたはコンフィグレーションを選択し、TFTP サーバの IP アドレス、バックアップを行うファイル名を指定します。

文法

backup [firmware | config] { *IP address* } { *filename* }

- ◆ firmware | config - ファームウェア、設定ファイルのどちらかを指定します。
- ◆ *IP address* - TFTP サーバの IP アドレスを指定します。
- ◆ *filename* - ファイル名の指定。任意の文字列を入力します。

例

```
8-Port Switch>backup firmware 192.168.1.10 config_backup
Start to upload run-time firmware file.....OK.
```

logout (exit) - ログアウトコマンド

ログイン中のユーザーからログアウトし、セッションを終了します。
logout と exit は同様の動作を行います。

例

```
8-Port Switch>logout

Press <ENTER> key to start.

Username:
```

Ping コマンド

ネットワーク上の他のノードにたいし、ICMP echo リクエストを送信します。

文法

ping -n {count} -l {length} -t -w {timeout} ip address

- ◆ -n {count} - 送信するパケット数を指定
- ◆ -l {length} - パケットのサイズを指定 (64~8148bytes)
- ◆ -t - この引数を付けると、「Esc」キーを押すまで Ping を送信し続けます。
- ◆ -w {timeout} - 各応答までの待ち時間を指定 (ミリ秒)
- ◆ ip address - 送信先 IP アドレス

例

ノード「192.168.1.7」へ 175bytes のパケットを 1 回送信します。

```
8-Port Switch>ping -n 1 -l 175 192.168.1.7
PING server 192.168.1.7
175 bytes from 192.168.1.7: icmp_seq=0, time<10ms
Sent 1 packets, received 1 OK, 0 bad
```

Reset

本機の再起動及び、設定を工場出荷状態に戻す際に使用します。

文法

reset [configuration | system]

- ◆ configuration - 設定内容を工場出荷状態に戻し、再起動を行います。
- ◆ system - 本機の再起動を行います。設定内容は保持されます。

例

本機の再起動を行います。

```
8-Port Switch>reset system
Reset system.....8-Port Switch>+
Booting Program Version 1.02.00, built at 08:42:45, Mar 30 2004

RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05900000, 16 blocks of 0x00010000 bytes each.
==> enter ^C to abort booting within 3 seconds .....

Start to run system initialization task

[System Configuration]
Company Name      :
Model Name       : 8-Port Switch
MAC Address      : 00:C0:F6:64:22:29
Firmware Version : 2.10.14 < Mar 1 2005 16:44:22 >
```

1.2.2 各種コマンド

admin - 管理ユーザ設定

管理者のユーザー名とパスワードを変更します。

文法

set admin

初期設定

username : admin

password : 123456

例

ユーザー名を「fxc123」パスワードを「56789」に変更します。

```
8-Port Switch>set admin

Input Old Username: admin
Input Old Password:

Input New Username: fxc123
Input New Password:
Confirm Password:
Successful to set new username and password!
```

[注意] 安全の為、初期設定パスワードの変更を行ってください。

[注意] 入力したパスワードは表示されません。

arl - ARL テーブル

本機の持つ ARL テーブルへ、MAC アドレスを静的に追加します。

本コマンドで作成した ARL テーブルを基に、“set security” コマンドの設定が反映されます。

“del arl” コマンドにより、登録した MAC アドレスを削除できます。

“show arl” コマンドを使用して、現在の ARL テーブルの内容を確認できます。

文法

set arl { MAC Adress } { port# }

del arl { MAC Adress } { port# }

find arl { MAC Adress }

show arl { MAC Adress }

- ◆ MAC Adress - MAC アドレスを指定
- ◆ port# - ポート番号を指定
- ◆ **find arl** - ARL テーブルから、MAC アドレスを検索します。
- ◆ **show arl** - ARL テーブルを表示します。

例

ARL テーブルにポート 6 の静的 MAC ID “00-00-01-02-03-35” を追加します。

```
8-Port Switch>set arl 00-00-01-02-03-35 6
Setting Static Mac is Successful!
```

ポート 5 の静的 MAC ID “00-00-01-02-03-33” を削除します。

```
8-Port Switch>del arl 00-00-01-02-03-33 5
Successful!
```

ARL テーブルを表示します。

```
88-Port Switch>show arl
Index  Port      Mac Address
=====
   1    3      00-12-15-15-10-20
   2    6      00-00-01-02-03-35
   3    7      00-C0-F6-11-22-33
=====
```

ARL テーブルから MAC アドレス “00-C0-F6-11-22-33” を検索します。

```
8-Port Switch>find arl 00-C0-F6-11-22-33
This MAC [00-C0-F6-11-22-33] is STATIC in port [7]
```

関連する項目

security - セキュリティ (P32)

eth0 - IP 設定

IP アドレスに関連した設定を行います。

設定内容を確認する場合には“show net” コマンドを使用します。

文法

```
set eth0 dhcp [ enable | disable ] ip {IP address} netmask {netmask} gateway {gateway}
show net
```

- ◆ **dhcp** [enable | disable] - DHCP サーバーからの自動設定を有効 / 無効
- ◆ **ip** {IP address} - IP アドレスを指定
- ◆ **netmask** {netmask} - サブネットマスクを指定
- ◆ **gateway** { gateway } - デフォルトゲートウェイのアドレスを指定
- ◆ **show net** -IP アドレス関連の設定内容を表示。

[注意] 本機に接続するノードが、同じサブネット上にない場合は、デフォルトゲートウェイの設定が必要です。

初期設定

DHCP : Disable (無効)

IP Address : 192.168.1.5

Netmask : 255.255.255.0

Gateway : 192.168.1.120

例

DHCP サーバーを無効、IP アドレスを 192.168.2.35、サブネットマスクを 255.255.255.0、デフォルトゲートウェイを 192.168.2.254 に設定しています。

```
8-Port Switch>set eth0 dhcp disable ip 192.168.2.35 netmask
255.255.255.0 gateway 192.168.2.254
Set DHCP client Disable successful!
Set IP address successful!
Set default gateway successful!
8-Port Switch>show net
[eth0] Network Configuration:
DHCP      : DISABLE
IP Address: 192.168.2.35
Netmask   : 255.255.255.0
Gateway   : 192.168.2.254
```

idle - アイドルタイム

本機では、CLIまたはWebインタフェースでの操作が一定時間行われなかった場合、自動的にログアウトを行う機能を備えています。本コマンドで、自動ログアウトが行われるまでの時間を設定できます。

文法

```
set idle { timeout value }
```

- ◆ *timeout value* - 自動ログアウトを実行するまでの秒数を指定します (30-3600 秒)

初期設定

600 秒 (10 分)

例

自動ログアウト - アイドルタイムアウトの時間を 20 分 (1200 秒) に設定します。

```
8-Port Switch>set idle 1200
Set idle time 1200 seconds successfully.
```

igmp - IGMP snooping

IGMP snooping を使用し、特定のマルチキャストサービスを受けたいホストにたいしてクエリを実行します。リクエストをしているホストが所属しているポートを特定し、それらのポートにのみデータを送ります。設定内容を確認する場合には "show igmp" コマンドを使用します。

文法

```
set igmp [ enable | disable ]
```

```
show igmp
```

- ◆ **igmp** [enable | disable] - IGMP snooping 機能を有効 / 無効にします。
- ◆ **show igmp** - IGMP snooping 設定情報を表示します。

初期設定

disable (無効)

例

IGMP snooping を有効にします。その後に IGMP 情報を表示します。

```
8-Port Switch>set igmp enable
IGMP function is enabled!
8-Port Switch>show igmp
[IGMP Configuration]
IGMP Switch      : Enabled
Total Groups     : 1
=====
[Group 1] IP Address : 239.0.0.1
      Member Port: 8
=====
```

mirror - ポートミラーリング

ポートミラーリングはネットワーク管理者にトラフィックの監視機能を提供します。監視対象のポートからパケットのコピーが転送され、監視をおこなうポートがこれらすべてのパケットを受信し、指定したポートでトラフィックの監視が可能になります。

文法

set mirror ingress div {value} mode [all | sa | da] mac {MAC Address} monitor {Port#}

set mirror egress div {value} mode [all | sa | da] mac {MAC Address} monitor {Port#}

- ◆ **ingress** - 入力パケットのキャプチャ
- ◆ **egress** - 出力パケットのキャプチャ
- ◆ **div {value}** - 全トラフィックのうち、採取するパケットの割合を指定。"10"と指定した場合、10パケット毎に1つのパケットのみを採取。全てのパケットを採取する場合には"1"を指定。
- ◆ **mode [all | sa | da]** - モニタリングするパケットのモードを選択します。
 - all : 全てのパケットをモニタリング。
 - sa : 送信元 MAC アドレスを指定してモニタリング。
 - da : 送信先 MAC アドレスを指定してモニタリング。
- ◆ **mac {MAC Address}** - モニタリングする送信元 / 送信先の MAC アドレスを指定 (mode で SA または DA を選択した場合のみ)
- ◆ **monitor {Port#}** - 被モニタリングポート (監視ポート) を指定します。"," で区切ることで、複数のポートを指定可能です。

set mirror port {Port#}

- ◆ **{Port#}** - モニタリングポート (監視ポート) を指定します。(1ポート)

set mirror [enable | disable]

- ◆ **[enable | disable]** - ポートミラーリング機能の有効 / 無効を指定。

del mirror

- ◆ ポートミラーリング機能を無効にします。

show mirror

- ◆ ミラーポートの設定情報を表示します。

初期設定

ミラーリング機能 : disable (無効)

例

ポートミラーリング機能を有効にし、ポート 5,6,7 番から出る全パケットの内、送信先 MAC アドレスが 00-c0-f6-11-22-33 のパケットをポート 8 番にてモニタリングします。
その後、ミラーポートの設定情報を表示しています。

```
8-Port Switch>set mirror enable
Enable mirror function successful!
8-Port Switch>set mirror port 8
Set mirror capture port successful!
Mirror capture port = 8
8-Port Switch>set mirror egress mode da mac 00-c0-f6-11-22-33
monitor 5,6,7
Set Egress mode successful!
Set Egress mac successful!
Set Egress monitor port successful!
Egress Monitor Port List: 5 6 7
8-Port Switch>show mirror
[Mirror Configuration]
Mirror Switch:Enabled
Capture port :8
Ingress DIV=1      Mode=ALL  MAC=00-00-00-00-00-00
      Port List:
Egress  DIV=1      Mode=DA   MAC=00-C0-F6-11-22-33
      Port List: 5 6 7
```

mvr - MVR (Multicast VLAN Registration)

MVR (Multicast VLAN Registration) 機能を設定します。

VLAN 機能は VLAN グループの間でトラフィックを分離します。しかしこの機能は同時に、異なる VLAN に所属するサブスクリバの IP マルチキャストトラフィックを分離します。MVR 機能は異なる VLAN に所属するサブスクリバが、1つの IP マルチキャスト VLAN を共有することを可能にします。これは VLAN のマルチキャストトラフィックを減少させます。

MVR 機能を使うためには、最初に IGMP Snooping 機能を有効にする必要があります。

本機は 4 つの MVR VLAN をサポートします。それらはインデックス 1,2,3,4 として参照されます。MVR 設定のいずれかを、コマンドを使ってインデックスに割り当てる必要があります。またすべての設定はインデックスされた MVR VLAN として割り当てられます。設定内容を確認する場合には "show mvr" コマンドを使用します。

文法

set mvr {vlan #} {active #} {name #} {vid #} {priority #} {mode #} {source # #} {receiver # # #}

- ◆ *vlan #* [1-4] - MVR VLAN のインデックスを指定します
- ◆ *active #* [1:Enable 0:Disable] - MVR VLAN を有効か無効かに設定します
- ◆ *name #* - MVR VLAN 名を設定します。
- ◆ *vid #* [1-4094] - MVR VLAN の VLAN ID を設定します
- ◆ *priority #* [0-7] - 802.1p の優先度を設定します。この VLAN の IGMP 管理パケットにタグが付加されているとき、ここで設定した優先度が割り当てられます。
- ◆ *mode #* [1:Dynamic 2:Compatible] - MVR 機能には 2 つの動作モードがあります。
1 つはダイナミックモード、もう 1 つはコンパチブルモードです。
ダイナミックモードでは、本機は MVR VLAN のすべての MVR ソースポートに IGMP Reports パケットを送信します。
コンパチブルモードでは、本機は IGMP Reports パケットを送信しません。(1 : ダイナミックモード 2 : コンパチブルモード)
- ◆ *source #* [Port1-8] # [0:untagged 1:tagged] - IP マルチキャストトラフィックの送信元である MVR VLAN のアップリンクポートを設定します。またポートがタグ付きかタグなしかを設定します。
- ◆ *receiver #* [+,-]# [Port1-8] # [0:untagged 1:tagged] - MMVR VLAN の IP マルチキャストトラフィックを受信するサブスクリバが接続されたポートを指定します。+,- オプションを使うことで MVR の受信ポートを追加、削除することができます。

MVR VLAN を設定した後、設定した MVR VLAN に IP マルチキャストグループを割り当てることができます。1 つの MVR VLAN に複数の IP マルチキャストグループを割り当てることができます。これらの IP マルチキャストグループはインデックスとして扱われます。

set mvr {group #} {active #} {index #} {name #} {start #} {end #}

- ◆ *group #* - IP マルチキャストグループのインデックスを指定します
- ◆ *active #* [1:Enable 0:Disable] - IP マルチキャストグループを有効か無効かに設定します。
- ◆ *index #* [1-4] - IP マルチキャストグループを割り当てる MVR VLAN を指定します
- ◆ *name #* [1-4094] - IP マルチキャストグループの名前を設定します
- ◆ *start #* [IP Address] - IP マルチキャストグループの始点の IP マルチキャストアドレスを指定します
- ◆ *end #* [IP Address] - IP マルチキャストグループの終点の IP マルチキャストアドレスを指定します

MVR VLAN と IP マルチキャストグループの両方を設定した後、MVR の受信ポートに接続されたサブスライバはそれらが異なる VLAN に所属していても、ソースポートから IP マルチキャストグループの範囲内で IP マルチキャストトラフィックを受信することができます。

show mvr [vlan | group]

このコマンドは現在の MVR の設定を表示します。
実行すると 4 つの MVR VLAN の設定を次々に表示します。

例

```
8-Port Switch>set mvr vlan 4 active 0 name 123 vid 2 priority 3 mode 1
set mvr vlan 4 active 0 name 123 vid 2 priority 3 mode 1
Set Multicast VLAN 4 inactive successful!
Set name of multicast VLAN successful!
Set vid of multicast VLAN successful!
Set priority of multicast VLAN successful!
Set mode of multicast VLAN successful!
```

age - エージングタイム

MAC アドレスのエージングタイムを設定します。

文法

age { *time* }

- ◆ *time* - エージングタイムを指定 (0-65535 秒 0 : エージング機能の無効)

初期設定

300 秒

例

MAC アドレスエージングタイムを 600 秒 (10 分) に設定します。

```
8-Port Switch>set age 600
Successful to set aging time
```

automode - オートモード

ポートのオートモード機能を設定します。本機には 2 種類のオートモードがあります。

- ◆ an mode - auto negotiation mode
対向の機器のオートネゴシエーション機能が無効になっている場合は an mode を選択します。
- ◆ ad mode - auto detection mode
対向の機器のオートネゴシエーション機能が有効の場合は ad mode を選択します。どちらのモードを選択するかは、各ネットワーク構成によって異なります。ほとんどのケースでは ad モードが推奨されています。

文法

set automode [an | ad]

show automode

- ◆ an - オートネゴシエーションモード
- ◆ ad - オートディテクションモード

初期設定

Auto Detect

例

オートモードをオートディテクションモードに設定します。

```
8-Port Switch>set automode ad
Set auto mode as "Auto Detect" successful!
8-Port Switch>show automode
[Auto Mode]: Auto Detect
```

loopback - ループバック検出機能

このコマンドはスイッチのループバック検出機能を設定します。機器が接続されたポートでループバック状態が発生した場合、送信されたすべてのパケットはスイッチに戻り、スイッチ上でパケットストームが引き起こされます。それはスイッチを不安定な状態にします。この機能を有効にするとループバック状態が発見されたとき、スイッチはそのポートを無効にします。ループバック状態から回復した後、"release" コマンドを実行するとポートを有効にすることができます。内容を確認する場合には "show loopback" コマンドを使用します。

文法

set loopback [enable | disable | release]

show loopback

- ◆ enable - ポート上でループバック機能を有効にします
- ◆ disable - ポート上でループバック機能を無効にします
- ◆ release - ループバック状態が検出されたポートのブロック状態を解除します
- ◆ **show loopback** - loopback の設定情報を表示します

初期設定

disable (無効)

例

loopback 検出機能を有効に設定後、ポートのリリースを実行し、ループバック設定情報を表示しています。

```
8-Port Switch>set loopback enable
Enable Loopback Detection successful!
8-Port Switch>set loopback release
Release all locked port successful!
8-Port Switch>show loopback
[Loopback Detection Function]:
Loopback Status      : Disable
Current Blocked ports: None
```

[注意] この機能は UTP ポートをループバックから防ぐために有効です。

mgr - 管理者グループのアクセス権

このコマンドは本機の管理のため、管理者グループと管理者グループのアクセス権を設定するために使用します。管理者を特定の IP アドレスと特定の IP サブネットに限定することができます。異なる管理者に、本機を管理するための異なるアクセス権を割り当てることができます。これにより本機のセキュリティを実現します。この機能では 4 つのユーザーグループをサポートします。内容を確認する場合には “show mgr” コマンドを使用します。

文法

```
set mgr [ enable | disable ] { index }
```

```
set mgr ipaddr { index } { IP Addr } { Net Mask }
```

```
set mgr mode { index } { Mode Type }
```

```
set mgr protocol { index } { 1 | 0 : http } { 1 | 0 : telnet } { 1 | 0 : snmp }
```

```
show mgr
```

- ◆ **mgr** [enable | disable] - 機能を有効 / 無効にします
 - *index*[1-4] : 設定を行うインデックスを指定します
- ◆ **ipaddr** - アクセスを許可する IP アドレス、サブネットマスクを設定します
 - *index*[1-4] : 設定を行うインデックスを指定します
 - *IP Addr* : IP アドレスを設定します
 - *Net Mask* : サブネットマスクを設定します。特定の IP アドレスからのアクセスのみ受け付ける場合は 255.255.255.255 を指定します。特定のサブネットからのアクセスを受け付ける場合は 255.255.255.255 以外を指定します
- ◆ **mode** - 指定した管理者のアクセス方式を設定します
 - *index*[1-4] : 設定を行うインデックスを指定します
 - *Mode Type*[1-2] : アクセス方式を指定します。1 を設定すると、そのインデックスの IP アドレスからのアクセスで設定を閲覧することができます。2 を設定すると、そのインデックスの IP アドレスからのアクセスで設定の閲覧と変更を行うことができます。
- ◆ **protocol** - 指定した管理者のリモートマネジメントの有効・無効の設定をします
 - *index* [1-4] : 設定を行うインデックスを指定します
 - 1 | 0 : *http* : Http アクセスの有効・無効の設定を行います。
1 で有効、2 で無効に設定できます
 - 1 | 0 : *telnet* : Telnet アクセスの有効・無効の設定を行います。
1 で有効、2 で無効に設定できます
 - 1 | 0 : *snmp* : SNMP アクセスの有効・無効の設定を行います。
1 で有効、2 で無効に設定できます
- ◆ **show mgr** - mgr の設定情報を表示します

例

インデックス 1 のモードタイプを 1、HTTP、Telnet、SNMP を全て有効にしています。

```
8-Port Switch>set mgr mode 1 1
Set access mode View for set 1 successful!
8-Port Switch>set mgr protocol 1 1 1 1
Set access protocol for set 1 successful!
```

port - ポート設定

本コマンドは、各ポートの設定を行います。
“show port” コマンドにて、ポートの設定状況及び、接続状態を表示します。

文法

```
set port { port# } name { name } admin [ enable | disable ] speed [ atuo | 10 | 100 | 1000 ]
duplex [ full | half ] flowctrl [ on | off ]
```

show port

- ◆ port { port# } - 設定を行うポートを指定。
- ◆ name { name } - ポート名を指定。
- ◆ admin [enable | disable] - ポートの有効 / 無効を指定。
- ◆ speed [atuo | 10 | 100 | 1000] - スピードを指定 (Autonegotiation, 10M, 100M, 1000M)
- ◆ duplex [full | half] - 通信モードを指定。(全二重、半二重)
- ◆ flowctrl [on | off] - フローコントロールの ON/OFF
- ◆ show port - ポートの設定情報および現在の接続情報を表示します。

初期設定

(全ポート)

名前 : 10/100M base-T 有効 / 無効 : 有効

通信速度・モード : オートネゴシエーション フローコントロール : OFF

例

ポート 1 番の名前を FXC_port1、speed/duplex を 100M Full、フローコントロール ON にし、ポート 2 番を無効にします。その後、ポートの現在の設定および状況を表示します。

```
8-Port Switch>set port 1 name FXC_port1 speed 100 duplex full flowctrl on
Set port name successful!
Set port speed successful!
Set port duplex successful!
Set port flow control successful!
8-Port Switch>set port 2 admin disable
Set port admin mode successful!
8-Port Switch>show port
[Port Configuration]
Port Name           Status  Disable  Auto.  Speed  Duplex  Flow
Control
1  FXC_port1         DOWN    NO       OFF    100    Full    ON
2  10/100M base-T    DOWN    YES      ON     10     Half    OFF
3  10/100M base-T    DOWN    NO       ON     10     Half    OFF
4  10/100M base-T    DOWN    NO       ON     10     Half    OFF
5  10/100M base-T    DOWN    NO       ON     10     Half    OFF
6  10/100M base-T    DOWN    NO       ON     10     Half    OFF
7  10/100M base-T    DOWN    NO       ON     10     Half    OFF
8  10/100M base-T    DOWN    NO       ON     10     Half    OFF
```

qos - Quality of Service

本機はポートベース、802.1p、ToS/DiffServ の優先度をサポートしています。それぞれのポートには4つの優先度（P0～P4）があります。それぞれのポートのトラフィックの順位決めには優先度の高いパケットを優先する SP(Strict Priority)、4つの優先度キューを使用する WRR(Weighted Round Robin) のどちらかを設定できます。

"show qos" コマンドで、現在の QoS の設定情報が表示できます。

文法

set qos [enable | disable]

set qos priority {port#} [high | low]

set qos flowctrl {port#} [on | off]

set qos 1p {port#} [on | off]

set qos mapping {priority tag} {queue}

set qos pm [wrr | sp]

set qos tdsel [tos | diffserv]

set qos dsport {port#} [on | off]

set dscp {dscp} {priority tag}

set dscp {tos} {queue}

show qos

- ◆ **qos** [enable | disable] - QoS の有効 / 無効を指定
- ◆ **priority** {port#} [high | low] - ポートベースの優先度を設定します。高い優先度が設定されたポートに入力されたパケットは常に最高の優先度（P3）のキューに転送されます。低い優先度が設定されたポートに入力されたパケットは常に最低の優先度（P0）のキューに転送されます。
 - port# : 設定するポートを指定します。
 - high | low : ポートの優先度を high または low に設定します。
- ◆ **flowctrl** {port#} [on | off] - このコマンドは QoS 機能が有効の場合に、ポートのフロー制御機能を有効にします。ポート設定にもフロー制御機能の有効・無効にする項目があります。これに関しては下の表を参照してください。

"set qos" でフロー コントロールを有効	"set port" でフロー コントロールを有効	フローコントロールオペレーション
有効	有効	有効
有効	無効	無効
無効	有効	無効
無効	無効	無効

フロー制御機能が有効の場合、本機はトラフィックが混雑したときにパケットロスを防ぐためポーズフレームを送信します。フロー制御機能が無効の場合、本機はトラフィックが混雑したときにパケットを破棄します。

[注意] QoS 機能とフロー制御機能の動作は衝突します。実際の QoS 要求のため、混雑が起こった場合に本機に入力されたパケットを優先度に基づいて転送させるためにはフロー制御機能を無効にしてください。

- *port#* : 設定するポートを指定します。
 - *on | off* : フロー制御機能を有効 / 無効に設定します。
- ◆ **1p** { *port#* } [*on | off*] - ポート上で 802.1p の優先度を有効・無効に設定します。
 - *port* : 設定するポートを指定します。
 - *on | off* : 802.1p の優先度を有効 / 無効にします。
 - ◆ **mapping** { *priority tag* } { *queue* } - 802.1p の優先度(0 ~ 7)を 4 つの優先度キューに割り当てます。
 - *priority tag* : 優先度キューを割り当てる 802.1p 優先度の値を設定します。
 - 割り当てる優先度キューを指定します。
 - ◆ **pm** [*wrr | sp*] - 優先度キューに入ったパケットを順位付けする方式を設定します。
 - *wrr* : 4 つの優先度キューにそれぞれ重み付けを行い、その重みの割合に応じて転送します。(P3 = 8、P2 = 4、P1 = 2、P0 = 1)
 - *sp* : 高い優先度を持つパケットを最初に転送します。
 - ◆ **tdsel** [*tos | diffserv*] - ToS 優先度か DiffServ 優先度を有効にします。
 - *tos* : ToS 優先度を有効にします。
 - *diffserv* : DiffServ 優先度を有効にします。
 - ◆ **dsport** { *port#* } [*on | off*] - ToS/DiffServ 機能を有効・無効に設定します。
 - *port#* : 設定するポートを指定します。
 - *on | off* : ToS/DiffServ 機能を有効 / 無効にします。
 - ◆ **set dscp** { *dscp* } { *priority tag* } - DSCP 値(0 ~ 63)を 802.1p 優先度(0 ~ 7)に割り当てます。すべての DSCP 値は 802.1p 優先度に割り当てることができます。
 - *dscp* (0-63) : 設定するポートを指定します。
 - *priority tag* (0-7)
 - ◆ **set dscp** { *tos* } { *queue* } - ToS 優先度(0 ~ 7)を優先度キュー(P0 ~ P3)に割り当てます。
 - *tos* (0-7) : 設定するポートを指定します。
 - *queue* : 割り当てる優先度キューを指定します。
 - ◆ **show qos** - QoS の設定情報を表示します。

初期設定

```
[Qos setting]   Disable   802.1p Priority
Tag7=P3,Tag6=P3,Tag5=P2,Tag4=P2,Tag3=P1,Tag2=P1,Tag1=P0,Tag0=P0
[Priority]      全ポート : Low
[フローコントロール]  全ポート : OFF
[802.1P]       全ポート : OFF
```

例

QoS 機能を有効にし、ポート 3 番のプライオリティを High に設定、フローコントロールを ON、プライオリティタグの 3 を P3 にマッピングします。その後に QoS の設定情報を表示します。

```
8-Port Switch>set qos enable priority 3 high flowctrl 3 on mapping 3 3
Qos setting = Enabled
Set port priority successful!
Port 3 flow control status = ON!
Mapping 802.1p Priority Tag 3 to P3
8-Port Switch>show qos
[QoS Configuration]
Qos setting      : Enabled
=====
802.1p Priority Tag 7 ==> P3
802.1p Priority Tag 6 ==> P3
802.1p Priority Tag 5 ==> P2
802.1p Priority Tag 4 ==> P2
802.1p Priority Tag 3 ==> P3
802.1p Priority Tag 2 ==> P1
802.1p Priority Tag 1 ==> P0
802.1p Priority Tag 0 ==> P0
=====
Port  Priority  Port  Priority  Port  Priority  Port  Priority
[ 1]    Low     [ 2]    Low     [ 3]    High    [ 4]    Low
[ 5]    Low     [ 6]    Low     [ 7]    Low    [ 8]    Low
=====
Port  FlowCtrl  Port  FlowCtrl  Port  FlowCtrl  Port  FlowCtrl
[ 1]   OFF     [ 2]   OFF     [ 3]   ON     [ 4]   OFF
[ 5]   OFF     [ 6]   OFF     [ 7]   OFF    [ 8]   OFF
=====
Port  802.1p  Port  802.1p  Port  802.1p  Port  802.1p
[ 1]   OFF   [ 2]   OFF   [ 3]   OFF   [ 4]   OFF
[ 5]   OFF   [ 6]   OFF   [ 7]   OFF   [ 8]   OFF
=====
```

snmp - SNMP (Simple Network Management Protocol)

本機の SNMP 機能を設定します。

"show snmp" で SNMP の現在の設定内容を表示します。

文法

```
set snmp name { name }
set snmp location { location }
set snmp contact { contact }
set snmp getcommunity { community name }
set snmp setcommunity { community name }
set snmp trapcommunity { index } {community name }
set snmp trapip { index } { trapip }
set snmp txtrap { index }
show snmp
```

- ◆ **name** { name } - 本機の名称を指定します。
- ◆ **location** { location } - 本機の設置場所を指定します。
- ◆ **contact** { contact } - 本機にトラブルが発生した場合の連絡先を指定します。
- ◆ **getcommunity** { community name } - Get コミュニティ名を指定します。
- ◆ **setcommunity** { community name } -Set コミュニティ名を指定します。
- ◆ **trapcommunity** { index } {community name }
 - *index* : Trap コミュニティ名を設定するインデックスを指定します。
 - *community name* : 指定したインデックスに Trap コミュニティを設定します。
- ◆ **trapip** {index} {trapip} - 802.1p の優先度(0 ~ 7)を 4 つの優先度キューに割り当てます。
 - *index* : Trap の送信先 IP アドレスを設定するインデックスを指定します。
 - *trapip* : 指定したインデックスに Trap を送信する IP アドレスを設定します。
- ◆ **txtrap** {index} - Trap をテスト送信します。テスト送信をするインデックスを指定します。

例

```
8-Port Switch>set snmp name ABC location AAA-1F contact JACK
Set SNMP system name successful!
Set SNMP system location successful!
Set SNMP system contact name successful!
```

trunk - トランク

本機は最大 4 つのトランクグループをサポートしています。
トランクグループは初期状態では無効になっています。
“show trunk” で、現在の設定情報が表示されます。“del trunk” で、トランクを削除できます。

文法

set trunk [enable | disable]

set trunk { +, - } { port# } { trunk }

del trunk { trunk number }

show trunk

dell trunk { trunk# }

- ◆ **trunk** { enable | disable } - トランク機能の有効 / 無効を指定。
- ◆ { +, - } { port# } - 追加したいポート番号を " + " の後に入力。トランクから削除したいポートを " - " の後に入力。
- ◆ { trunk } - 割り当てる対象のトランクグループを指定します。
- ◆ *trunk number* - 追加 / 削除するトランク番号を指定。
- ◆ **show trunk** - トランクの設定情報を表示します。
- ◆ **dell trunk** { trunk# } - 指定したトランクグループを削除します。

初期設定

disable (無効)

例

トランクを有効にし、ポート 1,3,5 をトランク 3 に追加後、トランク 3 からポート 3 を削除します。
その後にトランク 3 を削除します。

```
8-Port Switch>set trunk enable
Enable trunk function successful!
8-Port Switch>set trunk +1+3+5 3
Trunk Group 3 setting:
[TRUNK] [Port List]
=====
[ 3]    1  3  5
=====
8-Port Switch>set trunk -3+7 3
Trunk Group 3 setting:
[TRUNK] [Port List]
=====
[ 3]    1  5  7
=====
8-Port Switch>del trunk 3
OK to destroy trunk group 3
```

sta - スパニングツリープロトコル

本機でスパニングツリープロトコルの設定を行います。本機は STP (802.1d) と互換性のある RSTP (802.1w) を使用することができます。

“show sta” で、現在の設定情報が表示されます。

文法

set sta [enable | disable]

set sta bridge priority { *priority* } **hello** { *hello time* } **age** { *maximum age* } **delay** { *delay time* }

set sta port { *port#* } [enable | disable] **cost** { *cost* } **priority** { *priority* }

show sta

- ◆ **set sta** [enable | disable] - スイッチのスパニングツリー機能有効 / 無効を設定します。
- ◆ **sta bridge**
 - **priority** { *priority* } : ルートデバイス、ルートポート、指定ポートを選択するために必要なブリッジプライオリティを設定します (0-65535)。最も高いプライオリティ (priority が最も低い) を持つデバイスはスパニングツリープロトコルのルートデバイスになります。すべてのデバイスが同じプライオリティの場合、最も低い MAC アドレスを持つデバイスがルートデバイスになります。
 - **hello** { *hello time* } : 本機がスパニングツリーのルートデバイスの場合に、スパニングツリー管理パケットを送信する間隔を設定します。(1-10)
 - **age** { *maximum age* } : スパニングツリー管理パケットを受信していない場合のスパニングツリーのエイジングタイムを設定します。これはスパニングツリーの再作成を引き起こします。初期状態では 20 秒です。(6-40)
 - **delay** { *delay time* } : スパニングツリーの状態を変更 (リスニング状態からラーニング状態への移行) する前の最大待ち時間を設定します。この設定が必要とされるのは、すべてのデバイスがフレームの転送を始める前にトポロジの変更についての情報を受信する必要があるからです。加えて、各ポートはブロッキング状態に再び戻るような衝突情報 (一時的なデータループの発生など) を検知するための時間が必要です。(4-30)
- ◆ **sta port**
 - { *port#* } : ポート番号を指定します。
 - [enable | disable] : ポートごとの、STA 有効 / 無効を設定します。
 - **cost** { *cost* } : ループが発生した場合にデバイス間の最適経路を決定するためにこの値が使用されます。速度が速いポートには低い値が割り当てられ、パケットの転送が行われます。速度が遅いポートには高い値が割り当てられ、転送がブロックされます。推奨される値は 10M で 100 (50 ~ 600 の範囲)、100M で 19 (10 ~ 60)、1000M で 4 (3 ~ 10) です。
 - **priority** { *priority* } : ポートのプライオリティを設定します。スイッチ上のすべてのポートのパスコストが同じの場合、ループが発生したときに最も高いプライオリティ (priority が最も低い) のポートに転送されます。最も高いプライオリティのポートが複数ある場合、最も低いポート番号のポートに転送されます。(0-255)
- ◆ **show sta** - スパニングツリーの設定情報を表示します。

初期設定

STA : Disabled Bridge Priority : 32768 Bridge Hello Time : 2
Bridge Max Age : 20 Bridge Forward Delay : : 15 Port Priority : 128
Port Path Cost : 19 Port Status : Enabled

例

スイッチで STA を有効にし、ブリッジの設定を行います。その後にポート 3 を指定して、有効にした後、コスト / プライオリティの設定を行います。

```
8-Port Switch>set sta enable
Enable Spanning Tree function successful!
8-Port Switch>set sta bridge priority 100 hello 5 age 10 delay 5
Set priority successful!
Set hello time successful!
Set max age successful!
Set forward delay successful!
8-Port Switch>set sta port 3 enable
Enable Spanning Tree function of port 3 successful!
8-Port Switch>set sta port 3 cost 19 priority 100
Port 3 path_cost=19
Port 3 priority=100
```

http - HTTP アクセス

本機の HTTP を通した設定機能を有効・無効に設定します。ハッカーやワーム・ウイルスが頻繁に HTTP サーバーを攻撃しているならば、このコマンドで HTTP 機能を無効にしてください。

"show http" で、現在の設定情報が表示されます。

[注意] 本機がファイアウォール等の防御を行わずにインターネット環境下に接続されている場合、本機能で HTTP を無効にし、Telnet または SNMP からの管理を行うことを推奨します。

文法

set http [enable | disable]

show http

- ◆ enable | disable - HTTP 機能の有効 / 無効を設定します。
- ◆ **show http** - http 設定情報を表示します。

[注意] “set http” コマンド実行後、本機は自動的に再起動されます。

初期設定

Enable (有効)

例

HTTP 機能を無効に設定しています。

```
8-Port Switch>set http disable
Disable http function successful!
Reset system.....8-Port Switch>+
Booting Program Version 1.02.00, built at 08:42:45, Mar 30 2004

RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05900000, 16 blocks of 0x00010000 bytes
each.
==> enter ^C to abort booting within 3 seconds .....

Start to run system initialization task

[System Configuration]
Company Name      :
Model Name       : 8-Port Switch
MAC Address      : 00:C0:F6:64:22:29
Firmware Version : 2.10.14 < Mar  1 2005 16:44:22 >

Press <ENTER> key to start.
UCD-SNMP version 4.1.2

Username:admin
Password:
```

gvrp - GVRP (GARP VLAN Registration Protocol)

このコマンドは 802.1Q の GVRP 機能を有効・無効に設定します。この機能を有効にし、別の 802.1Q のネットワークデバイスからパケットを受信した場合、本機は 802.1Q VLAN を学習します。学習したリモートの 802.1Q VLAN はダイナミック 802.1Q VLAN テーブルに表示されます。

"show gvrp" で、現在の設定情報が表示されます。

文法

set gvrp [1:enable | 0:disable]

show gvrp

- ◆ 1:enable | 0:disable -GVRP の有効 / 無効を設定します。
- ◆ **show gvrp** - http 設定情報を表示します。

初期設定

Disable (無効)

例

GVRP を有効にします。

```
8-Port Switch>set gvrp 1
GVRP Protocol : Enabled
```

1qvlan - 802.1QVLAN

このコマンドは 802.1QVLAN の設定を行います。

"show 1qvlan" で、現在の設定情報が表示されます。

文法

set 1qvlan [*enable* | *disable*]

set 1qvlan ingressfilter [1 | 0]

set 1qvlan create { *VLAN ID* } { *VLAN name* }

set 1qvlan modify [+ | -]{ *Port#* } { *VLAN ID* } [1 : tagged | 0 : untagged]

set 1qvlan pvid { *Port#* } { *VLAN ID* } **mgrpvid** { *VLAN ID* } **priority** { *Port#* } { *priority* }

block { *Block VID* } **mode** [0: SVL mode | 1: IVL mode | 2: SVL/IVL mode]

del 1qvlan { *VLAN ID* }

show 1qvlan [*status* | *static* | *table* | *pvid*]

- ◆ **set 1qvlan** -1QVLAN の有効 / 無効を設定します。
 - ◆ **set 1qvlan ingressfilter** - イングレスフィルタリングの有効 (1)、無効 (0) を設定します。
 - ◆ **set 1qvlan create** - VLAN ID (1-4094) と VLAN 名を指定し、VLAN を作成します。
 - ◆ **set 1qvlan modify** - 作成した VLAN にポートを追加します。
 - [+ | -]{ *Port#* } : VLAN へポートを追加する場合は、ポート番号の前に「+」を付けます。削除をする場合は「-」を付けます。
 - *VLAN ID* : ポートを追加する VLAN の ID を指定します。
 - [1 | 0] : タグ付き、タグ無しを選択します。
 - ◆ **set 1qvlan pvid** - PVID 設定をおこないます。
 - *Port#* : 設定をおこなうポートを指定します。
 - *VLAN ID* : VLAN ID (1-4094) を設定します。
 - **mgrpvid** { *VLAN ID* } : マネージメント PVID を設定します。
 - **priority** { *Port#* } { *priority* } : タグプライオリティを設定します。
 - **block** { *Block VID* } : 802.1Q VLAN 機能にて、使用する VLAN ID の範囲を設定します。本機でサポートする VID は 1-4094 です。この VID は以下の表のように 8 つのブロックに分けられ、設定をしているブロックの VID のみがアクティブになります。
- | Block | Active VID | Block | Active VID |
|-------|-------------|-------|-------------|
| 0 | 1 ~ 511 | 4 | 2048 ~ 2559 |
| 1 | 512 ~ 1023 | 5 | 2560 ~ 3071 |
| 2 | 1024 ~ 1535 | 6 | 3072 ~ 3583 |
| 3 | 1536 ~ 2047 | 7 | 3584 ~ 4094 |
- **mode** [0: SVL mode | 1: IVL mode | 2: SVL/IVL mode] : VLAN モードを設定します。
 - ◆ **del 1qvlan** { *VLAN ID* } - VLAN ID を指定し、既存の VLAN を削除します。

- ◆ **show 1qvlan** - VLAN の各種設定を表示します。
 - *status* : VLAN ステータスを表示します。
 - *static* : 静的 VLAN テーブルを表示します。
 - *table* : 全ての VLAN テーブルを表示します。
 - *pvid* : PVID 情報を表示します。

初期設定

802.1Q VLAN : Enable Ingress Filter : Disable

Block : 0 Curent VLAN Mode : SVL

例

1QVLAN を有効にし、VLAN ID300、VLAN 名「fxc123」を作成し、ポート 5 番をタグポートとして追加します。その後に 1QVLAN テーブルを表示しています。

```
8-Port Switch>set 1qvlan enable
802.1Q VLAN : Enable
8-Port Switch>set 1qvlan create 300 fxc123
Create new 802.1Q VLAN successful with VID: 300(0x12c) and VLAN
Name: fxc123
8-Port Switch>set 1qvlan modify +5 300 1
8-Port Switch>show 1qvlan table
----- All 802.1Q VLAN Table -----

VLAN Type:    STATIC
VLAN ID   :    1(0x001) , VLAN Name: Default VLAN
Tagged Member Port   :
Untagged Member Port : 1 2 3 4 5 6 7 8

VLAN Type:    STATIC
VLAN ID   : 300(0x12c) , VLAN Name: fxc123
Tagged Member Port   : 5
Untagged Member Port :

----- Finish -----
```

dot1x - 802.1X

802.1X 機能の設定を行います。

“show dot1x” コマンドを使用して、現在の設定内容を確認できます。

文法

```
set dot1x [ enable | disable ] transparent re_au [ 0:disable | 1:enable ] reauthtime {count}
reauthcnt {count} reqcnt {count} sertime {period} supptime {period} quiettime {period}
txttime {period} rsip {IP Address} authport {port#} shkey {key} portauth {mode}
```

```
show dot1x [ config | radius | port ]
```

- ◆ **set dot1x** [*enable* | *disable*] - 802.1X の有効 / 無効を設定します。
- ◆ **transparent** - トランスピアレントモードに設定します。
- ◆ **re_au** [0:disable | 1:enable] - 802.1X 再認証を設定します。
- ◆ **reauthtime** { *period* } - 802.1X 再認証タイムアウトの間隔を設定します。
- ◆ **reauthcnt** { *count* } - 802.1X 再認証の回数を設定します。
- ◆ **reqcnt** { *count* } - 802.1X リクエストタイムの最大回数を設定します。
- ◆ **sertime** { *period* } - スイッチと RADIUS サーバ間のリクエストタイムアウト値を設定します。
- ◆ **supptime** { *period* } - スイッチとユーザ間のタイムアウト値を設定します。
- ◆ **quiettime** { *period* } - スイッチとユーザ間で、認証に失敗した際、次の認証プロセスまでの待ち時間を設定します。
- ◆ **txttime** { *period* } - スイッチからユーザへの認証リクエストのタイムアウト値を設定します。
- ◆ **rsip** { *IP Address* } - RADIUS サーバの IP アドレスを設定します。
- ◆ **authport** { *port#* } - 認証ポートを設定します。
- ◆ **shkey** { *key* } - スイッチと RADIUS サーバ間のセキュリティキーを設定します。
- ◆ **portauth** { *mode* } - 物理ポートの認証モードを設定します。
 - **auto** : ポートの認証結果に基づきます。
 - **fa** (Force-authenticated): ポートは常に認証状態になります。802.1X プロセスの結果は無視されます。
 - **fu** (Force-unauthenticated): ポートは常に非認証状態になります。802.1X プロセスの結果は無視されます。
 - **non** : 802.1X 無効。

◆ **show dot1x** [*config* | *radius* | *port*] -802.1X の設定情報を表示します。

- *config* : 802.1X 現在の設定内容を表示します。
- *radius* : RADIUS サーバに関する設定を表示します。
- *port* : ポート設定を表示します。

初期設定

802.1x Protocol : Disabled Re-authentication : Disabled
Re-authentication Timeout Period : 3600 Re-authentication Max Count : 2
Max Request Count : 2 Server Timeout Period : 30
Supplicant Timeout Period : 30 Quiet Timeout Period : 60
Tx Timeout Period : 30 Radius Server IP Address : 192.168.1.222
Radius Server Port Number : 1812 Security Key : 12345678

例

802.1X を有効にし、re_au を 3、RADIUS サーバ IP アドレスを 192.168.1.5 に設定しています。

```
8-Port Switch>set dot1x enable transparent re_au 1 txttime 3 rsip  
19  
2.168.1.5  
Enable 802.1x successful!  
Enable 802.1x re-authenticate function!  
Set re-authenticate time successful!  
Set transparent time successful!  
Set IP address of Radius server successful!
```

本機は MD5、TLS および PEAP の認証方式をサポートしています。

security - セキュリティ

arl コマンドにて、登録した MAC アドレスを基に、アクセス制御を設定します。

“show security” コマンドを使用して、現在の設定内容を確認できます。

文法

set security { port# } [1 (mode1) | 2 (mode2)]

show security

- ◆ port# - ポートを指定
- ◆ 1 (mode1) | 2 (mode2) - モードを指定します。
 - mode1 : Accept function 許可設定
許可設定を指定すると、ARL テーブルに指定されている MAC アドレスを持つノードからのみアクセスを許可します。
ARL テーブルのポート 1 に MAC アドレス 00-c0-f6-11-22-33 が登録されている状態でポート 1 に許可設定を適用した場合、00-c0-f6-11-22-33 からのアクセスのみが許可され、それ以外を全て拒否します。
 - mode2 : Reject function 拒否設定
拒否設定を指定すると、ARL テーブルに指定されている MAC アドレスを持つノードからのアクセスを拒否し、それ以外のノードからは全てアクセス可になります。
ARL テーブルのポート 1 に MAC アドレス 00-c0-f6-11-22-33 が登録されている状態でポート 1 に拒否設定を適用した場合、00-c0-f6-11-22-33 からのアクセスのみが拒否され、それ以外を全て許可します。
- ◆ show security - セキュリティの詳細情報を表示します。

初期設定

なし

関連する項目

arl - ARL テーブル (P8)

コマンドラインインタフェース コマンド

例

"show arl" にて現在の ARL テーブルを表示。ポート 5 にたいして mode1 を設定、ポート 3 にたいして mode2 を設定します。

```
8-Port Switch>show arl
Item  Port      Mac Address
=====
   1    5    00-40-26-B7-DB-12
   2    3    00-40-26-B5-13-11
   3    1    00-21-53-C3-AE-12
=====
8-Port Switch>set sec 5 1
[MAC Security Configuration]
=====
   Port      Static MAC Number      Security Control
=====
   1          1                      No Security
   2          0                      No Security
   3          1                      No Security
   4          0                      No Security
   5          1                      Accept function
   6          0                      No Security
   7          0                      No Security
   8          0                      No Security
=====
8-Port Switch>set sec 3 2
[MAC Security Configuration]
=====
   Port      Static MAC Number      Security Control
=====
   1          1                      No Security
   2          0                      No Security
   3          1                      Reject function
   4          0                      No Security
   5          1                      Accept function
   6          0                      No Security
   7          0                      No Security
   8          0                      No Security
=====
```

上記設定の結果、ポート 3 番は MAC アドレス 00-40-26-B5-13-11 からのアクセスのみ拒否し、それ以外の MAC アドレスからのアクセスは全て許可します。ポート 5 番は MAC アドレス 00-40-26-B7-DB-12 からのアクセスのみ許可し、それ以外の MAC アドレスからのアクセスは全て拒否します。

ratecontrol - レートコントロール

各ポートの最大トラフィックレートを設定します。

"show ratecontrol" コマンドで、現在の設定情報を表示します。

文法

set ratecontrol drop [0 | 1]

set ratecontrol {ingress | egress} {port} {rate}

show ratecontrol

- ◆ **drop** [0 | 1] - 入力トラフィックが、設定した最大レートを超えた場合の処理方法を指定します。
 - 1(drop enable) : パケットは破棄されます。
 - 0(drop disable) : パケットは破棄されず、フローコントロール処理が行われます。
- ◆ **ingress | egress** - 入力 (ingress) または出力 (egress) を指定。
- ◆ **port** - 設定を行うポートを指定。
- ◆ **rate** - レートを指定 (0-127)
 - 入力値 = 0 : : レートコントロールは無効になります。
 - 入力値 = 1~28 : 入力値 × 64kbps (例 入力値 15 : 960kbps)
 - 入力値 = 29~127 : (入力値 -27) × 1Mbps (例 入力値 108 : 81Mbps)
- ◆ **show ratecontrol** - レートコントロールの現在の設定を表示します。

初期設定

Packet Drop : disable (無効)

(全ポート) Ingress : disable (無効) Egress : disable (無効)

コマンドラインインタフェース コマンド

例

ポート 3 の入力にリミットレート 85Mbps を設定、ポート 5 の出力にレートリミット 192kbps を設定します。

```
8-Port Switch>set ratecontrol ingress 3 112
[Rate Control Configuration]
Packet Drop for Ingress Limit: Disable
=====
  Port          Ingress          Egress
=====
  1             Disable          Disable
  2             Disable          Disable
  3             85Mb            Disable
  4             Disable          Disable
  5             Disable          Disable
  6             Disable          Disable
  7             Disable          Disable
  8             Disable          Disable
=====
8-Port Switch>set ratecontrol egress 5 3
[Rate Control Configuration]
Packet Drop for Ingress Limit: Disable
=====
  Port          Ingress          Egress
=====
  1             Disable          Disable
  2             Disable          Disable
  3             85Mb            Disable
  4             Disable          Disable
  5             Disable          192Kb
  6             Disable          Disable
  7             Disable          Disable
  8             Disable          Disable
=====
```

stormcontrol - ストームコントロール

ストームコントロールの設定を行います。

本機は、ブロードキャストストーム、マルチキャストストーム、フラディングストームの各種コントロールに対応しています。

“show stormcontrol” コマンドでストームコントロール設定情報を表示します。

文法

set stormcontrol rate {rate} [bc | mc | fc]

show stormcontrol

- ◆ **rate** {rate} - ストームコントロールのレートを設定します。
 - rate 0 : コントロールレート 3.3%
 - rate 1 : コントロールレート 5%
 - rate 2 : コントロールレート 10%
 - rate 3 : コントロールレート 20%
- ◆ [bc | mc | fc] - 設定を適用するストームを指定します。
 - bc : (Broadcast) 送信元ポート以外のすべてのポートにパケットを送信します。
 - mc : (Multicast) グループに所属するポートにパケットを送信します。
 - fc : (Flooding) スイッチ上に MAC アドレスが見つからない場合に、送信元ポート以外のすべてのポートにパケットを送信します。
- ◆ **show stormcontrol** - ストームコントロールの設定情報を表示します。

初期設定

なし

例

Flooding ストームのレートを 0 に設定します。

```
8-Port Switch>set stormcontrol rate fd 11
Invalid Rate#! Rate# should be 0~3.
Syntax      : set stormcontrol rate [rate#]
Examples    : Set stormcontrol rate 0
Description: Set storm control rate as 3.3%
      Rate#      Control Rate
      0          3.3%
      1          5%
      2          10%
      3          20%
[11] argument is not found!
[Syntax]set StormControl [arg_1 data_1] [arg_1 data_1] ... [arg_n
data_n]
[Argument List]
rate..... Set Control Rate for Storm Control.
bc..... Set Broadcast Control for each Port.
mc..... Set Multicast Control for each Port.
fd..... Set Flooding Control for each Port.
```

telnet - Telnet

このページでは、本機の Telnet 機能を有効・無効に設定します。また本機の Telnet に接続するときのポート番号を変更することができます。

“show telnet” コマンドで設定情報を表示します。

文法

set telnet [enable | disable]

set telnet port { port# }

show telnet

- ◆ [enable | disable] - Telnet の有効 / 無効を設定します。
- ◆ { port# } - Telnet で使用するポート番号を設定します。
- ◆ **show telnet** - Telnet の設定情報を表示します。

例

Telnet を有効にし、ポート番号を 100 に設定します。その後に設定情報を表示しています。

```
8-Port Switch>set telnet enable
Enable telnet function successful!
8-Port Switch>set telnet port 100
8-Port Switch>show telnet
[Telnet Protocol Setting]
Telnet Status: Enabled
Port Number   : 100
```

show dynamic - 動的 MAC アドレステーブルの表示

MAC アドレステーブルを表示します。

文法

show dynamic

例

```
8-Port Switch>show dynamic
[Dynamic Adress Learning Table]
Item Port      Mac Address          VID
=====
1)   9         00-c0-f6-64-63-84    44 (0x02c)
2)   8         00-0a-e4-33-cd-26    0 (0x000)
=====
```

show cfg - 機器情報の表示

本機のモデルネーム、MAC ID およびファームウェアバージョンを表示します。

文法

show cfg

例

```
8-Port Switch>show cfg
[System Configuration]
Company Name      :
Model Name       : 8-Port Switch
MAC Address      : 00:C0:F6:64:63:84
Firmware Version : 2.12.01 < Aug 30 2007 22:14:16 >
```

show statistics - 統計情報の表示

各ポートの統計カウンタを表示します。

文法

show statistics { Port# }

- ◆ { port# } - 情報を表示したいポート番号を指定します。

例

ポート8の統計情報を表示しています。

```
8-Port Switch>show statistics 8

Rx Counter Statistics
Good Unicast Frame      =2477
Good Broadcast Frame    =1333
Good Multicast Frame    =2
802.3X MAC Control      =0
Total Receive Byte Count =455729
CRC Error                =0
Fragment                =0
Jabbers                  =0

Tx Counter Statistics
Good Unicast Frame      =2073
Good Broadcast Frame    =4
Good Multicast Frame    =0
802.3X MAC Control      =0
Total Transmit Byte Count =778569
```

エンターキーを押すことで、カウンタがリフレッシュされます。
それ以外のキーを押すと、カウンタの表示を終了します。

2. Web インタフェースからの設定

2.1 Web インターフェースへの接続

本機には管理用の Web サーバが搭載されています。Web ブラウザから設定を行うことができます。

Web インターフェースを使用する場合には、事前に以下の設定を行ってください。

- (1) コンソール接続または DHCP サーバを使用し、本機に IP アドレス、サブネットマスク、デフォルトゲートウェイを設定します。(詳細は P9 「eth0 - IP 設定」を参照して下さい)
- (2) コンソール接続で、ユーザー名とパスワードを設定します。Web インタフェースへの接続はコンソール接続の場合と同じユーザー名とパスワード使用します。
- (3) Web ブラウザから、設定した IP アドレスに接続し、ユーザー名とパスワードを入力すると、アクセスが許可され、本機のホームページが表示されます。

Web サーバへのアクセスが確立されると、以下の画面が表示されます。

LAN Management
8-Port Switch
2.12.01 < Aug 30 2007 22:14:16 >

System Configuration

Admin. Configuration

Port Configuration

Rapid Spanning Tree

Dynamic MAC Address Table

Static MAC Address Table

MAD Security Configuration

802.1Q VLAN Configuration

Static 802.1Q VLAN

802.1Q VLAN Table

802.1x Configuration

Trunk

Mirror

System Configuration

Main Board Information	
Firmware Version	2.12.01 < Aug 30 2007 22:14:16 >
Mac Address	00:C0:F6:64:63:84
Port Number	8
VLAN Max. Group	256
IGMP Max. Group	256
Loopback Detection	<input type="button" value="Test now!"/> <input type="button" value="Show Result"/> <input type="button" value="Release Port"/>
Auto Mode	<input checked="" type="radio"/> Auto Detect <input type="radio"/> Auto Negotiation
ARL Aging	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ARL Aging Time (seconds)	<input type="text" value="300"/>
<input type="button" value="Apply"/>	

System Information	
System Name	<input type="text"/>

Legend:
- Link Up (Green)
- Link Down (Blue)
- Port Disable (Orange)

2.2 Web インターフェースの操作方法

2.2.1 パネルの表示

Web インタフェースではポートの状態が画像で表示されます。各ポートのリンク状態を確認することができます。また、各ポートをクリックすることで各ポートの設定ページが表示されます。



2.2.2 設定

ページ上で設定変更を行った際は、必ず新しい設定を反映させるために [Apply] ボタン（または [Create]、[Delete] ボタン）を押してください。

1 ページ内の各項目ごとに [Apply] ボタンが設置されている場合は、必ず各設定を行うごとにその項目に対応する [Apply] ボタンを押してください。

2.3 システム設定

Main Board Information	
Firmware Version	2.12.01 < Aug 30 2007 22:14:16 >
Mac Address	00:C0:F6:64:63:84
Port Number	8
VLAN Max. Group	256
IGMP Max. Group	256
Loopback Detection	<input type="button" value="Test now!"/> <input type="button" value="Show Result"/> <input type="button" value="Release Port"/>
Auto Mode	<input checked="" type="radio"/> Auto Detect <input type="radio"/> Auto Negotiation
ARL Aging	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ARL Aging Time (seconds)	<input type="text" value="300"/>
<input type="button" value="Apply"/>	

System Information	
System Name	<input type="text"/>
Location	<input type="text"/>
Contact	<input type="text"/>
<input type="button" value="Apply"/>	

Network Configuration	
DHCP Client	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Address	<input type="text" value="192.168.1.5"/>
Network Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.120"/>
<input type="button" value="Apply"/>	

ファンクションリストから "System Configuration" を選択します。

本機に名前、設置場所及びコンタクト情報を設定することにより、管理する際に本機の識別を容易に行うことができます。

また、本機の基本情報 (MAC アドレス、ファームウェアバージョン等) を確認できます。

ネットワーク設定等もここで行えます。

Loopback Detection

ループバック検出機能により接続ケーブルのループバック問題を検出することができます。この機能を有効にすると、本機はループバックを検出するために定期的に ARP パケットを送信します。ループバック問題が検出されると、パケットストームを防止するために障害のあるポートを無効にします。障害の解消後は Release Port ボタンでポートを有効に戻します。

- ◆ Enable - ループバック検出機能を有効にします。
- ◆ Disable- ループバック検出機能を無効にします。
- ◆ Release Port - ループバック検出機能により無効になったポートを有効に戻します。

Auto Mode

- ◆ Auto Detect - 対向の機器のオートネゴシエーション機能が有効の場合は ad mode を選択します。
- ◆ Auto Negotiation - 対向の機器のオートネゴシエーション機能が無効になっている場合は an mode を選択します。

どちらのモードを選択するかは、各ネットワーク構成によって異なります。ほとんどのケースでは ad モードが推奨されています。

ARL Aging

- ◆ Enable - ARL テーブルエイジングタイムを有効にします。
- ◆ Disable- ARL エージングタイムを無効にします。

ARL Aging Time (seconds)

ARL テーブルがクリアされるまでの秒数を設定します。(初期設定値：300 秒、範囲：0-65535)

System name/Location/Contact

本機のシステム名 / 設置場所 / 管理者のコンタクト情報を入力します。

DHCP/IP Address/Network Mask/Gateway

DHCP、IP アドレス、ネットワークマスク、デフォルトゲートウェイの設定を行います。

本機は DHCP クライアント機能をサポートしています。DHCP クライアントが有効の場合、スイッチは DHCP サーバから IP 設定を取得します。DHCP サーバが見つからない場合、192.168.1.5 の初期設定 IP アドレスを使用します。

DHCP クライアント機能が無効の場合、本画面にて IP アドレス設定を行います。

2.4 Admin 設定

#	Enabled	Address / Net Mask	Mode	Http	Telnet	SNMP
1	<input checked="" type="checkbox"/>	0.0.0.0 / 0.0.0.0	Modify	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	0.0.0.0 / 255.255.255	View	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	0.0.0.0 / 255.255.255	View	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	0.0.0.0 / 255.255.255	View	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ユーザ名、パスワードの変更を行います。

Administrator Configuration

ネットワーク管理者の、ユーザ名/パスワードを変更できます。(初期設定: admin/123456)

Management IP Configuration

本機の管理に使用することができる IP アドレスおよび、各アドレスのアクセス権を設定できます。

関連する項目

admin - 管理ユーザ設定 (P7)

2.5 ポート設定

Port Configuration

Port Number	Name	Admin	Auto.	Speed	Duplex	Flow Control	
1	10/100M base-	Enable	Enabled	100M	Full	Off	Apply

Current Configuration

Port Number	Name	Link	Admin	Auto.	Speed	Duplex	Flow Control
1	10/100M base-T	Up	Enabled	Enabled	100M	Full	Off
2	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
3	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
4	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
5	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
6	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
7	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
8	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off

ファンクションリストから [Port Configuration] を選択します。

上段の [Port Configuration] で、選択したポートごとの各種設定を行います。

下段の [Current Configuration] では、設定情報及び、ポートのリンク状態を確認できます。

Port Configuration (ポート設定)

- (1) 設定を行うポートを選択します。
- (2) ポート名を入力します。
- (3) "Admin" の有効 / 無効を選択します。"disable" に設定した場合、このポートでは全てのネットワークアクセスが無効になります。
- (4) ポートのオート機能の有効 / 無効を設定します。オートモードは P41 「システム設定」にて "auto-negotiation" または "auto-detect" から選択をすることができます。
- (5) オートモードが無効の場合、"Speed"、"Duplex" にて、速度と duplex モードを設定します。
- (6) フローコントロール機能の有効 / 無効を設定します。(フローコントロールは、フローコントロール設定および QoS の両方で "ON" になっている場合に動作します)
- (7) [Apply] をクリックします。

2.6 スパニングツリー

Bridge Configuration	
Spanning Tree	Disable
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Maximum Age	20

Apply

Configuration STA Port

スパニングツリープロトコルの設定を行います。
ファンクションリストより "Rapid Spanning Tree" を選択します。
パラメータについては P24 「sta - スパニングツリープロトコル」を参照してください。
変更後は [Apply] をクリックしてください。
スパニングツリーのポート設定は "Configuration STA Port" で行います。

Bridge Port Number	
Port Priority (0..255)	128
Port State	None
Port Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Port Path Cost (1..65535)	19
Port Designated Root	00:00:00:00:00:00 [0]
Port Designated Cost	19
Port Designated Bridge	00:00:00:00:00:00 [0]
Designated Port	0: [0]
Port Forward Transitions	0

Apply

Configure STA Bridge

関連する項目

sta - スパニングツリープロトコル (P24)

2.7 MAC アドレステーブル

2.7.1 Dynamic MAC Address Table

Destination Port	
MAC Address	Static
00-12-3f-50-7c-0e	<input type="checkbox"/>

Add to Static Address Table

このページでは本機に接続されたポートの MAC アドレステーブルを表示します。

最初にポートと本機で学習された MAC アドレスを選択してください。

ユーザーはスタティック MAC アドレスとして割り当てられた MAC アドレスを選択できます。選択した後、"Add to Static Address table" をクリックします。すると選択した MAC アドレスはスタティック MAC アドレステーブルに移動し、このテーブルにはこれ以上表示されません。ページの左側のメニューから "Static MAC Address Table" をクリックするとスタティック MAC アドレスに割り当てられたアドレスリストを調べることができます。

スタティックアドレスの詳細については、スタティック MAC アドレスの項目を参照してください。

[注意] スイッチがエージングタイムの動作を行っているとき、不正な MAC アドレスが MAC アドレステーブルに時々発見されます。これらの不正な MAC アドレスはこれまでにポートにアクセスしたことのある機器であり、スイッチがそれらをテーブル内に学習しています。スイッチはエージングタイムが終わったとき、その MAC アドレスを消去します。ユーザーは正しい MAC アドレステーブルを得たいとき、エージングタイムを短くし Web ブラウザを再読み込みすることができます。正確な MAC アドレステーブルを得たとき、エージングタイムから回復します。

2.7.2 静的 MAC アドレステーブル

ID	MAC Address	Destination Port	Operation
1	00-12-3f-50-7c-0e	1	Delete

本機はスタティック MAC アドレスの割り当てをサポートしています。ユーザーは2つの方法でスタティック MAC アドレスを割り当てます。

- ダイナミック MAC アドレステーブルの MAC アドレスリストから選択します。
- 手動で割り当てます。スタティックに指定した MAC アドレスとポートを設定し、スタティック MAC アドレステーブルにこのエントリを追加します。

本機はこれらのスタティック MAC アドレスをエージアウトしません。

ユーザーがスタティック MAC アドレステーブルのエントリを削除したい場合、エントリの "Delete" ボタンをクリックしてスタティック MAC アドレスをテーブルから取り除いてください。

ポートセキュリティ機能について

MAC アドレスを使ったポートのセキュリティ機能を "MAC Security Configuration" のページで設定することができます。Accept か Reject のどちらかのモードを選択できます。Accept モードではスタティック MAC アドレスのみ、ポートを通してネットワークにアクセスできます。Reject モードではスタティック MAC アドレスだけ、ポートを通してネットワークにアクセスすることができません。

2.7.3 Mac セキュリティ

Port Number	Static MAC Number	Security Control
1	0	No Security ▼
2	0	No Security ▼
3	0	No Security ▼
4	0	No Security ▼
5	0	No Security ▼
6	0	No Security ▼
7	0	No Security ▼
8	0	No Security ▼

Apply

このページではポート上に設定したスタティック MAC アドレスのセキュリティモードを設定するために使用します。この機能には 3 つのオプションがあります。

各ポートに、登録されている MAC アドレスの数が表示されます。

- No Security
ポートにアクセスの制限を行いません。MAC アドレスを持つすべての機器がポートを通してネットワークにアクセスできます。
- Accept function
スタティック MAC アドレスとして設定されている機器のみポートを通してネットワークにアクセスできます。
- Reject function
スタティック MAC アドレスからのアクセスのみ拒否されます。それ以外の MAC アドレスを持つ機器だけポートを通してネットワークにアクセスできます。

関連する項目

静的 MAC アドレステーブル (P47)

2.8 VLAN

2.8.1 VLAN 設定

802.1Q VLAN Configuration

802.1Q VLAN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Apply
GVRP Protocol	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Apply
Ingress Filter	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Apply
VLAN Mode	<input checked="" type="radio"/> SVL <input type="radio"/> IVL <input type="radio"/> SVL/IVL	Apply
Active VLAN ID	Block 0 (1~511) ▼	Apply

Port VID

Management Port	1	Apply
-----------------	---	-------

Port Number	Port VID	Priority Setting
1 ▼	1	0 ▼

Port Number	Port VID	Priority Setting
1	1	0
2	1	0
3	1	0
4	1	0
5	1	0
6	1	0
7	1	0
8	1	0

このページでは 802.1Q VLAN 機能の設定を行います。

設定・表示項目

802.1Q VLAN

802.1Q VLAN の有効・無効を設定します。

GVRP Protocol

GVRP プロトコルは他のデバイス上の 802.1Q VLAN を学習し、ダイナミック 802.1Q VLAN テーブルに追加します。ここで GVRP プロトコルを有効・無効に設定することができます。

Ingress Filter

イングレスフィルタ機能はポートの入力側で VLAN のフィルタを行います。ポートが受信した VLAN がポートに設定した VLAN と同一の場合、出力ポートに転送します。それ以外は破棄します。

VLAN Mode

ここでは 802.1Q VLAN の動作を異なるモードから選択することができます。VLAN 機能には SVL(Shared VLAN)、IVL(Individual VLAN)、SVL/IVL の 3 つのモードがあります。

- SVL
本機は MAC アドレスだけを元にパケットの転送を行います。
- IVL
本機は MAC アドレスと VLAN ID を元にパケットの転送を行います。
- SVL/IVL
動作は IVL と同じです。しかしタグなしのポートは MDU/MTU の用途でアップリンクポートとして使用されます。

ほとんどの用途は SVL モードで対応できます。

Active VLAN ID

ここでは 802.1Q VLAN の動作に使用する有効な VLAN ID ブロックの範囲を設定します。本来の VLAN ID の範囲は 1 ~ 4096 です。しかし本機がサポートする有効な VLAN ID の範囲は最大 512 個のため、VLAN ID は下記のように 8 つのブロックに分割されて使用されます。

Block	Active VID	Block	Active VID
0	1 ~ 511	4	2048 ~ 2559
1	512 ~ 1023	5	2560 ~ 3071
2	1024 ~ 1535	6	3072 ~ 3583
3	1536 ~ 2047	7	3584 ~ 4094

ブロックのうちの 1 つが選択され、選択された VLAN ID の範囲のみ本機の 802.1Q の動作に使用されます。

Management Port

ここでは本機の管理用インターフェースを指定します。管理用インターフェースの PVID を指定することができます。HTTP、Telnet、SNMP によるネットワーク経由でのスイッチの管理ができるユーザーが、Management Port の PVID を持つ VID の VLAN のユーザーに限定されます。

Port PVID

この設定ではタグなしのパケットをタグ付きのパケットに変換します。Port PVID と Priority がパケットにタグとして追加されます。設定を行うには最初に Port Number からポート番号を選択します。次に Port PVID と Priority を割り当て、[Apply] をクリックすると設定が完了します。

2.8.2 Static 802.1Q VLAN

Create New Static VLAN	
VLAN ID	<input type="text"/>
VLAN Name	<input type="text"/> (Maximum length = 16)
<input type="button" value="Create"/>	

Show Static VLAN Table									
Select VLAN	1 (0x001) ▼								
VLAN ID	VLAN Type	VLAN Name							
1	STATIC	Default VLAN							
Port Number	1	2	3	4	5	6	7	8	
Untagged	<input checked="" type="radio"/>								
Tagged	<input type="radio"/>								
Non-member	<input type="radio"/>								
<input type="button" value="Apply"/> <input type="button" value="Delete"/>									

このページではスタティック 802.1Q グループを作成することができます。VLAN を作成するには、VLAN ID と VLAN 名を入力する必要があります。VLAN ID の範囲は 1 ~ 4096 です。VLAN ID は 802.1Q VLAN Configuration で設定した VLAN ID のブロックの範囲内のみ有効になります。

VLAN を作成した後、VLAN の設定を取得するために "Show Static VLAN Table" で VLAN を選択します。新しい VLAN は初期状態では空になっています。ここで VLAN に所属させるポートを選択肢、ポートにタグ付き・タグなしを設定することができます。その後、Apply をクリックして VLAN の設定を完了させます (VLAN の修正も同様の手順で行います)。

タグ付き・タグなしについて

タグ付きのポートでは常にパケットにタグが付いて送信されます。タグなしパケットをポートが受信した場合、タグ付きのポートに転送される前に受信ポートの PVID がタグとして付加されます。802.1Q VLAN ではタグを運びます。

タグなしポートでは常にパケットはタグが付かない状態で送信されます。タグ付きパケットをポートが受信した場合、タグなしポートに転送される前にパケットからタグが取り除かれます。ほとんどのネットワークアダプタ・デバイスはタグを付加しません。それらをタグ付きのポートに接続した場合、パケットにタグが付くためネットワークアクセスに失敗します。

ユーザーによる本機の管理について

Management Port PVID (802.1Q VLAN Configuration で設定) と同じ VLAN のユーザーのみ Web、Telnet、SNMP 経由で本機の管理ができます。他の VLAN のユーザーはネットワーク上から本機を管理することができません。

関連する項目

1qvlan - 802.1QVLAN (P28)

2.8.3 VLAN テーブル

802.1Q VLAN Table

Show VLAN Table								
Select VLAN		1 (0x001) ▾						
VLAN ID	VLAN Type	VLAN Name						
1	STATIC	Default VLAN						
Port Number	1	2	3	4	5	6	7	8
U & S	<input checked="" type="radio"/>							
U & D	<input type="radio"/>							
T & S	<input type="radio"/>							
T & D	<input type="radio"/>							

U & S : An Untagged and Static member.
U & D : An Untagged and Dynamic member.
T & S : A Tagged and Static member.
T & D : A Tagged and Dynamic member.

このテーブルは 802.1Q VLAN の活動を表示します。

Show VLAN Table の項目で VLAN を選択してください。選択した VLAN について、802.1Q VLAN の活動状態が表示されます。

GVRP プロトコルが有効の場合、このテーブルには学習されたりリモートの 802.1Q VLAN が表示されます。

2.9 802.1x 設定

802.1x Configuration

Authentication Configuration	
802.1x System Authentication Status	Disable <input type="button" value="v"/>
Re-authentication	Disable <input type="button" value="v"/>
Re-authentication Timeout Period	3600 (0.65535) seconds
Re-authentication Max Count	2 (0-10)
Max Request Count	2 (0-10)
Server Timeout Period	30 (0.65535) seconds
Supplicant Timeout Period	30 (0.65535) seconds
Quiet Timeout Period	60 (0.65535) seconds
Tx Timeout Period	30 (0.65535) seconds
<input type="button" value="Apply"/>	

Radius Server Configuration	
Radius Server IP Address	192.168.1.222
Radius Server Port Number	1812
Security Key	12345678
<input type="button" value="Apply"/>	

802.1x 機能は認証されたユーザーのみにポートへのアクセスを制限することができます。認証プロセスのため RADIUS サーバーが必要です。また本機はオーセンティケーターとして動作します。

設定・表示項目

802.1x System Authentication Status (Enable/Disable/Transparent)

- ◆ Enable - 認証モードで 802.1x 機能を有効にします。
- ◆ Disable - 802.1x 機能を無効にします。802.1x プロトコルのパケットは破棄されます。
- ◆ Transparent - 802.1x プロトコルのパケットは転送されますが、認証機能は動作しません。

Re-authentication (Enable/Disable)

ユーザーの再認証機能を有効にします。

Re-authentication Timeout

ここで設定された秒数経過するとユーザーの再認証を行います。

Re-authentication Max Count

スイッチとユーザーの間で行う認証の最大試行回数を設定します。

Max Request Count

スイッチと RADIUS サーバーの間で行う認証の最大試行回数を設定します。

Server Timeout Period

スイッチと RADIUS サーバーの間でリクエストがタイムアウトするまでの秒数を指定します。

Supplicant Timeout Period

これは最初の認証の後、スイッチとユーザー（802.1x の用語でユーザーはサブリカントと呼びます）間がタイムアウトするまでの秒数です。値の範囲は 0 ~ 65535 です。

Quiet Timeout Period

認証が失敗したとき、次の認証プロセスに移る前にスイッチとユーザー間で 802.1x が動作しない秒数です。

Tx Timeout Period

これはスイッチからユーザーへの認証リクエストがタイムアウトするまでの秒数です。リクエストは Re-authentication Max Count で設定した回数になるまで再送信されます。その後、認証失敗のメッセージが送信されます。値の範囲は 0 ~ 65535 です。

Radius Server IP Address

RADIUS サーバーの IP アドレスを指定します。

Radius Server Port Number

RADIUS サーバーのポート番号を指定します。

Security Key

RADIUS サーバーとの認証に使うセキュリティキーを指定します。

Port	Status	Authentication Mode
1	-	Force-Authorized
2	Yes	Force-Authorized
3	-	Force-Authorized
4	-	Force-Authorized
5	-	Force-Authorized
6	-	Force-Authorized
7	-	Force-Authorized
8	Yes	Force-Authorized

Apply

Port Authentication Configuration では本機のそれぞれのポートに認証モードの設定を行います。

Auto

通常の 802.1x 動作モードです。それぞれのポートで認証が行われます。

Force-Authorized

このモードは、ポートが常に 802.1x の認証が成功したものであると強制します。実際の認証結果は無視されます。

Force-Unauthorized

このモードは、ポートが常に 802.1x の認証が失敗したものであると強制します。実際の認証結果は無視されます。

None

このモードは設定したポートで 802.1x の動作を無効にします。

[注意] 本ページでは、各設定グループごとに [Apply] ボタンがあり、項目ごとに [Apply] を行う必要があります。例えば、「Authentication Configuration」の設定を行った後、[Apply] ボタンを押さずに「Radius Server Configuration」を行い「Radius Server Configuration」の [Apply] をクリックすると、「Authentication Configuration」で行った設定は適用されず、初期状態に戻ってしまいます。各グループの設定を行うごとに [Apply] ボタンで設定を適用してください。

2.10 トランク

Port Number	1	2	3	4	5	6	7	8
Group 1	<input type="radio"/>							
Group 2	<input type="radio"/>							
Group 3	<input type="radio"/>							
Group 4	<input type="radio"/>							
Non-trunk	<input type="radio"/>							

本機は4つのトランクグループをサポートしています。トランクグループは初期状態では無効になっています。トランク機能を使用したい場合は、下記の手順に沿って設定してください。

- (1) トランク機能を有効にする。
- (2) トランクにポートを割り当て、[Apply] をクリックする。
- (3) トランクからポートを取り外したい場合、そのポートを Non-trunk に指定して [Apply] をクリックする。選択したポートはトランクグループから取り外されます。

トランク機能を無効にしたい場合、Disable を選択して [Apply] をクリックしてください。スイッチはトランク設定を削除します。

冗長化について

トランク接続は冗長化機能をサポートしています。トランク接続したケーブルのどれかが破損した場合、そのケーブルを通過しているトラフィックはトランク接続されている別のケーブル上から自動的に転送されます。

関連する項目

trunk - トランク (P23)

2.11 ポートミラーリング

ポートミラーリングの機能を設定するには下記の手順を実行します。

- (1) ポートミラーリングを有効にします。
- (2) Capture Port (パケットをミラーするポート) を選択します。
- (3) 監視したいトラフィックの向き (ポートの入力方面、出力方面) により、Ingress が Egress のテーブルからモニターポートを選択します。
- (4) キャプチャ方式 (Filter Mode) を選択します。
 - ALL Packets
すべてのパケットをキャプチャします。
 - IDA
受信したパケットの送信先 MAC アドレスに一致するパケットのみキャプチャします。
 - ISA
受信したパケットの送信元 MAC アドレスに一致するパケットのみキャプチャします。
- (5) キャプチャしたパケットのうちミラーポートに送信する割合を選択します。初期状態ではキャプチャしたすべてのパケットをミラーポートに送信します。例えば 2 を設定するとキャプチャしたパケット 2 個のうち 1 個が、4 を設定するとキャプチャしたパケット 4 個のうち 1 個がミラーポートに送信されます。
- (6) [Apply] をクリックします。

ポートミラーリングを無効にしたい場合、Disable を選択して [Apply] をクリックしてください。

2.12 QoS

QoS

QoS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Apply
Priority Mechanism	<input checked="" type="radio"/> WRR (1:2:4:8) <input type="radio"/> Strict Priority	Apply
TOS/DiffServ Select	<input type="radio"/> TOS <input checked="" type="radio"/> DiffServ	Apply

Port Priority

Port Number	1	2	3	4	5	6	7	8
High	<input type="radio"/>							
Low	<input checked="" type="radio"/>							

Apply

Flow Control

Port Number	1	2	3	4	5	6	7	8
On	<input type="radio"/>							
Off	<input checked="" type="radio"/>							

Apply

本機はポートベース、802.1p、ToS/DiffServ の優先度をサポートしています。それぞれのポートには4つの優先度（P0～P4）があります。それぞれのポートのトラフィックの順位決めには優先度の高いパケットを優先するSP(Strict Priority)、4つの優先度キューを使用するWRR(Weighted Round Robin)のどちらかを設定できます。

QoS機能の設定を行うには下記の手順を実行します。

- (1) QoS を有効にします。
- (2) Priority Mechanism の欄にてトラフィックの順位付け方式を選択します。
- (3) フロー制御機能の設定を行います。フロー制御機能の設定は Port Configuration の設定の中でも可能です。Port Configuration と QoS のページの両方でフロー制御機能を有効にすると、ポート上でフロー制御機能が実際に有効になります。それ以外の組み合わせではフロー制御機能は実際に動作しません。パケットロスが発生するかどうか予期できない場合、フロー制御機能を有効にしてください。しかしこの場合、トラフィックの混雑が発生したときパケットの送信は本機によって中断されるため、実際の QoS の要求と衝突します。そのため本機はパケットに対して QoS の要求を実行することができません。
- (4) ポートベースの優先度を使用する場合、ポートに High もしくは Low の優先度を設定します。High が設定されたポートから受信されたパケットは、出力ポートの最も高い優先度のキューに転送されます。また Low が設定されたポートから受信されたパケットは、出力ポートの最も低い優先度のキューに転送されます。
- (5) 802.1p の優先度を使用する場合、802.1p 優先度の機能をポート上で有効にします。この機能は VLAN タグの優先度情報に基づいてパケットを転送します。その後、ポートの優先度キューに 802.1p 優先度（0～7）の割り当てを設定することができます。
- (6) ToS/DiffServ の優先度を使用する場合、ToS/DiffServ の優先度機能を有効にするポートを選択します。この機能は IP ヘッダの優先度情報に基づいてパケットを転送します。その後、[ToS/DiffServ Select] の項目で ToS か DiffServ のどちらかを有効にします。

- (7) DiffServ の優先度を適用する場合、それぞれの DSCP 値 (0 ~ 63) に 802.1p 優先度 (0 ~ 7) を割り当てます。その後、802.1p 優先度 (0 ~ 7) は優先度キュー (P0 ~ P3) に割り当てられることにより、優先度キューに対応づけられます。
- (8) ToS の優先度を適用する場合、ToS Precedence 値 (0 ~ 7) を優先度キュー (P0 ~ P3) に割り当てます。
- (9) [Apply] をクリックして設定を適用します。
QoS の動作を無効にしたい場合、Disable を選択して [Apply] をクリックします。

802.1p Enable

Port Number	1	2	3	4	5	6	7	8
On	<input type="radio"/>							
Off	<input checked="" type="radio"/>							

TOS/Differentiated Service Enable

Port Number	1	2	3	4	5	6	7	8
On	<input checked="" type="radio"/>							
Off	<input type="radio"/>							

802.1P Priority to Priority Queue Mapping

802.1P Tag	Priority Queue
Priority Tag 7	P3 <input type="button" value="v"/>
Priority Tag 6	P3 <input type="button" value="v"/>
Priority Tag 5	P2 <input type="button" value="v"/>
Priority Tag 4	P2 <input type="button" value="v"/>
Priority Tag 3	P1 <input type="button" value="v"/>
Priority Tag 2	P1 <input type="button" value="v"/>
Priority Tag 1	P0 <input type="button" value="v"/>
Priority Tag 0	P0 <input type="button" value="v"/>

IP TOS Precedence to Priority Queue Mapping

TOS Precedence	Priority Queue
111	P3 <input type="button" value="v"/>
110	P3 <input type="button" value="v"/>
101	P2 <input type="button" value="v"/>
100	P2 <input type="button" value="v"/>
011	P1 <input type="button" value="v"/>
010	P1 <input type="button" value="v"/>
001	P0 <input type="button" value="v"/>
000	P0 <input type="button" value="v"/>

DSCP to 802.1p Mapping

0	0	1	0	2	0	3	0	4	0	5	0	6	0	7	0
8	1	9	1	10	1	11	1	12	1	13	1	14	1	15	1
16	2	17	2	18	2	19	2	20	2	21	2	22	2	23	2
24	3	25	3	26	3	27	3	28	3	29	3	30	3	31	3
32	4	33	4	34	4	35	4	36	4	37	4	38	4	39	4
40	5	41	5	42	5	43	5	44	5	45	5	46	5	47	5
48	6	49	6	50	6	51	6	52	6	53	6	54	6	55	6
56	7	57	7	58	7	59	7	60	7	61	7	62	7	63	7

[注意] 本ページでは、各設定グループごとに [Apply] ボタンがあり、項目ごとに [Apply] を行う必要があります。例えば、"Port Priority" の設定を行った後、[Apply] ボタンを押さずに "Flow Control" の設定を行い "Flow Control" の [Apply] をクリックすると、"Port Priority" で行った設定は適用されず、初期状態に戻ってしまいます。各グループの設定を行うごとに [Apply] ボタンで設定を適用してください。

関連する項目

qos - Quality of Service (P19)

2.13 レートコントロール

Ingress/Egress Rate Control

Packet Drop for Ingress Limit Enable Disable

Rate = $N \times 64 \text{ Kb}$, with $N=1 \sim 28$
 $(N-27) \times 1 \text{ Mb}$, with $N=29 \sim 127$

Port Number	Ingress Rate Control		Egress Rate Control	
1	<input type="text" value="0"/> (0~127)	No Limit	<input type="text" value="0"/> (0~127)	No Limit
2	<input type="text" value="0"/> (0~127)	No Limit	<input type="text" value="0"/> (0~127)	No Limit
3	<input type="text" value="0"/> (0~127)	No Limit	<input type="text" value="0"/> (0~127)	No Limit
4	<input type="text" value="0"/> (0~127)	No Limit	<input type="text" value="0"/> (0~127)	No Limit
5	<input type="text" value="0"/> (0~127)	No Limit	<input type="text" value="0"/> (0~127)	No Limit
6	<input type="text" value="0"/> (0~127)	No Limit	<input type="text" value="0"/> (0~127)	No Limit
7	<input type="text" value="0"/> (0~127)	No Limit	<input type="text" value="0"/> (0~127)	No Limit
8	<input type="text" value="0"/> (0~127)	No Limit	<input type="text" value="0"/> (0~127)	No Limit

レートコントロール機能はそれぞれの物理ポートの最大トラフィックレートを制限することができます。制限できるトラフィックは入力と出力の両方です。

レートコントロールの範囲は 64kbps ~ 100Mbps です。ここでは設定時のルールについて説明します。

最大転送レート	レートコントロール値 (N)	転送レートの計算方法
制限なし	0	なし
64k,128k,192k, ~ 1792kbps	1 ~ 28	Rate=N × 64Kbps
2M,3M,4M ~ 100Mbps	29 ~ 127	Rate=(N-27) × 1Mbps

例えば Port2 のダウンロードトラフィックレートを 512Kbps に制限したい場合、Port2 の "Egress Rate Control" を 8 に設定します。

"Packet Drop Ingress Limit" は入力トラフィックが "Ingress Rate Control" の値を超えたときパケットを破棄する動作を行います。有効にすると、入力トラフィックのレートを制限するために余分なトラフィックは破棄されます。無効にすると、フロー制御機能が入力トラフィックを中断するために使用されます。

2.14 ストームコントロール

Storm Control

Control Rate	3.3%	Apply
Broadcast Control	<input type="radio"/> All <input type="radio"/> None <input checked="" type="radio"/> By Port	Apply
Multicast Control	<input type="radio"/> All <input type="radio"/> None <input checked="" type="radio"/> By Port	Apply
Flooding Control	<input type="radio"/> All <input type="radio"/> None <input checked="" type="radio"/> By Port	Apply

Port	Broadcast	Multicast	Flooding
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Port	Broadcast	Multicast	Flooding
1	-	-	-
2	-	-	-
3	-	-	-
4	-	-	-
5	-	-	-
6	-	-	-
7	-	-	-
8	-	-	-

ストームコントロール機能はパケットストームの最大トラフィックレートを制限することができます。ブロードキャスト、マルチキャスト、フラッディングの3つのストームを制限することができます。ポートごとにストームコントロールを有効にすることができます。ストームコントロールの設定は下記の手順を参照してください。

- (1) Control Rate を選択します。
- (2) 設定を適用するストームと、レートを制限するポート（全ポートに適用する、全ポートに適用しない、ポートごとに設定の3つから指定）を選択します。
- (3) レートの制限をポートごとに行う場合、ポートを指定して制限を適用するストームを選択します。設定が終わったら Apply をクリックします。

各ストームの意味については下の通りです。

- Broadcast 送信元ポート以外のすべてのポートにパケットを送信します。
- Multicast グループに所属するポートにパケットを送信します。
- Flooding スイッチ上に MAC アドレスが見つからない場合に、送信元ポート以外のすべてのポートにパケットを送信します。

2.15 Telnet

このページでは、本機の Telnet 機能を有効・無効に設定します。また本機の Telnet に接続するときのポート番号を変更することができます。

2.16 SNMP

Trap	IP Address	Community Name
Trap 1	0.0.0.0	public
Trap 2	0.0.0.0	public
Trap 3	0.0.0.0	public
Trap 4	0.0.0.0	public
Trap 5	0.0.0.0	public

このページでは GET/SET/Trap のコミュニティ名、Trap の動作のための IP アドレスを設定することができます。設定を行うと、SNMP の管理プログラムからこれらの設定を使用して本機を管理することができます。

2.17 IGMP

Group	Group Address	Members Port
1	239.0.0.1	2

IGMP 機能はネットワーク上での IP マルチキャストの動作のために使用されます。本機は IGMP が有効のデバイスから IP マルチキャストグループの情報を得るために IGMP Snooping 機能を使用することができます。学習した IP マルチキャストメンバーグループの情報はこのページに表示されます。本機はグループ情報から学習したメンバーポートに、IP マルチキャストトラフィックを転送します。IGMP Snooping 機能はこのページで有効・無効に設定することができます。

2.18 MVR

2.18.1 MVR VLAN

MVR VLAN Configuration	
MVR VLAN Index	1
Active	<input type="checkbox"/>
Name	
Multicast VLAN ID	1
802.1p Priority	0
Mode	<input checked="" type="radio"/> Dynamic <input type="radio"/> Compatible
Source port	1 Tagged

Receiver Port								
Port Number	1	2	3	4	5	6	7	8
Untagged	<input type="radio"/>							
Tagged	<input type="radio"/>							
Non-member	<input checked="" type="radio"/>							

Apply

このコマンドは MVR (Multicast VLAN Registration) 機能を設定するために使用します。VLAN 機能は VLAN グループの間でトラフィックを分離します。しかしこの機能は同時に、異なる VLAN に所属するサブスクリバの IP マルチキャストトラフィックを分離します。MVR 機能は異なる VLAN に所属するサブスクリバが、1つの IP マルチキャスト VLAN を共有することを可能にします。これは VLAN のマルチキャストトラフィックを減少させます。

MVR 機能を使うためには、最初に IGMP Snooping 機能を有効にする必要があります。

設定・表示項目

本機は 4 つの MVR VLAN をサポートします。それらはインデックス 1,2,3,4 として参照されます。MVR 設定のいずれかを、インデックスに割り当てる必要があります。またすべての設定はインデックスされた MVR VLAN として割り当てられます。

これらの設定については下記を参照してください。

Active

MVR VLAN を有効・無効にする。

Name

MVR VLAN を識別するための名前を割り当てます。

Multicast VLAN ID

この MVR VLAN に使用する VLAN ID を設定します。範囲は 1 ~ 4096 です。

802.1p Priority

802.1p 優先度 (0 ~ 7) を使用します。IGMP 管理パケットに VLAN タグが付加されているとき、この優先度の値が割り当てられます。

Mode

MVR 機能には 2 つの動作モードがあります。1 つはダイナミックモード、もう 1 つはコンパチブルモードです。ダイナミックモードでは、本機は MVR VLAN 内のすべての MVR ソースポートに IGMP Report パケットを送信します。コンパチブルモードでは、本機は IGMP Report パケットを送信しません。

Source Port

IP マルチキャストトラフィックの送信元である MVR VLAN のアップリンクポートを設定します。またポートがタグ付きかタグなしかを設定します。

Receiver Port

MVR VLAN の IP マルチキャストトラフィックを受信するサブスクリバラーが接続されたポートを指定します。

MVR VLAN を設定した後、設定した MVR VLAN に IP マルチキャストグループを割り当てることができます。1 つの MVR VLAN に複数の IP マルチキャストグループを割り当てることができます。

関連する項目

mvr - MVR (Multicast VLAN Registration)(P13)

2.18.2 MVR グループ

MVR Group Configuration

MVR VLAN Index: 1

Name	Start Address	End Address

Add New Group

Current Active Group

Index	Name	Start Address	End Address	Deactivate
1	new	224.0.0.9	224.0.0.12	<input type="checkbox"/>

Apply

MVR VLAN を設定した後、設定した MVR VLAN に IP マルチキャストグループを割り当てることができます。1 つの MVR VLAN に複数の IP マルチキャストグループを割り当てることができます。

MVR VLAN に IP マルチキャストグループを割り当てるために、最初に 1 つの MVR VLAN のインデックスを選択する必要があります。

設定・表示項目

MVR VLAN の IP マルチキャストグループのため、下記の設定を割り当てる必要があります。

Name

IP マルチキャストグループを識別するための名前を設定します。

Start Address

IP マルチキャストアドレスの開始アドレスを設定します。

End Address

IP マルチキャストアドレスの終了アドレスを設定します。

設定が終わった後、[Add New Group] をクリックします。

MVR VLAN と IP マルチキャストグループの両方を設定した後、MVR の受信ポートに接続されたサブスライバーはそれらが異なる VLAN に所属していても、ソースポートから IP マルチキャストグループの範囲内で IP マルチキャストトラフィックを受信することができます。

IP マルチキャストグループを削除したい場合、Deactivate にチェックを入れて [Apply] をクリックしてください。IP マルチキャストグループがリストから削除されます。

[注意] リストは編集機能をサポートしていません。IP マルチキャストグループを修正したい場合、最初にそれを削除してください。その後、もう一度新しい IP マルチキャストグループを作成します。

2.19 ポート統計情報

Statistics

Destination Port: 1 Refresh Interval (5 - 60) sec: 30

Rx Counter	Statistics
Good Unicast Frame	4116
Good Broadcast Frame	196
Good Multicast Frame	2
802.3X MAC Control	0
Total Receive Byte Count	528587
CRC Error	0
Fragment	0
Jabbers	0
Tx Counter	Statistics
Good Unicast Frame	3529
Good Broadcast Frame	4
Good Multicast Frame	0
802.3X MAC Control	0
Total Transmit Byte Count	1487291

Refresh Reset Statistics

このページではトラフィックの統計を見ることができます。違うポートのカウンタを取得する場合はポート番号を選択してください。

カウンタの更新間隔を変更するには "Refresh Interval" の値を変更します。[Refresh] ボタンをクリックするとすぐにカウンタをアップデートすることができます。

[Reset Statistics] ボタンを押すとカウンタをゼロにリセットすることができます。

2.20 システム管理

The screenshot shows a web interface titled "Maintenance Tools" with a light blue background. It contains four distinct sections, each with a pink header bar and a yellow content area. The sections are: 1. "System Backup" with instructions to press "Backup Setting" and buttons for "Backup Setting to binary file" and "Backup Setting to text file", followed by a text input field, a "参照..." button, and a "Restore Setting" button. 2. "System Restore Factory Default Settings" with instructions to press "Restore" and a "Restore" button. 3. "System Reset" with instructions to press "Reset" and a "Reset" button. 4. "System Upgrade" with instructions to click "START" and a text input field, a "参照..." button, and a "START" button.

本機はシステム管理ツールとして4つの機能をサポートしています。

System Backup

- Backup Setting to binary file
このページを表示している PC にバイナリ形式で本機の設定をバックアップします。
- Backup Setting to text file
このページを表示している PC に、編集ができるようにテキスト形式で本機の設定をバックアップします。
- Restore Setting
このページを表示している PC から設定のバックアップファイルを取得し、本機の設定をリストアします。

System Restore Factory Default Setting

本機の設定を工場出荷状態に戻します。

System Reset

本機をリセットします。

System Update

このページを表示している PC からシステムオペレーションソフトウェアをアップロードします。

FXC3008 Management Guide (FXC08-DC-200026-R1.0)

初版 2008年12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、万一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。
-

Management Guide
FXC3008

Management Guide
FXC3008