Future X Communications

FXC5012MPE
Management Guide

2015 年 5 月 Ver.1.2

FXC株式会社

FXC5012MPE 本マニュアルについて

- 本マニュアルでは、FXC5012MPE の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末を接続して、CLI （コマンドラインインタフェース）による簡易設定、または Web ブラウザにより設定を行います。
- 本マニュアルは FXC5012MPE に対応したマニュアルとなっています。機能はどの製品も同一ですが、ポート構成の違いにより一部設定項目や設定画面が異なる場合があります。

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

・下記事項は、安全のために必ずお守りください。

警告

● 安全のための注意事項を守る

注意事項をよくお読みください。製品全般の注意事項が記載されています。

● 故障したら使わない

すぐに販売店まで修理をご依頼ください。

● 万一異常が起きたら

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

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

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

● 電源ケーブルや接続ケーブルを傷つけない

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

● 内部に水や異物を入れない

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

● 内部をむやみに開けない

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

● 落雷が発生したらさわらない

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

● 油煙、湯気、湿気、ほこりの多い場所には設置しない

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

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

注意

● 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。

● VCCI クラス A 製品

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

はじめに 4
1 章 システム情報 7
1.1.1 Information 7
1.1.2 Configuration 10
1.2 Time (システムタイムの設定) 13
1.2.1 Manual 13
1.2.2 NTP 15
1.3 Account 15
1.4 IP 20
1.5 Syslog 23
1.6 SNMP 26
1.6.3 Users 29
2 章 設定方法 39
2.1 Port 39
2.1.1 Configuration 39
2.1.2 Port Description 41
2.1.3 Traffic Overview 42
2.1.4 Detailed Statistics 43
2.1.5 Qos Statistics 45
2.1.6 SFP Information 46
2.1.7 EEE 48
2.2 ACL 50
2.2.1 Ports 50
2.2.2 Rate Limiters 52
2.2.3 ACL Status 56
2.3 Aggregation 58
2.3.1 Static Trunk 58
2.3.2 LACP 60
2.4 Spanning Tree 65
2.4.1 Bridge Settings 66
2.4.2 MSTI Mapping 68
2.4.3 MSTI Poriorities 70
2.4.4 CIST Ports 71
2.4.5 MSTI Ports 73
2.4.6 Bridge Status 75
2.4.7 Port Status 76
2.4.8 Port Statistics 77
2.5 IGMP Snooping 78
2.5.2 VLAN Configuration 80
2.5.3 Port Group Fitering 81
2.5.4 Status 82
2.5.5 Group Infermation 84
2.5.6 IPv4 SSM information 85

2.6 MLD Snooping 87
2.6.1 Basic Configuration 88
2.6.2 VLAN Configuration 89
2.6.3 Port Group Fitering 91
2.6.5 Group Infermation 93
2.6.6 IPv6 SSM Information 95
2.7 MVR 96
2.7.1 Configuration 96
2.7.2 Port Group Allow 98
2.7.2 Groups Information 99
2.7.3 Statistics 100
2.8 LLDP 101
2.8.1 LLDP Configuration 101
2.8.2 LLDP Neighbours 104
2.8.3 LLDP-MED Configuration 106
2.8.4 LLDP-MED Neighbours 112
2.8.5 EEE 116
2.8.7 Port Statistics 118
2.9 PoE 120
2.9.1 Configuration 120
2.9.2 Status 122
2.9.3 Power Delay 123
2.9.4 Auto Checking 124
2.9.5 Scheduling 125
2.10.1 Configuration 127
2.10.2 Dynamic MAC Table 130
2.11 VLAN 132
2.11.1 VLAN Membership 132
2.11.2 Ports 134
2.11.3 Switch Status 136
2.11.4 Port Status 137
2.12 VOICE VLAN 139
2.12.1 Configuration 139
2.12.2 OUI 141
2.11.5 Private VLANs 142
2.11.6 MAC-based VLAN 145
2.11.7 Protocol -based VLAN 148
2.13 GARP 153
2.13.1 Configuration 153
2.13.2 Statistics 155
2.14 GVRP 156
2.14.1 Configuration 156
2.14.2 Statistics 158

2.15 QoS 159
2.15.1 Port Classification 159
2.15.2 Port Policing 162
2.15.3 Port Schedulers 164
2.15.4 Port Tag Remarking 170
2.15.5 Port DSCP 172
2.15.6 DSCP-Based QoS 174
2.15.7 DSCP Translation 176
2.15.8 DSCP Classification 178
2.15.9 QoS Control List 179
2.15.12 Storm Control 185
2.16 s-Flow Agent 186
2.16.1 Collector 186
2.16.2 Sampler 188
2.17 Loop Protection 190
2.17.1 Configureaion 190
2.18 Single IP 192
2.18.1 Configration 192
2.18.2 Information 193
2.19 Mirroring 194
2.20 Trap Event Severity 196
2.21 SMTP Configuration 197
2.22 UPnP 199
3章 セキュリティ 200
3.1 IP Source Guard 200
3.1.1 Configuration 200
3.1.2 Static Table 202
3.1.3 Dynamic Table 204
3.2 ARP Insprction 205
3.2.1 Configuration 205
3.2.2 Static Table 207
3.2.3 Dynamic Table 209
3.3 DHCP Snooping 210
3.3.1 Configuration 210
3.3.2 Statistics 211
3.4 DHCP Relay 213
3.4.1 Configuration 213
3.4.2 Statistics 215
3.5 NAS 217
3.5.1 Configuration 217
3.5.2 Switch Status 226
3.5.3 Port Status 228
3.6 AAA 231
3.6.1 Configuration 231
3.6.2 Radius Overview 235
3.6.3 Radius Detalls 237
3.7 Port Security 238
3.7.1 Limit Control 238
3.7.2 Switch Status 241

3.8 Acess Management 245
3.8.1 Configuration 245
3.9 HTTPS 248
3.10 Auth Method 249
4章 メンテナンス 250
4.1 Restart Device 250
4.2 Firmware 251
4.2.1 Firmware Upgrade 251
4.2.2 Firmware Selection 253
4.3 Save / Restore 254
4.3.1 Factory Defaults 254
4.3.2 Save Start 255
4.3.3 Save User 256
4.3.4 Restore User 257
4.4 Export / Import 258
4.4.1 Export Config 258
4.4.2 Import Config 259
4.5 Diagmostics 260
4.5.1 Ping 260
4.5.2 Ping6 262
4.5.3 VeriPHY 264
5章 コマンドインタフェース 265
5.1 コマンドラインインタフェースの利用 265
5.1.1 コマンドラインインタフェースへのアクセス 265
5.1.2 コンソール接続 266
5.1.3 Telnet 接続 266
5.1.4 コマンド上でのヘルプの表示 267

はじめに

この度は、弊社 FXC5012MPE をお買い上げ頂き誠にありがとうございます。
お使いになる前に、本書をよくお読みください。
また、お読みになった後は、後日お役に立つこともありますので必ず保管してください。
本書は、本製品を正しくご利用頂く上で必要な機能説明および操作方法について記述しています。

本機は主な設定は、イーサネットポート経由で PC から WEB ブラウザにておこないますが、基本的な設定を付属のコンソールケーブルを用いてコンソールポート経由でマネージメント機能にログインし行いことも可能です。

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。

設定方法

WEB ブラウザを使用してログインするには以下の手順に従ってください。
Step 1. WEB ブラウザを起動します。
Step 2. WEB ブラウザの[アドレス] に本製品の IP アドレスを入力し、Enter キーを入力します。
(初期設定時は IP アドレス、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。)

初期設定値

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

認証用アクセス画面

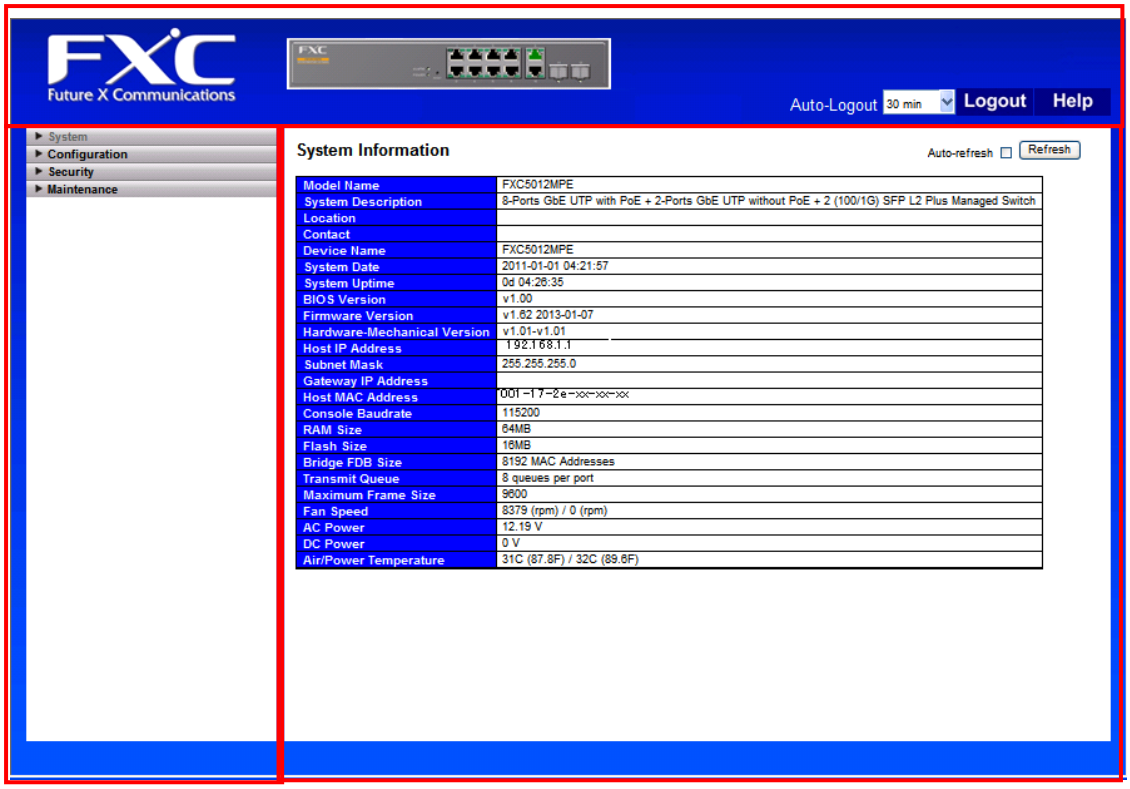
【注意】:
本機はユーザ管理機能をサポートしており、管理者のみがシステムを設定することが可能です。複数のユーザが管理者の ID を使用する場合は、システム設定を行うために最初にログインしたユーザのみ許可します。それ以外のユーザは、管理者の ID を使用しても、システムのモニタリングのみ可能です。最大 3 ユーザのみが同時にログインすることが可能です。

【注意】:
WEB ブラウザは 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。

画面の校正

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。

トップメニューウィンドウ



メニューウィンドウ　　メインウィンドウ

設定/表示項目

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 でリンクアップしている場合は橙で、1000M でリンクアップしている場合は緑で表します。
また各ポートをクリックすることによりカウンターメニューを表示します。
Auto-Logout からは自動的に WEB マネジメントからログアウトする時間を設定します。
Logout ボタンをクリックすることにより本製品からログアウトします。
Help からは表示メニューの Help を別ウィンドウで表示することが可能です。

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。

メインウィンドウ

メニューウインンドウで選択したメニューの設定項目、及びステータス情報を表示します。

1 章　システム情報

本製品のシステム情報を表示します。モデル名、システム名、システム管理者、デバイス名、システムの稼働時間、BIOS バージョン、ファームウェアのバージョン、ハードウェアのバージョン、ホスト MAC アドレス、デバイスポート、RAM サイズ、フラッシュサイズなどのシステムの基本情報が表示されます。 この情報によって、お使いのソフトウェアのバージョン、および MAC アドレス、ポート情報などを確認することができます。

1.1.1 Information

このメニューでは本製品のシステム情報を表示します。モデル名、システム、設置場所などのロケーション情報、システム管理者、デバイス名(ホスト名)、シテスムの時間、システムの稼働時間、BIOS バージョン、ファームウェアのバージョン、ハードウェアのバージョン、IPアドレスやサブネットマスク、ゲートウェイなどのIP情報、本製品の MAC アドレス、コンソールポートのボーレート、RAM サイズ、フラッシュサイズ、MAC アドレスの最大学習数などのシステムの基本情報が表示されます。 この情報によって、お使いのソフトウェアのバージョン、および MAC アドレス、ポート情報などを確認することができます。

System Information　Auto-refresh ☐ Refresh

Model Name	FXC5012MPE
System Description	8-Ports GbE UTP with PoE + 2-Ports GbE UTP without PoE + 2 (100/1G) SFP L2 Plus Managed Switch
Location	
Contact	
Device Name	FXC5012MPE
System Date	2011-01-01 18:19:47
System Uptime	0d 18:19:47
BIOS Version	v1.00
Firmware Version	v1.62 2013-01-07
Hardware-Mechanical Version	v1.01-v1.01
Host IP Address	192.168.11.237
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.11.1
Host MAC Address	00- 17-2e-xx-xx-xx
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600
Fan Speed	8571 (rpm) / 0 (rpm)
AC Power	12.19 V
DC Power	0 V
Air/Power Temperature	30C (86.0F) / 31C (87.8F)

Model name
本製品のモデル名を以下のとおり表示します。
FXC5012MPE

System description:
本製品のシステム情報を以下のとおり表示します。
8-Ports GbE UTP with PoE + 2-Ports GbE UTP without PoE + 2 (100/1G) SFP L2 Plus Managed Switch

Location:
本製品の設置場所など設定されたロケーション情報を表示します。

初期値ではロケーション設定は表示されませんが、1-1-2 Configuration メニューから任意の System Location 情報を設定することで、表示することが可能です。

Contact:
本製品のシステム管理者および連絡先などを表示します。
初期値ではシステム管理者および連絡先などコンタクト設定は表示されませんが、
1-1-2 Configuration メニューからシステム管理者および連絡先など System Contact 情報を設定することで、表示することが可能です。

Device name:
本製品のホスト名を表示します。
初期値ではホスト名などデバイス名は表示されませんが、Configuration メニューから System name 情報を設定することで、表示することが可能です。

System Date:
本製品のシステム時間を表示します。システム時間は Time メニューから Manul 設定、もしくは NTP 設定をいただくことにより取得することが可能です。
(フォーマット：西暦-月-日　時間：分：秒)

System up time:
本製品の電源を入れてからの稼働時間を表示します。
（フォーマット：稼働日数　時間：分：秒）

BIOS version:
本製品の BIOS のバージョンを表示します。

Firmware version:
本製品のファームウェアのバージョンを表示します。

Hardware-Mechanical version:
本製品のハードウェアのバージョンを表示します。

Host IP address:
本製品の IP アドレスを表示します。
(初期値：192.168.1.1)

Subnet Mask:
本製品 Subnet Mask を表示します。
(初期値：255.255.255.0)

Gateway IP Address:
本製品 Default gateway の値を表示します。
(初期値：192.168.1.254)

Host MAC address:
本製品の MAC アドレスを表示します。

Console Baudrate:

本製品のコンソールポートのボーレート(115200baud)を表示します。

RAM size:
本製品の RAM サイズ(64MB)を表示します。

Flash size:
本製品のフラッシュメモリのサイズ(16MB)を表示します。

Bridge FDB size :
本製品が学習できる Mac address の最大学習数(8,192 個)を表示します。

Transmit Queue :
デバイスの送信ハードウェアのプライオリティのキュー情報を表示します。
本製品では 8 つのレベルに分けられます。

Maximum Frame size:
本製品がフラグメントせずに転送できる最大フレームのサイズの情報(9,600byte)を
表示します。

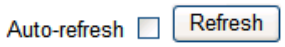
Fan Speed:
毎分ごとの FAN の回転数(rpm)を表示します。
本製品では 2 つの FAN を搭載していますが、1 つはもう一台が故障した際のバックアップとなるため、通常どちらかは「0rpm」と表示されます。

AC Power:
本製品 AC の入力電圧を表示します。

DC Power:
本製品ではサポートされておりません。

Air/Power Temperature:
本製品の温度情報を表示します。

Auto-refresh/Refresh



画面の表示内容を最新の状態に更新します。Auto-refresh を有効にした場合、
おおよそ 3 秒毎に表示内容を最新の状態に更新します。
また Refresh ボタンをクリックし、表示内容をその都度、最新に更新することも可能です。

1.1.2 Configuration

このメニューでは本製品の設置場所などのロケーション情報、機器のホスト名、管理者の連絡先などの情報を設定します。
また、設定した内容はシステム情報の各項目に反映され表示されます。

設定方法
WEB 画面のシステム情報を設定するには以下の手順に従ってください。
Step 1.　[System Information]→[Configuration]を選択します。
Step 2.　システム名、本製品の設置場所、管理者のコンタクト情報を入力します。
Step 3.　[Apply]をクリック、設定を反映させます。
Step 4.　[Maintenance]→[Save/Restore]→[Save start]を選択します。
Step 5.　[Save]をクリック、設定を保存します。

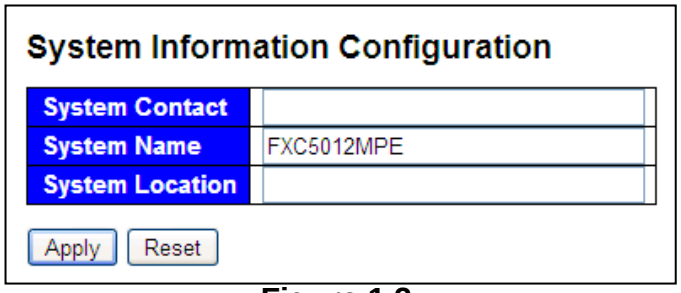


Figure.1.2

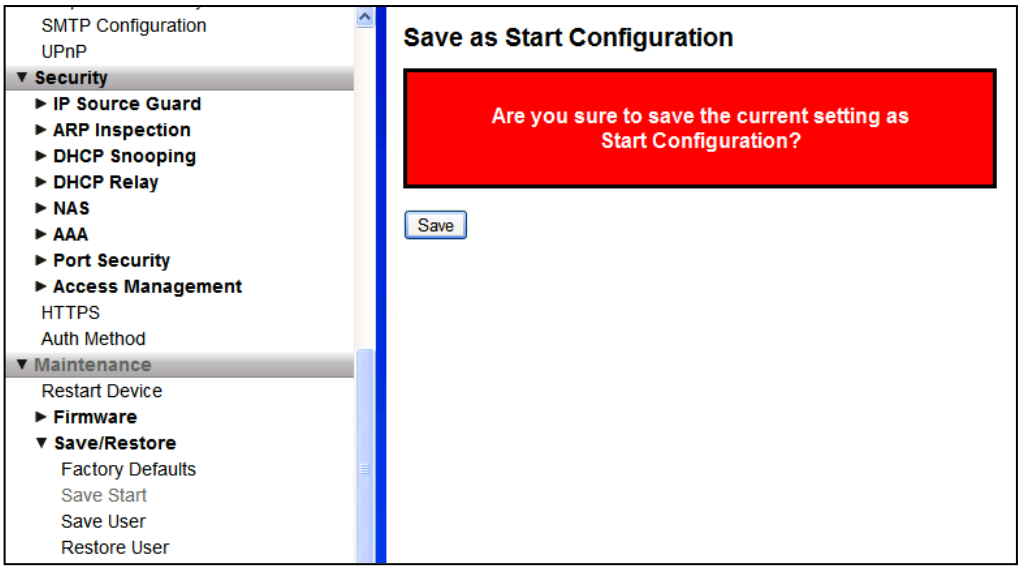
設定/表示項目

System Contact
本製品のシステム管理者および連絡先などを設定します。
半角英数大文字小文字文字及び、ASCⅡコードの 32(0x20)～126 に定められた
一部の記号(！, " ,#, $,%, &,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能で
最大 255 文字まで設定することが可能です。
この設定内容は、Figure1.1 Contact の表示に反映されます。

System Name
本製品のシステム名(ホスト名)を設定します。半角英数大文字小文字((A-Z、a-z、0-9)及び(-)を使用してください。この設定にスペースを用いる事はできません。
最初の文字は、必ず英数文字を使用してください。
また、最初の文字あるいは最後の文字には(-)を使用することはできません。
最大 255 文字まで設定が可能です。

System Location :

本製品の設置場所などロケーション情報を設定します。
半角英数大文字小文字文字及び、ASCⅡコードの 32(0x20)～126 に定められた一部の記号(！, " ,#, $,%, &,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能で最大 255 文字まで設定することが可能です。



1.1.3 CPU Loa

このメニューでは、本製品の CPU の稼働率をサンプリングした値の平均値について、それぞれ 100ms、1sec、10sec 間隔でグラフ化して表示します。

【注意】.
グラフの出力には、ご利用のブラウザが SVG(Scalable Vector Graphics)フォーマットをサポートしている必要があります。

1.2 Time (システムタイムの設定)

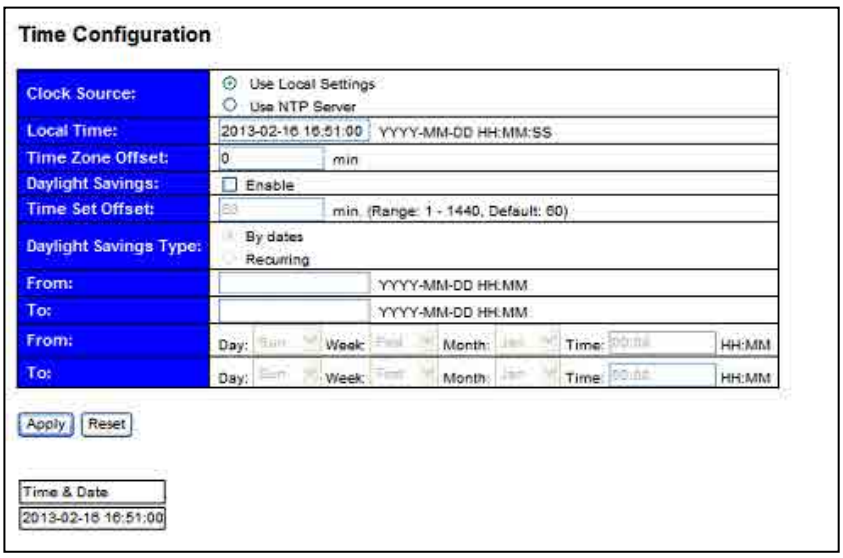
本製品のシステムタイムの設定を行います。システムタイムの設定は手動によるマニュアル設定、もしくはNTP サーバーのアドレスを登録し一定間隔で自動的に同期をとるNTP 設定が可能です。

1.2.1 Manual

このメニューでは、本製品のシステムタイムの時間設定を手動によるマニュアル設定にて行います。
Local Time の各項目に、指定のフォーマットで年月日及び時刻の入力をします。

設定方法

WEB 画面のシステムタイム情報を設定するには以下の手順に従ってください。
Step 1. [Time]→ [Manual]をクリックし[Time Configuration]メニューを開きます。
Step 2. [Clock Source] として[Use Local Settings]を選択します。
Step 3. タイムパラメータを下記のフォーマットで手動にて指定します。
(フォーマット:西暦-月-日　時間:分:秒)
Step 4. <Apply>ボタンをクリックし設定内容を適用します。



[内容] 本製品は、内部にハードウェアクロックソースを持たないため、システムタイムをマニュアルにて設定した後、機器を再起動した場合、設定は初期値に戻ります。

設定/表示項目

Clock Source:
本製品のシステムタイムのクロックソースとして“Use local Settings” または、
“Use NTP Server”を選択してください。Use NTP Server を選択した場合、
引き続き、NTP メニューから NTP サーバーのアドレスを入力してください。

Local Time:
マニュアル設定時、システムタイムを手動します。
また、現在のシステムタイムを表示します。

Time Zone Offset:
設定された本製品のシステムタイムと UTC の時刻との差分を分単位で
設定します。有効範囲は、「-720」 ～ 「780」分までです。

Daylight Saving:
サマータイムを採用する場合、Daylight Savings 機能を「Enable」とし有効にします。
サマータイムはデフォルトでディセーブルに設定されています。

Time Set Offset:
サマータイムを採用した場合の時刻との差分を分単位で設定します。
有効範囲は、「1」 ～ 「1440」分までです。

Daylight Savings Type:
サマータイムを採用する際の規則を [By Dates]あるいは[Recurring]の 2 タイプから
選択します。[Recurring]を選択した場合、サマータイムの規則は米国の規則をデフォルトとし、
Time Set Offset に自動的にデフォルト値として 60min が適用されます。
開始月日及び時刻と終了月日及び時刻をプルダウンメニューから設定してください。
また、ヨーロッパなど他の地域でサマータイムを採用する場合、[By Dates]を選択して
所定の Time Set Offset の値を設定してください。
また、開始年月日及び時刻と終了年月日及び時刻を手動にて入力してください。

1.2.2 NTP

このメニューでは、システムタイムを NTP サーバーと同期させ取得する場合、
クロックソースとなる NTP サーバーを IP アドレスもしくはホスト名を設定します。

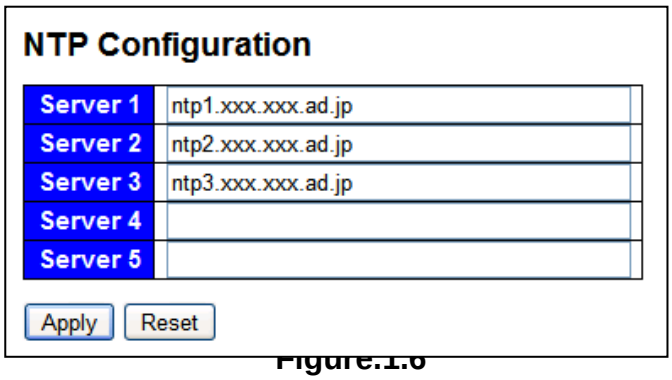


Figure.1.6

設定方法

WEB 画面の NTP を設定するには以下の手順に従ってください。
Step 1. [Time]→ [NTP]をクリックし[Time Configuration]メニューを開きます。
Step 2. NTP サーバーの値を入力します。
Step 3. <Apply>ボタンをクリックし設定内容を適用します。

1.3 Account

本製品にログインするユーザーのアカウント情報の管理を行います。
各アカウント情報は UserName、Password 及び Privilege Level（特権レベル）で管理されます。アカウントに設定された Privilege Level（特権レベル）応じて、本製品の設定やその変更の可否、もしくは閲覧のみに制限することなどが可能となります。

1.3.1 Users

このメニューでは、ログインするユーザーアカウント情報の登録、変更、削除を行います。
Privilege Level（特権レベル）は、Level 1～15 までの 15 段階となり、設定の閲覧のみが可能な Level 1、本製品のファームウェアのアップグレード、初期化など一部を除き、ほとんどの設定とその変更、削除が可能な Level 10、本製品にかかわる全ての設定とその変更、削除が可能な Level 15 から設定ください。
おおむね Guest として設定の閲覧のみを許可するアカウントには Level 5、一般ユーザーとして設定とその変更、削除を許可するアカウントには Level 10、管理者となるアカウントには Level 15 を設定するのが一般的です。
また、アカウント情報は最低 1～最大 20 人までアカウント情報を登録することができますが、最低1アカウントは、Privilege Level（特権レベル）が 10 以上のアカウントである必要があります。

設定方法

WEB 画面のアカウント情報を設定するには以下の手順に従ってください。
Step 1.　[Account]→[Users]を選択します。
Step 2.　<Add new user>ボタンをクリッします。
(既存のアカウント情報を変更する場合、該当の UserName をクリックして下さい)
Step 3.　UserSettings に任意の UserName、Password、Privilege Level を入力します。
Step 4.　[Apply]をクリック、設定を反映させます。
Step 5.　[Maintenance]→[Save/Restore]→[Save start]を選択します。

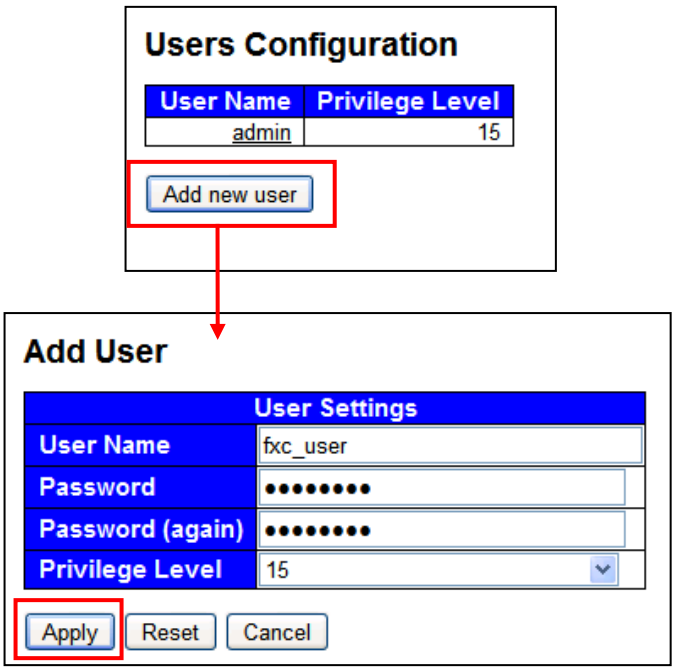


Figure.1.7

設定/表示項目

User Name :
本製品への時に使用するログインユーザー名を設定します。
半角英数大文字小文字((A-Z、a-z、0-9)及び(-)を使用してください。この設定にスペースを用いる事はできません。
最初の文字は、必ず英数文字を使用してください。
最初の文字あるいは最後の文字には(-)を使用することはできません。
1 文字から最大 32 文字まで設定が可能です。

Password
本製品のシステム管理者および連絡先などを設定します。
半角英数大文字小文字文字及び、ASCⅡコードの 32(0x20)～126 に定められた
一部の記号(！, " ,＃, $,%, &,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能で、
最大 32 文字まで設定することが可能です。
また、入力せず省略することも可能です。

Password (again)
パスワードを再度入力します。確認のため同じパスワードを入力してください。

Privilege Level :
ログインするユーザの Privilege Level(優先レベル)を設定します。
範囲は「1～15」となり、優先値が「15」の場合は、すべてのグループにアクセス可能です。
それ以外の値は、各グループの優先順位を参照してください。各グループへのアクセスを行うには、グループの優先レベルと同じか、それ以上に設定する必要があります。初期設定では、グループ優先「レベル 5」は読み取り専用、「レベル 10」は読み取り/書き込み可能です。システムのメンテナンス（ソフトウェアのアップロード、初期設定など）には Privilege Level(優先レベル)「15」が必要です。一般に優先レベル 15 は管理者用アカウント、レベル 10 はユーザ用アカウント、レベル 5 はゲスト用となります。

1.3.2 Privilge Level

このメニューでは、本製品がサポートする各機能に対して Privilege Level を個別に設定することが可能です。設定された Privilege Level と同一もしくはそれ以上の場合、その機能の設定、変更などが可能となります。

Privilege Level Configuration

Group Name	Privilege Levels
Account	10
Aggregation	15
Diagnostics	15
EEE	15
Easyport	15
GARP	15
GVRP	15
IP	15
IPMC Snooping	15
LACP	15
LLDP	15
LLDP MED	15
Loop Protect	15
MAC Table	15
MVR	15
Maintenance	15
Mirroring	15
PoE	10
Ports	10
Private VLANs	15
QoS	15
SFlow	15
SMTP	15
SNMP	15
Security	15
Single IP	10
Spanning Tree	15
System	10
Trap Event	10
UPnP	15
VCL	15
VLANs	15
Voice VLAN	15

Apply　Reset

Figure.1.8

設定方法

WEB 画面のアカウント情報を設定するには以下の手順に従ってください。
Step 1. [Account]→[Privilege Level]を選択します。
Step 2. 該当する[Group Name]に任意の[Privilege Level]を選択します。
Step 3. [Apply]をクリック、設定を反映させます。
Step 4. [Maintenance]→[Save/Restore]→[Save start]を選択します。

設定/表示項目

Group Name
Privilege level を指定するグループの識別名を指します。ほとんどの Group は、単一の機能（たとえば、LACP, RSTP あるいは QoS）で構成されていますが、以下のように複数の機能で Group が構成されているものもあります。

System:
Conatct 情報、Location情報、システムタイム情報

Security:
認証、システムアクセス管理、ポート（Dot1x ポート、MAC ベースおよび MAC アドレスの制限）、ACL、HTTPS, SSH, ARP 検査および IP ソースガード

IP: 'ping'以外のすべて
Port: 'VeriPHY'以外のすべて
Diagnostics: 'ping' および'VeriPHY'.
Maintenance: CLI-システムリブート、システムリストアの初期設定、システムパスワード、設定の保存、設定のロードおよびファーウェアのロード、WEB ユーザ、優先権レベル、メンテナンスのすべて

Debug: CLI 場合のみ.

Privilege Levels
Privilege Group は、グループへのアクセスの認証用の優先順位と同じか、それ以上でなければなりません。

1.4 IP

本製品の IPv4、IPv6 アドレスに関する設定と情報の表示を行います。
本製品では IPv4 及び v6 でのマネジメントに対応しており、手動でのマニュアルにより管理用の IP アドレスを設定することや、DHCP クライアント機能を有効として、DHCP サーバーから動的に取得することが可能です。

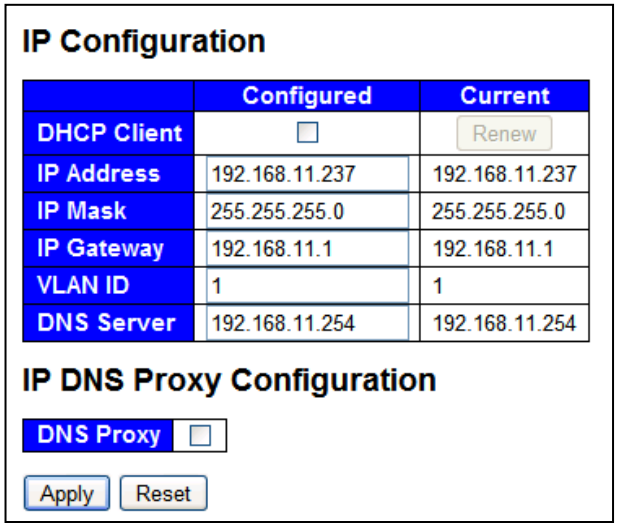
1.4.1 IPv4

このメニューでは静的に設定した場合及び、DHCP Client 機能を有効にした際の動的な IPv4 アドレスに関する設定とその情報の表示、DNS の代理応答機能となる DNS Proxy の設定を行います。

設定方法

IPv4 アドレスを設定する方法については、以下の手順に従ってください。

Step 1.　[IP]→[IPv4]をクリックします。
Step 2.　[Configured]を指定して、必要に応じて
Step 3.　<Apply>ボタンをクリックします。



【注意】: 「Configured」項目の IP 情報を変更すると、「Current」項目に有効な IP の設定が反映、表示されます
【注意】: IP アドレスはフォールバックされることはありません。

設定/表示項目

DHCP Client :
本製品の DHCP クライアント機能を有効化します。

IP Address :
本製品のマネジメント IP アドレスを設定します。

IP Mask :
本製品のサブネットマスクを設定します。

IP Gateway :
本製品のデフォルトゲートウェイのアドレスを設定します。
デフォルトゲートウェイのアドレスは、本製品に設定された IP アドレス、サブネットマスクと同一のネットワークセグメント上である必要があります。

VLAN ID:
マネージメント VLAN の VLAN ID を設定します。

DNS Server :
DNS サーバの IP アドレスを提供します。

DNS Proxy :
DNS プロキシーを有効にすると、クライアント PC からの要求に対して DNS サーバー代理でリクエストを送信します。

1.4.2 IPv6

このメニューでは、IPv6 アドレスに関する設定とその情報の表示を行います。
「Configured」項目の IPv6 情報を変更すると、「Current」項目に有効な IPv6 の設定が表示されます。

設定方法

IPv6 の設定方法については、以下の手順に従ってください。
Step 1. [IP]→[IPv6]をクリックします。
Step 2. IPv6 設定を指定し、必要に応じて「Auto Configuration service」を
　　有効にします。
Step 3. [Maintenance]→[Save/Restore]→[Save start]を選択します。

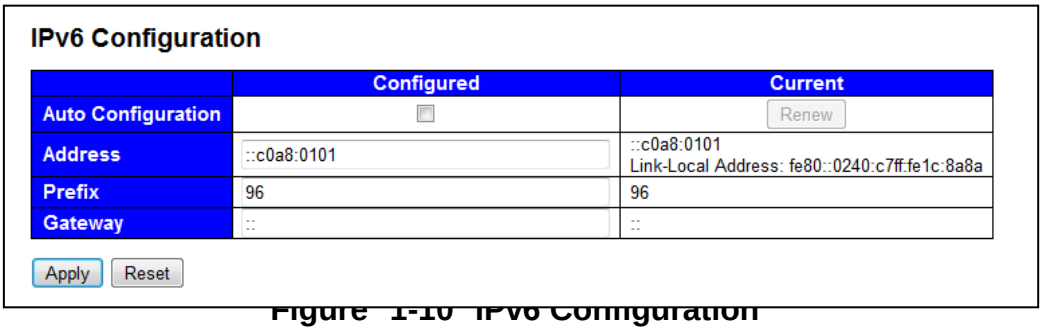


Figure 1-10 IPv6 Configuration

設定/表示項目

Auto Configuration :
IPv6 auto-configuration 機能を設定します。
RA(ルータ要請)に応じてルータなど IPv6 に対応した DHCP サーバーから自動設定を行うため IPv6 アドレスを提供します。
(IPv6 アドレスは、128 ビットを 16 ビットずつ「:」(コロン)で八つに区切り、それぞれ 0～FFFF の 16 進数で表します。)

Prefix :
本製品の IPv6 プレフィックスを提供します。使用可能な範囲は 1～128 です。

Gateway
本製品の IPv6 ゲートウェイアドレスを設定します。
(IPv6 アドレスは、128 ビットを 16 ビットずつ「:」(コロン)で八つに区切り、それぞれ 0～FFFF の 16 進数で表します。)

1.5 Syslog

本製品の Syslog 設定を行います。Syslog 機能を設定することにより、ロギングされたメッセージを外部の Syslog サーバに転送することができ、メッセージの分析/デバッグ及び、ネットワークのシステムの管理とセキュリティの向上に繋げることが可能となります。

1.5.1 Configuration

ここでは、Syslog サーバへの転送を有効とする設定方法について説明します。

設定方法
syslog の設定方法については、以下の手順に従ってください。
Step 1.　[Syslog]→[Configration]をクリックします。
Step 2.　Server Mode を[Enable]に設定します。
Step 3.　syslog サーバの IP アドレスを Server Address に設定します。
Step 4.　<Apply>ボタンをクリックします。
Step 5.　[Maintenance]→[Save/Restore]→[Save start]を選択します。

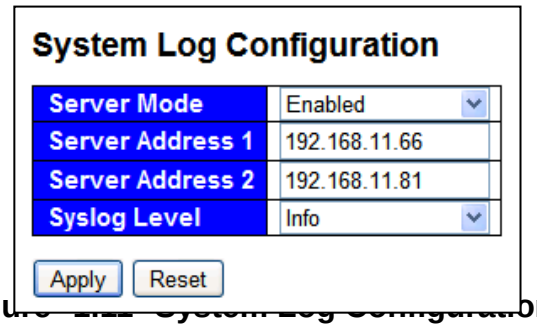


Figure 1.22 System Log Configuration

【注意】:　Syslog メッセージは 514/UDP ポートを用いて Syslog サーバーに送信されます。

設定/表示項目

Server Mode :
Syslog サーバのモードを選択します。このモードを有効にすると、syslog メッセージが、外部に設置した syslog　サーバに送信されます。
syslog プロトコルは UDP 通信をベースにしており、UDP ポート 514 で受信されます。、
また、syslog パケットは syslog サーバが存在しない場合でも送信されます。

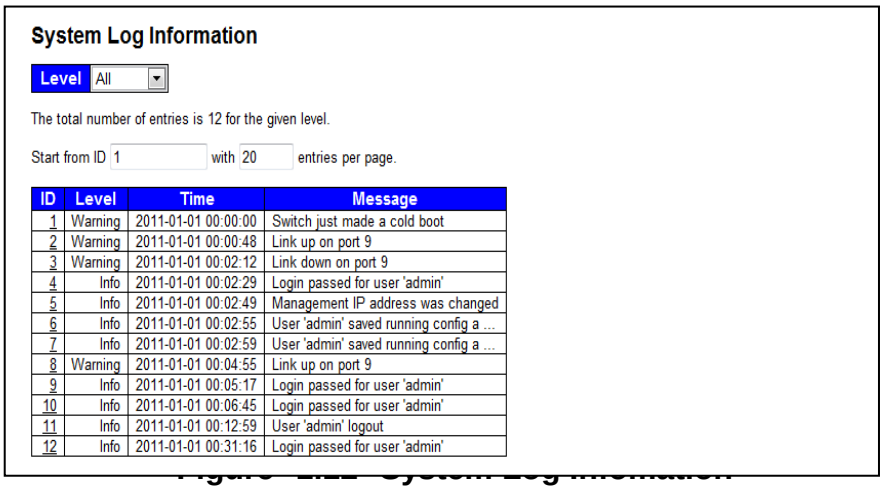
Enabled:
サーバモードを「有効」にします。
Disabled:
サーバモードを「無効」にします。

Server Address :
Syslog サーバのホストアドレスを IPv4 アドレスで設定します。

Syslog Level :
syslog サーバに送信するメッセージのレベル(重要度)を設定します。
設定可能なモードは下記のとおりです。

1.5.2 Log

このメニューでは本製品のシステムのログ情報を表示します。
ログを確認することによりネットワークのシステムの管理と運用、及びセキュリティに約立てることが可能となります。



ID	Level	Time	Message
1	Warning	2011-01-01 00:00:00	Switch just made a cold boot
2	Warning	2011-01-01 00:00:48	Link up on port 9
3	Warning	2011-01-01 00:02:12	Link down on port 9
4	Info	2011-01-01 00:02:29	Login passed for user 'admin'
5	Info	2011-01-01 00:02:49	Management IP address was changed
6	Info	2011-01-01 00:02:55	User 'admin' saved running config a ...
7	Info	2011-01-01 00:02:59	User 'admin' saved running config a ...
8	Warning	2011-01-01 00:04:55	Link up on port 9
9	Info	2011-01-01 00:05:17	Login passed for user 'admin'
10	Info	2011-01-01 00:06:45	Login passed for user 'admin'
11	Info	2011-01-01 00:12:59	User 'admin' logout
12	Info	2011-01-01 00:31:16	Login passed for user 'admin'

設定/表示項目

Level
システムログのエントリのレベルを表します。次のレベルをサポートしています。
<0> Emerg: System is unusable.
<1> Alert: Action must be taken immediately.
<2> Crit: Critical conditions.
<3> Error: Error conditions.
<4> Warning: Warning conditions.
<5> Notice: Normal but significant conditions.
<6> Info Information messages.
<7> Debug: Debug-level messages.

Auto-refresh /Refresh

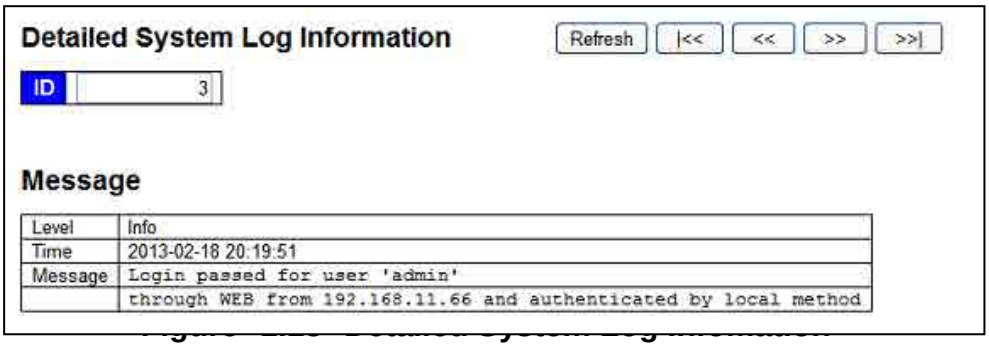
Auto-refresh ☐ Refresh

画面の表示内容を最新の状態に更新します。Auto-refresh を有効にした場合、
おおよそ 3 秒毎に表示内容を最新の状態に更新します。
また Refresh ボタンをクリックし、表示内容をその都度、最新に更新することも可能です。

1.5.3 Detail Log

このメニューでは本製品のログ情報の詳細を確認することが可能です。

詳細なログ情報の表示方法については、以下の手順に従ってください。
Step 1. [Syslog]→[Detailed Log]をクリックします。
Step 2. ログ情報が表示されます。



設定/表示項目

ID
システムログ情報の ID (>= 1)

Message
システムログ情報の詳細なメッセージ

1.6 SNMP

本製品の SNMP 機能の有効化、無効化、Community Strings の設定、Trap の設定など各種 SNMP 機能の設定を行います。

1.6.1 System

このメニューでは SNMP 機能の有効化、無効化及び、SNMPv3 認証の際に用いられる Engine ID の表示をします。

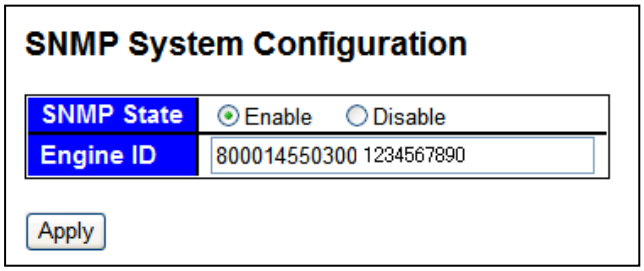


Figure 1.14 SNMP System Configuration

設定/表示項目

SNMP state

SNMP エージェント機能の有効化、無効化を設定します。
(初期値：有効)

Engine ID

SNMPv3 利用時に、エンティティ間で認証と暗号化に用いられる SNMP エンジンを同一のドメイン内で識別するための一意な ID を設定します。

1.6.2 Configuration

このメニューでは本製品の SNMP エージェントへのアクセスを許可する Get Community Strings と Set Community Strings の設定を行います。
では SNMPv1、SNMPv2c に対応しています。よりセキュアなユーザー認証機能を有する SNMPv3 を用いる場合は、SNMP マネージャーとなる装置との間(SNMP エンティティ間)で
Communite Table がサポートされている必要性があります。

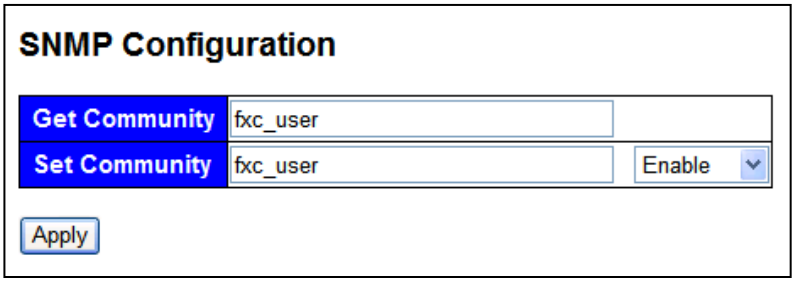


Figure　1.15　SNMP Configuration

設定/表示項目

Get Community
本製品の SNMP エージェントへの読み出し専用(read-only)を行う Community Strings の設定を行います。

半角英数大文字小文字文字及び、ASCⅡコードの 33(0x21)～126 に定められた

一部の記号(！, " ,＃,＄,%,＆,’ ,(,),* ,+,-,、 ,.,/,：,；,＞,＝,＜,？,@)の入力が可能であり、

最大 32 文字まで設定することが可能です。
(初期値：public)

Set Community
本製品の SNMP エージェントへの読み出しと書き込み(read-write)を許可する Community Strings の設定を行います。

半角英数大文字小文字文字及び、ASCⅡコードの 33(0x21)～126 に定められた

一部の記号(！, " ,＃,＄,%,＆,’ ,(,),* ,+,-,、 ,.,/,：,；,＞,＝,＜,？,@)の入力が可能であり、

最大 32 文字まで設定することが可能です。
(初期値：private)
Set Community を利用する場合、Enable に設定してください。

1.6.3 Communities

このメニューでは SNMPv1/v2c を用いた場合、コミュニティと SNMP マネージャの IP アドレスを組み合わせてセキュリティを向上させます。
Community 及び User Name は一意のものを設定してください。
最大のコミュニティ数は「4」となります。

設定方法

SNMP コミュニティの設定方法については、以下の手順に従ってください。
Step 1.　[SNMP]→[Communities]をクリックします。
Step 2.　[Add new community]をクリックします。
Step 3.　「SNMP communities」の項目を入力します。
Step 4.　<Apply>ボタンをクリックします。
※設定内容を修正/クリアしたい場合は<Reset>ボタンをクリックしてください。

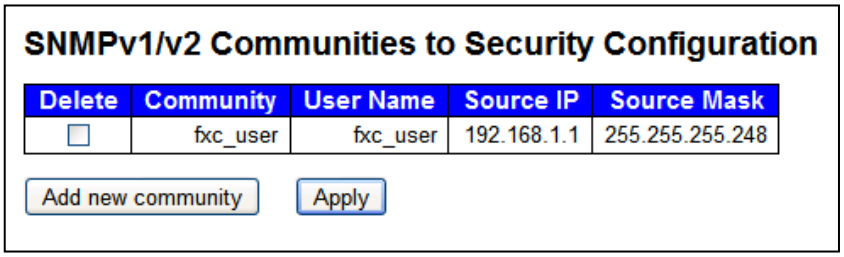


Figure　1.16 SNMPv1/v2 Communities to Security Configuration

設定/表示項目

Delete
設定値を削除します。
設定途中の内容であれば<Delete>ボタン→<Apply>ボタンをクリックすると、その該当項目が削除されます。
また、既に設定された Community であれば、<Delete>のチェックボックスにチェックを入れ<Apply>ボタンをクリックしてください。

Community
SNMPv3 エージェントにアクセスを許可する Community 名を設定します。
設定可能な文字の長さは 1～32 文字、ASCⅡコードの 33(0x21)～126 に定められた一部の記号(！, " ,#, $,%, &,' ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能であり、最大 32 文字まで設定することが可能です。
設定された Community 名は SNMPv3 での Security Name として扱われ、SNMPv1 または SNMPv2cCommunity Strings をマッピングします。

UserName:
SNMPv3 エージェントにアクセス可能な UserName のアクセス文字。

“UserName”は 1～32 文字です。
設定可能な文字の長さは 1～32 文字、ASCⅡコードの 33(0x21)～126 に定められた一部の記号(！, " ,＃, $,%, &,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能であり、最大 32 文字まで設定することが可能です。

Source IP
SNMPv3 エージェントへのアクセス可能のソースアドレスを指します。
Sorce IP と Source Mask と組み合わせるによりアクセス可能なサブネットを制限することが可能です。

Source Mask
SNMPv3 エージェントへのアクセス可能のソースアドレスに対するサブネットマスクを設定します。
Sorce IP と Source Mask と組み合わせるによりアクセス可能なサブネットを制限することが可能です。

1.6.3 Users

このメニューでは SNMPv3 を用いる場合、SNMP エンティティでのユーザーの設定の登録と、そのユーザー認証時のプロトコルとプライバシー機能(暗号化/複合化)の設定を行います。
ユーザー認証とプライバシー機能は、各ユーザー単位での設定が可能です。
盗聴、なりすまし、改ざんなどのネットワークのセキュリティに対する脅威から
SNMP の通信を保護することが可能です。

設定方法

SNMP ユーザを設定する方法については、以下の手順に従ってください。
Step 1. [SNMP]→[Users]をクリックします。
Step 2. [Add New User]ボタンをクリックします。
Step 3. UserName、Security Level などを設定します。
Step 4. [Apply]をクリック、設定を反映させます。
Step 4. [Maintenance]→[Save/Restore]→[Save start]を選択します。
Step 5. [Save]をクリック、設定を保存します。

設定/表示項目

User Name
設定可能な文字の長さは 1～32 文字、ASCⅡコードの 33(0x21)～126 に定められた一部の記号(！, " ,＃, $,%, &,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能であり、
最大 10 ユーザー、最大 32 文字まで設定することが可能です。

Security Level
ユーザー認証とプライバシー機能(暗号化/複合化)を用いる際のセキュティレベルの設定を行います。セキュリティレベルは以下の通りです。

NoAuth, NoPriv :認証プロトコルとプライバシー（暗号化）プロトコルは未設定です。
Auth, NoPriv :認証プロトコルは設定され、プライバシー (暗号化)プロトコルは設定されていません。
Auth, Priv :認証プロトコルとプライバシー(暗号化)プロトコルがともに設定されていることを示します。

Authentication Protocol
Auth が Security Level で設定された際に、使用する認証プロトコルを設定します。
本製品では MD5 プロトコルと SHA プロトコルをサポートしています。

MD5: 認証時に MD5 プロトコルを用います。
SHA: 認証時に SHA プロトコルを用います。

Authentication Password
Security Level で Auth level が選択された場合、認証用の Password の設定を行います。
Authentication Protocol として MD5 が選択された場合、英数字 8～32 文字でパスワードを設定してください。
また、SHA を選択した場合、英数字 8～40 文字で設定してください。
ASCⅡコードの 33(0x21)～126 に定められた一部の記号(！, " ,＃, $,
＆,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)を用いることも可能です。

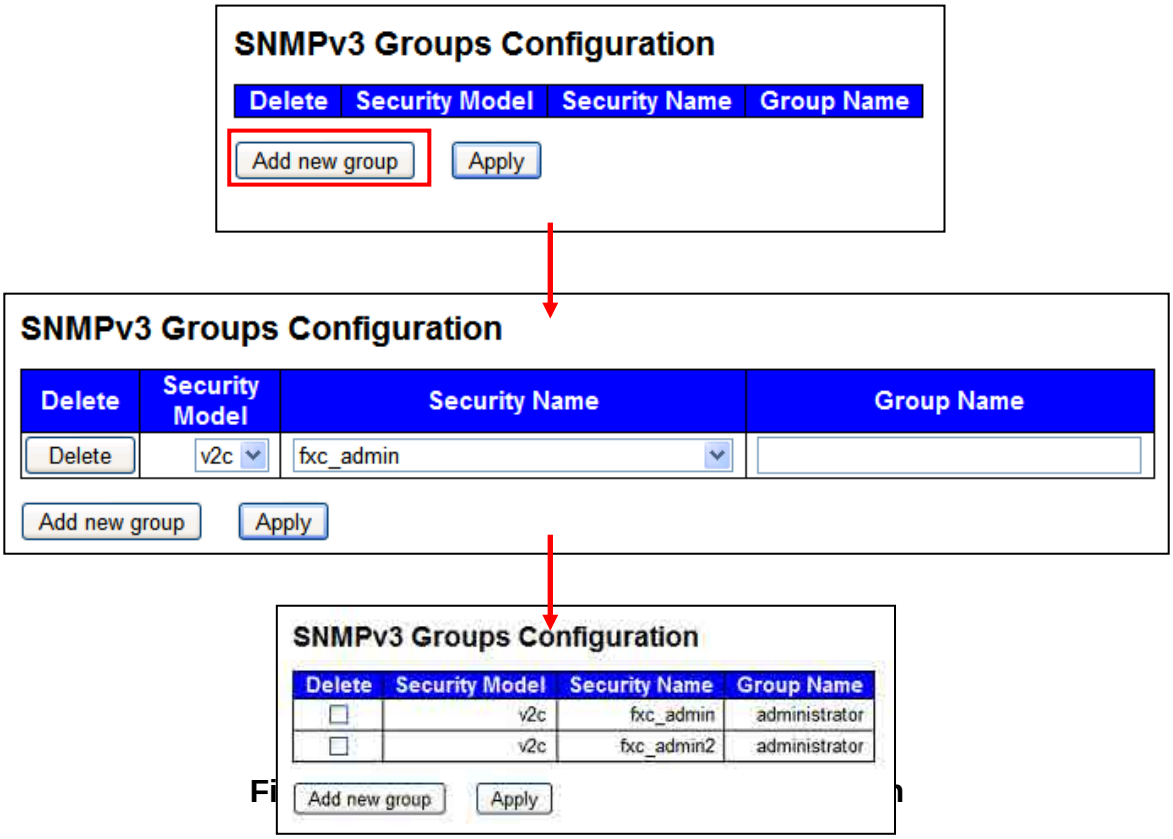
Privacy Protocol
Security Level で Priv level が選択された場合、SNMP の通信内容の DES に基づき共通鍵での暗号化を行います。

1.6.4 Groups

このメニューでは SNMPv3 グループテーブルを作成します。
新しいグループテーブルの作成をする場合、まず最初に Users メニュー、もしくは Communities メニューより、対応させる Security Name を設定ください。

設定方法

SNMP グループテーブルを設定するには、以下の手順に従ってください。
Step 1. [SNMP]→[Groups]をクリックします。
Step 2. [Add new group]をクリックし設定画面にログインします。
Step 3. Security Model/Security Name を選択、Group Name を設定します。
Step 4. <Apply>をクリックし設定を反映します。
Step 5. [Maintenance]→[Save/Restore]→[Save start]を選択します。
Step 6. [Save]をクリック、設定を保存します。



設定/表示項目

Delete
「Delete」の項目に☑して、<Save>ボタンをクリックすると値が削除されます。

Security Model
使用するセキュリティモデルを設定します。
v1: SNMPv1
v2c: SNMPv2c
usm: ユーザベースのセキュリティモデル(USM).

Security Name
SNMPv3 でのセキュリティ名(ユーザー名)が表示されます。
任意のセキュリティ名(ユーザー名)を選択してください。

Group Name
グループのアクセス名を設定します。
半角英数大文字小文字文字及び、ASCⅡコードの 32(0x20)～126 に定められた
一部の記号(！, " ,＃, $,%, &,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能で、
最大 32 文字まで設定することが可能です。

1.6.5 Views

このメニューでは SNMPv3 View Table の作成を行います。
View Table を作成する事によりグループ毎にアクセス可能な MIB ツリーを制限することが可能となります。

設定方法

Step 1. [SNMP]→[Views]をクリックします。
Step 2. <Add new View>ボタンをクリックします。
Step 3. 任意の[View Name]、「View Type」、「OID Subtree」を設定します。
Step 4. <Apply>ボタンをクリックします。
Step 5. [Maintenance]→[Save/Restore]→[Save start]を選択します。
Step 6. [Save]をクリック、設定を保存します。

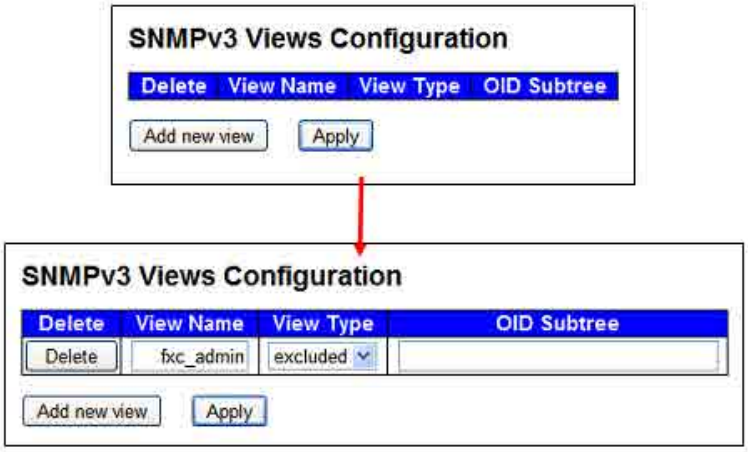


Figure 1.18 SNMPv3 Views Configuration

設定/表示項目

View Name
ビュー名を表す文字列。設定可能な値は「1～32 文字」です。
半角英数大文字小文字文字及び、ASCⅡコードの 32(0x20)～126 に定められた
一部の記号(！, " ,#, $,%, &,' ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能で、
最大 32 文字まで設定することが可能です。

View Type
エントリのビュータイプを指します。

included: ビューのサブツリーに含まれることを示すオプションのフラグ
excluded: ビューのサブツリーに含まれないことを示すオプションのフラグ。
通常、ビューエントリのビュータイプが「excluded」の場合は、'included'のビュータイプを持つ別のビューエントリがあり、その OID サブツリーにより'excluded'ビューエントリは上書きされます。指定したビューに追加するサブツリーのルート。設定可能な OID の長さは「1～128」です。数字またはアスタリスク(*)を使用します。

項目のインデックスキーは OID サブツリーとビュー名です。新しいアカウントを作成する場合は、<Add new view>ボタンをクリックして、ビュー情報に入ってから<Save>ボタンをクリックします。最大グループ数は「28」です。
画面上で SNMPv3 ビューテーブルを設定します。項目のインデックスキーはビュー名と OID サブツリーです。

1.6.6 Access

SNMPv3 へのアクセスの設定に使用します。エントリのインデックスキーは「グループ名」、「セキュリティモデル」および「セキュリティレベル」です。新しいアクセスカウントを設定するには、<Add new access>ボタンをクリックして、アクセス画面にはいってから<Save>ボタンをクリックしてください。最大グループ数は、「14」です。

設定方法

SNMP アクセスの設定を表示するには、以下の手順に従ってください。

Step1. [SNMP]→[Accesses]をクリックします。
Step 2. [Add new Access]をクリックします。
Step 3. SNMP アクセス用の設定項目を入力します。
Step 4. <Apply>をクリックします。
Step 5. [Maintenance]→[Save/Restore]→[Save start]を選択します。
Step 6. [Save]をクリック、設定を保存します。

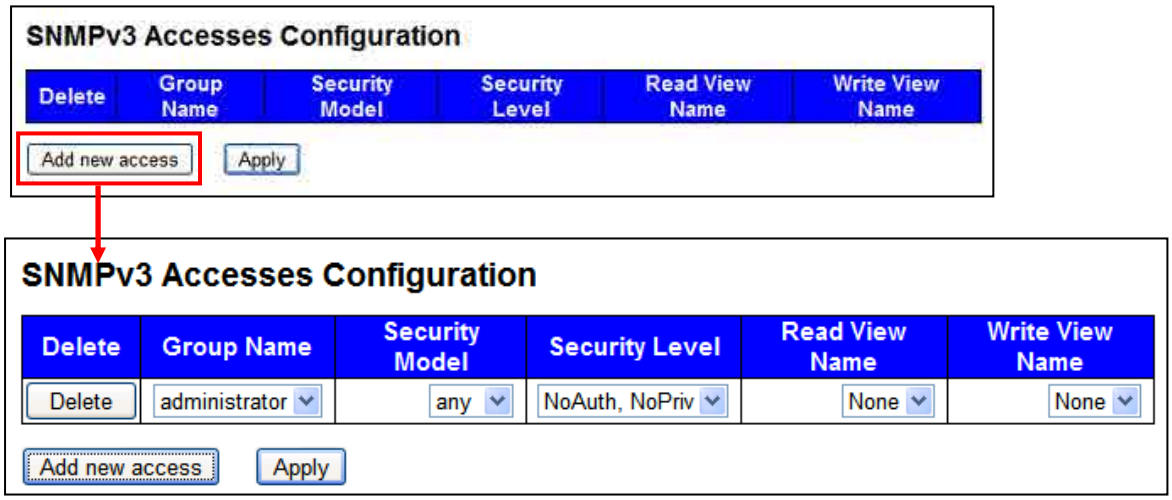


Figure 1.19 SNMPv3 Accesses Configuration

設定/表示項目

Delete
設定値がすべて削除されます。「Delete」をクリックして、<Save>ボタンをクリックすると項目が削除されます。

Group Name
グループ名が表示されます。任意のグループを選択してください。

Security Model
セキュリティモデルを指します。可能なセキュリティモデルは、次のとおりです。

any: セキュリティモデル (v1|v2c|usm).
v1: SNMPv1 用に予約
v2c: SNMPv2c 用に予約.
usm: ユーザベースのセキュリティモデル(USM).

Security Level
エントリのセキュリティモデルを設定します。
可能なセキュリティモデルは次のとおりです。

NoAuth, NoPriv：認証プロトコルとプライバシー（暗号化）プロトコルは未設定です。
Auth, NoPriv ：認証プロトコルは設定され、プライバシー (暗号化)プロトコルは設定されていません。
Auth, Priv ：認証プロトコルとプライバシー(暗号化)プロトコルがともに設定されていることを示します。

Read View Name :
読み出しアクセス可能なビュー名を設定します。このリクエストは現行の値を要求します。
可能な文字の長さは1～32 文字です。ASCII 文字の場合は、33～126 文字です。
設定可能な値は「1～32 文字」です。
半角英数大文字小文字文字及び、ASCⅡコードの 32(0x20)～126 に定められた
一部の記号(！, " ,＃, $,%, &,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能で、
最大 32 文字まで設定することが可能です。

Write View Name :
書き込みアクセス可能なビュー名。このリクエストは、新しい値を設定します。
設定可能な値は「1～32 文字」です。
半角英数大文字小文字文字及び、ASCⅡコードの 32(0x20)～126 に定められた
一部の記号(！, " ,＃, $,%, &,’ ,(,),* ,+,-,、 ,.,/, : , ; ,＞,＝,＜,？,@)の入力が可能で、
最大 32 文字まで設定することが可能です。

1.6.7 Tarp Host Configuration

このメニューでは、SNMP Trap の設定を行います。この機能を設定することにより、「機器に何かが起きたときに、それを管理者に通知する」事が可能となり、異常発生時などネットワークで運用されている本製品のイベントモニタリングを可能にします。

設定方法

SNMP のトラップ機能を設定するには、下記の手順に従ってください。

Step1. [SNMP]→[Trap]をクリックし、[Trap Host Configuration]画面を表示します。

Step 2. [No.]項目から任意の No. をクリックし、[Trap Host Configuration]の詳細を表示します。

Step 3. [Trap Version]、[Server IP]、[Community Name/Security Name]、[Serverity Level]など必要な情報を入力します。

Step 4. [Maintenance]→[Save/Restore]→[Save start]を選択します。

Step 5. [Save]をクリック、設定を保存します。

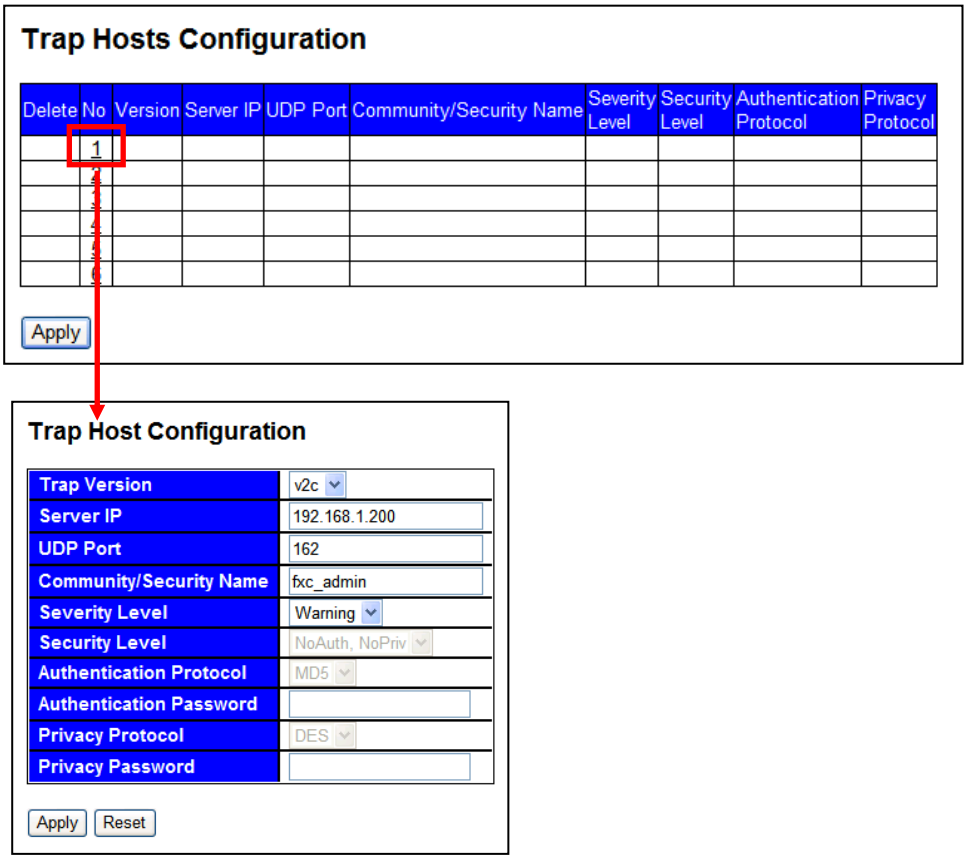


Figure　1.20 Trap Host Configuration

設定/表示項目

Delete:
<Delete>を選択して、<Apply>ボタンをクリックすると、項目が削除されます。

Trap Version:
v1、v2c トラップを選択することが可能です。

Server IP:
SNMPTrap レシーバーとなるホスト IP アドレスを指定します。

UDP Port:
ポート番号を指定します（初期設定: 162/UDP）

Community / Security Name:
“Community / Security Name”文字列の長さは、1-32 文字に制限されます。

Severity Level:
インベントにより発生した Trap の重要度・深刻度を表わします。
設定された Level 以上の

Info: 情報、警告、エラー情報を送信します。
Warning: 警告およびエラー情報を送信します。
Error: エラー情報を送信します。

Security Level:
SNMPv3 を Trap Version として選択したとき、セキュリティレベルの選択可能です。

NoAuth, NoPriv :認証プロトコルとプライバシー（暗号化）プロトコルは未設定です。
Auth, NoPriv :認証プロトコルは設定され、プライバシー (暗号化)プロトコルは設定されていません。
Auth, Priv :認証プロトコルとプライバシー(暗号化)プロトコルがともに設定されていることを示します。

Authentication Protocol:
SNMPv3 を Trap Version として選択し Auth 設定を行った場合、認証用プロトコルとして MD5、または SHA を選択可能です。

Privacy Protocol:
SNMPv3 を Trap Version として選択し Priv 設定を行った場合、DES による共通鍵での SNMP 通信を暗号化することが可能です。

2 章　設定方法

ここでは、ポート、レイヤ 2 ネットワークプロトコル（VLANs, QoS, IGMP, ACLs および PoE）および本機の設定方法など、ネットワークの基本設定について説明します。

2.1 Port

ここでは、ポートの設定方法について説明します。また、ポートの設定方法いにより、ポートを有効/無効にします。ポート情報、または機能のステータスをモニタリングします。

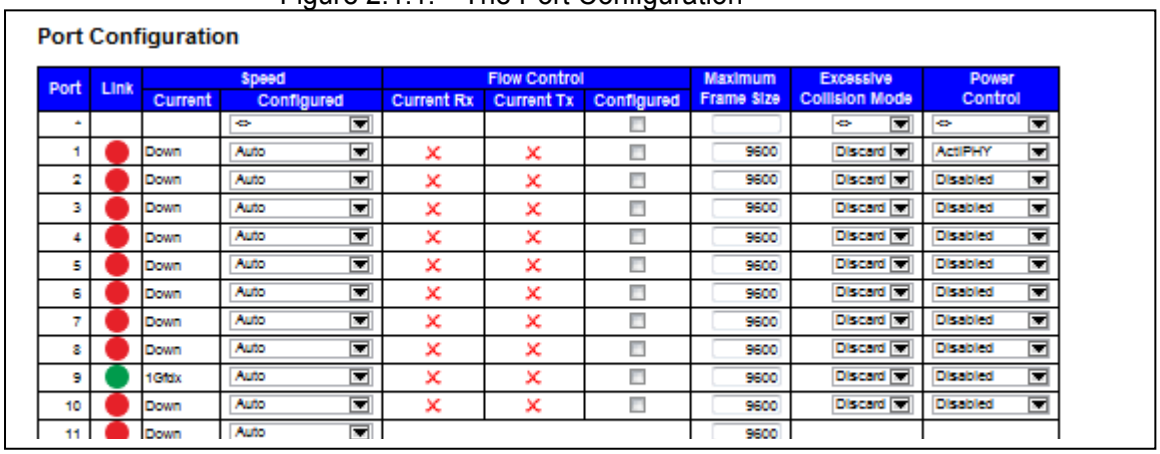
2.1.1 Configuration

ここでは、現行ポートの表示方法、および以下の設定を含む初期設定以外の設定方法について説明します。
リンクアップ/リンクダウン
通信速度（現行および設定 Speed (Current and configured)
フローコントロール(現行の Rx, Current Tx and Configured)
最大フレームサイズ
Excessive コリジョンモード
電源制御.

設定/表示項目

現行のポートの設定方法については、以下の手順に従ってください。
設定可能な文字数は「8 文字」～「32 文字」です。
Step 1.　[Configuration]→[Port]→[Configuration]をクリックします。
Step 2.　通信速度、フロー制御、最大フレームサイズ、Excessive コリジョンモードおよび電源制御を入力します。
Step 3.　<Save>ボタンをクリックします。

Figure 2.1.1:　The Port Configuration



設定/表示項目

Port :
論理ポート番号です。

Link :
現行のリンク状態が表示されます。緑色はリンクアップの状態を示し、赤色はリンクダウンの状態を指します。

Current Link Speed :
現在のポートの通信速度を指します。

Configured Link Speed :
該当ポートの通信速度を選択します。「Auto Speed」により、リンク先との高速通信が可能です。「Disabled」に設定することにより、ポートの設定が無効になります。
ここの設定は対向機器のポート設定と同じにしてください。

Flow Control :
「Auto Speed」を設定した場合は、リンク先に通知されるフロー制御の可・不可が表示されます。
固定通信速度に設定した場合は、通信速度は固定されます
現行の Rx はポートのポーズフレームを受信したかどうか、Tx はポート上のポーズフレームが送信されたかどうかを示します。Rx および Tx の設定値は、オートネゴシエーションの結果に応じて異なります。

Maximum Frame Size :
スイッチのポートに転送可能な最大フレームサイズを入力します。

Excessive Collision Mode :ポートの伝送コリジョンの動作を設定します。
Discard: 16 個のコリジョン後のフレームを破棄します (初期設定)。
Restart: 16 個のコリジョンの後バックオフアリゴリズム(衝突を検出した場合に，送信までの待ち時間の算出)を再開します。

Power Control :
「Usage」では、各ポートの現行の省エネルギーをパーセンテージで表示します。この値により、各ポートの電源消費モードを変更することができます。
Disabled:　省エネルギーをすべて「無効」にします。
ActiPHY:　リンクダウン時の省エネルギーを「有効」にします。
PerfectReach: リンクアップ時の省エネルギーを「有効」にします。
Enabled:　リンクアップ/ダウン時の省エネルギー を「有効」にします。

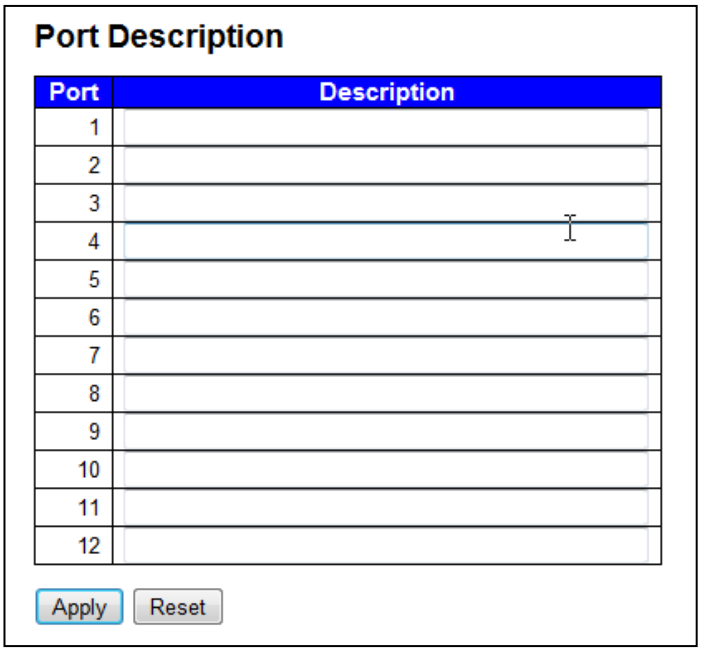
2.1.2 Port Description

ポート情報を設定します。対抗接続機器の各種情報を英文字で入力します。
例えば対向機器の情報などを設定します。

設定方法

ポートの設定方法については、以下の手順に従ってください。
Step 1.　[Configuration]→[Port]→[Port Description]をクリックします。
Step 2.　ポートのエイリアス、または英文字・数字を入力します。
Step 3.　<Save>ボタンをクリックします。

Figure 2.1.2:　The Port Configuration



設定/表示項目

Port :
論理ポート番号です。

Description :
デバイスポートを入力する際、“ # % & ‘ + ¥は使用しないでください。

2.1.3ari Traffic Overview

ここでは、ポートの統計情報について説明します。各ポートのトラフィックの統計情報の概要について説明します。現在接続されている装置のポートが画面上に表示されます。

設定方法

ポートの統計情報を表示する方法については、以下の手順に従ってください。
Step 1.　[Configuration]→[Port]→[Traffic Overview]をクリックします。
Step 2.　自動更新を行う場合は、「Auto-refresh」に☑を入れてください。
Step 3.　<Refresh>ボタンをクリックすると、ポート統計情報が更新され、<Clear>ボタンをクリックするとすべての情報が消去されます。

Figure 2.1.3:　The Port Statisitcs Overview

Port Statistics Overview　Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
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
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	49878	9922	6536219	3464126	0	0	0	0	13845
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

設定/表示項目

Port :
論理ポート番号

Packets :
1 ポートあたりの送受信されたパケット数

Bytes :
1 ポートあたりの送受信されたバイト数

Errors
受信したエラーフレーム数、および 1 ポートあたりのエラー送信数

Drops
入力コリジョン、または出力コリジョンにより破棄されたフレーム数.

Filtered
転送によりフィルタリングされたフレームの受信数

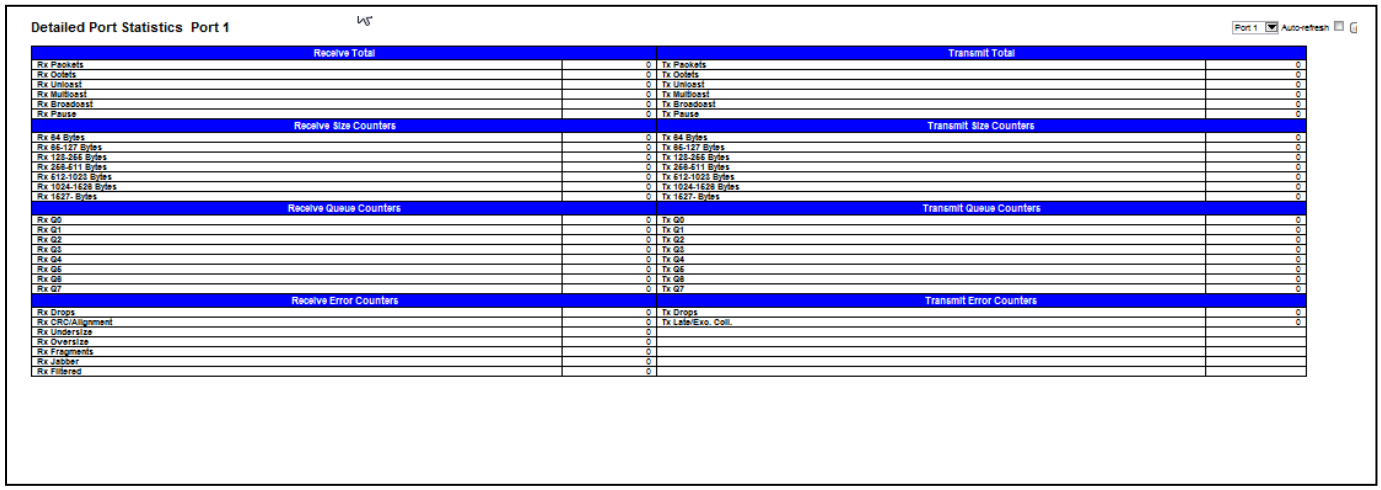
2.1.4 Detailed Statistics

特定のポートのトラフィックの統計情報の表示情報について説明します。ポートを設定した場合は、以下の画面のようにポートの詳細が表示されます。表示したいポート番号が画面右上に表示されます。表示されている数値は送受信したトラフィック、エラー、サイズの合計です。

設定方法

各ポートの統計情報を表示する方法については、以下の手順に従ってください。
Step 1.　[Configuration]→[Port]→[Detailed Statistics]をクリックします。
Step 2.　表示したいポート番号を設定した場合は、次の「Detailed Port statistica overview」の画面が表示されます。
Step 3.　自動更新を行う場合は、「Auto-refresh」に☑を入れてください。

Figure 2.1.4:　The Port Detail Statisitcs Overview



Detailed Port Statistics Port 1

Port 1 Auto-refresh

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1518 Bytes	0	Tx 1024-1518 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exo. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

設定/表示項目

Auto-refresh:
「auto-refresh」に☑を選択した場合は、ポートの統計情報が自動更新されます。

Upper left scroll bar:
表示したいポート（「Port-0」、「Port-1」）を選択して統計情報を指します。

Receive Total and Transmit Total
受信パケットの合計

Rx and Tx Packets :
パケット（良/不良）の送受信数

Rx and Tx Octets :
バイト（良/不良）の送受信数。FCS は含まれますが、フレーム指示ビットは含まれません。

Rx and Tx Unicast
ユニキャストパケット(良/不良) の送受信数

Rx and Tx Multicast :
マルチキャストパケット(良/不良)の送受信数

Rx and Tx Broadcast :
ブロードキャストパケット(良/不良)の送受信数

Rx and Tx Pause :
ポート上で送受信された MAC 制御フレーム数(「PAUSE」フレーム)

Receive and Transmit Size Counters
各フレームサイズに応じてグループごとに分けられた送受信したパケット(良/不良)数

Receive and Transmit Queue Counters
入力/出力キューごとに送受信されたパケット数

Receive Error Counters
受信したエラーパケット数

Rx Drops :
受信バッファまたは egress congestion が原因で破棄されたフレーム数.

Rx CRC/Alignment :
CRC、またはアライメントエラーを持つフレームの受信数

Rx Undersize :
有効な CRC を持つショート1フレームの受信数

Rx Oversize :
有効な CRC を持つ 2 つのロングフレームの受信数

Rx Fragments :
無効な CRC を持つ1つのショートフレームの受信数

Rx Jabber :
無効な CRC を持つ 2 つのロングフレームの受信数

Rx Filtered :
転送処理によってフィルタリングされたフレームの受信数
ショートフレームは、64 バイト未満のフレーム
ロングフレームは、設定された最大フレーム長より長いフレーム

Transmit Error Counters
送信エラーパケット数

Tx Drops :
出力バッファの輻輳により破棄されたフレーム数

Tx Late/Exc. Coll. :
過度のレートコリジョンにより破棄されたフレーム数

2.1.5 Qos Statistics

ここでは、QoS（特定ポートのキューカウンターの詳細、すべてのポートの異なるキュー）について説明します。ポートは画面のヘッダに表示されています。

設定方法

キューカウンタの表示方法は、以下の手順に従ってください。
Step 1.　[Configuration]→[Port]→[QoS Statistics]をクリックします。
Step 2.　自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3.　<Refresh>ボタンをクリックすると、ポート統計情報が更新され、<Clear>ボタンをクリックするとすべての情報が消去されます。

Figure 2.1.5:　The Queuing Counters Overview

Queuing Counters　Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	52520	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10386
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

設定/表示項目

Port :
論理ポート

Qn :
Qn はキュー番号、ポート単位の QoS キュー。Q0 は最下位のプライオリティキューです。

Rx/Tx :
キューごとのパケットの送受信数

Auto-refresh:
自動更新を行う場合は、「Auto-refresh」に☑をいれてください。

Upper right icon (Refresh, clear)
< refresh >ボタンをクリックしてキューカウンタを更新するか、手動で削除してください。

2.1.6 SFP Information

ここでは、本体に接続用の SFP モジュールについての詳細情報について説明します。情報には、コネクタタイプ、ファイバタイプ、波長、ボーレート、ベンダーOUI が含まれます。

設定方法

SFP 情報を表示するには、以下の手順に従ってください。

Step 1. [Configuration]→[Port]→[SFP Information]をクリックすると、次の画面が表示されます。

Figure 2.1.6:　The SFP Information Overview

SFP Information for Port 11

Connector Type	none
Fiber Type	none
Tx Central Wavelength	none
Bit Rate	none
Vendor OUI	none
Vendor Name	none
Vendor P/N	none
Vendor Revision	none
Vendor Serial Number	none
Date Code	none
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

設定/表示項目

Connector Type:
UTP, SC, ST, LC などのコネクタタイプが表示されます。

Fiber Type:
マルチモード、シングルモードなどのファイバーモードが表示されます。

Tx Central Wavelength:
850nm, 1310nm, 1550nm などの光ファイバー伝送セントラル波長を指します。

Baud Rate:
10M, 100M, 1G などのファイバーモジュールの最大ボーレートを指します。

Vendor OUI:
IEEE によって割り当てられたメーカーの OUI コードを指します。

Vendor Name:
モジュールメーカーの会社名を指します。

Vendor P/N:
モジュールメーカーの製品名が表示されます。

Vendor Rev (Revision):
モジュールのリビジョンが表示されます。

Vendor SN (Serial Number):
メーカーにより割り当てられたシリアル番号を指します。

Date Code:
SFP モジュールの製造日が表示されます。

Temperature:
SFP モジュールの現行温度が表示されます。

Vcc:
SFP モジュールの動作 DC 電圧が表示されます。

Mon1(Bias) mA:
SFP モジュールのバイアス電流

Mon2(TX PWR):
SFP モジュールの伝送出力が表示されます。

Mon3(RX PWR):
SFP モジュールの受信出力が表示されます。

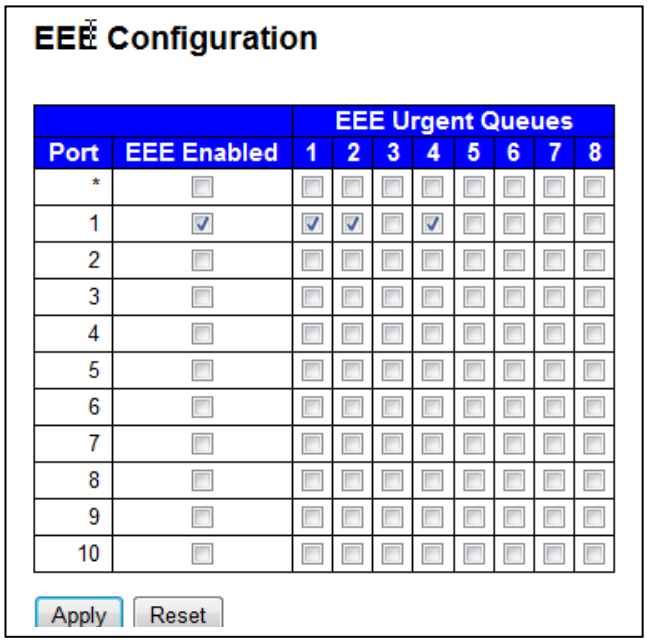
2.1.7 EEE

ここでは、現行の EEE ポートの確認および設定方法について説明します。
EEE は、 省エネのオプションにより、トラフィックの使用率が低い場合（またはトラフィックがない場合）は電源の消費を抑えます。
EEE は、トラフィックがない場合回路の電力を下げることにより動作します。データを入手すると、電源が「ON」になります。回路の電源が「ON」になるまでの時間を「wakeup time」といいます。初期設定時の「wakeup time」は、1G ビットの場合は「17us」、その他の通信速度の場合は「30us」です。EEE デバイスは、トラフィックの伝送時に送受信デバイスの回路の電源が「ON」になったことを確認するために「wakeup タイム」の値と一致している必要があります。
省エネを最大限にするには、回路はポートにデータを伝送する準備ができても直ちに開始せず、3000 バイト以下のデータが送信状態になるまで待機します。
3000 バイト以下のデータが伝送されるまで大幅な遅延が生じないように対応しており、データは常に「48us」後に伝送され、最大でも「48us」に wakeup タイムを加算した遅延のみです。
特定フレームの遅延を最小化にしたい場合は、フレームを特定のキュー(QOS による処理)にマッピングして、緊急のキューとしてマーク付けします。緊急キューが伝送したいデータを受け取ると、回路は直ちに「ON」になるため、遅延時間は wakeup タイムのみです。

設定方法

EEE 設定については、以下の手順に従ってください。
Step 1. [Configuration]→[Port]→[EEE]をクリックします。
Step 2. EEE 機能を有効にしたいポートを選択します。
Step 3. EEE Urgent キューレベル（1～8）。キューは 3000 バイトの伝送が可能になるまで待機します。
Step 4. <Save>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.1.7:　The EEE Configuration



設定/表示項目

EEE Port Configuration:
EEE ポートの設定現在選択しているスタックユニット に関するポートの設定情報

Port :
論理ポート番号

EEE Enabled :
ポートの EEE を有効にします。

EEE Urgent Queues :
キューセットは、データが伝送可能な状態になると、フレームの伝送を有効にします。
それ以外は、キューは 3000 バイトの伝送が可能になるまで待機します。

2.2 ACL

本機のアクセスコントロールリスト(ACL)は、パケットのフィルタリングに使用されるだけでなく、解析したり、伝送したいトラフィックのタイプでの設定が可能です。ACL は、イーサタイプ、IPv4, ARP プロトコル、MAC および VLAN パラメータなどに分けられます。
TCP/IP の標準/拡張アクセスリストで入力クラスの ACE を作成すると、ポートごとにポリシーを割り当てることができます。ポリシー番号は 1～8 までで、どのポートにも各ポリシーは適用可能なため、どのタイプの ACL ポリシーが動作しているか容易に判別することができます。

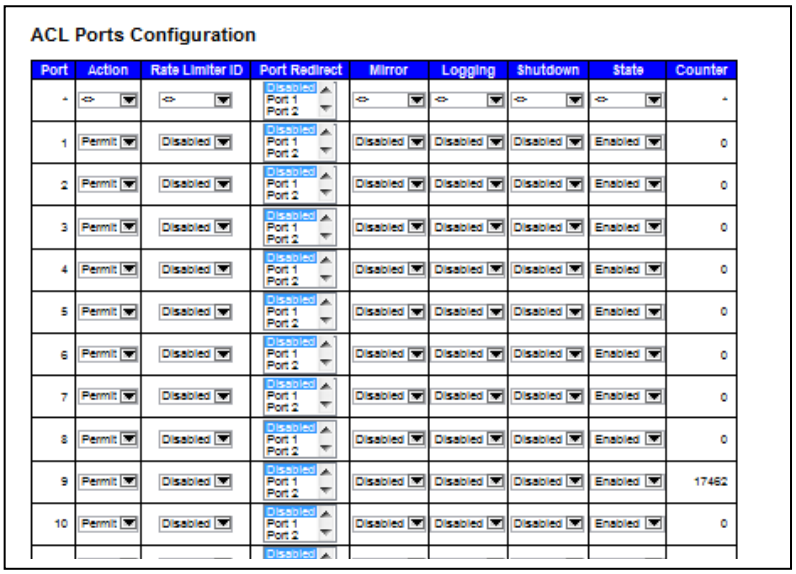
2.2.1 Ports

ここでは、各ポートの ACL パラメータ (ACE)の設定方法について説明します。フレームが特定の ACE と一致しない場合は、受信したフレームはこれらのパラメータによって異なります。

設定方法

ACL ポートの設定方法については、次の手順に従ってください。
Step 1. [Configuration]→[ACL]→[Port]をクリックします。
Step 2. 特定のパラメータの値を選択して、ポートの ACL の正しい値を設定します。
Step 3. <save>ボタンをクリックして、設定値を保存します。
Step 4. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。
Step 5. 設定が完了後、ポートのカウンタを確認してカウンタを更新する場合は<Refresh>ボタン、情報をクリアにしたい場合は<Clear>ボタンをクリックします。

Figure 2.2.1:　The ACL Ports Configuration



設定/表示項目

Port :
設定用の論理ポート

Action :
伝送を許可("Permit")するか、拒否("Deny")するかを選択します。
初期設定は、「Permit」です。

Port Redirect
コピーするポート選択します。設定可能な値は「Disabled」または特定のポート番号です。初期設定は「Disabled」です。

Rate Limiter ID :
ポートに適用するレートリミッタを選択します。設定可能な値は「Disabled」または「1～16」です。次項の Rate Limiter で値を設定し、その番号を設定します。

Mirror :
ポートのミラーリング機能を設定します。
Enabled: ポート上で受信したフレームをミラーリングします。
Disabled: ポート上で受信したフレームをミラーリングしません。
初期設定は、「Disabled」です。

Logging :
このポートのログ情報を指定します。
Enabled: ポート上で受信したフレームをシステムログにストアします。
Disabled: ポート上で受信したフレームをストアしません。
初期設定は「Disabled」です。システムログのメモリサイズおよびログレートは制限されます。

Shutdown :
ポートのシャットダウンを行います。
Enabled: フレームを受信した場合に、ポートは無効になります。
Disabled: ポートのシャットダウンは無効です。
初期設定は、「Disabled」です。

Counter :
ACE と一致したフレーム数をカウントします。

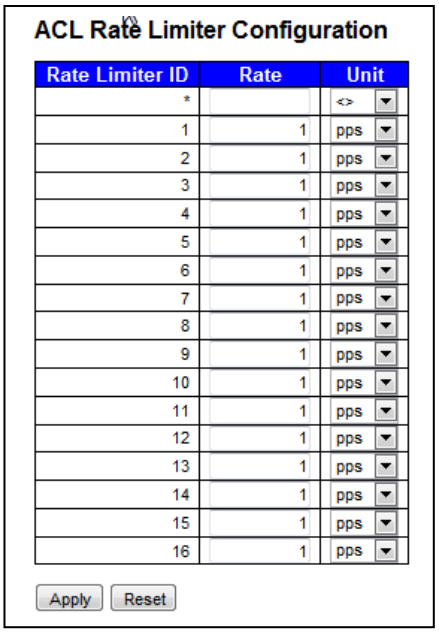
2.2.2 Rate Limiters

ここでは、ACL の Rate Limiter の設定方法について説明します。1～16 までの Rate Limiter のレベルに応じて、「pps」 または 「kbps」単位およびレートの値を設定することが可能です。

設定方法

ACL レートリミタの設定方法については、以下の手順に従ってください。
Step 1.　[Configuration]→[ACL]→[Rate Limiters]をクリックします。
Step 2.　「Rate」項目に「0」～「3276700」の値を設定してください。
Step 3.　単位(“pps”または“kbps”)をスクロールして選択します。
Step 4.　<Save>ボタンをクリックして、設定を保存します。
Step 5.　設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.2.2:　The ACL Rate Limiter Configuration



Rate Limiter ID	Rate	Unit
*		<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

設定/表示項目

Rate Limiter ID :
設定した ID

Rate:
設定可能な値は: 0～3276700（pps）、または 0, 100, 200, 300, ..., 1000000 （kbps）です。

Unit :
レートの単位を指定します。
pps: 秒単位のパケット数
kbps: 毎秒の Kbits

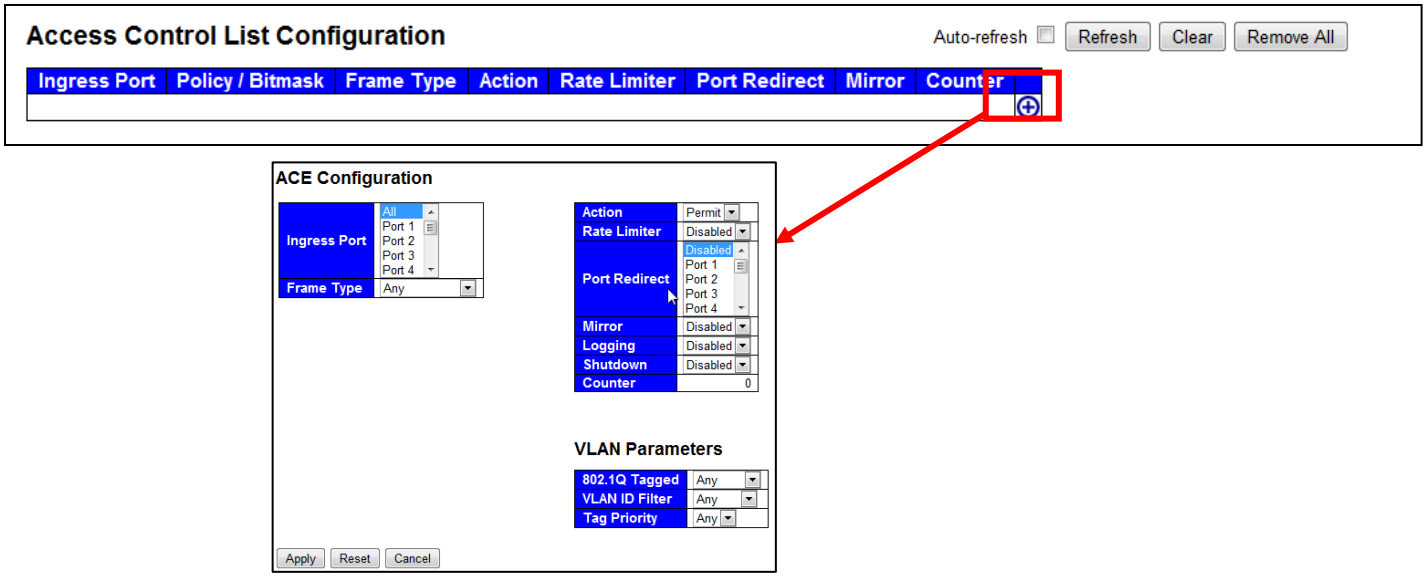
2.2.3 Access Control List

ACL（Access Control List）のルールの設定方法について説明します。
ACL は、IP アドレス、MAC アドレス、それ以外の特定の基準に適用する条件を許可/拒否を行うアクセスリストです。ACL の条件に対して個々に入力パケットのテストを行います。
許可（permit）ルールと一致するとパケットを受け取り、拒否（deny）ルールと一致するとパケットを破棄します。
ルールに一致しない場合は、フレームを受け取ります。それ以外は、レートリミット、他のポート、またはシステムログへのパケットのコピー、あるいはポートのシャットダウンなど一致するパケットを検出すると、その設定に従います。
ACL は、各スイッチで定義されている ACE で構成されており、各行にそれぞれ ACE について説明しています。ACE の最大数は「256」です。一番右側の⊕をクリックすると、新しい ACE がリストに追加されます。内部プロトコル用に予約されている ACE の編集/削除を行うことはできません。それらの、プライオリティは一番上になります。

設定方法

ACL の設定方法については、以下の手順に従ってください。
Step 1. [Configuration]→[ACL]→[Access Control List]をクリックします。
Step 2. ⊕ボタンをクリックして、新しい ACL を追加するか、他の ACL 修正ボタンをクリックして編集（編集、削除またはリスト内の関連場所への移行）を行います。
Step 3. ACE のパラメータを指定します。
Step 4. <Save>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。
Step 6. ACE 設定画面の項目を編集する場合は、表示項目はフレームタイプ、IP プロトコルタイプなどの選択項目によって異なります。ルールに一致する関連する基準を指定すると、ルール（「Rate Limiter」、「Port Copy」、「Logging」および「Shutdown」など）に一致した場合その処理を行います。

Figure 2.2.3:　The ACL Rate Limiter Configuration



設定/表示項目

Ingress Port :
ACE の入力ポートを指します。
Any: ACE は入力ポートと一致します。
Policy:　ACE は特定のポリシーをもつ入力ポートと一致します。
Port: ACE は特定の入力ポートと一致します。

Frame Type :
ACE のフレームタイプを指します。
Any:　　いかなるフレームタイプにも一致します。
Ethernet type:イーサネットタイプのフレームに一致します。
なお、IP および ARP フレームに対しては設定できません。
ARP:　　ARP/RARP フレームと一致します。
IPv4:　　すべての IPv4 フレームと一致します。

Action :
ACE の伝送処理を指します。
Permit: ACE と一致するフレームは伝送され学習されます。
Deny: ACE に一致するフレームは破棄されます。

Rate Limiter :
ACE のレートリミター番号を指します。設定可能な範囲は 1～16 です。「Disabled」が表示されている場合は、レートリミターは無効となります。

Port Redirect
コピーするポート選択します。設定可能な値は「Disabled」または特定のポート番号です。初期設定は「Disabled」です。

Mirror :
ポートのミラーリング機能を指定します。
Enabled: ポートで受信したフレームのミラーリングを行います。
Disabled: ポートで受信したフレームのミラーリングを行いません。
初期設定は、「Disabled」.です。

Logging :
ACE のログを指します。
Enabled: ACE と一致したフレームはシステムログに保存されます。
Disabled: ACE に一致したフレームはログを採取しません。
システムログのメモリサイズおよびログレートは制限されますので注意してください。

Shutdown :
ACE をシャットダウンします。
Enabled: フレームが ACE と一致した場合は、入力ポートは無効になります。
Disabled: ACE のシャットダウンは無効になります。

Counter :
フレームが ACE と一致した回数を指します。

VLAN Parameters
ACE の VLAN の設定を行います。

802.1Q Tagged
Any:どのタグでも一致します。
Enable:タグフィルタを設定します。
Disable:タグフィルタを設定しません。

VLAN ID Filter
VLAN ID を指定します。
Any:どの ID でも一致します。
Specific:VLAN ID を指定します。

Tag Priority
Any:どのプライオリティも一致します。
0 – 7:プライオリティを指定します。

修正ボタン
表の ACE(Access Control Entry)を修正するには、以下のボタンを使って編集してください。
:現行の行の前に新しい ACE を挿入します。
: Edits the ACE の行を編集します。
: ACE を上に移動します。
: ACE を下に移動します。
: ACE を削除します。
: リストの一番下に新しい項目を追加します。

2.2.3 ACL Status

各 ACL ユーザの ACL ステータスの表示方法について説明します。それぞれ定義されている ACE について説明しています。ハードウェアの制限により特定の ACE が適用されない場合コンフリクトが生じます。各スイッチの ACE の最大数は「256」です。

設定方法

ACLステータスを表示するには、次の手順に従ってください。
Step 1.　[Configuration]→[ACL]→[ACL status]をクリックします。
Step 2.　自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3.　<Refresh>ボタンをクリックすると、 ACLステータスが更新されます。

Figure 2.2.3:　The ACL Rate Limiter Configuration

ACL Status　Combined　Auto-refresh　Refresh

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
IP Management	All	ARP	Deny	Disabled	Disabled	Disabled	Yes	No	26901	No
IP Management	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Disabled	Yes	No	0	No
Reserved	All	EType	Permit	Disabled	Disabled	Disabled	No	No	0	No
Reserved	All	EType	Permit	Disabled	Disabled	Disabled	No	No	0	No

設定/表示項目

User :
ACL ユーザを指します。

Ingress Port :
ACE の入力物理ポートを指します。
Any: ACE はどの入力ポートにも一致します。
Policy: ACE は特定のポリシーを持つ入力ポートと一致します。
Port: ACE は特定の入力ポートと一致します。

Frame Type :
ACE のフレームタイプを指します。
Any:　ACE はどのフレームタイプにも一致します。
EType: ACE はイーサネットタイプのフレームと一致します。イーサネットタイプは ACE をベースとしており、IP フレームおよび ARP フレームとは一致しません。

【注記】:
イーサネットベース ACE は、IP および ARP フレームとは一致しないため 注意してください。
MAC アドレスでの ACE の設定は不可である点に注意してください。

Action :
ACE の転送処理を指します。
Permit: ACE と一致するフレームは伝送され学習されます。
Deny: ACE と一致するフレームは破棄されます。

Rate Limiter :
ACE のレートリミッタ番号を指します。設定可能な範囲は 1～16 です。「Disabled」が設定されている場合は，無効になります。

Port Copy :
ACE のポートへのコピーを行います。ACE と一致するフレームをポート番号にコピーします。設定可能な値は「Disabled」が設定されている場合は、無効になります。

Mirror :
ポートのミラーリング機能を設定します。設定可能な値は以下のとおりです:
Enabled: ポートで受信したフレームのミーリングを行います。
Disabled: ポートで受信したフレームのミラーリングを行いません。
初期設定は、「Disabled」です。

CPU :
特定の ACE と一致するパケットを CPU へ伝送します。

CPU Once :
特定の ACE と一致する最初のパケットを CPU へ伝送します。

Counter :
ACE がフレームと一致した回数を指します。

Conflict :
特定の ACE のハードウェアのステータスを指します。特定の ACE は、ハードウェア制限により適用されません。

2.3 Aggregation

アグリゲーションは、リンク集約を設定するために使用します。一つの論理ポートとして複数のポートに同じ通信速度、全二重でバンドルすることにより、論理ポートは複数のポートのバンド幅を集約して使用できます。イーサネット機器にバンド幅のアグリゲーションを設定することができます。たとえば、論理ポートで 3 つのファーストイーサネットポートを集約した場合、論理ポートは 1 つのファーストイーサネットポートの 3 倍のハンド幅となります。

2.3.1 Static Trunk

手動によるシンク集約の設定を行います。同じ通信速度、全二重の複数のポートを一つの論理ポートに設定することにより、複数のバンド幅で通信が可能です。
対向機器が同一の場合、使用することが可能です。

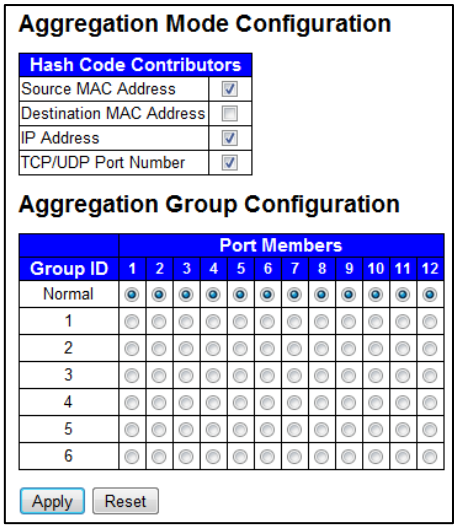
2.3.1.1 Static Trunk

トランク方式としてスタティックトランクを使用すると、固有のスタティック GroupID を選択して論理トランクポートを作成することができます。同一機器のリンクの両側のスタティックトランクを使用することをお勧めします。スタティックトランクを使用する際に通信速度が低い場合は“not ready”の状態になり、通信速度が速い場合のみアグリゲートされるため注意してください。

設定方法

トランクアグリゲーションのハッシュモードおよびアグリゲーショングループを設定するには、次の手順に従ってください。
Step 1.　[Configuration]→[Aggregation]→[Static Trunk]をクリックします。
Step 2.　アグリゲーションのハッシュモード機能を有効/無効にします。アグリゲーショングループの ID とポートメンバを選択してください。
Step 3.　<Save>ボタンをクリックして、値を保存します。
Step 4.　設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.3.1.1:　The Aggregation Mode Configuration



設定/表示項目

Hash Code Contributors
Source MAC Address :
送信元 MAC アドレスを使ってフレームの宛先ポートを算出します。☑を選択した場合は送信元 MAC アドレスが有効となり、☑を選択しない場合は無効になります。初期設定では、送信元 MAC アドレスは有効です。

Destination MAC Address :
宛先 MAC アドレスを使って、フレームの宛先ポートを算出します。☑を選択した場合は宛先 MAC アドレスが有効となり、☑を選択しない場合は無効になります。初期設定では、宛先 MAC アドレスは有効です。

IP Address :
IP アドレスを使ってフレームの宛先ポートを算出します。☑を選択した場合は IP アドレスが有効となり、☑を選択しない場合は無効になります。初期設定では、IP アドレスは有効です。

TCP/UDP Port Number :
TCP/UDP ポート番号を使ってフレームの宛先ポートを算出します。☑を選択した場合は TCP/UDP TCP/UDP ポート番号が有効となり、☑を選択しない場合は無効になります。初期設定では、TCP/UDP ポート番号は有効です。

Aggregation Group Configuration

Group ID :
設定内容のグループ ID を指します。"Normal"はアグリゲーションがないことを指します。ポートごとにグループ ID は1つのみ有効です。

Port Members :
それぞれポートは各グループ ID ごとにリストされます。☑を選択した場合はポートはアグリゲーションに設定され、☑を選択しない場合はポートはアグリゲーションから削除されます。デフォルト設定では、ポートにアグリゲーション機能はありません。アグリゲーションに設定できるポートは全二重のみで、各グループのポートの通信速度は同じ速度に設定してください。

2.3.2 LACP

リンク集約機能として、LACP(Link Aggregation Control Protocol)は IEEE 802.3ad 仕様に準拠しており、固有の LACP GroupID を選択して、論理上トランクポートを設定することができます。LACP を使用すると、
ポートは“論理トランクポート”用の固有 LACP GroupID を選択することができます。
LACP は、トランクポート(”アグリゲーター”とも呼ぶ)のメンバーにする前に対向機器とネゴシエーションを行います。LACP は、他のトランキング方式(スタティックトランク)よりもより安全です。

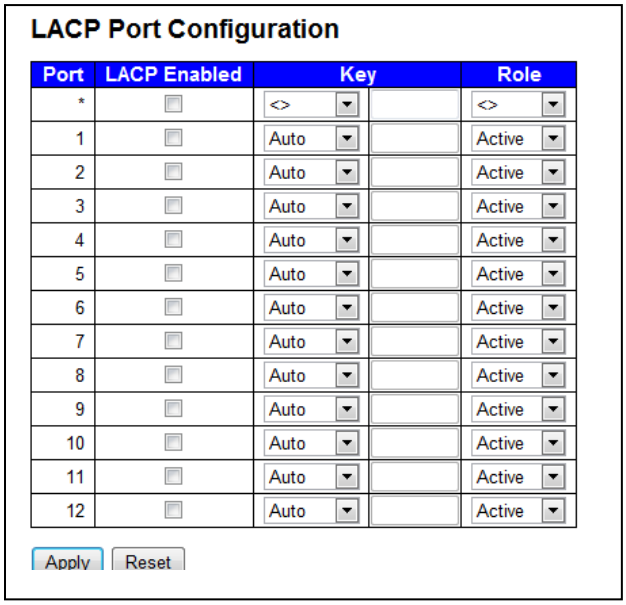
2.3.2.1 Configuration

現行の LACP ポートの設定を確認して、複数の待機状態のポートが LACP のトランクグループになるように変更することができます。
対向機器も LACP(Link Aggregation Control Protocol)は IEEE 802.3ad 仕様に準拠している必要があります。

設定方法

トランクアグリゲーションの LACP を設定するには、以下の手順に従ってください。
Step 1.　[Configuration]→[Aggregatopm]→[LACP]→[Configuration]をクリックします。
Step 2.　ポートの LACP の有効/無効を設定します。「Key」の項目から「Auto」または「Specific」のいずれかを選択します。初期設定は、「Auto」です。
Step 3. 「Role」の設定項目から「Active」または「Passive」のいずれかを選択します。初期設定は、「Active」です。
Step 4.　<Save>ボタンをクリックして、値を保存します。
Step 5.　設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.3.2.1:　The LACP Port Configuration



設定/表示項目

Port :
物理ポート番号を指します。

LACP Enabled :
Controls whether LACP の設定を行います。LACP は 2 ポート以上を同一パートナーと接続する場合にアグリゲーションを設定します。LACP は、スイッチにつき集約を「12」まで設定可能です。

Key :
「Key」の値（範囲: 1-65535）。「Auto」に設定した場合、物理的なリンク通信速度（10Mb = 1, 100Mb = 2, 1Gb = 3）に設定されます。「Specific」に設定した場合、対向と同じ値を設定してください。

Role :
LACP のステータスが表示されます。
Active：毎秒ごとに LACP パケットを伝送します。
Passive：リンク先からの LACP パケットの受信を待ちます。

2.3.2.2 System Status

LACP 機能を設定完了後、すべての LACP インスタンスのステータスの概要について説明します。

設定方法

LACP システムのステータスを表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[LACP]→[System Status]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、LACP システムのステータスが更新されます。

Figure 2.3.2.2:　The LACP System Status

LACP System Status

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners				

設定/表示項目

Aggr ID :
アグリゲーションインスタンスに関連のアグリゲーション ID。
LLAG の場合は、id は'isid:aggr-id'、GLAGs の場合は'aggr-id'として表記されます。

Partner System ID :
アグリゲーションパートナーのシステム ID (MAC アドレス)

Partner Key :
パートナーはアグリゲーション ID に割り当てられているキー

Last changed :
アグリゲーションが変更した時間

Local Ports :
本機/スタック用のアグリゲーションのポートが表示されます。"Switch ID:Port"と表記されます。

2.3.2.3 Port Status

ここでは、LACP 機能の設定を完了してからのすべての LACP インスタンスのポートステータスの概要について説明します。

設定方法

LACP ポートのステータスを表示するには、次の手順に従ってください。
Step 1. [Configuration]→[LACP]→[Port Status]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、LACP ポートのステータスが更新されます。

Figure 2.3.2.3:　The LACP Status

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-

設定/表示項目

Port :
ポート番号を指します。

LACP :
「Yes」は、LACP が有効に設定されポートのリンクが接続されている状態です。「No」の場合は、LACP が無効か、ポートのリンクが解除されている状態です。'Backup'は、ポートはアグリゲーショングループに設定できませんが、他のポートが解除されている場合のみ有効となることを表します。その間 LACP ステータスは無効となります。

Key :
このポートに割り当てられるキー。同じキーを持つポートのみがアグリゲート可能です。

Aggr ID :
アグリゲーショングループに割り当てられているアグリゲーション ID。ID 1 および 2 は GLAGs、IDs 3.14 は LLAGs です。

Partner System ID :
リンク先のシステム ID (MAC アドレス)

Partner Port :
ポートに接続されているリンク先のポート番号

2.3.2.4 Port Statistics

ここでは、LACP 機能の設定後のすべての LACP インスタンスのポートの統計情報の概要について説明します。

設定方法

LACP ポートのステータスを表示するには以下の手順に従ってください。
Step 1. [Configuration]→[Aggregation]→[LACP]→[Port Statistics]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、LACP 統計情報は更新されます。

Figure 2.3.2.4:　The LACP Statistics

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-

設定/表示項目

Port :
ポート番号を指します。

LACP Received :
各ポートで受信する LACP フレーム数が表示されます。

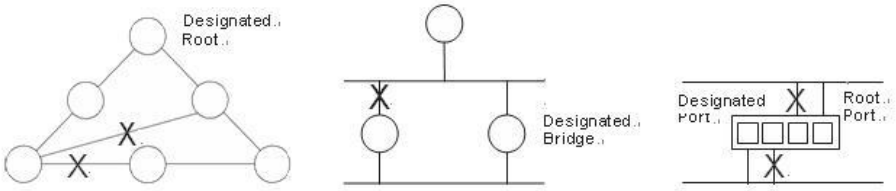
LACP Transmitted :
各ポートから送信された LACP フレーム数が表示されます。
Discarded :
各ポートで破棄されたアンノウン、または不正の LACP フレーム数が表示されます。

2.4 Spanning Tree

STP(スパニングツリープロトコル)は、LAN におけるループを検出し、スイッチ、ブリッジ、ルータ間でリンクのバックアップを行います。これにより、お使いのネットワーク環境で、スイッチは他のブリッジデバイス（STP 対応スイッチ、ブリッジ、ルータ）との間で相互に通信を行い、ステーション間で1つの通信経路を確立し、リンクが切れた場合に自動的にバックアップを行います。
ネットワークにおいてループ構成を構築した場合、いくつかの問題が発生します。
第一に、スイッチの間でブロードキャストパケットがループすることで、ブロードキャストストームと呼ばれる現象が起き、CPU リソースと帯域幅を消費します。

STP – STP は分散アリゴリズムを適用し、ブリッジ装置(STP-対応スイッチ、ブリッジまたはルータ)は、スパニングツリーネットワークの中核の役割を果たします。
各デバイスからルートデバイスにパケットを伝送する際にパスコストの一番低い各ブリッジ装置（ルートデバイス以外）のルートポートを選択します。
次に、LAN からデバイスにパケットを伝送する際にパスコストの一番低い各 LAN からのブリッジデバイスを選択します。

指定のブリッジデバイスに接続されたポートはすべて指定されたポートに割り当てられます。
パスとストの一番低いスパニングツリーを決定すると、すべてのルートポートと指定先のポートを有効にして、それ以外のポートを無効にします。そのため、ネットワークパケットはルートポートと指定先のポート間でのみデータの伝送を行い、ネットワークのループの可能性を軽減します。



安定したネットワークトポロジーを確立すると、ブリッジはすべてルートブリッジから Hello BPDUs (ブリッジプロトコルデータユニット)が送信されるのを待ちます。ブリッジが一定時間（Maximum Age）Hello BPDU を受信しない場合は、ブリッジはルートブリッジへのリンクが切れたと判断し、他のブリッジと通信を開始し、有効なネットワークトポロジーを構築します。

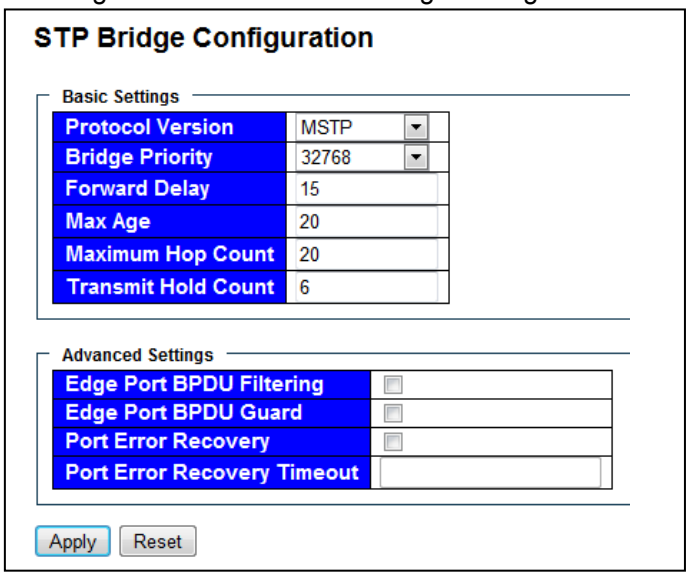
2.4.1 Bridge Settings

スパニングツリーブリッジおよびSTPシステムの設定方法について説明します。STPシステムの設定により、スタック内のすべてのSTPブリッジインスタンスによって使用できるようSTPシステムを設定することが可能です。

設定方法

スパニングツリー機能の設定方法は次の手順に従ってください。
Step 1. [Configuration]→[Spanning Tree]→[Bridge Settings]をクリックします。
Step 2. 「Basic Settings」の項目から選択して、値を入力します。
Step 3. 「Advanced settings」の項目で、☑を選択して有効/無効を設定してから、値を入力します。
Step 4. <Save>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.4.1:　The STP Bridge Configuration



設定/表示項目

Basic Settings

Protocol Version :
STP プロトコルのバージョン。
有効な値は STP, RSTP および MSTP から選択することができます。

Bridge Priority :
ブリッジのプライオリティを制御します。値が低いほど、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および MSTI インスタンス番号は、6 バイトの MAC アドレスで、ブリッジの識別子を形成します。MSTP の場合は、CIST の優先順位です。それ以外は、STP/RSTP ブリッジの優先順位です。

Forward Delay :
ルートおよび指定のポートをフォワーディング（STP 互換モードで使用）へ伝送す場合の STP ブリッジによる遅延。設定可能な値は「4～30 秒」です。

Max Age :
ルートブリッジの場合ブリッジにより伝送された情報の最大経過時間。
設定可能な値は「6～40 秒」です。MaxAge は<= (FwdDelay-1)*2 に設定する必要があります。

Maximum Hop Count :
MSTI リージョンのバウンダリで生成された MSTI 情報の残りのホップ数の初期値を定義します。ルートブリッジにより伝送される BPDU 情報を定義します。
設定可能な値は、「6～40」までのホップ数です。

Transmit Hold Count :
ブリッジポートが毎秒送信可能な BPDU の数。これを超えると、次の BPDU の伝送に遅延が生じます。設定可能な値は「1～10」までの BPDU（秒単位）で表示されます。

Advanced Settings

Edge Port BPDU Filtering :
エッジに設定されたポートは BPDU の送受信を制御します。

Edge Port BPDU Guard :
エッジとして設定されたポートが BPDU の受信を無効にするかどうかを制御します。
ポートは、エラー/無効な状態になると、有効なトポロジーから取り除かれます。

Port Error Recovery :
ポートがエラー/無効な状態の場合は一定時間後自動的に有効になります。リカバリ不可の場合は、ポートを無効にして、正常な STP を再構築します。システムをリブートすることにより消去されます。

Port Error Recovery Timeout :
エラー/無効な状態のポートが有効になるまでの時間。設定可能な値は、「30～86400 秒(24 時間)」

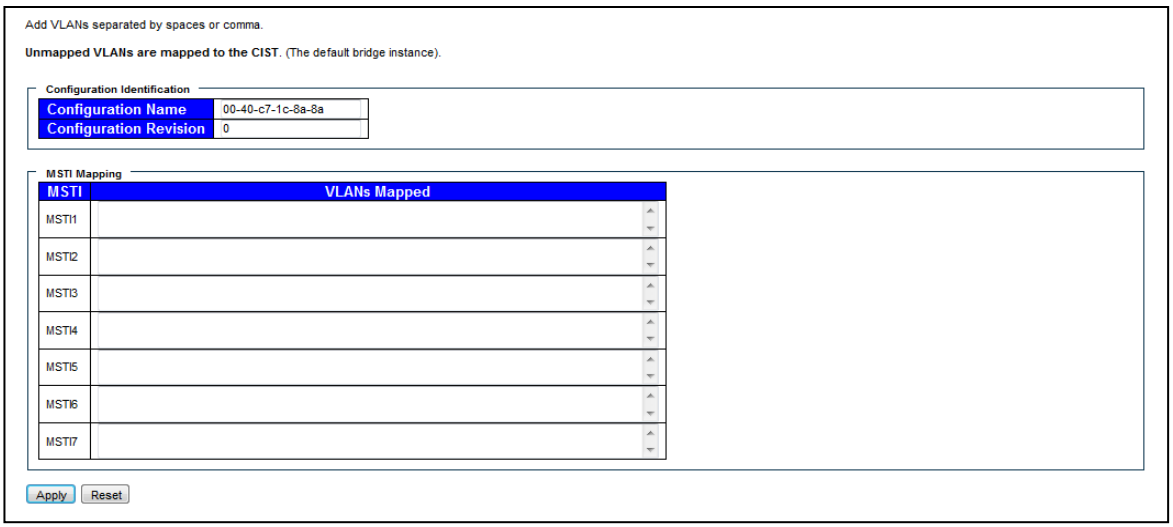
2.4.2 MSTI Mapping

ブリッジインスタンスのスイッチにスパニングツリープロトコルを設定する場合は、マッピングされていない VLAN を受信するため、CIST はマッピングには使用できません。MSTI にマッピングしたい VLAN のリストを設定する必要があります。設定の際、VLAN はコンマ/スペースで区切る必要があります。VLAN は、1 つの MSTI にのみマッピングされ、未使用の MATI は空のままです（例えば、マッピングされた VLAN がない場合）。現行の STP の MSTI ブリッジインスタンスの優先順位を確認するだけでなく、変更することが可能です。

設定方法

スパニングツリーの MSTI のマッピングの設定方法については、以下の手順に従ってください。
Step 1. [Configuration]→[Spanning Tree]→[MSTI Mapping]をクリックします。
Step 2. 「configuration identification」の項を入力後、「VLANs Mapped」メニューを入力してください。
Step 3. <Save>ボタンをクリックして、値を保存します。
Step 4. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.4.2:　The MSTI Configuration



設定/表示項目

Configuration Identification

Configuration Name :
MSTI mapping への VLAN を識別する名前。ブリッジは、MSTI's (Intra-region).のスパニングツリーを共有するために、名前およびリビジョン（下記参照）、VLAN と MSTI のマッピング設定を共有する必要があります。名前は最大「32 文字」です。

Configuration Revision :
上記の名前の MSTI 設定のリビジョン。設定可能な値は「0～65535」です。

MSTI Mapping
MSTI :
ブリッジのインスタンス。CIST はマッピングには使用不可です。VLAN を受信しても、マッピングされません。

VLANs Mapped :
MSTI にマッピングされた VLAN のリスト。VLAN は、コンマ/スペースで区切ってください。
それぞれの VLAN が MSTI マッピングが可能なのは1つのみです。MSTI が使用されていない場合は、空白になります（たとえば、VLAN が設定されていない場合）。

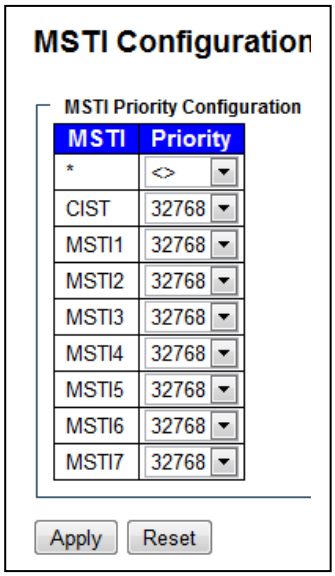
2.4.3 MSTI Poriorities

ブリッジインスタンスのスイッチ上に STP を実行した場合は、CIST は初期設定のインスタンスで必ず「有効」です。ブリッジの優先順位を制御する場合は、数値が低くなるほど、優先順位が高くなります。ブリッジの優先順位と MSTI 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形成します。
ここでは、現行の STP の MSTI ブリッジのインスタンスの優先順位を確認できるだけでなく、変更することが可能です。

設定方法

スパニングツリーの MSTI の優先順位を設定する方法については、以下の手順にしたがってください。
Step 1. [Configuration]→[Spanning Tree]→[MSTI Priorities]をクリックします。
Step 2. 優先順の最大値は「240」、初期設定では「128」です。
Step 3. <Save>ボタンをクリックして、値を保存します。
Step 4. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.4.3:　The MSTI Configuration



設定/表示項目

MSTI :
ブリッジのインスタンス。CIST は初期設定のインスタンスであり、常に有効です。

Priority :
ブリッジの優先順位を設定します。数値が低いほど、優先順位は高くなります。
ブリッジの優先順位および MSTI 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
形成します。

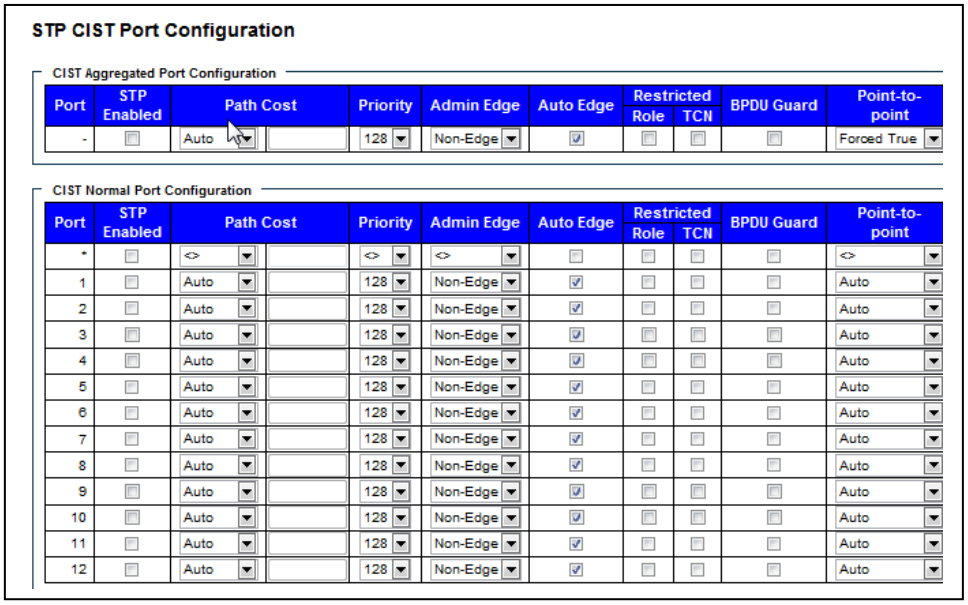
2.4.4 CIST Ports

ブリッジインスタンスのスイッチ上で STP を実行する場合、CIST ポートを設定する必要があります。
ここでは、ユーザは現行の STP の CIST ポートの設定を確認できるだけでなく、変更することも可能です。

設定方法

スパニングツリーの CIST ポートを設定するには、以下の手順に従ってください。
Step 1.　[Configuration]→[Spanning Tree]→[CIST Ports]をクリックします。
Step 2.　「CIST Aggregated Port」のメニューからすべての項目の値を選択してください。
Step 3.　STP を有効する場合は「STP Enabled」の項目に☑を入れ、「CIST normal Port configuration」の項目にそれぞれ入力してください。
Step 4.　<Save>ボタンをクリックして、値を保存します。
Step 5.　設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.4.4:　The STP CIST Port Configuration



設定/表示項目

Port :
論理 STP ポートのポート番号を指します。

STP Enabled :
STP を有効／無効を設定します。

Path Cost :
ポートのパスコストを制御します。自動設定により、802.1D 推奨値を使って物理的な通信速度に応じて適切なパスコストを設定します。特定の設定により、ユーザによって設定された値を入力することも可能です。パスコスは、ネットワークの有効なトポロジーを設定する際に使用します。パスコストの低いポートは、パスコストの高いポート用に転送ポートして使用されます。設定可能な値は「1～200000000」です。

Priority :
ポートの優先順位を設定します。同じポートコストを持つポートのプライオリティの設定に使用します(上記を参照)。

AdminEdge :
operEdge フラグの設定/クリアを開始するかを制御します(ポートを初期化する際は、初期の operEdge 状態に戻ります)。

AutoEdge :
ブリッジポート上で自動エッジの検索が可能かどうかを制御します。これにより、operEdge はポート上で BPDU が受信されたかどうか判断することができます。

Restricted Role :
この機能が有効の場合は、スパニングツリーの最も高い優先順位を持つ場合でも、CIST あるいは MSTI 用のルートポートとして選択できません。
これらのポートは、ルートポートが設定されると代替ポートとして選択されます。これらのブリッジは管理者により制御できないため、ネットワーク管理者によって設定を行い、ネットワークのコア部分以外のブリッジがスパニングツリーの有効なトポロジーに影響を与えるのを防ぎます。この機能は、「ルートガード」とも呼ばれます。

Restricted TCN :
この機能が有効な場合、受信したトポロジーの変更通知、他のポートへのトポロジーの変更を伝達できません。ステーションの設置場所の情報が不正に学習された場合、スパニングツリーの有効なトポロジーを変更後一時的に接続を切ります。
ネットワーク管理者はネットワークのコア部分以外のブリッジが、リージョン内のアドレスがフラッシュしないよう回避することができます。これらのブリッジは、管理者により完全に制御できない場合は、接続先の LAN のリンク状態は頻繁に切断されます。

BPDU Guard :
この機能が有効な場合は、ポートは有効な BPDU を受信するとすぐに無効になります。同じブリッジの設定とは異なり、ポートのエッジのステータスはこの設定には影響を与えません。この設定によりエラー/無効な状態になったポートは、ブリッジのポートエラーリカバリ設定の対象にもなります。

Point to Point :
ポートはシェアードメディア以外の 2 点間通信の LAN への接続するかどうかを制御します。これは自動的に決定されるか、「true」か「false」のいずれかに強制設定されます。伝送状態への移行がシェアードメディアより 2 点間通信 LAN のほうが高速になります。

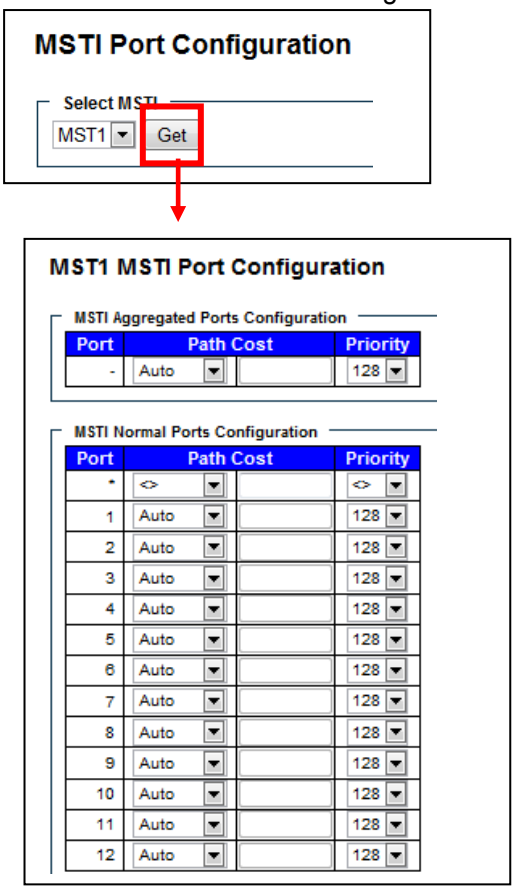
2.4.5 MSTI Ports

ユーザが現行の STP の MSTI ポートの設定を確認できるだけでなく、変更することも可能です。
MSTI ポートは仮想ポートで、各 MSTI ごとに有効な CISTZ（物理上）を個々にインスタンスを設定し、ポートに適用します。実際の MSTI ポートの設定オプションを表示する前に MSTI インスタンスを選択しておく必要があります。物理上の MSTI ポートの設定、およびアグリゲートポートが含まれます。

設定方法

スパニングツリーの MSTI ポートの設定を行うには、以下の手順に従ってください。
Step 1. [Configuration]→[Spanning Tree]→[MSTI Ports]をクリックします。
Step 2. 「MST1」または「MSTI Port」を選択します。
Step 3. <Get>ボタンをクリックして、それぞれ「MSTI Port configuration」の各設定を行います。
Step 4. <Save>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.4.5:　The MSTI Port Configuration



設定/表示項目

Port :
対応する STP CIST (および MSTI)ポートのポート番号を指します。

Path Cost :
ポートのパスコストを制御します。自動設定により、802.1D 推奨値を使って物理的な通信速度に応じて適切なパスコストを設定します。特定の設定により、ユーザによって設定された値を入力することも可能です。パスコストは、ネットワークの有効なトポロジーを設定する際に使用します。パスコストの低いポートは、パスコストの高いポート用に転送ポートして使用されます。設定可能な値は「1～200000000」です。

Priority :
ポートの優先順位を制御します。同じポートコストをもつポートの優先順位を制御するために使用可能です。

Buttons
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.4.6 Bridge Status

MSTI ポートの設定方法とブリッジのステータスについて説明します。すべての STP ブリッジインスタンスのステータスの概要を提供します。画面には、各 STP ブリッジインスタンスの情報が表示されます。

設定方法

STP のブリッジステータスを設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[Spanning Tree]→[Bridges Status]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、STP ブリッジが更新されます。

Figure 2.4.6:　The STP Bridges status

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:40:C7:1C:8A:8A	80:00-00:40:C7:1C:8A:8A	-	0	Steady	-

設定/表示項目

MSTI :
ブリッジインスタンス。STP のブリッジのステータスも表示されます。

Bridge ID :
ブリッジインスタンスのブリッジ ID

Root ID :
現行で選択されているルートブリッジのブリッジ ID

Root Port :
ルートポートとして割り当てられたポート

Root Cost :
ルートパスコスト。ルートブリッジの場合は「0」です。その他のすべてのブリッジの場合は、ルートブリッジの最下位コストパスのポートパスコストの合計です。

Topology Flag :
ブリッジインスタンスのトポロジー変更のフラグの現行の状態

Topology Change Last :
最後のトポロジーが変更してからの経過時間

2.4.7 Port Status

STP 設定後、STP ポートのステータスを表示することができます。また現在選択されているスイッチの物理ポートとして STP の CIST ポートのステータスを表示することができます。

設定方法

STP ポートのステータスを表示するには、以下の手順に従ってください。
Step 1.　[Configuration]→[Spanning Tree」→[Port Status]をクリックします。
Step 2.　自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3.　<Refresh>ボタンをクリックすると、随時更新されます。

Figure 2.4.7:　The STP Port status

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-

設定/表示項目

Port :
論理 STP ポートのポート番号

CIST Role :
CIST ポートの現行の STP ポートの役割。ポートの役割は、「IternatePort」、「BackupPort」、「RootPort」、「DesignatedPort Disabled」のいずれかになります。

CIST State :
CIST ポートの現行の STP ポートの状態。ポートの状態は、「Blocking」、「Learning」、「Forwarding」の
いずれかになります。

Uptime
ブリッジポートを最後に初期化してからの経過時間

2.4.8 Port Statistics

STP 設定方法とSTP 統計情報を表示について説明します。ブリッジポートの STP 統計情報のブリッジの詳細カウンタが表示されます。

設定方法

STP のポートステータスを表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[Spanning Tree]→[Port Statistics]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、STP ブリッジの情報が更新されます。

Figure 2.4.8:　The STP Statistics

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

設定/表示項目

Port :
論理 STP ポートのポート番号を指します。

MSTP :
BPDU によりポート上で送受信された MSTP フレーム数

RSTP:
BPDU によりポート上で送受信された RSTP フレーム数

STP :
BPDU によりポート上で送受信された STP フレーム数

TCN :
BPDU によりポート上で送受信されたレガシートポロジー変更通知の回数

Discarded Unknown :
BPDU によりポート上で受信（破棄）された不明なスパニングツリーフレームの数

Discarded Illegal :
BPDU によりポート上で受信（破棄）された不正なスパニングツリーのフレーム数

2.5 IGMP Snooping

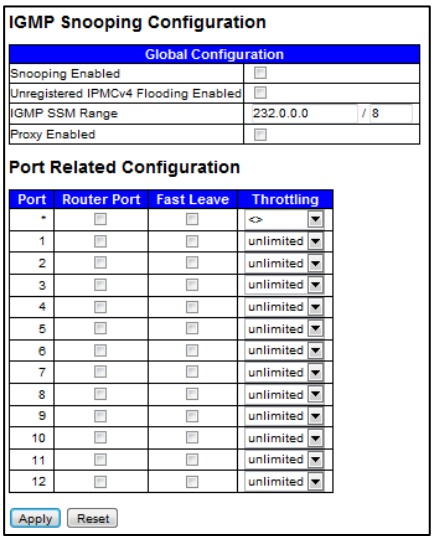
IGMP スヌーピングを設定することで、マルチキャストグループの、メンバーポートのみへのへのマルチキャストの伝送を行います。そうすることで、IP マルチキャストパケットがネットワーク上で動作している間メンバー以外の帯域幅の消費を防ぎます。
IGMP スヌーピングを設定しない場合は、マルチキャストパケットの伝送機能は無効となり、ブロードキャストパケットと同じ扱いになります。
IP マルチキャストルーター/スイッチおよび IP マルチキャストホスト間のパケット交換のタイプの問い合わせ、通知、leave 機能により、メンバーポートへの参加/脱退した際マルチキャストテーブルの情報の更新を行うことが可能です。この機能により、一旦 IP マルチキャストパケットを受信すると、指定した IP マルチキャストグループに参加したメンバーへパケットの伝送を行います。
パケットは、ユーザが予め構築されていないマルチキャストグループにマルチキャストパケットを移行しようとすると IGMP スヌーピングにより破棄されます。

ツリー構造のルートに近いルータに接続させるために基本の IGMP スヌーピンの設定方法について説明します。このインタフェースは上り回線用であるため、ルータは IGMP が実装されている必要があります。

設定方法

IGMP のスヌーピングを設定するには以下の手順に従ってください。
Step 1. [Configuration]→[IGMP Snooping]→[Basic Configuration]をクリックします。
Step 2. 「Global configuration」メニューの項目を選択します。
Step 3. ルーターポートに設定したいポート番号に☑を入れるか、「Fast Leave function」を「有効/無効」に設定してください。
Step 4. 「Throtting」メニューから値を選択します。
Step 5. <Save>ボタンをクリックして、値を保存します。
Step 6. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.6.1:　The IGMP Snooping Configuration



設定/表示項目

Snooping Enabled:
システムの IGMP スヌーピングを有効にします。

Unregistered IPMC Flooding enabled
未登録の IPMC トラフィックのフラッディングを有効にします。

Leave Proxy Enabled :
IGMP Leave Proxy を有効にします。この機能により、ルータ側への不要な leave メッセージの伝送を防ぎます。

Proxy Enabled :
IGMP Proxy を有効にします。この機能により、ルータ側への不要な join および leave メッセージの伝送を防ぎます。

Router Port :
ルーターポートとして動作するポートを指定します。ルータポートは本機のポートで、レイヤ 3 のマルチキャストデバイスまたは IGMP クエリアへ移行します。
アグリゲーションメンバーポートをルーターポートとして選択する場合は、アグリゲーション全体がルーターポートとして動作します。

Fast Leave :
ポートの fast leave を「有効」にします。

Throttling :
ポートが属するマルチキャストグループの数の制限します。
Buttons
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

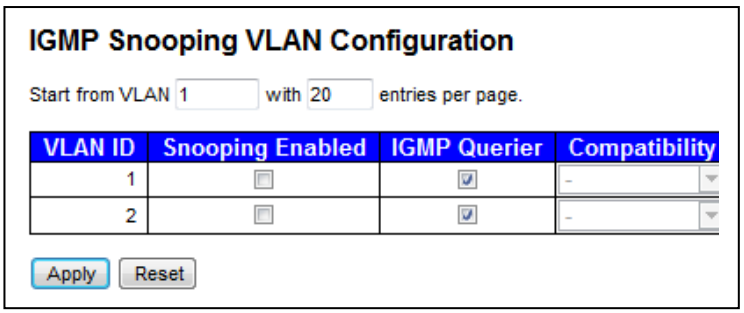
2.5.2 VLAN Configuration

IGMP スヌーピング機能を持つ VLAN 設定手順について説明します。各設定画面には、VLAN テーブル内の最大 99 項目まで表示されます。初期設定では 20 項目ずつ、画面ごとにエントリに入力します。初期設定では、1 画面につき VLAN テーブルの先頭から最初の 20 項目が表示されます。VLAN テーブルで一番低い VLAN ID をもつ VLAN が表示されます。「VLAN」に値を入力して、VLAN テーブルの開始位置を選択することができます。<Refresh>ボタンをクリックすると、テーブルの内容が更新されるか、VLAN テーブル内の一番近い値が表示されます。

設定方法

IGMP スヌーピングの VLAN 設定を行うには、以下の手順に従ってください。
Step 1. [Configuration]→[IGMP Snooping]→[VLAN Configuration]をクリックします。
Step 2. 「Snooping」を設定したい場合は、☑を入れて、値を入力します。
Step 3. <Refresh>ボタンをクリックするとデータが更新され、”<<”あるいは”>>“ をクリックすると前後の項目に移動します。
Step 4. <Save>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.6.2:　The IGMP Snooping VLAN Configuration.



設定/表示項目

Snooping Enabled :
VLAN ごとにシステムの IGMP スヌーピングを有効にします。

Buttons
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

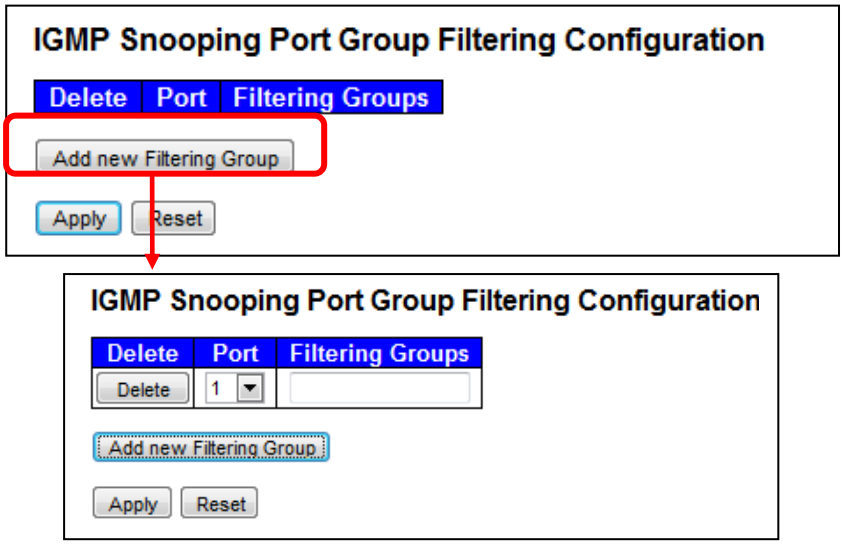
2.5.3 Port Group Fitering

IGMP ポートのグループのフィルタリングの設定方法について説明します。IGMP フィルタリング機能により、制御することができます。大都市圏、または集合住宅住戸のようなネットワークアプリケーション環境では、ユーザは利用しているポートのマルチキャストグループを制御することができます。これにより、加入タイプ、サービスプランに応じて IP/TV などのマルチキャストサービスの使用を制御することができます。この機能では、IP マルチキャストを設定して個々のポートに関連付けることにより、ポートごとにマルチキャストのフィルタリングを行うことが可能です。IGMP には1つまたは複数のマルチキャストグループが含まれ、グループへのアクセスの許可/禁止を行います。マルチキャストグループへのアクセスが禁止されている IGMP が適用されている場合は、IGMP は IP マルチキャストのトラフィックの要求が破棄されたことをポートはグループからの IP マルチキャストトラフィックは受信できません。フィルタリングがマルチキャストグループのアクセスを許可した場合は、ポートからの IGMP レポートは通常の処理用に転送されます。
IGMP フィルタリングでは、IGMP メンバー「Join レポート」のみを制御し、IP マルチキャストトラフィックの転送を行う機能とは関係ありません。

設定方法

IGMP スヌーピングのポートのグループの設定を行うには、以下の手順に従ってください。
Step 1. [Configuration]→[IGMP Snooping]→[Port Group Filtering]をクリックします。
Step 2. 「Add new Filtering Groups」をクリックします。
Step 3. 「Port Group Filtering」メニューで、「Filtering Groups」の欄に値を入力します。
Step 4. <Save>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.6.3:　The IGMP Snooping Port Group Filtering Configuration



設定/表示項目

Delete :
削除したい項目を選択して、<Save>ボタンをクックすると削除されます。

Port :
設定したいポートを選択して、IGMP スヌーピングポートグループのフィルタリング機能を有効にします。

Filtering Groups :
フィルタリングを行う IP マルチキャストグループ を設定します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

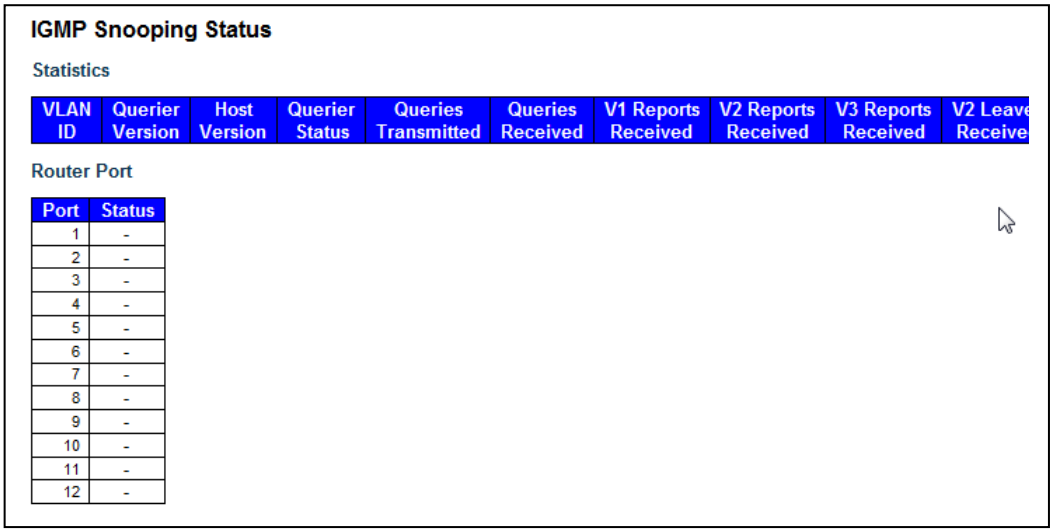
2.5.4 Status

IGMP スヌーピングの設定および IGMP スヌーピングのステータスが表示されます。

設定方法

IGMP スヌーピングのステータスを表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[IGMP Snooping Status]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、「IGMP Snooping Status」の情報が更新されます。
Step 4. <Clear>ボタンをクリックすると、「IGMP Snooping Status」の情報が消去されます。

Figure 2.6.4:　The IGMP Snooping Status.



設定/表示項目

VLAN ID :
エントリの VLAN ID

Querier Version :
現在動作しているクエリのバージョン

Host Version :
現在動作しているホストのバージョン

Querier Status :
クエリのステータスが"ACTIVE" または "IDLE"が表示されます。

Queries Transmitted :
クエリの送信数.

Queries Received
クエリの受信数.

V1 Reports Received :
V1 レポートを受信した数

V2 Reports Received :
V2 レポートを受信した数

V3 Reports Received :
V3 レポートを受信した数

V2 Leaves Received :
V2 Leaves を受信した数.

Auto-refresh
自動更新に☑を入れると、ログ情報が自動的に更新されます。
Upper right icon (Refresh, clear):
<Refresh>ボタンをクリックするとステータスが更新され、<Clear>ボタンをクリックすると手動で削除することができます。

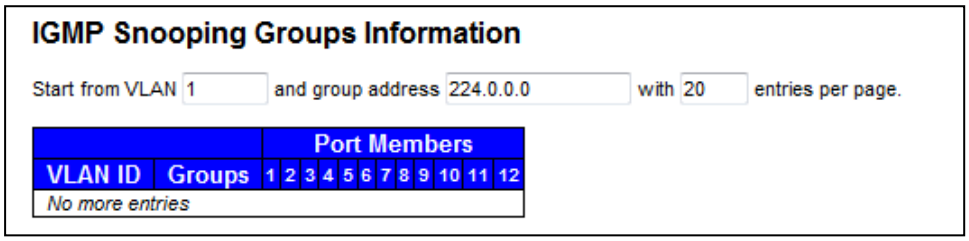
2.5.5 Group Infermation

IGMP スヌーピング機能を設定すると、IGMP スヌーピンググループの情報を表示することができます。
IGMP のグループテーブル内の項目が表示されます。
IGMP グループのテーブルは、VLAN ID ごと、グループごとにソートされています。
現在表示されている表の最後の項目が参照されます。最後に達すると、"No more entries"とメッセージが表示されるため最初から開始してください。

設定方法

IGMP スヌーピンググループ情報を表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[IGMP Snooping]→[Group Information]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、「IGMP Snooping Groups」のエントリを更新します。
Step 4. “<<“あるいは”>>“ を使って、前後のメニューに移動します。

Figure 2.6.5:　The IGMP Snooping Groups Information.



設定/表示項目

"Start from VLAN"および"group"の項目に値を入力すると、IGMP グループテーブルの開始位置を選択することができます。現在表示されているテーブルの最後の項目が参照されます。最後に達すると、"No more entries"とメッセージが表示されるため最初から始めてください。

VLAN ID :
グループの VLAN ID

Groups :
表示したいグループのグループアドレス

Port Members :
グループのポート

Auto-refresh
自動更新に☑を入れると、ログ情報が自動的に更新されます。

Upper right icon (Refresh, <<, >>)
IGMP グループのステータスを手動で更新します。 “<<“あるいは”>>“ を使って、前後のメニュー/画面に移動します。

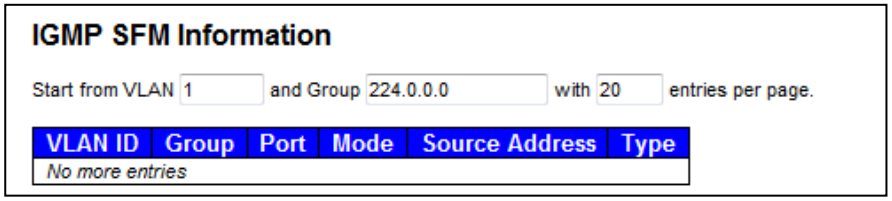
2.5.6 IPv4 SSM information

SSM（送信元特定マルチキャスト）は、データグラム配送モデルの1つであり、放送アプリケーションとしても知られる一対多アプリケーションをもっともよくサポートしています。SSM はオーディオ/ビデオ放送アプリケーション環境用の中核のネットワーク技術です。
SSM 配送モードでは、IP マルチキャストの受信側ホストは、IGMP バージョン 3(IGMPv3)を採用し、チャネル(S, G)に加入します。このチャンネルに加入するには、受信側のホストはソースホスト S からグループ G に送信された IP マルチキャストトラフィックを受信することを示します。
ネットワークはソースホスト S からグループ G に送信された IP マルチキャストトラフィックをチャンネル(S, G)に加入しているネットワーク内のすべてのホストに配信します。
SSM はネットワーク、またそれぞれのソースホスト内でもグループアドレスの割り当ては必要ありません。同じソースホスト上で動作している各アプリケーションはそれぞれの SSM グループを使用する必要があります。各ソースホスト上で動作しているアプリケーションはネットワーク上で過度のトラフィックを引き起こすことなしに SSM グループアドレスを任意に使用することができます。232.0.0.0/8 (232.0.0.0～232.255.255.255)範囲内のアドレスは IANA によって SSM 用に保持されます。当スイッチでは任意の IP マルチキャストアドレス用の SSM も設定することができます。

設定方法

IGMPv3 および IPv4 の SSM 情報を表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[IGMP Snooping]→[IPv4 SSM Information]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、「IGMPv3 IPv4 SSM Information」の情報が更新されます。
Step 4.“<<“あるいは”>>“ をクリックすると、前後のメニューに移動します。

Figure 2.6.6:　The IGMPv3 IPv4 SSM Information.



設定/表示項目

各画面では、IGMPv3 SSM(送信元特定マルチキャスト) 情報が 99 項目まで表示されます。初期設定では、画面ごに項目を表示すると、画面には、IGMPv3 情報の先頭から最初の 20 項目が表示されます。
「Start from VLAN」および「Group」の項に値を入力することにより、ユーザは IGMPv3 情報テーブルの開始店を選択することができます。
現在表示されている表の最後の項目が参照されます。最後に達すると、"No more entries"とメッセージが表示されるためボタンをクリックすると最初から開始します。

IGMPv3 Information Table Columns

VLAN ID :
グループの VLAN ID

Group :
表示されたグループのグループアドレス

Port :
スイッチの物理ポート番号

Mode :
VLAN ID、ポート番号、グループアドレスごとのフィルタリングモードを示します。「Include」または「Exclude」のいずれかです。

Source Address :
ソースの IP アドレス。システムは、フィルタリング用の IP ソースアドレスの総数を「128」に制限します。

Type :
タイプを表します。「Allow」あるいは「Deny」のいずれかです。

Auto-refresh
自動更新に☑を入れると、ログ情報が自動的に更新されます。

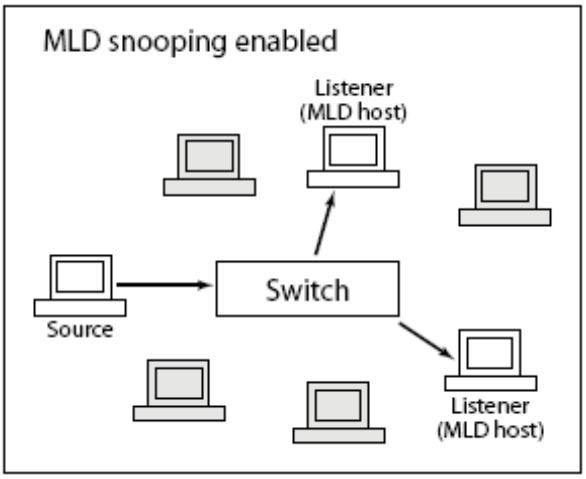
Upper right icon (Refresh, <<, >>)
IGMP グループのステータスを手動で更新することができます。また”<<”または”>>“ を使って前後の項目/ページに移動します。

2.6 MLD Snooping

IPv6 マルチキャストトラフィックの、MLD スヌーピング機能をサポートしています。これにより IPv6 マルチキャストグループのみにトラフィックの転送が可能です。

【注意】
デスクトップ会議のようなアプリケーションは、ネットワークノードはソースおよび MLD ホストとして動作することに注意してください。
MLD は MLD ホストとしての役割でのみノードと通信を行います。

ソースノードはパケットをマルチキャストアドレスへ送信することによりマルチキャストトラフィックを作成します。IPv6 では、最初の 8 ビットのアドレス（“FF”はアドレスの最初の 2 文字）がマルチキャストアドレスとなり、どのノードもアドレスがアプリケーションに送信されたトラフィックを受信するのを待ちます。ソースおよび宛先システム上で動作するアプリケーションソフトウェアは使用するマルチキャストアドレスを決定します（注意：アプリケーションソフトウェアの機能で、MLD の機能ではありません。）
VLAN 上で MLD スヌーピングが有効な場合は、スイッチは不要なマルチキャストトラフィックを最小限に抑えます。スイッチが指定されたマルチキャストアドレス用のマルチキャストトラフィックを受信した場合、そのアドレス用の MLD ホストを持つ VLAN 上のポートにのみトラフィックを伝送します。MLD ホストを持たない VLAN 上のポートのトラフィックを破棄します。



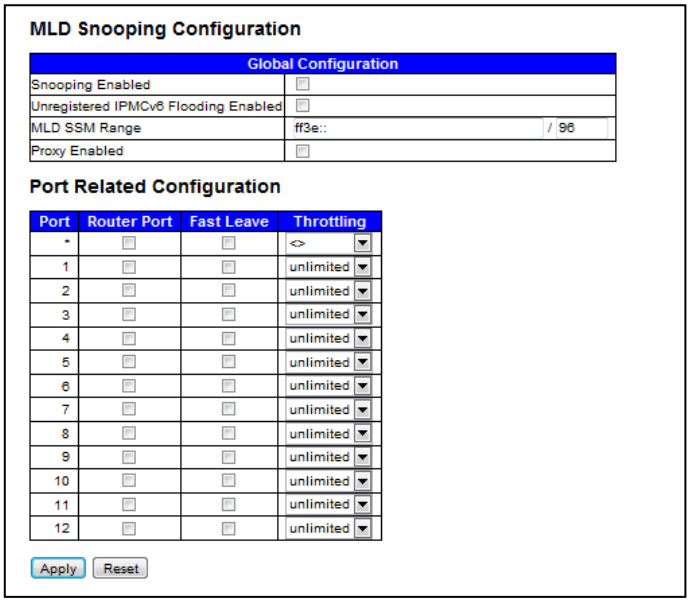
2.6.1 Basic Configuration

ここでは、MLD スヌーピングの基本設定方法について説明します。

設定方法

MLD スヌーピング設定方法については、以下の手順に従って下さい。
Step 1.　[Configuration]→[MLD Snooping]→[Basic Configuration]をクリックします。
Step 2.　「Global configuration」の項目を「enable」または「disable」に設定します。ルーターポートおよび「Fast Leave」に設定したポートを☑を入れて、選択します。
Step 3.　Throtting モードを「unlimited」または「1～10」までの値を選択します。
Step 4.　<Save>ボタンをクリックして、値を保存します。
Step 5.　設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.6.1:　The MLD Snooping Basic Configuration.



設定/表示項目

Snooping Enabled :
システムの MLD スヌーピング機能を有効にします。

Unregistered IPMC Flooding enabled :
未登録の IPMCv6 トラフィックのフラッディングを有効にします。未登録の IPMCv6 トラフィックのフラッディングにより、ネイバーディスカバリが正常に実行できませんので注意してください。

MLD　SSM　Renge:
SSM(送信元特定マルチキャスト)のアドレスの範囲を設定します。

Proxy Enable:
プロキシの設定をします。

Port:
物理ポートのインデックス。

Fast Leave :
ポートの Fast Leave 機能を有効にします。

Router Port :
ルータポートとして動作するポートを指定します。ルータポートとはレイヤ 3 マルチキャストデバイスまたは MLD Querier のイーサネットスイッチ上のポートです。アグリゲーションメンバーポートがルートポートして選択された場合は、アグリゲーション全体がルートポートとして動作します。

Throttling :
スイッチポートが属するマルチキャストグループの数を制限します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

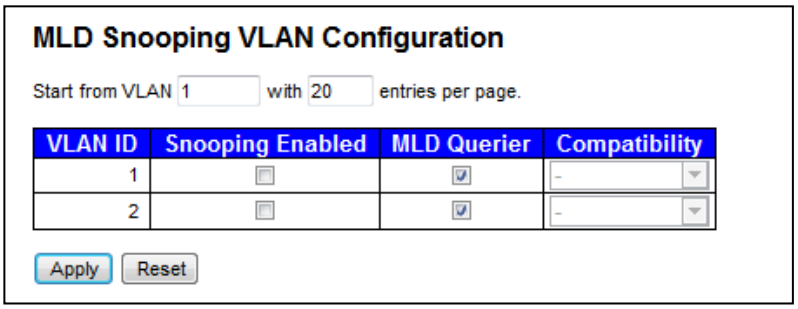
2.6.2 VLAN Configuration

VLAN 上で MLD スヌーピングを有効にすると、アドレスの MLD ホストをもつ VLAN のポートにのみトラフィックを伝送し、指定したマルチキャストアドレスの不要なマルチキャストトラフィックを最小限にします。MLD ホストを持たない VLAN 上のポートのトラフィックは破棄されます。現在表示されている表の最後の項目が参照されます。最後に達すると、"No more entries"とメッセージが表示されるためボタンをクリックすると最初から開始します。

設定方法

MLD スヌーピングの VLAN 設定を行うには、次の手順に従ってください。
Step 1. [Configuration]→[MLD Snooping]→[VLAN Configuration]をクリックします。
Step 2. 画面ごとに「VLAN ID」を指定します。
Step 3. <Refresh>ボタンをクリックすると、MLD スヌーピング VLAN の値を更新します。
Step 4. “<<“あるいは”>>“ を使って、前後のメニューに移動します。

Figure 2.6.2:　The MLD Snooping VLAN Configuration.



設定/表示項目

VLAN ID :
エントリの VLAN ID

MLD Snooping Enabled :
VLAN ごとの MLD スヌーピングを有効にします。VLAN を最大 64 までの設定可能です。

MLD Querier:
VLAN の MLD クエリアーを有効にします。

Comptibility:
MLD のバージョンを指定します。

Auto-refresh
自動更新に☑を入れると、ログ情報が自動的に更新されます。

Upper right icon (Refresh, <<, >>)
IGMP グループのステータスを手動で更新します。“<<“あるいは”>>“を使って、前後のメニュー/画面に移動します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

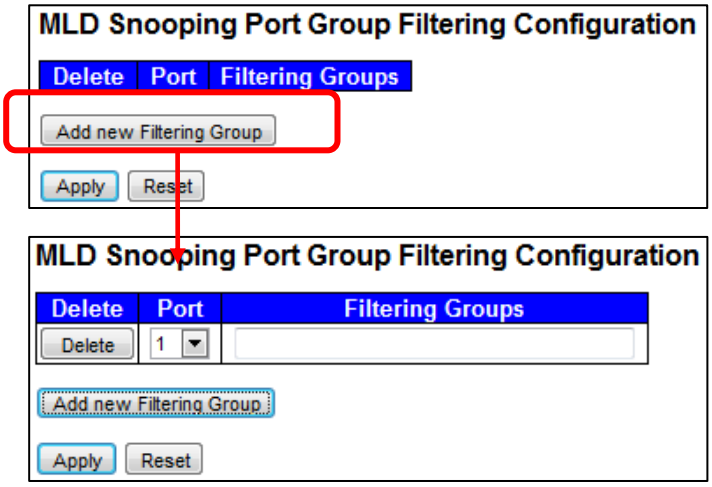
2.6.3 Port Group Fitering

MLD スヌーピング機能におけるポートグループのフィルタリングの設定方法について説明します。ここでは、新規フィルタリンググループの作成、およびセーフティポリシーの設定方法を説明します。

設定方法

MLD スヌーピングポートグループコンフィグレーションの設定方法については、以下の手順に従ってください。
Step 1. [Configuration]→[MLD Snooping]→[Port Group Filtering]をクリックします。
Step 2. 「Add new Filtering Group」をクリックして、新しいフィルタリンググループを追加します。
Step 3. ポートごとに、「Filtering Groups」を入力します。
Step 4. <Save>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.6.3:　The MLD Snooping Port Group Filtering Configuration



設定/表示項目

Delete :
削除したい項目を選択して、<Save>ボタンをクックすると削除されます。

Port :
論理ポート番号。ポートを選択してフィルタリンググループに設定します。

Filtering Groups
フィルタリングの対象となる IP マルチキャストグループ

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

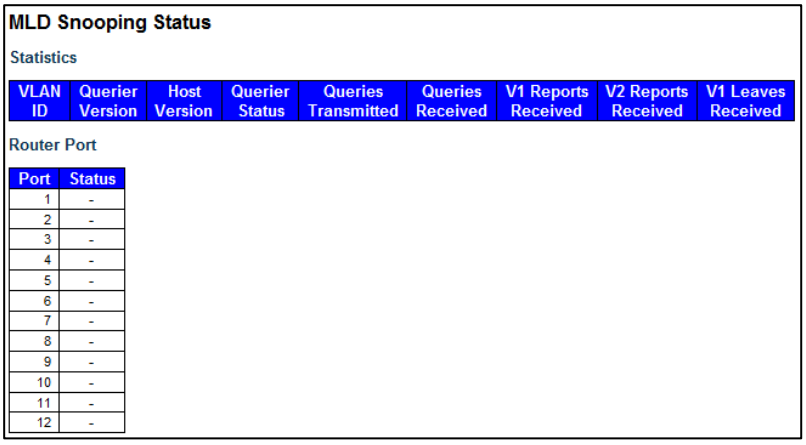
2.6.4 Status

MLD スヌーピングを設定後、MLD スヌーピングのステータスの詳細の表示方法について説明します。MLD スヌーピングステータスの詳細情報について確認することができます。

設定方法

MLD スヌーピングのステータスを表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[MLD Snooping]→[Status]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、「MLD Snooping Status」の項目が更新されます。
Step 4. <Clear>ボタンをクリックすると、「MLD Snooping Status」が消去されます。

Figure 2.6.4:　The MLD Snooping Status



設定/表示項目

VLAN ID :
エントリの VLAN ID

Querier Version :
現在動作しているクエリのバージョン

Host Version :
現在動作しているホストのバージョン

Querier Status :
クエリーのステータスを"ACTIVE"または"IDLE"で表示します。

Queries Transmitted :
クエリーの送信回数

Queries Received :
クエリーの受信回数

V1 Reports Received :
V1 レポートの受信回数.

V2 Reports Received :
V2 レポートの受信回数.

V1 Leaves Received :
V1 Leaves の受信回数.

Auto-refresh :
自動更新に☑を入れると、ログ情報が自動的に更新されます。

Upper right icon (Refresh, <<, >>)
IGMP グループのステータスを手動で更新します。 “<<“あるいは”>>“ を使って、前後のメニュー/画面に移動します。

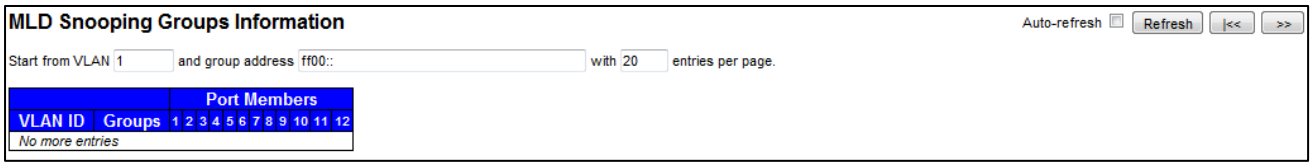
2.6.5 Group Information

MLD スヌーピンググループ情報の設定方法について説明します。

設定方法

MLD スヌーピンググループ情報の表示方法について、以下の手順に従ってください。
Step 1. [Configuration]→[MLD Snooping]→[Group Information]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、MLD スヌーピンググループの項目を更新します。
Step 4. <Clear>ボタンをクリックすると、MLD スヌーピンググループ情報をクリアにします。

Figure 2.6.5:　MLD スヌーピンググループ情報



設定/表示項目

各設定画面には、MLD グループテーブル内の最大 99 項目まで表示されます。初期設定では 20 項目で、画面ごとにエントリに入力します。初期設定では、1 画面につき MLD テーブルの先頭から最初の 20 項目が表示されます。
「Start from VLAN」および「group」の値を入力すると、MLD の先頭を選択することができます。
参照時は、現在表示されている表の最後の項目が表示されます。最後に達すると、"No more entries"とメッセージが表示されるためボタンをクリックすると最初から始まります。

VLAN ID :
グループの VLAN ID.

Groups :
表示されているグループのグループアドレス.

Port Members :
グループ内のポート Auto-refresh :
自動更新に☑を入れると、ログ情報が自動的に更新されます。

Upper right icon (Refresh, <<, >>):
IGMP グループのステータスを手動で更新します。“<<“あるいは”>>“ を使って、前後のメニュー/画面に移動します。

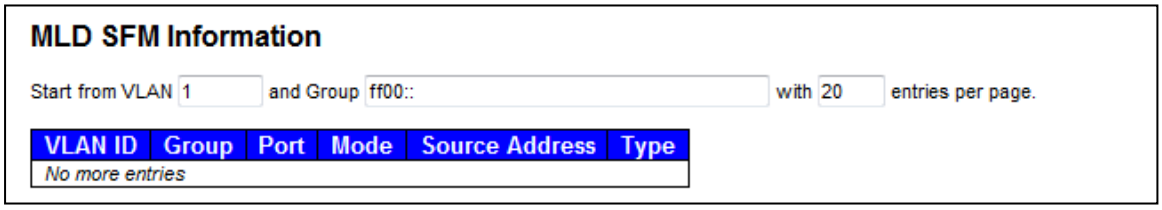
2.6.6 IPv6 SSM Information

MLDv2 情報の項目を設定方法について説明します。MLDv2 情報テーブルは VLAN ID ごと、次にグループごと、そしてポート番号によって分類されます。同じグループの各ソースアドレスは1つの項目として処理されます。
各画面では、MLDv2 SSM 情報テーブルからの項目が 64 個まで表示されます。「entries per page」メニューはデフォルト設定では「20」です。まず MLDv2 情報テーブルの最初の 20 項目が表示されます。

設定方法

MLDv2 IPv6 SSM 情報を表示するには、以下の手順に従ってください。
Step 1.　[Configuration]→[MLD Snooping]→[IPv6 SSM Information]をクリックします。
Step 2.　自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3.　<Refresh>ボタンをクリックすると、MLDv2 IPv6 SSM 情報が更新されます。
Step 4.　“<<“あるいは”>>“ を使って、前後のメニューに移動します。

Figure 2.6.6:　The IPv6 SSM Information



設定/表示項目

MLDv2 Information Table Columns

VLAN ID :
グループの VLAN ID

Group :
マルチキャストグループアドレス.

Port :
スイッチの物理ポート番号

Mode :
VLAN ID、ポート番号、グループアドレスごとに保持されているフィルタリングモード。「Include」あるいは「Exclude」を選択可能です。

Source Address :
ソースの IP アドレス。システムは、フィルタリング用の IP ソースアドレスの総数を「128」に制限します。

Type :
タイプを表します。「Allow」あるいは「Deny」のいずれかです。

2.7 MVR

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 への転送を可能にします。例えば、マルチキャストテレビジョンアプリケーションでは、STB(セットトップボックス)をもつ PC またはテレビの場合、マルチキャストストリームを受信することができます。複数の、またはPCは 1 つの加入者のポートに接続することにできます。MVR 受信側ポートとして設定されたスイッチのポートです。
加入者がチャンネルを選択する場合は、STB または PC は IGMP join メッセージを Switch に送信して適切なマルチキャストと結合させます。マルチキャスト VLAN 間でマルチキャストデータを送受信するアップリンクポートは「MVR ソースポート」と呼ばれます。

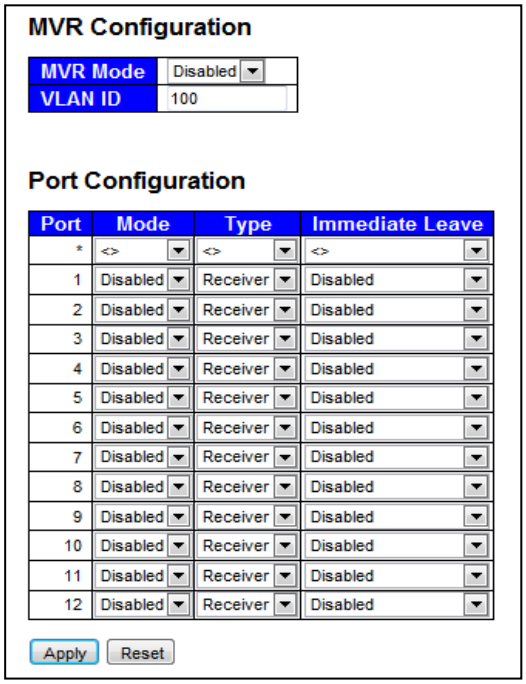
2.7.1 Configuration

MVR 基本設定方法について説明します。

設定方法

MLD スヌーピングポートのグループの設定方法については、以下の手順に従ってください。
Step 1. [Configuration]→[MVR]→[Configuration]をクリックします。
Step 2. 「MVR mode」を有効/無効にして、すべての値を入力してください。
Step 3. <Save>ボタンをクリックして、値を保存します。
Step 4. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.7.1:　The MVR Configuration



設定/表示項目

MVR Mode :
システムの MVR を有効/無効にします。

VLAN ID :
マルチキャスト VLAN ID を指定します。

Mode :
ポートの MVR を有効にします。

Type :
ポートの MVR ポートのタイプを指定します。

Immediate Leave :
ポートの「fast leave」を有効にします。

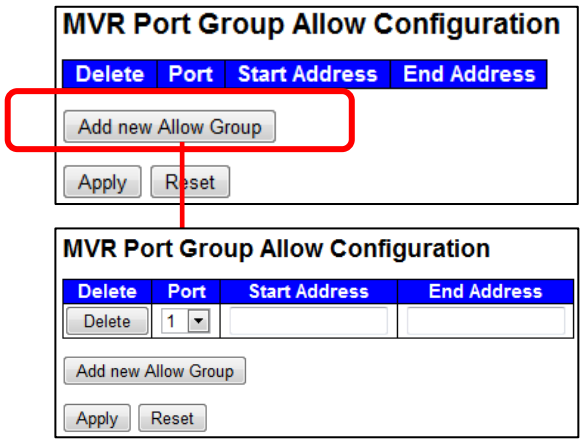
Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.7.2 Port Group Allow

許可するマルチキャストグループの基本設定方法について説明します。

設定方法

許可するマルチキャストグループの設定方法については、以下の手順に従ってください。
Step 1. [Configuration]→[MVR]→[MVR Port Group Allow Configuration]をクリックします。
Step 2. 「Add new Allow Group」をクリックしてください。
Step 3. ポートを選択し、マルチキャストグループの開始アドレスと終了アドレスを入力してください。
Step 4. <Apply>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。



設定/表示項目

Delete :
許可するグループを削除します。

Port:
レシーバの接続されるポートを指定します。

Start Address:
許可するマルチキャストグループの最初のアドレスを指定します。

End Address:
許可するマルチキャストグループの最後のアドレスを指定します。

Buttons:
Apply – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

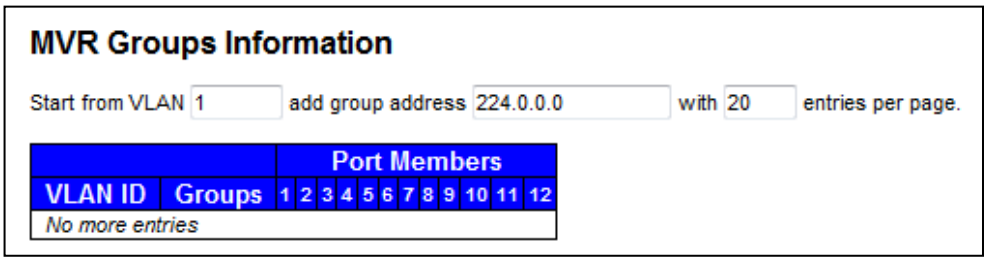
2.7.2 Groups Information

ここでは、MVR グループの表示方法について説明します。
MVR グループの項目は、まず VLAN ID、グループごとに表示されます。

設定方法

MVR グループ情報を表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[MVR]→[Groups Information]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. <Refresh>ボタンをクリックすると、MVR グループ情報が更新されます。
Step 4. “<<“あるいは”>>“ を使って、前後のメニューに移動します。

Figure 2.7.2:　The MVR Groups Information



設定/表示項目

MVR Group Table Columns

VLAN ID :
グループの VLAN ID.

Groups :
表示されているグループのグループ ID

Port Members :
グループ内のポート.

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, <<, >>):
「Refresh」ボタンをクリックして MVR グループの情報を更新するか、矢印キー(“<<”、または”>>“)を使って画面/項目を移動します。

2.7.3 Statistics

MVR を設定後、MVR の統計情報の表示方法について説明します。

設定方法

MVR 統計情報の表示方法については、次の手順に従ってください。
Step 1.　[Configuration]→[MVR]→[Statistics]をクリックします。
Step 2.　自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3.　<Refresh>ボタンをクリックすると、MVR 統計情報の項目が更新されます。

Figure 2.7.3:　The MVR Statistics　Information

MVR Statistics

VLAN ID	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
100	0	0	0	0

設定/表示項目

VLAN ID :
マルチキャスト VLAN ID

V1 Reports Received :
V1 レポートの受信回数.

V2 Reports Received :
V2 レポートの受信回数.

V3 Reports Received :
V3 レポートの受信数.

V2 Leaves Received :
V2 Leaves の受信数

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

2.8 LLDP

本機は LLDP をサポートしています。現在お使いのスイッチの現行の情報については、Link Layer Discovery Protocol (LLDP)により、標準方式で本機が隣接する装置に通知したり、隣接する LLDP デバイスについて学習することが可能です。
LLDP は、ネットワーク装置によって使用されているインターネットプロトコルサイトのベンダーニュートラルリンクレイヤプロトコルで、それぞれの ID、ケイパビリティ、IEEE 802 ローカルエリアネットワーク上の隣接装置、主に有線イーサネットについて通知します。プロトコルは IEEE 802.1AB として標準化されています。

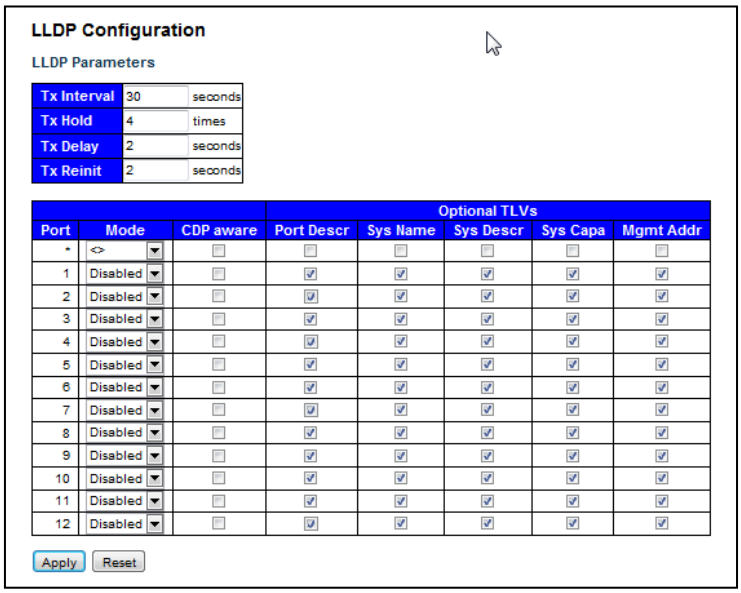
2.8.1 LLDP Configuration

ポートごとに LLDP 設定を行うことができます。設定すると、すぐに適用されます。現行の LLDP ポートの設定情報を確認して、設定を行うことができます。

設定方法

LLDP を設定するには、以下の手順に従ってください。
Step 1.　[Configration]→[LLDP configuration]をクリックします。
Step 2.　「LLDP」の値を修正します。
Step 3.　LLDP メッセージの送受信に必要なモードに設定します。
Step 4.　通知メッセージの TLV メニューの情報を指定します。
Step 5.　<Save>ボタンをクリックします。

Figure 2.8.1:　The LLDP Configuration



設定/表示項目

Tx Interval :
本機は近隣装置に LLDP フレームを定期的に送信して、ネットワーク探索情報が更新されます。LLDP フレームの送信間隔は「Tx Interval」の項目で設定します。設定可能な値は「5～32768 秒」です。

Tx Hold :
各 LLDP フレームには、LLDP フレームの情報の値が有効な時間についての情報が含まれます。LLDP の有効な時間は「Tx Interval」ごとに「Tx Hold」に設定されます。
設定可能な値は「2～10 回」です。

Tx Delay :
設定が変更されると (IP アドレスなど)、新しい LLDP フレームが伝送されますが、LLDP フレーム間の時間は常に「Tx Delay」の値になります。「Tx Delay」は、「Tx Interval」の値の 1/4 以下の値に設定する必要があります。
設定可能な値は「1 ～ 8192 秒」です。

Tx Reinit :
ポートを無効にすると、LLDP が無効になるか、スイッチが再起動し、LLDP シャットダウンフレームが近隣装置に送信され、LLDP 情報が無効になったことを通知します。Tx Reinit は、シャットダウンフレームと新しい LLDP の初期化までの時間を制御します。

LLDP Port Configuration
現在選択されているスタックユニットに関連のある LLDP ポートの設定情報が表示されます。

Port :
論理 LLDP ポートのポート番号を指します。

Mode :
「LLDP」モードを選択します。
Rx only : LLDP 情報は送信されませんが、近隣装置から受信した LLDP 情報が分析されます。
Tx only : 近隣ユニットから受信した LLPD 情報を破棄します。
Disabled: LLDP 情報は送信せず、近隣装置から受信 LLDP 情報を破棄します。
Enabled: LLDP 情報は送信せず、近隣装置から受信した LLDP 情報を分析します。

CDP Aware :
CDP (Cisco Discovery Protocol)を受信したときの挙動の設定を行います。
CDP の動作は受信した CDP フレームのデコードに制限されます（本機は CDP フレームを送信しません）。ポート上の LLDP が有効な場合は CDP フレームのデコードのみ行います。
CDP の TLV のみ、LLDP 近隣装置のテーブル内の対応するフィールドにマッピングすることができます。
その他の TL V はすべて破棄されます（認識されない CDP の TLV および破棄された CDP フレームは LLDP 統計情報に表示されます）。
CDPN の TLV は、以下のように LLDP 近隣装置のテーブルにマッピングされます。
・"Device ID" は、LLDP の "Chassis ID" にマッピングされます。

・"Address"は、LLDP の"Management Address" にマッピングされます。
CDP アドレスの TLV には、複数のアドレスを含めることができますが、最初アドレスのみ LLDP 近隣装置のテーブルに表示可能です。
・"Port ID"は、LLDP の"Port ID"にマッピングされます。
・"Version and Platform"は LLDP の "System Description" にマッピングされます。
CDP および LLDP は共に"system capabilities"をサポートしていますが、CDP ケイパビリティは LLDP の部分でないケイパビリティをカバーします。これらのケイパビリティは LLDP 近隣装置のテーブルの"others"に表示されます。
すべてのポートの CDP 検知が「無効」な場合、近隣装置から受信した CDP フレームを伝送します。
少なくとも 1 ポートの CDP 検知が「有効」な場合、CDP フレームはすべてスイッチにより無効になります。

【注記】:
ポートの CDP 検知を無効にすると、CDP 情報はすぐに削除されず、一定のホールドタイムを過ぎると消去されます。

Port Descr :
オプション TLV: "port description"が、送信された LLDP 情報に含まれます。

Sys Name :
オプション TLV: "system name"が、送信された LLDP 情報に含まれます。

Sys Descr :
オプション TLV: "system description"が、送信された LLDP 情報に含まれます。

Sys Capa :
オプション TLV: "system capability"が、送信された LLDP 情報に含まれます。

Mgmt Addr :
オプション TLV: "management address"が、送信された LLDP 情報に含まれます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

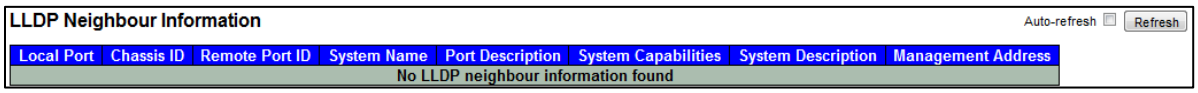
2.8.2 LLDP Neighbours

すべての LLDP 近隣装置の状態について説明します。表示されたテーブルには、検出された LLDP 近隣装置の各ポートの情報が表示されます。

設定方法

LLDP 近隣装置を表示するには、以下の手順に従ってください。
Step 1.「LLDP Neighbours」をクリックします。
Step 2. <Refresh>ボタンをクリックすると、画面は手動で更新されます。
Step 3. <Auto-refresh>ボタンをクリックすると、画面は自動で更新されます。

Figure 2.8.2:　The LLDP Neighbours information



【注記】:
お使いのネットワークに LLDP 対応の装置がない場合は、テーブルには “No LLDP neighbour information found”のメッセージが表示されます。

設定/表示項目

Local Port :
LLDP フレームを受信したポート

Chassis ID :
Chassis ID は、近隣装置の LLDP フレームの ID です。

Remote Port ID :
リモートのポート ID は、近隣装置のポートの ID です。

System Name :
近隣装置によって通知された名前です。

Port Description :
近隣装置によって通知されたポートについての説明しています。

System Capabilities :
ここでは、これは近隣装置の種類を示します。
以下のデバイスの種類が表示されます。
1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved
ケイパビリティを「有効」にすると、ケイパビリティの後ろに(+)、ケイパビリティの「無効」にすると(-)が表示されます。

Management Address :
管理アドレスは上位層に使用される近隣装置のアドレスであり、ネットワーク管理によって検出されます。近隣装置の IP アドレスを保持することができます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
LLDP 近隣装置情報を手動で更新することができます。

2.8.3 LLDP-MED Configuration

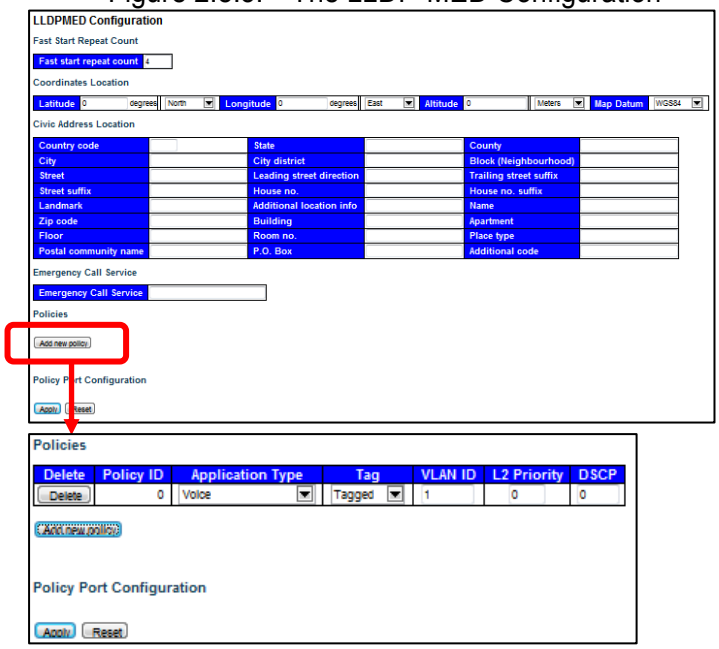
MED「Media Endpoint Discovery」は、LLDP の拡張機能として”LLDP-MED”としても知られており、次の機能をサポートしています。
LAN ポリシー(VLAN, Layer 2 Priority および Diffserv の設定)の自動検出により、簡単にネットワークを利用することができます。「デバイスロケーション検知」により、ロケーションのデータベースの作成などのサービスが可能になります。

PoE エンドポイントの拡張および自動電源の管理
在庫管理、この機能によりネットワークの管理者によるネットワーク装置を追跡して、それぞれの特徴（メーカー、ソフトウェア/ハードウェアのバージョン、シリアルまたは資産番号）の管理が可能になります。
LLDP-MED の設定が可能。この機能は LLDP-MED をサポートする VoIP 装置に適用されます。

設定方法

LLDP-MED を設定するには、以下の手順に従ってください。
Step 1. [Configration]→[LLDP-MED Configuration]をクリックします。
Step 2.「Fast start repeat count」の値を修正してください。初期設定値は「4」です。
Step 3.「Coordinates Location」の値を修正してください。
Step 4.「Civic Address Location」の値を入力してください。
Step 5. 新しく追加する場合は、<Add new policy>ボタンをクリックします。
Step 6. <Save>ボタンをクリックすると、次の「Policy Port Configuration」が表示されます。
Step 7. 各ポートの「Policy ID」を設定します。
Step 8. <Save>ボタンをクリックします。

Figure 2.8.3:　The LLDP-MED Configuration



設定/表示項目

Fast start repeat count
エンドポイントの高速スタートアップおよび緊急コールサービスロケーション ID 検出は、VoIP システムのとても重要な要素です。さらに、制限された LLDPU(LLDP の PDU)のスペースを保持したり、セキュリティおよびシステムの整合性の問題を軽減するために、特定のエンドポイントのタイプに関する情報の一部を通知する際（例えば、ボイスネットワークポリシーを許可された音声対応装置にのみ通知する場合）に最適です。
LLDP-MED は、関連のある特性を得るために、プロトコルとプロトコルの最上位層のアプリケーション層の間で LLDP-MED Fast Start の相互作用を定義します。
まず、ネットワーク接続装置は、LLDPDU の LLDP TLVs のみの送信を行います。
LLDP-MED エンドポイント装置を検出すると、LLDP-MED capable ネットワーク接続装置は関連のあるポート上で出力中の LLDPDUs に LLDP-MED TLVs の通知を開始します。

新しい近隣装置と LLDP-MED の情報をより早く共有するために、新規の LLDP-MED 近隣装置を検出すると、LLDP-MED アプリケーションは 瞬時に LLDPDU の高速で送信を開始します。
近隣装置間の通信時に LLDP フレームをロスとする可能性があるため、近隣装置が LLDP フレームを受信できるように fast start 通信を複数回繰り返し行うことを推奨します。Fast start リピートカウントでは、fast start 通信を繰り返し行う回数を指定することができます。推奨値は「4 回」です。新しい情報をもつ LLDP フレームを受信すると、1 秒間隔で 4 つの LLDP フレームが送信されます。
LLDP-MED および LLDP-MED Fast Start 方式は、ネットワーク接続装置を含む LAN インフラストラクチャ間のリンク、またはそれ以外のリンクを行うのではなく、LLDP-MED ネットワーク接続装置およエンドポイントデバイス間のリンク上でのみ動作することを目的としています。

Latitude :
緯度は、最大 4 桁の 0-90 度範囲内に標準化されています。赤道の北/南へのいずれかの方向を指定することが可能です。

Longitude :
経度は、最大 4 桁の 0-180 度範囲内に標準化されています。本初子午線の東/西へのいずれかの方向を指定することが可能です。

Altitude :
標高は、最高 4 つの数字で-32767～32767 の内に標準化されます。2 つの高度と使用する測定単位（メートルまたはフロア数）を指定します。
メートル: 指定の垂直のデータによって定義された高度のメーターが表示されます。
フロア数: 異なるフロア間の寸法をもつビルの床から床の次元を持っている建物においてより適切な形式で高度を表わすこと。
高度=0.0 は建物の外でさえ意味があり、与えられた経緯度の地上高度を表わします。建物の内部の場合、0.0 は、正面玄関で地上高度からの床面の高さを表します。

Map Datum :

測地系は、オプションで、測地系とは地図を作成する上でその地図の座標表示方法の基になっているルールです。GPS で測位した緯度経度を地図上で確認する為、あるいは GPS の測位データーを電子地図上で表示させるためには GPS の測地系と地図の測地系を合せる必要があります。
WGS84: 1984 年世界測地系、本初子午線名：グリニッジ
NAD83/NAVD88: 1983 年北米測地系、1988 年北米垂直測地系
NAD83/MLLW: 1983 年北米測地系、平均低低潮
Civic Address Location
ロケーション　IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country code :
ISO 3166 の国番号（2桁）　大文字の ASCII 文字- 例：DK, DE あるいは、US.

State :
全国細別(州、県、地域、州、県)。

County :
国、County, parish, 郡 (日本), district.

City :
都市、郡区、市(日本) - 例:コペンハーゲン

City district :
都市部門、自治町村、都市地区、監視、町(日本)。

Block (Neighbourhood) :
近隣、ブロック

Street :
街 - 例:Poppelvej。

Leading street direction :
Leading street direction - 例: N.
Trailing street suffix :
町名番地のサフィックス- 例: SW.

Street suffix :
Street suffix - 例: Ave, Platz.

House no. :
番地- 例: 21.

House no. suffix :
番地 suffix - 例: A, 1/2.

Landmark :
ランドマーク、あるいは不正アドレス - 例: Columbia University.

Additional location info :
追加ロケーション情報- 例: South Wing.

Name :
名前(住宅およびオフィス占有者) – 例: Flemming Jahn.

Zip code :
郵便番号- 例: 2791.

Building :
ビル(構造) - 例: Low Library.

Apartment :
Unit (Apartment, suite) - 例: Apt 42.

Floor :
Floor - 例: 4.

Room no. :
部屋番号- 例: 450F.

Place type :
Place type - 例: オフィス

Postal community name :
郵便のコミュニティー名 - 例: Leonia.

P.O. Box :
私書箱(郵便局 BOX) - 例:12345

Additional code :
補足コード – 例: 1320300003.

Emergency Call Service:
緊急電話サービス: (例えば、E911 および緊急電話サービス ELIN 識別子データフォーマットは従来の CAMA か ISDN のトランクベースの PSAP への緊急電話時に使用されるような ELIN 識別子を動作させるために定義されます。このフォーマットは、数の数字ストリング(緊急職業に使用される ELIN に対応)から成ります。

Policies
ネットワークポリシー検出機能により、関連のあるレイヤ2およびレイヤ 3 の属性（一連のポートの特定のプロトコルのアプリケーションに適用される）に併せて、VLAN 設定の検出および不適合の場合の診断が可能になります。不適切なネットワークポリシーの設定は VoIP 環境で非常に重要な問題であり、その結果度々音質の低下やサービスロスを起こる可能性があります。
ポリシーは、サービスロス/ビデオサービスなどの特定のリアルタイムのネットワークポリシーの要件をもつアプリケーションと使用することを目的としています。
通知されるネットワークポリシーの属性は、以下のとおりです。

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)
ネットワークポリシーは、指定したポートでサポートされる複数のアプリケーションと関連して、通知される可能性があります。アプリケーションのタイプのアドレスは以下のとおりです。
1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signalling（条件に応じて、上記のメディアの異なるネットワークポリシーをサポートします。）
大規模なネットワークは、組織全体の複数の VoIP ポリシー、アプリケーションのタイプごとに異なるポリシーをサポートしています。LLDP-MED により、複数のポリシーはポートごとに通知することが可能となり、それぞれ異なるアプリケーションタイプに対応しています。同じネットワーク接続装置上の異なるポートは認証されたユーザ ID、またはポート設定に応じて各種ポリシーを通知することができます。
LLDP-MED は、ネットワーク接続装置とエンドポイント間以外のリンク上で動作しないため、LAN の内部のアグリゲートリンク上で動作する複数のネットワークポリシーを通知する必要はありませんので、ご注意ください。

Delete :
ポリシーを削除します。<Delete>ボタンをクリックした後、<Save>ボタンをクリックすると削除されます。

Policy ID :
ポリシーの ID。これは、自動生成され、特定のポートにマッピングされるポリシーを選択時に使用されます。

Application Type :
アプリケーションタイプの用途については、以下のとおりです。
1. Voice
専用 IP 電話端末機およびその他の双方向音声サービスをサポートする同様の設備用です。これらの装置は異なる VLAN 上で通常配置され、データアプリケーションと分けることにより、配置が容易になり、セキュリティが強化されます。
2. Voice Signalling (conditional)
音声メディアよりも音声シグナリング用の各種ポリシーを要するネットワークトポロジー用。このアプリケーションタイプは、ネットワークポリシーが音声アプリケーションポリシーで通知されたもの同一であれば通知を行いません。
3. Guest Voice
ゲストユーザ向け「制限された機能のセット」と、独自の IP 電話装置と同様の双方向音声サービスをサポートする設備をもつビジター向けです。
4. Guest Voice Signalling (conditional)
ゲストボイスメディア以外のゲストボイスの信号化用の異なるポリシーを要するネットワークトポロ ジー向け。このアプリケーションタイプは、ネットワークポリシーがゲストボイスアプリケーションのポリシーと同じ場合は、通知を行いません。

5. Softphone Voice

パソコンやノートパソコンなどのデータ中心のデバイス上のソフトフォン用。 エンドポイントのクラスは'untagged'VLAN または単一のタグ付きデータ固有の VLAN 用に設定されます。ネットワークポリシーが'untagged'VLAN 用に定義されている場合（「以下のタグ付きフラグを参照」）は、L2 プライオリティフィールドは無効となり、DSCP 値のみが適切な値です。
6. Video Conferencing
専用テレビ会議装置および同様の同時双方向ビデオ/オーディオサービス用です。
7. Streaming Video
ブロードキャストまたはマルチキャストベースのビデオコンテンツ配布、および特定のネットワークポロシー処理を要するストリーミングビデオサービス用のアプリケーション向けです。
バッファをもつ TCP 対応のビデオアプリケーションは、対象になりません。
8. Video Signalling (conditional)
ビデオメディアではなく、ビデオ信号用の異なるポロシーを要するネットワークトポロジー向けです。
ネットワークポリシーがすべてビデオ会議用のアプリケーションポリシーと同じ場合は、アプリケーションタイプの通知を行いません。

Tag :
指定したアプリケーションのタイプが'tagged'あるいは'untagged' VLAN を使用しているかどうかを示します。「タグなし」は、タグなしフレームの書式を用いて、「IEEE 802.1Q-2003」によって定義されたタグヘッダは含まれません。
この場合、VLAN ID およびレイヤー2 のプライオリティは無視され、DSCP 値のみ有効です。
「タグなし」は、IEEE 802.1Q タグ付きフレームの書式を用いて、VLAN ID および Layer 2 のプライオリティ値とDSCP 値を使用します。タグ付きには、タグヘッダという追加フィールドが含まれます。タグ付きフレームには、「IEEE 802.1Q-2003」で定義されているプライオリティのタグ付きフレームも含まれます。

VLAN ID :
IEEE 802.1Q-2003 に定義されているポートの VLAN 識別子(VID)

L2 Priority :
L2 プライオリティは、指定したアプリケーションタイプ用のレイヤ2のプライオリティです。L2 プライオリティは、IEEE 802.1D-2004 で定義されたレベル(0～7)のプライオリティのいずれかを指定することができます。「0 の A」値は、IEEE 802.1D-2004 で定義されている初期設定のプライオリティを使用してることを意味します。DSCP には、64 個のコードポイントの値(0～63)の 1 つが含まれます。

DSCP :
DSCP 値を使って、IETF RFC 2474 で定義されている指定のアプリケーションの Diffserv ノードの動作を提供します。「0 の A」値は、RFC 2475 で定義されている初期設定の DSCP 値を使用していることを示します。

Adding a new policy :
<add a new policy>をクリックして、新規ポロシー用のアプリケーションタイプ、Tag、VLAN ID、L2 プライオリティおよび DSCP を入力して<Save>ボタンをクリックします。

Port Policies Configuration :

どのポートも認証されたユーザ ID、またはポート設定に応じて、同一のネットワークポリシーの固有のネットワークポリシー、または各種属性を通知します。

Port :
設定に適用されるポート番号

Policy Id :
指定したポートに適用される一連のポリシー。対応するポリシーに☑を入れることにより、選択することができます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.8.4 LLDP-MED Neighbours

LLDP-MED 近隣装置.のステータスについて説明します。
テーブルには、検出した LLDP 近隣装置の各ポートの情報が表示されます。この機能は、LLDP-MED をサポートする VoIP 装置に適用されます。

設定方法

LLDP-MED 近隣装置を表示するには、以下の手順に従ってください。
Step 1. 「LLDP-MED neighbours」をクリックします。
Step 2. <Refresh>ボタンをクリックすると、画面は手動で更新されます。
Step 3. <Auto-refresh>ボタンをクリックすると、画面は自動で更新されます。

Figure 2.8.4:　The LLDP-MED Neighbours information

【注記】:
お使いのネットワークに LLDP-MED 対応装置がない場合は、テーブルには“No LLDP-MED neighbour information found”と表示されます。

設定/表示項目

Port :
LLDP フレームを受信したポート.

Device Type :
LLDP-MED 装置は主に 2 つのタイプ（ネットワーク接続装置およびエンドポイント装置）から構成されています。
LLDP-MED ネットワーク接続装置 の定義は下記のとおりです。
LLDP-MED ネットワーク接続装置は TIA-1057 で定義されたおり、LLDP-MED エンドポイント装置用の IEEE802 準拠の LAN インフラストラクチャへのアクセスを行います。
1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (履歴を含む)
4. IEEE 802.11 Wireless Access Point
5. TIA-1057 によって定義された IEEE 802.1AB および ME エクステンションをサポートし、任意の方法
を介して IEEE802 フレームを中継可能な装置
LLDP-MED エンドポイント装置の定義
LLDP-MED エンドポイント装置は TIA-1057 で定義されており、IEEE 802 LAN ネットワークのエッジに位置しており、LLDP-MED フレームワークを使った IP コミュニケーションサービスに参加しています。
LLDP-MED エンドポイント装置の分野では、LLDP-MED スキームは、以下に定義されているように、エンドデバイスクラスに分けられます。
LLDP-MED エンドポイント装置クラスは、以前のエンドポイント装置クラスに定義されたケイパビリティに応じて定義されます。

LLDP-MED Generic Endpoint (Class I) :
LLDP-MED ジェネリック・エンドポイント (Class I)の定義は、TIA-1057 で定義されているベースの LLDP 検出サービスを要するエンドポイント製品にすべて適用可能ですが、IP メディアはサポートしておらず、エンドユーザ向け通信機器として作用します。装置には、IP 通信コントローラ（これに制限されない）、その他の通信に関連のあるサーバ、TIA-1057 で定義されている基本サービスを要する装置は含まれません。このクラスに定義されている検出サービスには、LAN コンフィグレーション、装置の設置場所、ネットワークポロシー、電力管理および在庫管理が含まれます。

LLDP-MED Media Endpoint (Class II) :
LLDP-MED メディアエンドポイント (Class II)の定義は、IP メディアケイパビリティを持つエンドポイントの製品すべてに適用されますが、または特定のエンドユーザとのに関連ありません。ケイパビリティには、ジェネリック・エンドポイント・クラス (Class I)向けに定義されたケイパビリティがすべて含まれ、更にメディアストリーミングに関連のある要素が含まれます。たとえば、製品カテゴリとして、Voice / Media Gateways, Conference Bridges, Media Servers などが含まれます。
このクラスに定義されている検知サービスにはメディアタイプ固有のネットワークレイヤポリシー検知が含まれます。

LLDP-MED Communication Endpoint (Class III) :
LLDP-MED 通信エンドポイント (Class III)では、IP メディアをサポートするエンドユーザ通信機器として動作するエンドポイント製品に適用可能です。

ケイパビリティには、ジェネリック・エンドポイント (Class I) およびメディアエンドポイント(Class II)クラスで定義されたケイパビリティのすべてが含まれ、更にエンドユーザデバイスに関連のある要素まで含まれます。
例えば、製品カテゴリは、IP フォン、PC ベースソフトトフォン、あるいはエンドユーザ向け通信機器などがあります。
このクラスで定義されている検出サーバには、設置場所検知（ECS / E911 情報）、L2 スイッチ、在庫管理が含まれます。

LLDP-MED Capabilities :
LLDP-MED ケイパビリティでは、近隣装置の LLDP-MED ケイパビリティについて説明します。可能なケイパビリティについては、以下のとおりです。
1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved
Application Type：
アプリケーションタイプは、エンドポイント、またはネットワーク接続装置によって通知されるネットワークポリシー用に定義されたアプリケーションの主な機能を示します。

設定可能なアプリケーションタイプは下記のとおりです。

1. Voice
専用 IP 送受器および双方向音声サービス用の同様の機器向け。これらの機器は通常個々の VLAN を採用することにより、データアプリケーションから隔離して、配置を容易に、かつセキュリティを強化します。
2. Voice Signalling
音声メディア用以外の音声信号用の各種ポロシーを要するネットワークトポロジー向け。
3. Guest Voice
専用の IP 送受器や双方向音声サービス用のその他の同様の装置をもつゲストユーザやビジター向けの異なる制限された feature-set 音声サービスをサポート。
4. Guest Voice Signalling
ゲスト用音声メディア以外のゲスト用音声信号用の各種ポリシーを要するネットワークトポロジー向け。
5. Softphone Voice
パソコンやノートパソコンなどの.データ中央装置上のソフトフォンアプリケーション向け。
6. Video Conferencing
専用テレビ会議装置および双方向ビデオ/オーディオサービス.用の同様の装置向け。
7. Streaming Video
ブロードキャスト/マルチキャストベースのビデオコンテンツ配信および特定のネットワークポロシー処理を要するストリーミングビデオサービス用の同様のアプリケーション向け、バッファをもつ TCP によって異なるビデオアプリケーションは、このアプリケーションタイプの対象となりません。
8. Video Signalling
ビデオメディア用ではなく、ビデオ信号用の別のポロシーを要する. ネットワークトポロジー向け。

Policy :
ポリシーとは、エンドポイントデバイスがデバイスに要するポリシーの通知を行う状態を指します。
「Defined」あるいは「Unknown」のいずれかを選択可能です。
Unknown: 指定したアプリケーションタイプのネットワークポロシーが現在認識されていない。
Defined: ネットワークポロシーが定義されている状態

TAG :
TAG は、指定したアプリケーションタイプがタグ付き/タグなし VLAN を使用しているかどうかを示します。
Untagged: デバイスは、タグなしフレームの書式を使用し、IEEE 802.1Q-2003 で定義されているタグヘッダは含まれません。Tagged: IEEE 802.1Q タグ付きフレームの書式を使用しています。

VLAN ID :
VLAN ID は、IEEE 802.1Q-2003 で定義されているポート用の VLAN 識別子(VID) 。値（1～4094）を使って、有効な VLAN ID を定義します。IEEE 802.1Q-2003 で定義されているプライオリティタグ付きフレームを使用している場合は、0 の値（プライオリティタグ付き）を使用します。これは、IEEE 802.1D プライオリティレベルのみが重要で、その代わりに入力ポートの初期設定の PVID を使用します。

Priority :
プライオリティは、指定したアプリケーションタイプに使用したいレイヤ2のプライオリティ。
8レベルのプライオリティ（0～7）の1つです。

DSCP :
DSCP は、IETF RFC 2474 で定義されている指定のアプリケーションタイプの Diffserv ノード動作用の DSCP 値。64 コードのポイント値(0～63)の1つが含まれます。

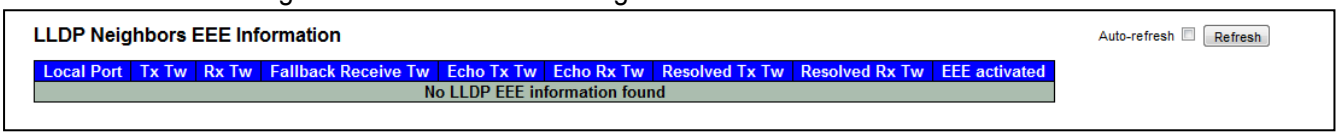
2.8.5 EEE

EEE 省エネルギーを使って、トラフィック遅延により、省電力を行います。リンク上でトラフィックの送信前の起動に要する間、電源を「OFF」にすることにより遅延が発生します。
これを、"wakeup time"と言います。
遅延を最小限に抑えるために、LLDP を使って、それぞれの tx と rx の wakeup time についての情報を交換します。
LLDP によって交換された EEE 情報の概要について説明します。

設定方法

LLDP の EEE 近隣装置を表示するには、以下の手順に従ってください。:
Step 1. [LLDP]→[EEE]をクリックすると、検出した EEE 装置が表示されます。
Step 2. <Refresh>ボタンをクリックすると、画面は手動で更新されます。
Step 3.<Auto-refresh>ボタンをクリックすると、画面は自動で更新されます。

Figure 2.8.6:　The LLDP Neighbours EEE information



【注記】:
お使いのネットワークに EEE 機能が有効な装置がない場合は、テーブルには、“No LLDP EEE information found”と表示されます。

設定/表示項目

Local Port :
LLDP フレームを送受信したポート

Tx Tw :
LPI のディアサート後、データの送信を阻止可能なパスを送信するリンクパートナーの最大時間 e

Rx Tw :
送信機に対して、受信側がスリープ状態から起動するまでの許容時間を抑えるためのリンクパートナーの時間。

Fallback Receive Tw :
リンクパートナー側の fallback receive Tw
受信側のリンクパートナーはトランスミッタに代替用の指定の Tw_sys_tx を通知します。受信側のリンクパートナーは保存用とは異なるレベルを持っている可能性があるため、トランミッタに更に効率的な割り当て用が可能な追加情報を提供します。Receive Tw_sys_tx の値と同じオプションの初期設定値を提供しません。

Echo Tx Tw :
リンクパートナーのエコーTx の Tw 値
それぞれのエコーの値は、リモートリンクパートナーのそれぞれの値のローカルリンクパートナーのエコーとして定義されます。ローカルリンクパートナーはリモートリンクパートナーからのエコー値を受信すると、最新の値がリモートリンクパートナーにより受信、登録、あるいは処理されたかどうかを判断することができます。
例えば、ローカルリンクパートナーがローカル MIB の値に一致しないエコーパラメータを受信した場合は、ローカルリンクパートナーはリモートリンクパートナーのリクエストが古い情報であると判断します。

Echo Rx Tw :
リンクパートナーのエコーRx の Tw 値

Resolved Tx Tw :
このリンク用に解決された Tx の Tw 値
※ リンクパートナではありません。
このリンク（LLDP を介して変換された EEE 情報に応じて）に使用される実際の"tx wakeup time "の解決値

Resolved Rx Tw :
このリンク用に解決された Rx の Tw。
※ リンクパートナではありません。
このリンク（LLDP を介して変換された EEE 情報に応じて）に使用される実際の"tx wakeup time "の解決値

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

2.8.7 Port Statistics

2 つのカウンタが表示されます。「Global counters」では、スタックスイッチ全体、「local counters」では現在選択されているスイッチのポート単位のカウンタが表示されます。

設定方法

LLDP 統計情報を表示するには、以下の手順に従ってください。
Step 1. [Configration]→[LLDP]→[Port Statistics]をクリックして、統計情報が表示されます。
Step 2. <Refresh>ボタンをクリックすると、画面は手動で更新されます。
Step 3. <Auto-refresh>ボタンをクリックすると、画面は自動で更新されます。
Step 4. <Clear>ボタンをクリックすると、すべてのカウンタ値が消去されます。

Figure 2.8.7:　The LLDP Port Statistics information

Global Counters	
Neighbour entries were last changed	2011-01-01 00:00:00 (10579 sec. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics

Local Counters							
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Age-Outs
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0

設定/表示項目

Neighbour entries were last changed at :
最後の項目が削除/追加された時間が表示されます。最後に変更後の経過時間も表示されます。

Total Neighbours Entries Added :
スイッチが再起動してから追加された新しい項目数が表示されます。

Total Neighbours Entries Deleted :
スイッチが再起動してから削除された新しい項目数が表示されます。

Total Neighbours Entries Dropped :
テーブルがいっぱいになり、破棄された LLDP フレーム数が表示されます。

Total Neighbours Entries Aged Out :
有効期間が切れて、削除されたエントリ数が表示されます。

Local Counters
テーブルには、各ポートの次の項目が表示されます。

Local Port :
LLDP フレームを送受信したポート

Tx Frames :
ポート上の LLDP フレームの送信数 .

Rx Frames :
ポート上の LLDP フレームの受信数

Rx Errors :
エラーをもつ LLDP フレームの受信数

Frames Discarded :
受信したフレームで内部テーブルがいっぱいになると、 LLDP フレームがカウントされ破棄されます。この場合、LLDP 規格では、"Too Many Neighbours"と表示されます。シャーシ ID とリモートポート ID がテーブル内にない場合、LLDP フレームは新しいエントリを必要とします。指定のポートのリンクが切れたり、LLDP シャットダウンフレームを受信したり、エントリのエージングが切れると、エントリがテーブルから削除されます。

TLVs Discarded :
各 LLDP フレームには、TLVs という複数の情報が含まれます。
TLV に問題がある場合は、カウントされ破棄されます。

TLVs Unrecognized :
アンノウンタイプの値をもつ正しい TLV の数

Org. Discarded :
TLV の受信数

Age-Outs :
各 LLDP フレームには、LLDP 情報の有効な時間（エイジアウト）が含まれます。エイジアウトまでに新しい LLDP フレームを受信しない場合は、LLDP 情報は削除され、エイジアウトカウンターが増えます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, Clear):
<Refresh>ボタンをクリックすると、統計情報が更新され、<Clear>ボタンをクリックすると、エントリが削除されます。

2.9 PoE

PoE（Power Over Ethernet）は、標準のイーサネットケーブルを介してリモート装置に電力を送信するために使用します。主に電力供給が困難な場所に設置された Web カメラ、スイッチングハブ、無線 LAN アクセスポイント、IP 電話機などで利用されます。

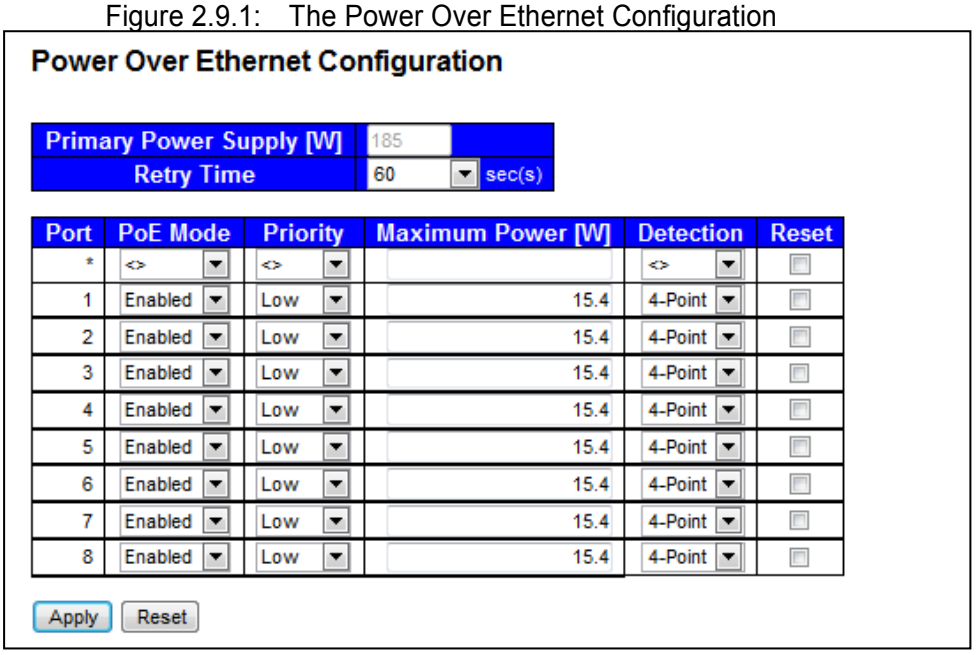
2.9.1 Configuration

ここでは、現行の PoE ポートの設定の設定、およびすべての PoE 供給電力の表示方法について説明します。

設定方法

PoE(Power Over Ethernet)の設定方法については、以下の手順に従ってください。
Step 1. [Configration]→[PoE]→[Configuration]をクリックします。
Step 2. 設定されている電源、電源管理モードを指定して、PoE あるいは PoE+、プライオリティを選択します。
Step 3. <Save>ボタンをクリックします。

Figure 2.9.1:　The Power Over Ethernet Configuration



設定/表示項目

Power Over Ethernet Configuration

Primary Power Supply [W] :
本機は、PoE 電源を搭載しています。PD の給電する量を決定する場合は、まず給電可能な量を設定する必要があります。

ポートの設定

Port :
論理ポート番号

POE Mode:
ポートの PoE 動作状況を示す PoE モード
Disabled: ポートの PoE を無効にします。
Enabled : PoE IEEE 802.3af/at を有効にします。

Priority :
ポートのプライオリティ。このプライオリティには3レベル（Low、High および Critical）
リモート装置が給電可能な電力以上必要な場合のプライオリティです。一番プライオリティの低いポートは、プライオリティの一番高いポートをもつポートからの開始を中止します。

Maximum Power :
最大電力値はリモート装置に給電可能な最大電力をワット単位の数値で表します。

Detection:
給電の検知方法
Legacy: 従来の検知方法
4-Point: 信頼性の高い 4 ポイント検出
Both: 上記両方の検知方法

【注記】:
IEEE802.3at 対応のポートを設定したい場合は、最大許容値は「30W」です。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合は、ローカルに変更した内容を取り消して、元の値に戻します。

2.9.2 Status

この画面では、PoE ポートのステータスを確認することが可能です。

設定方法

PoE のステータスを表示するには、以下の手順に従ってください。
Step 1. [Configration]→[PoE]→[Status]をクリックします。
Step 2. PoE のステータスが表示されます。
Step 3. <Refresh>ボタンをクリックします。

Figure 2.9.2:　The Power Over Ethernet Status

Power Over Ethernet Status　　Auto-refresh ☐ Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

設定/表示項目

Local Port :
論理ポート番号.

PD Class :
指定した電流と一致するPDの電源クラスが表示されます。クラスごとに、通常の動作時にPDが必要とする電力量について表示します。

Power Requested :
PD が保持したい電力量が表示されます。

Power Allocated :
PD に割り当てたい電力量が表示されます。

Power Used :
PD が現在使用している電力量が表示されます。

Current Used :
PD が現在使用している電流が表示されます。

Priority :
ユーザによって設定されたポートのプライオリティが表示されます。

Port Status :
ポートのステータスが表示されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、PoE ポート情報が更新されます。

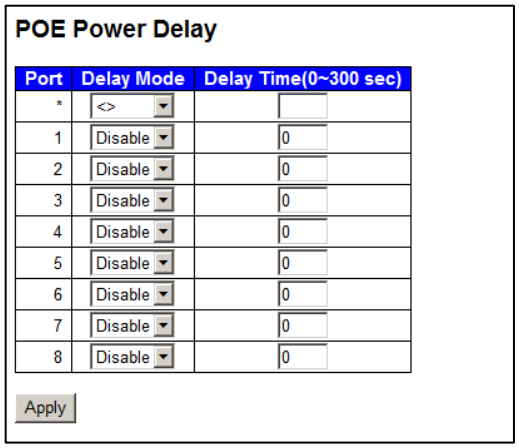
2.9.3 Power Delay

電源供給時に同期をとりやすくするために、遅延時間を設定できます。

設定方法

Step 1. Power Delay を設定するには、[Configration]→[PoE]→[Power Delay]をクリックすると、以下の画面が表示されます。

2.9.3 POE Power Delay



設定/表示項目

Port
理論ポート番号

Delay Mode
遅延の発生の有効/無効の設定

Delay Time
遅延時間を 0 から 300 秒までの間で設定します。

2.9.4 Auto Checking

接続された PD へ Ping による死活監視を行います。

設定方法

Step 1. Auto Checking を設定するには、[Configration]→[PoE]→[Auto Checking]をクリックすると、以下の画面が表示されます。

2.9.4 POE Auto Checking

POE Auto Checking

Ping Check Disable

Port	Ping IP Address	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)
1	0.0.0.0	30	3	error=0 ,total=0	Nothing	15
2	0.0.0.0	30	3	error=0 ,total=0	Nothing	15
3	0.0.0.0	30	3	error=0 ,total=0	Nothing	15
4	0.0.0.0	30	3	error=0 ,total=0	Nothing	15
5	0.0.0.0	30	3	error=0 ,total=0	Nothing	15
6	0.0.0.0	30	3	error=0 ,total=0	Nothing	15
7	0.0.0.0	30	3	error=0 ,total=0	Nothing	15
8	0.0.0.0	30	3	error=0 ,total=0	Nothing	15

Apply

設定/表示項目

Ping Check
PD への死活監視の有効/無効をシステムとして、設定します。

Port
理論ポート番号

Ping IP Address
PD の IP アドレスを設定

Interval-Time
監視間隔時間の設定

Retry Time
監視の繰り返し回数の設定

Failuer Log
エラーログ表示

Failuer Action
応答がなかった場合の動作の設定。
Nothing;何の動作も実行しない。
Reboot Remote PD;
該当ポートのリセットにより PD の再起動する。

Rboot Time
リブート時間の設定（秒）

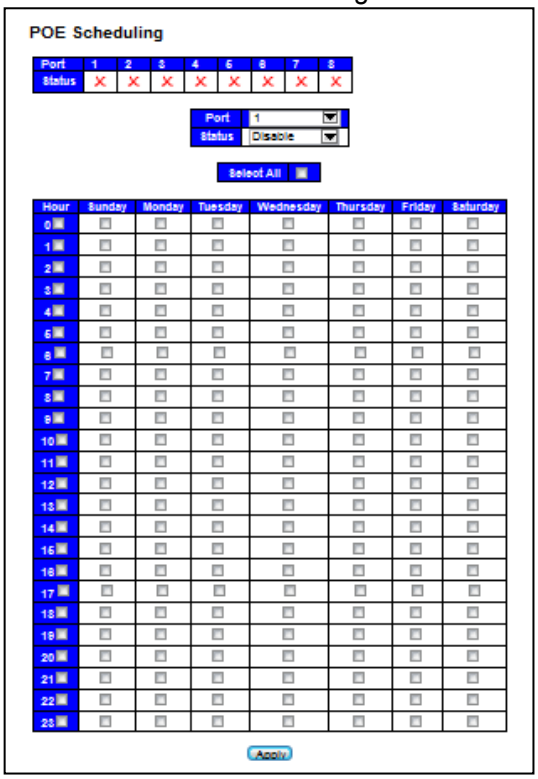
2.9.5 Scheduling

ポート毎に電源供給時間のスケジュールを設定できます。

設定方法

Step 1. スケジュール機能を設定するには、[Configration]→[PoE]→[Scheduling]をクリックすると、以下の画面が表示されます。

2.9.5 POE Scheduling



設定/表示項目

Port/Status
現在の設定状態

Port
物理ポート番号

Status
設定の有効/無効

Select All
すべて選択

Hour (0-24)
設定時間 （1 日）

Sunday – Saturday (Week)
設定曜日（1 週間）

2.10 Fitering Data Base

MAC アドレスによるフィルタリングの設定を行います。
本機は、どのポートのフレームが送信されたかを認識するためにMACアドレスをポートにマッピングするテーブルを作成します。管理者がポート間のマッピングを固定したい場合は、スタティックエントリはネットワーク管理者によって設定されます。
入力フレームの、MAC アドレス(ソース MAC アドレス)により、MAC アドレスが表示されます。ソース MAC アドレスは本機で使用され、ダイナミック MAC アドレスをもつ MAC アドレスを自動的に更新します。設定可能なエイジタイム後に、対応するソース MAC アドレスをもつフレームが検出されない場合は、ダイナミックエントリは MAC テーブルから削除されます。

2.10.1 Configuration

MAC アドレステーブはここで設定します。ダイナミック/スタティックテーブルのエントリのタイムアウトを設定します。

設定方法

MAC アドレステーブル を設定するには、以下の手順に従ってください。
[Configration]→[Filtering Data Base]をクリックします。

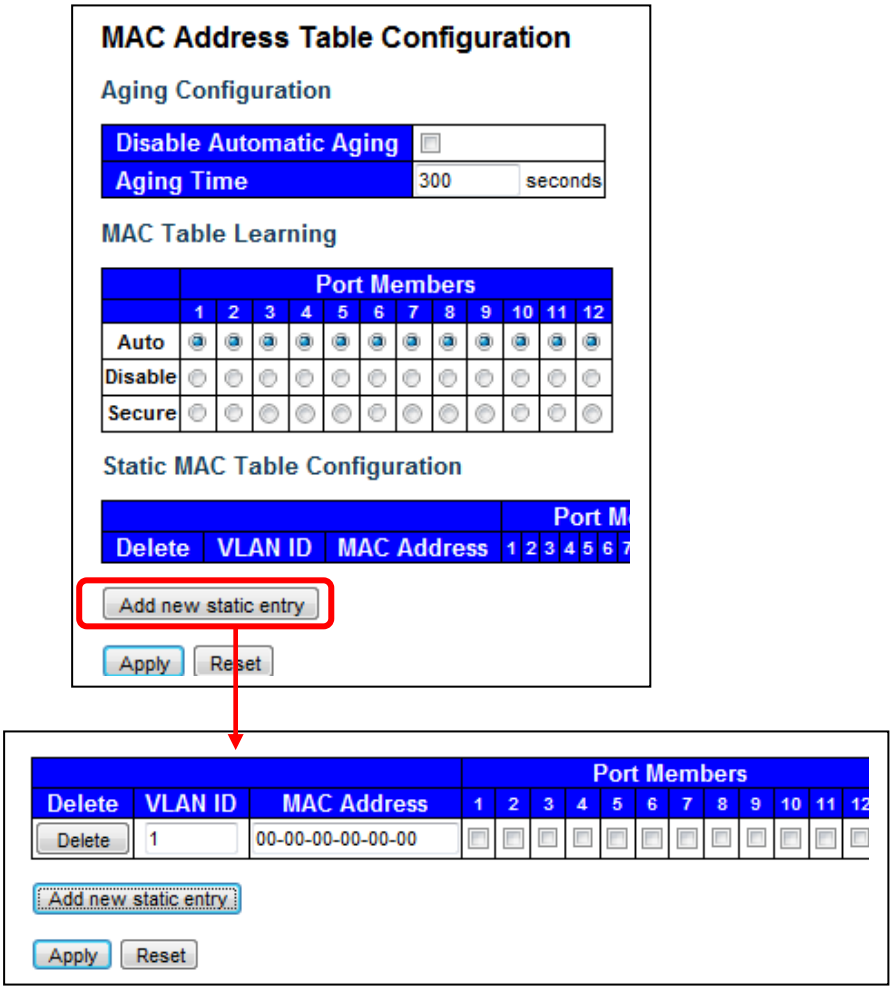
Aging Configuration
1. [Configuration]をクリックします。.
2. 「Disable Automatic Aging」および「Aging Time」を設定します。
3. <Save>ボタンをクリックします。

MAC Table Learning

1. [Configuration]をクリックします。.
2. 「Port Members」を「Auto」、「Disable」、「Secure」から選択します。
3. <Save>ボタンをクリックします。

Static MAC Table Configuration
1. [Configuration]→[Add new Static entry]をクリックします。
2. 「VLAN IP」および「Mac address」、「Port Members」の値を入力します。
3. <Save>ボタンをクリックします。

Figure 2.10.1:　The MAC Address Table Configuration



設定/表示項目

Aging Configuration :
初期設定では、ダイナミックエントリは「300 秒」後に MAC テーブルから削除されます。これを「エージング」とも呼びます。エージングタイムの値を設定します。設定可能な「10～1000000 秒」です。「Disable automatic aging」の項目に☑を入れると、ダイナミックエントリの自動エージング機能が無効になります。

MAC Table Learning
指定されたポートの学習モードがグレイ表示されている場合は、別のモジュールにより制御されているため、値を変更することはできません。
たとえば、モードが 802.1X.の MAC ベース認証の場合です。
各ポートは次の設定に応じて学習を行います。
Auto :
アンノウンのソース MAC をもつフレームを受信するとすぐに自動的に学習を行います。
Disable :
学習は行いません。
Secure :
スタティック MAC 項目のみ学習しますが、その他のフレームはすべて破棄します。

【注記】:
学習モードに変更される前に、スイッチの管理に使用されるリンクがスタティック Mac テーブルに追加されたことを確認してください。
管理用リンクが切れた場合は、別の non-secure ポート、またはシリアルインタフェースを介してスイッチに接続することによってのみリストアすることが可能です。

Static MAC Table Configuration
MAC テーブルのスタティックエントリが表示されます。スタティック MAC テーブルには、64 エントリが含まれます 64 エントリはスタック全体用で、各スイッチ用ではありません。MAC テーブルは、まず VLAN ID ごとに表示され、次に MAC アドレスごとに表示されます。

Delete :
削除したい項目を選択して、<Save>ボタンをクックすると削除されます。

VLAN ID :
エントリの VLAN ID

MAC Address :
エントリの MAC アドレス.

Port Members :
メンバーポートには☑がついています。ポートを修正する場合は☑を入れてください。

Adding a New Static Entry :
スタティック MAC テーブルの<add a new entry> をクリックします。新しいエントリの VLAN ID、 MAC アドレス、およびポートメンバを指定して、<Save>ボタンをクリックします。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

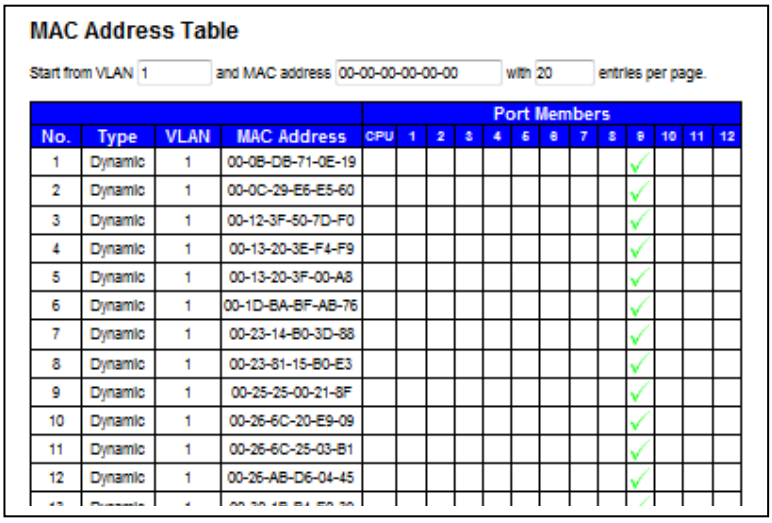
2.10.2 Dynamic MAC Table

MAC テーブルの項目が表示されます。 MAC テーブルには、最大「8192 個」 まで表示され、まず、VLAN ID ごとに、次に MAC アドレスごとに表示されます。

設定方法

「MACアドレステーブル」の表示方法については、以下の手順に従ってください。
Step 1.　　[Configration]→[Filtaring Data Bese]→[Dynamic MAC Table]をクリックします。
Step 2. 「VLAN address」および「MAC address」を指定します。
Step 3.　　MAC アドレステーブルが表示されます。

Figure 2.10.2:　The Dynamic MAC Address Table information



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

				Port Members												
No.	Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
1	Dynamic	1	00-0B-DB-71-0E-19										√			
2	Dynamic	1	00-0C-29-E6-E5-60										√			
3	Dynamic	1	00-12-3F-50-7D-F0										√			
4	Dynamic	1	00-13-20-3E-F4-F9										√			
5	Dynamic	1	00-13-20-3F-00-A8										√			
6	Dynamic	1	00-1D-BA-BF-AB-76										√			
7	Dynamic	1	00-23-14-B0-3D-88										√			
8	Dynamic	1	00-23-81-15-B0-E3										√			
9	Dynamic	1	00-25-25-00-21-8F										√			
10	Dynamic	1	00-26-6C-20-E9-09										√			
11	Dynamic	1	00-26-6C-25-03-B1										√			
12	Dynamic	1	00-26-AB-D6-04-45										√			

設定/表示項目

No.:
MAC アドレスの連番号

Type :
エントリがスタティック/ダイナミックエントリのいずれかが表示されます。

VLAN :
エントリの VLAN ID.

MAC address :
エントリの MAC アドレス.

Port Members :
エントリのメンバーのポート.

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, Clear, <<, >>):
手動で MAC アドレスを更新するか、<Clear>ボタンをクリックして MAC テーブルをクリアにします。
“<<”または”>>“ をクリックして、画面を上下に表示してください。

2.11 VLAN

管理用の特定の VLAN を指定するには、管理 VLAN を使って、VLAN のポートに接続されているワークステーションからの IP 接続を行います。この接続には、VSM、SNMP および Telnet 接続を行うことができます。初期設定では、有効な管理 VLAN は VLAN1 ですが、どの VLAN も管理 VLAN window を使って管理 VLAN として指定することができます。管理 VLAN は一度に 1 つのみ有効です。

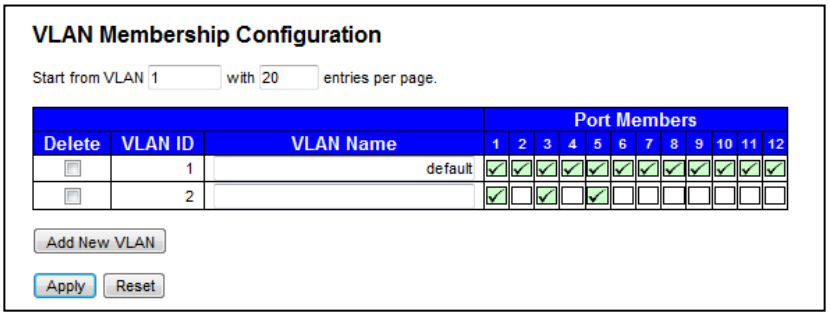
2.11.1 VLAN Membership

選択したスイッチの VLAN メンバーのモニタリングや修正を行います。VLAN は 4094 個（VLAN1 を含む）までサポートしています。ここでは、VLAN の追加/削除以外に、各 VLAN のポートメンバーへの追加/削除を行うことができます。

設定方法

VLANメンバーの設定を行うには、次の手順に従ってください。
Step 1.　[Configration]→[VLAN]→[VLAN membership]をクリックします。
Step 2. 管理VLAN IDを「0～4094」の範囲内で入力します。
Step 3.　<Apply>ボタンをクリックします。

Figure 2.11.1:　The VLAN Membership Configuration



設定/表示項目

Delete :
VLAN エントリを削除するには、☑を入れて<Apply>をクリックしてください。スタック内の選択されたスイッチのエントリを削除します。

VLAN ID :
特定の VLAN の ID を指します（1～4094）。

VLAN Name :
VLAN 名を示します。VLAN 名は英文字、または数字のいずれかのみ使用可です。既存の VLAN エントリの VLAN 名を編集したり、新しいエントリに追加することもできます。
VLAN 名は省略可能です。

Port Members :
各 VLAN ID ごとに各ポートのチェックボックスが表示されます。VLAN にポートを設定するには、ボックスに☑を入れます。VLAN からポートを削除するには、そのポートが選択されていないことを確認してください。初期設定では、メンバーのポートはありませんので、すべてのポートは☑されていない状態です。

Add New VLAN :
<add new VLAN>ボタンをクリックすると、空の行がテーブルに追加されます。必要に応じて、VLAN を設定することができます。設定可能な VLAN ID の値は「1～4094」です。
<Apply>ボタンをクリックすると、VLAN は「有効」になります。
VLAN には、最低でも 1 つのポートをメンバに追加する必要があります。
<Apply>ボタンをクリックすると、機器のポートメンバーをもたない VLAN は削除されます。
<Reset>ボタンをクリックすると、追加された新規 VLAN の設定を取り消すことができます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

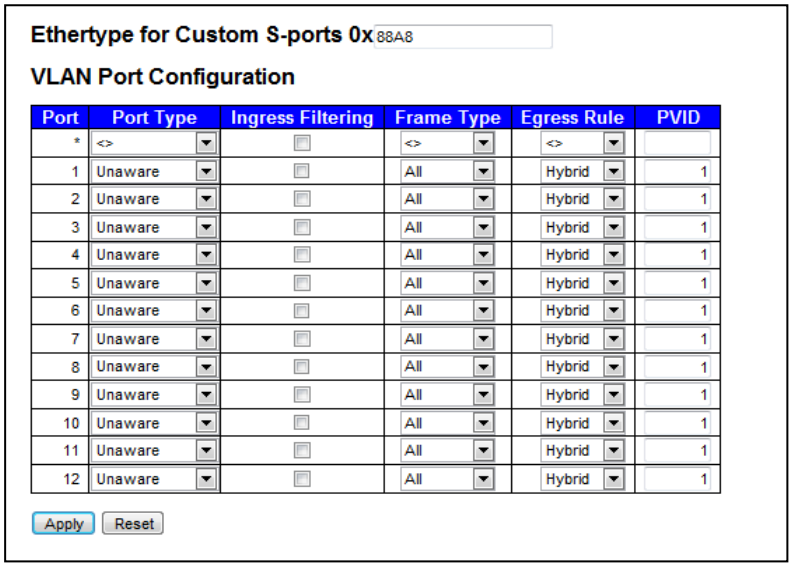
2.11.2 Ports

VLAN のタグルール設定の機能は、ユーザは各ポートに VID 番頭を入力することができます。
VID 番号の範囲は「1～4094」です。また各ポートへのフィルタリングルールも選択可能です。本機に適用可能な入力フィルタリングのルールは2つあり、それぞれ「ポートに設定された VID と一致する VID を持つパケットのみ伝送すること」と「タグなしフレームを破棄すること」です。各ポートの役割は「Access」、「Trunk」、「Hybrid」から選択することが可能です。

設定方法

VLAN ポートの設定を行うには、次の手順に従ってください。
Step 1.　[Configration]→「VLAN Port Configuration」をクリックします。
Step 2.　「VLAN Port Configuration」を値を入力します。
Step 3.　<Apply>ボタンをクリックします。

Figure 2.11.2:　The VLAN Port Configuration



設定/表示項目

Ethertype for Custom S-ports :
ポートタイプの「Custom S-ports」用のイーサネットタイプを指定します。これは、Custom S-ports すべてにグローバル設定です。カスタムイーサタイプによってユーザはポートのイーサネットタイプの値を、802.1Q-tagged/802.1p-tagged フレーム上の標準の 0x8100 イーサネットタイプの値を使用しない場合に設定します。上部の「Ethertype for Custom S-ports 0x」の部分で値を変更することができます。

Port :
論理ポートの番号です。

Port Type :
ポートタイプは次のいずれかになります:
「Unaware」,「Customer port(C-port)」,「Service port(S-port)」,「Custom Service port(S-custom-port)」
※ 通常の IEEE802.1Q-VLAN の設定は、ポートタイプに「C-Port」を設定します。
ポートタイプが「Unaware」の場合は、フレームはすべて Port VLAN ID にグループ化され、タグは削除されます。
サービスタグ(S-Tag)は、キャリア網内の転送に用いられる4byte の VLAN タグ。
イーサネットタイプは、0x88-a8 の値に設定されます。
カスタマタグ(C-Tag)は、ユーザ網内の転送に用いられる 4byte の VLAN タグ。

Ingress Filtering :
ポートの入力フィルタリングを有効にするには、ボックスに☑を入れてください。この値によって VLAN 入力処理は異なります。入力フィルタリング が有効で、かつ入力ポートがフレームごとに分類された VLAN のメンバーでない場合は、フレームは破棄されます。
初期設定では、入力フィルタリングは無効になります（ボックスは☑されていません）。

Frame Type :
ポートが受信するフレームについて、フレームすべて、またはタグ付き/タグなしフレームのいずれかを受信するかどうかを設定します。この値によって、VLAN 入力処理が異なります。ポートがタグ付きフレームのみを許可する場合、ポートで受信されたタグなしフレームは破棄されます。初期設定では、「All」に設定されます。

Egress Rule:
送信フレームにタグを付与するか、削除するかを設定します。
Hybrid タグ・タグなし両方に設定します。
Trunk 出力フレームにタグを付与します。
Access 出力フレームのタグを削除します

PVID
ポートが所属している NativeVLAN を設定します。
設定可能な値は 「1～ 4095」です。初期設定は、「1」です。

【注記】:
ポートは VLAN ID と同じ VLAN のメンバに設定する必要があります。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.11.3 Switch Status

すべての VLAN 情報を収集して、「Staic」、「NAS」、「MVRP」、「MVP」、「音声用 VLAN」、「MSTP」、「GVRP」、「Combined」の中からいずれかの方法で通知します。

設定方法

VLAN メンバーの状態を表示するには、以下の手順に従ってください。
Step 1. [Configration]→[VLAN]→[Switch Status]をクリックします。
Step 2. 「Staic」、「NAS」、「MVRP」、「 MVP」、「音声用 VLAN」、「MSTP」、「GVRP」「Combined」のいずれかから選択します。
Step 3. メンバー情報が表示されます。

Figure 2.11.3:　The VLAN Membership Status for Staticuser

設定/表示項目

VLAN USER (以下の VLAN ユーザを選択することが可能です:)

次の VLAN ユーザのタイプを選択して表示することができます。
　Static:　CLI/Web/SNMP の VLAN を表示します。。
　NAS :　認証 VLAN による VLAN を表示します。
　GVRP : マルチプル LAN 登録プロトコルにる VLAN を表示します。
　VoiceVLAN:音声用 VLAN 、IP フォンなどの音声用 VLAN を表示します。
　MVR :　MVR による VLAN を表示します。
　MSTP :　MSTP により作成された VLAN グループが表示されます。

VLAN ID :
特定の VLAN の ID を指します。

VLAN Membership :
VLAN メンバーの画面では、選択された VLAN ユーザ(Combo Box によって許可されたユーザ)によって設定されたすべての VLAN の現行の VLAN ポートメンバーが表示されます。「ALL VLAN Users」を選択する場合は、VLAN ユーザの情報が表示されます(初期設定)。VLAN メンバーにより、VLAN ID にクラス分けされたフレームは VLAN メンバーポート上で伝送可能です。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、VLAN 項目を手動で更新します。

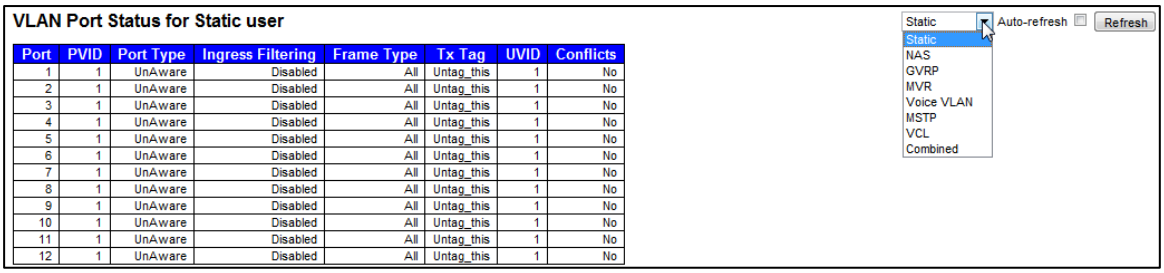
2.11.4 Port Status

ポートステータスは、VLAN のステータスをすべて収集し、「Staic」 、「NAS」、「GVRP」、「 MVP」、「音声用 VLAN」、「MSTP」、「GVRP」、「Combined」の順序で通知を行います。

設定方法

VLAN のポートのステータスの表示方法については、以下の手順に従ってください。
Step 1 [Configration]→[VLAN]→[Port Status」をクリックします。
Step 2. 「Staic」 、「NAS」、「GVRP」、「 MVR」、「Voice-VLAN」、「MSTP」、「VCL」「Combined」のいずれかから選択します。
Step 3. ポートのステータス情報が表示されます。

Figure 2.11.4:　The VLAN Port Status for Static user



Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No
11	1	UnAware	Disabled	All	Untag_this	1	No
12	1	UnAware	Disabled	All	Untag_this	1	No

設定/表示項目

Port :
設定用の論理ポート.

PVID :
ポートの VLAN 識別子が表示されます。設定可能な値は、「1 ～4094」です。初期設定は「1」です。

Port Type :
ポートのタイプが表示されます。
ポートのタイプは、いずれも「Unaware」、「C-port」、「S-port」、「Custom S-port」のいずれかになります。 ポートタイプが「Unaware」の場合は、フレームはすべてポートの VLAN ID ごとに分けられ、C-port の場合はカスタマーポート、(通常の IEEE802.1Q-vlan はこのタイプが表示されます。)S-port の場合はサービスポート、Custom S-port の場合は“Custom TPID”をもつ S-port になります。

Ingress Filtering :
ポートの入力フィルタリングが表示されます。この値によって VLAN 入力処理が異なります。入力フィルタリングが有効な場合、入力ポートがクラス分けされた VLAN のメンバーでない場合は、フレームは破棄されます。

Frame Type :
ポートがすべてのフレーム、またはタグ付きフレームのみを受け取るかが表示されます。この値によって VLAN 入力処理が異なります。 ポートがタグ付きフレームのみを受け取る場合は、タグなしフレームを受信すると破棄します。

Tx Tag :
出力フィルタリングフレームのステータス（タグ付き/タグなし）が表示されます。

UVID :
UVID (タグなし VLAN ID)が表示されます。ポートの UVID によって、出力側のパケットの挙動が決定されます。

Conflicts :
コンフリクト（リソースの重複）の有/無が表示されます。一時的な VLAN ユーザは VLAN メンバー、または VLAN ポートのコンフィグを設定する場合は、以下のコンフリクトが発生する可能性があります。

- 機能上のコンフリクト
- ハードウェア制限によるコンフリクト.
- ユーザモジュール間のコンフリクト

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

2.12 VOICE VLAN

音声用 VLAN は、音声用のトラフィック用に設定された VLAN です。音声用 VLAN に接続された音声装置をもつポートを追加すると、音声データ用の QoS に関する設定を行うことができるため、音声用のトラフィックおよび音声の品質のプライオリティの伝送を行うことが可能になります。

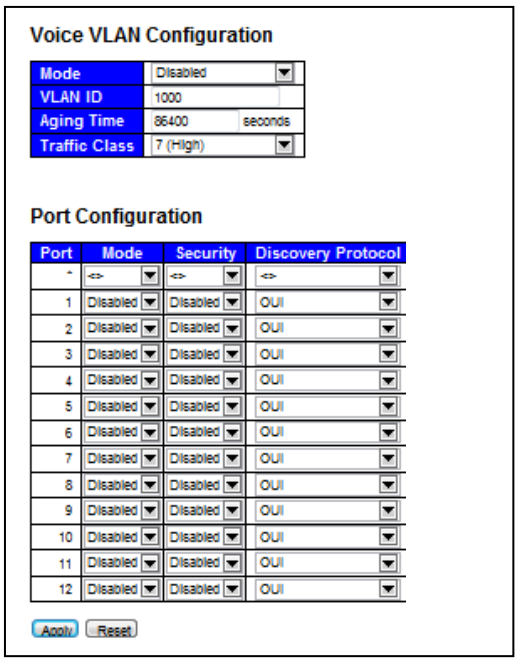
2.12.1 Configuration

音声用の VLAN 機能により、音声用 VLAN 上で音声用のトラフィックの伝送が可能になるため、スイッチは、ネットワークのトラフィックをクラス分けし、優先処理を行うことができます。
VLAN は、音声用とデータ用に 2 つに分けての使用することをお勧めします。スイッチに IP 装置を接続する前に、独自の GUI を介して、IP フォンの音声用 VLAN ID を正しく設定する必要があります。

設定方法

音声用 VLAN を設定するには、以下の手順に従ってください。
Step 1.　[Configration]→[VLAN]→[Configuration]をクリックすると、「The Voice Configration」画面が表示されます。モードを「Enabled」に設定します。
Step 2.　「VLAN ID」、「Aging Time」、「Traffic Class」の値をそれぞれ入力します。
Step 3.「Port Configuration」メニューの「Port Mode」、「Security」、「DiscoveryProtocol」の値をそれぞれ入力します。
Step 4.　<Apply>ボタンをクリックします。

Figure 2.12.1:　The Voice VLAN Configuration



設定/表示項目

Mode :
音声用 VLAN モードを指します。音声用 VLAN を有効にする前に、MSTP 機能を無効にする必要があります。入力フィルタリングのコンフリクトを回避することが可能です。
可能なモードは下記のとおりです
Enabled:音声用 VLAN モードを「有効」にします。
Disabled:音声用 VLAN モードを「無効」にします。

VLAN ID :
音声用 VLAN ID が表示されます。システムの固有の VLAN ID であり、各ポートの PVID とは異なります。値が管理 VID, MVR VID, PVID と同じ場合は、設定にコンフリクトが生じてしまいます。設定可能な範囲は「1」～「4095」です。

Aging Time :
音声用 VLAN のエージングタイムを設定します。
設定可能な範囲は、「10 秒」～「10000000 秒」です。セキュリティモード、または自動検出モードが有効な場合に使用します。それ以外の場合は、ハードウェアのエージングタイムに応じて異なります。実際のエージングタイムは[age_time; 2 * age_time]間隔で設定されます。

Traffic Class :
音声用 VLAN トラフィッククラスを指します。音声用 VLAN 上のトラフィックはすべてこのクラスに適用されます。

Port Mode :
音声用 VLAN ポートモードを指します。
ポートのモードが有効な場合は、音声用 VLAN を有効にする前に MSTP を無効に設定する必要があります。入力フィルタリングによるコンフリクトを回避することができます。

Disabled: 音声用 VLAN を解除します。
Auto: 自動検出モードを有効にします。特定のポートに接続されている VoIP フォンがあるかどうかを検出し、音声用 VLAN メンバーを自動的に設定します。
Forced:音声用 VLAN に手動にて設定します。

Port Security :
音声用 VLAN ポートのセキュリティモードを指します。 この機能が有効な場合は、音声用 VLAN の電話機以外の MAC アドレスは 10 秒以内にブロックされます。
設定可能なポートのモードは、以下のとおりです。
Enabled:音声用 VLAN セキュリティモードを「有効」にします。
Disabled:音声用 VLAN セキュリティモードを「無効」にします。

Port Discovery Protocol :
音声用 VLAN ポートディスカバリプロトコルを指します。自動検出モードがう有効な場合のみ動作します。ディスカバリプロトコルを"LLDP"あるいは"Both"に設定するには、LLDP 機能を有効にする必要があります。ディスカバリプロトコルを"OUI"あるいは "LLDP"に変更すると、自動検出プロセスを再開します。
設定可能なプロトコルは、下記のとおりです。
OUI:　OUI アドレスにより、電話機を検出します。
LLDP: LLDP により電話通信機器 を検出します。
Both:　OUI および LLDP の両方

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

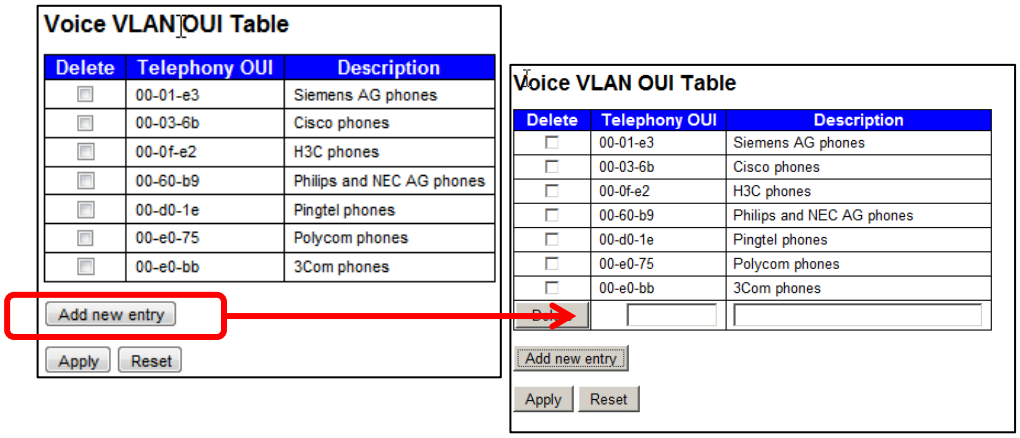
2.12.2 OUI

音声用 VLAN OUI 画面の設定方法について説明します。最大エントリ数は「16」です。
OUI テーブルを修正すると、OUI プロセスの自動検索を再開します。

設定方法

「Voice VLAN OUI Table」を設定するには、以下の手順に従ってください。
Step 1. [Configration]→[VLAN]→[Voice VLAN]→[QUI]をクリックすると、「Voice VLAN QUI Table」画面が表示されます。画面下の<Add new entry>ボタン をクリックするか、「音声用 VLAN OUI table」メニューの"Delete"に☑を入れます。
Step 2. 新しいエントリを追加する場合は、それぞれ「Telephony OUI」、「Description」の項目を入力します。
Step 3.　<Apply>ボタンをクリックします。

Figure 2.12.2:　The voice VLAN OUI Table



設定/表示項目

Delete :
削除したい項目を選択して、 <Apply>ボタンをクックすると削除されます。

Telephony OUI :
「telephony OUI」のアドレスは、IEEE によりベンダーに割り当てられた固有の識別子です。6 文字までに制限され、書式は"xx-xx-xx" (x は 16 進数)になります。

Description :
OUI アドレスの記述。電話通信機器のベンダを示します。設定可能な値は「0～32」です。

Add new entry :
<Add a new entry>を追加すると、新しいエントリが追加されます。 空のエントリが追加されるので,「Telephony OUI」、「Description」をそれぞれ入力します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.11.5 Private VLANs

プライベート VLAN の場合は、アップリンクを共有しダウンリンクグループ同士の通信は許可されていません。プライベート VLAN により、ポートグループ間のセキュリティと、アップリンクのリソースの共有が可能です。

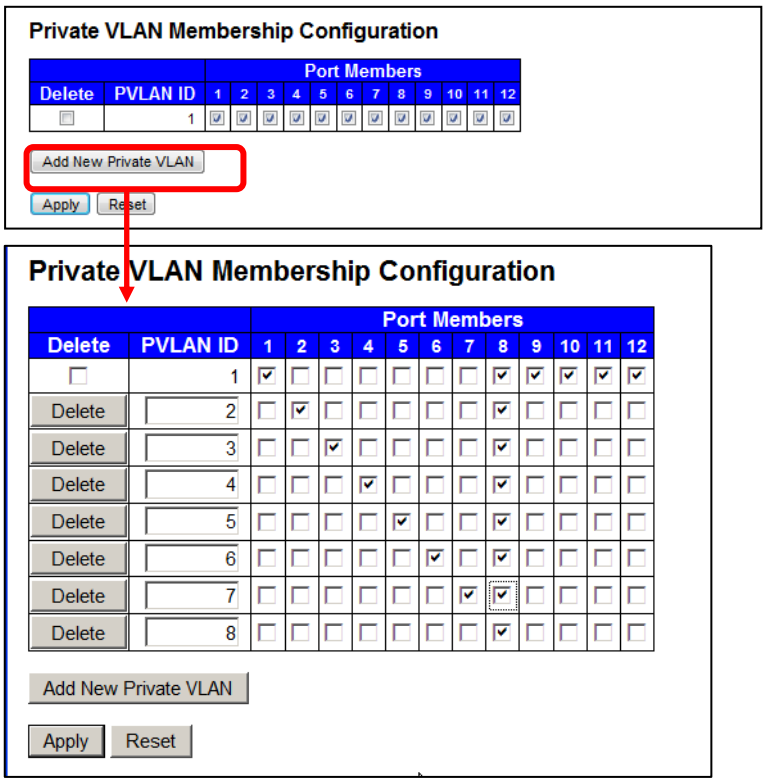
2.11.5.1 Private VLANs Membership

ここでは、プライベート VLAN の追加/削除可能です。
各プライベート VLAN のポートメンバーの追加/削除することができます。各プライベート VLAN の VLAN ID とプライベート VLAN ID は同じ値になります。ポートは、パケット伝送を可能にするために、VLAN およびプライベート VLAN の両方のメンバーとなる必要があります。初期設定では、ポートはすべて VLAN unaware であり、VLAN 1 かつプライベート VLAN1のメンバーに設定されています。VLAN unaware ポートは VLAN メンバーについては1つのみですが、複数のプライベート VLAN のメンバーにも設定可能です。

設定方法

プライベート VLAN を設定するには、以下の手順に従ってください。
Step 1. [Configration]→[Private VLANs]→[Privat VLAN Membership]をクリックすると、「Privat VLAN Membership Configration」画面が表示されます。
Step 2. <Add New Private VLAN>ボタンをクリックします。
「Private VLAN ID」および「Port Members」をそれぞれ入力します。
Step 3. <Apply>ボタンをクリックします。

Figure 2.11.5.1:　The Private VLAN Membership Configuration



設定/表示項目

Delete :
プライベート VLAN を削除するには、ボックスに☑を入れて削除します。エントリは、 <Apply> ボタンをクリックすると削除されます。

Private VLAN ID :
特定のプライベート VLAN ID を指します。
独立ポートの数の VLAN を作成し、ID を設定します。

Port Members :
プライベート VLAN ID ごとに、各ポートのチェックボックスが表示されます。プライベート VLAN にポートを設定するにチェックボックスに☑を入れてください。プライベート VLAN からポートを削除する場合は、ボックスから☑を外してください。初期設定ではポートはすべてメンバーではありません。
個々のポートを独立させたい場合は、各 VLAN に 1 ポートのみ設定します。

Adding a New Private VLAN :
プライベート VLAN を作成します。
個々のポートを独立させた対場合は、必要数の VLAN を作成します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

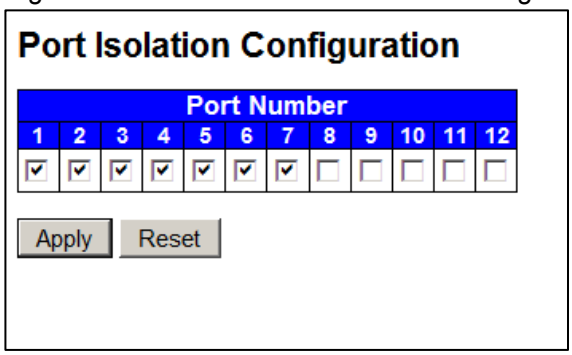
2.11.5.2 Port Isolation

ポートの独立の方法について説明します。
ここでは、プライベート VLAN のポートのポートの隔離を有効/無効にする設定の説明をします。
同じ VLAN およびプライベート VLAN 上の隔離されたポートから VLAN のポートメンバーを切り離すことが可能です。

設定方法

ポート隔離設定を行うには、以下の手順に従ってください。
Step 1. [Configration]→[VLAN]→[Private VLAN]→[Port Isolation]をクリックします。
Step 2. ポート隔離を有効にしたいポートを☑します。
Step 3. <Apply>ボタンをクリックします。

Figure 2.11.5.2:　The Port Isolation Configuration



設定/表示項目

Port Members :
プライベート VLAN の各ポートごとにチェックボックスが表示されます。☑を入れると、ポートの分離が可能になります。☑を入れないと、ポートの分離が無効になります。
初期設定では、すべてのポートの分離は「無効」となります。
なお、共通のアップリンクポートには、☑を入れないでください。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.11.6 MAC-based VLAN

MAC ベース VLAN は、フレームのソース MAC アドレスに応じてタグなしフレームを伝送する VLAN を決定します。
ポート A およびポート B が同一の VLAN に設定されている場合は、端末装置がポート B を介してネットワークにアクセスした後、ポート A（セキュリティ問題を問題を引き起こす）を介してネットワークにアクセスした際と同じリソースにアクセスします。ユーザアクセスを提供し、データセキュリティを確保するために、MAC ベース VLAN テクノロジが進められています。
MAC ベース VLAN は MAC アドレスによって VLAN メンバをグループ化します。MAC ベース VLAN を使って、デバイスはソース MAC アドレスに応じて、タグなしフレームに VLAN タグを追加します。MAC ベース VLAN は、端末装置向けに柔軟なネットワークアクセスを行うために、802.1X などのセキュリティ技術に応じて使用されます。

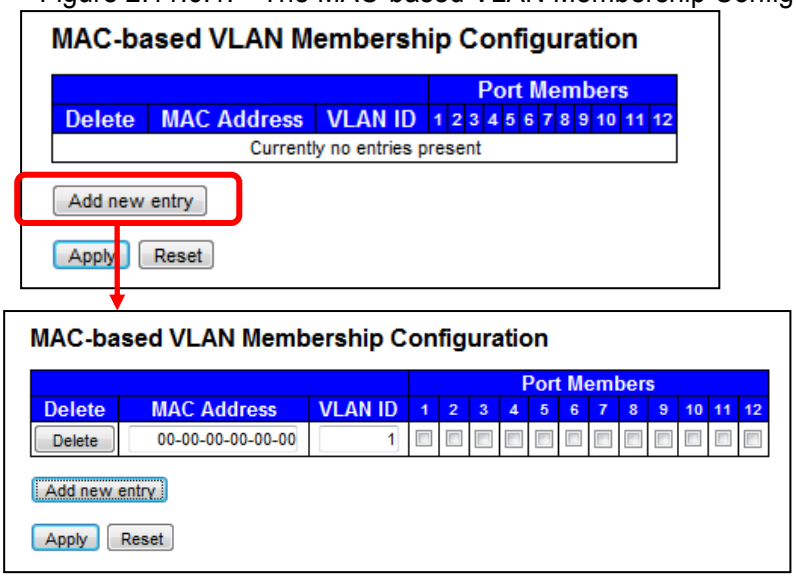
2.11.6.1 Configuration

MAC ベース VLAN を設定します。この画面では、 MAC ベース VLAN のエントリの追加/削除を行い、各ポートにエントリを割り当てます。ここでは、スタティックエントリのみ表示されます。

設定方法

MAC アドレスベース VLAN を設定するには、以下の手順に従ってください。
Step 1. [Configration]→[VLAN]→[MAC address-based　VLAN configuration]、[Add new entry]をクリックします。
Step 2.　MAC アドレスおよび VLAN ID を入力します。
Step 3. <Apply>ボタンをクリックします。

Figure 2.11.6.1:　The MAC-based VLAN Membership Configuration



設定/表示項目

Delete :
MAC ベース VLAN のエントリを削除するには、<Delete>ボタンをクリック後、 <Apply>ボタンをクリックします。スタック内の選択されたスイッチのエントリが削除されます。

MAC Address :
MAC アドレスを設定します。

VLAN ID :
VLAN ID を設定します。

Port Members :
MAC ベース VLAN ごとに各ポートのチェックボックスが表示されます。 MAC ベース VLAN にポートを設定するには、ボックスに☑を入れてください。MAC ベース VLAN からポートを削除するには、ボックスから☑を外してください。初期設定では、ポートのメンバーは設定されていません。

Add New Entry
<add a new entry>ボタンをクリックすると、新しい MAC ベース VLAN のエントリが表示されます。空白の行がテーブルに追加され、MAC ベース VLAN のエントリが必要に応じて設定可能です。ユニキャスト MAC アドレスを MAC ベース VLAN のエントリ用に設定します。ブロードキャストまたはマルチキャスト MAC アドレスは使用できません。設定可能な VLAN ID の値は「1～4094」です。
<Save>ボタンをクリックすると、選択したスタックスイッチの MAC ベース VLAN のエントリが有効になります。 <Apply>ボタンをクリックすると、どのスタックにもポートメンバーを持たない MAC ベース VLAN は削除されます。<Reset>ボタンをクリックすると、MAC ベース VLAN の追加が取り消されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.11.6.2 Status

ここでは、MAC ベース VLAN ユーザにより設定された各種 MAC ベース VLAN について表示します。現在、サポートしているユーザタイプは、以下のとおりです。

NAS :ポートベースの認証を行います。ここでは、サプリカント、認証子、認証サーバ間の通信が含まれます。
Staic:登録した MAC アドレスにより設定されたポートメンバを表示します。

設定方法

MAC ベース VLAN を設定を表示するには、以下の手順に従ってください。
Step 1. [Configraiton]→[VLAN]→[MAC-based VLAN]→[Status」をクリックします。
Step 2. 「Staic NAS Combined」の値を入力します。
Step 3. MAC ベース情報が表示されます。

Figure 2.11.6.2:　The MAC-based VLAN Membership Status for User Static

設定/表示項目

MAC Address :
MAC アドレスが表示されます。

VLAN ID :
VLAN ID が表示されます。

Port Members :
MAC ベース VLAN のポートメンバーが表示されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、MAC ベース VLAN のメンバー情報が更新されます。

2.11.7 Protocol -based VLAN

プロトコルベース VLAN について説明します。プロトコルには、イーサネット LLC SNAP プロトコルが含まれます。

LLC
Logical Link Control (LLC)データ通信プロトコルレイヤは、データリンク層（レイヤ2）の上位サブレイヤです。いくつかのネットワークプロトコル(IP, IPX, Decnet and Appletalk)がマルチポイントのネットワークで共存したり、同じネットワークメディア上でデータの伝送を行うと、フローコントロールや ARQ(自動再送要求)のエラー管理システムを提供することも可能です。

SNAP
SNAP（サブネットワークアクセスプロトコル)は、 IEEE 802.2 LLC を用いたネットワーク、8 ビットの 802.2 の SAP(サービスアクセスポイント)によって識別可能な多くのプロトコル上で多重化するシステムです。SNAP は、イーサネットタイプのフィールドの値によってプロトコルを識別し、ベンダ固有のプロトコル識別子のスペースもサポートしています。IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 およびそれ以外の IEEE 802 物理ネットワーク層、 802.2 LLC 向けの FDDI などの IEEE 802 以外の物理ネットワーク層も同様に併用します。

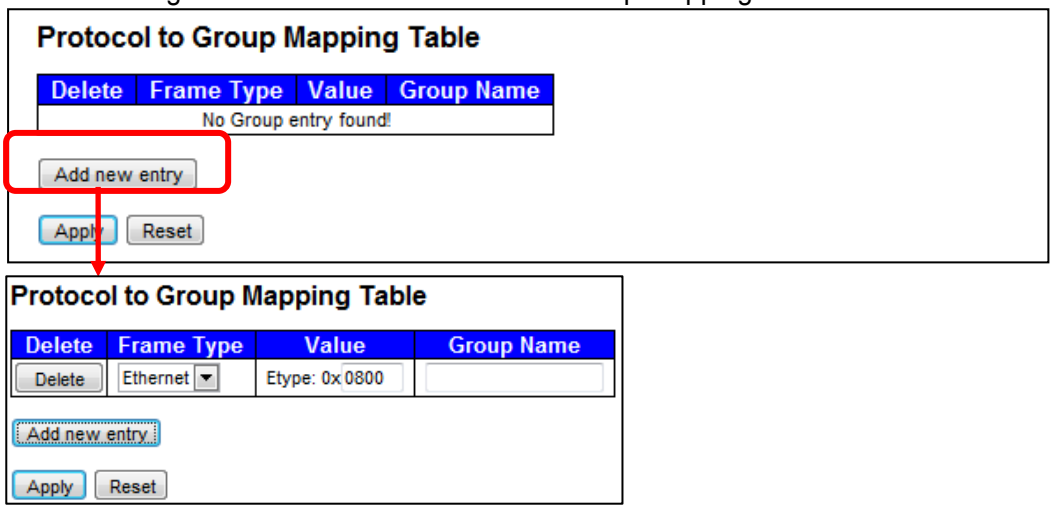
2.11.7.1 Protocol to Group

グループ名(グループごとに固有)のマッピングエントリに新規のプロトコルを追加したり、選択したスタックのスイッチのマッピングされているエントリを削除することが可能です。

設定方法

プロトコルベース VLAN を設定するには、以下の手順に従ってください。
Step 1.　[Configraiton]→[VLAN]→[protocol- based VLAN]→[Protocol to Group]をクリックすると、「Protocol to Group Mapping Table」画面が表示されます。
Step 2.　<Add new entry>ボタンをクリックすると、新しい画面が表示されるのでそれぞれフレームタイプを「Ethernet」、「LLC」、「SNAP」から選択して、グループ名を入力します。
Step 3.　<Apply>ボタンをクリックします。

Figure 3.12.7.1:　The Protocol to Group Mapping Table



設定/表示項目

Delete :
エントリを削除したい場合は、ボックスに☑を入れてください。
<Apply>ボタンをクリックすると、エントリが削除されます。

Frame Type :
フレームタイプは、以下の値のいずれかになります。
1. Ethernet
2. LLC
3. SNAP

【注記】:
フレームのタイプを変更すると、次のメニューの値は、選択した新しいフレームタイプによって異なります。

Value :
このメニューで入力可能な有効な値は、フレームタイプで選択した値によってよって異なります。

3つの各フレームタイプに応じて、以下の内容に注意してください。
1. Ethernet:設定可能な値は、「0x0600-0xffff」です。
2. LLC: この場合の有効な値は、2 つの値で構成されています。
 a. DSAP: 1-byte long string (0x00-0xff)
 b. SSAP: 1-byte long string (0x00-0xff)

3. SNAP: この場合の有効な値は、2 つの値で構成されています。
a. OUI: OUI (Organizationally Unique Identifier)は、xx-xx-xx の書式の値、文字列の対(xx)は、16 進数の値、設定可能な値は「0x00～0xff」です。
b. PID: OUI が16進数の 000000 の場合、プロトコル ID は SNAP の上位で動作しているプロトコルのイーサネットタイプ(EtherType)の値です。OUI は、特定の組織の OUI であり、プロトコル ID は、SNAP の上位で動作しているプロトコルに対して組織によって割り当てられた値です。つまり、OUI の値が”00-00-00”の場合は、PID の値は etype (0x0600-0xffff)となり、OUI の値が”00-00-00”以外の場合は、PID の有効値が”0x0000”から”0xffff”までの任意の値になります。

Group Name :
有効なグループ名は、どのエントリも英文字(a-z、あるいは A-Z)と整数 (0-9)を組み合わせた 16 文字以内の固有の値となります。

【注記】:
特殊文字とアンダースコア(_)は使用できません。

Add New Entry
マッピングテーブルの[add a new entry]をクリックします。必要に応じて、それぞれの値を入力してください。 [Reset]ボタンをクリックすると、新しく追加したエントリが取り消されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

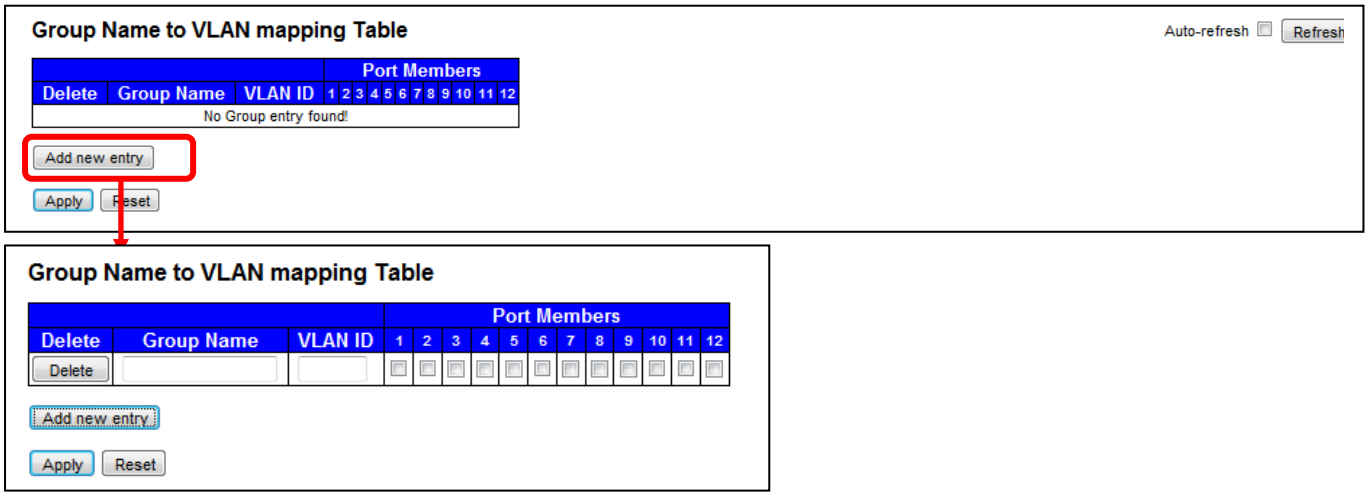
2.11.7.2 Group to VLAN

ここでは、指定のスタックスイッチ用の VLAN にすでに設定したグループ名をマッピングする方法について説明します。

設定方法

設定した VLAN マッピングテーブルにグループ名を表示するには、以下の手順に従ってください。
Step 1.　[Configration]→[VLAN]→[Group Name VLAN configuration]をクリックして、<Add new entry>ボタンをクリックします。
Step 2.　グループ名と VLAN ID を入力します。
Step 3　<Apply>ボタンをクリックします。

Figure 2.11.7.2:　The Group Name of VLAN Mapping Table



設定/表示項目

Delete :
VLAN マップエントリのグループ名を削除します。 <Apply>ボタンをクリックすると反映されます。

Group Name :
有効なグループ名は、どのエントリも英文字(a-z、あるいは A-Z)と整数 (0-9)を組み合わせた 16 文字以内の固有の値となります。VLAN にマッピングしたいグループ名はグループマッピングテーブルにプロトコルで表示する必要があり、画面内の他の既存のマッピングエントリを再度使用することはできません。

VLAN ID :
マッピングを行うグループ名の ID が表示されます。設定可能な VLAN ID は、「1～4095」です。

Port Members :
「Group Name to VLAN ID mapping」の表に、各ポートのチェックボックスが表示されます。ポートをマッピングに設定するには、ポートに☑を入れてください。ポートをマッピングから削除するには、ボックスが選択されていないことを確認してください。
初期設定では、メンバー以外のポートはすべて選択されていません。

Adding a New Group to VLAN mapping entry :
マッピングテーブルの[add a new entry]をクリックします。空のエントリが追加されるので、必要に応じてそれぞれの値を入力してください。VLAN ID の有効な値は「1～4095」です。
<Reset>ボタンをクリックすると、新しい追加項目が取り消されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、プロトコルグループのマッピング情報が更新されます。

2.13 GARP

GARP(Generic Attribute Registration Protocol) は、ブリッジ LAN の装置（例えば、エンドステーション、スイッチ）は、VLAN 識別子などの属性値を登録/解除することができます。ブリッジ LAN の装置に属性を通知し、GARP は属性値の登録/解除のアーキテクチャー、動作ルール、ステートマシーンおよび変数を定義します。
スイッチ、またはエンドステーションへの GARP の参加は、各ポートまたはスイッチに関連のある GARP アプリケーション、GID（GARP 情報宣言）から構成されます。ブリッジ内の同じアプリケーション用の GARP パーティシパント間の情報の伝播は、GIP(GARP Information Propagation)によって実行されます。プロトコルの変更がグループ MAC アドレス、関連のある GARP アプリケーションに定義されている PDU 形式を使って、LLC タイプ 1 サービスにより GARP パーティシパント間でプロトコルの変換が行なわれます。

2.13.1 Configuration

スイッチのポート用向けの GARP の基本設定を行うことができます。現在選択されているスタックユニットに関する設定情報が画面ヘッダに表示されます。

設定方法

「GARP Port Configuration」を設定するには、以下の手順に従ってください。
Step 1.　[Configration]→[GARP]をクリックします。
Step 2.「GARP Configuration」の値を入力します。
Step 3.　<Apply>ボタンをクリックします。

Figure 2.13.1:　The GARP Port Configuration

GARP Port Configuration　Auto-refresh ☐ Refresh

Port	Timer Values			Application	Attribute Type	GARP Applicant
	Join Timer	Leave Timer	Leave All Timer			
1	200	600	10000	GVRP	VLAN	normal-participant
2	200	600	10000	GVRP	VLAN	normal-participant
3	200	600	10000	GVRP	VLAN	normal-participant
4	200	600	10000	GVRP	VLAN	normal-participant
5	200	600	10000	GVRP	VLAN	normal-participant
6	200	600	10000	GVRP	VLAN	normal-participant
7	200	600	10000	GVRP	VLAN	normal-participant
8	200	600	10000	GVRP	VLAN	normal-participant
9	200	600	10000	GVRP	VLAN	normal-participant
10	200	600	10000	GVRP	VLAN	normal-participant
11	200	600	10000	GVRP	VLAN	normal-participant
12	200	600	10000	GVRP	VLAN	normal-participant

Apply　Reset

設定/表示項目

Port :
GARP 設定可能なポートのリストが表示されます。
ポートベースで設定可能なタイプは以下のとおりです。
Timer Values
Applicantion
Attribute Type
GARP Applicant

Timer Values :
「Join timer」、「Leave Timer」および「Leave All Timers」の値をそれぞれ設定します。単位は、マイクロセカンドです。

Join Timer　:
初期設定値は「200ms」です。

Leave Timer :
設定可能範囲は「600-1000ms」です。
初期設定値は「600ms」です。

Leave All Timer :
初期設定値は「10000ms」です。

Application :
現在サポートせれているアプリケーションは「GVRP」です。

Attribute Type :
現在サポートされている属性のタイプは、「VLAN」です。

GARP Applicant:
ローカルで特定のポートのアプリカントのステートマシーンの動作を設定するために使用します。
特定ポートの GARP のステートマシンの挙動をローカルで設定します。

normal-participant:
GAR プロトコル変換時にアプリカントのステートマシーンが正常に動作します。アプリカントのステートマシンは GARP 変換時に正常に動作します。

non-participant:
アプリカントのステートマシーンはプロトコル動作に参加しません。アプリカントのステートマシンはプロトコルのオペレーションを行いません。
初期設定では、「normal participant」です。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

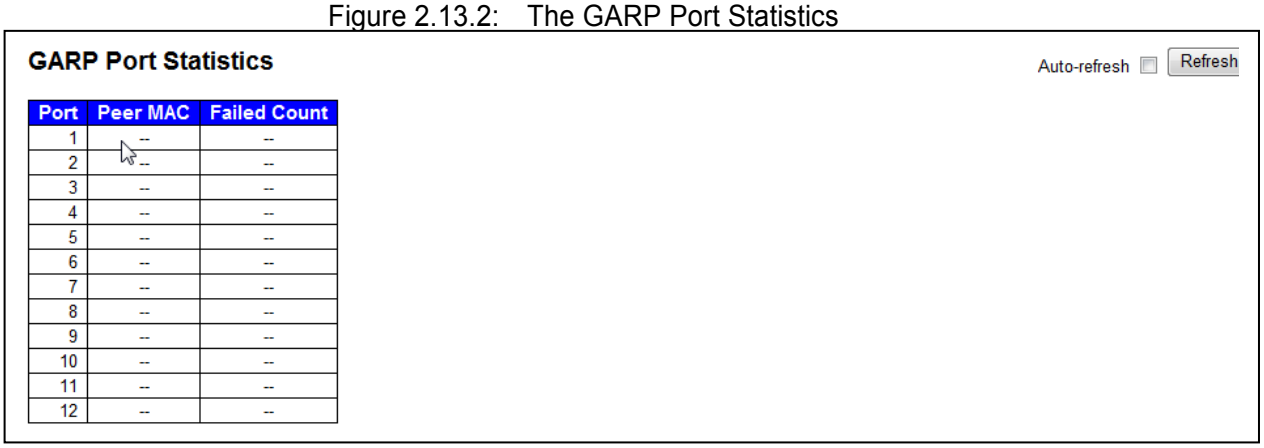
2.13.2 Statistics

スイッチポートの GARP のポートの統計情報が表示されます。現在選択されているスタックユニットに関連のあるポートの統計情報は、画面のヘッダに表示されます。

設定方法

GARP ポートの統計情報を表示するには、以下の手順に従ってください。
Step 1.　[Configration]→[GARP]→[Statistics]をクリックします。
Step 2.　GARPカウンタ情報を表示したいポートを選択します。
Step 3.　<Refresh>ボタンをクリックすると、GARP統計情報が更新されます。

Figure 2.13.2:　The GARP Port Statistics



Port	Peer MAC	Failed Count
1	--	--
2	--	--
3	--	--
4	--	--
5	--	--
6	--	--
7	--	--
8	--	--
9	--	--
10	--	--
11	--	--
12	--	--

設定/表示項目

Port :
各ポートの GARP 統計情報がリストに表示されます。

Peer MAC :
Peer MAC は、GARP フレームを受信した近隣スイッチの MAC アドレスです。

Failed Count :
失敗した回数が表示されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

2.14 GVRP

GVRP は、GARP（Generic Attribute Registration Protocol）をベースとしており、主に VLAN のグループメンバの情報を動的に保持するために使用します。GVRP は、GARP アプリケーションを介して、VLAN 登録サービスを提供する機能を備えています。
これにより、GID（GARP Information Declaration）を使って、スイッチ/ステーション間の通信を行うために、属性データーベースおよび GARP 情報(GIP)と関連のあるポートを保持します。GID 情報および GIP を介して、GVRP ステートマシーンは VLAN ごとに動的 VLAN 登録エントリの情報を保持し、情報データベース、現在アクティブなメンバーに関連のある VLAN を設定かつ更新を行うために GVRP-aware デバイスにそれらの情報を通知します。

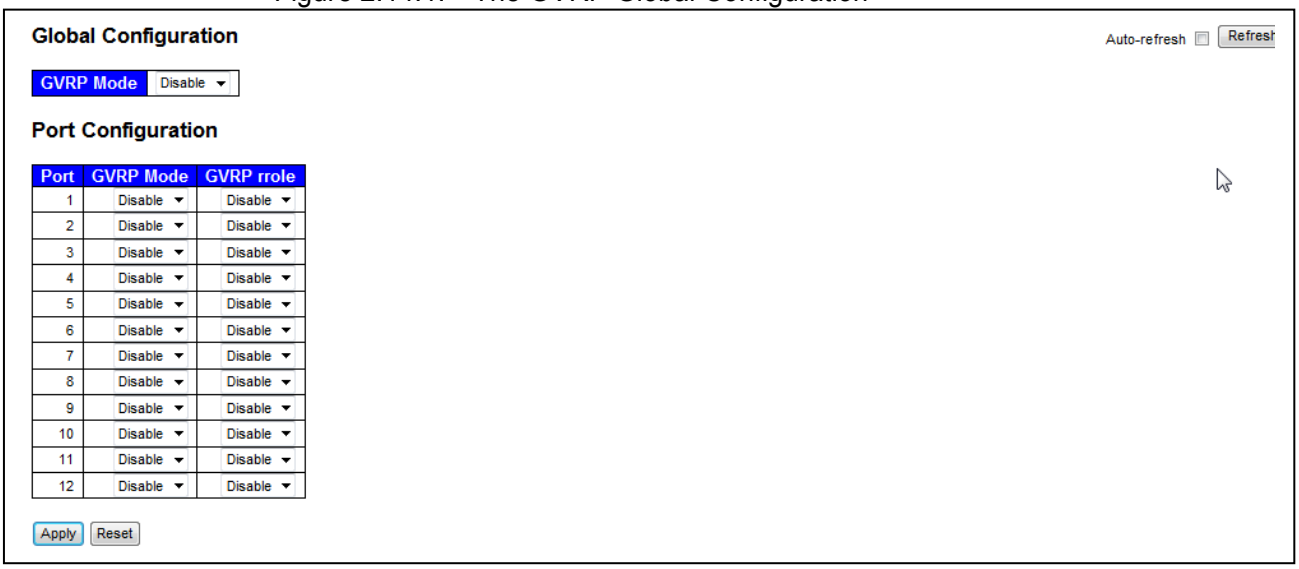
2.14.1 Configuration

ポートに関する GVRP の基本設定を行うことが可能です。現在選択されているスタックユニットに関する設定情報が画面ヘッダに表示されます。

設定方法

GVRP ポートを設定するには、以下の手順に従ってください。
Step 1.　[GVRP configure]をクリックします。
Step 2.　「Port Configuration」の値をそれぞれ入力します。
Step 3.　<Apply>ボタンをクリックします。

Figure 2.14.1:　The GVRP Global Configuration



設定/表示項目

GVRP Mode :
GVRP モードはグローバル設定です。このモードを「Enable」に設定すると GVRP が有効になり、「Disable」に設定すると無効になります。スタック時に、この設定コマンドによりスタック内のスレーブすべてにメッセージを送信します。
初期設定 GVRP モードは「Disable」です。

Port :
各ポートの GVRP に設定可能なポートのリストが表示されます。ポートベースで設定可能なモードは以下のとおりです。
1. GVRP Mode
特定のポートの GVRP モードを有効/無効に設定します。
Disable: ポートの GVRP モードを「無効」にします。
Enable: ポートの GVRP モードを「有効」にします。
初期設定値は「disable」です。
2. GVRP rrole
インタフェース上の制限された役割を設定します。
Disable: ポートの GVRP を「無効」にします。
Enable: ポートの GVRP を「有効」にします。
初期設定値は「Disable.」です。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

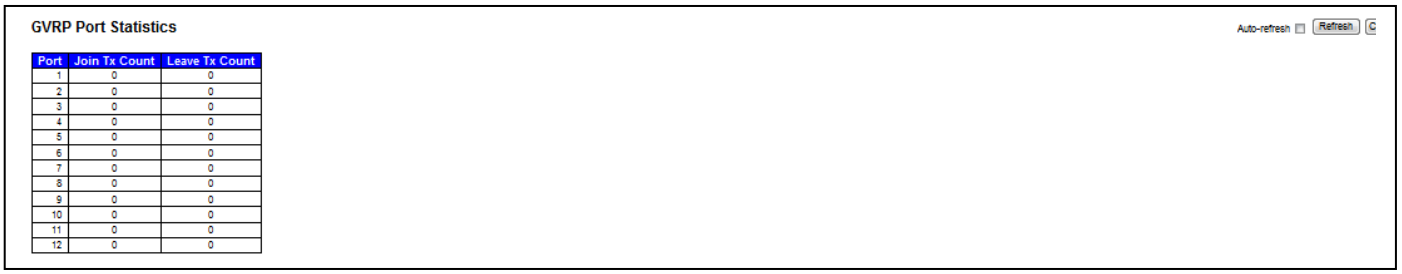
2.14.2 Statistics

スイッチのポートの GVRP ポートの基本統計情報が表示されます。現在選択されているスタックユニットに関する統計情報が画面のヘッダに表示されます。

設定方法

GVRP ポートの統計情報 を表示するには、以下の手順に従ってください。
Step 1. [GVRP statistics]をクリックします。
Step 2. GVRP カウンタ情報を表示させたいポートを選択します。
Step 3. <Refresh>ボタンをクリックすると、GVRP 統計情報が更新されます。

Figure 2.14.2:　The GVRP Port Statistics



Port	Join Tx Count	Leave Tx Count
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

Port :
表示したいポートのカウンタと統計情報のポートリストが表示されます。

Join Tx Count :
「Join tx Count」が表示されます。

Leave Tx Count :
「Leave Tx Count」が表示されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

2.15 QoS

本機は、strict あるいは weighted fair キューのスケジュールをもつポートごとに 4 つの QoS キューをサポートしています。IEEE 802.1p、Ethertype、VID、 IPv4/IPv6 DSCP および UDP/TCP ポートに応じて、プログラム可能な拡張 Qos 分類の QCL（Qos コントロールリスト）をサポートしています。
QoS クラスへの受信フレームの分類する際に非常に柔軟性が高いです。
Qos 分類は、IPv4 および IPv6 DSCP、IPv4 TCP/UDP ポート番号、およびタグ付きフレームのユーザのプライオリティなどのレイヤ 4 までの情報を検索します。フレームに割り当てられた QoS クラスはデバイスを介して、特定の QoS クラスに設定された内容に応じて、キューイング、スケジュール化、フレームへのコンジェスチョン制御保証を行います。スイッチは、ジャンボフレームなどのトラフィックに応じて QoS クラスのパフォーマンスを提供する拡張メモリ制御システムをサポートします。
super priority queue は専用メモリを持ち、プライオリティが非常に高いキューです。
QoS クラスキューがすべて輻湊の状態でも、ingress super priority キューにより、トラフィックは CPU への伝送用に受信かつキュー状態の CPU トラフィックとして認識されます。

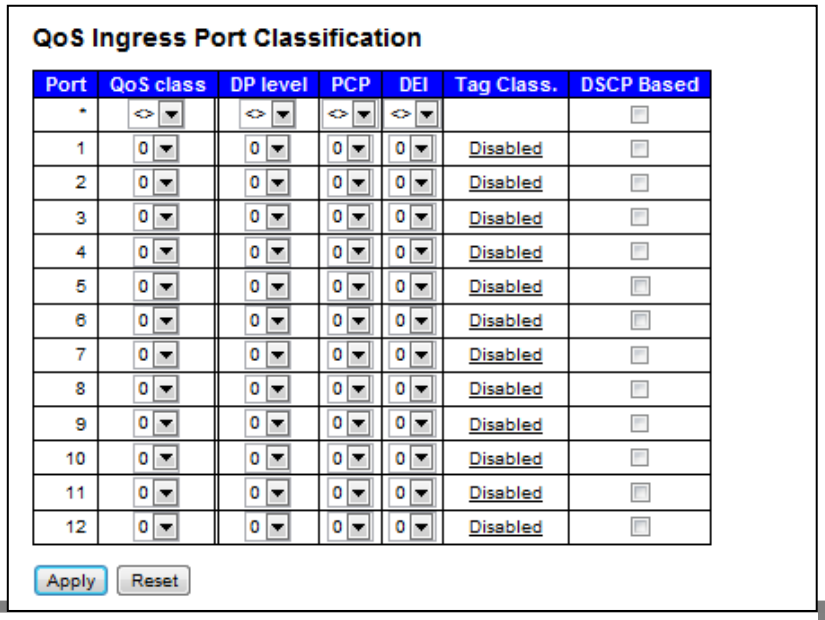
2.15.1 Port Classification

ポートの QoS 入力クラス分けに関する基本設定を行うことができます。スタックに関する設定情報が画面ヘッダに表示されます。

設定方法

QoS ポートクラス分けを設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→[Port Classification]をクリックします。
Step 2. 「QoS class」、「DP Level」、PCP および DEI の値をそれぞれ設定します。
Step 3. <Apply>ボタンをクリックして、値を保存します。
Step 4. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.15.1:　The QoS Configuration



設定/表示項目

Port :
設定対象のポート

QoS class :
初期設定の QoS クラスを定義します。フレームの QoS クラスはその他の設定ではクラス分けすることはできません。QoS クラス、キュー、プライオリティ間で 1 対1でマッピングを行います。QoS クラスのプライオリティが「0」の場合が一番低くなります。

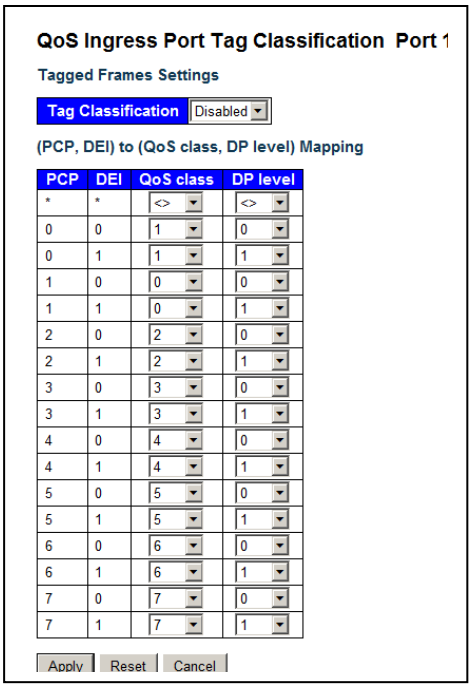
DP level :
初期設定の DP レベルを制御します。

PCP :
タグなしフレームの初期設定の PCP を制御します。

DEI :
タグなしフレームの初期設定の DEI を設定します。

Tag Class. :
タグ付きフレームのクラス分けモードが表示されます。
Disabled: タグ付きフレームの初期設定の QoS クラスおよび DP レベルを使用しません。
Enabled: タグ付きフレームのマッピングされた PCP および DEI の値を QoS クラスにマッピングします。

クリックすると以下の画面が表示されます。



PCP	DEI	QoS class	DP level
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

設定/表示項目

Tag Classification
タグの情報でクラス分けをする(Enable)/しない（Disable）を選択します。

PCP:
タグフレームの PCP の値(0～7)

DEI
タグフレームの DEI の値(0,1)

QoS Class
PCP と DEI により QoS クラスを選択します(0～7)。

DP Level
DP レベルを選択します(0,1)。
設定後<Apply>をクリックします。

DSCP Based :
DSCP ベース QoS 入力ポートのクラス分けを「有効」にします。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

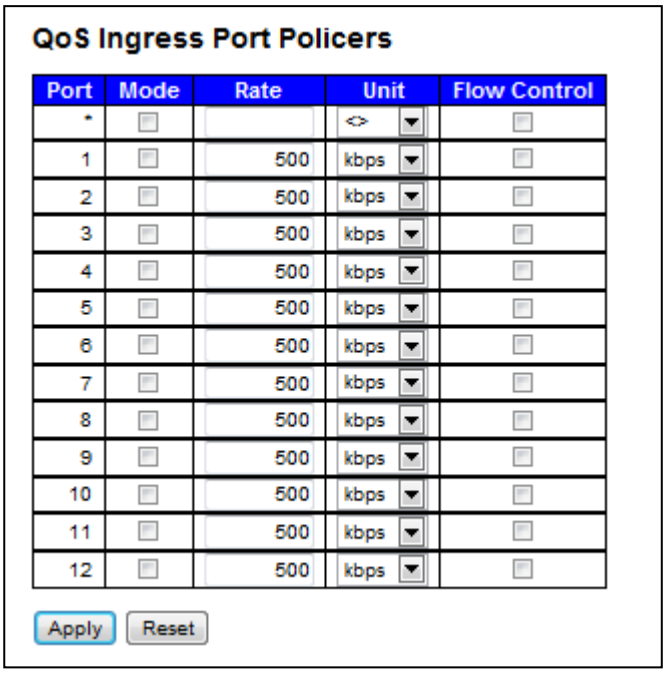
2.15.2 Port Policing

ここでは、QoS 入力ポートのスイッチのポートのポリシーの概要について説明します。ポートポリシングはトラフィックフローを制限したり、特定レートを超えたフレームを制御するのに便利です。ポリシングは、音声およびビデオは常にトラフィックの高速レートが必要なため、主にデータフローやビデオフローに便利です。

設定方法

QoS Port Schedulers を表示するには、以下の手順に従ってください。
Step1.　Configuration]→[QoS]→[Port Policing]をクリックします。
Step2.　指定ポートを選択して、「QoS Ingress Port Policers」を有効にしたいポートに☑を入れて、制限速度を入力します。
Step3.　制限速度の単位を「kbps」、「Mbps」、「fps」および「kfps」から選択します。<Save>ボタンをクリックして、設定を保存します。

Figure 2.15.2:　The QoS Ingress Port Policers Configuration



QoS Ingress Port Policers

Port	Mode	Rate	Unit	Flow Control
*			<>	
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	

Apply　Reset

設定/表示項目

Port :
スケジューラ設定用のポート番号

Enabled :
「QoS Ingress Port Policers」機能を「有効」にしたいポートを選んで、☑を入れてください。
Rate :
ポートの通信速度の制限を設定します。初期設定は「500」です。

Unit :

単位を「kbps」、「Mbps」、「fps」および「kfps」から選択します。初期設定は「kbps」です。

Flow Control:
フローコントロールの機能を「有効」にしたいポートを選んで、☑を入れてください。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

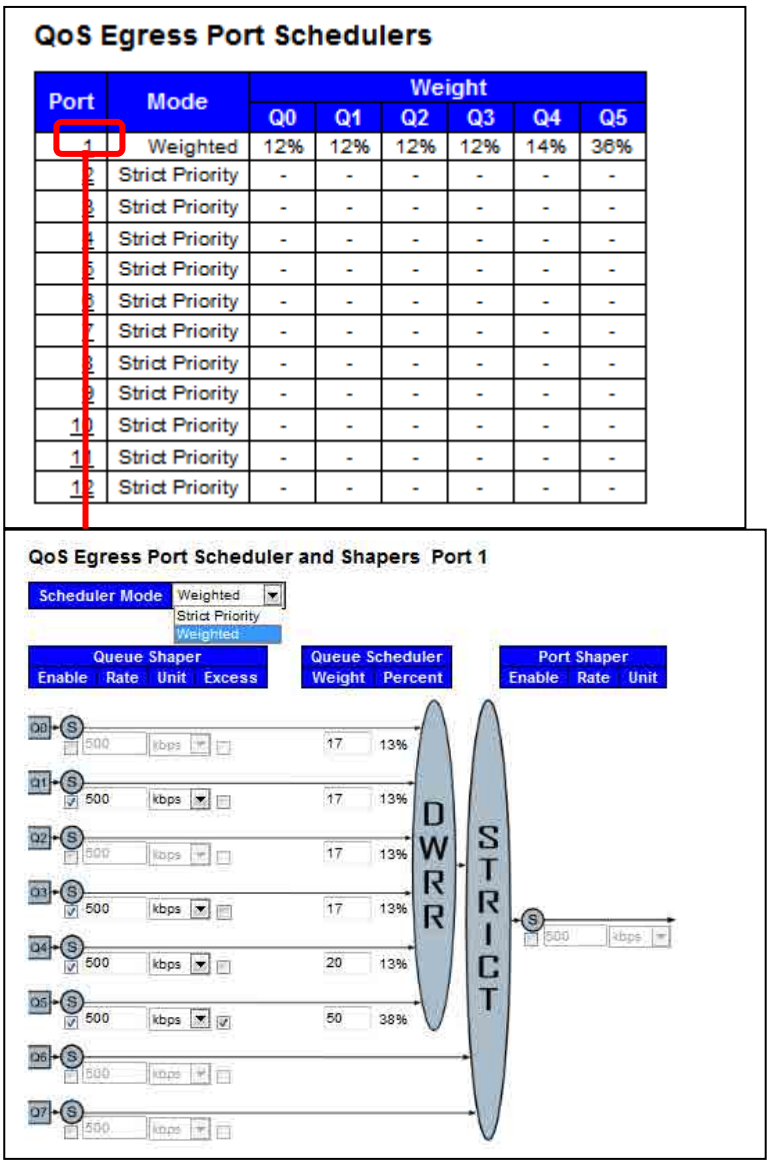
2.15.3 Port Schedulers

ポートの「QoS Egress Port Schedulers」の概要について説明します。現在選択されているスタックのポートが画面ヘッダに表示されます。

設定方法

QoS Port Schedulers を設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS, Port Schedulers]をクリックします。
Step 2.「QoS Egress Port Schedulers」画面が表示されます。

Figure 2.15.3:　The QoS Egress Port Schedules



設定/表示項目

Port :
スケジューラ設定用のポート番号

Mode :
このモードのスケジュールモードを設定します。

Weight　:
キューおよびポートの weight が表示されます。

Scheduler Mode :
スケジューラモードが"Strict Priority"あるいは"Weighted"を設定します。

Queue Shaper Enable :
ポートのキューシェーピングがこのキューに対して有効かどうかを定義します。
「有効」にしたいポートを選んで、☑を入れてください。

Queue Shaper Rate :
キューのシェイパーのレートを定義します。初期設定は、「500kbps」です。この値は単位が"kbps"の場合は「100」～「1000000」、単位が" Mbps "の場合は「1」～「1000」に制限されます。

Queue Shaper Unit :
キューシェイパーレートの単位は"kbps"、あるいは"Mbps"のいずれを設定可能です。初期設定は、「kbps」です。

Queue Shaper Excess :
キューが超過帯域幅を使用可能かどうかを定義します。

Queue Scheduler Weight :
このキューのウェイトを制御します。初期設定は「17」です。この値は「1」～「100」に制限されます。"Scheduler Mode"が「Weighted」に設定されている場合のみ表示されます。

Queue Scheduler Percent :
このキューのウェイトをパーセンテージで表示します。“Scheduler Mode”が「Weighted」に設定されている場合のみ表示されます。

Port Shaper Enable :
ポートシェイパーが有効かどうかを定義します。

Port Shaper Rate :
キューのシェイパーのレートを定義します。初期設定は、「500kbps」です。この値は単位が"kbps"の場合は「100」～「1000000」、単位が" Mbps"の場合は「1」～「1000」に制限されます。

Port Shaper Unit :

ポートシェーバーの測定単位を"kbps" あるいは "Mbps"で定義します。初期設定は "kbps"です。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

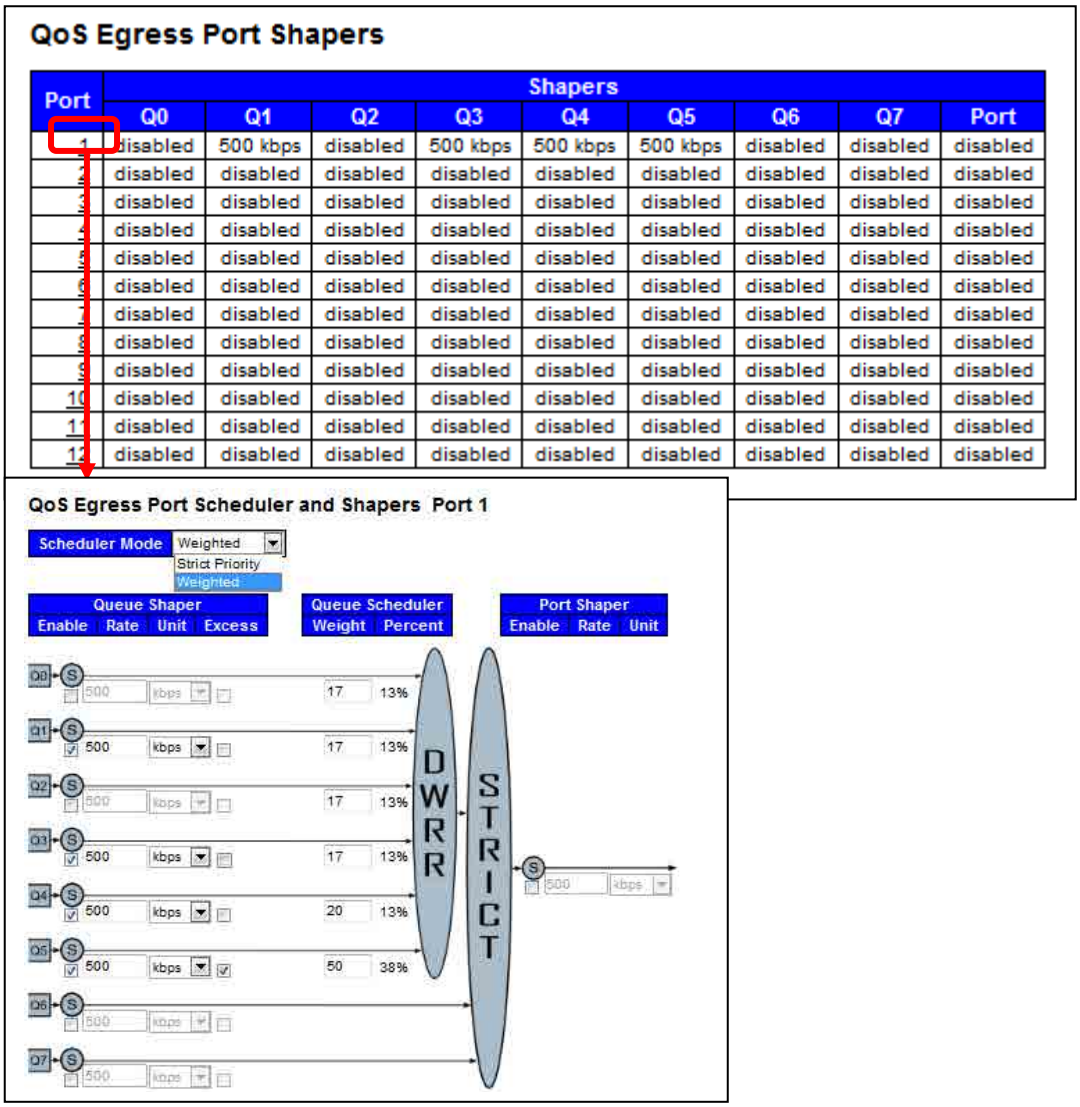
2.15.4 Port Shaping

ポートの QoS Egress Port Shaping の概要について説明します。現在選択されているスタックのポートの詳細については、画面ヘッダに表示されます。

設定方法

QoS Port Shapers を設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→[Port Shapers]をクリックします。
Step 2.「QoS Egress Port Shapers」が表示されます。

Figure 2.15.4:　The QoS Egress Port Shapers



設定/表示項目

Port :
シェイパー設定用のポート番号

Shapers　:
実際のキューシェイパーレート、例えば、「Disabled」 あるいは実際のシェイパーレート（"800 Mbps"）が表示されます。

Shapers (Port) :
「Disabled」または実際のシェイパーレート"800 Mbps"）が表示されます。Scheduler Mode : スケジューラモードが"Strict Priority" 、あるいは"Weighted"のいずれかを選択します。

Queue Shaper Enable :
ポートのキューシェーピングがこのキューに対して有効かどうかを定義します。
「有効」にしたいポートを選んで、☑を入れてください。

Queue Shaper Rate :
キューのシェイパーのレートを定義します。初期設定は、「500kbps」です。この値は単位が "kbps"の場合は「100」～「1000000」、単位が" Mbps "の場合は「1」～「1000」に制限されます。

Queue Shaper Unit :
キューシェイパーレートの単位は"kbps"、あるいは"Mbps"のいずれを設定可能です。初期設定は、「kbps」です。

Queue Shaper Excess :
キューが過度の帯域を使用可能かどうかを設定します。

Queue Scheduler Weight :
このキューの weight を制御します。初期設定は「17」です。この値は、「1-100」に制限されます。
“Scheduler Mode”が「Weighted」に設定されている場合のみ表示されます。

Queue Scheduler Percent :
このキューの weight をパーセンテージで表示します。“Scheduler Mode”が「Weighted」に設定されている場合のみ表示されます。

Port Shaper Enable :
ポートシェイパーが有効かどうかを定義します。

Port Shaper Rate :
キューのシェイパーのレートを定義します。初期設定は、「500kbps」です。この値は単位が "kbps"の場合は「100」～「1000000」、単位が" Mbps "の場合は「1」～「1000」に制限されます。

Port Shaper Unit :

ポートシェイパーレートの単位を"kbps" または "Mbps"から選択します。初期設定は、「kbps」です。
Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

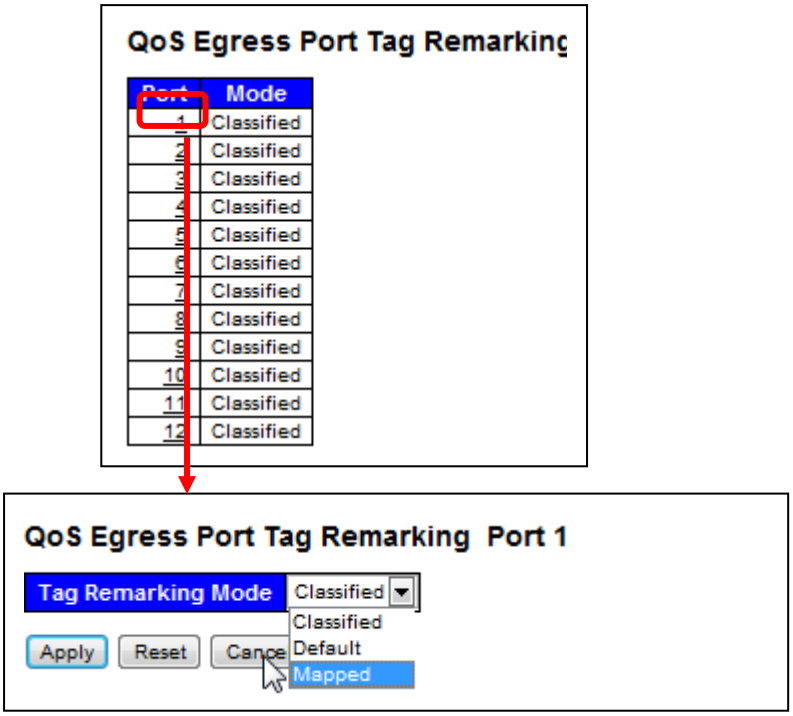
2.15.4 Port Tag Remarking

スイッチのポートの QoS Egress Port Tag Remarking の概要について説明します。

設定方法

QoS Port Tag Remarking を設定するには、以下の手順に従ってください。
Step 1.[Configuration]→[QoS]→[Port Tag Remarking]をクリックします。

Figure 2.15.5:　The Port Tag Remarking



設定/表示項目

Port :
設定用の論理ポート。タグを設定するポート番号をクリックします。

Mode
ポートのタグが表示されます。
Classified: クラス分けした PCP/DEI 値を使用します。
Default: 初期設定の PCP/DEI の値を使用します。
Mapped: QoS クラスおよび DP レベルのマッピングされたバージョンを使用します

Tag Remarking Mode :
このポートのタグモードを選択します。
Classified: クラス分けした PCP/DEI の値を使用します。
Default: 初期設定の PCP/DEI の値を使用します。
Mapped: QoS クラスおよび DP レベルのマッピングされたバージョンを使用します

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。
Cancel – 変更を取り消す場合使用します。

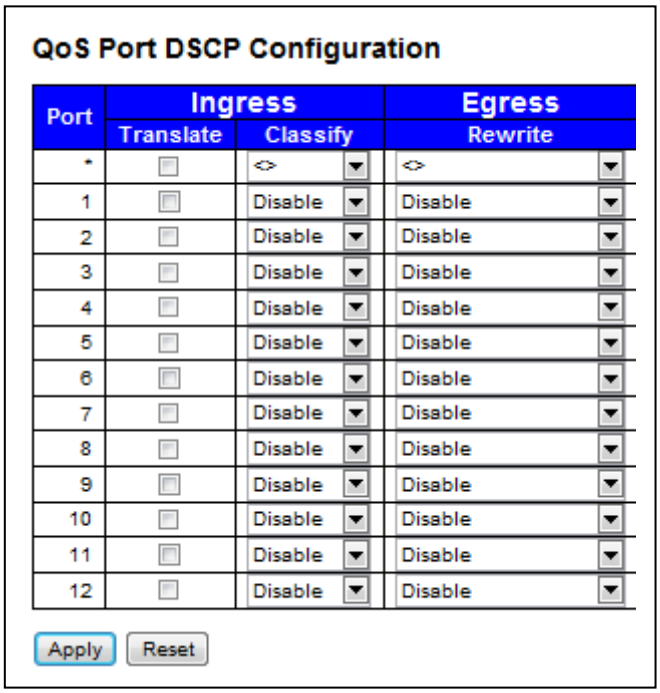
2.15.5 Port DSCP

スイッチのポートすべての QoS Port DSCP の基本設定を行うことが可能です。現在選択されているスタックユニットに関する設定情報が画面ヘッダに表示されます。

設定方法

QoS Port DSCP の値を設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→[Port DSCP]をクリックします。
Step 2. Ingress の「Translate」を有効にしたい場合は☑を入れて、「Classify」メニューを選択します。
Step 3. Egress の「Rewrite」の項目を選択します。
Step 4. <Apply>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.15.6:　The QoS Port DSCP Configuration



設定/表示項目

Port :
DSC 入力/出力の設定が可能なポートのリストが表示されます。

Ingress :
出力の設定では、各ポートの入力変換およびクラス分けを変更することができます。
入力で設定可能な値は以下の 2 つです。

Translate : 「Ingress Translation」を有効にするには、☑を入れてください。

Classify: ポートのクラス分けには、下記の 4 つの値があります。

Disable:受信 DSCP クラス分けをしない。
DSCP=0:受信した DSCP が「0」かどうかを設定します（有効な場合は変換されます）。
Selected:特定の DSCP の DSCP Translation 画面で指定した、クラス分けが可能な特定の DSCP のみ設定します。
All: DSCP をすべてクラス分けします。

Egress :
Port Egress Rewriting については、以下のいずれかになります。
Disable : 値を変更しない。
Enable　: マッピングせずに値を変更可能にします。
Remap DP Unawer:「DSCP Translation」で設定した、「Remap DP0」フィールド値が設定されます。
Remap DP Aware: 「DSCP Translation」で設定した、「Remap DP1」フィールド値が設定されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。
Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

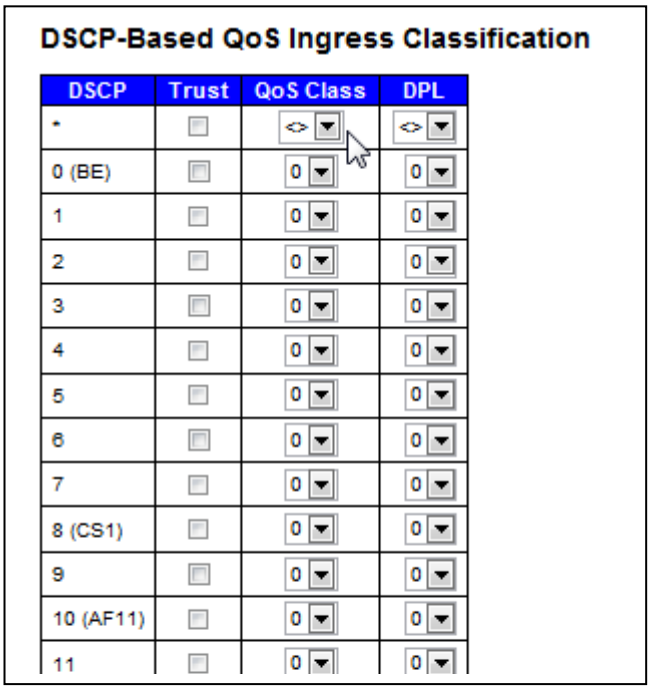
2.15.6 DSCP-Based QoS

DSCP ベースの QoS モードを設定します。スイッチの QoS について DSCP ベースの QoS Ingress Classification の設定を行うことができます。

設定方法

DSCP ベースの QoS 入力クラス分けの値を表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→{DSCP-Based QoS]をクリックします。
Step 2. DSCP の「Trust」に☑を入れて、有効/無効にしてください。
Step 3. QoS クラスおよび DPL の値を選択します
Step 4. <Apply>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルしたい場合は、<Reset>ボタンをクリックしてください。

Figure 2.15.7:　The DSCP-Based QoS Ingress Classification Configuration



設定/表示項目

DSCP :
サポートされている DSCP の最大値は「64」です。

Trust :
DSCP 値が正しい場合は、☑を入れてください。

QoS Class :
QoS クラスの値は 0～7 の任意の値です。
DPL :

破棄の優先レベルを設定します(0、1)。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、「DSCP-Based QoS Ingress Classification」情報が更新されます。

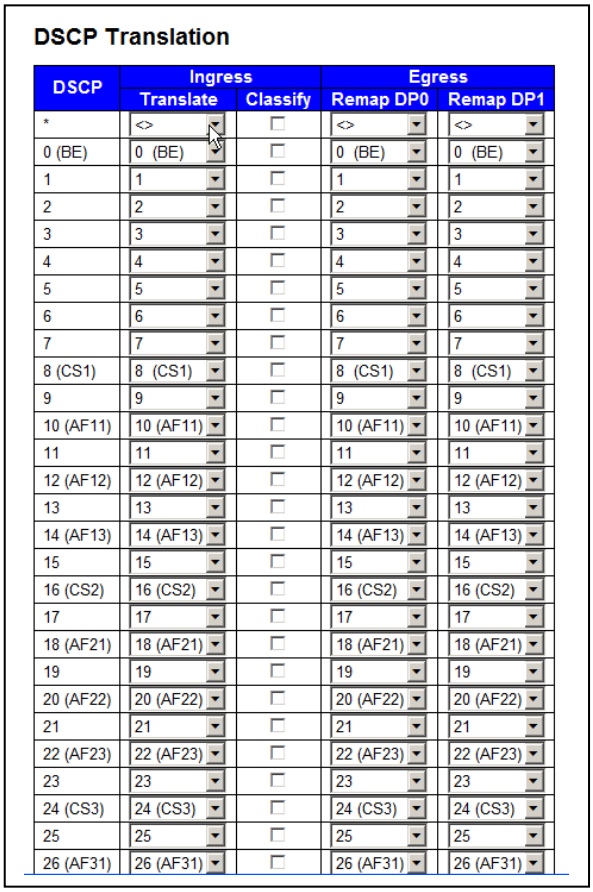
2.15.7 DSCP Translation

本機全体の QoS DSCP 変換の基本的な設定方法について説明します。入力/出力の DSCP 変換を行います。

設定方法

DSCP 変換の設定方法については、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→[DSCP Translation]をクリックします。
Step 2. 「Ingress」の「Translate」、「Egress」の「Remap DP0」および「Remap DP1」の値を選択します。
Step 3. 「Classify」を☑を入れて有効/無効にします。
Step 4. <Apply>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.15.8:　The DSCP Translation Configuration



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☐	<>	<>
0 (BE)	0 (BE)	☐	0 (BE)	0 (BE)
1	1	☐	1	1
2	2	☐	2	2
3	3	☐	3	3
4	4	☐	4	4
5	5	☐	5	5
6	6	☐	6	6
7	7	☐	7	7
8 (CS1)	8 (CS1)	☐	8 (CS1)	8 (CS1)
9	9	☐	9	9
10 (AF11)	10 (AF11)	☐	10 (AF11)	10 (AF11)
11	11	☐	11	11
12 (AF12)	12 (AF12)	☐	12 (AF12)	12 (AF12)
13	13	☐	13	13
14 (AF13)	14 (AF13)	☐	14 (AF13)	14 (AF13)
15	15	☐	15	15
16 (CS2)	16 (CS2)	☐	16 (CS2)	16 (CS2)
17	17	☐	17	17
18 (AF21)	18 (AF21)	☐	18 (AF21)	18 (AF21)
19	19	☐	19	19
20 (AF22)	20 (AF22)	☐	20 (AF22)	20 (AF22)
21	21	☐	21	21
22 (AF23)	22 (AF23)	☐	22 (AF23)	22 (AF23)
23	23	☐	23	23
24 (CS3)	24 (CS3)	☐	24 (CS3)	24 (CS3)
25	25	☐	25	25
26 (AF31)	26 (AF31)	☐	26 (AF31)	26 (AF31)

設定/表示項目

DSCP :
サポートしている DSCP の最大値は「64」です。DSCP の設定可能な範囲は「0 ～ 63」です。

8Ingress :
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 がまず新しい DSCP に変換されます。

DSCP 変換方法には、次の 2 通りがあります。
Translate : 入力側の DSCP は DSCP 値(0-63)のいずれかに変換可能です。
Classify : 出力側の「Classification」に☑を入れて有効にします。

Egress :
出力側の設定可能な値は以下のとおりです。
Remap DP0 : DP 値「0」の場合の DSCP 値を選択します。再度マッピングを行いたいメニューから DSCP の値を選択します。DSCP 値は「0～63」です。
Remap DP1 : 再度マッピングを行いたいメニューから値を選択します。DSCP 値は「0～63」です。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、DSCP 変換の情報が更新されます。

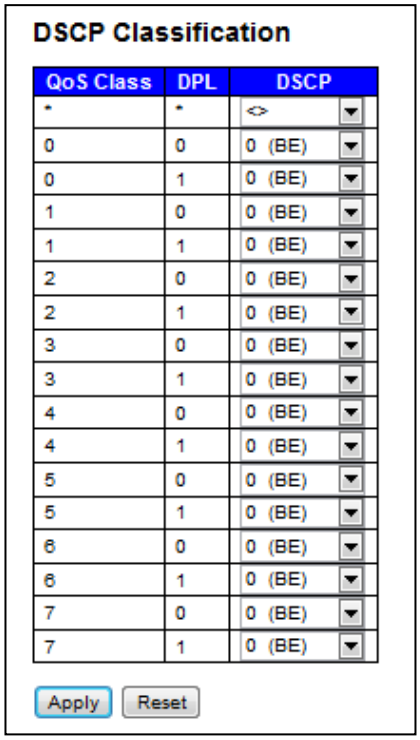
2.15.8 DSCP Classification

DSCP 値を QoS クラスおよび DPL 値にマッピングすることが可能です。現在選択されている スタックユニットに関する設定情報が画面ヘッダに表示されます。

設定方法

「DSCP Classification」の値を設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→[DSCP Translation]をクリックします。
Step 2. 「DSCP」の値を選択します。
Step 3. <Apply>ボタンをクリックして、値を保存します。
Step 4. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.15.9:　The DSCP Classification Configuration



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

設定/表示項目

QoS Class :
設定可能な QoS クラス値は「0～7」です。 QoS クラス (0-7)は次の値にマッピング可能です。

DPL :
廃棄優先レベル(0-1)の値です。

DSCP :
DSCP メニューから DSCP の値(0-63)を選択して、DSCP を対応する QoS クラスおよび DPL 値にマッピングします。

Buttons:
Save – 変更内容を保存します。

Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、DSCP クラス分類情報が更新されます。

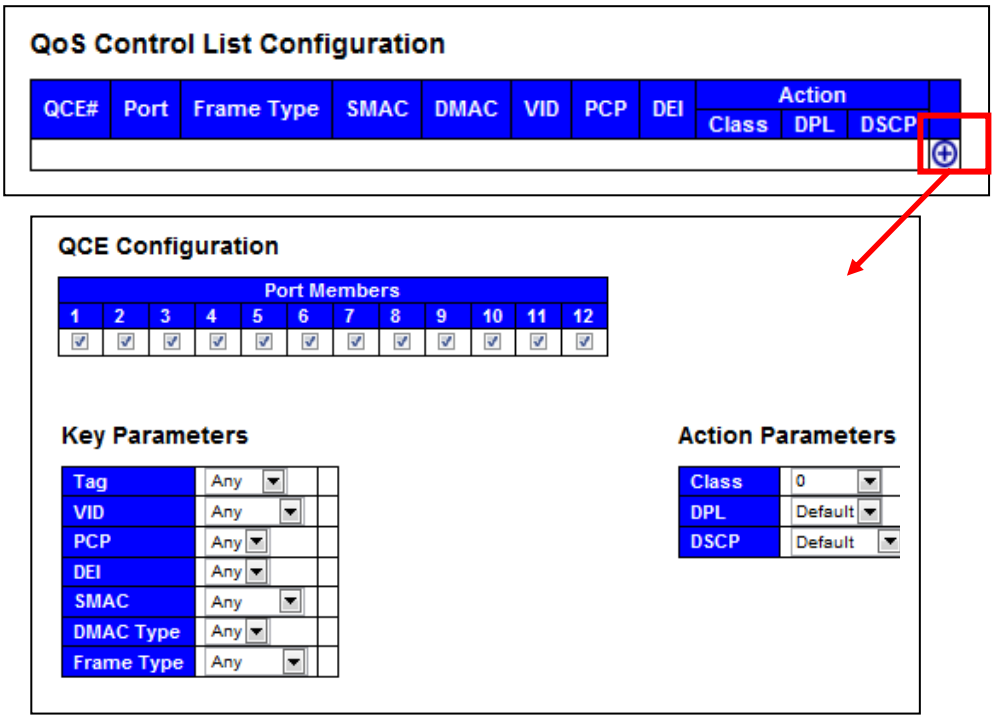
2.15.9 QoS Control List

QCE から構成されている QoS Control List(QCL)が表示されます。各スイッチの QCE の最大数は「256」です。右側の⊕をクリックすると、新しい QCE がリストに追加されます。

設定方法

「QoS Control List」の値を設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→[QoS Contol List]をクリックします。
Step 2. ⊕ をクリックすると、新しい QoS コントロールリストが表示されます。
Step 3. ポートメンバーに☑を入れると、QCE ルールに設定されます。
Step 4. <Apply>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.15.10:　The QoS Control List Configuration



設定/表示項目

QCE# :
QCE のインデックスが表示されます。

Port :
QCE に設定したポートのリストが表示されます。

Frame Type :
受信するフレームを検索するフレームのタイプが表示されます。
Any:すべてのフレームタイプに一致します。
Ethernet: イーサネットフレーム (Ether Type 0x600-0xFFFF 対応)
LLC: フレーム(LLC)のみが有効
SNAP: フレーム（SNAP)
IPv4: QCE は IPV4 フレーム
IPv6: QCE は IPV6 フレーム

SMAC :
ソース MAC アドレスの OUI フィールドが表示されます（MAC アドレスの最初の3バイト）

DMAC :
受信フレームの宛先 MAC アドレスのタイプを指定します。設定可能な値は、以下のとおりです。
Any:すべての宛先 MAC アドレスも許可します。
Unicast: ユニキャスト MAC アドレスのみ許可します。
Multicast: マルチキャスト MAC アドレスのみ許可します。
Broadcast: ブロードキャスト MAC アドレスのみ強化します。
初期設定は「Any」です。

VID :
特定の VID 、または VID の範囲のいずれか(VLAN ID)が表示されます。
VID の範囲は「1」～「4094」、あるいは「Any」です。

Conflict :
QCE ステータスが表示されます。QCE の追加に必要なリソースが設定できない場合があります。 この場合、「Yes」の場合はコンフリクトのステータスが表示され、それ以外は通常「No」です。

【注記】:
QCE の設定を変更したり、削除することでコンフリクトは解消されるため
<'Refresh>ボタンをクリックしてください。

Action :
設定した値が QCE の値と同じ場合は、アクションとして「Class」、「DPL」および「DSCP」のいずれかとして処理されます。
Class:
QoS クラス。 フレームが QCE と一致する場合は、キューイングされます。

DPL:
破棄手順レベル。フレームが QCE と一致した場合は、DP レベルは DPL の下に表示される値に設定されます。

DSCP:
フレームが QCE と一致した場合は、DSCP は DSCP の下に表示された値に設定されます。

Modification Buttons :
各 QCE (QoS Control Entry)を変更するには、以下のボタンをクリックしてください。
: 現在の行の前に新しい QCE を挿入します。
: QCE.を編集します。
: QCE をリストの先頭に移動します。
: QCE をリストの一番最後に移動します。
: QCE を削除します。
: QCE リストの一番下に新しいエントリを追加します。

Port Members :
QCL エントリのポートメンバーを設定したい場合は☑を入れてください。初期設定では、すべてのポートが選択されています。

Key Parameters :
キー設定は、以下のとおりです。
Tag フィールドは、または、'Tag'または、'Any' を設定できます。

VID:
VID の有効な値は、「1」～「4094」のいずれかか、「Any」です。
特定の値、Range を選択すると、VID の範囲を入力することができます。

PCP（Priority Code Point）:
PCP の有効値は (0～7)、あるいは (0-1, 2.3, 4.5, 6-7, 0-3, 4.7)の範囲、または「Any」のいずれかです。
DEI: DEI の有効な値は、「0」、「1」あるいは「Any」のいずれかです。

SMAC(Source MAC address):
3 バイト(OUI) あるいは 「Any」のいずれかです。

DMAC(Destination MAC type):
設定可能な値はユニキャスト (UC)、マルチキャスト (MC)、ブロードキャスト (BC)、あるいは「Any」のいずれかです。

Frame Type:
フレームのタイプは、以下の値のいずれかになります。
1. Ethernet
2. LLC
3. SNAP

4. IPv4
5. IPv6

【注記】:
フレームのタイプについて、それぞれ以下に説明します。
1. Any : フレームのすべてのタイプを許可します。
2. Ethernet : イーサネットタイプ。
有効なイーサネットタイプは「0x600～0xFFFF」の範囲内の値か、「Any」のいずれかになります。初期設定値は「Any」です。
3. LLC: SSAP アドレス。有効な SSAP(ソースアクセスポイント)は、「0x00～ 0xFF」の範囲内の値か、「Any」のいずれかです。
初期設定は 「Any」です。
DSAP アドレス。有効な DSAP(宛先サービスアクセスポイント)は、「0x00～0xFF」の範囲内の値か「Any」のいずれかです。
初期設定は「Any」です。
制御アドレス。制御アドレスは、「0x00～0xFF」の範囲内の 制御アドレスは有効の有効制御アドレスは「0x00」から「0xFF」に変更可能で、あるいは「Any」。初期設定は「Any」です。
4. SNAP : PID。
有効な PID(a.k.a イーサネットタイプ) は 0x00-0xFFFF の範囲内の値か、「Any」のいずれかです。初期設定値は「Any」です。
5. IPv4 : プロトコル。
プロトコル番号: (0-255, TCP、または UDP) 、あるいは「Any」のいずれかです。
Source IP:
「Any」または、ソース IP の特定の値、およびマスク
DSCP :
特定の DSCP 値、範囲、あるいは「Any」が設定できます。
DSCP 値は、BE, CS1-CS7, EF あるいは AF11-AF43 を含む「0～63」の範囲。
IP Fragment:フラグメントフレームであるかどうか。「yes」、「no」または「any」を設定します。
6. IPv6 :プロトコル(Next Header)。IP プロトコル番号 (0-255, TCP、または UDP)あるいは「Any」です。
Source IP(32 LSB): IPv6 ソースアドレス: (a.b.c.d)。「Any」または、32 LS bits(最下位ビット)表記の IPv6 アドレス。
DSCP :
特定の DSCP 値、範囲、あるいは「Any」が設定できます。
DSCP 値は、BE, CS1-CS7, EF あるいは AF11-AF43 を含む「0～63」の範囲。

Action Configuration :
Class: QoS クラス(0-7)を設定します。
DP: DP レベル(0,1)を設定します。
DSCP:DSCP 値あるいは PHB 値(0-63, BE, CS1-CS7, EF or AF11-AF43)を設定します。

Buttons:

Save – 変更内容を保存します。Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

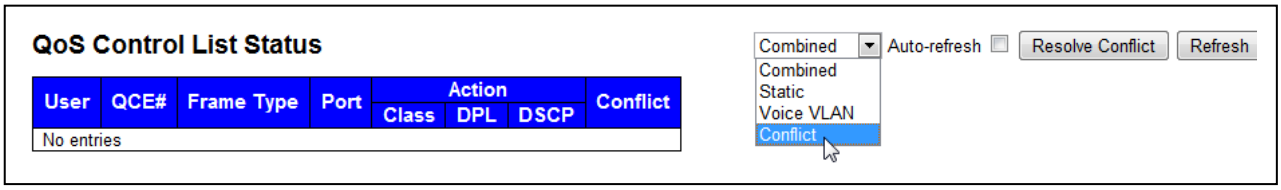
2.15.11　QCL Status

各種 QCL ユーザによる QCL ステータスの設定/表示方法について説明します。 それぞれの項目には定義されている QCE が表示されます。ハードウェアの制限により、特定の QCE がハードウェアに適用されない場合はコンフリクトが生じます。それぞれのスイッチの QCE の最大数は「256」です。

設定方法

QoS Control List Status を表示するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→[QCL Status]をクリックします。
Step 2. 自動更新を行う場合は、「Auto-refresh」に☑をいれてください。
Step 3. 「Combined」、「static」、「Voice VLAN」および「Conflict」のいずれかを選択します。
Step 4. <Refresh>ボタンをクリックすると、MVR グループのエントリが更新されます。

Figure 2.15.11:　The QoS Control List Status



設定/表示項目

User :
QCL ユーザを指します。
QCE#
QCE.のインデックスを指します。

Frame Type :
受信フレームを検索したいフレームのタイプを示します。設定可能なフレームタイプは以下のとおりです。
Any: QCE はすべてのフレームタイプに一致します。
Ethernet: イーサネットフレームのみ有効 (イーサネットタイプが「0x600-0xFFFF」の場合)
LLC: フレーム(LLC)
LLC: フレーム(SNAP)
IPv4: QCE は IPV4 フレーム
IPv6: QCE は IPV6 フレーム

Port :
QCE で設定したポートのリストが表示されます。

Action :
設定した値が QCE のフレームの値と同じ場合は、アクションとして「Class」、「DPL」および「DSCP」のいずれかが表示されます。

Class:
クラス分けされた QoS クラス。 フレームが QCE と一致する場合は、キューイングされます。キューの状態となります。

DPL:
破棄手順レベル。フレームが QCE と一致した場合は、DP レベルは DPL の下に表示される値に設定されます。

DSCP:
フレームが QCE と一致した場合は、DSCP は DSCP の下に表示された値に設定されます。

Conflict :
QCE ステータスが表示されます。QCE の追加に必要なリソースが設定できない場合があります。 この場合、「Yes」の場合はコンフリクトのステータスが表示され、それ以外は「No」です。QCE の設定を削除す ることによりコンフリクトは解消されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Resolve Conflict :
クリックすると、コンフリクトの問題が解決されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

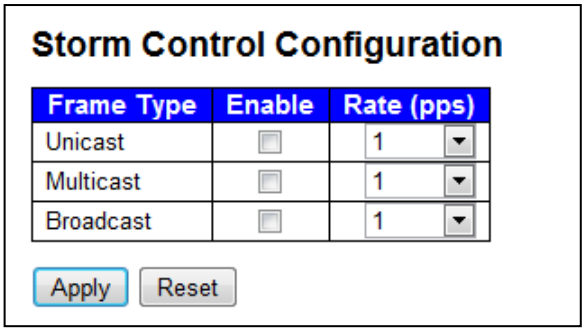
2.15.12 Storm Control

ストーム制御の設定方法について説明します。
T ストーム制御の実装により、ユニキャスト、マルチキャスト、またはブロードキャストのストームを防ぐことができます。例えばアクセス層のユーザポートでストーム制御の実装により、特定のホストポートがネットワークへ送信できるトラフィック量を制限できます。

設定方法

ストームコントロールを設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[QoS]→[Storm Control Configuration]をクリックします。
Step 2. フレームのタイプを選択して、ストームコントロールを有効にします。
Step 3. レートを選択します。
Step 4. <Apply>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.17.12:　The Storm Control Configuration



設定/表示項目

Frame Type :
ユニキャスト、マルチキャスト、またはブロードキャストそれぞれに設定します。

Enable :
指定されたフレームタイプのストームコントロール機能を有効/無効にします。

Rate :
単位は、毎秒ごとのパケット数 (pps)。 設定可能な値は: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K. , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K. , 1024K, 2048K, 4096K, 8192K, 16384K あるいは 32768K です。
「1 kpps」は実際には「1002.1 pps」です。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.16 s-Flow Agent

スイッチの sFlow コレクタの設定でモニタリング/修正を行うことができます。サポートしているコレクタは 1 個のみです。 ここでは、sFlowコレクタごとに、sFlow コレクタの IP タイプ、sFlow コレクタの IP アドレス、ポート番号を設定可能です。

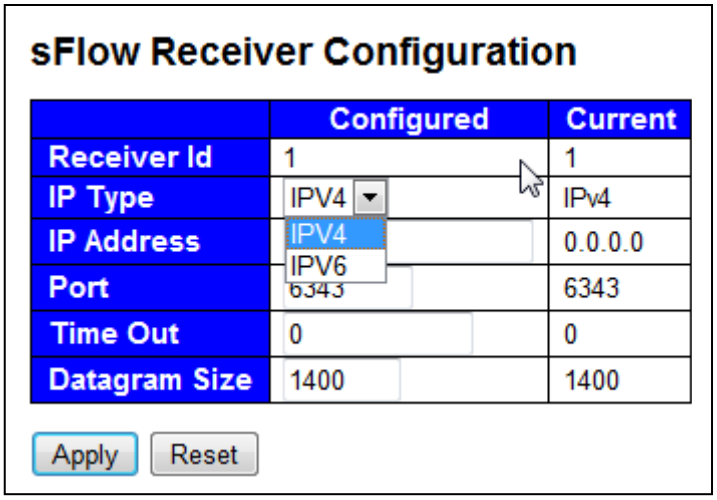
2.16.1 Collector

"Current " 項目では、現在設定されている sFlow コレクタ、Configured" 項目では新しいコレクタの設定が表示されます。

設定方法

sFlow エージェントを設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[sFlow Agent]→[Collector]をクリックします。
Step 2. コレクタの ID の値を設定します。
Step 3. IP タイプについては、「IPv4」または「IPv6」のいずれかを選択します。
Step 4. <Apply>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.16.1:　The sFlow Collector Configuration



設定/表示項目

Reciver ID:
コレクタの ID

IP Type :
コレクタの IP のタイプを選択します。初期設定では、「IPv4」です。「IPv4」または「IPv6」のいずれかを選択することができます。

IP Address :
設定可能な IP アドレスを入力します。IP を使って、sFlow エージェントによって送信された sFlow サンプルのモニタリングを行います。初期設定では、IP は「0.0.0.0」に設定され、新しいエントリが追加されます。

Port :
sFlow エージェントに対応するポートをコレクタに設定します。ポート番号の値を入力します。設定可能な範囲は「1」～「65535」です。設定に必要なプロトコルによって使用されていないポート番号です。初期設定は「6343」です。

Time out :
コレクタがサンプルを受信するまでの期間。一度期限が切れると、サンプラーはサンプルの送信を中止します。値を期限が切れる前に設定します。
値の範囲は「0」～「2147483647」です。初期設定は、「0」に設定されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

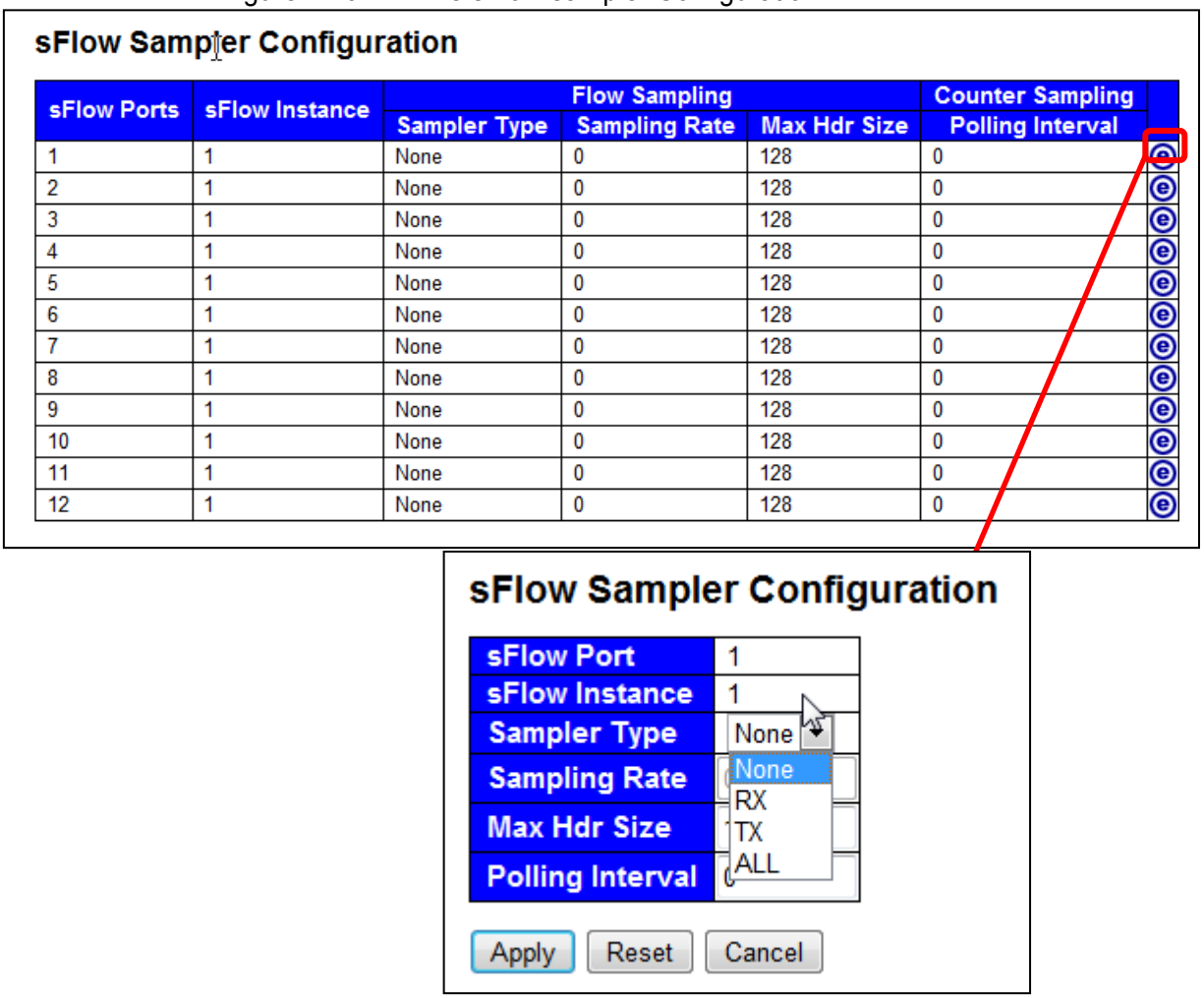
2.16.2 Sampler

要件に応じて、設定/編集可能な sFlow サンプラーが表示されます。定義されているサンプリングレートに応じて、N パケット/オペレーション分の 1 がランダムにサンプリングすることができます。
サンプリングタイプは、100%正確な結果ではないですが、正しい数値を提供します。

設定方法

sFlow エージェントを設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[Flow Agent, sampler]をクリックします。
Step 2. をクリックして、sFlow サンプラーの値を設定します。
Step 3. サンプルのタイプを「None」、「Tx」、「Rx」あるいは「All」から選択します。
Step 4. <Apply>ボタンをクリックして、値を保存します。
Step 5. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.16.1:　The sFlow sampler Configuration



設定/表示項目

sFlow Ports :
sFlow を設定するポート番号のリスト

sFlow Instance :
ポート番号に対して設定されている sFlow インスタンス

Sampler Type :
ポート上で設定されているサンプラーのタイプは、「None」、「Rx」、「Tx」あるいは「All」のいずれかから
1 つ選択してください。
初期設定は、「 None」です。

Sampling Rate :
ポートのサンプリングレート.

Max Hdr Size :
サンプルのフレームのヘッダサイズ

Counter Polling Interval :
カウンタサンプリングのポーリング間隔

Buttons:
- データのソースサンプルの設定を編集します。
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。
Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

2.17 Loop Protection

ループ検知を使って、トラフィックの状態を検知します。ポートからループ検知用のフレームを送信します。その MAC アドレスが、ポートからの MAC アドレスと同じ場合は、ループ検知が発生していることを表します。ループ検知フレームを受信するとポートはロックされます。ロックされたポートを再開させたい場合は、ループパスを検出して取り除いてから<Resume>ボタンをクリックしてください。

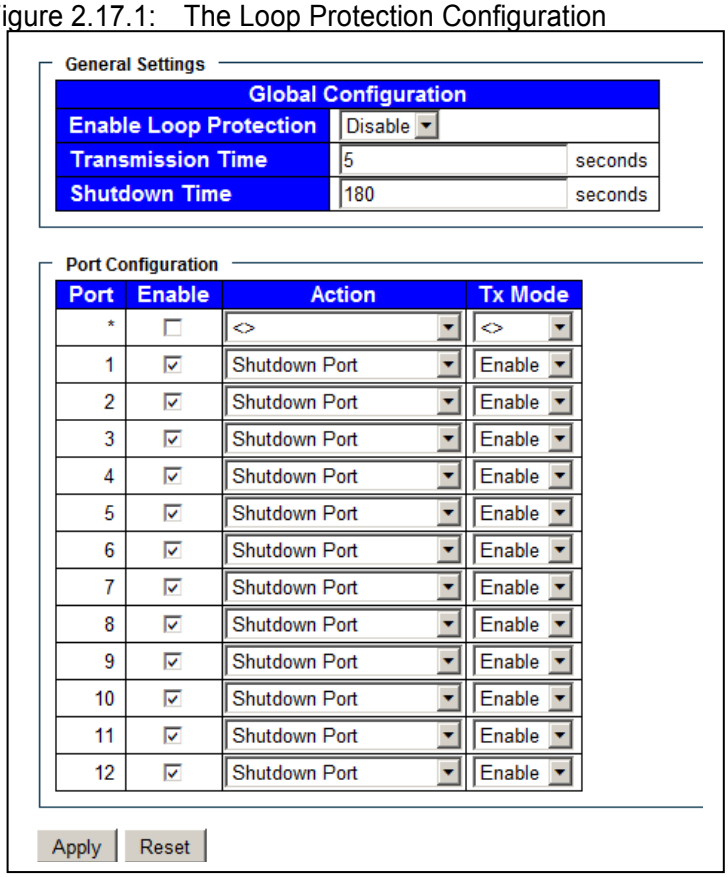
2.17.1 Configureaion

ループ検知の設定方法について説明します。

設定方法

ループ検知を設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[Loop Protection]→[Configuration]をクリックします。
Step 2. ループ検知機能を設定したポートに☑を設定してくだい。
Step 3. <Apply>ボタンをクリックして、値を保存します。
Step 4. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.17.1:　The Loop Protection Configuration



設定/表示項目

Port No:
ポート番号が表示されます（ポート番号:1～12）

Detection Port - Enable:
ポート番号に☑を入れると、検知機能が有効になり、ループ検知を行います。ループを検知するとポートはロックされ、ループが検知されない場合は、ポートはロック解除された状態となります。

cked Port - Resume:
ポート番号に☑を入れると、検知機能が有効になり、ループ検知を行います。ループを検知するとポートはロックされ、ループが検知されない場合は、ポートはロック解除された状態となります<Resume>ボタンをクリックすると、ロックされたポートはロック解除されます。
<Resume>ボタンをクリックしない場合は、ロックされたままの状態になります。

2.18 Single IP

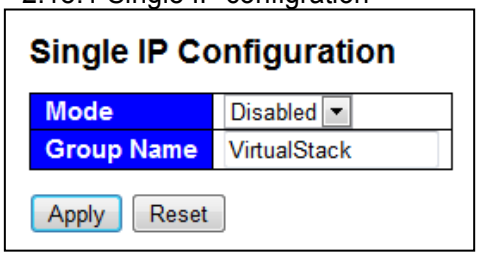
この機能により、単一 **IP** アドレスで複数の同一機器の制御を可能にする機能です。

2.18.1 Configration

設定方法

Step 1. [Configuration]→[Single IP]→[Configuration]をクリックすると、以下の画面が表示されます。

2.18.1 Single IP configration



設定/表示項目

Mode:機能を無効、マスター、スレーブのいずれかに設定します。

Group Name:グループのメンバーには、同一名を設定します。

Apply – 変更内容を保存します。

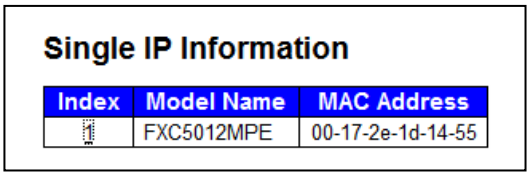
Reset- ローカルに変更した内容を取り消して、元の値に戻します。

2.18.2 Information

設定方法

Step 1.　[Configuration]→[Single IP]→[Information]をクリックすると、下の画面が表示されます。

2.18.2 Single IP Information



設定/表示項目

Index:グループ内の機器の ID。クリックすることでスレーブに接続可能です。

Model Name:スレーブのシステム名

MAC Address:スレーブの MAC アドレス

2.19 Mirroring

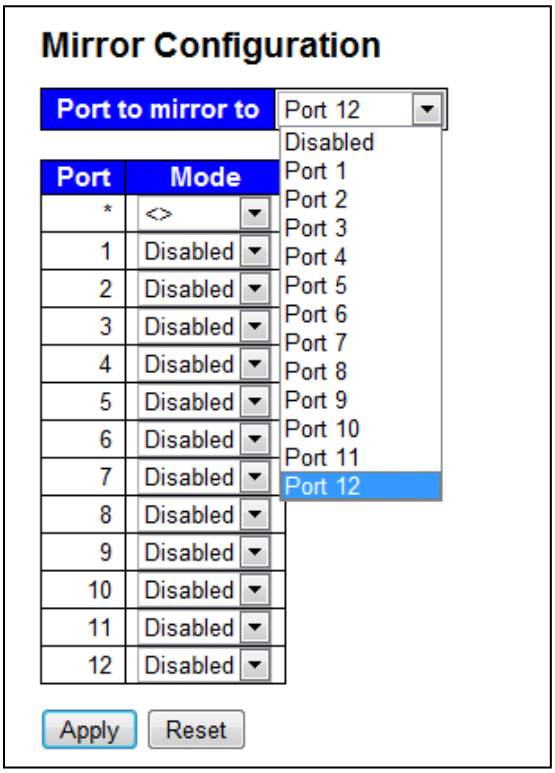
ミラーリングは、ネットワークのトラフィックのモニタリングを行います。リアルタイムに通信の解析を行うために、ソースポートからターゲットポートへのトラフィックのミラーリングを行います。ロジックアナライザ、または RMON プローブに接続して、通信に影響を与えずにソースポートのトラフィックを解析することができます。

設定方法

ミラーリング機能を設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[Mirroring]をクリックします。
Step 2. ミラーリングを行いたいポートを選択します。
Step 3. モードの値を「Disabled」、「Enable」、「TX Only」および「RX Only」から選択します。
Step 4. <Apply>ボタンをクリックして、値を保存します。

設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.19.1:　The Mirror Configuration



設定/表示項目

Port to mirror on :
ミラーリングを行いたいポートをミラーポートと指します。source (rx) または destination (tx) のミラーr ングを有効/無効にします。

Mirror Port Configuration
Port :
設定用の論理ポート.

Mode :
ミラーモードを選択します。
Rx only（受信）:
ポート上でミラーポートで受信したフレームのミラーリングを行います。送信されたフレームのミラーリングは行いません。
Tx only ：
ポート上でミラーポートに送信したフレームのミラーリングを行います。受信したフレームのミラーリングは行いません。
Disabled ：送受信したフレームのミラーリングを行いません。
Enabled ：ミラーポート側で送受信したフレームのミラーリングを行います。

【注記】:
指定したフレームの場合は、フレームは伝送のみを行うため、ミラーポート上の Tx フレームのミラーリングを行うことはできません。そのため、選択したミラーポートのモードは、「Disabled」、または「Rx only」に制限されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

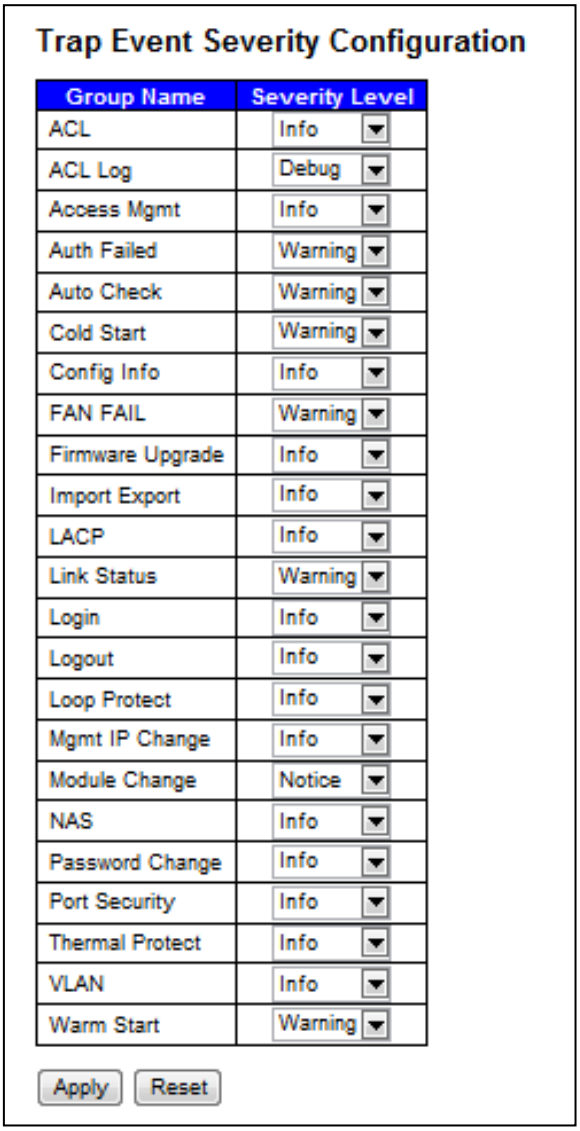
2.20 Trap Event Severity

機能ごとに異なるアラームトラップを設定することができる機能です。イベントログを入手する際に使用します。トラップイベントの機能により、既定のトラップイベントが発生すると、トラップ情報を送信します。

設定方法

Trap Event Severity を設定するには、以下の手順に従ってください。
Step 1. [Configuration]→[Trap Event Severity Configuration]をクリックします。
Step 2. グループ名のレベルを設定します。
Step 3. <Apply>ボタンをクリックして、値を保存します。
Step 4. 設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.20.1:　The Trap Event Severity Configuration



設定/表示項目

Group Name :
トラップイベントの定義について説明します。

Severity Level :
イベントタイプを「Emerg」、「Alert」、「Crit」、「Error」、「Warming」、「Notice」、「Info and Debug」から選択します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

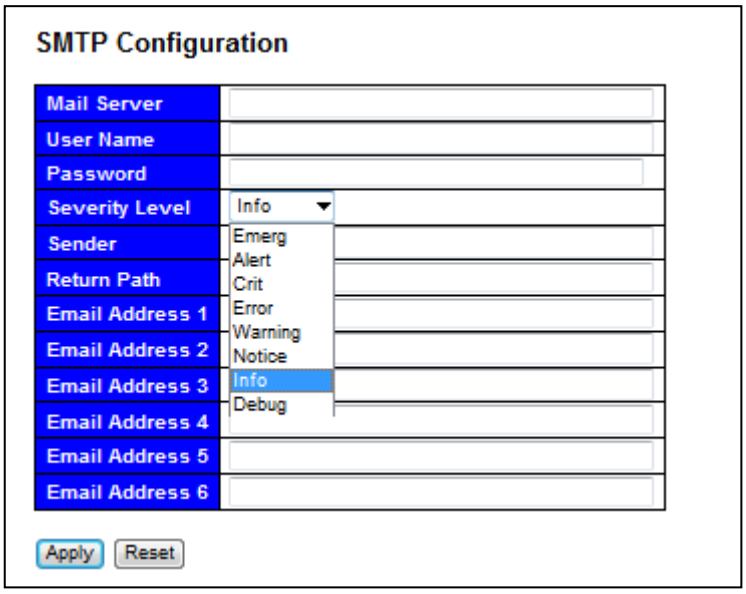
2.21 SMTP Configuration

アラームトラップの設定も使用します。スイッチがアラームを出すと、SMTP サーバによりアラームメールが送信されます。

設定方法

SMTP を設定するには、以下の手順に従ってください。
Step 1.　[Configuration]→[SMTP Configuration]をクリックします。
Step 2.　「Sevelty」レベルを選択します。
Step 3.　それぞれ空白の欄に値を入力します。
Step 4.　<Apply>ボタンをクリックして、値を保存します。
Step 5.　設定をキャンセルする場合は、<Reset>ボタンをクリックすると元の値に戻ります。

Figure 2.21.1:　The SMTP Configuration



設定/表示項目

SMTP 設定画面で表示されるメニューは以下のとおりです。

Mail Server :
メールの送信先のサーバの IP アドレスを指定します。

Username :
メールサーバのユーザ名を指定します。

Password :
メールサーバのパスワードを指定します。

Sender　:
メールの送信者名を設定します。

Return-Path :
メールの返信先のパスを送信者のアドレスとして設定します。

Email Address 1-6 :
アラームメッセージの受信先のメールアドレス

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

2.22 UPnP

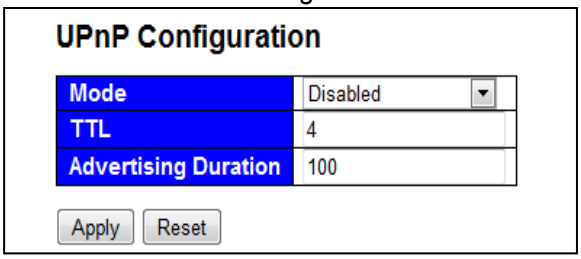
ここでは、UPnP の設定を行います。XML 技術をベースに開発された、ネットワーク機器どうしの相互自動認識方式です。
本機能を利用して"Windows Live Messenger"サービスなど、UPnP 機能対応アプリケーションを NAT による IP アドレスやポート番号の変換を気にすることなく、しかも複数のパソコンから同時にご利用いただけます。
本機とパソコンの UPnP 機能をご利用になると、Windows Live Messenger や Windows Messenger、MSN Messenger を複数台のパソコンでご利用になれます。

本機能をご利用になるには、本商品とパソコン側の設定が必要です。
ただし、本商品の設定は、初期値で「Disable」になっていますので、本機およびパソコン側で UPnP 機能の設定をすることにより、利用可能となります。

設定方法

Step 1. [Configuration]→[Single IP]→[UpnP]をクリックすると、以下の画面が表示されます。
Step 2. この機能を有効にする場合は、モードを「Enable」に設定してください。

2.22 UPnP Configration



設定/表示項目

Mode:UPnP の有効／無効を設定します。

TTL:生存時間を設定します(秒単位)。

Adertising Duration:UPnP で開いてる時間(秒)

3章　セキュリティ

ここでは、IP ソースガード、ARP Inspection、DHCP スヌーピング、AAA などのローカルネットワークのセキュリティを拡張するためのセキュリティの設定について説明します。

3.1 IP Source Guard

スイッチの IP ソースガードの設定方法について説明します。IP ソースガードを使ってスイッチのポートを有効/無効にします。

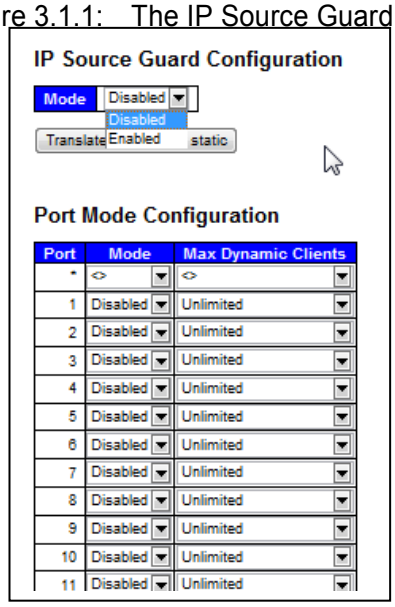
3.1.1 Configuration

以下の IP ソースガードの設定方法について説明します。
Mode (Enabled and Disabled)
Maximum Dynamic Clients (0, 1, 2, Unlimited)

設定方法

IP ソースガードを設定するには、以下の手順に従ってください。
Step 1. [Security]→[IP Source Guard]→[Configuration]をクリックして、IP ソースガードのモードを
「Enabled」に設定します。
Step 2. ポートモードのモードを「Enabled」に設定します。
Step 3. 特定ポートの 最大ダイナミッククライアントを「0」、「1」、「2」、「Unlimited」から選択します。
Step 4. <Apply>ボタンをクリックします。

Figure 3.1.1:　The IP Source Guard Configuration



設定/表示項目

Mode:
グローバル IP ソースガードを設定します。モードを有効にすると、設定された ACE はすべて破棄されます。

Translate Dynamic to Static:
クリックすると、動的アドレステーブルが静的テーブルに変換されます。

Port Mode Configuration :
ポートの IP ソースガードを有効にします。指定したポートのグローバルモードおよびポートモードを有効にすると、IP ソースガードが有効になります。

Max Dynamic Clients :
指定ポート上で学習可能なダイナミッククライアントの最大数を指定します。値は、「0」、「1」、「2」または「unlimited」のいずれかです。ポートモードが有効で、最大ダイナミッククライアントの値が「0」の場合は、特定ポートのスタティックエントリに一致する IP パケット転送のみ可能ということを意味します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

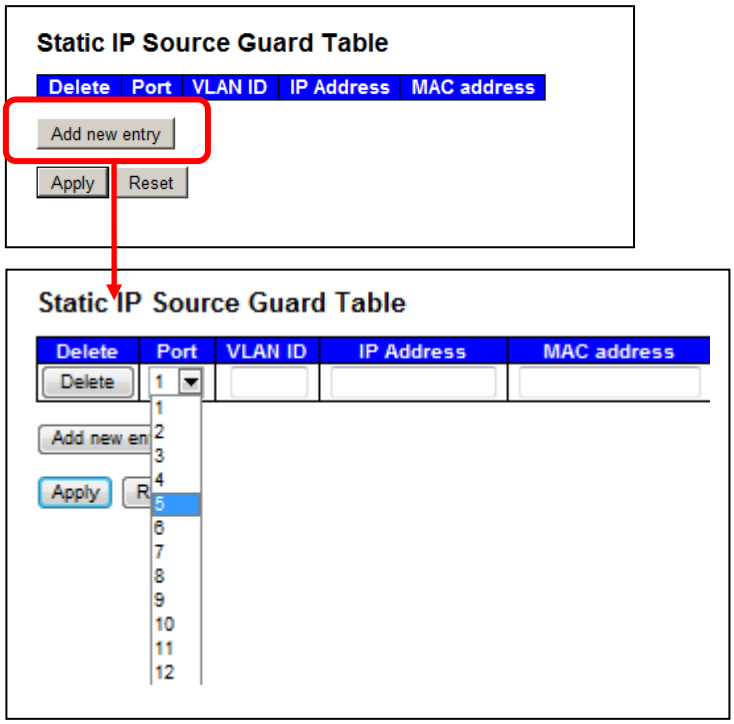
3.1.2 Static Table

本機のスタティック IP ソースガードについて説明します。スタティック IP ソースガードを使って、エントリを管理することができます。

設定方法

スタティック IP ソースガードを設定するには、以下の手順に従ってください。
Step 1. [Security]→[IP Source Guard]→[Static Table]をクリックして、<Add new entry>ボタンをクリックします。
Step 2. エントリのポート、VLAN ID、IP アドレス、MAC アドレスを設定します。
Step 3. <Apply>ボタンをクリックします。

Figure 4.1.2:　The Static IP Source Guard Table



設定/表示項目

Delete :
削除したい項目を選択して、 <Apply>ボタンをクックすると削除されます。

Port :
設定用の論理ポート.

VLAN ID :
設定用の VLAN ID.

IP Address :
設定可能なソース IP アドレス.

MAC address :
設定可能なソース MAC アドレス.

Adding new entry :
<Add new entry>をクリックして、スタティック IP ソースガードテーブルに新しいエントリを追加します。それぞれ「Port」、「 VLAN ID」、「IP address」および「IP Mask for the new entry」に値を入力後、
<Apply>ボタンをクリックします。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

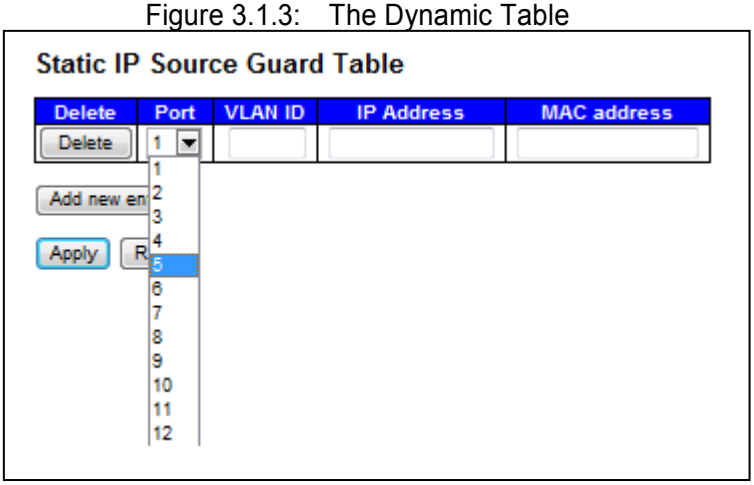
3.1.3 Dynamic Table

ここでは、ダイナミック IP ソースガードテーブルの値の設定方法について説明します。ダイナミック IP ソースガードテーブルを使って、エントリを管理することが可能です。

設定方法

ダイナミック IP ソースガードテーブルの設定方法については、以下の手順に従ってください。
Step 1.　開始ポート、VLAN ID、IP アドレスおよび画面ごとにエントリ数を設定します。
Step 2.　<Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.1.3:　The Dynamic Table



設定/表示項目

Port :
スイッチのポート番号

VLAN ID :
IP トラフィックが許可したい VLAN-ID

IP Address :
ユーザ IP アドレス.

MAC Address :
ソース MAC アドレス

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, <<, >>):
<Refresh>ボタンをクリックすると、情報が更新されます。矢印キー（”<<”, “>>“ ）を使って画面を移動します。

3.2 ARP Insprction

ARP Inspection について説明します。ARP Inspection を使って、ARP テーブルを管理することができます。

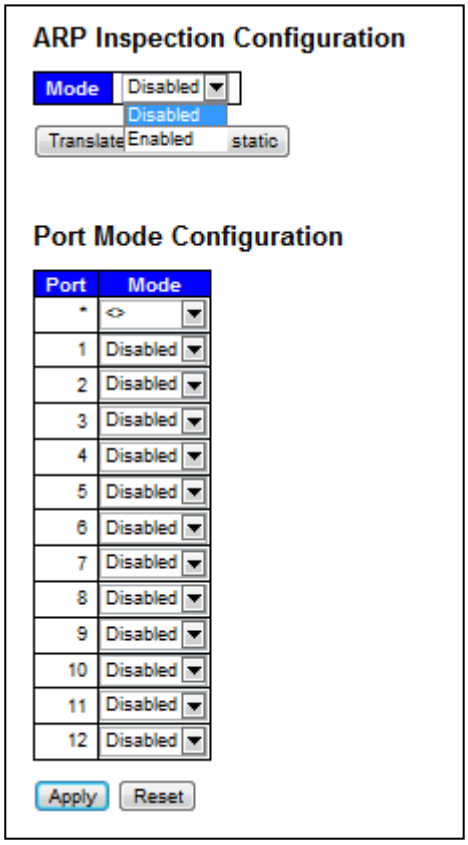
3.2.1 Configuration

以下の ARP Inspection の設定方法について説明します。
Mode (Enabled and Disabled)
Port (Enabled and Disabled)

設定方法

ARP Inspection を設定するには、以下の手順に従ってください。
Step 1.　ARP Inspection のモードを「Enabled」に設定します。
Step 2.　ポートモードのモードを「Enabled」に設定します。
Step 3.　<Apply>ボタンをクリックします。

Figure 3.2.1:　The ARP Inspection Configuration



設定/表示項目

Mode :
ARP Insprction を有効/無効に設定します。

Port Mode Configuration :
指定のポート ARP Insprction を有効にします。指定のポートのグローバルモード/ポートモードの両方を有効にした場合のみ ARP Insprction は「有効」になります。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

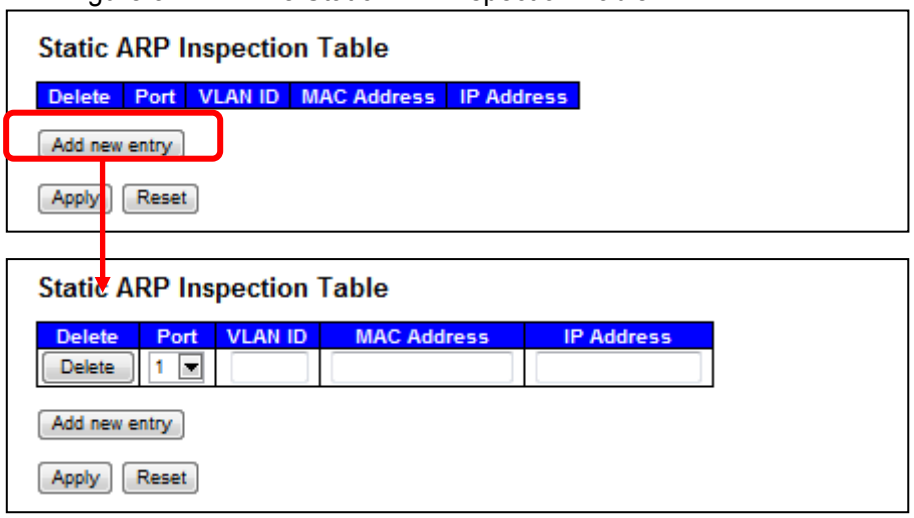
3.2.2 Static Table

スタティック ARP Insprction テーブルの値の設定方法について説明します。
スタティック ARP テーブルを使って、ARP エントリを管理することが可能です。

設定方法

スタティック ARP Inspeciton テーブを設定するには、以下の手順に従ってください。
Step 1.　<Add new entry>ボタンをクリックします。
Step 2.　ポート、VLAN ID, IP アドレスおよび MAC アドレスを入力します。
Step 3.　<Apply>ボタンをクリックします。

Figure 3.2.2:　The Static ARP Inspection Table



設定/表示項目

Delete :
削除したい項目を選択して、 <Apply>ボタンをクックすると削除されます。

Port :
設定用の論理ポート.

VLAN ID :
設定用の VLAN ID.

MAC Address :
ARP リクエストパケットの設定可能なソース MAC アドレス

IP Address :
ARP リクエストパケットの設定可能なソース IP アドレス

Adding new entry :
< add a new entry >ボタンをクリックすると、スタティック ARP Inspection テーブに新しいエントリが追加されます。新しいエントリのポート、VLAN ID、 IP アドレスおよび MAC アドレを指定します。設定終了後、 <Apply>ボタンをクリックします。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

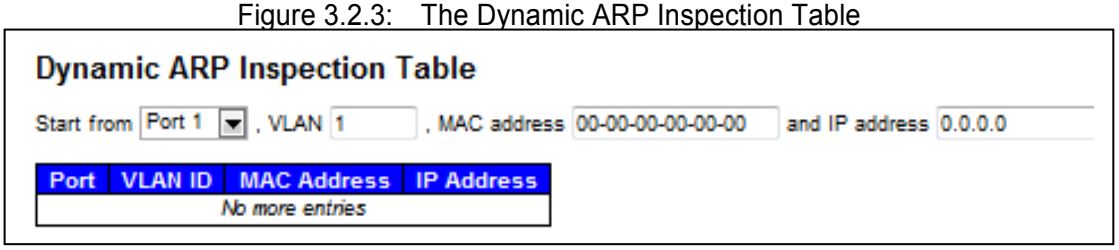
3.2.3 Dynamic Table

ダイナミックARP Inspectionテーブルの設定方法について説明します。ダイナミックARPテーブルには、最大1024個まで設定可能で、かつポート、VLAN ID、MACアドレス、IPアドレスごとにソートされます。

設定方法

ダイナミック ARP Insprction テーブルを設定するには、以下の手順に従ってください。
Step 1. 開始するポート、VLAN ID、MAC アドレス、IP アドレス、画面ごとのエントリ数を入力します。
Step 2. <Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.2.3:　The Dynamic ARP Inspection Table



設定/表示項目

Port :
スイッチのポート番号

VLAN ID :
ARP トラフィックが許可された VLAN-ID

MAC Address :
エントリのユーザの MAC アドレス

IP Address :
エントリのユーザ IP アドレス

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, <<, >>):
<Refresh>ボタンをクリックすると、情報が更新されます。矢印キー（”<<”, “>>“ ）を使って画面を移動します。

3.3 DHCP Snooping

DHCP スヌーピングの設定方法について説明します。DHCP スヌーピングにより、侵入者によるネットワークへの独自の DHCP サーバの追加を回避します。

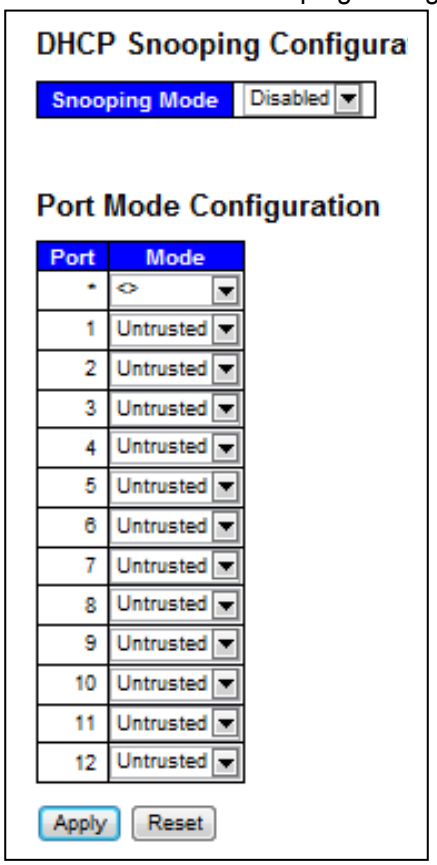
3.3.1 Configuration

以下の DHCP スヌーピングの設定方法について説明します。
Snooping Mode (Enabled and Disabled)
Port Mode Configuration (Trusted, Untrusted)

設定方法

DHCP スヌーピング を設定するには、以下の手順に従ってください。
Step 1.　[Security]→[DHCP Snooping]→[Configration]をクリックすると以下の画面が表示されます。
DHCP スヌーピングのモードを「Enabled」に設定します。
Step 2.　ポートモードの特定のポートを「Trusted」に設定します。
Step 3.　<Apply>ボタンをクリックします。

Figure 3.3.1:　The DHCP Snooping Configuration



設定/表示項目

Snooping Mode :
DHCP スヌーピングモードが表示されます。可能なモードは以下のとおりです。
Enabled: Enable DHCP スヌーピングモードを有効にします。DHCP スヌーピングが有効な場合は、DHCP リクエストメッセージが指定のポートに転送され、指定のポートからのパケットのみ応答することができます。
Disabled: DHCP スヌーピング　のモードを「無効」にします。

Port Mode :
DHCP スヌーピング　のポートモードを指します。
ポートの設定可能なモードは、以下のとおりです。
Trusted: ポートを DHCP　メッセージの信頼のあるソースに設定します。
Untrusted: ポートを DHCP　メッセージの信頼のないソースに設定します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

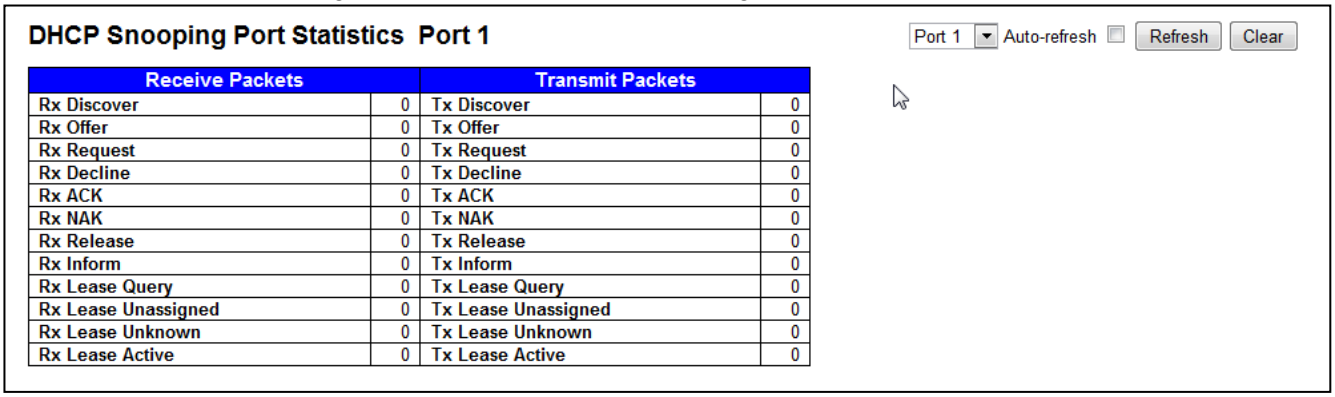
3.3.2 Statistics

DHCP スヌーピングの統計情報について説明します。統計情報では、DHCP スヌーピングモードが有効、かつリレーモードが無効な場合のみ表示されます。DHCP クライアントの DHCP パケットはカウントされません。

設定方法

DHCP スヌーピングの統計情報を設定するには、以下の手順に従ってください。
Step 1.　[Security]→[DHCP Snooping]→[Statistics]をクリックっして、モリタリングしたいポートを指定します。
Step 2.　<Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.3.2:　The DHCP Snooping Port Statistics



Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

設定/表示項目

Rx and Tx Discover :
送受信したパケットのうち、検出したパケット数 (値「1」のオプション 53)

Rx and Tx Offer :
送受信したパケットのうち、オファーしたパケット数(値「2」のオプション 53)

Rx and Tx Request :
送受信したパケットのうち、リクエストしたパケット数(値「3」のオプション 53)

Rx and Tx Decline :
送受信したパケットのうち、拒否されたパケット数(値「4」のオプション 53)

Rx and Tx ACK :
送受信したパケットのうち、ACK 数(値「5」のオプション 53)

Rx and Tx NAK :
送受信したパケットのうち、NAK 数(値「6」のオプション 53)

Rx and Tx Release :
送受信したパケットのうち、リリースした数(値「7」オプション 53)

Rx and Tx Inform :
送受信したパケットのうち、リリースした数(値「8」オプション 53)

Rx and Tx Lease Query :
送受信したパケットのうち、リースクエリーの数(値「10」オプション 53)

Rx and Tx Lease Unassigned :
送受信したパケットのうち、割り当てられたなかったリースの数(値「11」オプション 53)

Rx and Tx Lease Unknown :
送受信したパケットのうち、アンノウンリースの数(値「11」オプション 53)

Rx and Tx Lease Active :
送受信したパケットのうち、リースがアクティブな数(値「13」オプション 53)

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, Clear):
<Refresh>ボタンをクリックすると、情報が更新されます。<clear>ボタンをクリックすると、エントリが消去されます。

3.4 DHCP Relay

ここは、DHCP リレーを介して DHCP リクエストを別の特定の DHCP サーバに転送する方法について説明します。DHCP サーバは別のネットワーク上にある可能性があります。

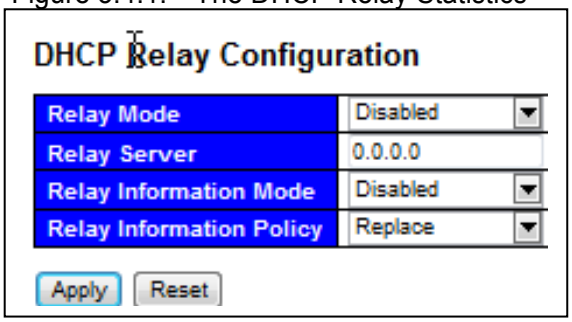
3.4.1 Configuration

ここでは、DHCP リレーの設定方法について説明します。
Relay Mode (Enabled and Disabled)
Relay Server IP setting
Relay Information Mode (Enabled and Disabled)
Relay Information Mode Policy (Replace, Keep and Drop)

設定方法

DHCP Relay を設定するには、以下の手順に従ってください。
Step 1. 「DHCP リレー設定」メニューのリレーモードを「Enabled」を選択します。
Step 2. リレーサーバの IP アドレスを指定します。
Step 3. 「DHCP リレー設定 」メニューのリレー情報モードを「Enabled」を選択します。
Step 4. リレー情報ポリシーの項目に「Replace」、「Keep and Drop」のいずれかを設定します。)
Step 5. <Apply>ボタンをクリックします。

Figure 3.4.1:　The DHCP Relay Statistics



設定/表示項目

Relay Mode :
DHCP リレーモードのオペレーションが表示されます。
Enabled:　DHCP リレーモードを「有効」にします。DHCP リレーモードが有効な場合、サーバ./クライアントが同じサブネットドメインにない場合は、エージェントにより、クライアント/エージェント間で DHCP メッセージの送受信が行われます。セキュリティの観点から DHCP ブロードキャストメッセージはフラッディングされません。
Disabled: DHCP リレーモードを「無効」にします。

Relay Server :

DHCP リレーサーバの IP アドレスを指します。サーバ./クライアントが同じサブネットドメインにない場合は、エージェントにより、クライアント/エージェント間で DHCP メッセージの送受信が行われます。

Relay Information Mode :
DHCP リレー情報モードのオプションを指します。
Enabled: DHCP リレー情報を「有効」にします。DHCP リレーモードが有効な場合、エージェントは、DHCP サーバへの転送時に DHCP メッセージに特定情報（オプション 82）が挿入したり、DHCP クライアントへの伝送時に DHCP メッセージから特定情報（オプション 82）を取り除いたりします。
Disabled: DHCP リレー情報を「無効」にします。

Relay Information Policy :
DHCP リレー情報のオプションのポリシーを指します。DHCP リレー情報モードを「有効」にすると、 エージェントがリレーエージェント情報を含む DHCP メッセージを受信すると、ポリシーを実行します。リレー情報が「有効」な場合、DHCP でのみ動作します。

Replace:
受信時に DHCP メッセージが含まれている場合は、オリジナルのリレー情報に置き換えます。

Keep:
受信時に DHCP メッセージを含む場合は、オリジナルのリレー情報をそのまま保持します。

Drop:
リレー情報が含まれている DHCP メッセージを受信した場合は破棄します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

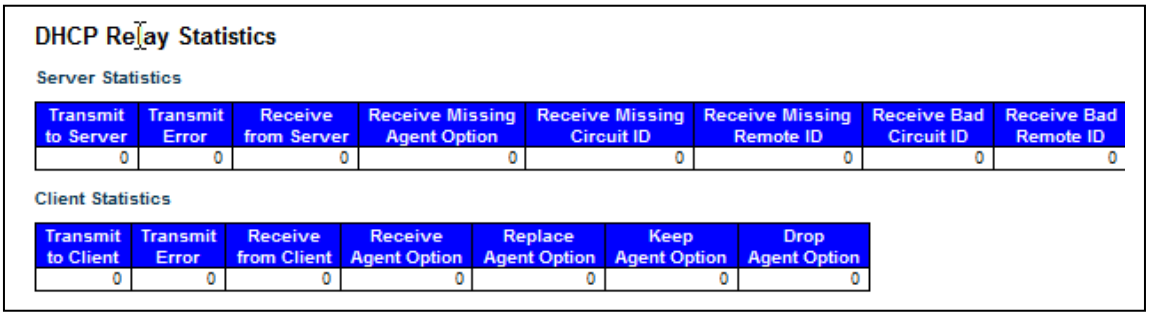
3.4.2 Statistics

DHCP リレーの統計情報について説明します。DHCP リレーが有効な場合のサーバ/クライアントのパケットのカウントが表示されます。

設定方法

DHCP スヌーピングの統計情報を設定するには、以下の手順に従ってください。
Step 1.　<Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.4.2:　The DHCP Relay Statistics



DHCP Relay Statistics

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

設定/表示項目

Transmit to Server :
クライアントからサーバにリレーされるパケット数

Transmit Error :
クライアントに送信中にエラーとなったパケット数

Receive from Server :
サーバから受信したパケット数

Receive Missing Agent Option :
エージェントのオプションのない、パケットの受信数

Receive Missing Circuit ID :
サーキット ID オプションが紛失したパケットの受信数

Receive Missing Remote ID :
リモート ID のオプションが紛失したパケットの受信数

Receive Bad Circuit ID :
サーキット ID オプションが既知のサーキット ID に一致しないパケット数

Receive Bad Remote ID :
リモート ID オプションが既知のリモート ID に一致しないパケット数
Client Statistics

Transmit to Client :
サーバからクライアントにリレーされたパケット数

Transmit Error :
サーバに送信中ににエラーとなったパケット数

Receive from Client :
サーバから受信したパケット数

Receive Agent Option :
リレーエージェント情報のオプションを持つパケットの受信数

Replace Agent Option :
リレーエージェント情報のオプションにリプレースされたパケットの受信数

Keep Agent Option :
リレーエージェント情報もつパケット数

Drop Agent Option :
リレーエージェント情報を受信して破棄されたパケット数

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, Clear):
<Refresh>ボタンをクリックすると、情報が更新されます。<clear>ボタンをクリックすると、エントリが消去されます。

3.5 NAS

本機の NAS の値を設定します。NA サーバにより、インターネットアクセス、カンフェレンスコール、共有プリンタからの書類のプリントなどの各種リソースを使って、ユーザはインターネットに簡単にログインすることができます。

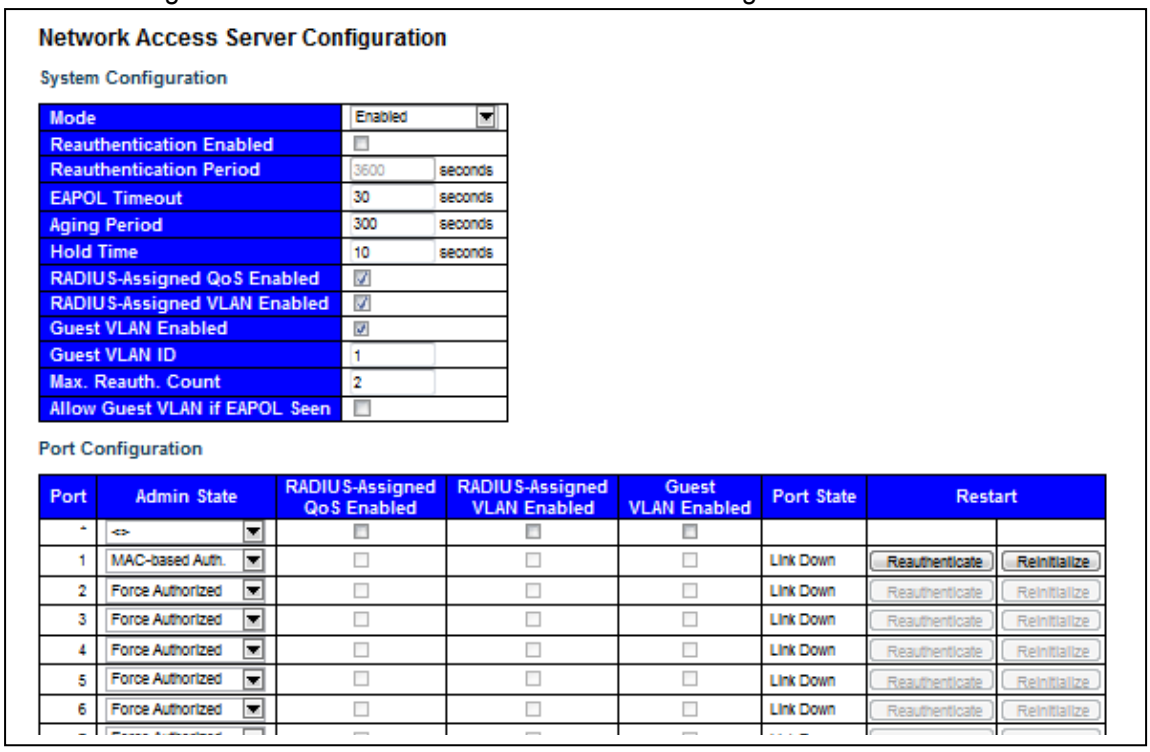
3.5.1 Configuration

IEEE 802.1X, MAC ベースの認証システム、ポートの設定の NAS の設定方方について説明します。NAS の設定は、システム、ポートワイドの 2 つから構成されます。

設定方法

ネットワークアクセスサーバのシステム設定を行うには、以下の手順に従ってください。
Step 1. [Security]→[NAS]→[Configration]をクリックすると、以下の画面が表示されるので、ネットワークアクセスサーバのモードを「Enabled」に設定します。
Step 2.「Reauthentication Enabled」に☑を入れます。
Step 3. 再認証時間を設定します (初期設定では、「3600 秒」です)。
Step 4. EAPOL のタイムアウトを設定します(初期設定は「30 秒」です)。
Step 5. エージングタイムを設定します (初期設定は「300 秒」です).
Step 6. Hold タイムを設定します(初期設定は 「10 秒」です)。
Step 7.「RADIUS-Assigned QoS Enabled」を☑します。
Step 8.「RADIUS-Assigned VLAN Enabled」を☑します。
Step 9.「Guest VLAN Enabled」を☑します。
Step 10.「Guest VLAN ID」を入力します。
Step 11.「Max. Reauth. Count」を入力します。
Step 12.「Allow Guest VLAN if EAPOL Seen」を☑します。
Step 13. <Apply>ボタンをクリックします。

Figure 3.5.1:　The Network Access Server Configuration



設定/表示項目

Mode :
スイッチのスタックの NAS がグローバルで「有効/無効」を設定します。グローバルで「無効」にすると、すべてのポートのフレームの伝送を許可します。

Reauthentication Enabled :
この項目に☑すると、再認証時間によって指定した時間を過ぎると、正しく認証されたサプリカント/クライアントが再認証されます。802.1X 対応のポートを使って、新しいデバイスがポートにプラグインされていないか、サプリカントに接続されいないかを検出します。
MAC ベースのポートについては、RADIU サーバの設定が変更される場合のみ有用です。スイッチとクライアント間の通信は含まれません。そのため、クライアントがポート上にあるということではありません（以下、「エージングタイム」を参照）。

Reauthentication Period :
接続先のクライアントの再認証を行うタイムを秒単位で設定します。再認証の項目を☑した場合のみ有効です。設定可能な値は「1 秒」～「3600 秒」です。

EAPOL Timeout :
Request Identity EAPOL フレームの再送時間を設定します。設定可能な値は「1」～「255 秒」です。MAC ベースポートには影響ありません。

Aging Period :
この設定は、次のモードに適用されます。例えば、MAC アドレス用のポートセキュリティ機能を使用するモードです。
• Single 802.1X
• Multi 802.1X

• MAC-Based Auth.
NAS モジュールが MAC アドレス用にポートセキュリティモジュールを使用する場合、ポートセキュリティモジュールは定期的に MAC アドレスの動作を確認し、一定時間内に何も検出場合はリソースを開放します。ここでは、この時間を制御し、「10 秒」～「1000000 秒」の値に設定します。再認証が「有効」かつポートが 802.1X ベースモードの場合は、ポートに接続されていないサプリカントは次の再認証時に取り除かれるため、特に重要ではありません。再認証が「無効」な場合は、エントリのエイジングによりリソースを開放します。
「MAC-based Auth」モードの場合は、スイッチ/クライアント間の通信間での再認証は行われないため、クライアントが接続されているかどうか検出されず、エントリのエイジングを行うことにより、リソースを開放します。

Hold Time :
MAC アドレス用のポートセキュリティを使用して、次のモードに適用されます。
• Single 802.1X
• Multi 802.1X
• MAC-Based Auth.

クライアントがアクセスを拒否した場合:
RADIUS サーバがクライアントアクセスを拒否したか、RADIUS サーバがタイムアウトを要求したかのいずれか（"Configuration→Security→AAA"画面で指定したタイムアウトに応じて）。クライアントは認証　されない状態のままです。hold timer は、認証中はカウントされません。
「MAC-based Auth」モードでは、スイッチは、hold time の間、クライアントから受信した新しいフレームを無視します。
Hold Time は、「10 秒」～「1000000 秒」の値に設定されます。

RADIUS-Assigned QoS Enabled :
RADIUS-assigned QoS は、トラフィッククラスの中央管理を行うことを言い、正常に認証されたサプリカントから受信したトラフィックがスイッチに割り当てられます。RADIUS サーバはこの機能を利用するために、特殊な RADIUS 属性を送信するように設定する必要があります（詳細については、「RADIUS-Assigned QoS Enabled」を参照してください）。
「RADIUS-Assigned QoS Enabled」の項目を☑を入れて、RADIUS-server に割り当てられた QoS クラスの機能を「有効/無効」に設定します。この機能を「有効」にすると、各ポートの設定の同等の機能により RADIUS-server に割り当てられた QoS クラスの機能が「有効」かどうかを判別され、無効にすると、すべてのポート上でこの機能は「無効」になります。

RADIUS-Assigned VLAN Enabled :
RADIUS-assigned VLAN では、スイッチ上で正しく認証されたサプリカントに置き換えた VLAN の中央制御をいます。受信したトラフィックはクラス分けされ、RADIUS 指定の VLAN に変換されます。RADIUS サーバを設定し、この機能を利用するために特殊な RADIUS 属性を伝送する秘具用があります（詳細については、「RADIUS-Assigned QoS Enabled」を参照してください）。
「RADIUS-Assigned VLAN Enabled」の項目を☑を入れて、VLAN-server に割り当てられた VLAN の機能を「有効/無効」に設定します。この機能を「有効」にすると、各ポートの設定の同等の機能により RADIUS-server に割り当てられ VLAN の機能が「有効」かどうかを判別され、「無効」にすると、すべてのポート上でこの機能は「無効」になります。

Guest VLAN Enabled :
Guest VLAN は特殊 VLAN です。 通常、制限のあるネットワークアクセスでは、VLAN クライアントは、ネットワーク管理者により定義されたタイムアウトを過ぎると、VLAN クライアントに置き換えられます。スイッチは、以下にリストされた Guest VLAN に接続/解除するには一連のルールに従いします。
"Guest VLAN Enabled"メニューを使って、「有効/無効」に設定します。この機能を「有効」にすると、ポートが Guest VLAN に移行可能かどうかを判別します。「無効」にすると、Guest VLAN への設定機能は すべてのポート上で「無効」になります。

Guest VLAN ID :
ポートが Guest VLAN.に移行した場合の Port VLAN ID の値です。この値は Guest VLAN のオプションが有効な場合のみ変更可能です。設定可能な値は「1」～「4095」の範囲内です。

Max. Reauth. Count :
Guest VLAN への移行を考慮する前に応答せずに、スイッチにより EAPOL Request Identity フレームの送信回数はここで調整します。この値は、Guest VLAN のオプションが有効な場合のみ、変更可能です。設定可能な値は、「1」～「255」の範囲内です。

Allow Guest VLAN if EAPOL Seen :
ポートのライフタイムに応じて EAPOL フレームが受信されたかどうかを記憶します。一度スイッチが Guest VLAN への移行を検討すると、オプションが「有効/無効」かをまず確認します。この機能が無効な場合（初期設定）は、ポートのライフタイムに応じて EAPOL フレームが受信されなかった場合は Guest VLAN に入ります。「有効」にすると（☑を入れると）、ポートのライフタイムに応じて EAPOL フレーが受信された場合でも Guest VLAN に切り替えます。この値は、Guest VLAN のオプションが有効な場合のみ変更可能です。

Port Configuration :
スタック内の選択したスイッチ上の各ポートについて表示されます。

Port :
適用可能なポート番号を指します。

Admin State :
NAS が「有効」な場合は、 ポートの認証モードを制御します。以下のモードが設定可能です。

Force Authorized :
このモードでは、スイッチは、ポートのリンクが「ON」の場合、ポートの上のクライアントは認証なしでネットワークへのアクセスが許可されます。

Force Unauthorized :
このモードでは、ポートのリンクが「ON」の場合、EAPOL Failure フレームを送信します。ポート上のクライアントはすべてネットワークへのアクセスは拒否されます。

Port-based 802.1X :
802.1X-world では、ユーザはサプリカント、スイッチは認証者、RADIUS サーバは認証サーバと言います。認証者は、「中間者攻撃」として動作し、サプリカントと認証サーバ間のリクエスト/応答の転送を行
います。

サプリカント/スイッチ間で送信されたフレームは、特殊な 802.1X フレームで、「EAPOL（EAP Over LANs）」と言います。EAPOL フレームは EAP PDUs (RFC3748).をカプセル化します。スイッチ/ RADIUS サーバ間で送信されたフレームは RADIUS パケットです。RADIUS パケットもスイッチの IP アドレス、名前、サプリカントのポート番号のような属性と共に EAP PDUs をカプセル化します。EAP は、とても柔軟に対応可能で、MD5-Challenge、 PEAP および TLS などの各種認証方式も可能です。重要なことは、認証者（スイッチ）は、サプリカントおよび認証サーバが使用している認証方式や、特定の方式に必要なフレームを交換するための情報について把握する必要がありません。フレームの EAP 部分を対応するタイプ（EAPOL、または RADIUS) にカプセル化するして伝送するだけです。
認証が完了すると、RADIUS サーバにより成功/失敗の結果を含む特殊なパケットが送信されます。サプリカントにこの結果を伝送する意外に、スイッチはサプリカントに接続されたポート上トラフィックをブロックしたり、ブロックを解除するために使用します。

【注記】:
2 つのバックエンドサーバが「有効」、かつサーバのタイムアウトが「X 秒」（AAA 設定画面）、最初のサーバが現在ダウンしている（ただし、電源がついている）の場合、サプリカントから新しい EAPOL Start フレームを受信すると、現在実行しているバックエンド認証サーバをキャンセルするため、サプリカントが. EAPOL スタートフレームを X 秒より速い速度で再送しても認証されません。
サーバが失敗（X 秒以内のため）、同じサーバはスイッチからの次のバンクエンドの認証サーバのリクエストにコンタクトします。この方法は永続的にループを行うため、サーバのタイムアウトは、サプリカントの EAPOL 開始フレームの再伝送レートよりも小さくなります。

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

Multi 802.1X :
ポートベース 802.1X 認証の場合は、一旦サプリカントをポート上で正しく認証すると、ポート全体がネットワークトラフィックに対して開放されます。
これにより、ポートに接続されたその他のクライアント（例えば、ハブを介して）は、正しく認証されたクライアントと合致し、認証されてない場合でもネットワークアクセスを入手することができます。
このセキュリティの違反を取り締まるために、「multi 802.1X 変数」を使用します。

「multi 802.1X 変数」は IEEE 規格ではありませんが、ポートベース 802.1X と同じ特徴を備えています。「multi 802.1X」は、1 つ以上のサプリカントが同時に同じポート上での認証が可能です。各サプリカントは個々に認証され、ポートセキュリティを介して MAC テーブルで入手されます。「multi 802.1X」は、ポートに接続されたサプリカントすべてに、スイッチから送信されたリクエストに応答させようとするため、スイッチからサプリカントに送信された EAPOL フレームの宛先 MAC アドレスとしてマルチキャスト BPDU MAC アドレスを使用することはできません。
その代わりに、最初の EAPOL Start、または EAPOL Response Identity フレームから入手したサプリカントの MAC アドレスを使用します。サプリカントとが接続されてない場合を除き、スイッチは BPDU マルチキャスト MAC アドレスを宛先アドレスとして使用し、
EAPOL Request Identity フレームを送信します（ポート上のサプリカントを起動させるため）。
ポートに接続可能なサプリカントの上限は、ポートセキュリティのミット制御機能を使用して制限することができます。

MAC-based Auth.:
ポートベースの 802.1X とは異なり、MAC ベース認証は標準ではないですが、業界で採用された唯一の成功事例です。
MAC ベース認証は”クライアント”と呼ばれ、スイッチはクライアントの代わりにサプリカントとして動作します。クライアントによって送信された最初のフレーム（どのタイプのフレームも）は、スイッチにより SNOOP されます。これは、後続の EAP を RADIUS サーバと交換して、クライアントの MAC アドレスを交互に使用します。6 バイトの MAC アドレスは次の形式の文字列に変換されます。"xx-xx-xx-xx-xx-xx"、つまり、(-)は、小文字の 16 進数を区切るために使用されます。スイッチは、MD5-Challenge 認証方式のみをサポートしているため、RADIUS サーバもこれに応じて設定する必要があります。認証が完了すると、RADIUS サーバは認証が成功/失敗したことを通知します。スイッチは、順次にポートセキュリテモジュールを介して、特定のクライアントのトラフィックをブロックしたり、許可したりします。
クライアントからのフレームがスイッチに伝送されます。EAPOL フレームはこの認証に含まれまれないため、MAC ベース認証は 802.1X とは関係がありません。

ポートベースの 802.1X を介した MAC ベース認証は、 同じポート（例えば、サードパーティのスイッチ、またはハブ）に接続可能で、個々の認証が必要です。802.1X ベース認証を介した MAC ベース認証の利点として、クライアントは認証を要するサプリカントのソフトウェアは必要ありません。欠点としては、悪意のあるユーザによって MAC アドレスを悪用される恐れがあります（装置の MAC アドレスが有効な場合、RADIUS ユーザは誰にでも使用可能）。
また MD5-Challenge 方式のみサポートしています。ポートに接続可能なクライアントの上限は、ポートセキュリティリミット制限機能を使って制限することができます。

RADIUS-Assigned QoS Enabled :
RADIUS-Assigned VLAN がグローバルでも、指定のポートでも「有効」な場合、サプリカントが正しく認証されると、RADIUS によって送信された RADIUS Access-Accep パケットで搬送された VLAN ID 情報に反応します有効な場合は、ポートの Port VLAN ID はこの VLAN ID に変更され、このポートは VLAN ID,のメンバーに設定されます。ポートは強制的に VLAN unaware モードになります。一度割り当てられると、ポートで受信したトラフィックはすべて割り当てられ、RADIUS-assigned VLAN ID に切り替えられます。

認証に失敗するか、または RADIUS Access-Accept パケットが VLAN ID を持たない場合、その値が無効な場合は、サプリカントはポートに存在しません。ポートの VLAN ID は直ちに元の VLAN ID（RADIUS-assigned を行わず、管理者によって変更される）に戻されます。
このオプションは、シングルクライアントモードにのみ有効です。
• Port-based 802.1X
• Single 802.1X

QoS クラスの識別用の RADIUS 属性:
RFC4675 に定義されている User-Priority-Table 属性は Access-Accept パケットの QoS クラスを識別する基礎を作成します。パケット内に属性が最初に検出された場合のみ有効です。以下のルールに従ってください。
属性の値の中の 8 オクテットすべてが同じで、”0”～”3”までの ASCII 文字で構成されます。
これは、[0; 3]範囲内の QoS クラスに変換されます。

RADIUS-Assigned VLAN Enabled :
RADIUS-Assigned VLAN がグローバルでも、指定のポートでも「有効」な場合、サプリカントが正しく認証されると、RADIUS によって送信された RADIUS Access-Accep パケットで搬送された VLAN ID 情報に反応します有効な場合は、ポートの Port VLAN ID はこの VLAN ID に変更され、このポートは VLAN ID のメンバーに設定されます。ポートは強制的に VLAN unaware モードになります。一度割り当てられると、ポートで受信したトラフィックはすべて割り当てられ、RADIUS-assigned VLAN ID に切り替えられます。
認証に失敗するか、または RADIUS Access-Accept パケットが VLAN ID を持たない場合、その値が無効な場合は、サプリカントはポートに存在しません。ポートの VLAN ID は直ちに元の VLAN ID（RADIUS-assigned を行わず、管理者によって変更される）に戻されます。
このオプションは、シングルクライアントモードにのみ有効です。
• Port-based 802.1X
• Single 802.1X
VLAN 割り当て用のトラブルシューティングを行う場合は、[Monitor]→[VLANs]→[VLAN Membership and VLAN Port]をクリックしてください。
この画面では、これらのモジュールは一時的に現行の Port VLAN 設定を上書きします。
VLAN ID 識別用の RADIUS 属性:
RFC2868 および RFC3580 は、Access-Accept パケットの VLAN ID 識別用の属性をベースを形成します。
以下の基準を使用します。
• Tunnel-Medium-Type, Access-Accept パケットに Tunnel-Type および Tunnel-Private-Group-ID 属性があること。
• スイッチは、同じタグの値をもつ最初の属性を探して、次の要件をみたすこと。(Tag == 0 を使用する場合は、Tunnel-Private-Group-ID はタグを含める必要はありません):
  - Tunnel-Medium-Type の値は、"IEEE-802" (ordinal 6)に設定すること.
  - Tunnel-Type の値は、VLAN" (ordinal 13)に設定すること。
  - Tunnel-Private-Group-ID の値は、ASCII の文字列であること（'0'-'9 までの範囲）。
これは、VLAN ID を示す 10 進数として解釈されます）。最初の'0'は破棄されます。
最終値は、[1; 4095]の範囲内です。
Guest VLAN Enabled :
Guest VLAN は、グローバルでも、指定したポート上で「有効」な場合は、スイッチは、以下のルールに従い、ポートを「Guest VLAN」に切り替えます。

オプションは、EAPOL-based モードに対して有効です。
• Port-based 802.1X
• Single 802.1X
• Multi 802.1X
VLAN 割り当て用のトラブルシューティングを行う場合は、[Monitor]→[VLANs]→[VLAN Membership and VLAN Port]をクリックしてください。
この画面では、これらのモジュールは一時的に現行の Port VLAN 設定を上書きします。

Guest VLAN Operation:
Guest VLAN のポートのリンクが「ON」になると、スイッチは EAPOL Request Identity フレームの送信を開始します。フレームの伝送数が上限を超えると、再認証を行います。Count フレームを受信し、EAPOL フレームを受信しない場合は、スイッチは Guest VLAN になったとみなされます。
EAPOL Request Identity フレームの送信間隔は EAPOL Timeout で設定されます。
Allow Guest VLAN if EAPOL Seen が有効な場合は、ポートは Guest VLAN になります。無効な場合は、EAPOL フレームがポート上で受信されているかどうかを確認するために履歴をまずチェックします（ポートのリンクが切れたり、ポートの管理状態が変更されると履歴は消去されます）。有効な場合は、Guest VLAN に置きかえれらます。それ以外は、Guest VLAN に切りかえらず、EAPOL タイムアウトによって指定された速度で EAPOL Request Identity フレームの送信を継続して行います。一度 Guest VLAN になると、ポートは認証され、ポート上の接続されているクライアントはすべてこの VLAN へのアクセスを許可します。スイッチは、Guest VLAN になると、EAPOL Success フレームを送信しません。
Guest VLA の間、スイッチは、EAPOL フレームのリンクをモニタリングします。これらのフレームを受信すると、スイッチは、ポートを Guest VLAN から取り出し、ポートモードに応じてサプリカントの認証を開始します。
EAPOL フレームを受信すると、ポートは Guest VLAN に戻れなくなります。"Allow Guest VLAN if EAPOL Seen" は「無効」になります。

Port State :
ポートの現行の状態。以下の値のいずれかになります。
Globally Disabled: NAS はグローバルに「無効」です。
Link Down: NAS はグローバルに「有効」ですが、ポートのリンクはありません。
Authorized: ポートは「Force Authorized」または「single-supplicant」モード、サプリカントは認証されます。
Unauthorized: ポートが「Force Unauthorized」または「single-supplicant」モードの場合は、サプリカントは RADIUS サーバにより正しく認証されません。
X Auth/Y Unauth: ポートが「multi-supplicant」モードの場合、現行の X クライアントは認証されますが、Y クライアントは認証されません。

Restart :
2 つのボタンをそれぞれ使用可能です。ボタンは認証されている場合のみ有効で、ポートの管理状態が EAPOL ベースモードか、MAC ベースモードの場合です。
ボタンをクルックすると、画面の設定の変更は無効になります。
Reauthenticate：ポートの停止時間が切れる（EAPOL ベース認証）と再認証が行われます。MAC ベース認証の場合は、再認証が直ちに行われます。
ポート上で正しく認証されたクライアントにのみ有効です。

Reinitialize: ポート上のクライアントを強制的に再起動することにより、直ちに再認証を行います。再認証が実行されている間、クライアントは認証されていない状態になります。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

3.5.2 Switch Status

各ポートの NAS ステータス情報について説明します。ステータスには、Admin 状態、ポート状態、最新ソース、最新 ID、QoS クラスおよびポート VLAN ID があります。

設定方法

NAS Switch Status を設定するには、以下の手順に従ってください。
Step 1. <Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.5.2: The Network Access Server Switch Status

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	MAC-based Auth.	Link Down				
2	Force Authorized	Link Down				
3	Force Authorized	Link Down				
4	Force Authorized	Link Down				
5	Force Authorized	Link Down				
6	Force Authorized	Link Down				
7	Force Authorized	Link Down				
8	Force Authorized	Link Down				
9	Force Authorized	Authorized				
10	Force Authorized	Link Down				
11	Force Authorized	Link Down				
12	Force Authorized	Link Down				

設定/表示項目

Port :
ポート番号を指します。クリックすると、このポートの NAS 統計情報が表示されます。

Admin State :
ポートの現行の管理状態。設定可能な値については、「NAS Admin State」を参照してください。

Port State :
ポートの現行の状態。個々の状態の詳細についは、「NAS Port State」を参照してください。

Last Source :
EAPOL ベース認証用に受信した最新の EAPOL、かつ MAC ベース認証用の新規クライアントから受信した最新のフレームで実行されたソース MAC アドレス。

Last ID :
EAPOL ベース認証用に受信した最新の Response Identity EAPOL フレーム、かつ MAC ベース認証用の新規クライアントから受信した最新のフレームで実行されたソース MAC アドレスで実行されたユーザ名(サプリカントの ID)。
QoS Class :

RADIUS サーバによってポートに割り当てられた QoS クラス。

Port VLAN ID :
NAS によりポートに付加された VLAN ID。 Port VLAN ID が NAS によって上書きされない場合は、空白のままになります。
RADIUS サーバによって割り当てられてた VLAN ID。"(RADIUS-assigned)"が VLAN ID に追加されます。
ポートが Guest VLAN に切り替えれれた場合は、"(Guest)" が VLAN ID に追加されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

3.5.3 Port Status

EAPOL ベースの IEEE 802.1X が動作している特定のスイッチポート用の詳細な NAS 統計情報について説明します。

設定方法

NAS Port Status Configuration を設定するには、以下の手順に従ってください。
Step 1. 選択したいポートを指定します。
Step 2. <Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.5.3: The NAS Statistics

設定/表示項目

Port State

Admin State :
ポートの現行の管理状態が表示されます。設定可能な値については、「NAS Admin State」を参照してください。

Port State :
ポートの現行状態。個々の状態の詳細については、「NAS Port State」を参照してください。

QoS Class :
RADIUS サーバにより割り当てられた QoS クラス。 QoS クラスが指定されていない場合は、空白のままです。

Port VLAN ID :
NAS によりポートに付加された VLAN ID。 Port VLAN ID が NAS によって上書きされない場合は、空白のままになります。
RADIUS サーバによって割り当てられてた VLAN ID。"(RADIUS-assigned)"が VLAN ID に追加されます。ポートが Guest VLAN に切り替えれた場合は、"(Guest)" が VLAN ID に追加されます。

Port Counters

EAPOL Counters :
サプリカントフレームはのカウンタは以下の管理状態で有効です。
- Force Authorized
- Force Unauthorized

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

Backend Server Counters :
バックエンド(RADIUS)フレームは、以下の管理状態で有効です。
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Last Supplicant/Client Info :
認証を行う最新のサプリカント/クライアント情報。この情報は、以下の管理状態で有効です。
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Selected Counters
Selected Counters :
ポートが以下の管理状態の場合、選択したカウンタテーブルが表示されます。
- Multi 802.1X
- MAC-based Auth.

テーブルがポートカウンタテーブルと同じかつポートカウンタテーブルの隣にあります。MAC アドレスが現在選択されていない場合は、空白のままになります。
テーブルを設定するには、以下のテーブルから付属の MAC アドレスのいずれかを選択します。

Attached MAC Addresses Identity :
Response Identity EAPOL フレームで受信したサプリカントの ID が表示されます。
ここに☑を入れると、サプリカントの EAPOL および Backend Server カウンタが選択したカウンタテーブルに表示されます。サプリカントが付属されていない場合は、表示されません。
MAC ベース認証には有効ではありません。

MAC Address :
Multi 802.1X の場合は、付属のサプリカントの MAC アドレスが表示されます。
MAC ベース認証の場合は、Selected Counters テーブルにクライアントの MAC アドレスが表示されます。☑をいれると、リンクによりクライアントの Backend Server のカウンタが表示されます。クライアントが付属してない場合は、”No clients attached”と表示されます。

VLAN ID
ポートセキュリティモジュールを介して、現在対応しているクライアントの VLAN ID が表示されます。

State :
クライアントの認証/非認証が可能です。認証状態の場合は、フレームをポートに伝送可能です。非認証状態の場合はブロックされます。バックエンドサーバによりクライアントが正しく認証されなかった場合は、非認証の状態となります。何らかの原因により認証に失敗した場合は、クライアントは「Hold Time」の間認証されないままの状態になります。

Last Authentication :
クライアントの最新の認証日時（成功、かつ失敗した場合）が表示されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, Clear):
<Refresh>ボタンをクリックすると、情報が更新されます。<Clear>ボタンをクリックすると、すべてのエン
トリが削除されます。

3.6 AAA

お使いのネットワークへのアクセス制御を行う AAA (Authentication, Authorization, Accounting)サーバについて説明します。AAA サーバは、AAA サーバ用の設定を含むオブジェクトの作成/管理を行う TACACS+、あるいは RADIUS サーバです。

3.6.1 Configuration

TACACS+、あるいは RADIUS サーバの AAA 設定方法について説明します。

設定方法

AAA の標準設定を行うには、以下の手順に従ってください。
1. Timeout を設定します(初期設定は 15 秒間)
2. Dead Time を設定します (初期設定は 300 秒間)

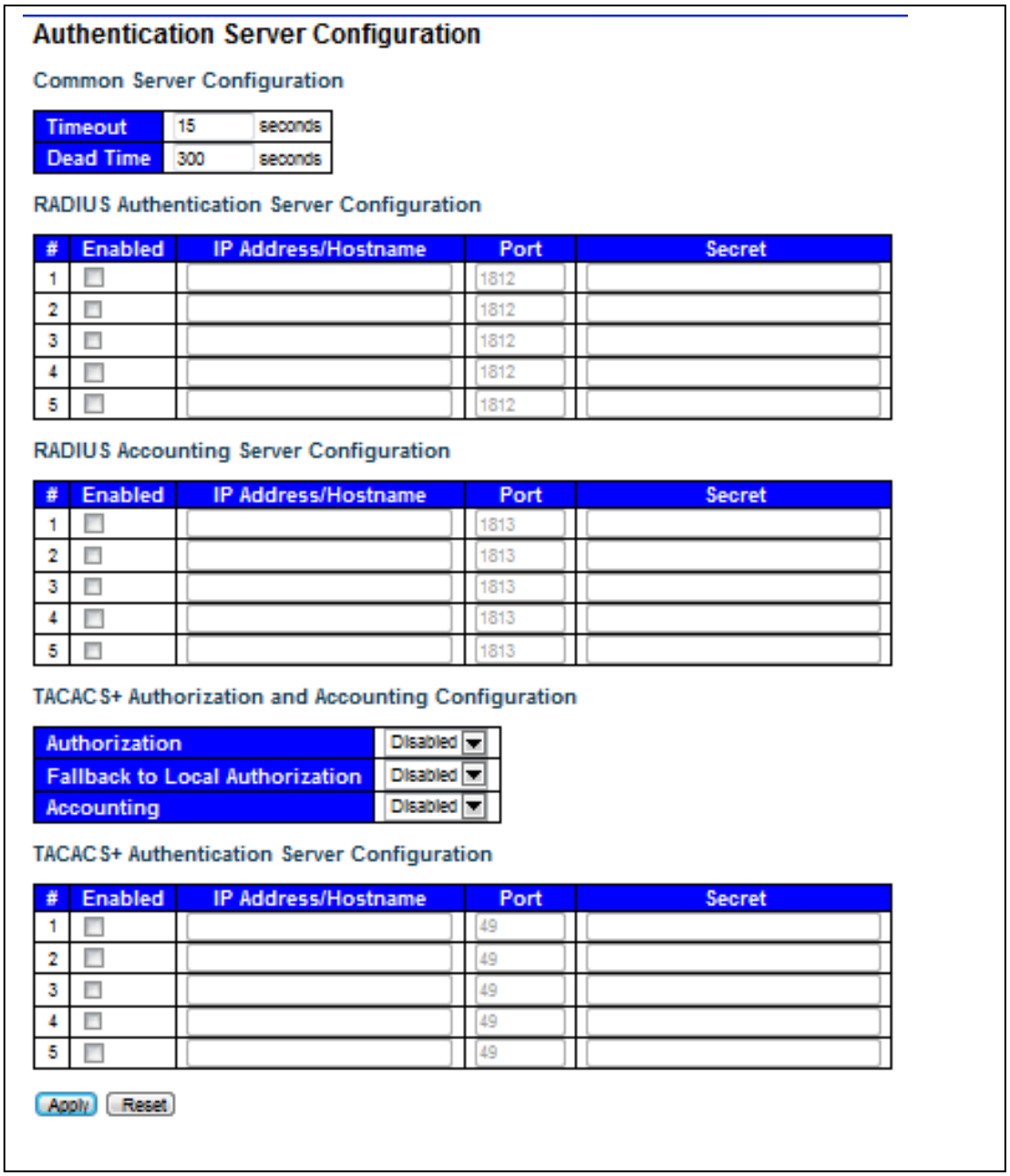
AAA の TACACS+認証およびアカウントを設定するには、以下の手順に従ってください。
1. 認証を「Enabled」に設定します。
2. ローカル認証へのフェールバックを「Enabled」に設定します。
3. アカウントを「Enabled」に設定します。

AAA の RADIUS 認証サーバのを設定するには、以下の手順に従ってください。
1. 「Enabled」を.
2. Radius サーバの IP アドレス、あるいはホスト名を入力します。
3. Radius サーバの認証ポートを指定します (初期設定は「1812」)。
4. Radius サーバの Secret を入力します。

AAA の RADIUS アカウントサーバを設定するには、以下の手順に従ってください。
1. 「Enabled」をチェックします。
2. Radius サーバの IP アドレス、あるいはホスト名を入力します。
3. Radius サーバのアカウントを入力します(初期設定は「1813」)。
4. Radius サーバの Secret を入力します。

AAA の TACACS+認証サーバ を設定するには、以下の手順に従ってください。
1. 「Enabled」をチェックします。
2. TACACS+サーバの Radius サーバの IP アドレス、あるいはホスト名を入力します。
3. TACACS+サーバの Radius サーバのアカウントを入力します(初期設定は「1813」)。
4. TACACS+サーバの Secret を入力します。

Figure 3.5.3.1:　The Common Server Configuration



設定/表示項目

Timeout :
タイムアウト。この値は、「3～3600 秒」の範囲内の値に設定可能です。サーバからの応答を待つ最大時間です。サーバがこのタイムフレーム内で応答しない場合はダウンしたとみなし、次の有効なサーバがあればそちらにて切り替えて継続します。
RADIUS サーバは UDP プロトコルを使用します。紛失したフレームを処理するために、タイムアウトの間隔は等間隔で 3 つのサブインターバルに分けられます。サブインターバル内に応答がない場合は、再度リクエストが送信されます。この方法により、RADIUS サーバは 3 回まで問い合わせ後、応答がなければダウンした状態とみなします。

Dead Time :
デッドタイム。この値は「0～3600 秒」の範囲内の値に設定可能です。この間は、前回のリクエストに対する応答に失敗したサーバには新しいリクエストの送信は行いません。これにより、既にダウンしたとみなされたサーバへのアクセスを回避することが可能です。「デッドタイム」を「0」より大きい値に設定すると、複数のサーバが設定されている場合のみこの機能が有効です。

RADIUS Authentication Server Configuration
RADIUS 認証サーバにつき、1つずつ設定項目があります。

:
RADIUS 認証サーバの番号。以下のメニューが適用されます。

Enabled :
Enable このメニューに☑を入れると、RADIUS 認証サーバが「有効」になります。

IP Address/Hostname :
RADIUS 認証サーバの IP アドレス、またはホスト名。 IP アドレスは、10 進表記で表記されます。

Port :
RADIUS 認証サーバ用の UDP ポート。ポートを「0」に設定すると、初期設定のポート (1812) が RADIUS 認証サーバ上で使用されます。

Secret :
RADIUS 認証サーバとスイッチスタック間で最大 29 文字のシークレットが共有します。
RADIUS Accounting Server Configuration
RADIUS アカウンティングサーバにはそれぞれ以下の設定項目があります。

:
RADIUS アカウンティングサーバの番号。以下のメニューが適用されます。

Enabled :
Enable このメニューに☑を入れると、RADIUS アカウンティングサーバが「有効」になります。

IP Address/Hostname :
RADIUS アカウンティングサーバの IP アドレス、またはホスト名。IP アドレスは、10 進表記で表記されます。

Port :
RADIUS アカウンティングサーバ用の UDP ポート。ポートを「0」に設定すると、初期設定のポート(1813)が RADIUS アカウンティングサーバ上で使用されます。

Secret :
RADIUS アカウンティングサーバとスイッチスタック間で最大 29 文字のシークレットが共有します。

TACACS+ Authentication Server Configuration

TACACS+認証サーバにはそれぞれ以下の設定項目があります。
:
TACACS+認証サーバ。以下のメニューが適用されます。

Enabled :
このメニューに☑を入れると、TACACS+認証サーバが「有効」になります。

IP Address/Hostname :
TACACS+認証サーバの IP アドレス、またはホスト名。 IP アドレスは、10 進表記で表記されます。

Port :
TACACS+認証サーバ用の TCP ポート。ポートを「0」に設定すると、初期設定のポート(49)がTACACS+認証サーバで使用されます。

Secret :
TACACS+認証サーバとスイッチスタック間で最大 29 文字のシークレットが共有します。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

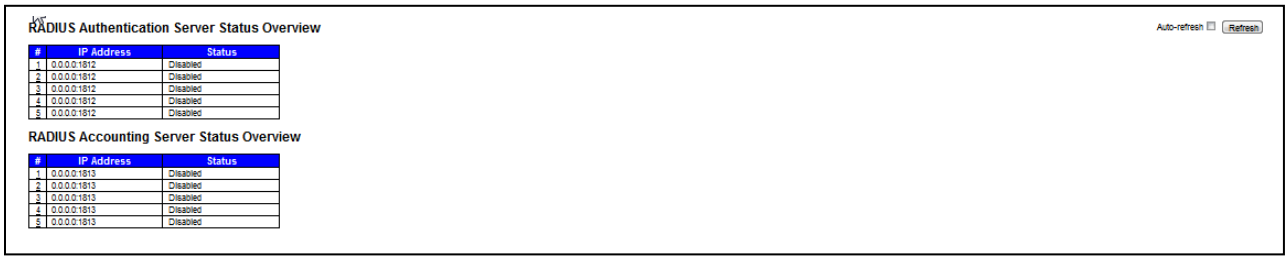
3.6.2 Radius Overview

機能が正常に動作しているかどうかを確認するために、RADIUS 認証およびアカウントサーバのステータスについて説明します。

設定方法

RADIUS Overview Configuration を設定するには、以下の手順に従ってください。
Step 1. [Security]→[AAA]→[Radius Overview]をクリックすると、以下の画面が表示されます。
<Auto-reflash>に☑を入れると、自動的更新されます。

Figure 4.6.2:　The RADIUS Authentication Server Status Overview



設定/表示項目

:
RADIUS サーバの番号。サーバの詳細な統計情報について表示されます。

IP Address :
サーバの IP アドレスおよび UDP ポート番号 (<IP Address>:<UDP Port>表記)

State :
サーバの現行の状態。以下の値のいずれかを選択してください。
Disabled: サーバは「無効」。
Not Ready: サーバは「有効」。だだし、IP 通信確認ができていない状態です。
Ready: サーバは有効。だだし、IP 通信確認ができていない状態です。RADIUS モジュールはアクセス可能な状態です。
Dead (X seconds left): サーバにアクセスを試行しますが、設定したタイムアウト内に応答がなかったためサーバは一時的に「無効」の状態ですが、デッドタイムを過ぎると再度「有効」になります。この状態になるまでの残り時間は”()”で表示されます。
複数のサーバが「有効」な場合のみこの状態になります。複数のサーバが使用可能な状態になった場合のみ、この状態はなります。

RADIUS Accounting Servers
:
RADIUS サーバの番号。サーバの詳細な統計情報が表示されます。

IP Address :
サーバの IP アドレスおよび UDP ポート番号(<IP Address>:<UDP Port> 表記)
State :

サーバの現行の状態。以下の値のいずれかに設定してください。
Disabled: サーバを「無効」です。
Not Ready: サーバは「有効」。だだし、IP 通信確認ができていない状態です。
Ready: サーバは「有効」です。
だだし、IP 通信確認ができていない状態です。 RADIUS モジュールはアカウンティングを受信可能な
状態です。

Dead (X seconds left):
このサーバにアカウンティングを実行しましたが、設定した時間内に応答がなかったため、一時的に使用不可の状態となりますが、dead-time を過ぎると、再度使用可能な状態になります。
この状態になるまでの残り時間が秒単位で表示されます。複数のサーバが使用可能な状態になった場合のみ、この状態はなります。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

3.6.3 Radius Detalls

RADIUS 認証およびアカウントサーバの詳細な統計情報が表示されます。
統計情報は、RFC4668 に規定された RADIUS 認証クライアント MIB に基づいています。

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

設定方法

RADIUS の設定を行うには、以下の手順に従ってください。
Step 1.　[Security]→[AAA]→[Radius Detalls]をクリックすると、以下の画面に表示されます。
Step 2.　<Auto-reflash>に☑を入れると、自動更新されます。

Figure 3.6.3:　The RADIUS Authentication Statistics

RADIUS Authentication Statistics

Receive Packets		Transmit Packets	
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		

Other Info	
IP Address	0.0.0.0:1812
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		

Other Info	
IP Address	0.0.0.0:1813
State	Disabled
Round-Trip Time	0 ms

設定/表示項目

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, Clear):
<Refresh>ボタンをクリックすると、情報が更新されます。<Clear>ボタンをクリックすると、すべてのエントリが削除されます。

3.7 Port Security

本機のポートセキュリティの設定について説明します。
ポートセキュリティの機能を使って、MAC アドレスを制限することにより、インタフェースへ入力を制限します。

3.7.1 Limit Control

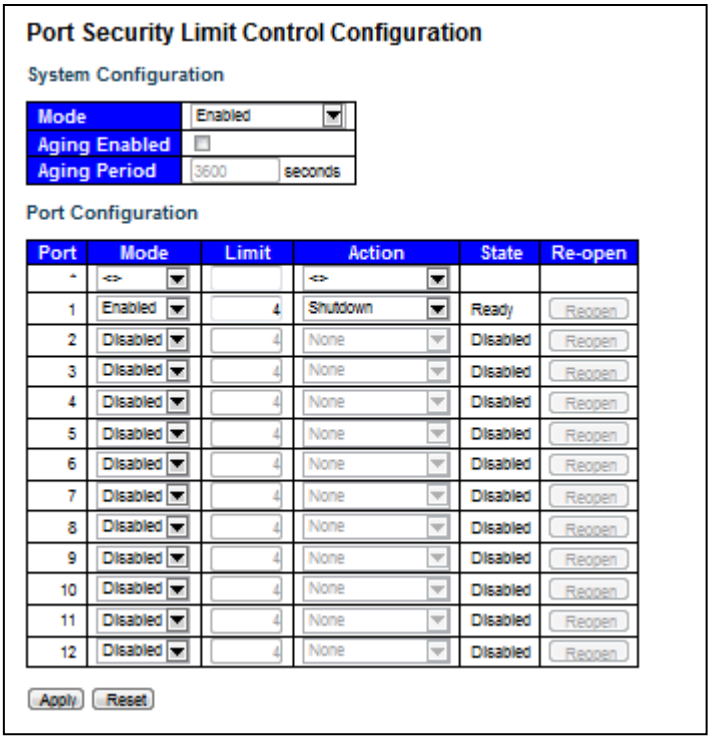
本機のポートセキュリティの設定方法について説明します。ポートセキュリティ機能を使って、MAC アドレスを制限することにより、インタフェースへ入力を制限します。

設定方法

リミット制御のシステム設定を行うには、以下の手順に従ってください。
[Security]→[Port Security]→[Limit Control]をクリックすると、以下の画面が表示されます。
Step 1. システム設定のモードを「Enabled」にします。
Step 2. 「Aging Enabled」に☑を入れます。
Step 3. Aging Period」の値を入力します(初期設定は 3600 秒)。

リミット制御のポート設定を行うには、以下の手順に従ってください。
Step 1. ポート設定のモードを「Enabled」にします。
Step 2. ポートのリミットでは、MAC アドレスの上限を入力します。
Step 3. アクションを設定します(Trap、Shutdown、Trap および Shutdown)。
Step 4. <Apply>ボタンをクリックします。

Figure 3.7.1:　Port Security Limit Control Configuration



設定/表示項目

System Configuration Mode :
スイッチスタックのリミット制御がグローバル設定で有効/無効を示します。グローバル設定で「無効」の場合は、その他のモジュールは基本機能を使用しますが、チェックを制限するため対応するアクションは無効になります。

Aging Enabled :
このメニューに☑を入れると、セキュア MAC アドレスはエイジングタイム内でエイジングを行います。

Aging Period :
このメニューに☑を入れると、エイジングタイムは、この入力した値によって制御されます。その他のモジュールがセキュア MAC アドレスの基本的なポートセキュリティを使用している場合は、エイジングタイムに対する他の要件があります。基本的なポートセキュリティは機能を使用するすべてのモジュールよりもエイジングタイムが短くなります。エイジングタイムは、「10」～「10,000,000」間の値になります。

Port Configuration
テーブルには、スタック内の選択されたスイッチのポートごとに設定します。

Port :
以下の設定が適用されるポート数。

Mode :
ポートのリミット制御を設定します。リミット制御を有効にしたい場合は「enable」に設定してください。指定のポートでリミット制御を有効にしないで、基本的なポートセキュリティ機能を使用している可能性があるため注意してください。

Limit :
ポートで設定可能な MAC アドレスの上限。 値は「1024」以下に設定してください。制限を超えると、対応する処置が行われます。
新規の MAC アドレスが Port Security-enabled ポートに表示されると、その分の MAC アドレス数がスタックスイッチの各ポートの MAC アドレスの合計数から差し引かれます。
すべてのポートが同じテーブルから差し引かれるため、ポートがすでに使用可能な MAC アドレスを使用している可能性があるため、設定した上限は認められません。

Action :
上限に達すると、スイッチは次のいずれか実行します。
None: ポートの MAC アドレスの制限値を超えることは許可されず、以降のアクションは実行しません。

Trap:
Limit + 1 の MAC アドレスを受信した場合は、SNMP トラップが送信されます。エイジングが無効な場合は、SNMP トラップが 1 つのみ送信されます。エイジング有効な場合は、トラップが送信され、新しい SNMP トラップが制限を超えたすべてに送信されます。
Shutdown: Limit + 1 の MAC アドレスを受信した場合は、ポートはシャットダウンされます。

すべてのセキュア MAC アドレスがポートから取り除かれ、新しいアドレスは学習されません。リンクが物理的に接続されず、再度ポートに接続した場合は、ポートはシャットダウンされた状態になります。ポートを再度開く方法は 3 つあります。
1. スタックを再起動するか、新しいスイッチをマスターに設定します。
2. ポート、またはスタックスイッチ上のポートのリミット制御は、無効にするか、または再度有効にします。
3. <Reopen>ボタンをクリックします。

Trap & Shutdown:
Limit + 1 MAC アドレスを受信すると、上記のとおり"Trap"および"Shutdown"が実行されます。

State :
ポートのリミット制限での現行の状態が表示されます。以下の 4 つの値のいずれかをとります。
Disabled: リミット制御はグローバル設定でも、ポート上でも「無効」になります。
Ready: 上限に達していないため、すべてのアクションが表示されます。
Limit Reached: ポートの上限に達したことを示します。”Action”の項目に「None」または「Trap」を設定した場合、その内容に応じて実行します。
Shutdown: ポートがリミット制御モジュールによりシャットダウンされたことを示します。”Action”の項目に「Shutdown」または「Trap & Shutdown.」を設定した場合、その内容に応じて実行します。

Re-open Button :
ポートはこのモジュールでシャットダウンされた場合は、このボタンをクリックして再度開くことができます。この場合は「enable」に設定してください。その他の方法については、「Action」の「Shutdown」を参照ください。

【注記】:
「reopen」ボタンをクリックすると、画面が更新されます。
確定されていない変更内容は消えてましまいます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

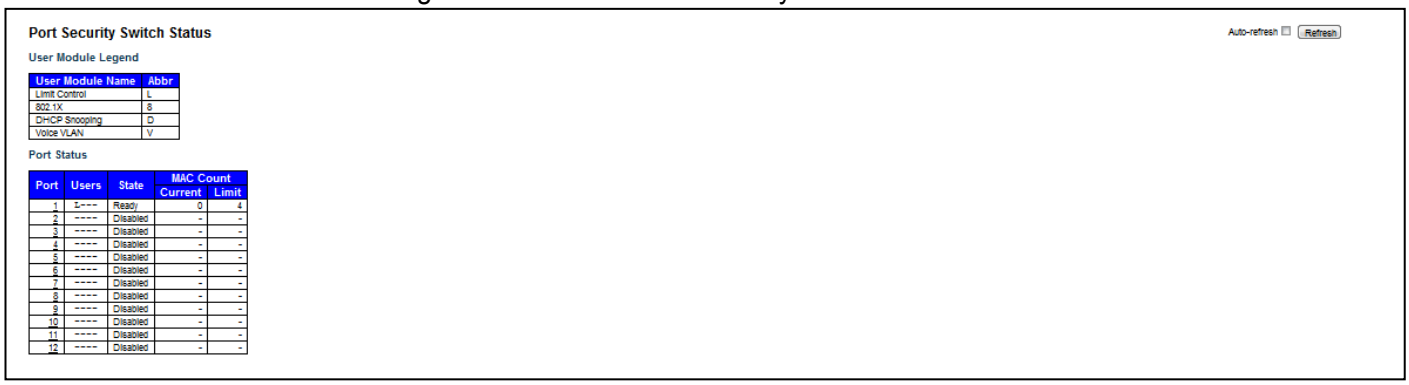
3.7.2 Switch Status

ポートセキュリティのステータスが表示されます。ポートセキュリティは、直接設定を行いわず、他のモジュール（ユーザモジュール）で間接的に設定を行います。
アンノウン MAC アドレスからのフレームはポートセキュリティモジュールにパスされます。これにより、すべてのユーザモジュールに新規MACアドレスを伝送するか、ブロックするかを確認します。MAC アドレスを伝送状態にする場合は、有効なユーザモジュールがすべて MAC アドレスを伝送することに合意する必要があります。1つでもブロックすると、ユーザモジュールが伝送を許可するまでブロックされた状態になります。このステータス画面は、2 つの項に分けられ、1 つはユーザモジュール、もう 1 つは実際のポートステータスについてそれぞれ説明します。
ません。

設定方法

ポートセキュリティのスイッチのステータス を設定するには、以下の手順に従ってください。
Step 1. [Security]→[Port Security]→[Switch Status]をクリックすると、以下の画面が表示されます。<Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.7.2:　The Port Security Switch Status



設定/表示項目

User Module Legend :
ポートセキュリティサービスを要求するユーザモジュールのすべてが表示されます。

User Module Name :
ポートセキュリティサービスを要求するモジュールの完全名.

Abbr :
ユーザモジュールの一文字略語。これは、ポートステータステーブルのユーザの項で使用されます。

Port Status :
テーブルには、スタック内の選択したスイッチのポートごとに表示します。

Port :
ステータスに適用されるポート番号。ポート番号をクリックすると、特定のポートのステータスが表示されます。

Users :
ユーザモジュールにはそれぞれポートセキュリティの有効/無効を切り替えることができます。'-'は、対応するユーザモジュールが「無効」であることを示します。ここでは、”Abbr”内の文字はユーザモジュールの略語で、ポートセキュリティは「有効」であることを示します。

State :
ポートの現行の状態を示します。以下の 4 つの値あら選択してください
Disabled: 現在ポートセキュリティサービスを使用したユーザモジュールはありません。
Ready: ポートセキュリティサービスは、少なくとも複数のユーザモジュールで使用中で、アンノウン MAC アドレスからのフレームの受信を待機している状態です。

Limit Reached:
ポートセキュリティサービスは、リミット制御ユーザモジュールにより「有効」です。
モジュールは、限界に近づいることを表し、MAC アドレスは受信されません。

Shutdown:
ポートセキュリティサービスは、リミット制限ユーザモジュールにより「有効」です。
制限を超えていることを示します。WEB 画面上でリミット制限設定が管理上再度オープンされない限り、MAC アドレスがポート上で学習されません。

MAC Count (Current, Limit) :
2 つのメニューでは、現在学習している MAC アドレス数の数（伝送およびブロックされた数）およびポート上で学習可能な MAC アドレス数の限度がそれぞれ表示さます。
ポート上で有効なユーザモジュールがない場合は、”(-)”が表示されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh):
<Refresh>ボタンをクリックすると、情報が更新されます。

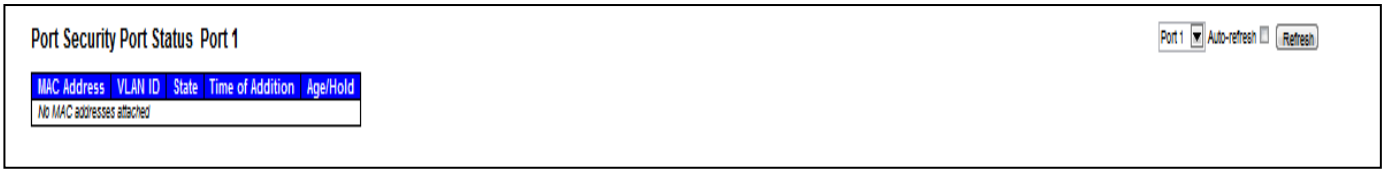
3.7.3 Port Status

ポートセキュリティモジュールによる MAC アドレスについて説明します。
ポートモジュールは、直接設定を行わず、他のモジュール（ユーザモジュール）で間接的に設定を行います。
アンノウン MAC アドレスからのフレームはポートセキュリティモジュールにパスされます。これにより、すべてのユーザモジュールに新規MACアドレスを伝送するか、ブロックするかを確認します。MAC アドレスを伝送状態にする場合は、有効なユーザモジュールがすべて MAC アドレスを伝送することに合意する必要があります。1つでもブロックすると、ユーザモジュールが伝送を許可するまでブロックされた状態になります。

設定方法

ポートセキュリティのステータスを設定するには、以下の手順に従ってください。
Step 1. [Security]→[Port Security]→[Port Status]をクリックすると、以下の画面が表示されます。
モニタしたポート番号を指定します。
Step 2. <Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.7.3:　The Port Security Port Status



設定/表示項目

MAC Address & VLAN ID :
ポートの MAC アドレスおよび VLAN ID。MAC アドレスを学習しない場合は、"No MAC address attached"と表示されます。

State :
対応する MAC アドレスがブロックされたか、伝送されたかどうかが表示されます。ブロック状態の場合は、トラフィックの送受信を行いません。

Time of Addition :
ポートで MAC アドレスが最初に受信された日時が表示されます。

Age/Hold :
複数のユーザモジュールが MAC アドレスのブロックを行う場合は、hold time（数秒間）が切れるまでブロック状態のままです。すべてのユーザモジュールは、MAC アドレスを伝送し、エイジングを有効にする場合は、ポートセキュリティモジュールは MAC アドレスによりトラフィックが伝送されているかどうかを定期的にチェックします。
エイジンングタイム（秒単位）が切れても、フレームが伝送されない場合は、MAC アドレスは MAC テーブルから取り除かされます。新しいエイジングが開始します。

エイジングが「無効」、またはユーザモジュールが MAC アドレスを無制限に保持している場合は、”(-)”と表示されます。

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。
Upper right icon (Refresh):

3.8 Acess Management

HTTP/HTTPS、 SNMPおよびTELNET/SSHなどのスイッチのアクセス管理テーブルの方法について説明します。 イーサネット LAN、インターネットを介して、スイッチを管理することが可能です。

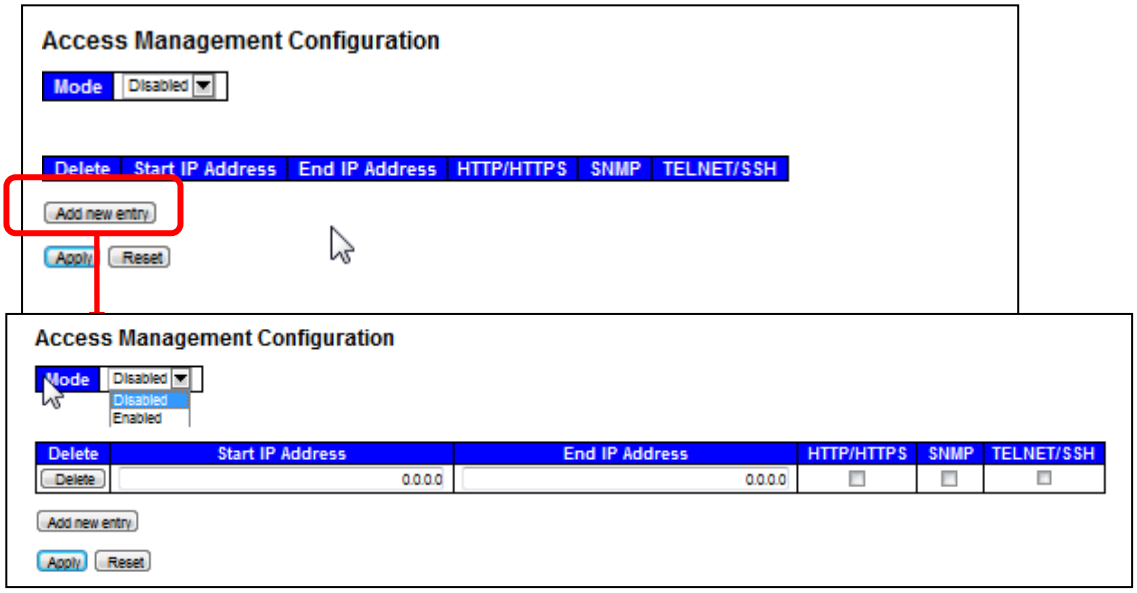
3.8.1 Configuration

スイッチのアクセス管理テーブルの方法について説明します。
最大エントリ数は「16」です。アプリケーションのタイプがアクセス管理エントリのいずれかと一致した場合は、スイッチへのアクセスが可能になります。

設定方法

アクセス管理を設定するには、以下の手順に従ってください。
Step 1. [Security]→[Access Management]→[Configration]をクリックすると、以下の画面が表示されます。アクセス管理設定のモードを「Enabled」にします。
Step 2. <Add new entry>ボタンをクリックします。
Step 3. 「Start IP Address」、「End IP Address」を指定します。
Step 4. アクセス管理方式(HTTP/HTTPS、SNMP および TELNET/SSH)を指定します。
Step 5. <Apply>ボタンをクリックします。

Figure 3.8.1:　The Access Management Configuration



設定/表示項目

Mode :
アクセス管理モードが表示されます。
Enabled: アクセス管理モードを「有効」にします。
Disabled: アクセス管理モードを「無効」にします。

Delete :
削除したい項目を選択して、 <Apply>ボタンをクックすると削除されます。

Start IP address :
アクセス管理エントリの開始 IP アドレスが表示されます。

End IP address :
アクセス管理エントリの終了 IP アドレスが表示されます。

HTTP/HTTPS :
ホスト IP アドレスが IP アドレスの範囲内の場合、HTTP/HTTPS インタフェースからスイッチにアクセス可能なホストが表示されます。

SNMP :
ホスト IP アドレスが IP アドレスの範囲内の場合、SNMP インタフェースからスイッチにアクセス可能なホストが表示されます。

TELNET/SSH :
ホスト IP アドレスが IP アドレスの範囲内の場合、TELNET/SSH インタフェースからスイッチにアクセス可能なホストが表示されます。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

3.8.2 Statistics

HTTP、HTTPS、SSH、TELNET および SSH などのアクセス管理の統計情報の詳細について表示します。

設定方法

アクセス管理機能を設定するには、以下の手順に従ってください。

Step 1. [Security]→[Access Management]→[Statics]をクリックすると、以下の画面が表示されます。
<Auto-reflash>に☑を入れると、自動的更新されます。

Figure 3.8.2:　The Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

設定/表示項目

Interface :
スイッチにアクセス可能なリモートアクセスを介したインタフェースタイプ。

Received Packets :
アクセス管理モードが「有効」な場合のインタフェースから受信したパケット数

Allowed Packets :
アクセス管理モードが「有効」な場合の　インタフェースから許可されたパケット数

Discarded Packets. :
アクセス管理モードが「有効」な場合のインタフェースから破棄されたパケット数

Auto-refresh :
「Auto-refresh」に☑を選択した場合は、情報が自動更新されます。

Upper right icon (Refresh, Clear):
<Refresh>ボタンをクリックすると、情報が更新されます。<Clear>ボタンをクリックすると、すべてのエントリが削除されます。

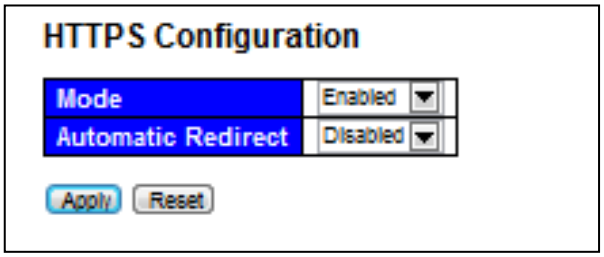
3.9 HTTPS

スイッチへのアクセス用に HTTP の設定方法について説明します。
HTTPS は、認証およびデータ暗号化を組み合わせたプロトコルで、ブラウザを介して暗号化された通信を提供します。

設定方法

HTTPS Configuration を設定するには、以下の手順に従ってください。
Step 1. HTTPS 設定のモードを「Enabled」にします。
Step 2. 「Automatic Redirect」項目を「Enabled」 に設定します。
Step 3. <Apply>ボタンをクリックします。

Figure 3.9.1:　The HTTPS Configuration



設定/表示項目

Mode :
HTTPS ノードが表示されます。
Enabled: HTTPS モードを「有効」にします。
Disabled: HTTPS モードを「無効」にします。

Automatic Redirect :
HTTPS リダイレクトモードが表示されます。HTTPS モードが「有効」な場合に、WEB ブラウザを HTTP に切り替えます。
Enabled: HTTPS のリダイレクトモードを「有効」にします。
Disabled: HTTPS のリダイレクトモードを「無効」にします。

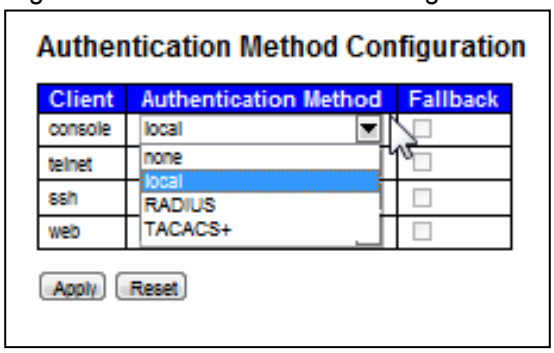
3.10 Auth Method

管理クライアントインタフェースのいずれかを介してスイッチスタックにログインする際、認証したユーザの設定方法について説明します。

設定方法

認証方式を設定するには、以下の手順に従ってください。
Step 1. モニタしたいクライアント(コンソール, telent, ssh, web) を選択します。
Step 2. 認証方式を「none」、「local」、「radius」、「tacacs+」から選択します。
Step 3. 「Fallback」に☑を入れ、 <Apply>ボタンをクリックします。

Figure 3.10.1:　The HTTPS Configuration



設定/表示項目

Client :
設定を行う管理クライアントは下記を適用します。

Authentication Method :
認証方式は、以下の値のいずれかに設定してください。
None　: 認証は「無効」かつログイン不可
local　: 認証用にローカルユーザデータベースを使用
radius : 認証用にリモート RADIUS サーバを使用
tacacs+ : 認証用にリモート TACACS+サーバを使用

Fallback :
このメニュを有効にすると、ローカル認証のフォールバックが「有効」になります。
設定した認証サーバのいずれも設定できない場合は、認証にはローカルユーザデータベースが有効です。認証方式が'none' または 'local'以外の値に設定されている場合にのみ有効です。

Buttons:
Save – 変更内容を保存します。
Reset- <Save>をクリックする前の場合、ローカルに変更した内容を取り消して、元の値に戻します。

4章　メンテナンス

本機の再起動、ファームウェアのアップデート、保存/リストア、Import/Export, および診断機能などのローカルネットワークのパフォーマンスを上げるためのスイッチメンテナンス設定について説明します。

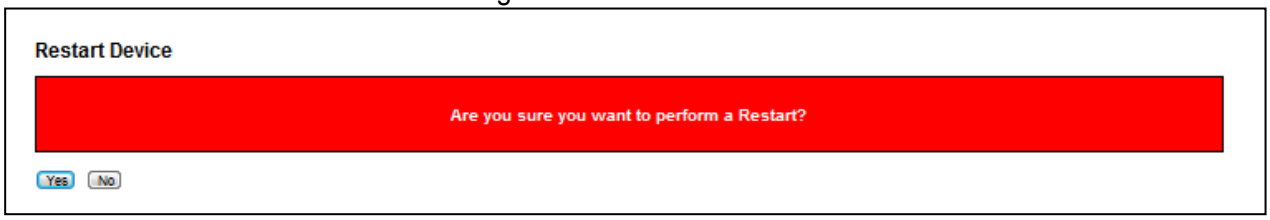
4.1 Restart Device

メンテナンスの要件として、スイッチの再起動の方法について説明します。本機に保存した設定ファイルまたはスクリプトは以降使用可能です。

設定方法

本機の再起動を行うには、以下の手順に従ってください。
Step　1. [Maintenance]→[Restart Device]をクリックします。
Step　2. <Yes>ボタンをクリックします。

Figure 4.1.1:　The Restart Device



設定/表示項目

Restart Device :
本機の再起動を行うことができます。再起動後自動的にブートします。

ボタン:
Yes – 本機は再起動します。
No　– 再起動は取り消されます。

4.2 Firmware

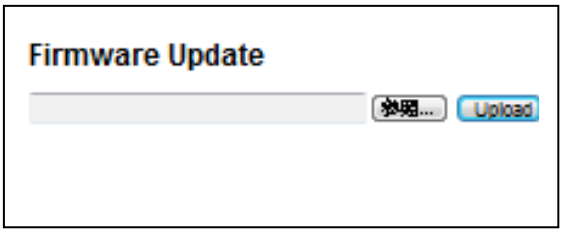
4.2.1 Firmware Upgrade

ファームウェアのアップグレード方法について説明します。本機では、ファームウェアのアップグレードを行うことにより、付加価値のある機能を提供します。

設定方法

ファームウェアのアップグレードを設定するには、以下の手順に従ってください。
[Maintenance]→[Firmware]→[Firmware Upgrade]をクリックすると以以下の画面が表示されます。
Step 1.　<参照…>ボタンをクリックして、ファームウェアを選択します。
Step 2.　<Upload>ボタンをクリックします。

Figure 4.2.1:　The Firmware update



設定/表示項目

ボタン ：
参照... – ファームウェアの URL およびファイル名を選択します。
Upload – お使いのパソコンまたはサーバに保存されているファームウェアのアップロードを開始します。

【注記】:
スタックスイッチを制御するファームウェアのアップロードを容易に行うことができます。ソフトウェアをアップロードすると、管理スイッチのソフトウェアがすべて更新されます。ソフトウェアイメージのアップロードが完了すると、画面にファームウェアのアップデートが開始された旨のメッセージが表示されます。1分後、ファームウェアは更新され、スタック内の管理スイッチはすべて再起動します。

WARNING:
ファームウェアがアップデートされている間、WEB へのアクセスが中断したようにみえます。また、ファームウェアのアップデート中は、前面の LED が 10 Hz ごとに点滅します。この時、デバイスを再起動したり、電源を切ったすると、正常にアップグレードできなくなる可能性があるため注意してください。

4.2.2 Firmware Selection

ファームウェアの選択を行うには、以下の設定を行ってください。

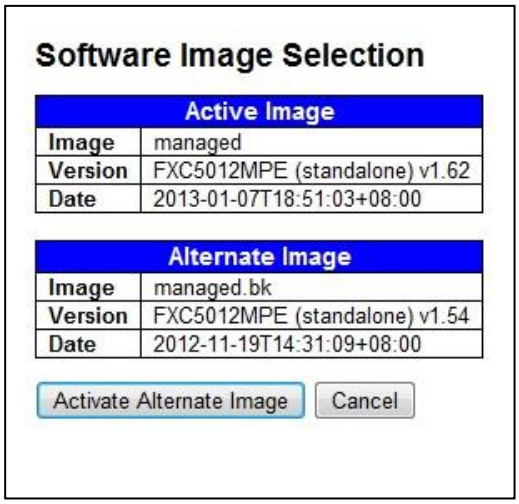
設定方法

ファームウェアの選択を行うには、[Maintenance]→[Firmware]→[Firmware Selection]をクリックします。

Step 1.　Activate Alternate Image ボタンをクリックします。

Step 2.　<OK>ボタンをクリックします。

4.2.2 firmware Selection



4.3 Save / Restore

メンテナンスに必要な操作として、reset to Factory Defaults, Save Start, Save User, Restore User などの本機の設定の保存、およびリストア方法について説明します。

4.3.1 Factory Defaults

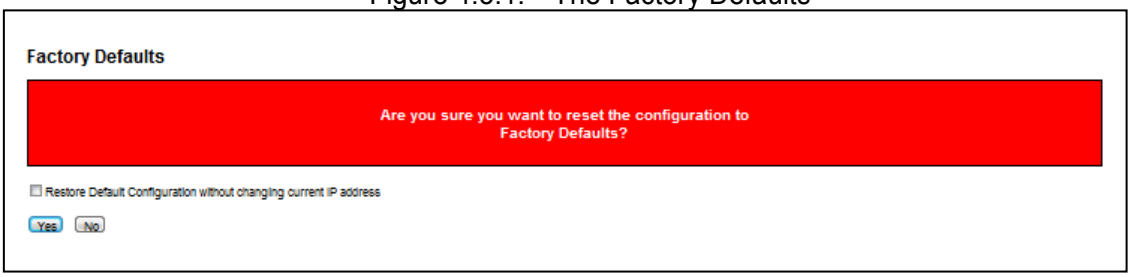
工場出荷時の設定に戻す方法について説明します。コンフィグレーションファイル、またはスクリプトをすべて初期設定に戻します。

設定方法

工場出荷時の設定に戻す方法は、以下の手順に従ってください。
Step 1. [Maintenance]→[Save/Restore]→[Factory Defaults]をクリックします。
Step 2. <Yes>ボタンをクリックします。
※ 現在設定されている IP アドレスを初期化したくない場合は、以下のチェックボックスにチェックを入れて<Yes>ボタンをクリックしてください。

☑ Restore Default Configuration without changing current IP address

Figure 4.3.1:　The Factory Defaults



設定/表示項目

ボタン:
Yes – リセットされ工場出荷時の設定に戻ります。
No –　設定をリセットせずに、「Port State」画面に戻ります。

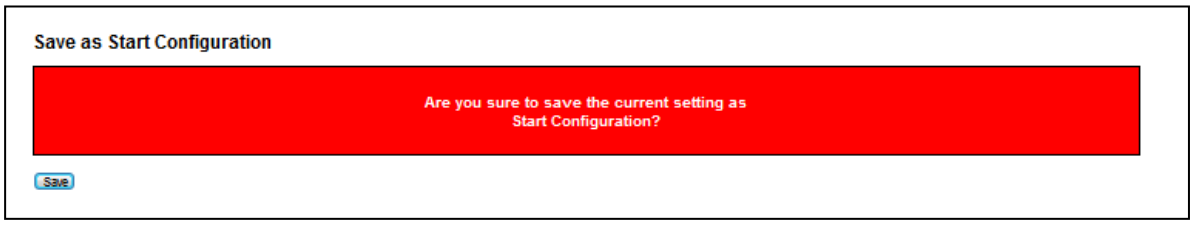
4.3.2 Save Start

本機の初期設定を保存する方法について説明します。現行の設定ファイルはすべて XML 形式で保存されます。

設定方法

初期設定を保存するには、以下の手順に従ってください。
Step 1. [Maintenance]→[Save/Restore]→[Save Start]をクリックします。
Step 2. <Yes>ボタンをクリックします。

Figure 4.3.2:　The Save Start configuration



設定/表示項目

ボタン:
Save – 現在の設定値が初期設定として保存されます。

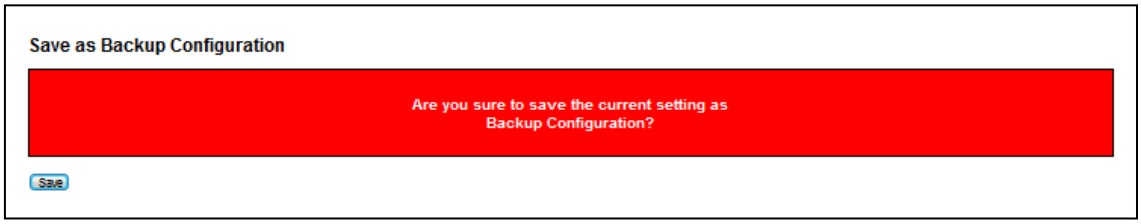
4.3.3 Save User

ユーザ情報の保存方法について説明します。現行の設定ファイルはすべて XML 形式で保存されます。

設定方法

ユーザ情報を保存するには、以下の手順に従ってください。
Step 1.　[Maintenance]→[Save/Restore]→[Save User]をクリックします。
Step 2.　<Yes>ボタンをクリックします。

Figure 4.3.3:　The Save as Backup Configuration



設定/表示項目

ボタン:
Save – 現行の設定値をバックアップとして保存します。

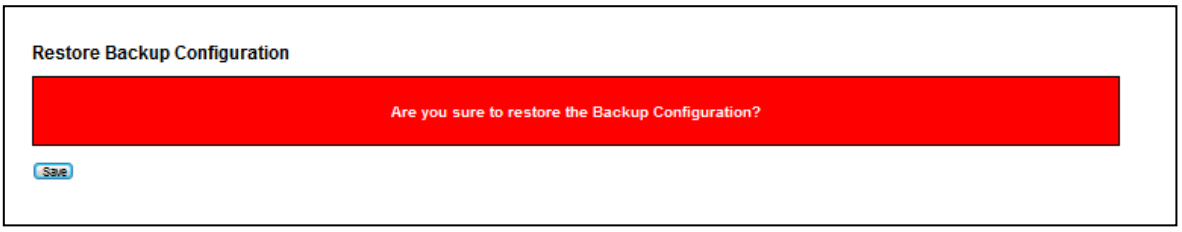
4.3.4 Restore User

ユーザ情報のリストア方法について説明します。現行のコンフィグレーションファイルはすべて XML 形式でリストアされます。

設定方法

ユーザによる設定情報を保存するには、以下の手順に従ってください。
Step 1. [Maintenance]→[Save/Restore]→[Restore User]をクリックします。
Step 2.<Yes>ボタンをクリックします。

Figure 4.3.4:　The Restore the Backup Configuration



設定/表示項目

ボタン:
Save – 本機のバックアップにリストアします。

4.4 Export / Import

本機の設定のエクスポート/インポート方法について説明します。現行の設定ファイルはすべて XML 形式で保存されます。

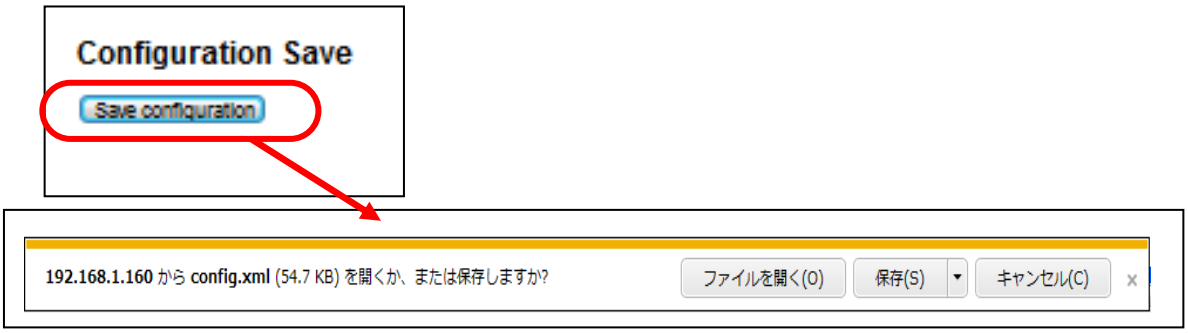
4.4.1 Export Config

メンテナンスの要件に応じて、本機の設定のエクスポートの方法について説明します。
現行の設定ファイルはすべて XML 形式で保存されます。

設定方法

エクスポート設定を行うには、以下の手順に従ってください。
Step 1. [Maintenance]→[Export/Import]をクリックします。
Step 2. 画面下にメッセージが表示されますので、＜保存＞をクリックして、お使いのデバイスにファイルを保存します。

Figure 4.4.1:　The Restore the Backup Configuration



設定/表示項目

ボタン:
保存 – お使いのパソコンまたはサーバに設定値を保存します。

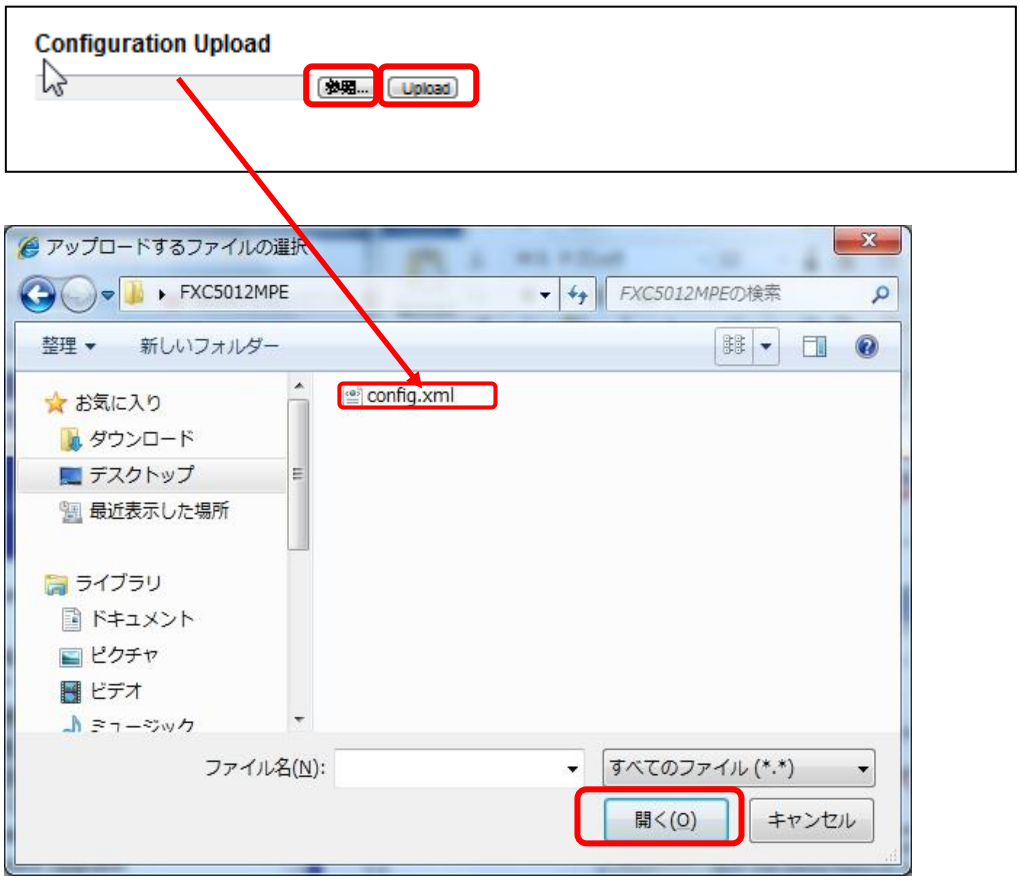
4.4.2 Import Config

メンテナンスの要件として、本機の設定のインポート方法について説明します。現行の設定ファイルはすべて XML 形式で保存されます。

設定方法

インポート設定を行うには、、以下の手順に従ってください。
Step 1.　<参照…>をクリックして、お使いのデバイスのコンフィグレーションファイルを選択します。
Step 2.　<開く>をクリックします。
Step 3. <Upload>ボタンをクリックします。

Figure 4.4.2:　The Import Config



設定/表示項目

ボタン ：
参照...　ー　設定したい URL およびファイル名を選択します。
Upload　ー　パソコンまたはサーバに保存された設定のアップロードを開始します。

4.5 Diagmostics

基本的なシステムの診断機能について説明します。ユーザはシステムに問題がないか確認することが可能です。基本的なシステムチェックには、ICMP Ping、ICMPv6 および VeriPHY ケーブル診断機能があります。

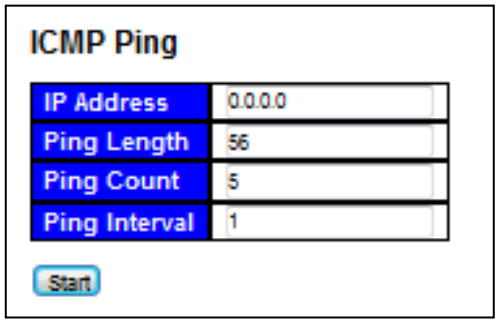
4.5.1 Ping

IPv6 接続用のトラブルシューティングには、ICMP PING パケットを発行することができます。

設定方法

ICMP PING を行うには、以下の手順に従ってください。
[Diagnostics]→[Ping]をクリックすると、以下の ICMP Ping 画面が表示されます。
Step 1. IP Address に IP アドレスを入力します。
Step 2. Ping Length にパケットサイズを入力します。
Step 3. <Start>ボタンをクリックします。

Figure 4.5.1:　The ICMP Ping



設定/表示項目

IP Address:
Ping を行いたいデバイスの IP アドレスを設定します。

Ping Length:
ICMP のパケットサイズを設定して、その他のデバイスに ping を行います。

Start:]本機に設定されている ICMP パケットサイズを使って、デバイスの ping を開始します。
ICMP パケットが 5 つ送信され、応答を受信するとシーケンス番号、往復時間が 表示されます。すべてのパケットの応答がすべて受信されるか、タイムアウトすると、画面は自動的に更新されます。

PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

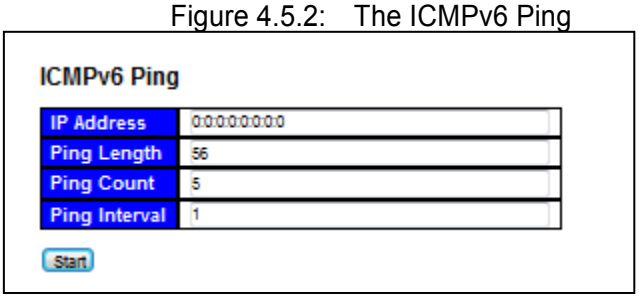
4.5.2 Ping6

IPv6 接続性についての問題のトラブルシューティングを行うには、ICMPv6 PING パケットを発行することができます。

設定方法

[Diagnostics]→[Ping6]をクリックすると、以下の ICMPv6 Ping 画面が表示されます。
Step 1. IP Address に IP アドレスを入力します。
Step 2. Ping Length にパケットサイズを入力します。
Step 3. <Start>ボタンをクリックします。

Figure 4.5.2:　The ICMPv6 Ping



設定/表示項目

IP Address :
IPv6 をもつ宛先 IP アドレス

Ping Size :
ICMP パケットのペイロードサイズ。設定可能な値は、「8 バイト」～「1400 バイト」です。

Start:
本機に設定されている ICMP パケットサイズを使って、デバイスの ping を開始します。

ICMP パケットが 5 つ送信され、応答を受信するとシーケンス番号、往復時間が表示されます。全てのパケットの応答がすべて受信されるか、タイムアウトすると、画面は自動的に更新されます。
PING server 10.10.132.20
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

4.5.3 VeriPHY

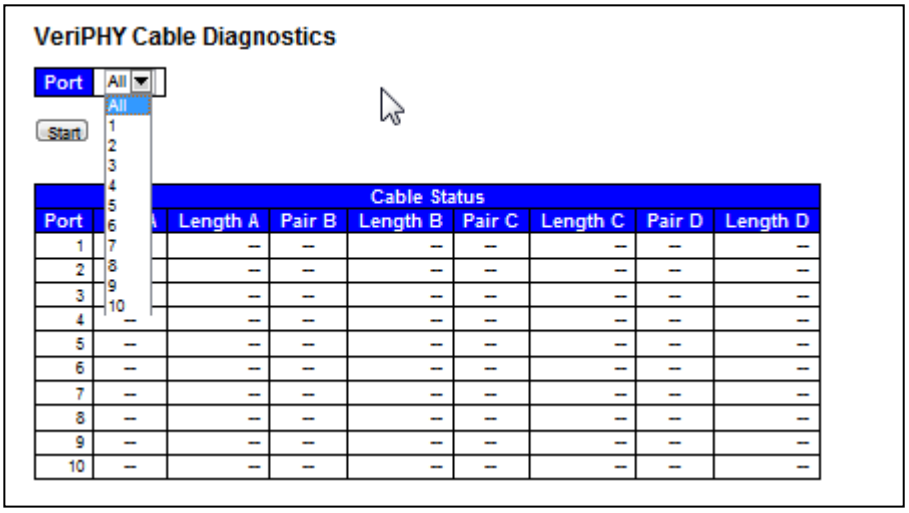
VeriPHY ケーブル診断について説明します。 ポートをすべて選択した場合約「15 秒」かかります。
診断が完了すると、画面は自動的に更新され、ケーブル診断表にその結果が表示されます。

【注記】:
VeriPHY は、ケーブルの長さが 7 ～140 メートルの範囲内でのみ有効です。10/100Mbps ポートは、VeriPHY が動作中にリンクダウンするため、10/100Mbps 管理ポート上で VeriPHY が動作している場合は、本機は VeriPHY が完了するまで応答をストップします。

設定方法

VeriPHY ケーブル診断機能を設定するには、以下の手順に従ってください。
Step 1. チェックしたいポートを指定します。
Step 2. <Start>をクリックします。

Figure 4.5.3:　The VeriPHY



設定/表示項目

Port :
VeriPHY ケーブル診断を行いたいポートを指定します。
Cable Status :
Port: ポート番号
Pair: ケーブルペアのステータス
Length: ケーブルペアの長さ (メートル単位)

5章 コマンドインタフェース

5.1 コマンドラインインタフェースの利用

5.1.1 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。
ただし、コマンドラインインタフェースで設定できる機能は下記の項目のみです。
各項目の概略は、「5.1.3 コマンド上でのヘルプの表示」を参照してください。
すべての設定が可能なのは WEB インタフェースからのみとなります。

auto-logout
diagnostic
exit
help
history
Ip
ipv6
Logout
reboot
restore
save
system

5.1.2 コンソール接続

コンソールポートへの接続は以下の手順で行います。

接続方法

1. 機器背面の左部のコンソールポートに同梱のコンソールケーブルのを接続します。
2. 片方を PC などの COM ポートに接続します。
3. PC の COM ポートをターミナルエミュレータで開きます。
   (COM ポート番号は PC で確認してください。)

   下記設定値を設定してください。

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

（1）コンソールプロンプトでユーザ名とパスワードを入力します。初期設定のユーザ名は"admin"、パスワードも同じく"admin"となっています。
（2）ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。
（3）終了時には"quit"又は"exit"コマンドを使用しセッションを終了します。
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が表示されます。

5.1.3 Telnet 接続

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

【注意】:
工場出荷時には、本機は **DHCP** サーバー経由で **IP** アドレスが割り振られる設定に なっています。

IP アドレスとデフォルトゲートウェイの設定例は以下の通りです。
本機を外部と接続されたネットワークに接続する場合には、登録された IP アドレスを設定する必要があります。独立したネットワークの場合には内部で自由に IP アドレスを割り当てることができます。
本機の IP アドレスを設定した後、以下の手順で Telnet セッションを開始することができます。
(1)リモートホストから Telnet コマンドと本機の IP アドレスを入力します。

(2)プロンプト上でユーザ名とパスワードを入力します。ログインすると Switch#”と表示されます。
(3)ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。
(4)終了時には"quit"又は"exit"コマンドを使用しセッションを終了します。
【注意】:　同時に最大 4 セッションまでの Telnet 接続が可能です。

5.1.4 コマンド上でのヘルプの表示

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

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

account	管理アクセスの基本ユーザ名、パスワードを設定を行います。 詳細については、「5.1.3.1　ACCOUNT Commands of CLI」を参照ください。
auto-logout	自動ログアウトする前に動作していない時間を設定します。
diagnostic	診断ツールが表示されます。詳細については、「5.1.3.2 Diagnostic Commands of CLI」を参照してください。
exit	前の設定モードに戻るか、または CLI セッションを終了します。
help	コマンド上で"help"コマンドを入力することで、簡単なヘルプ情報が表示されます。また"?"と入力するとキーワードやパラメータのコマンド文法が表示されます。
history	過去に使用したコマンドのリストが表示されます。
Ip	システムのインターネットプロトコルが表示されます。詳細については、「5.1.3.3 IP Commands of CLI」を参照してください。
ipv6	システムの ipv6 アドレスが表示されます。 詳細については、「5.1.3.4 IPV6 Commands of CLI」を参照してください。
Logout	ログアウト(接続を解除)します。
reboot	本機の再起動を行います。
restore	Default　-　工場出荷時の設定に戻します。 user　　-　ユーザ設定値に戻します。
save	Start　　-　実行中の設定を初期設定値として保存します。 user　　-　実行中の設定をユーザ設定値として保存します
system	システム情報が表示されます。 詳細については、「5.1.3.5 SYSTEM of CLI」を参照してください。

5.1.4.1 ACCOUNT

Account Commands

コマンド	機　能
add	ユーザのアカウントを追加/修正します。
delete	ユーザのアカウントを削除します。
show	ユーザのアカウント情報が表示されます。

add　ユーザのアカウントを追加/修正します。

SYNTAX

add guest *<1-15> <word>*

Parameter

<1-15>　ユーザの優先順位を示します。

<WORD> ユーザ名用に最大32文字まで使用可能です。

例

```
Switch(account)# show
User Name                    Privilege Level
------------------  ----------------------------  ------------
admin                                   15
Switch(account)#
```

delete　新規ユーザを設定するには、パスワードを入力後確認してください。

SYNTAX

delete <WORD>

Parameter

ユーザ名用に最大 32 文字まで使用可能です。

例:

```
Switch(account)# delete 12
Switch(account)# show
User Name                       Privilege Level
-------------------------------- ----------------
```

show　ユーザのアカウント情報が表示されます。

SYNTAX

Show <*name*>

例:

```
Switch(account)# show
User Name                       Privilege Level
-------------------------------- ----------------
admin                                     15
Switch(account)#
```

auto-logout　自動ログアウトするまでの時間を設定します。

例:

```
Switch# auto-logout 300
```

5.1.4.2 Diagnostic

コマンド	機　能
Ping	Ping コマンドを発行して、ネットワーク診断を行います。
ping6	Ipv6 の Ping コマンドを発行して、ネットワーク診断を行います。

Ping　Ping コマンドを発行して、ネットワーク診断を行います。

SYNTAX

ping <ip-hostname>　<2-1452>

Parameter

<ip-hostname>　ホスト名、または IP アドレス
<2-1452>　ICMP のエコーパケットのサイズ

例:

```
Switch(diagnostic)# ping 192.168.1.6 60
PING server 192.168.1.6
recvfrom: Operation timed out
```

Ping6　Ipv6 の Ping コマンドを発行して、ネットワーク診断を行います。

SYNTAX

Ping6<ip-hostname> <60-1400>

Parameter

<ip-hostname>　ホスト名、または IP アドレス
<2-1452>　ICMP のエコーパケットのサイズ

例:

```
Switch(diagnostic)# ping6 192.168.1.1 60
PING6 server ::44ed:d80:e816:fc80
sendto
```

5.1.4.3 IP Commands of CLI

コマンド	機　能
dhcp	DHCP クライアントを有効/無効にします。
mgmt-vlan	管理用 VLAN ID を設定します。
name-server	DNS の IP アドレスを設定します。
dns-proxy	DNS プロキシーの設定をします。
setup	IP アドレスを設定します。
show	IP 情報が表示されます。

Dhcp　DHCP クライアントを有効/無効にします。

SYNTAX

Dhcp *<disable><enable>*

Parameter

disable　DHCPクライアントを「無効」にします。

enable　DHCPクライアントを「有効」にします。

例:

```
Switch(ip)# dhcp enable
Switch(ip)#
```

mgmt-vlan　管理用 VLAN ID を設定します。

SYNTAX

mgmt-vlan <1-4094>

Parameter

<1-4094>　管理用VLAN ID（使用可能範囲:1 ～ 4094秒）

例:

```
Switch(ip)# mgmt-vlan 1
Switch(ip)#
```

name-server　DNS の IP アドレスを設定します。

SYNTAX

name-server <ip-address>

Parameter

<ip-address>　DNS IP address

例:

```
Switch(ip)# name-server 168.95.1.1
Switch(ip)#
```

dns-proxy　DNS プロキシーの設定をします

SYNTAX

Dns-proxy <*disable*><*enable*>

Parameter

disable　dns-proxyを「無効」にします。

enable　dns-proxyを「有効」にします。

Setup　管理IPアドレスを設定します。

SYNTAX

Setup <ip-address><ip-mask><ip-address>

Parameter

<ip-address>　IPアドレス

<ip-mask>　IPサブネットマスク

<ip-address>　ゲートウェイIPアドレス

例:

```
Switch(ip)# setup 192.168.1.100 255.255.255.0 192.168.1.254
Switch(ip)#
```

show　IP 情報が表示されます。

SYNTAX

Show

例:

```
Switch(ip)# show
DHCP Client         : Enabled
Active Configuration : Static
IP Address          : 192.168.1.100
Subnet Mask         : 255.255.255.0
```

5.1.4.4 IPV6

コマンド	機　能
autoconfig	IPv6 の autoconfig モードを設定します。
setup	IPv6 アドレスを設定します。
Show	IPv6 情報が表示されます。

Autoconfig　IPv6 の autoconfig モードを設定します。

SYNTAX

Autoconfig *<disable><enable>*

Parameter

disable　autoconfigモードを「無効」にします。

enable　autoconfigモードを「有効」にします。

例:

```
Switch(ipv6)# autoconfig  disable
Switch(ipv6)#
```

Setup　管理 IPv6 アドレスを設定します。

SYNTAX

Setup <ipv6-address>

Parameter

<ipv6-address>

128 ビットを 16 ビットずつ 8 つに“:” (コロン)で区切った数値列を、16 進数で表記します。連続する“0” は省略可能です。また、“::” は 16 ビットの 0 が複数連続していることを示します。“::” は、どこでも使用できますが、省略できるのは一カ所のみです。

例)'::192.1.2.34'

<1-128>　IPv6 prefix

例

```
Switch(ipv6)# setup 2004::208  128
Switch(ipv6)#
```

show　　ipv6情報が表示されます。

SYNTAX

Show <config><current>

<config>　Ipv6設定情報が表示されます。

<current>　現在適用されているIpv6アドレスが表示されます。

例:

```
Switch(ipv6)# show current
Active Configuration for IPv6: (Static with Stateless)
Link-Local Address : fe80::0240:c7ff:fe1c:8a97
Address            : 2004::0208
Prefix             : 128
Gateway            : ::
```

5.1.4.5 SYSTEM

コマンド	機　能
show	システム情報が表示されます。

contact　システム担当者を設定します。

Syntax

contact *<system contact information>*

Parameter

<system contact information>　システム担当者の情報を最大 255 文字まで入力します。

例:

```
Switch(system)# contact administrator
Switch(system)# show
Model Name                : PSGS-2314J
System Description         : 10-Port 10/100/1000Base-T + 4 (100/1G) SFP PoE+ L
2 Plus Managed Switch
Location                  :
Contact                   : administrator
Device Name                : PSGS-2314J
System Uptime              : 07:30:19
Current Time               : 2011-08-03 16:39:20
```

Description デバイスの特性についてのシステム情報を設定します。

Syntax

description *<system description>*

Parameter

<system description > システム情報について、最大255文字まで表示します。

例：

```
Switch(system)# description l2 advance managed switch
Switch(system)# show
Model Name                : PSGS-2314J
System Description         : l2 advance managed switch
Location                  :
Contact                   : administrator
Device Name                : PSGS-2314J
System Uptime              : 07:37:30
Current Time               : 2011-08-03 16:46:31
BIOS Version               : v1.00
Firmware Version           : v0.87
Hardware-Mechanical Version  : v1.00-v1.00
Series Number              : TIM0123456789
Host IP Address            : 192.168.1.1
Subnet Mask                : 255.255.255.0
Gateway IP Address         : 0.0.0.0
Host MAC Address           : 00-01-c1-00-00-00
Console Baudrate           : 115200
RAM Size                  : 64
Flash Size                : 16
CPU Load (100ms, 1s, 10s)    : 0%, 2%, 3%
Bridge FDB Size            : 8192 MAC addresses
Transmit Queue             : 8 queues per port
Maximum Frame Size         : 9600
```

Location　システムの設置場所を設定します。

Syntax

location *<system location>*

Parameter

<system location> システムの設置場所について、最大256文字まで入力します。

例：

```
Switch(system)# location Taiwan Taipei
Switch(system)# show
Model Name                : PSGS-2314J
System Description         : l2 advance managed switch
Location                  : Taiwan Taipei
Contact                   : administrator
Device Name               : PSGS-2314J
System Uptime             : 07:41:20
Current Time              : 2011-08-03 16:50:21
BIOS Version              : v1.00
Firmware Version           : v0.87
Hardware-Mechanical Version  : v1.00-v1.00
Series Number             : TIM0123456789
Host IP Address            : 192.168.1.1
Subnet Mask               : 255.255.255.0
Gateway IP Address         : 0.0.0.0
Host MAC Address           : 00-01-c1-00-00-00
Console Baudrate           : 115200
RAM Size                  : 64
Flash Size                : 16
CPU Load (100ms, 1s, 10s)    : 0%, 1%, 2%
Bridge FDB Size            : 8192 MAC addresses
Transmit Queue             : 8 queues per port
Maximum Frame Size         : 9600

Switch(system)#
```

Device name　デバイス名、またはエリアスを設定します。

Syntax

name *<system name>*

Parameter

<system name>　デバイス名について、最大255文字まで入力可能です。

例：

```
Switch(system)# name sales-departmen
Switch(system)# show
Model Name                : PSGS-2314J
System Description         : l2 advance managed switch
Location                  : Taiwan Taipei
Contact                   : administrator
Device Name               : sales-departmen
System Uptime             : 07:46:19
Current Time              : 2011-08-03 16:55:20
BIOS Version              : v1.00
Firmware Version           : v0.87
Hardware-Mechanical Version  : v1.00-v1.00
Series Number             : TIM0123456789
Host IP Address            : 192.168.1.1
Subnet Mask               : 255.255.255.0
Gateway IP Address         : 0.0.0.0
Host MAC Address           : 00-01-c1-00-00-00
Console Baudrate           : 115200
RAM Size                  : 64
Flash Size                : 16
CPU Load (100ms, 1s, 10s)    : 0%, 2%, 3%
```

show　システムの詳細情報について説明します。

Syntax

show

Parameter

なし

例:

```
Switch(system)# show
Model Name                : FXC5012MPE
System Description         : 8-Ports GbE UTP with PoE + 2-Ports GbE
UTP without PoE + 2 (100/1G) SFP L2 Plus Managed Switch
Location                 :
Contact                  :
Device Name               : FXC5012MPE
System Uptime             : 05:33:44
Current Time              : 2011-01-01 05:33:44
BIOS Version              : v1.00
Firmware Version           : v1.62 2013-01-07
Hardware-Mechanical Version  : v1.01-v1.01
Series Number             : 033F01000002
Host IP Address            : 192.168.11.237
Subnet Mask               : 255.255.255.0
Gateway IP Address         : 0.0.0.0
Host MAC Address           : 00-40-c7-1c-8a-97
Console Baudrate           : 115200
RAM Size                 : 64
Flash Size               : 16
CPU Load (100ms, 1s, 10s)    : 18%, 13%, 13%
Bridge FDB Size            : 8192 MAC addresses
Transmit Queue             : 8 queues per port
Maximum Frame Size          : 9600
Fan Speed                : 8571 (rpm) / 0 (rpm)
AC Power                 : 12.19 V
DC Power                 : 0 V
Temperature               : 33C (91.4F) / 34C
```

FXC5012MPE Management Guide
（FXC13-DC-200005-R1.2）

初版	2013 年 3 月
第二版	2015 年 4 月
第三版	2015 年 5 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
FXC5012MPE

Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide
FXC5012MPE
Management Guide

FXC5012MPE Management Guide

FXC13-DC-200005-R1.2

FXC株式会社