Future X Communications

ES1018V2
ES1024V2
Management Guide

2009年6月 Ver.2.0

FXC株式会社

本マニュアルについて

- **本マニュアルでは、**ES1018V2/ES1024V2 **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。**
- **本マニュアルは** ES1018V2 **と** ES1024V2 **の両方に対応したマニュアルとなっています。機能はどちら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。**
- **本マニュアルに記載している機能は、ファームウェアバージョン** 1.05.06 **以降の製品に対応しています。**

目次

製品取り扱い時のご注意

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

・下記事項は、安全のために必ずお守りください。

● 安全のための注意事項を守る

注意事項をよくお読みください。製品全般の注意事項が記載されています。

● 故障したら使わない

すぐに販売店まで修理をご依頼ください。

● 万一異常が起きたら

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

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

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

● 電源ケーブルや接続ケーブルを傷つけない

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

● 内部に水や異物を入れない

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

● 内部をむやみに開けない

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

● 落雷が発生したらさわらない

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

● 油煙、湯気、湿気、ほこりの多い場所には設置しない

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

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

● ぬれた手で電源プラグやコネクタに触らない

感電の原因となります。

● 指定された電源コードや接続ケーブルを使う

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

● 指定の電圧で使う

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

● コンセントや配線器具の定格を超えるような接続はしない

発熱による火災の原因となります。

● 通風孔をふさがない

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

・毛足の長いジュウタンなどの上に直接設置しない。

・布などでくるまない。

● 移動させるときは、電源ケーブルや接続ケーブルを抜く

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

1. コンソール接続による基本設定

この度は、ES1018V2、ES1024V2 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あります。

本機はマネージメント端末を接続してマネージメント機能の設定をおこないます。

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、最初に RS-232C シリアルポート経由でマネージメント機能にログインし、本機に適切な IP アドレス、サブネットマスク、デフォルトゲートウェイを割り当てる必要があります。

1.1 初期設定

以下の手順で、コンソールのハードウェア接続を行ってください。

（1）シリアルケーブルの片方を本機の RS-232C コネクタへ接続し、もう一方を PC のシリアルポートへ接続します。

（2）PC のターミナルエミュレータ（Windows98/2000/XP ハイパーターミナル等の VT100/ANSI に対応した）を起動し、ターミナルエミュレータを下表のとおり設定します。

設定項目	設定
通信速度	9600bps
データビット	8bit
パリティ	なし
ストップビット	1bit
フロー制御	なし

（3）スイッチの電源を投入します。

全ての設定が正しく行われていれば、スイッチの電源投入後、ターミナルプログラムに起動画面が表示されます。

初期化メッセージが表示された後、以下の画面で停止します。

```
......

Start to run system initialization task.
[System Configuration]
Company Name      :
Model Name        : ES1018V2
MAC  Address      : 00:00:00:01:53:47


Firmware version: 1.01.04
Press <ENTER> key to start.
```

「Enter」キーを押すことで、エミュレータの画面に CLI マネージメントのログインプロンプトが表示されます。デフォルトのユーザアカウントは、ユーザ名、パスワード共に "admin" です。ログイン画面で入力することで、マネージメント機能にログインします。

1.2 CLI コマンド

1.2.1 ? コマンド

"?" と入力することで、コマンドリストを表示することができます。

```
ES1018V2>?
[Command List]
?.............. Help commands
default........ Restore to factory default setting
help........... Help commands
logout......... Logout
ping........... Ping a specified host with IP address
reset.......... Reset system
set............ Set commands
show........... Show commands
```

1.2.2 Default コマンド

設定を工場出荷時の状態に戻します。

"default" と入力すると、Yes/No の確認がされます。

```
ES1018V2>default
All current setting will be lost after restoring default!
Are you sure to restore default setting now?(Y/N)
```

"y" と入力すると、スイッチの設定が工場出荷状態に戻り、再起動が行われます。

"n" と入力すると、何も変更は行われず元の画面に戻ります。

1.2.3 Help コマンド

"？" コマンドと同様に、コマンドリストを表示します。

1.2.4 Logout コマンド

ログアウトをおこないます。

1.2.5 Ping コマンド

他のネットワークデバイスに対して Ping を送信することができます。

コマンド構文は以下になります。

ping [-n count] [-l length] [-t] [-w timeout] ip

-n count ：送信する Echo リクエストの回数

-l length ：バッファサイズ（64 ～ 8148）

-t ：<ESC> キーを押すまで Ping を送信

-w ：リプライが戻ってくるまでの待ち時間（単位：ミリ秒）

-ip ：IP アドレス

1.2.6 Reset コマンド

スイッチのリセットを行います。

"reset" **と入力すると、**Yes/No **の確認がされます。**

```
ES1018V2>reset
Are you sure to reset switch now?(Y/N)
```

"y" **と入力すると、スイッチの再起動が行われます。**
"n" **と入力すると、何も変更は行われず元の画面に戻ります。**

1.2.7 set コマンド

スイッチの IP **設定および、管理者権限のユーザ名・パスワードの設定をおこないます。**

[set admin]

管理者権限のユーザ名・パスワードの設定をおこないます。

[set net]

スイッチの IP **アドレス設定をおこないます。**

コマンド構文は以下になります。

set net [dhcp] [ip *ip*] [netmask *netmask*] [gateway *gateway*] ip

-dhcp **：**dhcp **クライアントの有効**
-ip **：**IP **アドレス**
-netmask **：ネットマスク**
-gateway **：ゲートウェイ** IP **アドレス**

本機は DHCP **クライアント機能をサポートしています。**

DHCP **を有効にした場合、スイッチは起動時に、**IP **設定を** DHCP **サーバから取得します。**

"show net" **コマンドにて** DHCP **設定をおよび現在の** IP **設定を確認することができます。**

DHCP **が有効に設定されているのにもかかわらず、スイッチがネットワーク上に** DHCP **サーバを見つけられない場合、**"BOOTP/DHCP failed on eth0" **というメッセージが表示され、**"192.168.1.1/255.255.255.0" **という** IP **設定が使用されます。**

DHCP **が無効時、手動で** IP **設定（**IP **アドレス、ネットマスク、ゲートウェイ）をおこなえます。例えば、**"set net ip 192.168.1.250 netmask 255.255.255.0 gateway 192.168.1.154" **というように入力します。**

1.2.8 show net コマンド

スイッチの IP **設定情報を表示します。**

```
ES1018V2>show net
[eth0] Network Configuration:
DHCP       : DISABLE
IP Address: 192.168.1.12
Netmask    : 255.255.255.0
Gateway    : 192.168.1.2
```

2. Web コンソール

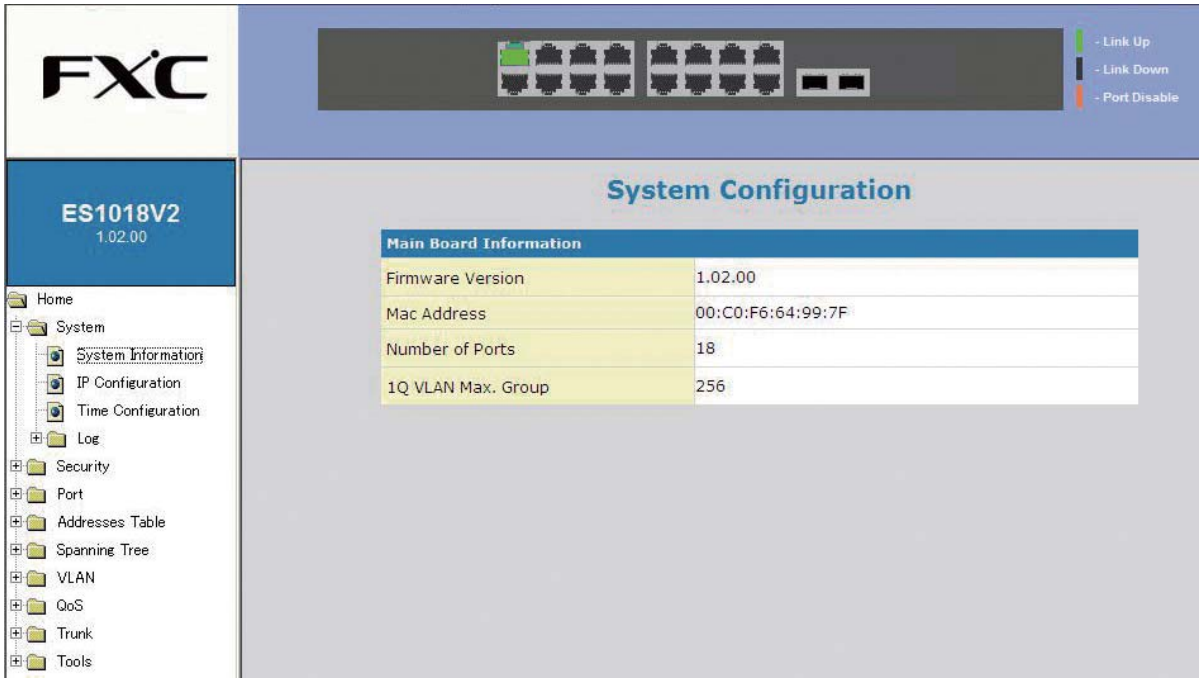
イーサネットポート経由でマネージメント機能に接続する前に、シリアルポート経由で本機にログインし、適切な IP アドレス、サブネットマスク、デフォルトゲートウェイを本機に設定する必要があります。（1.2.7 項「set コマンド」を参照してください）

Web ブラウザを起動し、設定した IP アドレスを入力します。

ログイン画面が表示されるので、ユーザ名とパスワードを入力します。

（デフォルトユーザ名とパスワードはどちらも "admin" です。）

以下のようにホームページが表示されます。



左側がファンクションリストになります。設定を行いたい項目をここから選択します。

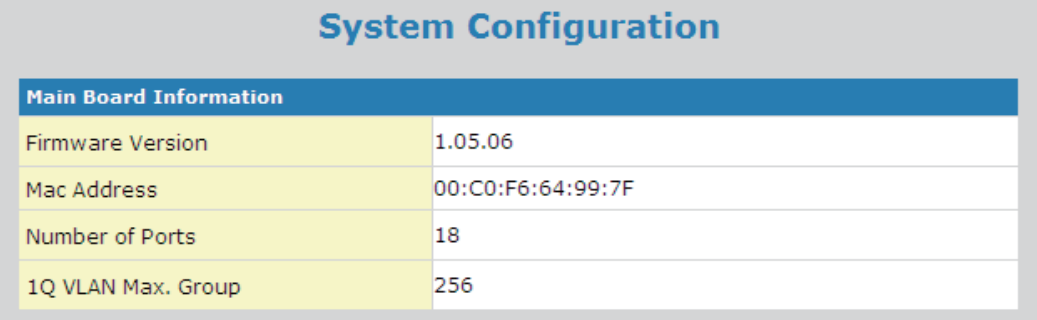
上部はスイッチのリンク状態を表示しています。

中央が各機能のオペレーションを行う場所になります。

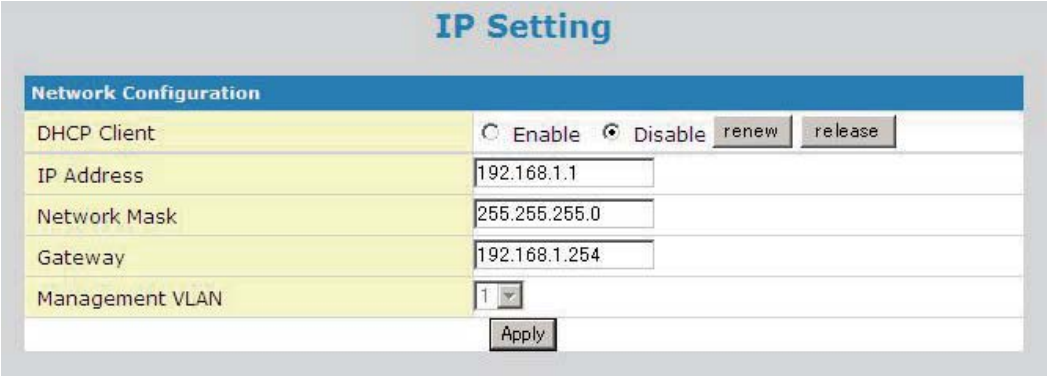
2.1 システム

2.1.1 システム情報の表示

“System Configuration“ にて、スイッチのシステム情報を表示します。ファームウェアバージョン、MAC アドレス、接続ポート番号、最大 VLAN グループ数を確認することができます。



2.1.2 IP 設定



スイッチの IP 設定を行います。

DHCP クライアント機能の有効 / 無効、および各種 IP 項目の手動設定が行えます。

Management VLAN

設定に使用する管理 VLAN ID を設定します。

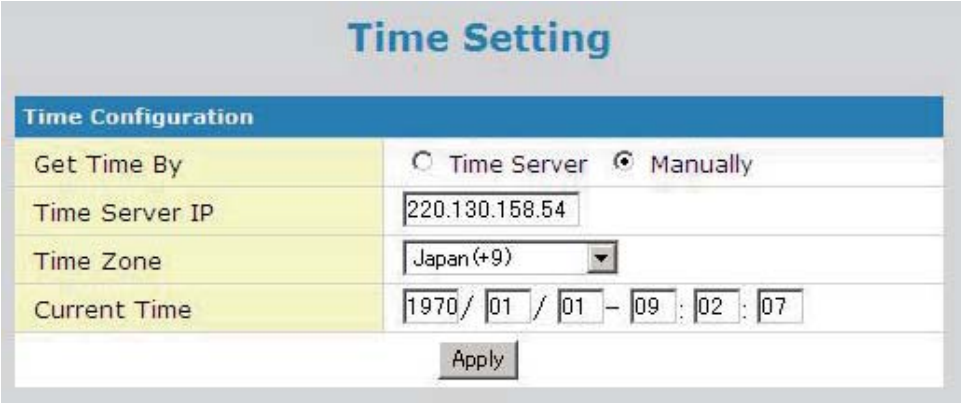
【renew】

DHCP クライアント機能が有効の場合、IP アドレスのリースタイムをリフレッシュすることができます。もし、ブートアップ時に IP アドレス設定が取得されない場合、【renew】ボタンをクリックしてみてください。

【release】

DHCP クライアント機能が有効で、IP 設定が取得されている場合、現在割り振られている IP アドレスをリリースすることができます。【release】ボタンをクリック後に、【renew】ボタンをクリックして、新しい IP 設定の取得を行ってください。

2.1.3 時刻の設定

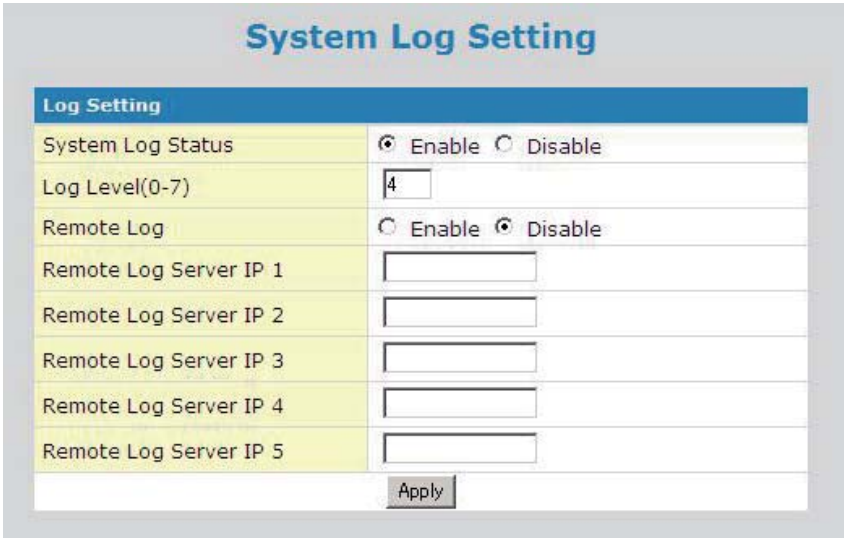


システム時刻を設定するには以下の 2 **つの方法があります。**

- **タイムサーバより時刻情報を取得**
  本機は NTP **プロトコルをサポートしています。**“Get Time by Time Server“ **を選択し、**Time **サーバの** IP **アドレス、**Time Zone **を指定します。**
- **手動で時刻を設定**
  “Get Time by Manually“ **を選択し、現在の時刻を手動で設定します。**

2.1.4 Log

【System Log Setting】



システムログ機能の設定および採取したログの表示を行えます。この機能が有効の場合、スイッチはログファイルにイベントを記録します。

ローカル Logging **には、最大** 512 **の記録が可能です。もし** 512 **以上のイベントが発生した場合、古い記録から上書きされていきます。もしリモート** syslog **サーバが使用可能な場合、イベント記録を** syslog **サーバに送信することも可能です。**

System Log Status

Syslog 機能の有効 / 無効を設定します。

Log Level(0-7)

ログレベルは以下を参照してください。

レベル	名前	解説
7	debug	デバッグメッセージ
6	Informational	情報メッセージ
5	Notice	重要なメッセージ
4	Warnings	警告メッセージ
3	Errors	エラー状態を示すメッセージ
2	Critical	重大な状態を示すエラーメッセージ
1	Alerts	迅速な対応が必要なメッセージ
0	Emergency	システム不安定状態を示すメッセージ

Remote Log

リモート Syslog 機能の有効 / 無効

Remote Log Server IP

リモート Logging で使用する、syslog サーバ IP アドレスを設定。最大 5 つまでの syslog サーバをサポートしています。イベントログはこれらの syslog サーバへ同時に送られます。

【Logs Table】

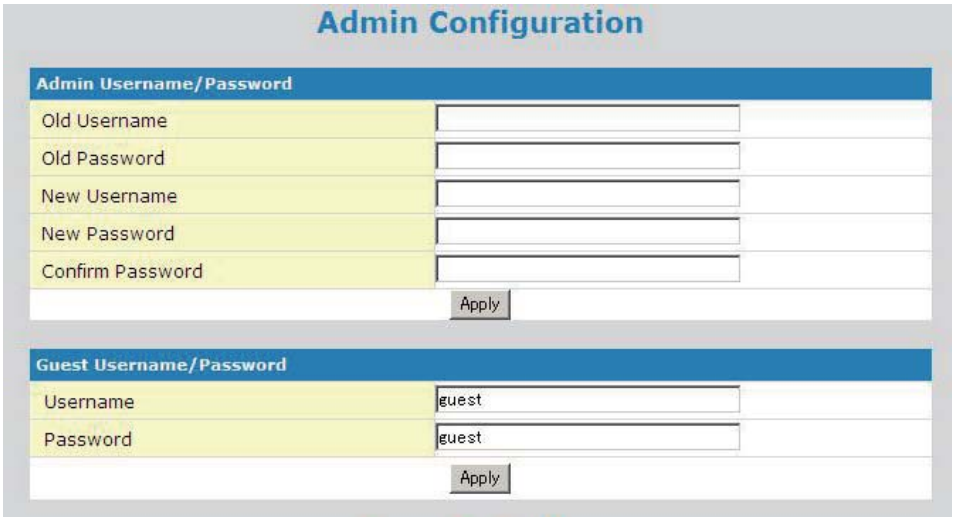
ログをここで確認できます。

"Clear log" ボタンを押すと、ローカルログテーブルを削除します。

2.2 セキュリティ

セキュリティ機能の設定を行います。

2.2.1 ユーザアカウント



Administrator Username/Password

ネットワーク管理者自身は変更ができます。（初期設定：admin/admin）

Guest Username/Password

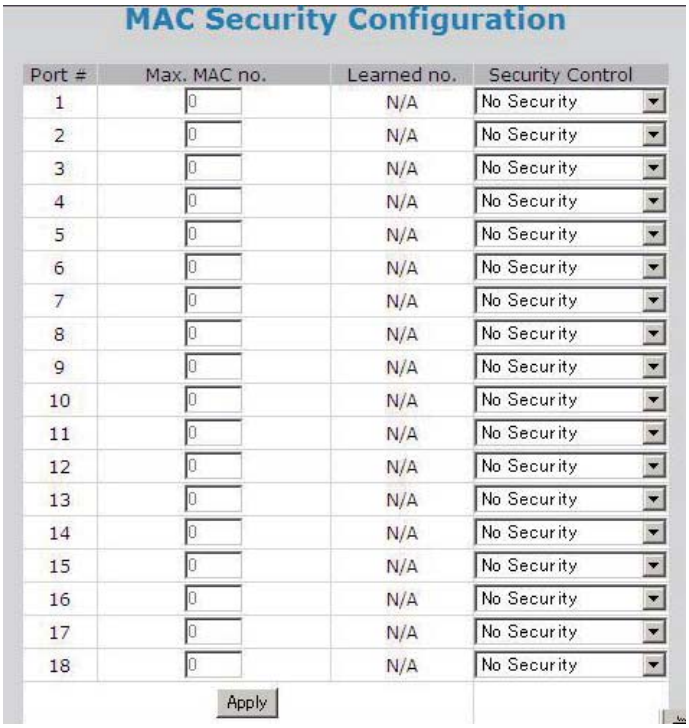
ゲストユーザ用のユーザ名 / パスワードを設定します。ゲストユーザはスイッチの設定表示のみ実行可能です。

【Security Policy】

本機の管理を実行することができる IP アドレスを設定します。

[注意] 必ず一つの IP/ サブネットを使用可能にすることを忘れないでください。
もし、全ての IP/ サブネットからの接続が不可能に設定してしまった場合は、コンソールから "default" コマンドを使用し、全ての設定を工場出荷状態に戻す必要があります。

2.2.2 MAC セキュリティ



MAC ID セキュリティモードには、ポートの静的 MAC ID フィルタ（ Static Mac ID Filetr on Port）と、ポートの動的 MAC ID 数制限（Dynamic Mac ID Number Limit on Port）があります。

Static Mac ID Filetr on Port

ポートに指定した静的 MAC アドレスのみがネットワークにアクセルすることが可能で、その他の MAC アドレスはポートで拒否されます。" MAC ポートバインディング " とも呼ばれます。

（1）静的 MAC ID セキュリティを適用するポートで、"Security Control" を "Accept" に設定し、"Apply" をクリックします。

（2）【Address Table】の、【Static Address】にて、ネットワークアクセスを許可する静的 MAC アドレスを設定します。

Dynamic Mac ID Number Limit on Port

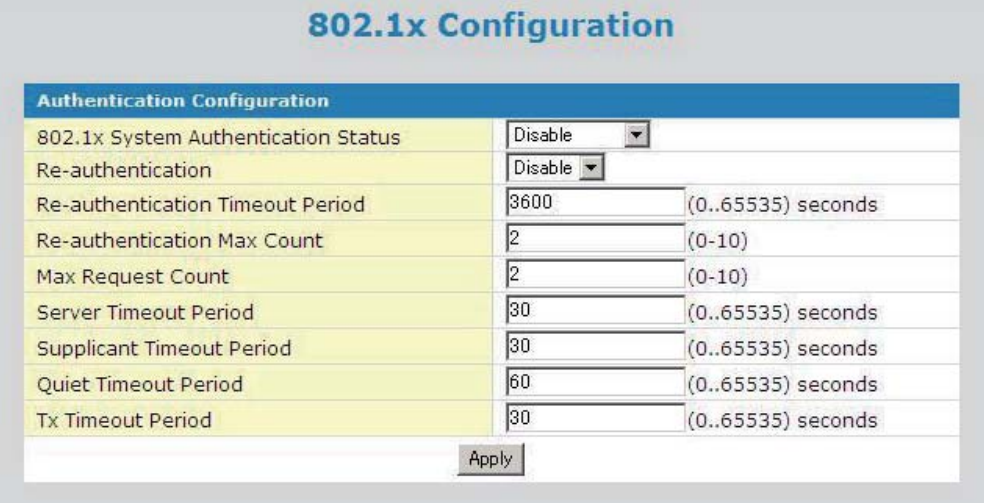
ポートを通過してネットワークにアクセスする MAC ID の数に制限をかけることができます。例えば、5 つの MAC ID 番号をポート 2 で許可した場合、ユーザが誰であるかは問わず、最大 5 ユーザが許可されます。

（1）動的 MAC ID 数制限を適用するポートで、"Security Control" を "Limited by MAC no." に設定後、"Max. MAC no." を指定します。

（2）"Apply" をクリックします。

2.2.3 802.1x ユーザ認証（802.1x Configuration）

802.1X ポートベースネットワークアクセスコントロールは、ユーザ情報の認証をおこなうことによって、ユーザのネットワークへのアクセスを制限する手段を提供します。これは、802.1X が有効に設定されているポートを経由する場合、認証なしにユーザがネットワークリソースへアクセスすることを制限します。



802.1x Authentication Status

Enable：認証モードで 802.1x 機能を有効にします。

Disable：認証モードで 802.1x 機能を無効にします。

Transparent：802.1x プロトコルのパケットは転送されますが、認証機能は動作しません。

Re-authentication (enable/disable), Timeout Period and Max Count

Re-authentication：ユーザーの再認証機能を有効にします。

Max Count：スイッチとユーザーの間で行う認証の最大試行回数を設定します。

Max Request Count and Server Timeout Period:

Max Request Count：スイッチと RADIUS サーバーの間で行う認証の最大試行回数。

Server Timeout Period：スイッチと RADIUS サーバーの間でリクエストがタイムアウトするまでの時間。

Supplicant Timeout Period

最初の認証の後、スイッチとユーザー（802.1x の用語でユーザーはサプリカントと呼びます）間がタイムアウトするまでの秒数（範囲：0~65535）

Quiet Timeout Period

認証が失敗したとき、次の認証プロセスに移る前にスイッチとユーザー間で 802.1x が動作するまでの時間。

Tx Timeout Period

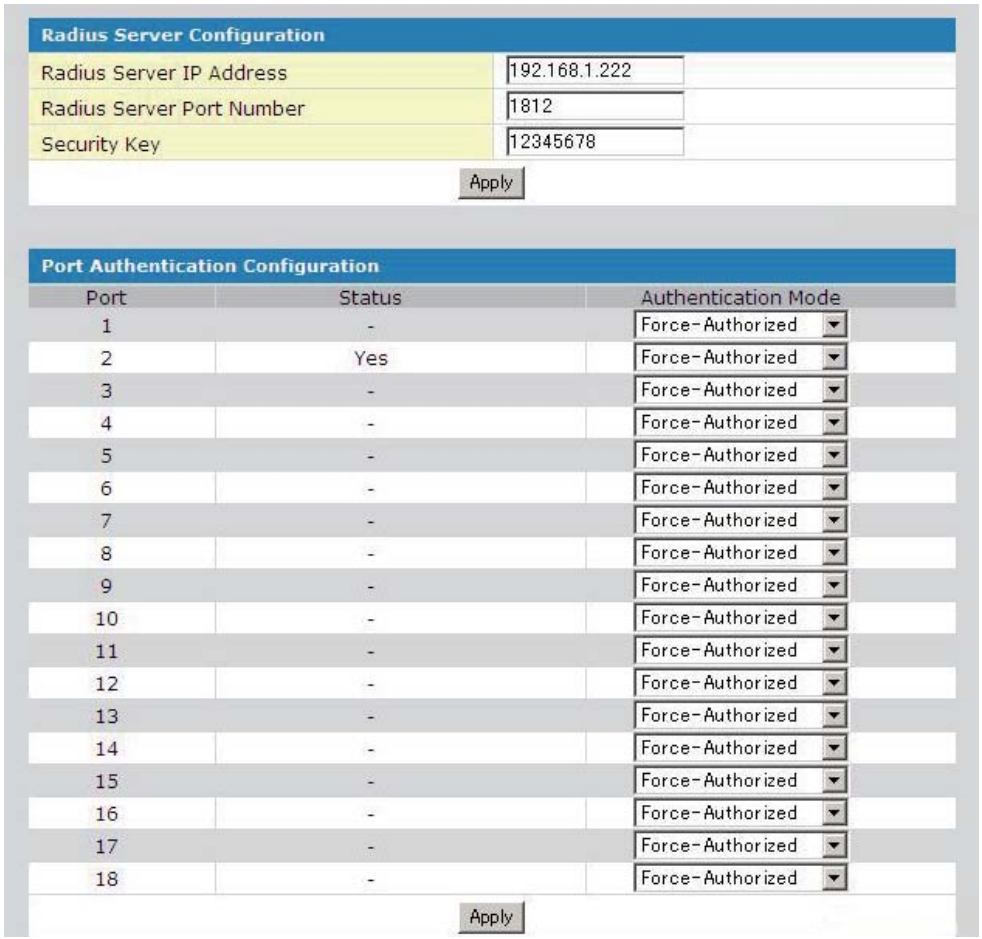
スイッチからユーザーへの認証リクエストがタイムアウトするまでの秒数。リクエストは Re-authentication Max Count で設定した回数になるまで再送信されます。その後、認証失敗のメッセージが送信されます。（範囲：0~65535）

【Radius Server Configuration】

この機能は、スイッチと RADIUS **サーバ間の設定を行います。**

RADIUS **サーバの** IP **アドレス、プロトコルポート番号、セキュリティキーを設定できます。**

【Port Authentication Configuration】



各ポートで使用する、認証ポートを設定します。

Auto

ポートは、認証サーバとサプリカントでやり取りされる認証結果に基づき認証状態または非認証状態に設定されます。

Force-Authorized

ポートは、認証状態に設定されます。

Force-Unauthorized

ポートは、非認証状態に設定されます。

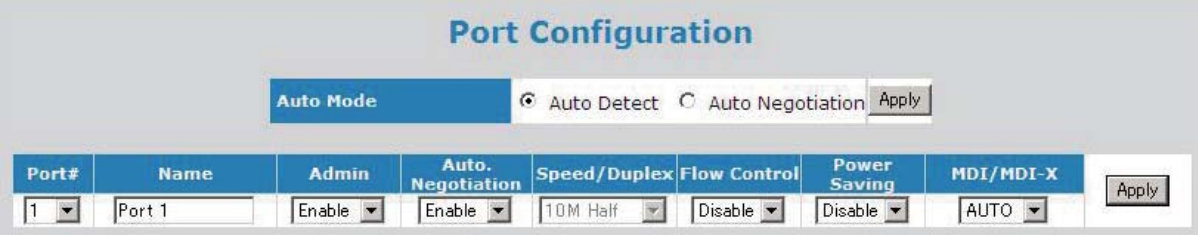
None

ポートは、802.1x **オペレーション無効になります。**

2.3 ポート

ポートスピード設定、最大パケットサイズ、ポートミラーリング、ポート帯域制御等、ポート解析等の設定をおこないます。

2.3.1 ポート設定



Auto Mode

"auto" **が無効に設定時、オペレーションモードを選択することができます。**

Port Setting

（1）**設定を行うポートを選択します。**

（2）**ポート名を入力します。**

（3）"Admin" **を** Enable **か** Disable **か選択します。もし** "Disable" **を選択した場合、ポートは全てのネットワークにたいして無効となります。**

（4）**ポートの** "Auto" **を** Enable **か** Disable **から選択します。**"Auto" **が無効時、モードは** Auto-negotiation **または** Auto-detect **機能にできます。**

（5）"Auto" **が無効時、**"Speed/Duplex" **にて、通信速度および** Duplex **モードを設定できます。**

（6）"Flow Control" **の** Enable/Disable **を選択します。**

（7）**ポートのパワーセービング機能の** Enable/Disable **を選択します。有効にした場合、ポートはリンクダウン時に低電力モードになります。**

（8）MDI/MDI-X **オペレーションモードを選択します。ここでは、**"Auto"、"MDI" **または** "MDI-X" **が選べます。**
- Auto：**自動認識によって、適したモードでの接続をおこないます。**
- MDI：MDI **モードで接続をおこないます（機器同士の接続用）**
- MDI-X：MDI-X **モードにで接続をおこないます（ユーザ** PC **との接続用）**

（9）"Apply" **をクリックします。**

ポート情報

Current Setting & Link Status

Port#	Name	Admin	Auto. Negotiation	Speed/Duplex	Flow Control	Power Saving	Link Status
1	Port 1	Enable	Enable	0M Half	Disable	Disable	Down
2	Port 2	Enable	Enable	100M FULL	Disable	Disable	UP
3	Port 3	Enable	Enable	0M Half	Disable	Disable	Down
4	Port 4	Enable	Enable	0M Half	Disable	Disable	Down
5	Port 5	Enable	Enable	0M Half	Disable	Disable	Down
6	Port 6	Enable	Enable	0M Half	Disable	Disable	Down
7	Port 7	Enable	Enable	0M Half	Disable	Disable	Down
8	Port 8	Enable	Enable	0M Half	Disable	Disable	Down
9	Port 9	Enable	Enable	0M Half	Disable	Disable	Down
10	Port 10	Enable	Enable	0M Half	Disable	Disable	Down
11	Port 11	Enable	Enable	0M Half	Disable	Disable	Down
12	Port 12	Enable	Enable	0M Half	Disable	Disable	Down
13	Port 13	Enable	Enable	0M Half	Disable	Disable	Down
14	Port 14	Enable	Enable	0M Half	Disable	Disable	Down
15	Port 15	Enable	Enable	0M Half	Disable	Disable	Down
16	Port 16	Enable	Enable	0M Half	Disable	Disable	Down
17	Port 17	Enable	Enable	0M Half	Disable	Disable	Down
18	Port 18	Enable	Enable	0M Half	Disable	Disable	Down

Name

ポート名

Admin

現在のポートのステータス（Enable/Disable）

Auto

現在のポート Auto **ステータス**（Enable/Disable）

Speed/Duplex

ポートがリンクアップ状態の場合、ポートの速度 /Duplex **モードを表示。**

Flow Control

現在のフローコントロール状態

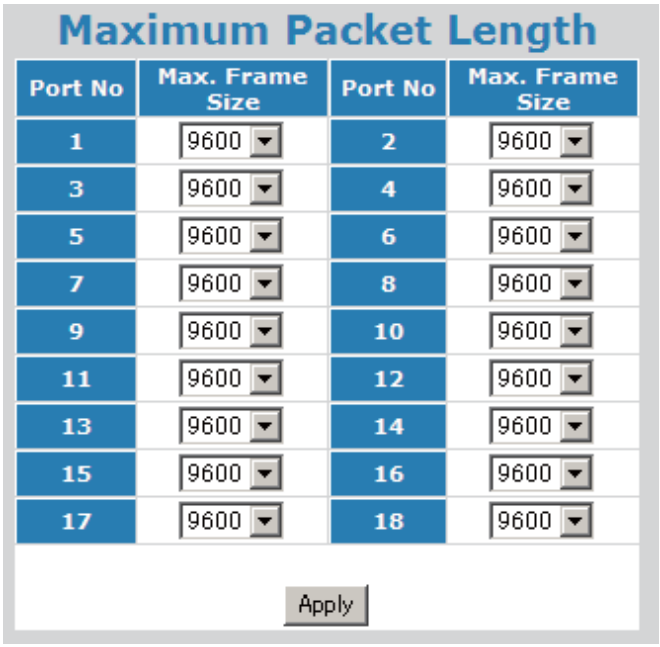
Power Saving

現在のパワーセービングモードの状態（Enable/Disable）

Link

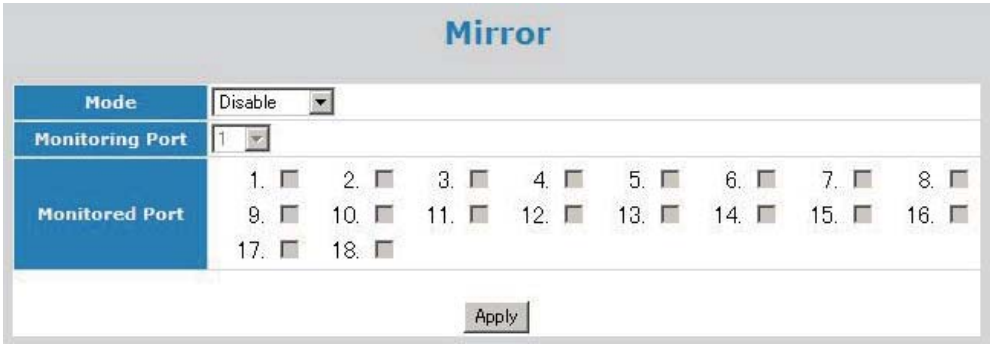
それぞれのポートのリンク状態

2.3.2 パケットサイズ



本機はジャンボフレーム機能をサポートしており、最大パケットサイズは 9600byte/packet になります。ここで、各ポートの最大パケットサイズを設定することができます。

2.3.3 ポートミラーリング



Mode

ポート名

Monitering Port

キャプチャポートを設定します。ミラー機能が有効時、非モニタポートからこのポートへトラフィックがコピーされます。

Monitering Port

非モニタポート。このポートからモニタポートへトラフィックはコピーされます。

[注意] 本機は Rx データのミラーリングのみサポートしています。

2.3.4 帯域制御

本機は各ポートの、入力 / 出力トラフィック制御および、ブロードキャスト / マルチキャスト / ユニキャストストーム制御をサポートしています。

Rate Control Configuration

ポートの入力 / 出力帯域制御を行います。

（1）**まず** "Unit" **を指定し、**"Apply" **をクリックします。**

（2）**ポート番号を選択します。**

（3）**入力（**Ingress**）、出力（**Egress**）トラフィックに対し、レートリミット数を入力します。**"0" **は制御無しです。**"Apply" **をクリックします。**

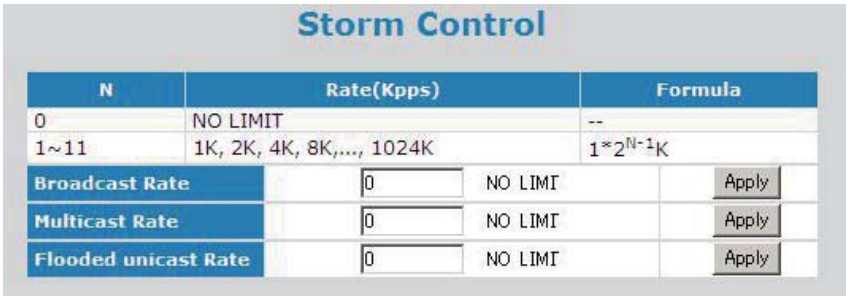
“ Packet Drop for Ingress Limit ”機能について

入力トラフィックレートがレートリミット値を越えた際、スイッチはパケットを破棄するか、トラフィックを中断することができます。

- Packet Drop **有効：**
  ポートのフローコントロールは無効になり、パケットの破棄をおこないます。
- Packet Drop **無効：**
  ポートのフローコントロールは有効になり、入力トラフィックレートがリミット値を越えた場合、ポーズフレームが送信されます。

Storm Control Configuration

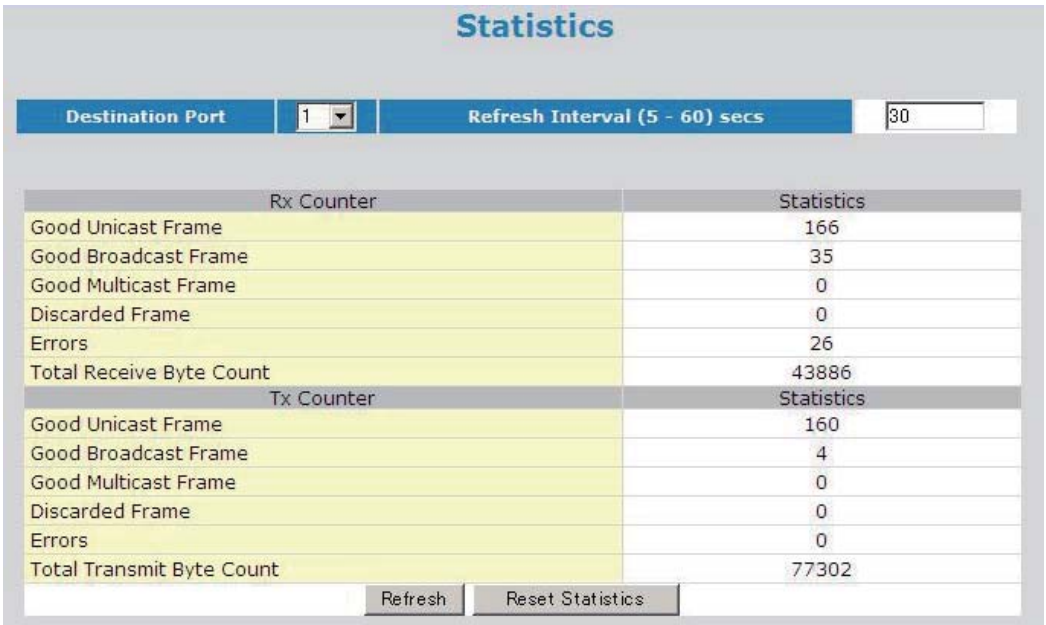
ブロードキャスト / マルチキャスト / ユニキャストストームのレートを設定します。



最大ストームレートを設定します。

[注意] ストームレートは pps（packet per xecond）で設定します。

2.3.5 ポート統計（Port Statistics）



ポートを選択し、カウンタを表示します。

【Refresh】

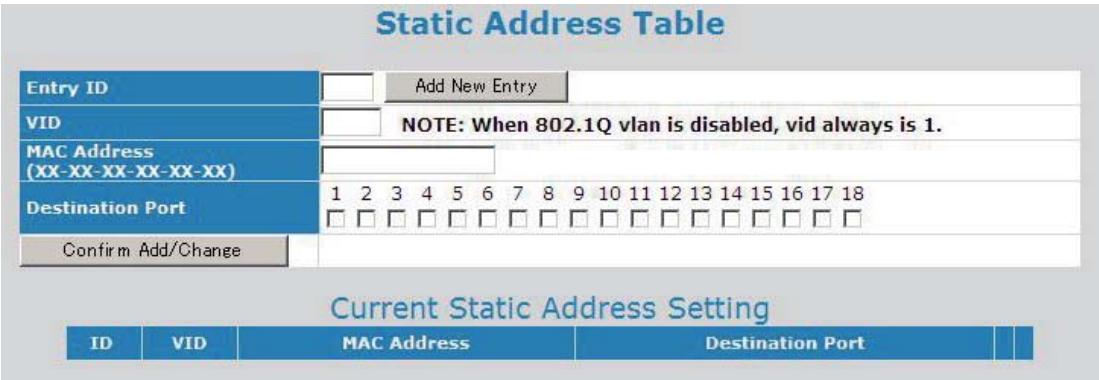
カウンタは自動的にリフレッシュされます。
リフレッシュを行う間隔を指定できます。

【Reset Statistics】

カウンタを "0" **にリセットします。**

2.4 アドレステーブル

2.4.1 静的アドレス



本機はスタティック MAC **アドレスの割り当てをサポートしています。**

以下のステップで、静的 MAC **アドレスを割り当てることができます。**

（1）Entry ID：**静的アドレステーブル内のエントリ** ID **から指定します。**

（2）VLAN ID：802.1Q **が無効の場合、**VID **は常に** 1 **になります。**

（3）MAC **アドレス：静的** MAC **アドレスを指定します。**

（4）**選択した静的アドレスにポートを選択します。**

（5）【Confirm Add/Change】**ボタンをクリックします。**

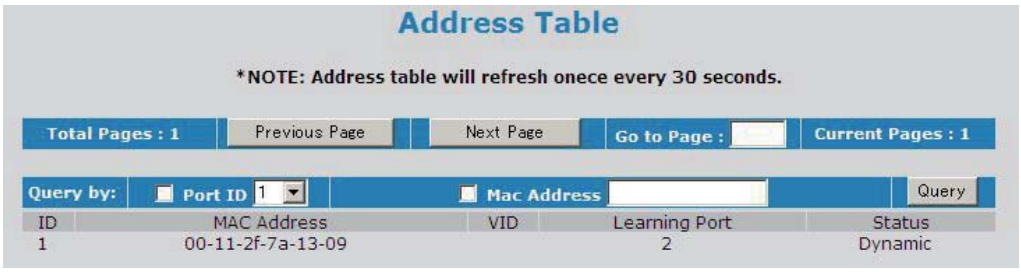
これで、エントリはテーブルに追加されます。

"Current Static Address Setting" **テーブルでは、エントリの編集および削除が行えます。**

もし。静的 MAC **アドレステーブル内のエントリを削除したい場合、エントリの**【Delete】**ボタンをクリックしてください。**

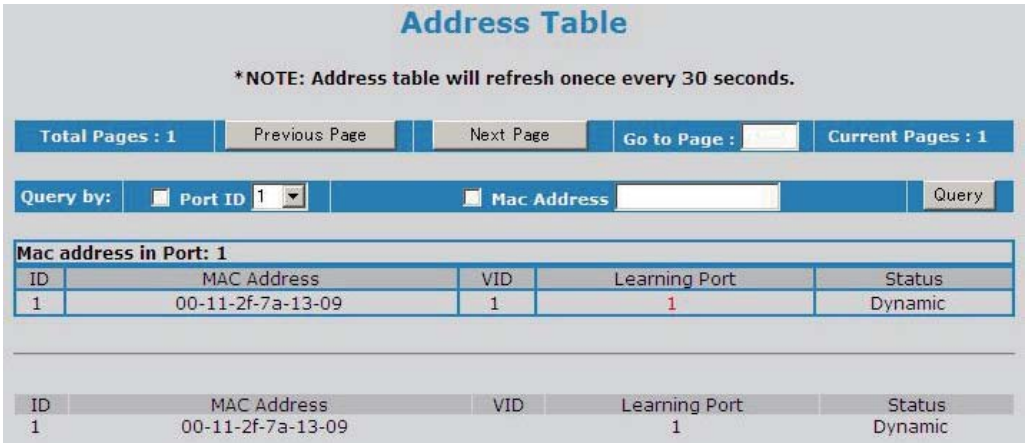
修正を行いたい場合は、エントリの【Edit】**ボタンをクリックし、編集を行った後に**【Confirm Add/Change】**ボタンをクリックしてください。**

2.4.2 動的アドレス



スイッチで学習された動的 MAC アドレスを表示します。このテーブルは、30 秒毎にリフレッシュされます。

本機はクエリ機能をサポートしています。クエリ機能を選択し、クエリターゲットを入力後【Query】をクリックすると、結果が表示されます。



2.4.3 アドレスエージング

スイッチは、MAC アドレスを ARL テーブルへ自動的に学習します。

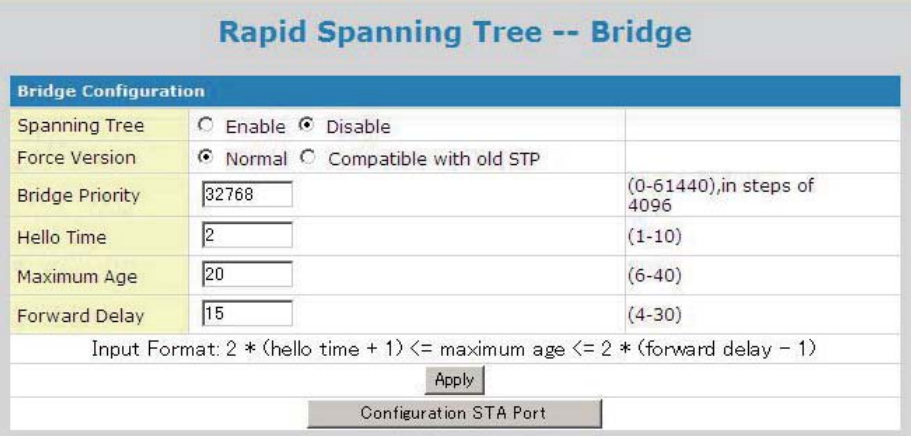
同じ MAC アドレスがある一定期間、再度受信されることがない場合、これらのアドレスはテーブルから消去されます。このオペレーションはエージングと呼ばれます。

このエージングオペレーションを無効にし、ARL テーブルから学習した MAC アドレスが消去されることがないようにできます。

また、エージングオペレーションを行う間隔の設定もできます。（初期設定：300 秒）

2.5 スパニングツリー

【Rapid Spanning Tree--Bridge】



Enable/Disable

スパニングツリー機能の有効 / 無効

Force Version

"Normal" **選択時、**RSTP （Rapid Spanning Tree）**で動作します。**
"Compatible with old STP" **選択時には、**old Spanning Tree **モードで動作します。**

Bridge Priority

ルートデバイス、ルートポート、指定ポートを選択するために必要なブリッジプライオリティを設定します。最も高いプライオリティ（priority **が最も低い）を持つデバイスはスパニングツリープロトコルのルートデバイスになります。すべてのデバイスが同じプライオリティの場合、最も低い** MAC **アドレスを持つデバイスがルートデバイスになります。**
（範囲：0~61440）

Hello Time

本機がスパニングツリーのルートデバイスの場合に、スパニングツリー管理パケットを送信する間隔を設定します。（範囲：1~10　**初期設定：**2 **秒）**

Maximum Age

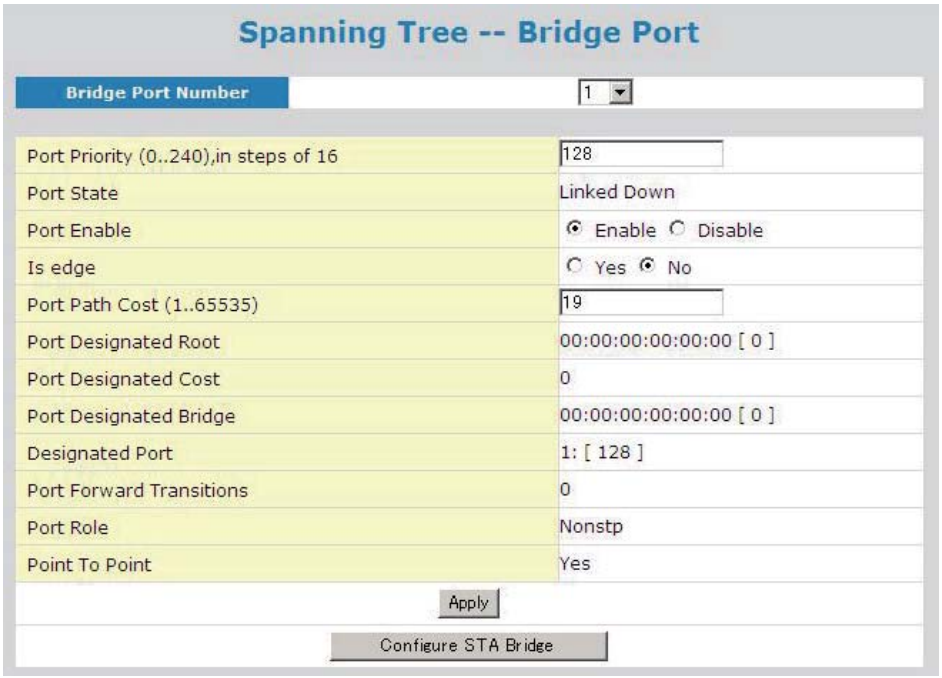
スパニングツリー管理パケットを受信していない場合のスパニングツリーのエージングタイムを設定します。これはスパニングツリーの再作成を引き起こします。（範囲：6 ～ 40　**初期状態：**20 **秒）**

Forward Delay

スパニングツリーの状態を変更（リスニング状態からラーニング状態への移行）する前の最大待ち時間を設定します。この設定が必要とされるのは、すべてのデバイスがフレームの転送を始める前にトポロジの変更についての情報を受信する必要があるからです。加えて、各ポートはブロッキング状態に再び戻るような衝突情報（一時的なデータループの発生など）を検知するための時間が必要です。（範囲：4 ～ 30　**初期設定値：**15）

【ポートの設定】

【Configuration STA Port】をクリックします。ポートの RSTP/STP の設定が行えます。



Bridge Port Number

設定を行うポートを指定します。

Port Priority

ポートのプライオリティを設定します。スイッチ上のすべてのポートのパスコストが同じの場合、ループが発生したときに最も高いプライオリティ（priority が最も低い）のポートに転送されます。最も高いプライオリティのポートが複数ある場合、最も低いポート番号のポートに転送されます（範囲：0 ～ 240　初期設定値：128）

Port State

現在ポートで動作しているスパニングツリー

Port Enable

ポートのスパニングツリー機能の有効 / 無効

Is edge

本機がネットワークツリーの "Edge" である場合、"Yes" を選択してください。

Port Path Cost

ループが発生した場合にデバイス間の最適経路を決定するためにこの値が使用されます。速度が速いポートには低い値が割り当てられ、パケットの転送が行われます。速度が遅いポートには高い値が割り当てられ、転送がブロックされます。推奨される値は 10M で 100（50 ～ 600 の範囲）、100M で 19（10 ～ 60）、1000M で 4（3 ～ 10）です。（範囲：1 ～ 65535）

Port Designated Root

このセグメントおよびブリッジプライオリティのブリッジ ID **を表示します。**

Port Designated Cost

ルートブリッジの、ルートポートと Designated **ポート間のパスコストを表示します。**

Port Designated Bridge

スイッチのブリッジ ID **およびブリッジプライオリティ設定を表示します。**

Designated Port

ポート番号およびポートプライオリティを表示します。

Port Forward Transitions

ポートの、フォワーディングトランジッションカウンタ。

Port Role

オペレーションポート。もしポートがリンクダウンしている場合、ポートロールは "Nonstp" **になります。**

Point To Point

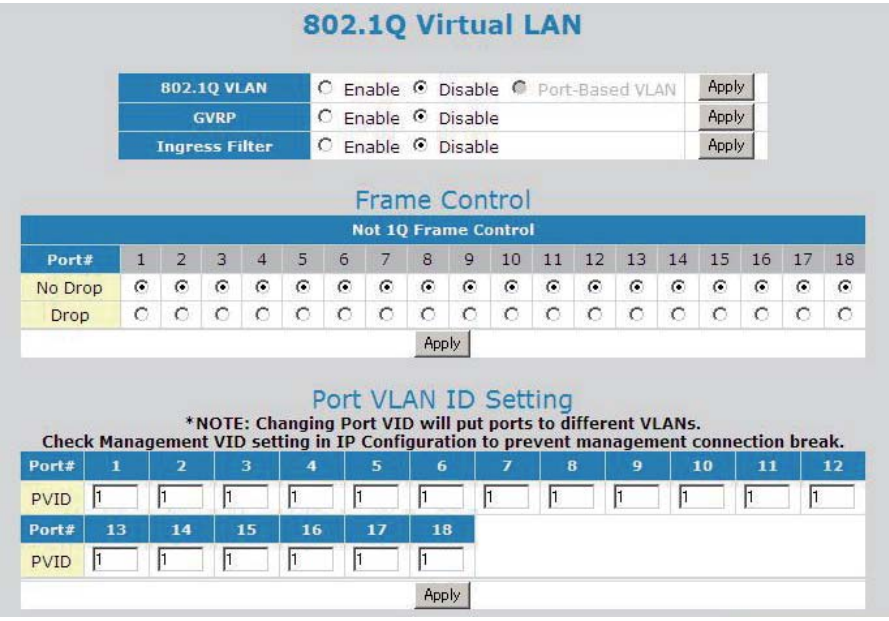
ポートのポイント - **ポイントリンク。**

2.6 VLAN

本機は、802.1Q VLAN**、**VLAN **ポートベース** VLAN**、プライベート** VLAN **をサポートしています。**.

2.6.1 802.1Q VLAN

802.1Q VLAN 設定



802.1Q VLAN

802.1Q VLAN **の有効・無効を設定します。**

GVRP

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

Ingress Filter

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

【Frame Control】

802.1Q **以外のフレーム（タグ無しパケット）を破棄します。**

【Port VLAN ID Settings】

ポート VLAN ID **の設定をおこないます。**

VLAN タグルール

802.1QVLAN では、すべてのポートはタグポートまたはアンタグポートに設定できます。

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

その役割は、802.1Q VLAN グループ機能のための "Trunk" になります。

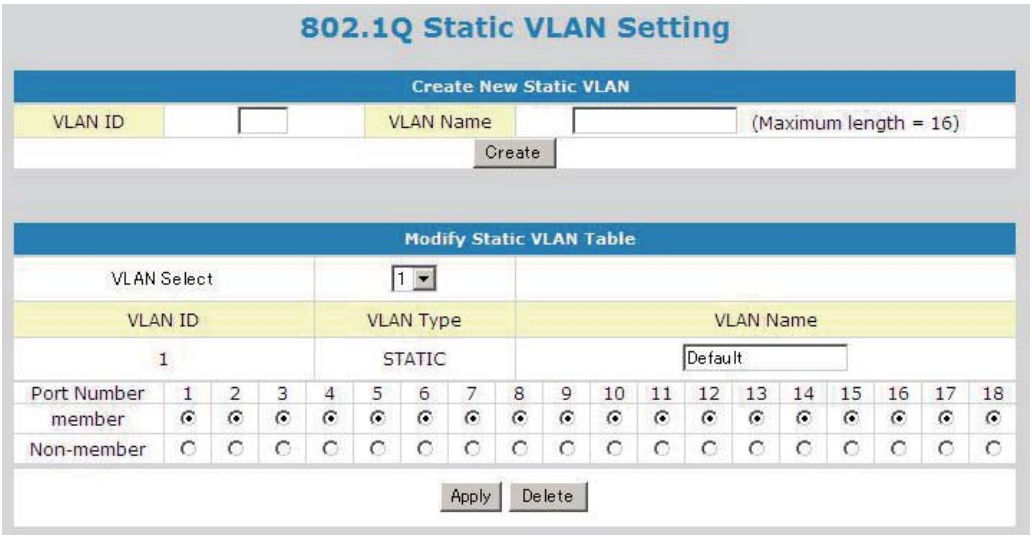
タグなしポートでは常にパケットはタグが付かない状態で送信されます。

その役割は、ユーザのための "Access" 接続になります。

接続するデバイスに応じて、ポートを "Trunk" または "Access" に設定することができます。

ポートを "Hybrid" に指定した場合、基本的にはタグポートとして動作しますが、アンタグ VID に定義された VLAN で動作するパケットにたいしては、アンタグポートとして機能します。

Static 1Q VLAN



802.1Q VLAN の作成

（1）"Create New Static VLAN" に VLAN ID および VLAN 名を入力ます。”Create” をクリックすることで VLAN が作成されます。（VLAN ID の範囲：1 ～ 4094）

（2）"Modify Static VLAN Table" を選択します。デフォルトでは空になっています。VLAN ポートを選択し、"Apply" をクリックします。

802.1Q VLAN の修正

（1）"Modify Static VLAN Table" で VLAN を選択します。

（2）設定の編集を行い、"Apply" をクリックします。

802.1Q VLAN の削除

（1）"Modify Static VLAN Table" で VLAN を選択します。

（2）"Delete" をクリックし、VLAN を削除します。

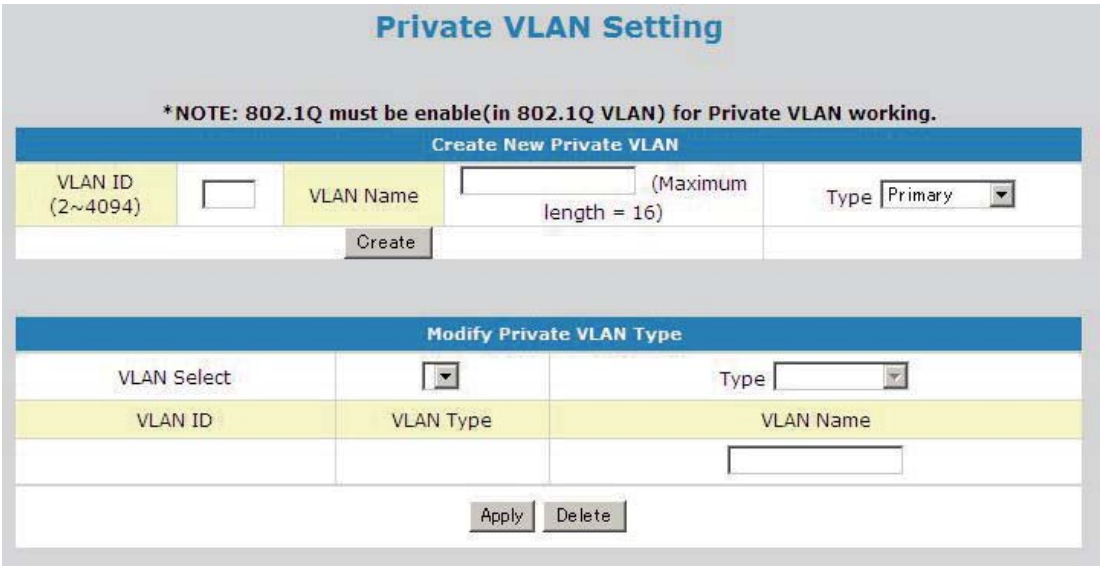
VLAN テーブル

静的および動的 VLAN が表示されます。

ポートの "S" は静的メンバー、"D" は動的メンバーです。

2.6.2 プライベート VLAN（Private VLAN）

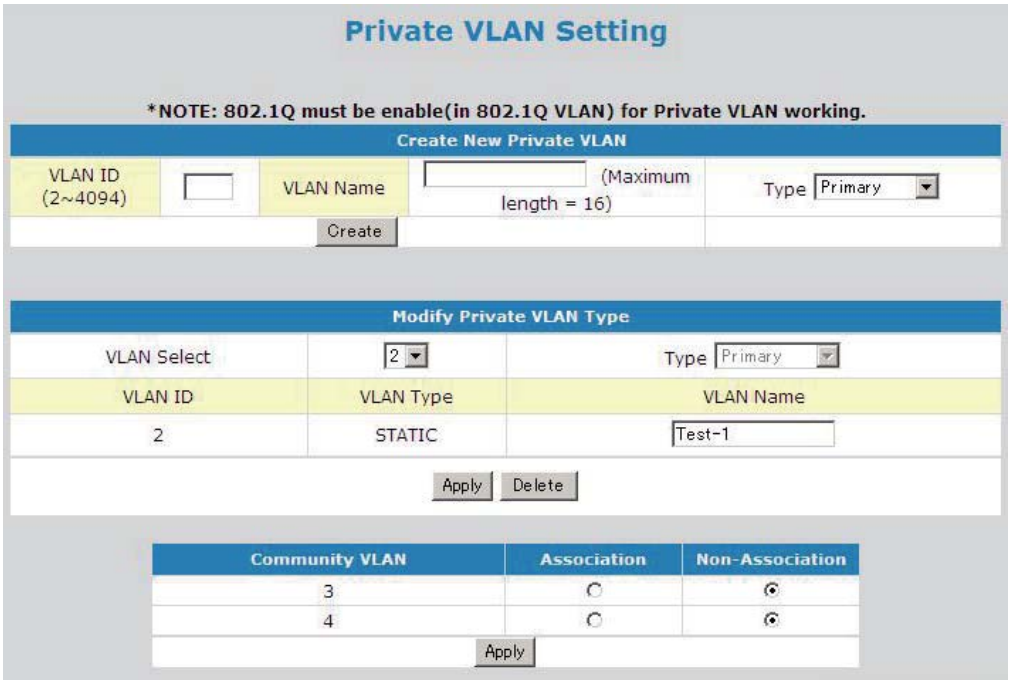
Private VLAN 設定



プライベート VLAN は以下の手順で作成します。

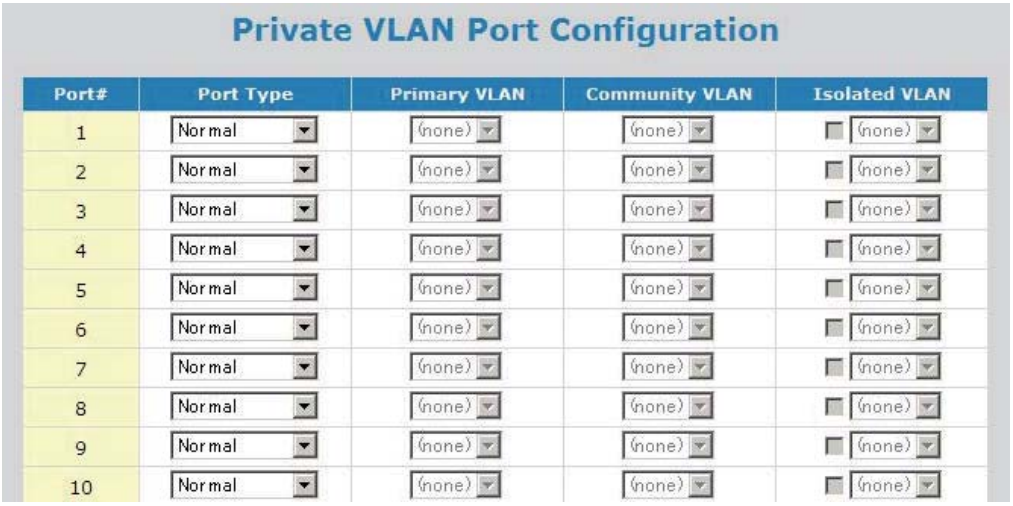
（1）VLAN グループを作成し、"Primary", "Community", または "Isolated" を指定します。

（2）Community VLAN と Primary VLAN の関連付けを行います。もしひとつ以上の Primary VLAN が存在する場合、まず Primary VLAN を選択し、その後に関連付けを行います。



ポート設定

VLAN を作成後、VLAN にポートを登録します。



ポートには ”Normal”、“Host” 、” Promiscuous” の 3 種類があります。

”Normal” は、プライベート VLAN の代わりに標準的なオペレーションを行います。

“Host” は、Community VLAN または Isolated VLAN になれます。

” Promiscuous” は Primary VLAN または Isolated VLAN になれます。

以下の手順でポートの関連付けを行います。

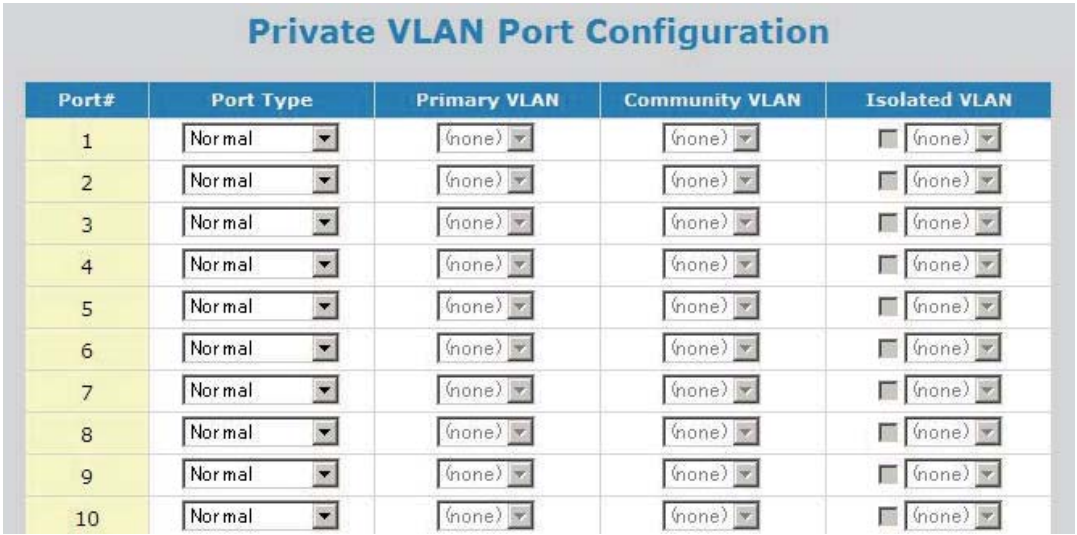
（1）ポートのタイプを選択します。

（2）"Host" の場合、Community VLAN または Isolated VLAN を選択します。

（3）” Promiscuous” の場合、Primary VLAN または Isolated VLAN を選択します。

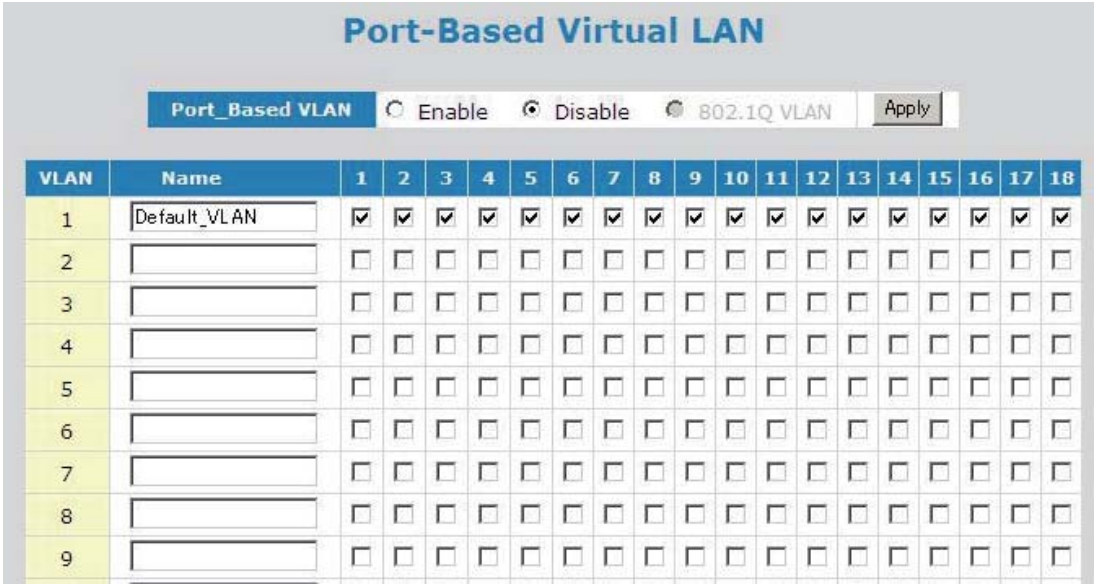
（4）（1）～（3）を繰り返し、ポートの関連付けを完了します。

（5）"Apply" をクリックします。



[注意]　Isolate mode は未サポートとなります。

2.6.3 ポートベース VLAN（Port-based VLAN）



以下の手順でポートベース VLAN の設定を行います。

（1）Port-based VLAN **を有効にし、**"Apply" **をクリックします。**

（2）VLAN **ネームを設定します。**

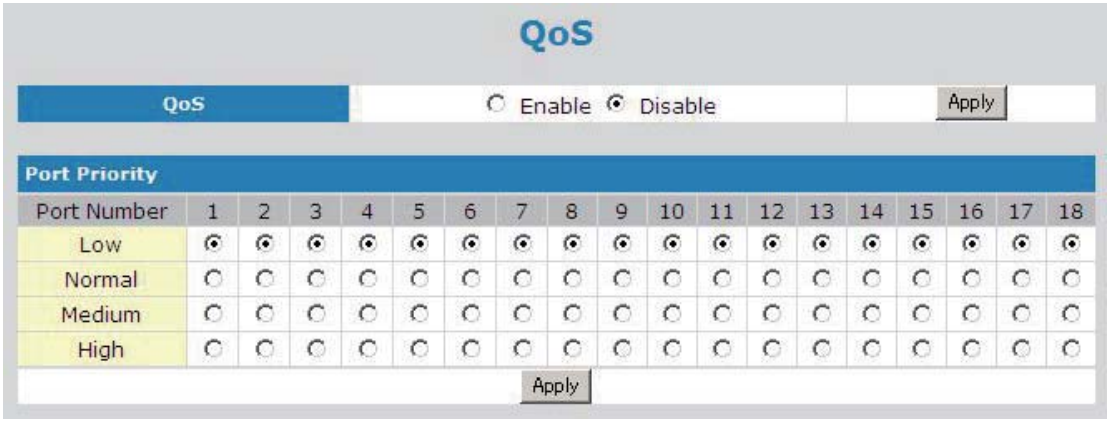
（3）**それぞれの** VLAN **に所属させるポートを選択します。**

（4）"Apply" **をクリックします。**

2.7 QoS

本機はポートベース、802.1p、DSCP **の優先度をサポートしています。**

2.7.1 QoS 情報



QoS

QoS **機能の有効 / 無効を設定します。**

802.1P Enable

ポートごとの 802.1P **プライオリティ機能の有効 / 無効を設定します。**"VLAN Tag Priority" **ページで、**802.1P **プライオリティ値（**0 ～ 7**）をプライオリティキューにマッピングします。**

DSCP Enable

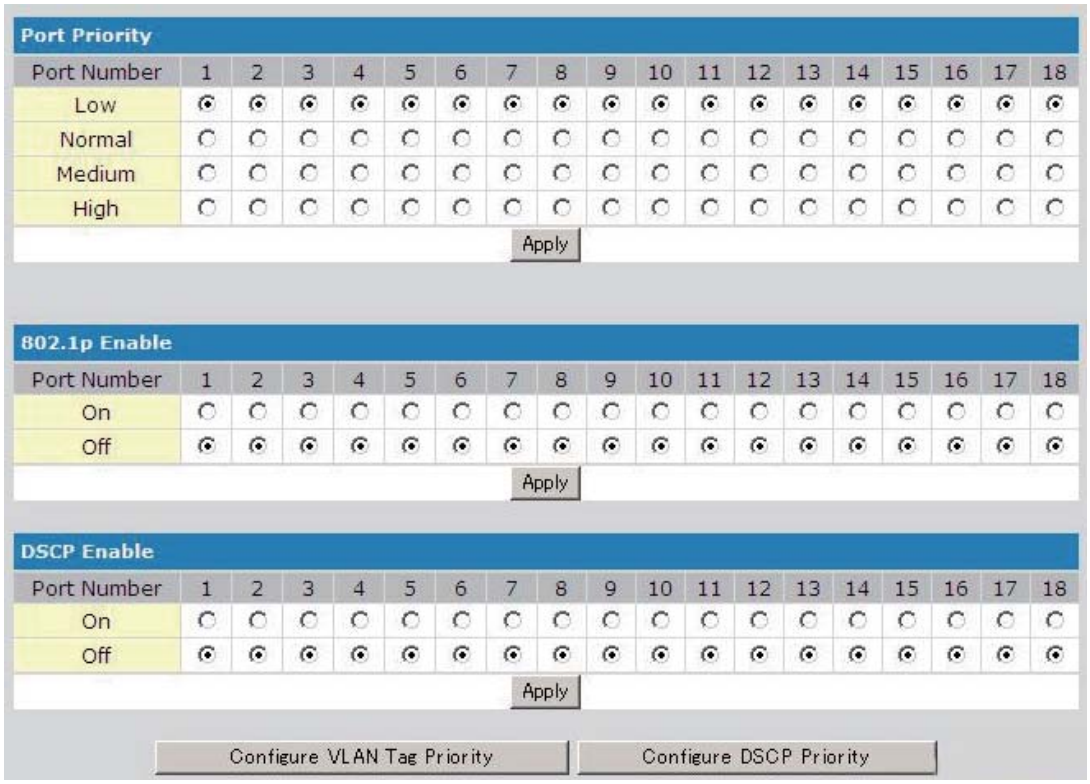
ポートごとの、DSCP（Differential Service Code Point）**プライオリティの有効 / 無効を設定します。**7 **つの** DSCP **値（**0 ～ 63**）をプライオリティキューにマッピングします。**

【Configure VLAN Tag Priority】

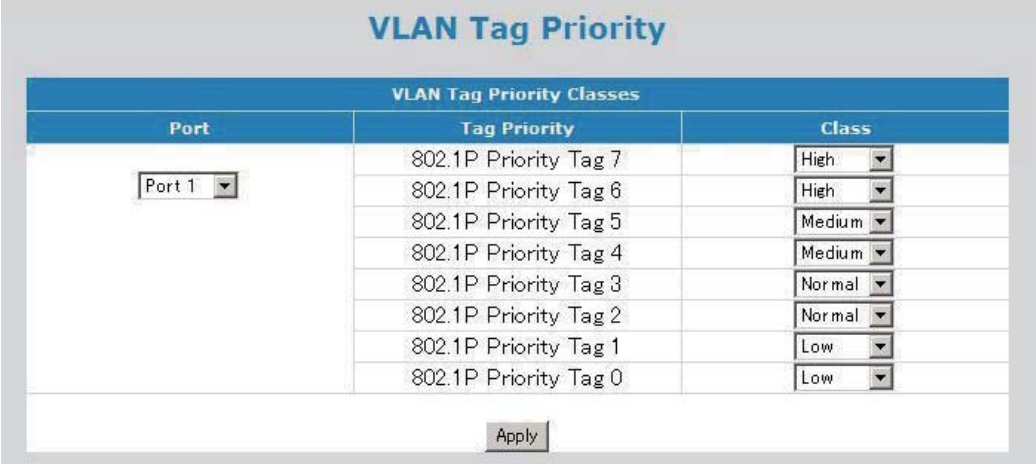
クリックすることで "VLAN Tag Priority" **ページへ移動します。**802.1P **プライオリティ値（**0 ～ 7**）をプライオリティキューへマッピングします。**

【Configure DSCP Priority】

クリックすることで "IP Differential Service (DiffServ) Configuration" **ページへ移動します。**DSCP **プライオリティ値（**0 ～ 63**）をプライオリティキューへマッピングします。**



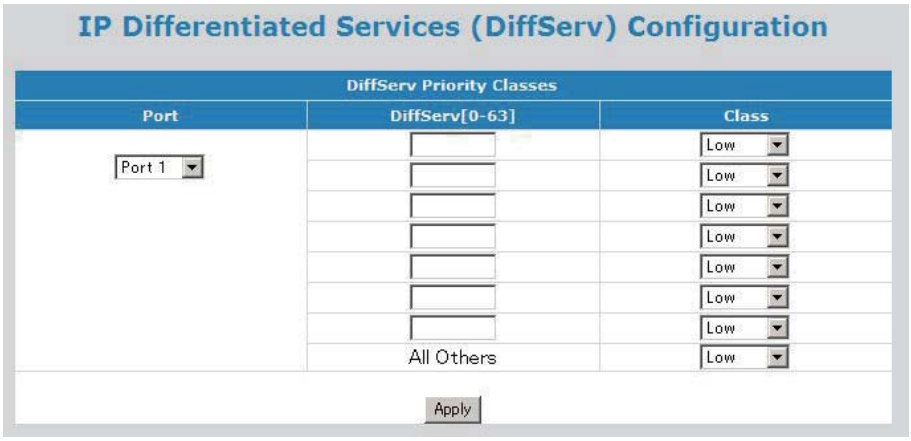
【802.1P Priority Mapping】



VLAN **タグの、**802.1P **プライオリティ値（**0 ～ 7**）が** QoS **に使用されます。**

ここで、プライオリティ値をプライオリティキュー（High/Middle /Normal/Low**）へマッピングすることができます。**

【DiffServ Priority Mapping】



DSCP プライオリティは、IP パケット ToS フィールドを QoS に使用します。

ここで、7 つの DSCP 値（0 ～ 63）をプライオリティキュー（High/Middle /Normal/Low）に定義することができます。

2.7.2 キューモード

本機は、Strict Priority と WRR（Weight Round Robin）をサポートしています。

2.7.3 キュースケジューリング

WRR 使用時の、プライオリティキューのウェイト設定を行います。

2.8 トランク

本機は 8 つのトランクグループをサポートしています。
トランクグループは静的トランクまたは LACP（Link Aggregation Control Protocol）で設定を行うことができます。

2.8.1 トランク情報

トランクを設定するには、以下のステップを実行してください。
（設定が完了するまで、トランクケーブルの接続を行わないでください）

（1）まず、トランク機能を有効にします。

（2）"Grp#" からトランクグループを選択します。

（3）メンバーポートを選択します。

（4）"Apply" をクリックします。

（5）（1）～（4）を繰り返し、その他のトランクグループを設定してください。

[注意] ポートがいずれかのトランクグループの静的ポートに使用されている場合、LACP 機能は無効になります。

2.8.2 LACP ポート設定

ここでは LACP **機能の設定を行います。**

LACP **を設定するには、以下のステップを実行してください**
（設定が完了するまで、トランクケーブルの接続を行わないでください）

（1）**まず、**"Trunk Information" **ページにて、トランク機能を有効にし、**"Apply" **をクリックします。**

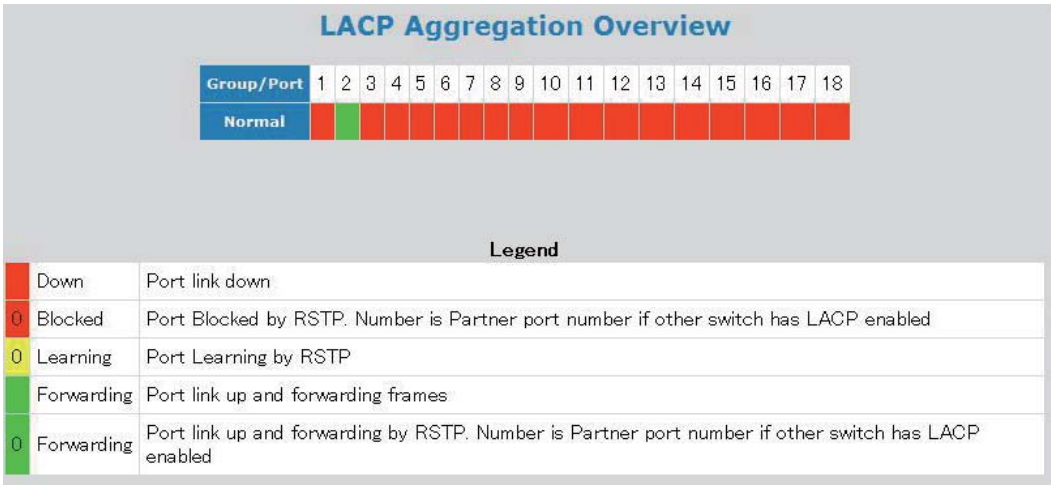
（2）**システムプライオリティを割り当てます。（範囲：**1 ～ 65535　**一番高い番号が一番低いプライオリティになる）**

（3）LACP **ポートを選択します。**

（4）"Apply" **をクリックします。**

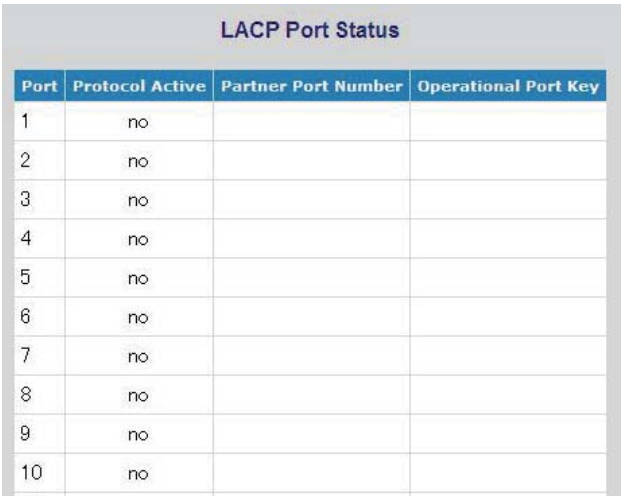
[注意]　ポートがすでに静的トランクグループに属している場合、LACP ポートのメンバーになることはできません。静的ポートが LACP　**ポートに選択されている場合、"Apply" をクリックした後に警告の画面が表示されます。**

2.8.3 LACP ポートの状態



LACP プロトコルのランニングステータスです。
この画面で、現在のステータスを確認することができます。LACP トランクが作成されている場合、ポートグループメッセージが表示されます。

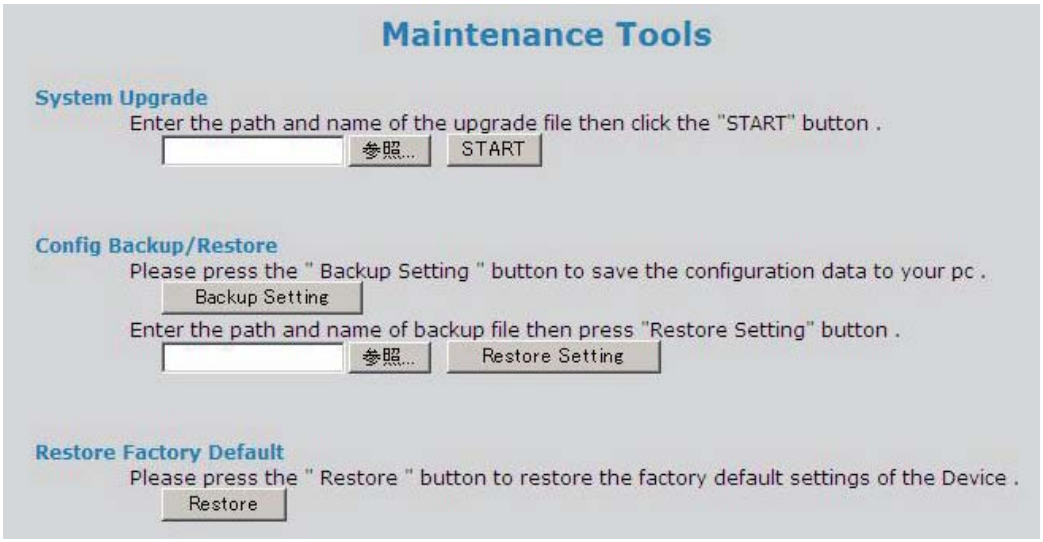
"Refresh" をクリックすることで最新の情報にアップデートできます。
下のテーブルは、各ポートの LACP の有効 / 無効を表示します。



2.9 ツール

以下の機能はシステムメンテナンスに使用されます。

2.9.1 メンテナンスツール



System Upgrade

Web **マネージメント** PC **より、システムオペレーションソフトウェアのアップグレードをおこないます。**

Config Backup/Restore

[Backup Setting] **ボタンをクリックします。スイッチのバックアップ設定を行うことができます。**

設定ファイルを選択後、[Restore Setting] **ボタンをクリックすることで、スイッチの設定を初期状態に戻すこともできます。**

Restore Factory Default

スイッチの設定を工場出荷状態に戻すことができます。

Reset System

スイッチのリブートを行います。

2.9.2 Ping

スイッチより、ネットワーク上のデバイスへ Ping **を送信することができます。**

Target IP address

Ping **送信先** IP **アドレスを指定します。**

count

Ping **を送信する回数を指定します。**

Timeout

Ping **送信のタイムアウト値を指定します。**

上記の設定を行った後、"Apply" **をクリックします。**

2.10 ソフトウェアアップデートとバックアップ

本機はソフトウェアアップデートおよび設定のバックアップ / アップデート / リストア機能をサポートしています。

これらには 2 **通りの手順があります。**

2.10.1 コンソール

XModem **プロトコルをサポートする** VT100 **互換のターミナルソフトウェアを利用し**

シリアル接続で行えます。

この機能は run-time **コードと** boot **コードのアップデートに使用できます。**

（boot **コードは、メインプログラムが起動する前の、システム起動時のみ動作します）**

ソフトウェアにコンソールを使用する場合、ターミナルソフトウェアのボーレートを 38400 **に設定してください。**

その後スイッチの再起動をおこないます。

スイッチの起動時に、<Ctrl> **と** <C> **キーを押すと、以下のメッセージが表示されます。**

```
Boot Menu
============================
0: Start the Run-time code
1: Upgrade Run-time code
2: Upgrade Boot Code

=> Select:
```

- Start Run-Time Code
  この項目を選択すると、システムはブートプロセスを続行します。通常のオペレーションをおこなうため、ボーレートを 9600 **に設定してください。**

- Upgrade Run-time Code
  ターミナルプログラムから、Xmodem **で** run-time **コード（メインコード）のアップデートをおこないます。**
  この項目を選択した場合、以下のメッセージが表示されます。

```
Waiting to receive file by Xmodem ....
```

  ターミナルプログラムの " **ファイル送信** " **機能を選択し、**Xmodem **プロトコルとアップデートファイルを指定すると、ファイルアップグレードが開始します。**

- Upgrade Boot Code
  ターミナルプログラムから、Xmodem **で** boot **コードのアップデートをおこないます。**
  ターミナルプログラムの " **ファイル送信** " **機能を選択し、**Xmodem **プロトコルとアップデートファイルを指定すると、ファイルアップグレードが開始します。**

2.10.2 Web ブラウザ

Web **ブラウザから** http **プロトコルを利用しておこないます。詳細は** P35 **「ツール」を参照してください。**

ES1018V2/ES1024V2 Management Guide (FXC08-DC-200019-R2.0)

初版	2008 **年** 9 **月**
第 2 **版**	2008 **年** 10 **月**
第 3 **版**	2009 **年** 6 **月**

Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide
ES1018V2ES1024V2
Management Guide

FXC株式会社