

LAYER3 INTELLIGENT SWITCH

FML-24

PLANEX COMMUNICATIONS INC.

本製品を安全にお使いいただくために

⚠ 警告

本製品をご利用の際は、以下の注意点を必ずお守りください。これらの事項が守られない場合、感電、火災、故障などにより使用者の重傷または死亡につながるおそれがあります。

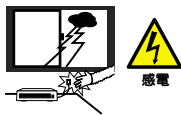
分解・改造・修理はダメ！

各部のネジを外したり、カバーを開けたりしないでください。また製品内部の部品を改造・交換しないでください。感電や火災につながるおそれがあります。



雷のときはさわらないで！

雷が発生している間は、製品各部およびケーブルにさわらないでください。感電するおそれがあります。



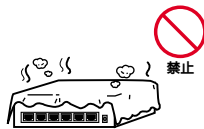
正しい電圧で使用して！

指定の電圧以外で使用すると誤動作や火災につながるおそれがあります。



通気口をふさがないで！

内部に熱がこもり、誤動作や火災につながるおそれがあります。



タコ足配線・無理な配線はダメ！

コンセントや電源タップの定格を超えて電気製品を接続すると、発熱し火災につながる危険があります。



電源コードをつけて移動しないで！

本製品を設置・移動する際は、必ず電源コードを前もって抜いておいてください。電源コードを入れたまま移動し、コードが傷つくと誤動作や火災につながるおそれがあります。



液体・異物は入れないで！

製品内部に液体や異物が入ると、ショートして火災が発生したり、誤動作したりする可能性があります。

万一異物や液体が入ってしまった場合は、電源コードをコンセントから外して弊社サポートセンターまでご連絡ください。



電源コードは傷つけないで！

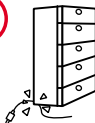
火災・感電につながるおそれがありますので、電源やACアダプタのコードは絶対に加工したり傷つけたりしないでください。また以下の点を守ってコードを傷めないようにしてください。

コードの上に物を載せない

熱源の側にコードを置かない

コードをかじる癖のあるペットは隔離する

(かじった部分からショートし発火する危険があります)



設置・保管場所をもう一度確認して！

以下の場所での本製品のご利用や保管は避けてください。これらの場所で設置・保管を行うと誤動作や感電、火災につながる危険があります。

- ・本製品が落下する可能性のある不安定な場所
- ・直射日光のあたる場所
- ・高温または多湿の場所（暖房器具の側も含む）
- ・急激に温度変化する可能性のある場所（結露のおそれがある所）
- ・振動の激しい場所
- ・ほこりの多い場所
- ・静電気を帯びやすい場所（絨毯の上も含む）
- ・腐食性のガスが発生する場所



おねがい

本製品のお手入れ

- ・本製品のお手入れは乾いた柔らかい布で行ってください。
- ・汚れがひどい場合は、水で薄めた中性洗剤に布を浸し、かたく絞って本製品を拭いてください。また最後に乾いた布で軽く拭いてください。
- ・台所用中性洗剤以外は使わないでください。シンナーやベンジン、ワックス、アルコールが入ったものは使用できません。

目次

| | | |
|-----|----------------------------|-----|
| 第1章 | はじめに | |
| | 1. 概要 | 4 |
| | 2. 特長 | 5 |
| | 3. 梱包内容の確認 | 6 |
| | 4. 各部の名称 | 6 |
| 第2章 | インストール | |
| | 1. 本製品の設置 | 10 |
| | 2. 電源ケーブルの接続 | 12 |
| 第3章 | スイッチの管理 | |
| | 1. 設定オプション | 14 |
| | 2. シリアルポートとの接続 | 15 |
| | 3. ネットワーク経由での接続 | 16 |
| 第4章 | コンソールインターフェイス | |
| | 1. 基本操作 | 18 |
| | 2. ログインスクリーン | 19 |
| | 3. Main Menu | 20 |
| | 4. System Information Menu | 21 |
| | 5. Management Setup Menu | 24 |
| | 6. Device Control Menu | 38 |
| | 7. Network Monitor Menu | 77 |
| | 8. System Restart Menu | 103 |
| | 9. Exit | 104 |
| 第5章 | Webベース管理 | |
| | 1. Webベース管理エージェントについて | 105 |
| | 2. Webブラウザインターフェイスを操作する | 106 |
| | 3. メインウィンドウ | 106 |
| | 4. Mgmt Setup | 114 |
| | 5. Device Control Menu | 125 |
| | 6. Network Monitor | 158 |
| | 7. System Restart Menu | 185 |

第6章 詳細解説

| | |
|---|-----|
| 1. レイヤ2スイッチング | 186 |
| 2. マルチキャスト・スイッチング | 189 |
| 3. スパニングツリーアルゴリズム | 190 |
| 4. レイヤ3スイッチング | 193 |
| 5. 初期設定 | 193 |
| 6. IPスイッチング | 194 |
| 7. Routing Path Management(ルーティングパスの管理) | 196 |
| 8. ICMP Router Discovery | 197 |
| 9. ルーティングプロトコル | 198 |
| 10. RIP/RIP-2 動的ルーティングプロトコル | 199 |
| 11. OSPFv2動的ルーティングプロトコル | 201 |
| 12. 非IPプロトコル・ルーティング | 202 |
| 13. VLAN | 202 |
| 14. VLANへのポート割り当て | 204 |
| 15. ポート・オーバーラッピング | 205 |
| 16. ポートベースVLAN | 205 |
| 17. 自動VLAN登録 (GVRP) | 206 |
| 18. タグ付/タグ無しフレームの転送 | 207 |
| 19. VLANグループの接続 | 207 |
| 20. マルチキャストフィルタリング | 209 |
| 21. IGMPスヌーピング | 210 |
| 22. IGMPプロトコル | 211 |
| 23. GMRPプロトコル | 212 |
| 24. DVMRPルーティングプロトコル | 213 |
| 25. CoS (Class-of-Service) サポート | 214 |
| 26. セキュリティ機能 | 215 |
| 27. SNMPコミュニティストリング | 215 |
| 28. ユーザー名およびパスワード | 216 |
| 29. MACアドレスフィルタ | 216 |
| 30. IPアドレスフィルタ | 216 |
| 31. SNMP管理ソフトウェア | 217 |
| 32. リモート監視 (RMON) | 217 |

| | | |
|-----|---------------|-----|
| 付録A | RS232Cのピンアサイン | 220 |
| 付録B | 製品仕様 | 221 |
| 付録C | 用語集 | 224 |
| 付録D | 出荷時設定 | 227 |

《マニュアル内の表記について》

本マニュアル内では製品の名称を本製品と表記します。区別が必要な場合は製品型番で表記します。

User's Manual Version 1.0

No.PCM-00-10-JF/YM-FML24

1.はじめに

1. 概要

FML-24はIEEE802.3 10BASE-TおよびIEEE802.3u 100BASE-TX規格に準拠したラックマウント・サイズのレイヤ3/レイヤ2ファストイーサネット・マネージメント・スイッチです。FML-24は、ASICによるワイヤースピードIPルーティング機能を実現します。

オートネゴシエーションに対応したRJ-45 STPポートを24ポートと1ポートIEEE802.3z 1000BASE-SXモジュールがインストール可能な拡張スロットを1スロット装備しています。

本製品は802.1QVLAN機能や802.1pプライオリティ制御、802.1dスパニングツリー、マルチキャストなどの機能に加えSNMP、Webベース・マネジメント、Telnet、RS232Cコンソールなどでネットワーク管理が可能です。また、RMONを使用したStatistics , History ,Alarm ,Eventの4グループをサポートしておりシステム管理者の負担を軽減します。

2. 特長

IEEE802.3 10BASE-T、IEEE802.3u 100BASE-TX規格に準拠
100BASE-TX/10BASE-T接続用のRJ-45 STPポートを24ポート装備
1000Base-SXオプションモジュール用拡張用スロットを2ポート装備

Autonegotiation機能により、転送速度(100/10Mbps)および転送モード(全二重/半二重)を自動認識可能

合計8.52Gbpsの帯域幅をサポート

MACアドレステーブルを装備し、最高32KのMACアドレスを自動学習可能

4MByteの packets バッファを装備

フローコントロール対応(全二重時IEEE802.3x、半二重時バックプレッシャー)

標準19インチラックにマウント可能

IEEE802.1Q VLANに準拠(ポートベース256グループ)

IEEE802.1Q/p準拠により2レベルのプライオリティ管理

IEEE802.1d スパニングツリー準拠

2/4/8ポートTrunkに対応

IGMPマルチキャストに対応

RIP , RIP-2 , に対応

SNMP、Webベースマネージメント、Telnetを使用したネットワーク管理が可能

MIB2、BridgeMIBに対応

ネットワーク管理用のRS-232Cコンソールポート(D-SUB9ピン)を装備

Statistics、History、Alarm、Eventの4グループのRMONに対応

冗長電源に対応

3. 梱包内容の確認

パッケージには、以下の付属品が含まれます。

FML-24本体

設定用RS232Cケーブル

電源ケーブル

ラックマウント用金具 2個

ネジ

ゴム足 4個

保証書

このユーザズ・マニュアル

不足品がある場合は、販売店または弊社テクニカルサポートまでお問い合わせください。

4. 各部の名称

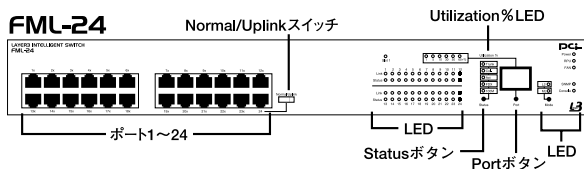


図1-1 FML-24 前面図

前面パネル

「ポート1~24」

100BASE-TX/10BASE-Tツイストペアケーブル接続用のRJ-45ポートです。

「Normal/Uplinkスイッチ」

ポート24をアップリンクポートとして使用する場合は、スイッチをUplink側に設定してください。

「Link LED」

ポートのリンクが確立すると点灯します。

「Status LED」

Statusボタンで選択されている項目の状態を点灯または点滅で表示します。

「Status ボタン」

Status LEDで表示させたい項目を選択します。100M、FDX、Act、Col、Trunkから選択可能です。

100M：100BASE-TXでポートのリンクが確立すると点灯します。

FDX：ポートが全二重モードで通信中は点灯します。

Act：ポートがデータの送受信中は点滅します。

Col.：ポートでコリジョンが検出されると点滅します。

Trunk：トランクポートとして設定されているポートのLEDが点灯します。

「Utilization % LED」

ポートボタンで選択されているポートの使用率を1、5、10、30、50、65 + パーセントで表示します。

「Port ボタン」

Utilization % LEDで表示させたいポートを選択します。

「Mode LED」

Layer2またはML(マルチレイヤ)モードを選択します。

「Power LED」

ハブに電源が入ると点灯します。

「RPU LED」

冗長化電源が接続されている場合に点灯します。

「FAN LED」

側面のFanが正常に動作している場合は点灯します。

背面パネル

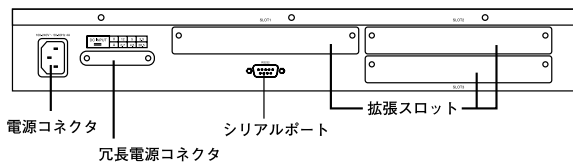


図1-2 FML-24 背面図

「拡張スロット」

1000BASE-SXオプションモジュールをインストールして使用します。

「シリアルポート」

コンピュータと付属のシリアルケーブルを接続します。

「電源コネクタ」

電源ケーブルを接続します。

「冗長電源コネクタ」

冗長電源ユニットを接続します。

裏面ステッカー

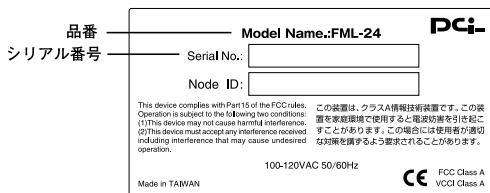


図1-3 裏面ステッカー

「品番」

本製品の製品型番です。

「シリアル番号」

本製品のシリアルナンバーです。製品外箱に記載されているものと同じ番号です。ユーザ登録時に必要となります。また、製品故障時などにサポートを受ける場合にも必要となります。

2. インストール

本章では、本製品のインストール方法を説明します。本製品はデスクトップなど平らな場所でそのままお使いいただけるほか、標準の19インチラックにもマウントすることが出来ます。FML-24のインストールの概略は、以下の通りです。

1. 製品をパッケージから取り出す。
2. 製品本体を設置する。
3. 電源ケーブルを接続する。
4. 各端末、イーサネットハブおよびイーサネットスイッチと接続する。

1. 本製品の設置

本製品は、必ずデスクトップなどの平ら場所で使用してください。他のハブとカスケードして設置する必要がある場合は、19インチラックへの収納を推奨します。

注意 本マニュアルの製品仕様で定められている温度、湿度内で近くに熱源がない場所に本製品を設置してください。又、本製品のファン取りつけ口に埃などが堆積しない様に注意してください。十分な冷却が出来ない場合、誤動作または、故障などの原因になります。

デスクトップへの設置

1. 製品底面の4隅に、付属のゴム足をはり付けます。
2. 本製品を平らな場所に設置してください。

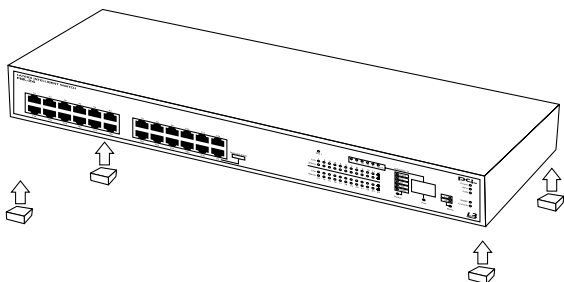


図2-1 ゴム足の取り付け

ラックマウントへの取り付け

以下の手順で本製品を19インチラックに取り付けてください。

1. 本製品の底面に既にゴム足がついてある場合は、すべてゴム足を取り外してください。
2. 製品側面にある、ラックマウント用のネジ穴を確認してください。
3. 付属のネジを使って、ラックマウント用金具を製品側面にとりつけます。プラスのドライバーをお使いください。

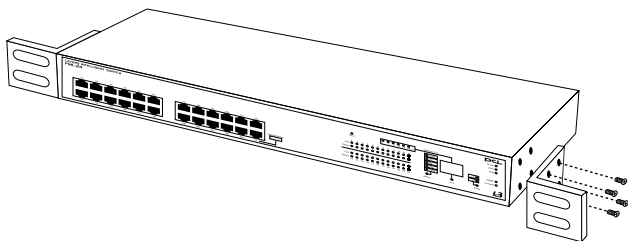


図2-2 ラックマウント用金具の取り付け

4. 本製品をラック内に配置し、ラックマウント用金具上の穴と、19インチラックのシャーシ上の穴とを合わせます。
5. 19インチラックに付属しているマウント用ネジを4つ用意し、ラックマウント用金具に差し込んで固定してください。

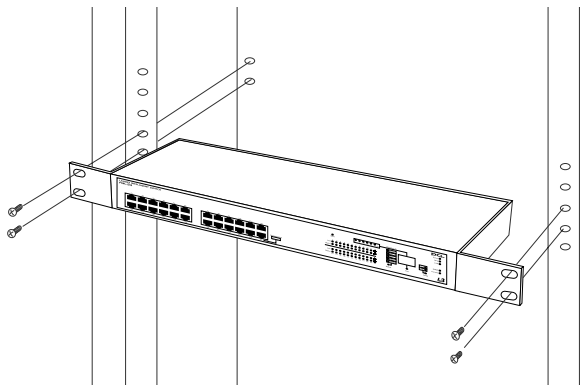


図2-3 ラックへの取り付け

2. 電源ケーブルの接続

電源ケーブルの接続は、以下の方法で確実に行ってください。

1. 製品背面の電源ケーブル接続部に、電源ケーブルを接続します。
2. 電源ケーブルを、3芯タイプのプラグに対応した(アース対応)コンセントに接続します。
3. Power LEDがに点灯していれば正常です。

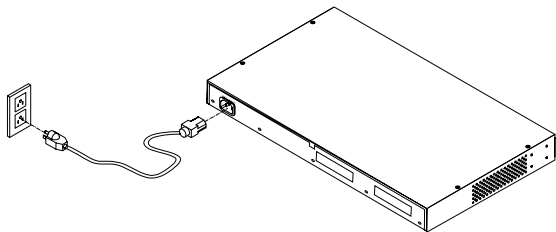


図2-4 電源ケーブルの接続

注意 本製品は起動時に自己診断テスト及び設定の読みこみを行います。そのため、電源投入から使用開始までの時間はしばらくかかります。

3. スイッチの管理

1. 設定オプション

本製品は優れた管理エージェントを搭載しており、メニュー式の設定プログラムを使って本製品の設定および管理を行えるようになっていきます。当プログラムは、製品背面のシリアルポートに直接アクセス可能なほか、Telnetを使ったネットワーク経由での接続にも対応しています。

管理エージェントはSNMPを採用しています。SNMPエージェントと管理ソフトウェアを使用することにより、本製品はネットワーク上のどのPCからでも管理することが可能となっています。

管理エージェントにはさらにHTTP Webエージェントも含まれます。Webエージェントは、ネットワークに接続されているどのコンピュータからでも標準のWebブラウザ経由で使用することが可能です。

システム設定プログラムとSNMPエージェントは、以下の管理機能を提供します。

- 各ポートを有効/無効に設定
- 各ポートの通信モードを設定
- SNMPパラメータ設定
- ネットワークVLANへのポート追加
- IPルーティングおよびマルチキャストVLANの設定
- システム情報および統計の表示
- スパニングツリー用に本製品を設定
- システムファームウェアのダウンロード

2. シリアルポートとの接続

製品本体のシリアル・コンソールインターフェース(RS-232)ポート経由でパソコンを接続し、本製品の設定および監視を行うことができます。当ポートはメス型DB-9コネクタを使ったDCE(データ通信機器)接続ポートです。コンソールポートを使用される場合は、ターミナルユーティリティがインストールされているパソコンが必要となります。

注意 Windows95/98に標準でインストールされるターミナルユーティリティでは矢印キーが正常に動作しません。WindowsNT/2000もしくは汎用のターミナルユーティリティを使用してください。

1. ターミナルユーティリティの設定

- ・ 19,200ボー(デフォルト設定)
- ・ パリティなし
- ・ 8ビット
- ・ 1ストップビット
- ・ Window Terminal Emulatorオプションは「なし(NO)」に設定
- ・ Terminal Preferences で Function、Arrow、Controlキーはすべて有効に設定

2. シリアル接続ケーブル

DB-9オス型コネクタ付ストレートRS232ケーブル が付属しています。ご使用のコンピューターがDB-9オス型コネクタを装備しているか確認してください。(ほとんどのコンピューターでDB-9オス型コネクタが使用出来ます。)

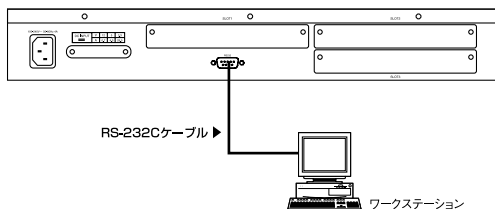


図3-1 RS232Cケーブルとの接続

3. ネットワーク経由での接続

ネットワーク経由で本製品に搭載されているエージェントに接続する前に、まずコンソール接続を行って、このエージェントにIPアドレス、サブネットマスクおよびデフォルトゲートウェイ(レイヤ2モード時)をそれぞれ正しく設定する必要があります。本製品のIPパラメータ設定が完了すると、接続されたネットワーク内であればどこからでも本製品上の設定プログラムにアクセスできるようになります。アクセスはTelnetで行えるほか、Webブラウザ経由でも接続できるようになっています。(対応ブラウザ：Internet Explorer 4.0以降、Netscape Navigator 4.0以降)

注意 1. デフォルトではBOOTPは無効に設定されています。 2. VLANグループには、それぞれ固有のIPインターフェースアドレスを割り当てるのが可能です。このため管理ステーションに接続しているポートが複数VLANに所属している場合は、本製品はこれらのどのIPアドレスからでも管理することが可能となります。 3. 本製品上で使用可能なTelnetセッションは一つだけとなっています(複数セッションを実行することはできません)。 4. 本製品上のプログラムでは、本製品の基本的な設定機能のみアクセス可能となっています。すべてのSNMP管理機能にアクセスするには、SNMP対応のネットワーク管理ソフトウェアを別途ご利用ください。

4. コンソールインターフェイス

コンソールインターフェイスを利用した設定方法を説明します。本文ではシリアルポートからアクセスした場合の操作方法を中心に説明していますがTelnet経由でのアクセスでも同様の操作が可能です。

1. 基本操作

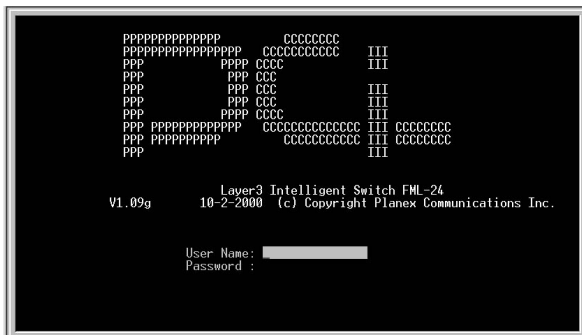
本製品への設定の追加または削除及び更新を行った場合は必ず各スクリーン内にあるApplyを実行してください。一部の設定を除き更新された内容は直ぐにシステムに反映されます。

使用可能キー一覧

- ・ 矢印キー
- ・ Tabキー
- ・ Enterキー

2.ログインスクリーン

本製品のシリアルポートに直接接続するか、またはTelnet接続を行うと、以下のログインスクリーンが表示されます。



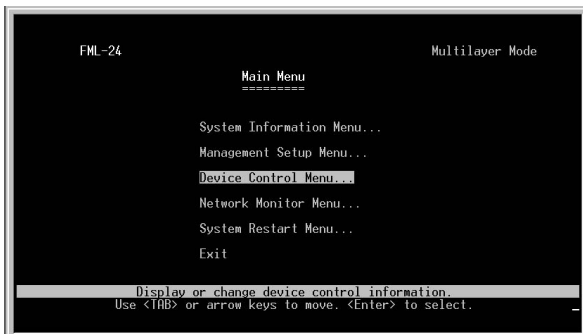
本製品に初めてログインした場合の(使用可能な)ユーザーアカウントはデフォルトで「admin」に設定されています。パスワードは設定されていないので注意してください。Admin (管理者)アカウントはすべての設定パラメータおよび統計に対して読み書きを行う権限がありますが、これに対しguest (ゲスト)アカウントでは管理プログラム上で読みとりのみ実行可能(リードオンリー)となっています。

パスワードを設定するには Management Setup Menuから User Configurationを選択します。パスワードは15文字までの半角英数字が設定可能となっており、大文字・小文字の区別は行いません。

注意 デフォルト設定では、ログイン時のパスワード再入力はいく回まで可能となっています。三度目のパスワードも間違えて入力された場合、接続は自動的に切断されます。

3.Main Menu

システム設定プログラムでは、1)システムパラメータの設定、2)本製品およびその全ポートの管理・制御、ならびに、3)ネットワークの状況監視が行えるようになっています。



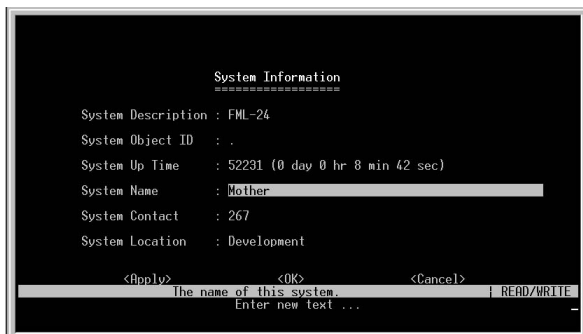
注意 現在選択されているオプションの説明は画面一番下のハイライト部分に表示されます。画面上右端には、本製品がレイヤ2スイッチ/マルチレイヤールーティングスイッチのどちらのモードで動作しているかが文字列で表示されます。

4. System Information Menu



System Information

システム監理者への連絡先やハードウェア/ソフトウェアのバージョン情報など、システムの基本的な情報を参照する場合は System Information Menu を使用します。



「System Description」

システムのハードウェア情報を入力してください。

「System Object ID」

本製品のネットワーク管理サブシステム用MIB IIオブジェクト識別子が表示されます。

「System Up Time」

現在起動している管理エージェント(management agent)の稼働時間が表示 (注: 最初の値は1/100秒) されます。

「System Name *」

本製品に設定されている名称を入力してください。

「System Contact *」

本製品の管理者の情報を入力してください。

「System Location *」

システムの設置場所を入力してください。

* 最大99文字までの入力が可能です。画面に表示されるのは最初の45文字までとなります。残り部分を表示するには矢印キーを使用してください。

Switch Information

本製品のハードウェア/ファームウェアのバージョン番号および電源状態を参照して確認することができます。



「Hardware Version」

マザーボードのハードウェアバージョンが表示されます。

「Firmware Version」

ROM内に保存されているシステムファームウェアのバージョンが表示されます。

「Serial Number」

マザーボードのシリアル番号が表示されます。

「Port Number」

本製品上のポート数が表示されます。

「Internal Power Status」

主電源の使用/非使用が表示されます。

「Redundant Power Status」

予備電源の使用/非使用が表示されます。

「Fan Power Status」

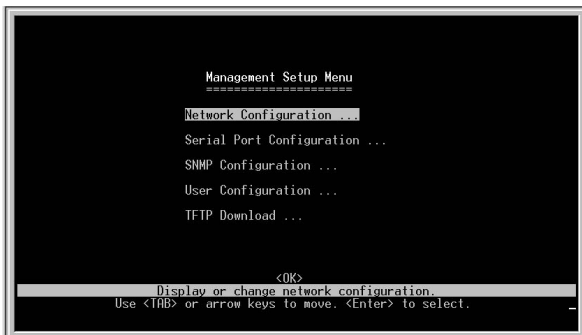
ファン電源の使用/非使用が表示されます。

「Expansion Slot 1」

本製品背面の拡張モジュールスロットにオプションモジュールがインストールされている場合にモジュールのタイプを表示します。

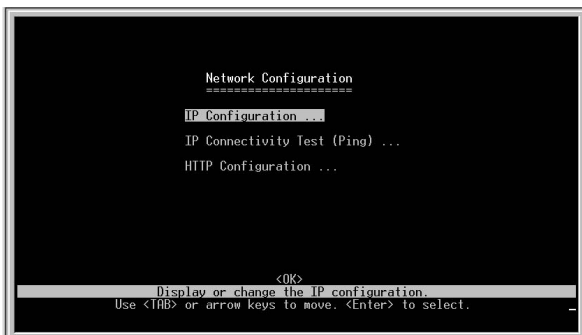
5.Management Setup Menu

初めてシステムにログインした場合は、確実に通信が行えるようにするため通信パラメータの調整を行う必要があります(Serial Port Configuration)。本製品用のIPアドレスを設定し(Network Configuration / IP Configuration)、管理者およびユーザのパスワードを設定します(User Configuration)。これらの情報は、必ず紙に書き写して安全な場所に保存するようにしてください。またコミュニティストリング(文字列)の設定も行ってください(SNMP Configuration)。コミュニティストリングは、管理ソフトウェアを使用して製品上SNMPエージェントへのアクセスを制限します。



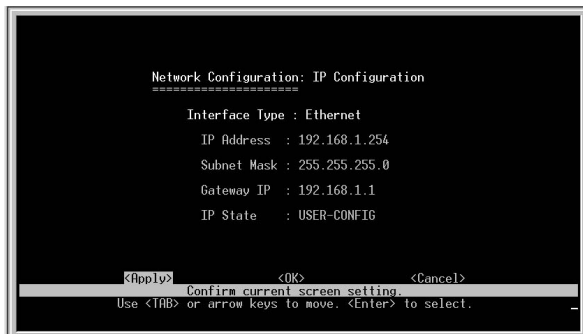
Network Configuration

IP設定(* 1)、PING関連およびHTTP(Webエージェント)を設定します。



IP Configuration

起動オプションを設定したり、また本製品のIPパラメータを設定する場合はIP Configurationスクリーンを使用します。本設定はレイヤー2モード時のみ選択可能です。



「Interface Type」

イーサネット上でIPが利用されていることを示します。

「Subnet Mask」

本製品のサブネットマスクです。当マスクは、特定のサブネットヘルツする際使用されるホストアドレス・ビットを示します。

「IP Address」

現在管理を行っている本製品のIPアドレスです。本製品はUDP/IPトランスポートプロトコル経由でのSNMPに対応しています。この環境では、インターネット上から本エージェントにアクセスする全てのシステム(ネットワーク相互接続機器およびPCなど)はそれぞれIPアドレスが設定されている必要があります。

有効なIPアドレスはピリオド(.)で区切られた四つの番号で表されます。各番号はそれぞれ0~255の範囲で設定します。当設定プログラムは、この形式以外の入力は受け付けないようになっています。

「Default Gateway」

システムのエージェントから管理ステーションにトラップメッセージを渡す際に使用するゲートウェイを指します。

注意 管理ステーションが別のIPセグメント上に存在する場合は必ずゲートウェイを指定してください。

「IP State」

IP機能を手動設定で有効にするか、Boot Protocol (BOOTP) で有効にするかを設定します。設定可能なオプションは以下の通りです。

「USER-CONFIG」

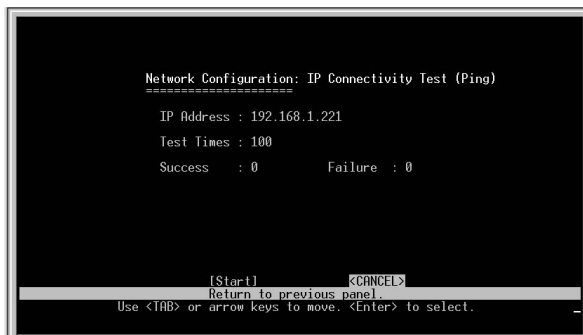
IP機能は、デフォルトまたはユーザーの指定するIP設定に基づき有効となります。(デフォルト設定)

「BOOTP Get IP」

IPは有効となりますが、BOOTPの応答を受信するまで実際に機能しません。本製品は、BOOTPのIPアドレスを確認するため、定期的にBOOTP要求をブロードキャストします。(BOOTP設定値にはIPアドレス、デフォルトゲートウェイおよびサブネットマスクの各情報が含まれます。)

IP Connectivity Test

インターネット上の指定サイトに本製品から接続可能か確認する場合はIP Connectivity Testを使用します。以下に画面内容を説明します。



「IP Address」

Pingテストを行う相手先のIPアドレスです。

「Test Times」

指定サイトに対しIGMPエコー要求を送信する回数を指定します。回数は1～1000回の間で指定可能です。

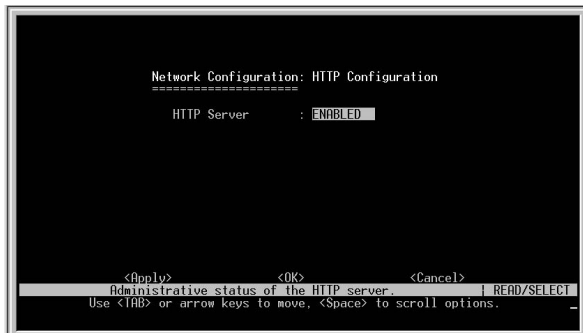
「Success/Failure」

Pingに対し、指定サイトが応答した(もしくはしなかった)回数を示します。

■ **注意** Pingは10m/s間隔で行われます。

HTTP Configuration

本製品上のWebエージェントを有効または無効に設定します。



「HTTP Server」

製品上のWebエージェントへのアクセスを有効/無効に設定

■ **注意** Port 80はHTTPサービス用に既に確保されています。

Serial Port Configuration

本製品背面のシリアルポートにVT100互換機器を接続することで、本製品上の設定プログラムへのアクセスが可能となります。当ポートの通信パラメータは以下のSerial Port Configurationスクリーンからアクセス可能となっています。



「Management Mode」

ポート設定は端末との直接接続用です。

「Baud rate」

機器間のデータ転送速度です。9600、19200および38400のいずれかが選択可能です。

「Data bits」

RS-232ポートのデータ長が設定可能です。7及び8が選択可能です。

「Parity」

RS-232ポートのパリティを設定します。

none(なし)/odd(奇数)/even(偶数)が設定可能です。

「Time-Out」

本製品に接続された機器で一定時間入力がない場合、現在の接続を自動的に切断します。設定範囲：0～100分(0=無効に設定)

「Auto Refresh」

コンソールセッション内でコンソール情報を更新する間隔を指定します。更新する情報にはSpanning Tree Information ,Port Configuration ,Port Statistics およびRMON Statisticsなどが含まれます。設定範囲：0～255秒(0=無効に設定)

SNMP Configuration

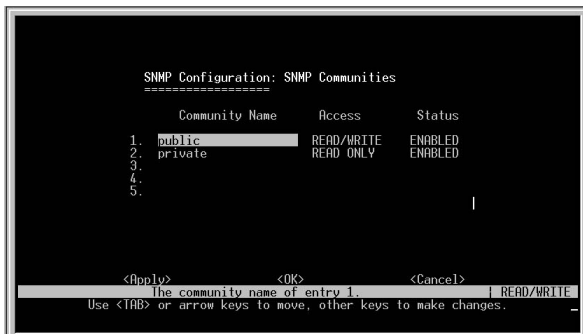
SNMP(Simple Network Management Protocol)関連の設定内容を表示・変更する場合は SNMP Configurationスクリーンを使用します。本製品搭載のSNMPエージェントは、本製品ハードウェアの状態ならびにその各ポートを通過するトラフィックを監視します。これらの情報は、ネットワークに接続されているコンピュータ(NMS=ネットワーク管理ステーション)からアクセスすることが可能です。本製品上エージェントへのアクセス権はコミュニティストリングにより制限されます。本製品と接続する際、NMSはまず有効なコミュニティストリングを送信して認証を受ける必要があります。以下に、コミュニティストリングの設定およびこれと関連するトラップ機能につき解説します。

「Send Authentication Fail Traps」

いずれかのSNMP要求に失敗すると指定IPトラップマネージャにトラップメッセージを送信します。(デフォルトでは有効に設定されています。)

SMMP Communitys

管理アクセスを許可されているコミュニティストリングの設定方法を説明します。



「Community Name」

管理アクセスが許可されているコミュニティ名(エントリ)です。最大19文字までの文字列が入力可能です。

「Access」

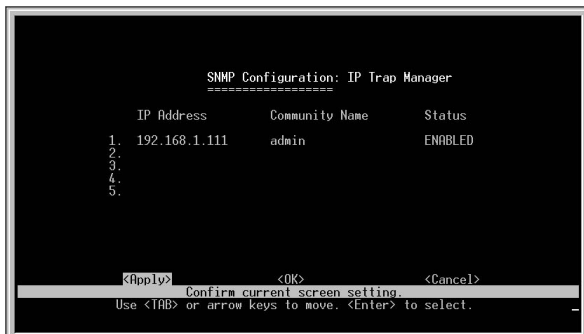
管理アクセスは、Read Only(読み取り専用)か Read/Write(読み書き可)のいずれかのみ設定可能です。

「Status」

エントリの管理ステータスをenabled (有効)またはdisabled(無効)に設定します。

IP Trap Manager

本製品から認証失敗メッセージや他のトラップメッセージを受信する管理ステーションを設定します。トラップマネージャは最大5つまで指定することが可能です。



「IP Address」

トラップマネージャのIPアドレスです。

「Community Name」

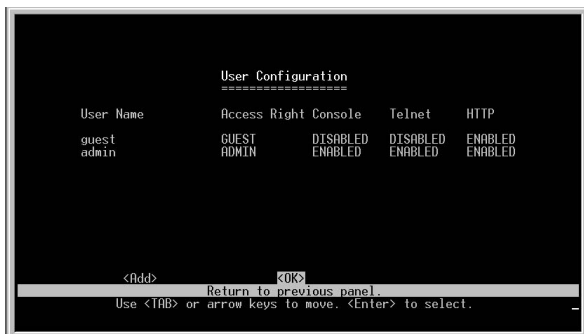
トラップ管理アクセス用のコミュニティを指定します。

「Status」

選択されたエントリの管理ステータスをenabled(有効)またはdisabled(無効)に設定します。

User Configuration

ユーザー名とパスワードで管理アクセスを制限する場合は User Configurationメニューを使用します。ユーザーにはAdministrator(管理者)とGuest(ゲスト)の二種類があります。SNMPエージェント関連パラメータへ書き込み権限はAdministratorにのみ与えられています。このため、出来る限り早急にAdministrator用のユーザー名とパスワードを設定し、この情報を書き留めて安全に保存するようにしてください。(パスワードを忘れてしまったり、またSystem Configuration Programへアクセスできなくなった場合は弊社テクニカルサポートまでご連絡ください。)



「User Name」

ユーザー名を指定します。ユーザーには、端末、TelnetおよびHTTP経由で本製品にアクセスすることが許可されます。

「Access Right」

ADMIN：全スクリーンにおいて読み書きを許可

GUEST：全スクリーンにおいて読み取りのみ許可

「 Console 」

端末経由での管理を許可/禁止します。

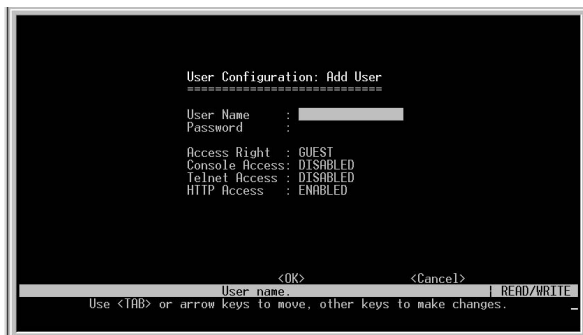
「 Telnet 」

Telnet経由での管理を許可/禁止します。

「 HTTP 」

HTTP (Webブラウザ) 経由での管理を許可/禁止します。

ユーザーを追加する場合はカーソルを <Add> に移動してエンターキーを押してください。



「 User Name 」

ユーザー名を指定します。ユーザーには、端末、TelnetおよびHTTP経由で本製品にアクセスすることが許可されます。

「 Password 」

最大11文字の半角英数字でパスワードを指定します。パスワードは文字の大文字・小文字を区別しません。

「 Access Right 」

ADMIN : 全スクリーンにおいて読み書きを許可

GUEST : 全スクリーンにおいて読み取りのみ許可

「 Console Access 」

端末経由での管理を許可/禁止します。

「 Telnet Access 」

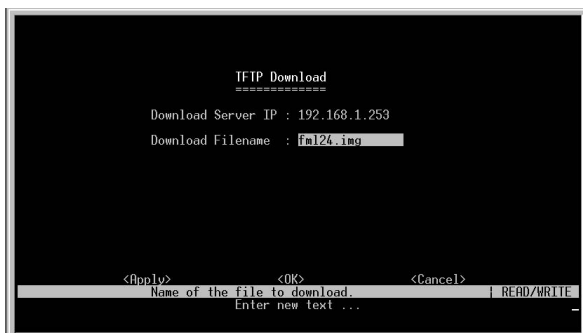
Telnet経由での管理を許可/禁止します。

「 HTTP Access 」

HTTP(Webブラウザ)経由での管理を許可/禁止します。

TFTP Download

本製品内蔵フラッシュROM内に最新版ソフトウェアをダウンロードする場合はTFTP Download メニューを使用します。ダウンロードするファイルはバイナリまたはイメージファイルである必要があります。(エージェントは他の形式のファイルは受け付けません)ダウンロードの成否は、TFTPサーバへの接続性およびネットワーク接続の状態に依存します。最新ソフトウェアをダウンロードすると、エージェントは本製品を自動的に再起動します。



「Download Server IP」

TFTPサーバのIPアドレスです

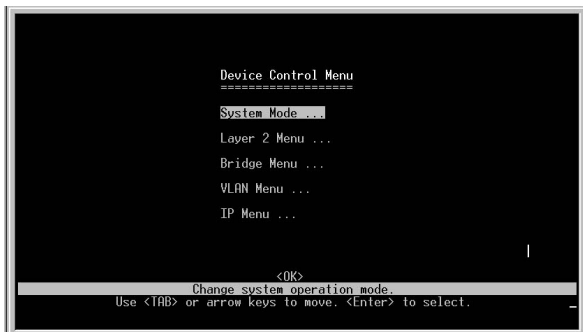
「Download Filename」

ダウンロードするバイナリファイルを指します。

注意 ファームウェアのダウンロードは他にWebエージェントからも可能です。

6.Device Control Menu

Device Control メニューからは、ポートモード、ポートミラーリング、ポート・トランッキング、スパニングツリー、バーチャルLAN、IP サブネット、マルチキャストフィルタリングおよびルーティングプロトコルなど本製品の多くの機能を設定することが可能です。



System Mode

本製品はレイヤ2スイッチまたはマルチレイヤ・ルーティングスイッチとして動作します。レイヤ2スイッチとして設定された場合、フィルタリングおよびフォワーディングの決定はすべて厳密にMACアドレスに基づいて行われます。またマルチレイヤ・ルーティングスイッチとして動作した場合、本製品はすべての非IPプロトコル(NetBEUI、NetWare、AppleTalkなど)パケットをMACアドレスに基づいてスイッチし、すべてのIPパケットを指定されたルーティングプロトコルに基づいてルートします。

注意 システムの動作モードを変更すると本製品は自動的に再起動しますのでご注意ください。



「Layer 2」

全てのプロトコルのトラフィックからフィルタリングおよびフォワーディングの決定をMACアドレスベースで実行します。

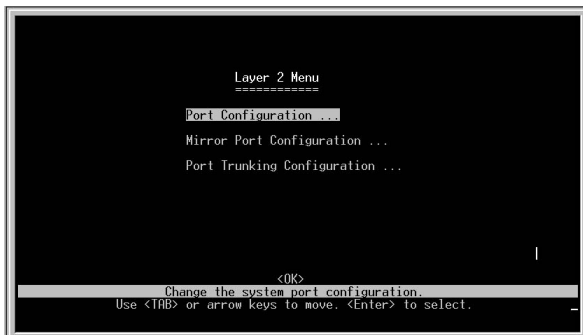
「Multilayer」

全ての非IPプロトコルトラフィックにつき、MACアドレスベースでスイッチングを実行します。またすべてのIPトラフィックをルートします。

注意 マルチレイヤモードで動作している場合、IPメニューが有効になるかわりに「IP設定(レイヤ2モード)」メニューが無効になります。マルチレイヤモードで動作中にVLANグループ同士で通信を行う必要がある場合はすべてVLANグループにIPインターフェースを設定する必要があります。

Layer 2 Menu

各ポートの通信モード、ポートミラーリングおよびポート・トラッキングを設定します。



Port Configuration

本製品上の、指定ポートまたはモジュールの通信パラメータを表示/変更します。設定可能なオプションには、管理ステータス、Auto-Negotiation、デフォルトの通信速度およびデュプレックスモードおよび使用フローコントロールなどがあります。

| Layer 2 Menu: Port Configuration (Port 1-12) | | | | | | | |
|--|-------------|--------------|----------------|--------------|--------------|--------------|-----------|
| Port | Link Status | Admin Status | Auto Negotiate | Default Type | Current Type | Flow Control | Jack Type |
| 1 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 2 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 3 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 4 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 5 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 6 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 7 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 8 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 9 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 10 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 11 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |
| 12 | Off | ENABLED | ENABLED | 10HDX | 10HDX | Off | RJ-45 |

<Apply> <OK> <Cancel> <Prev Page> <Next Page>
 Administrative status for port 1. READ/SELECT
 Use <TAB> or arrow keys to move, <Space> to scroll options.

「Link Status」

ポートが外部機器と正常に接続しているかどうかを示します。

「Admin Status」

コリジョンが多発するなど、異常動作を起こしたポートを無効にし、問題が解決した後またそのポートを有効にします。セキュリティ上の理由でいずれかのポートを無効にすることも可能です。

「Auto Negotiate」

ポート速度、デュプレックスモードおよびフローコントロールのオートネゴシエーションを有効または無効に設定します。1000BASE-SXポートは全/半二重およびフローコントロールのオートネゴシエーションを行いますが、速度は1000Mps固定となります。

「Default Type」

オートネゴシエーションが無効となっている場合、ポートは表示されたスピードおよび転送モードに設定されます。

「Current Type」

現在の転送速度および転送モードを表示します。

「Flow Control」

フローコントロールを有効/無効に設定します。本製品のバッファが一杯の場合、フローコントロールは、エンドステーションや本製品と直接接続されたセグメントから送られてくるトラフィックを遮断してパケットの損失を防ぎます。有効に設定されている場合、半二重ではバックプレッシャーを、また全二重ではIEEE802.3xフローコントロールを使用します。

「Jack Type」

各ポートのジャックの種類を表示します。

「Port 1-24」

RJ-45

「Port 25」

SC

Mirror Port Configuration

本製品上のいずれかのポート(ソースポート)から送られるトラフィックを他のポート(ターゲットポート)にコピー(ミラー)してリアルタイムでトラフィックを解析することが可能です。ターゲットポートにロジックアナライザやRMONプローブなどを接続すると、現状の通信にまったく影響を与えることなく、ソースポートを通過するトラフィックを解析することができます。なお、ポート上のトラフィックをミラーするには、ソース・ターゲットの両ポートとも同じVLANに所属している必要があります。



「Enable Port Mirror」

ミラー機能を有効/無効に設定します。

「Mirrored Ports(Tx/Rx)」

指定ポート上で送信または受信したトラフィックをミラーします。ミラーポートを指定する場合はカーソルを<Add>に合わせてエンターキーを押してください。

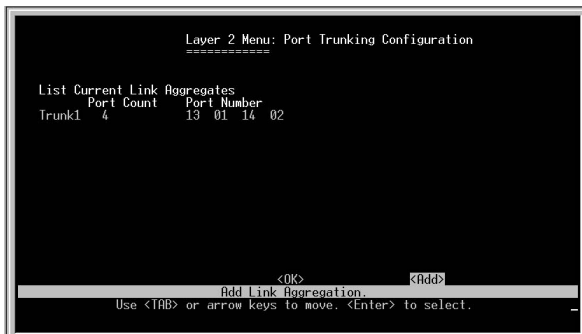
「Monitor Port」

ミラーポート上の送信/受信トラフィックはこのポート上で複製します。

注意 ポートトランクを通過するトラフィックを調べる場合など、複数のポートを一つのポートにミラーすることは可能となっています。ただし、トラフィックの負荷が通常～多大の場合、いくつかパケットが失われる場合があります。

Port Trunking Configuration

複数のポートを合わせて一つのリンクとして使用することにより、ネットワーク接続の帯域幅を増やしたり、いずれかのポートが使用不可となった場合でも他の予備ルートを使用して接続を維持するなどの冗長化が可能になります。この技術は「トランク」と呼ばれるもので、本製品同士であればトランク接続を行うことができます。本製品上のRJ-45ポートは、2/4/8ポートをまとめて一本のリンク(トランク)にすることにより、全二重通信時にそれぞれ合計400/800/1600Mbpsまでの帯域幅を提供します。トランク内の各ポート上の負荷を分散する以外にも、実際に二台のスイッチ間でトランク接続を行う前に、Port Trunking Configurationメニューを使って各機器のトランク設定を行う必要があります。なおポート・トランキングを行う際は以下の点にご注意ください。



トランクポートとして追加可能なポートはRJ-45ポートのみ使用可能です。

1つのトランクに割り当てられたポートは、他のトランクに割り当てては出来ません。

トランクの設定を両方のスイッチで行う必要があります。

トランクポートは、両方のスイッチで通信モードやVLAN設定などを同じにする必要があります。

トランクに割り当てられたポートはミラー/モニターポートには指定できません。

トランク内のポートを移動したりVLAN上で追加/削除する際は、すべて1グループ単位でまとめて移動/追加/削除を行ってください。

スパニングツリーアルゴリズムは、トランク内の全ポートを1つのリンクとして扱います。

ループの発生を防ぐためにも、スイッチ間を接続する前にトランクを有効にするようにしてください。

「Trunk #」

各トランクはこの番号で識別します。

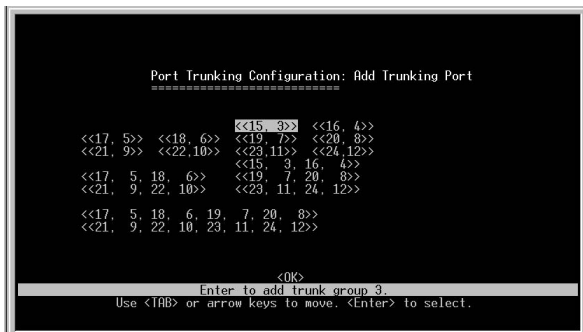
「Port Count」

トランクは2/4/8ポートで構成可能です。

「Port Number」

各トランクに割り当てられているポートです。

トランクを設定する場合はカーソルを <Add> に移動してエンターキーを押してください。設定可能なポート構成は以下の通りです。



・2ポートTrunk

```

<< 13, 1 >> << 14, 2 >> << 15, 3 >> << 16, 4 >>
<< 17, 5 >> << 18, 6 >> << 19, 7 >> << 20, 8 >>
<< 21, 9 >> << 22, 10 >> << 23, 11 >> << 24, 12 >>
  
```

・4ポートTrunk

```

<< 13, 1, 14, 2 >> << 15, 3, 16, 4 >>
<< 17, 5, 18, 6 >> << 19, 7, 20, 8 >>
<< 21, 9, 22, 10 >> << 23, 11, 24, 12 >>
  
```

・8ポートTrunk

```

<< 13, 1, 14, 2, 15, 3, 16, 4 >>
<< 17, 5, 18, 6, 19, 7, 20, 8 >>
<< 21, 9, 22, 10, 23, 11, 24, 12 >>
  
```

トランクを削除する場合は、削除したいするエントリを反転表示させてEnterキーを押します。ポートトランクを切断する場合は、事前に以下の点をご確認ください。

Configuration Menu経由でポートトランクを切断する場合は、最初にトランク内の全ポートを無効にするか、すべてのネットワークケーブルを取り外す必要があります。この操作を行わないとループが発生する恐れがあります。

ポートトランク内のいずれか一つのリンクを無効にする場合は、まず該当するネットワークケーブルを外し、そのリンクの両端をそれぞれConfiguration Menu上で無効にする必要があります。この結果リンクを通過するトラフィックは自動的にトランク内の他のリンクに配分されるため、多量のトラフィックを失うことはありません。

Bridge Menu

スパニングツリー・アルゴリズムの設定やブリッジ全体のGMRP (GARP Multicast Registration Protocol)およびGVRP(GART VLAN Registration Protocol)設定、またトラフィッククラスのプライオリティしきい値やアドレスのエージングタイムを設定することが可能です。

スパニングツリーアルゴリズム(STA)はネットワークループを検出しこれを無効にするほか、スイッチ・ブリッジおよびルータ間で冗長化を実現できます。本製品はSTAに対応しているため、ネットワーク内の他のSTA対応スイッチ/ブリッジ/ルータと連絡をとりあい、ネットワーク上のどの二つの機器間においても、常にルートが一つだけとなるよう調整します。また通常使用しているリンクが使用不可となっても、代替りのリンクを自動的に提供して通信をそのまま続行することが可能です。

```

Bridge Menu: Bridge Configuration
=====
Spanning Tree      : ENABLED      GMRP                : DISABLED
Bridge Priority     : 32768        GVRP                : DISABLED
Hello Time (in seconds) : 2          Priority Threshold   : 4
Forward Delay (in seconds): 15      Aging Time (in seconds): 300
Max age (in seconds) : 20

<Apply>           <OK>           <Cancel>
The status of the spanning tree. | READ/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Bridge Configuration

```

Bridge Menu: Bridge Configuration
=====
Spanning Tree      : ENABLED      GMRP                : DISABLED
Bridge Priority     : 32768        GVRP                : DISABLED
Hello Time (in seconds) : 2          Priority Threshold   : 4
Forward Delay (in seconds): 15      Aging Time (in seconds): 300
Max age (in seconds) : 20

<Apply>           <OK>           <Cancel>
Confirm current screen setting.
Use <TAB> or arrow keys to move, <Enter> to select.

```

「Spanning Tree」

有効に設定するとSTA対応ネットワークに参加できるようになります。

「Bridge Priority」

ルート機器、ルートポートおよび指定(designated)ポートを選択します。優先度の最も高い機器がSTAルート機器となります。ただし全機器の優先度が同じ場合は、最も低いIMACアドレスを持ったデバイスがルート機器となります。設定範囲は 0 ~ 65535 となっており、低い数字ほど優先度は高くなります。

「Hello Time」

ルート機器が設定メッセージを送信する間隔を秒で指定します。設定可能な最小値は1となっており、最大値は10秒もしくは $\{(\text{Max. Message Age} \div 2) - 1 \}$ のうちいずれか低い方となります。

「Forward Delay」

リスニング ラーニング フォワーディングのステート移行を実行する前にルート機器が待機する最大時間を秒単位で設定します。どの機器もフレーム転送を開始する前にトポロジの変更情報を受信する必要があるため、ここで設定するディレイ時間が必要となります。また各ポートも、矛盾する情報がないかどうかリスニングする時間が必要となります。リスニングの結果矛盾する情報が存在する場合はブロッキング状態に移行しますが、リスニングの時間がないとデータがループする恐れがあります。

ディレイの設定可能な最大値は30秒です。最小値は4秒もしくは $\{(\text{Max. Message Age} \div 2) + 1 \}$ のうちいずれか大きい方となります。

「Max (Message) Age」

各機器が再設定を試みる前に待機する時間を指定します。この時間の間、設定メッセージが届かない場合は再設定を行います。指定ポート(designated port)を除く全ポートは、一定間隔で設定メッセージを受信します。各ポートとも、最後に受信した設定メッセージに含まれるSTA情報がエージアウトすると、そのポートは接続されたLANの指定ポートとなります。そのポートがルートポートであった場合は、ネットワークに接続されたデバイスポートの中から新しくルートポートが選出されます。最小値は 6秒もしくは $\{ 2 \times (\text{Hello Time} + 1) \}$ のうちいずれか大きい値となるほか、最大値は40秒もしくは $\{ 2 \times (\text{Forward Delay} - 1) \}$ のうちいずれか小さい値となります。

「GMRP」

GMRP(GARP Multicast Registration Protocol)を使用すると、ネットワーク機器側でエンドステーションをマルチキャストグループに登録できるようになります。

本製品全体でGMRPを有効にすると、各ポートごとにGMRPを有効または無効にできるようになります。本製品はIGMPスヌーピングもサポートしているため、マルチキャスト・フィルタリングが行えるようになっています。

「GVRP」

GVRP(GARP VLAN Registration Protocol) は、各スイッチがネットワーク上の必要なVLANメンバーを登録できるよう、互いにVLAN情報を交換する手段を提供します。VLANの自動登録を許可する場合や、ローカルスイッチを超えて広がるVLANを使用する場合などは当機能を有効(Enabled)に設定してください。

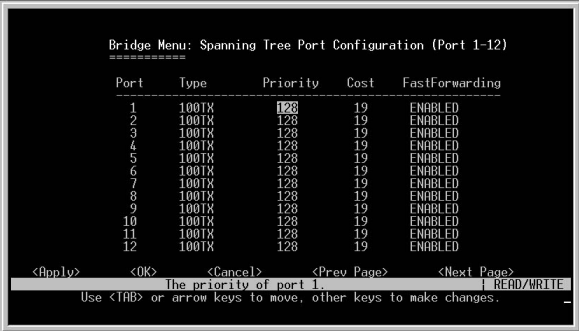
「 Priority Threshold 」

本製品は、2つのプライオリティ・キューを使ったQoSをサポートしており、各ポートではWeighted Fair Queuing (WFQ)を採用しています。IEEE802.1pでは最大8個まで別々のトラフィック・クラスを定義することが可能です。このため、プライオリティがこのしきい値と同じかこれより高いパケットは、高いプライオリティ用のキューに移動します。

「 (Address) Aging Time 」

動的に学習したフォワーディング情報をエージアウトするためのタイムアウト値を秒単位で設定します。設定可能範囲は 10 ~ 415 秒です。

Spanning Tree Port Configuration



Bridge Menu: Spanning Tree Port Configuration (Port 1-12)
=====

| Port | Type | Priority | Cost | FastForwarding |
|------|-------|----------|------|----------------|
| 1 | 100TX | 128 | 19 | ENABLED |
| 2 | 100TX | 128 | 19 | ENABLED |
| 3 | 100TX | 128 | 19 | ENABLED |
| 4 | 100TX | 128 | 19 | ENABLED |
| 5 | 100TX | 128 | 19 | ENABLED |
| 6 | 100TX | 128 | 19 | ENABLED |
| 7 | 100TX | 128 | 19 | ENABLED |
| 8 | 100TX | 128 | 19 | ENABLED |
| 9 | 100TX | 128 | 19 | ENABLED |
| 10 | 100TX | 128 | 19 | ENABLED |
| 11 | 100TX | 128 | 19 | ENABLED |
| 12 | 100TX | 128 | 19 | ENABLED |

<Apply> <OK> <Cancel> <Prev Page> <Next Page>
The priority of port 1. | READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

「Priority」

STAアルゴリズム内での、ポートの使用優先度(プライオリティ)を設定します。スイッチ上の全ポートでパスコストが同じ場合は、プライオリティの最も高い(数値の最も小さい)ポートがスパンニングツリー内でのアクティブリンクとして設定されます。プライオリティが最大のポートが複数存在する場合は、ポートの識別値が最も低いものが有効となります。なお識別値は0~255の範囲で設定可能です。

「(Path) Cost」

スパンニングツリーアルゴリズムは、このパスコストをもとに機器間における最適なパスを決定します。このため、より高速なメディアには低い値を、また低速メディアには高い値を設定する必要があります。(パスコストはポート・プライオリティより先に優先されます。)以下に、デフォルトおよび推奨設定を示します。

Ethernet : 100 (50 ~ 600)

Fast Ethernet : 19 (10 ~ 60)

Gigabit Ethernet : 4 (3 ~ 10)

最大レンジは 0 ~ 65535 となっています。

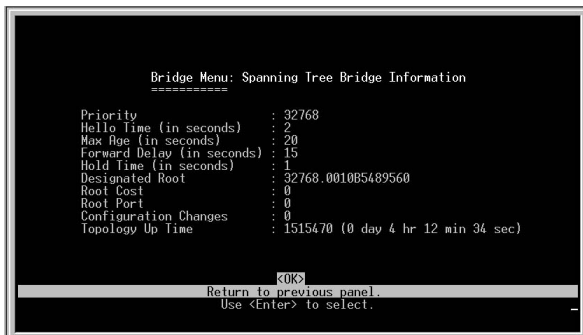
「Fast Forwarding *」

指定ポート上で、ファスト・スパニングツリーモードを有効/無効に設定します。このモードでは、ポートはBlocked、ListeningおよびLearningの各ステートを飛ばして直接Forwardingステートに移行します。

* 末端ノードではフォワーディングループは発生しないため、これらのノードでは、通常の検出(convergence)時間で許されているより高速にスパニングツリーのステート移行を行うことが可能です。ファストフォワーディングは末端ノードおよびサーバ上でより高速に最適経路の検出が行えるほか、他のSTAに関連したタイムアウト問題も克服することが可能です。(重要 : ファスト・スパニングツリーモードは、末端デバイスと接続しているポートのみとなっておりますのでご注意ください。)

Spanning Tree Bridge Information

STA Bridge Informationスクリーンには、ブリッジ(本製品)全体のSTA情報の概要が表示されます。



「Priority」

本製品は、このプライオリティ値をもとにルート機器、ルートポートおよび指定ポート (designated port) を選出します。プライオリティの最も高いものがSTAルート機器となります。全機器のプライオリティが同じである場合は、最も低いIMACアドレスを持つ機器がルート機器に選ばれます。

「Hello Time」

ルート機器が設定メッセージを送信する間隔を秒単位で設定します。

「Max Age」

各機器が再設定を試みる前に、設定メッセージ受信のため待機する最大時間を秒単位で設定します。

「Forward Delay」

ルート機器がそのステートをリスニング ラーニング フォワーディングと移行する前に待機する時間を秒単位で設定します。

「Hold Time」

連続してConfiguration BPDUを送信する際の、各送信間の最小間隔を設定します。

「Designated Root」

スパニングツリー内で、本製品がルート機器であると認めた機器のプライオリティおよびMACアドレスを示します。

「Root Cost」

本製品上のルートポートからルート機器までのパスコストです。

「Root Port」

本製品上のポートのうち、ルートに最も近いもののポート番号です。本製品は、このポートを通してルート機器との通信を行います。ルートポートが存在しない場合は、本製品自体がスパニングツリーネットワーク内のルート機器として割り当てられています。

「Configuration Changes」

スパニングツリーがこれまで再設定された回数です。

「Topology Up Time」

スパニングツリーが最後に再設定されてから経過した時間です。

Spanning Tree Port Information

| Bridge Menu: Spanning Tree Port Information (Port 1-12) | | | | | |
|---|-------|----------|-----------------|--------------------|-----------------|
| Port | Type | Status | Designated Cost | Designated Bridge | Designated Port |
| 1 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.1 |
| 2 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.2 |
| 3 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.3 |
| 4 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.4 |
| 5 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.5 |
| 6 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.6 |
| 7 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.7 |
| 8 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.8 |
| 9 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.9 |
| 10 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.10 |
| 11 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.11 |
| 12 | 100TX | DISABLED | 0 | 32768.0010B5489560 | 128.12 |

<OK> <Prev Page> <Next Page>
Return to previous panel.
Use <TAB> or arrow keys to move. <Enter> to select.

「Status」

スパンニングツリー内における、ポートの現在の状態を表示します。

「Disabled」

ポート上で何もリンクが確立していないか、ポートがユーザーにより無効に設定されています。もしくは自己診断で不良が認められた可能性があります。

「Blocking」

ポートはSTA設定メッセージを受信しますが、パケットは転送しません。

「Listening」

トポロジ上の変更のため、ポートはブロッキング状態を抜けて設定メッセージの送信を開始します。しかしパケットはまだ転送しません。

「 Learning 」

ポートは矛盾する情報を受信しておらず、Forward Delayで設定されている時間間隔で設定メッセージを既に送信しました。ポートアドレスはクリアされ、ポートはまたアドレス学習を開始します。

「 Forwarding 」

ポートはパケットを転送し、アドレス学習を続行します。

ポートステータスは以下のルールにより決定されます

他にSTA準拠のブリッジ機器が同一セグメント上に存在しない場合、そのポートは常に Forwarding状態となります。

スイッチ上の二つのポートが同一セグメントに接続されており、また他にSTA機器がそのセグメントに接続されていない場合、IDのより小さいポートがパケット転送を行い、他方のポートはブロックされます。

本製品起動時、ポートはすべてブロックされます。この後、ポートのうちいくつかはリスニング、ラーニングそしてフォワーディングへとそれぞれ移行します。

「 Designated Cost 」

現在のスパンニングツリー設定内で、パケットがそのポートからルートに移動する際のコストです。メディアの速度が遅いほどコストは高くなります。

「 Designated Bridge(ID)」

このポートがスパンニングツリーのルートに到達するため、途中通過しなければならない機器のプライオリティおよびMACアドレスを表示します。

「Designated Port(ID)」

本製品がスパンニングツリーのルートと通信する際、途中通過しなければならない指定(designated)ブリッジ機器のプライオリティおよびポート番号を表示します。

VLAN Menu

VLAN設定メニューでは、本製品上のどのポートもLANグループに割り当てることができます。本製品では最大256のLANグループが設定可能となっています。従来のルータを使ったネットワークでは、ブロードキャスト・トラフィックは別々のドメインに分けられていました。スイッチは元々ブロードキャストドメインを想定して製造されていないため、IPXやNetBEUIトラフィックを扱う大規模ネットワークではブロードキャスト・ストームが発生する恐れがあります。IEEE802.1Qに準拠した本製品のVLANを使用することにより、複数のネットワーク・ノードを別々のブロードキャストドメインに任意で割り当て、ブロードキャスト・トラフィックを最初のグループ内のみ制限することが可能です。またVLANは、より安全かつ整然としたネットワーク環境を提供します。



VLAN Port Configuration

GARP、デフォルトVLAN識別子、デフォルトポート・プライオリティ、接続リンクのVLANタグging、GVRPおよびGMRPステータス、ポートが所属していないVLANグループに対して送られてきたフレームのフィルタリングを設定します。

GARP

GVRPとGMRPは、ブリッジLAN内のクライアント用サービスに対し、クライアント属性を登録/抹消する際にGARP(Group Address Registration Protocol)を使用します。

各GARPタイマのデフォルト値は、データ速度やメディア接続方法に依存しません。GMRPまたはGVRPの登録/抹消において何か不具合が発生していない限り、これらの設定値は変更しないようにしてください。

各ポートのVLAN属性の変更、VLANグループのポート・メンバーシップを設定を設定します。

```
VLAN Menu: VLAN Port Configuration
=====

GARP Configuration

Join Time      20 Centiseconds
Leave Time      60 Centiseconds
Leave All Time 1000 Centiseconds

VLAN and Priority

Port VID              1
Port Default Priority 0
VLAN Tagging          Rx All, Tx Untag
GVRP                  ENABLED
GMRP                  ENABLED
Ingress Filtering     DISABLED

Port 1 <Apply> <OK> <Cancel> <Prev Port> <Next Port>
The join time for the port. | READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.
```

「Join Time」

グループ内でリクエストまたはクエリーを送る送信間隔を1/100秒単位で設定します。

「Leave Time」

グループから離れる前にポートが待機する時間を1/100秒単位で設定します。Leave Timeは、少なくともJoin Timeの二倍以上に設定する必要があります。このように設定することにより、LeaveまたはLeave Allメッセージが発信されたあと、参加希望者 (applicants) は、ポートが実際にグループを離れる前に再参加できるようになります。

「Leave All」

Leave Allクエリーメッセージをグループ参加者に送信してから、ポートがグループを離れるまでの間隔を1/100秒単位で設定します。グループに再参加するノードから発生するトラフィック量を最小限に止めるためにも、Leave AllはLeave Timeより相当に大きく設定する必要があります。

「IGMP Snooping Configuration」

IGMPマルチキャスト・フィルタリングを設定します。

VLAN and Priority

VLAN、ポートプライオリティ、GVRPおよびGMRPのデフォルト値を設定します。

「Port VID」

このポートで受信したタグなしフレームに割り当てられるVLAN IDです。

「Port Default Priority *1」

イングレス(着信するパケットの)プライオリティ値を設定します。この値より低いものは低プライオリティ用キューに、またこれと同じか、より高いプライオリティのものは高プライオリティ用キューに渡します。

「VLAN Tagging *2」

このポートから送信するフレームにVLANタグを追加するかどうかを指定します。

*1 本製品は二つのプライオリティ・キューを使ったQoSに対応しており、各ポートともWeighted Fair Queuing をサポートしています。着信したフレームのうちVLANタグの無いものは、その着信ポートのデフォルト・イングレス・ユーザープライオリティ情報が追加(タギング)され、出力ポートで適切なプライオリティ・キューに渡されます。どのイングレスポートも、デフォルトのプライオリティ設定は0となっています。このため、着信フレームのうちプライオリティ・タグのないものはすべて低プライオリティ用キューに渡されます。(なお、出力ポートが関連VLANのタグ無しメンバーである場合は、これらのフレームは送信される前にすべてのVLANタグを外されます。)

*2 1~2台のスイッチのみを使った小規模のポートベースVLANを作成する場合は、ポートを同一のタグ無しVLANに割り当て、これらスイッチ間のVLAN接続には別の接続を使用することが可能です。

しかし本製品を超えて広がっているVLANグループに参加する場合は、そのグループ用のVLAN IDを使用することをおすすめします。なおVLAN IDを使用する方法には1)レイヤ2モードのVLANタグgingと、2)マルチレイヤモードの一般PVID使用の二種類があります。本製品をレイヤ2モードでご利用の場合、複数のスイッチをまたがるような大機後VLANグループに割り当てられているポートは、VLANタグgingを必ず使用してください。

マルチレイヤモード使用時の制限

ただしマルチレイヤモードでご利用の場合は、現状ではタグgingを無効にし、リンクの両側においてPVIDを同じに設定し(接続機器がVLAN対応の場合)このVLANを他グループと接続する場合はさらにIPインターフェースを設定する必要があります。また本製品がマルチレイヤモードで動作している場合は、いずれのVLANも重複させることはできません。(これらの制限は、将来提供されるファームウェア・バージョンからは取り除かれる予定です。)

「GVRP」

このポートのGVRP機能を有効/無効に設定します。無効に設定した場合、このポートで受信されたGVRPパケットは破棄され、他ポートからGVRP登録が(このポートに)広がることもありません。

注意 この設定を有効とするには、まず本製品全体でGVRPを有効にする必要があります。

「GMRP」

このポート上でGMRPを有効/無効に設定します。有効に設定されていると、当ポートはエンドステーションのマルチキャストグループへの登録を許可します。

注意 この設定を有効とするには、まず本製品上でGMRPを有効にする必要があります。

「Ingress Filtering *3」

有効に設定すると、受信したVLAN宛のフレームのうち、このイングレスポート(Ingress Port)がメンバーセットに含まれていないフレームはイングレスポートで破棄されます。

*3 この制限は、GVRPやSTPといった、VLANに依存しないBPDUフレームに対しては無効となります。ただしGMRPなどのVLANに依存するBPDUフレームは影響を受けます。

「IP Menu *4」

各VLANグループへのIPインターフェイスの設定、VLANのポートグループ設定、システム全体のユニキャストおよびマルチキャスト・ルーティングプロトコル設定、IGMPスヌーピング設定、OSPFエリア設定を行えます。

*4 本製品がマルチレイヤモードで動作中の場合のみ設定可能です。

VLAN Table Configuration

新規のVLANグループ作成や既存のVLANグループの設定を変更を行います。

```
VLAN Menu: VLAN Table Configuration
=====
VLAN      Port      1      2      slot1
1         123456789012345678901234 1
          SSSSSSSSSSSSSSSSSSSSSSS S

-: Normal
S: Static
X: Forbidden

Page : 1 <Apply> Total: 1 Pages
<OK> <Prev Page> <Next Page> <Add>
Enter page number than press 'Apply' to see VLAN group. | READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.
```

「VLAN」

現在表示されているVLANのIDです。1～2048の範囲で設定可能です。

「Port」

ポートエントリの状態を示します。

「-」

GVRPを使用してポートメンバーシップを決定します。

「S」

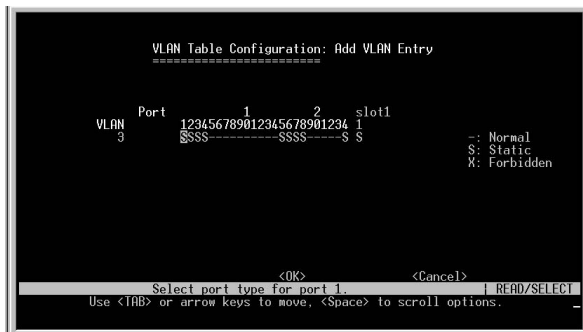
ポートを静的(static)エントリとして追加します。

「X」

ポートのGVRPを無効にします(ポートは含みません)。

削除したポートがタグ無しポートとして他のどのグループにも割り当てられていない場合、そのポートは自動的にVLANグループ1にタグ無しポートとして割り当てられます。

新規でVLANグループを追加するにはAddにカーソルを移動してエンターキーを押してください。



「VLAN」

VLANIDを入力してください。

「Port 1 24 Slot1」

VLANグループに参加させたい場合はSを設定してください。

注意 カーソルを<Next Page>または<Prev Page>に合わせてエンターキーを押すと、テーブル内容をスクロールできます。特定ページを表示する場合はPage Fieldに希望のページ番号を入力し、カーソルを<Apply>に移動してエンターキーを押します。いずれかのVLANグループを変更する場合は、テーブル内の該当するエントリにカーソルを移動してEnterキーを押してください。VLANグループを追加する場合はカーソルを<Add>に移動してEnterキーを押してください。

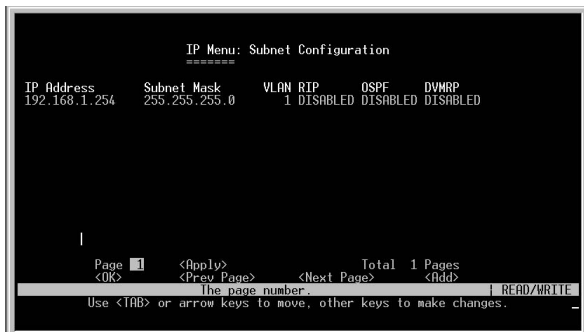
IP Menu

本製品がマルチレイヤモードに設定されている場合に本製品上の各VLANのIPサブネットや、IGMPおよびユニキャスト/マルチキャストルーティングプロトコルの設定を行います。



Subnet Configuration

本製品に設定したVLANグループ同士を通信させる場合はそれぞれのVLANグループにIPインターフェースを設定する必要があります。本製品を帯域内(in-band)で使用する場合でも、管理用に最低一つのVLAN用のIPサブネットアドレスを設定する必要があります。



「IP Address」

指定VLANインターフェースと関連づけられるIPアドレスです。

「Subnet Mask」

特定サブネットにルーティングする際に使用されるホストアドレスの、アドレスビットを示すテンプレートです。「1」に対応する各ビットはネットワーク/サブネット番号の一部となっています。また「0」に対応する各ビットはホスト番号の一部となっています。

「VLAN」

IPインターフェースが追加されているVLANグループを表示します。

「RIP」

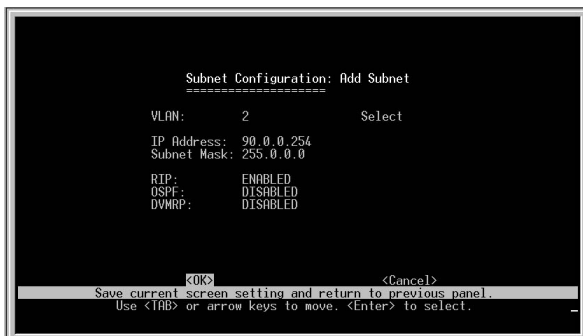
設定したインターフェイスに対しユニキャストルーティング用のルーティング情報プロトコルであるRIPが有効または無効に設定されているかを表示します。

IPインターフェースを新しく追加する場合は、Subnet Configurationメニューの<Add>にカーソルを移動してエンターキーを押してください。Add Subnetスクリーンが表示されます。インターフェイスを追加したいVLANグループを選択した後、IPアドレスの設定、必要なルーティングプロトコルを有効にしてください。本メニューからVLANグループの作成および編集を行うことも可能です。

注意 ユニキャスト/マルチキャスト・ルーティングプロトコルの詳細を設定する場合は、新規インターフェイスを追加後、一旦Subnet Configurationメニューに戻り登録したIPアドレスを選択し、Modify Subnetスクリーン上で「Advanced」設定を選択してください。

Add Subnet

VLANグループの新規作成または既存グループのメンバー編集を行う場合は、Add SubnetスクリーンでSelectを選択します。



「VLAN」

IPインターフェイスを追加したいVLANグループを入力してください。

「Select」

VLANの作成/編集を行う場合はこのオプションを選択します。

「IP Address」

IPアドレスを入力してください。

「Subnet Mask」

特定サブネットにルーティングする際に使用されるホストアドレスの、アドレスビットを示すテンプレートです。「1」に対応する各ビットはネットワーク/サブネット番号の一部となっています。また「0」に対応する各ビットはホスト番号の一部となっています。

「RIP」

ユニキャストルーティング用のルーティング情報プロトコルの有効/無効を設定します。

ポートグループの設定

VLANグループの新規作成または既存グループのメンバー編集を行う場合は、Add SubnetスクリーンでSelectを選択します。



「VLAN」

本製品上に既に設定されているVLANです。

「Port」

ポートエントリの種類を表示します。

「S」

ポートを静的エントリとして追加します。

「P」

ポートを静的エントリとして追加し、さらに当ポートのPVIDをこのVLAN IDに設定します。

注意 <Next Page>または<Prev Page>ボタンを使うと、テーブル内容をスクロールできます。特定ページを表示する場合はPage Field に希望のページ番号を入力して<Apply> ボタンを押します。VLANを編集する場合は、テーブル内の該当するエントリを反転表示させてEnterキーを押してください。新規にVLANを追加する場合は <Add> ボタンを押してください。

IPインターフェースの変更

IPインターフェースを変更する場合は、Subnet Configurationメニュー内で該当するIPアドレスにカーソルを移動してEnterキーを押してください。Modify Subnetスクリーンでは、Advancedオプションを選択してユニキャスト/マルチキャストルーティングプロトコルの設定が可能です。ここではAdvancedオプションを説明します。

RIP(Routing Information Protocol)

RIPのAdvancedオプションでは、複数のルータがお互いにルーティングテーブルの情報を交換する方法を設定します。本製品上でRIPを有効にすると、本製品はネットワーク内の全機器に対し30秒おきにRIPメッセージをブロードキャストし、他のルータからRIPメッセージを受信した際は自身のルーティングテーブルを自動的に更新します。RIPメッセージにはIPアドレスおよび、本製品から各通信先ネットワークまでのメトリック(ホップ数)が含まれます。

1) 認証タイプの指定、2) 指定ポート上でルーティングメッセージ送受信に使用するプロトコル、3) 最適パス計算時に使用するデフォルト・メトリックおよび、4) Poison Reverseの有効/無効がそれぞれ設定可能です。

「 Authentication Type 」

認証(authentication)は、ルーティング情報が正当なサイトから送信されたものであることを保証します。

「 Authentication Key 」

認証を有効にするために必要なパスワードです。認証ストリングは半角英数字で最長16文字まで設定可能です。ストリングは大文字・小文字を区別します。

「 Send Type 」

このポートから送信されるトラフィックで使用されているプロトコルです。

RIP1 Broadcast : ルート情報は、RIPv1を使ってネットワーク上の他のルータにブロードキャストされます。

RIP2 Broadcast : ルート情報は、RIPv2を使ってネットワーク上の他のルータにブロードキャストされます。

RIP2 Multicast : ルート情報は、RIPv2を使ってネットワーク上の他のルータにマルチキャストされます。

「 Do Not Send 」

本製品は、ネットワークに接続された他のルータから送られてくるルート情報を受動的に監視します。

「 Receive Type 」

このポートで受信可能なルーティングプロトコルメッセージの種類です。RIP1 , RIP2 , RIP1/RIP2またはDisabled (受信しない) に設定可能です。

「Default Metric」

メトリックとは、本製品と通信先ネットワークとの間のホップ数を指します。「デフォルトメトリック」は、当インターフェースから発信されたRIP更新(情報)に含まれるデフォルトルートを指します。0と設定すると、デフォルトルートは何も発信されず、他のルータから発信されたデフォルトルートが伝播するようになります。値は0～15の範囲で設定可能です。

「Poison Reverse *」

ルートを最初に入手したインターフェースポートまで、ルートを逆に伝播します。ただし距離のベクター・メトリックは無限大に設定されます。

* ルーティング情報が送信元までループすることを阻止する方法の一つです。なお、同じ目的のため本製品では「Split Horizon」も有効となっていますのでご注意ください。

Protocol Configuration

本製品全体でユニキャスト/マルチキャスト・ルーティングプロトコルを有効/無効に設定します。



「RIP」

ユニキャストルーティング用のルーティング情報プロトコルを有効/無効に設定します。

「OSPF」

Open Shortest Path First（最短パスを最初に開く）ユニキャスト・ルーティングプロトコルを有効/無効に設定します。

「DVMRP」

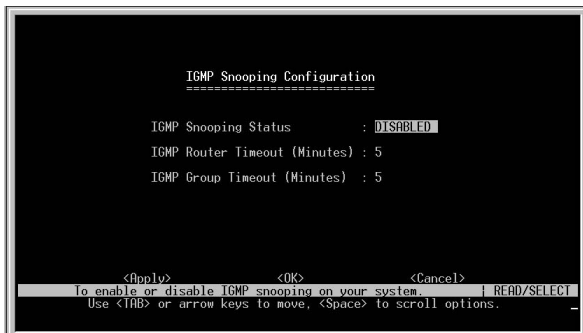
Distance-Vector Multicast Routing Protocol(距離-ベクターマルチキャストルーティングプロトコル)を有効/無効に設定します。

注意 システム全体でプロトコルを有効にした後は、*Subnet Configuration* メニューを使って、いずれか特定のサブネットでこれらのプロトコルを個別に有効/無効に設定できるようになります。

IGMP Snooping Configuration

ビデオカンファレンスやストリーミング・オーディオといった、リアルタイムアプリケーションに対応するため本製品ではマルチキャストを採用しています。マルチキャストサーバは、各クライアントと個別に接続を行う必要はありません。サーバ自体はネットワークに対しそのサービスをブロードキャストするだけにとどまり、マルチキャストの受信を希望するホストは各々のローカルマルチキャスト・スイッチ/ルータに登録します。この方法でマルチキャスト・サーバの要求するネットワーク・オーバーヘッドを縮小することは確かに可能ですが、トラフィック(サービス)がそれを必要としているホストにのみ供給されるようにするためにも、ブロードキャスト・トラフィックが通過するすべてのスイッチ/ルータにおいて、ブロードキャストパケットは慎重にカットする必要があります。

本製品ではIGMP (Internet Group Management Protocol)を使って、本製品と接続されているホストのうち、特定のマルチキャスト・サービスを希望するものを監視することが可能です。IGMPはそのサービスで使用されているIPマルチキャストグループを参照し、同様のリクエストを受信したすべてのポートをこのグループに追加します。



「IGMP Status」

有効の場合、本製品はネットワークトラフィックを監視してどのホストがマルチキャストトラフィックの受信を希望しているかを確認します。これを「IGMPスヌーピング」と呼びます。

「IGMP Router Timeout」

スイッチ上のポートで、ここで指定された時間の間マルチキャストプロトコルパケットの受信を停止したものはIGMPフォーウェイングリストから除かれます。タイムアウトは3～5分の間で設定可能です。

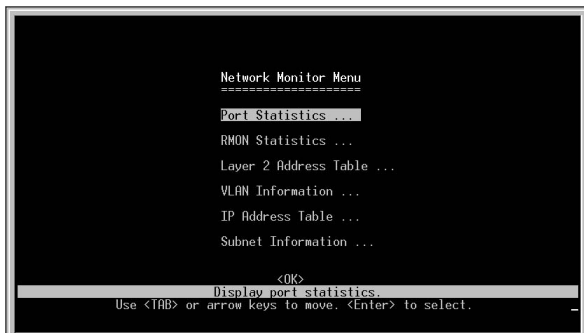
「IGMP Group Timeout」

指定ポート上で、いずれかのIPマルチキャストアドレスに対するIGMP Reportメッセージが検出されてから、本製品がそのエントリをリストから削除するまでの時間を設定します。値は3～5分の間で設定可能です。

注意 IGMPプロトコルセット全体は、DVMRPとともに自動的に有効/無効に設定されます。

7.Network Monitor Menu

Network Monitor Menuでは、ポート統計、RMON統計、静的ユニキャスト/マルチキャストアドレステーブルおよびMACアドレス・フィルタテーブルのそれぞれの情報を参照することが可能です。



Port Statistics

Port Statisticsスクリーンでは、各ポートのInterface GroupおよびEthernetMIBに関する主な統計情報が表示されます。これらの情報は、ポート不良や負荷の異常増大など、本製品上で発生する可能性のある問題を識別する際に使用されます。表示される値は、最後にシステムを再起動した時点からの累計です。



Port Numberにカーソルを移動して参照したいポート番号を入力した後、エンターキーを押し<Apply>を選択してください。

「Interface In Octets」

このインターフェース上で受信されたオクテット数の合計です。値にはフレーミング・キャラクタも含まれます。

「In Unicast Pkts」

高位層プロトコルに渡されたサブネットワーク-ユニキャストパケットの数です。

「In Non-Unicast Pkts」

高位層プロトコルに渡された、非ユニキャスト(サブネットワーク-ブロードキャストまたはサブネットワーク-マルチキャスト)パケット数を指します。

「 In Discards 」

高位層プロトコルへ転送するのを防ぐため、なにもエラーが検出されなかったにも関わらず廃棄される受信(インバウンド)パケットの数を指します。これらのパケットを廃棄する理由には、バッファ領域を空ける目的も含まれます。

「 In Errors 」

エラーが含まれるため高位層プロトコルに転送できない受信(インバウンド)パケット数です。

「 Alignment Errors 」

アライメントエラー(同期に失敗したデータパケット)数です。

「 Out Octets 」

このインターフェースから送信されたオクテットの総計です(フレーミングキャラクタも含まれます)。

「 Out Unicast Pkts 」

高位層プロトコルの要求によりサブネット-ユニキャストアドレスに送信されたパケットの総計です(破棄または送信されなかったパケットも含む)。

「 Out Non-Unicast Pkts 」

高位層プロトコルの要求により、非ユニキャスト(サブネットワーク-ブロードキャストまたはサブネットワーク-マルチキャスト)アドレスに送信されたパケットの総計です(破棄または送信されなかったパケットも含む)。

「Out Discards」

高位層プロトコルへ転送するのを防ぐため、なにもエラーが検出されなかったにも関わらず廃棄される送信(アウトバウンド)パケットの数を指します。これらのパケットを廃棄する理由には、バッファ領域を空ける目的も含まれます。

「Out Errors」

エラーのため送信できなかったアウトバウンドパケット数です。

「CRC Errors」

当機器で検出された、イーサネットCRC(Cyclic Redundancy Check)エラー数です。

「Ethernet Single Collisions」

正常に送信されたフレームのうち、一回のコリジョンにより送信が禁止されたものの数を示します。

「Deferred Transmissions」

送信メディアがビジー状態のため、特定インターフェース上での一回目の送信試行が失敗したフレームの数です。

「Excessive Collisions」

過度のコリジョンのため送信に失敗したフレームの数です。

「Drop Events」

リソース不足のためパケットがドロップ(廃棄)されたイベントの総計です。

「Octets」

当ポートを通過するオクテット数です。

「Multiple Collisions」

正常に送信されたパケットのうち、複数回のコリジョンにより送信が禁止されたものの数を示します。

「Late Collisions」

パケット送信中、64オクテット以降に検出されたコリジョン数です。

「Carrier Sense Errors」

フレーム送信を試みた際、キャリアセンス状態が失われたか、もしくはこの状態にまったくならなかった回数を示します。

「Fragments」

64オクテットより短い受信フレーム(ただしフレーミングビットは除き、FCSオクテットは含む)のうち、FCSもしくはアライメントエラーを起こしたものの総計です。

「Jabbers」

1518オクテットより長い受信フレーム(ただしフレーミングビットを除き、FCSオクテットを含む)のうち、FCSまたはアライメントエラーを持ったものの総計です。

■ **注意** 各統計情報の更新はデフォルトで10秒毎におこないます。

RMON Statistics

RMON Statisticsスクリーンでは、RMONグループ1の各ポートの主な統計情報を参照することができます。(RMONグループ2、3および9を参照するにはSNMP管理ソフトウェアを使用してください。)以下のスクリーンでは、各ポートを通過するトラフィックの総合的な統計情報を示しています。RMON Statisticsスクリーンでは、各ポートを通過する異なる種類・サイズのフレームの合計カウントを含む、多くの統計情報にアクセスできるようになっています。なお、表示される値はシステムが最後に再起動した時点からの累計です。

| Network Monitor Menu: RMON Statistics | | | |
|---------------------------------------|-----------|-----------------------|---------|
| ===== | | | |
| Drop Events | : 0 | Jabbers | : 0 |
| Received Bytes | : 5981508 | Collisions | : 0 |
| Received Frames | : 65666 | 64 Byte Frames | : 26307 |
| Broadcast Frames | : 30979 | 65-127 Byte Frames | : 16025 |
| Multicast Frames | : 35049 | 128-255 Byte Frames | : 4876 |
| CRC/Alignments Errors | : 0 | 256-511 Byte Frames | : 1073 |
| Undersize Frames | : 0 | 512-1023 Byte Frames | : 0 |
| Oversize Frames | : 0 | 1024-1518 Byte Frames | : 0 |
| Fragments | : 0 | 1519-1536 Byte Frames | : 0 |

| | | | |
|-----------------|-----------|-------------|-------------|
| Port Number: 25 | <Apply> | <Reset> | <Reset All> |
| <OK> | <Refresh> | <Next Port> | <Prev Port> |

Apply port number for Port Statistics.
Use <TAB> or arrow keys to move. <Enter> to select.

Port Numberにカーソルを移動して参照したいポートを入力しエンターキーを押し<Apply>を選択してください。

「Drop Events」

リソース不足のためパケットが廃棄されたイベントの総計です。

「Received Bytes」

ネットワーク上で受信したデータの合計バイト数です。この情報は、Ethernetの利用状況を確認する上で有効なデータとなっています。

「Received Frames」

フレーム(不良フレーム、ブロードキャスト/マルチキャストフレーム)の総受信数を示します。

「Broadcast Frames」

受信された有効フレームのうち、ブロードキャストアドレスに転送されたものの総計です。これにはマルチキャストパケットは含まれませんのでご注意ください。

「Multicast Frames」

受信された有効フレームのうち、このマルチキャストアドレスに転送されたものの総計です。

「CRC/Alignments Errors」

CRC/アライメントエラー(FCSまたはアライメントエラー)の総計です。

「Undersize Frames」

受信フレームのうち、長さが64オクテットより短いことを除けば他に問題が検出されなかったフレームの総計です。なおFCSオクテットはこれに含まれますが、フレーミングビットは除きます。

「Oversize Frames」

受信フレームのうち、長さが1518オクテットより長いことを除けば他に問題が検出されなかったフレームの総計です。なおFCSオクテットはこれに含まれますが、フレーミングビットは除きます。

「Fragments」

受信フレームのうち、64オクテットより短くかつFCSかアライメントエラーが含まれるものの総計です。なおFCSオクテットはこれに含まれますが、フレーミングビットは除きます。

「Jabbers」

受信フレームのうち、1518オクテットより長くかつFCSかアライメントエラーが含まれるものの総計です。なおFCSオクテットはこれに含まれますが、フレーミングビットは除きます。

「Collisions」

このEthernetセグメント上で発生するコリジョンの予想発生数です。

「64 Byte Frames」

送受信したフレームのうち、長さが64オクテットのものの総計です。これには不良パケットやFCSオクテットが含まれますが、フレーミングビットは除きます。

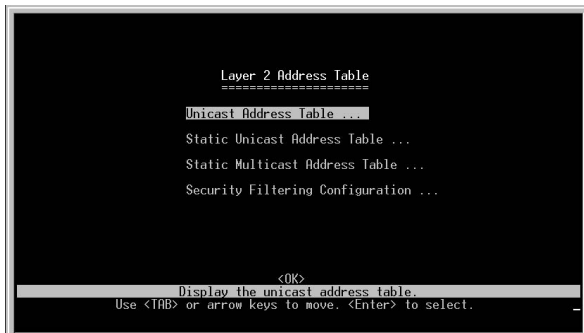
「65-127 Byte Frames, 128-255 Byte Frames, 256-511 Byte Frames, 512-1023 Byte Frames, 1024-1518 Byte Frames, 1519-1536 Byte Frames」

送受信したフレームのうち、長さがこの範囲内のものの総計です。これには不良パケットやFCSオクテットが含まれますが、フレーミングビットは除きます。

注意 デフォルト設定では、各統計は10秒ごとに更新(リフレッシュ)するようになっています。

Layer 2 Address Table

このメニューでは、ユニキャストアドレステーブル、静的ユニキャスト/マルチキャストアドレステーブルおよびセキュリティフィルタテーブルを参照することができます。



Unicast Address Table

ユニキャストアドレステーブルには、各ポートと関連付けられたMACアドレス(これらのアドレスと関連付けられた送信元(ソース)ポート)が含まれます。Address Table内に表示される各情報につき解説します。

| Layer 2 Address Table: Unicast Address Table | | | | | |
|--|------|---------|-------------------|------|---------|
| ===== | | | | | |
| Address | Port | Status | Address | Port | Status |
| 00-00-E8-7B-F7-89 | 25 | Learned | 00-00-E8-8F-CE-24 | 25 | Learned |
| 00-05-02-09-29-51 | 25 | Learned | 00-10-5A-80-7E-88 | 25 | Learned |
| 00-10-B5-00-00-53 | 25 | Learned | 00-10-C6-05-D5-63 | 25 | Learned |
| 00-10-C6-05-E6-EA | 25 | Learned | 00-10-DC-05-56-7F | 25 | Learned |
| 00-10-DC-13-05-53 | 25 | Learned | 00-10-DC-14-08-77 | 25 | Learned |
| 00-10-DC-17-09-73 | 25 | Learned | 00-10-DC-17-11-34 | 25 | Learned |
| 00-10-DC-17-54-6D | 25 | Learned | 00-10-DC-18-08-69 | 25 | Learned |
| 00-10-DC-1A-03-41 | 25 | Learned | 00-10-DC-1A-03-61 | 25 | Learned |
| 00-10-DC-1A-04-12 | 25 | Learned | 00-10-DC-1A-06-23 | 25 | Learned |
| 00-10-DC-1B-04-95 | 25 | Learned | 00-10-DC-1B-06-19 | 25 | Learned |
| 00-10-DC-1B-08-94 | 25 | Learned | 00-10-DC-1B-08-95 | 25 | Learned |
| 00-10-DC-1C-01-88 | 25 | Learned | 00-10-DC-1C-04-03 | 25 | Learned |

Page 1 <Apply> Total 3 Pages
 <OK> <Next Page> <Prev Page>
 Return to previous panel.
 Use <TAB> or arrow keys to move. <Enter> to select.

「Address」

本製品上で参照できるノードのMACアドレスです。

「Port」

自身のアドレステーブルにこのMACアドレスを持つポートです。

「Status」

アドレスステータスを表示します。

「Learned」

動的(ダイナミック)に学習。

「Static」

SNMPネットワーク管理ソフトウェアにより永久に固定。

注意 <Next Page>または<Prev Page>にカーソルを移動してエンターキーを押すとアドレステーブルの内容をスクロールできます。特定ページを表示する場合はPage Fieldに希望のページ番号を入力して<Apply> ボタンを押してください。

Static Unicast Address Table

Static(静的)ユニキャストアドレステーブルを使って、ホスト機器のMACアドレスを本製品上の特定ポートに割り当てることができます。静的ユニキャストアドレスはエージアウトしないほか、他のポート上で学習することはできません。このテーブル内にある送信元アドレスを持ったパケットが他のポートに届いても、このパケットはそこで破棄されます。以下に、Static Unicast Address Table 内の各項目につき解説します。

| Layer 2 Address Table: Static Address Table | | | |
|---|------|---------|------|
| Address | Port | Address | Port |
| 30-30-30-30-30-30 | 1 | | |

Page 1 <Apply> Total 1 Pages
<OK> <Next Page> <Prev Page> <Add>
Return to previous panel.
Use <TAB> or arrow keys to move. <Enter> to select.

「Address」

本製品に接続されているホスト機器のMACアドレスです。

「Port」

ホスト機器の接続されているポートです。

注意 指定ポートにMACアドレスを割り当てる場合は、<Add> ボタンを使用します。アドレスを削除または変更する場合は、対象のアドレスにカーソルを移動してEnterキーを押してください。またアドレステーブルをスクロールする場合は<Next Page> か<Prev Page> にカーソルを移動してEnterキーを押してください。特定ページを表示する場合はPage Fieldにカーソルを移動して参照したいページ番号を入力し<Apply> を選択してEnterキーを押してください。

Static Multicast Address Table

Static Multicast Address Tableを使って、特定のマルチキャストサービス用に使用するVLANグループに対し、接続先MACアドレスおよびこれに対応するポートを割り当てることができます。静的マルチキャストアドレスはエージアウトしないほか、これらのアドレスを持ったトラフィックは、このテーブルで指定されているポートにしか転送できないようになっています。

| Layer 2 Address Table: Multicast Address Table | | | |
|--|--------------------------|------|-------|
| ===== | | | |
| VLAN | Address | Port | slot1 |
| 1 | 123456789012345678901234 | 1 | |

Page 1 <Apply> Total 1 Pages
<OK> <Next Page> <Prev Page> <Add>
Return to previous panel.
Use <TAB> or arrow keys to move. <Enter> to select.

「VLAN」

このマルチキャストサービスに対応するVLANグループを入力してください。

「Address」

マルチキャストサービスの供給先(送信先)MACアドレスを入力してください。

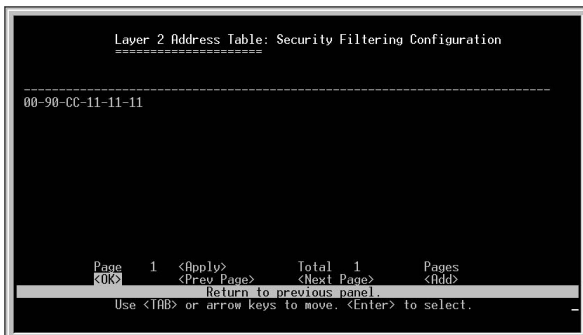
「Port」

マルチキャストトラフィックを転送したいポート番号を入力してください。

注意 一つまたは複数のポートに送信先MACアドレスを割り当てる場合は、カーソルを<Add>に移動してEnterキーを押してください。アドレスを削除または変更する場合は、対象のアドレスにカーソルを移動してEnterキーを押してください。またアドレステーブルをスクロールする場合は<Next Page>か<Prev Page>にカーソルを移動してEnterキーを押してください。特定ページを表示する場合はPage Field に参照したいページ番号を入力してカーソルを<Apply>に移動しEnterキーを押してください。

Security Filtering Configuration

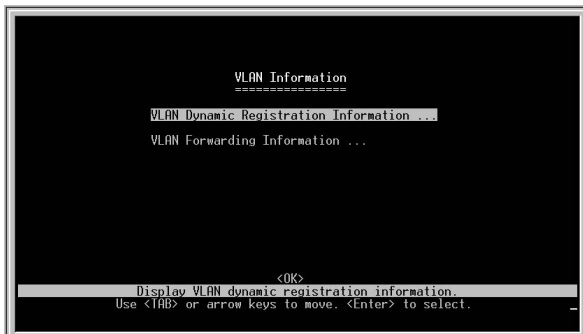
セキュリティ面でリスクのあるノードや故障中のノードは、本製品上でフィルタする(切り離す)ことができます。セキュリティ・フィルタリングを使って、指定MACアドレスのホストから送信されるトラフィックをすべて破棄することができます。同様に、本製品ではSecurity Filtering Configurationテーブル内で登録されている送信元/送信先アドレスを持つトラフィックをフィルタすることが可能です。



注意 セキュリティフィルタにMACアドレスを追加する場合は、<Add> ボタンを使用します。アドレスを削除または変更する場合は、対象アドレスにカーソルを移動してEnterキーを押してください。またアドレステーブルをスクロールする場合は<Next Page> か<Prev Page>にカーソルを移動してEnterキーを押してください。特定ページを表示する場合はPage Field に参照したいページ番号を入力してカーソルを<Apply>に移動しEnterキーを押してください。

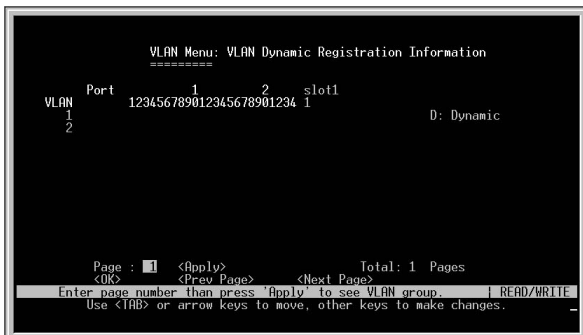
VLAN Information

以下の各メニューは、GVRP経由で自動的に学習されたポートの情報および、動的または静的で設定された、VLANトラフィック転送用ポートの情報を表示します。



VLAN Dynamic Registration Information

GVRPにより自動的に学習されたポートを表示します。



注意 ダイナミック・レジストレーションテーブルアドレステーブルをスクロールする場合は<Next Page>か<Prev Page>にカーソルを移動してEnterキーを押してください。特定ページを表示する場合はPage Fieldに希望のページ番号を入力して<Apply> ボタンを押してください。

VLAN Forwarding Information

VLANトラフィック転送用の、動的または静的に設定されたポートを表示します。

```
VLAN Menu: VLAN Forwarding Information
=====
VLAN  Port          1          2          slot1
1      123456789012345678901234 1
      SSSSSSSSSSSSSSSSSSSSSSSSS S      S: Static
2      SSSS                      SSSSS S      D: Dynamic

Page : 1 <Apply> Total: 1 Pages
      <OK> <Prev Page> <Next Page>
Enter page number than press 'Apply' to see VLAN group. | READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.
```

注意 画面ををスクロールする場合は<Next Page>か<Prev Page>にカーソルを移動してEnterキーを押してください。特定ページを表示する場合はPage Fieldに参照したいページ番号を入力して<Apply>にカーソルを移動しEnterキーを押してください。

IP Address Table

このメニューでは、1)静的ルート、2)動的に学習されたルート、3)未知のネットワークアドレス用のデフォルトルート、4)マルチキャストグループ、および5)セキュリティフィルタの各IPアドレステーブルを表示します。



ARP Table

ARP(Address Resolution Protocol)は、ホストのインターネットアドレスからそのイーサネットアドレスを割り当てる方法を定義します。ARPにより検出されたIP <-> MACアドレスのキャッシュ情報を表示します。

| IP Address Table: ARP Table | | | |
|-----------------------------|-------------------|------|------|
| IP Address | MAC Address | VLAN | Port |
| 169.254.248.56 | 00-80-45-10-d5-1b | 1 | 25 |
| 192.168.1.1 | 00-40-05-51-e4-5f | 1 | 0 |
| 192.168.1.5 | 00-80-87-80-ac-57 | 1 | 25 |
| 192.168.1.6 | 00-80-87-80-6c-18 | 1 | 25 |
| 192.168.1.10 | 00-40-05-42-a0-31 | 1 | 25 |
| 192.168.1.16 | 00-40-05-a0-45-f8 | 1 | 25 |
| 192.168.1.19 | 00-a0-ae-00-77-5d | 1 | 25 |
| 192.168.1.20 | 00-40-05-a0-5d-94 | 1 | 25 |
| 192.168.1.25 | 00-a0-ae-00-1d-ce | 1 | 25 |
| 192.168.1.26 | 00-a0-ae-00-4a-f2 | 1 | 25 |
| 192.168.1.28 | 00-10-c6-05-d5-63 | 1 | 0 |
| 192.168.1.33 | 00-10-dc-15-55-3e | 1 | 25 |

Page 1 <OK> <First Page> <Next Page>

Return to previous panel.

Use <TAB> or arrow keys to move. <Enter> to select.

「IP Address」

ブロードキャストメッセージをもとに、ARPはこのIPアドレス用の物理アドレスを検出します。

「MAC Address」

IPアドレスに対応しているMACアドレスが表示されます。

「VLAN」

ホストに割り当てられているVLANグループが表示されます。

「Port」

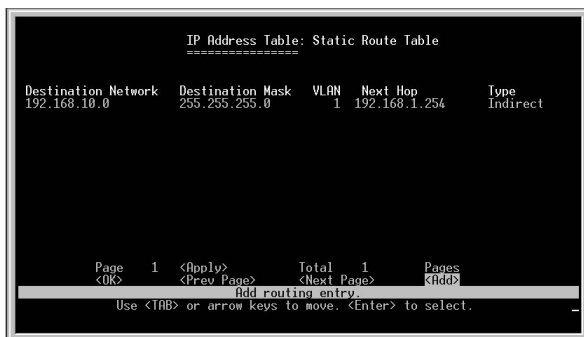
ホスト機器と接続しているポートが表示されます。

注意 <First page> または <Next Page> にカーソルを移動してEnterキーを押すとアドレステーブルをスクロールさせることができます。

Static Route Table

本製品では、ユニキャストまたはマルチキャスト・ルーティングプロトコルを使用し、他のIPネットワーク/サブネットホストへのルートをダイナミックに学習するよう設定できるようになっています。しかし特定の通信先へのルートがこれらのプロトコルで学習できない場合や、通信先にトラフィックを送信する際指定のパスを使用させたい場合は、Static Route Tableを使って静的パスを設定することも可能です。

静的ルートを定義する前に、本製品上で少なくともIPインターフェイスを一つ設定する必要があります。静的ルートは動的(ダイナミック)に学習したルートより優先されるほか、ユーザーがテーブルから削除するか、対応するIPインターフェイスを本製品から削除しない限りテーブル内から消えることはありません。



「Destination Network」

通信先のネットワークグループが表示されます。

「Destination Mask」

サブネットマスクが表示されます。

「Next Hop」

次のホップにあたるルータのIPアドレスが表示されます。

「Type」

Destination networkへのIPルートの種類が表示されます。

本製品は以下のルートをサポートしています。

Direct : 直接接続されているサブネットワーク

Indirect : リモートIPサブネットワークまたはリモートホスト
アドレス

Myself : 特定IPサブネットワーク上のスイッチIPアドレス

Bcast : サブネットワーク・ブロードキャストアドレス

Mcast : IPマルチキャストアドレス

Invalid : フィルタ対象となる不正IPアドレス

注意 <Next Page> か <Prev Page> にカーソルを移動してEnterキーを押すとstaticroute tableをスクロールすることができます。特定ページを表示する場合はPage Fieldに参照したいページ番号を入力して<Apply>にカーソルを移動しEnterキーを押してください。静的ルートを変更する場合は、希望のエントリにカーソルを移動してEnterキーを押してください。静的ルートを追加する場合は<Add>にカーソルを移動してEnterキーをおしてください。

Routing Table

認識されているすべてのイーサネット・ネットワークおよび対応 VLAN までの各ルートを表示します。ルーティングプロトコルで学習されたルートおよび手動設定されたルートは、すべてこの Routing Table に含まれます。

```
IP Address Table: Routing Table
=====
Destination Network  Destination Mask  VLAN  Next Hop      Type      Protocol
0.0.0.0              0.0.0.0          1     192.168.1.1   Indirect  Mgmt
192.168.10.0        255.255.255.0   1     192.168.1.254 Indirect  Mgmt
192.168.1.0         255.255.255.0   1     192.168.1.254 Direct   Local

Page 1 <Apply> Total 0 Pages
<OK> <Prev Page> <Next Page> <Flush RIP>
Return to previous panel.
Use <TAB> or arrow keys to move. <Enter> to select.
```

「Destination Network」

通信先のネットワーク/サブネット/ホストです。

「Destination Mask」

適合するビットを指定するサブネットマスクです。Destination Maskにより設定されたビットがDestination Networkと一致する場合、ルーティングエントリはパケットに使用(適用)されます。

「VLAN」

ゲートウェイまたはDestination AddressはこのVLAN内に存在します。

「Next Hop」

次のホップにあたるルータのIPアドレスです。

「Type」

Destination networkのIPルートの種類です。本製品は以下のルートをサポートしています。

Direct : 直接接続されているサブネットワーク

Indirect : リモートIPサブネットワークまたはリモートホストアドレス

Myself : 特定IPサブネットワーク上のスイッチIPアドレス

Bcast : サブネットワーク・ブロードキャストアドレス

Mcast : IPマルチキャストアドレス

Invalid : フィルタ対象となる不正IPアドレス

「プロトコル」

ルートは以下のいずれかの方法で学習されます。

Local : 手動設定

Mgmt : SNMPで設定

ICMP : ICMPリダイレクト経由で入手

RIP : RIPプロトコルで学習

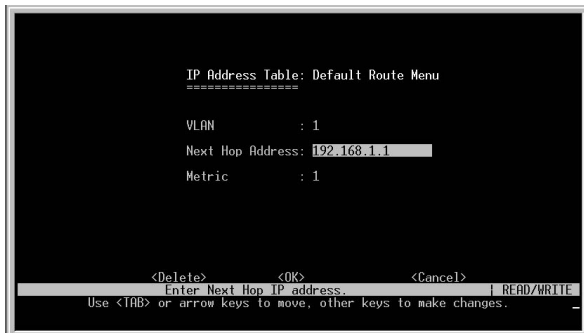
OSPF : OSPFプロトコルで学習

Other : 他の手段で学習

注意 <Next Page>または<Prev Page>にカーソルを移動してEnterキーを押すとルーティングテーブルをスクロールできます。特定ページを表示する場合は、Page Fieldにページ番号を入力して<Apply>にカーソルを移動してEnterキーを押してください。

Default Route

不明なネットワークに宛てられたすべてのトラフィックを本製品から転送するための転送先ルータを設定します。デフォルトルートはRIPプロトコル経由で学習可能なほか、手動で設定することも可能です。本製品上にデフォルトルートが何も存在しない場合、そのルーティングテーブル内のエントリと一致しないパケットは破棄されます。デフォルトルートを手動で設定する場合は、以下のテーブル上でNext Hopを指定してください。



「VLAN」

デフォルトルータへのIPインターフェースを持つVLANです。

「Next Hop Address」

デフォルトルータのIPアドレスです。

「Metric」

デフォルトルータに到達するまで必要なホップ数です。

IP Multicast Registration Table

本製品上で活動中のすべてのマルチキャストグループを表示します。表示される情報にはマルチキャストIPアドレスおよびこれに対応するVLANなどが含まれます。

```
IP Address Table: IP Multicast Registration Table
=====
VLAN      Multicast IP      1          2          slot1      Learned by
123456789012345678901234 1          123456789012345678901234 1          slot1

Page 1      <Apply>          Total 0 Pages
<OK>      <Prev Page>     <Next Page>
The page number. | READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.
```

「VLAN」

表示されたマルチキャストサービスの受信を要求した、ホストメンバーの所属するVLANが表示されます。

「Multicast IP」

特定のマルチキャストサービスを表す、送信元(ソース)IPアドレスが表示されます。

「Multicast Group Port Lists」

表示されたVLANグループに所属するポートが表示されます。

「Learned by」

このエントリが動的に学習されたのか、IGMPスヌーピング経由で学習されたのかを示します。マルチキャストパケットがポートを通過するのを本製品が検出した場合、エントリは動的(ダイナミック)に学習されます。逆にIGMPレジストレーションパケットがポートを通過するのを検出した場合は、IGMPスヌーピングにより学習します。

注意 アドレステーブルをスクロールさせる場合は、<Next Page> か<Prev Page>にカーソルを移動してEnterボタンを押してください。特定ページを表示する場合はPage Field に参照したいページ番号を入力して<Apply>にカーソルボタンを押してください。

IP Security Filtering Configuration

いずれかのノード上でセキュリティ上の問題が認められた場合は、そのアドレスをIP Security Filterに登録し、このノードへのトラフィックをすべてフィルタできるようにになっています。当テーブル上のいずれかのエントリと一致する送信元/送信先IPアドレスを持つパケットは、本製品を通過する際にフィルタされます。



注意 <Next Page>または<Prev Page>にカーソルを移動してEnterキーを押すとルーティングテーブルをスクロールできます。特定ページを表示する場合は、Page Fieldにページ番号を入力して<Apply>にカーソルを移動してEnterキーを押してください。エントリを追加する場合は<Add>にカーソルを移動してEnterキーを押してください。

Subnet Information

本製品上で設定されているすべてのIPインターフェースを表示します。当テーブルにはゲートウェイアドレスおよびこれに対応するVLANのほか、このアドレスを使用するメンバーポートも表示します。

| IP Address | Subnet Mask | VLAN | 1 | 2 | slot1 |
|---------------|---------------|------|--------------------------|---|-------|
| 192.168.1.254 | 255.255.255.0 | 1 | SSSSSSSSSSSSSSSSSSSSSSSS | S | |

Page 1 of 1
<OK> <Apply> Total 1 Pages
<Prev Page> <Next Page>
The page number. | READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

「IP Address」

本製品上のIPインターフェースのアドレスです。

「Subnet Mask」

サブネットマスクが表示されます。

「VLAN」

当IPインターフェースと関連づけられているVLANグループが表示されます。

8.System Restart Menu

システムを再起動又は再起動時に工場出荷時の設定に戻すかどうかを設定します。管理エージェントをリセットする場合は、Main MenuでRestartコマンドを実行してください。



「Reload Factory Defaults」

工場出荷時のデフォルト設定を読み込みます。

「Restart」

本製品を再起動します。

注意 本製品は、再起動時に必ずPOST（電源投入時の自己診断）を実行します。また工場出荷時の設定を読み込むよう設定しない限り、それまでのすべてのシステム情報も保持します。

9.Exit

設定プログラムを終了し、本製品との現在のセッションを切断する場合はMain Menu内のExitコマンドを実行してください。

5. Webベース管理

1. Webベース管理エージェントについて

コンソールからのメニュー式の設定プログラムに加え、本製品にはHTTP Webエージェントが内蔵されています。本エージェントは、標準のWebブラウザを搭載したPCであれば、ネットワーク上のどのPCからでもアクセスすることが可能です。(インターネットエクスプローラ4.0以降およびネットスケープナビゲータ4.0以降に対応しています。)

このWebブラウザ管理インターフェイスでは本製品の設定が行えるほか、ネットワーク上の動作も監視できるようになっています。また本Webインターフェイスからは、本製品のMIBおよびRMONデータベースを使ったSNMP管理機能の数々にアクセスすることが可能です。

Webブラウザから本製品にアクセスする前に、以下の作業が完了していることをあらかじめご確認ください。

シリアルポート経由での接続またはBOOTPプロトコルを使って、本製品にIPアドレス、サブネットマスクおよびデフォルトゲートウェイ(レイヤ2モード用)が設定されていること。

シリアルポート経由での接続でAdministrator(管理者)用ユーザー名およびパスワードが設定されていること。Webエージェントは、製品内蔵の設定プログラムで使用されているのと同じ管理者用ユーザー名およびパスワードで管理を行います。

2. Webブラウザインターフェイスを操作する

Webブラウザインターフェイスにアクセスするには、まずユーザー名とパスワードを入力する必要があります。デフォルトのユーザー名はadminとなっており、パスワードは設定されていません。管理者は、すべての設定パラメータおよび統計において読み書きアクセスが実行できるようになっています。

3.メインウィンドウ

ご利用のWebブラウザが本製品のWebエージェントに接続すると、メインウィンドウが表示されます。ホームページの左側にはメインメニューが表示されるほか、右側にはシステム情報が表示されます。メインメニューからの各リンクを使用して他のメニューへ移行または設定パラメータおよび統計データを表示することが可能です。

The screenshot displays the web interface for the PCI-24 switch. The top navigation bar includes the PCI-24 logo, the text 'LAYERS INTELLIGENT SWITCH FML-24', and a 'Mode' dropdown menu currently set to 'Active'. Below the header, there are tabs for 'System Information' and 'Switch Information'. The main content area is titled 'FML-24 Manager' and contains a table with the following data:

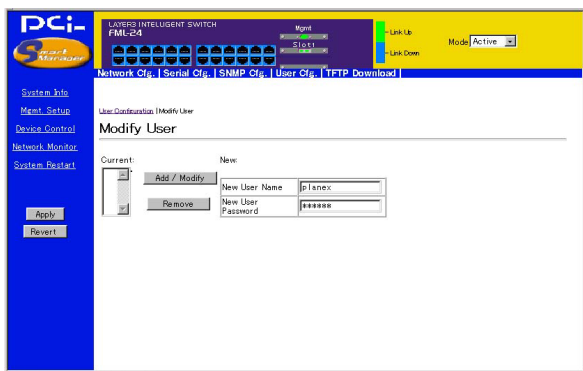
| | |
|----------------|---------------------|
| System Name | FML-24 |
| Object ID | 0.0 |
| Location | Beve lop |
| Contact | j271 |
| System Up Time | 0 d 0 h 15 min 13 s |

Below the table, there are three links with descriptions:

- [Tech](#) -Connect to User Interface
- [Support](#) -Send mail to technical support
- [Contact](#) -Contact to Web Page

The left sidebar contains the following menu items: System Info, Mgmt. Setup, Device Control, Network Monitor, and System Restart. At the bottom of the sidebar, there are 'Apply' and 'Revert' buttons.

初めてこの管理エージェントにアクセスされた場合は、新しい管理者(Administrator)名およびパスワードを設定し、紙などに記録してこれを安全な場所で保管してください。メインメニューから Mgmt.Setupを選択し、上側のメニューバーから User.Cfgを選びます。Modify.Userを選択し、管理者用の新しい名前およびパスワードを入力してください。ユーザー名およびパスワードは、どちらも半角英数文字で最長16文字まで設定可能です。どちらも大文字・小文字の区別は行いません。



注意 デフォルト設定では、(ログイン時)パスワードは三回まで入力可能となっています。三度目も間違ってもパスワードが入力された場合、接続は自動的に切断されます。

設定可能オプション

設定可能なパラメータには、それぞれダイアログボックスからリストボックスが用意されています。いずれかのページ上で設定内容を変更した場合は、必ず画面一番下の Apply ボタンを押して変更内容を更新してください。以下に、使用可能な設定ボタンについて解説します。



「Apply」

指定された値をSNMPエージェントにセットします。

「Revert」

指定した値をキャンセルし、Applyボタンが押される前の状態に戻します。

パネル表示

Webエージェント上のポート画像では、本製品上各ポートのリンクおよび動作状況を確認することができます。いずれかのポートを直接クリックすると、そのポートの統計および設定情報が表示されます。「Mgmt」と表示されているシリアルポートをクリックすると、Console Configurationスクリーンが表示されます。フロントパネル上の他のポートをクリックすると、Switch Informationスクリーンが表示されます。



Port State Display (ポート状態表示)

いずれかのポートをクリックすると、ポート状態の概要が表示されるほか、Etherlike統計およびRMON統計が表示されます。

The screenshot shows the web interface for a PCI Layer 2 Intelligent Switch (FML-24). The interface includes a navigation menu on the left with options like System Info, Mgmt. Setup, Device Control, Network Monitor, and System Restart. The main content area displays the configuration for a specific port, including its name, type (1000BASE-SX), and various status indicators. Below this, there are two tables: 'Port Statistics' and 'RMON Statistics'.

| Name | |
|---------------------|-------------|
| Type | 1000BASE-SX |
| Admin Status | Enable |
| Link Status | on |
| Speed Status | Auto-1000M |
| Duplex Status | Full |
| Flow Control Status | DISABLED |
| VLAN ID | 1 |

| Port Statistics | | | |
|------------------------|--------|-----------------------|--------|
| In Octets | 304531 | Out Octets | 427416 |
| In Unicast Pkts. | 1120 | Out Unicast Pkts. | 1116 |
| In Non-Unicast Pkts. | 1948 | Out Non-Unicast Pkts. | 735 |
| In Discards | 0 | Out Discards | 0 |
| In Errors | 0 | Out Errors | 0 |
| Alignment Errors | 0 | CRC Errors | 0 |
| Single Collisions | 0 | Multiple Collisions | 0 |
| Deferred Transmissions | 0 | Late Collisions | 0 |
| Excess Collisions | 0 | Carrier Sense Errors | 0 |
| Drop Events | 0 | Fragments | 0 |
| Octets | 741947 | Jobs | 0 |

「Type」

ポートの種類を表示します。

100TX : 10BASE-T/100BASE-TX

1000SX : 1000BASE-SX

「Admin Status」

ポートが有効であるか、または1)異常動作か2)セキュリティ上の理由で無効となっているかを示します。

「Link Status」

ポートと外部機器との間で有効な接続があるかどうかを示します。

「Speed Status」

現在のポート速度を表示します。

「Duplex Status」

ポートの現在の通信モードを表示します。

「Flow Control Status」

使用中のフローコントロールの種類を表示します。フローコントロールは、本製品に直接接続されているエンドステーションから送られるトラフィックを遮断してフレームの損失を防ぎます。

「VLAN」

このポートで受信された、タグ無しフレームに割り当てられるVLAN IDです。同じタグ無しのVLANにポートを割り当てる場合はPVIDを使用してください。

コンソール設定

エージェントモジュール(本製品)のシリアルポートと帯域外コンソール接続を行うことが難しい場合は、Webエージェントを通じて、シリアルポートの現在の設定を表示・変更することが可能です。これらの設定を参照または変更する場合は、本製品イメージ上のシリアルポートのアイコンをクリックしてください。

The screenshot shows the web interface of a PCI Layer 2 Intelligent Switch (FML-24). The top navigation bar includes links for Port Statistics, RMON Statistics, L2 Table, VLAN Info, IP Address Table, and Subnet Info. The main content area is titled "Serial Port Configuration" and contains a table of settings:

| | |
|-----------------------|--------------|
| Console Baud Rate | 19200 |
| Console Data Bits | 8 |
| Console Stop Bits | 1 |
| Console Parity | None |
| Console Time-Out | 0 minute(s) |
| Console Auto-Retrieve | 10 second(s) |

On the left side of the interface, there is a vertical menu with links for System Info, Mgmt. Setup, Device Control, Network Monitor, and System Restart. Below these links are "Apply" and "Revert" buttons.

「Baud rate」

機器間でデータを送信する速度です。

設定範囲：9600/19200/38400ボー

「Time-Out」

この時間の間、接続機器から何も入力がないと現在のセッションは自動的に切断されます。設定範囲：0～100分（0＝無効に設定）

「Data bits」

RS-232ポートのデータビットを設定します。設定範囲：7,8

「Stop bits」

RS-232ポートのストップビットを設定します。設定範囲：1,2

「Parity」

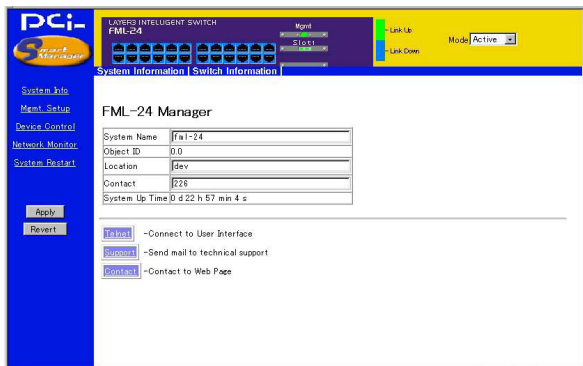
RS-232ポートのパリティを設定します。設定範囲：none/odd/even

System Information Menu

システム監理者への連絡先やハードウェア/ソフトウェアのバージョン情報など、システムの基本的な情報を参照する場合は System Information Menuを使用します。

System Information

システムの設定情報や、システムの内容を簡単に確認する場合は System Information スクリーンを参照してください。



「System Name *」

本製品に割り当てられている名称です。

「Object ID」

本製品のネットワーク管理サブシステム用MIB IIオブジェクト識別子です。

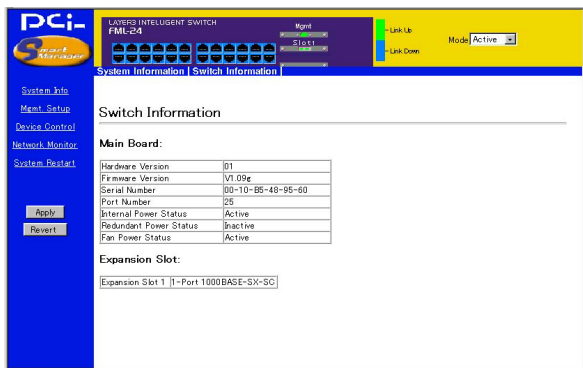
「System Up Time」

現在起動している管理エージェント (management agent) の稼働時間を表示します

* 最大255文字までの入力が可能です。画面に表示されるのは最初の45文字までとなります。矢印キーで残り部分を表示することができます。

Switch Information

本製品マザーボードのハードウェア/ファームウェアのバージョン番号および電源状態を確認する場合は Switch Information スクリーンを参照してください。



「Main Board Serial Number」

マザーボードのシリアル番号です。

「Port Number」

本製品上のポート数です。

「Hardware Version」

マザーボードのハードウェアバージョンです。

「ROM Version」

ROM内システムファームウェアのバージョンです。

「Internal Power Status」

主電源の使用/非使用を表示します。

「Redundant Power Status」

予備電源の使用/非使用を表示します。

「Fan Power Status」

ファン電源の使用/非使用を表示します。

「Expansion Slot 1」

モジュール装着時にその内容を表示します。

4. Mgmt.Setup

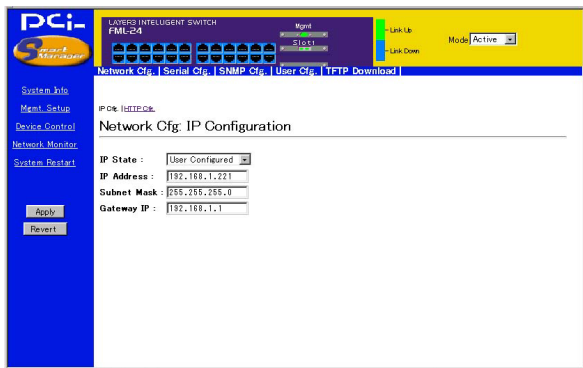
初めてシステムにログインした場合は、管理者およびユーザーのパスワードを設定します (User Configuration)。これらの情報は、必ず紙に書き写して安全な場所に保存するようにしてください。またコミュニティストリング (文字列) の設定も行ってください (SNMP Configuration)。コミュニティストリングは、帯域内管理ソフトウェアを使って製品上SNMPエージェントへのアクセスを制限します。Management Setup Menuで使用可能なオプションを以下に示します。

Network Configuration

IP設定、Ping設定およびHTTP (Webエージェント)設定を含みます。

IPcfg

起動オプションおよび本製品のIPパラメータを設定する場合や、同時に接続可能なTelnetセッションの最大数を設定する場合はIP Configurationスクリーンを使用します。



「IP State」

IPアドレスを手動設定で有効とするか、またはBoot Protocol (BOOTP)で設定するかを決定します。

USER-CONFIG : IP機能は、デフォルトまたはユーザーの指定するIP設定に基づき有効となります。(デフォルト設定)

BOOTP Get IP : IPは有効となりますが、BOOTPの応答を受信するまで実際に機能しません。本製品は、BOOTPのIPアドレスを確認するため、定期的にBOOTP要求をブロードキャストします (BOOTP設定値にはIPアドレス、デフォルトゲートウェイおよびサブネットマスクの各情報が含まれます)。

「IP Address」

現在管理を行っている本製品のIPアドレスです。本製品はUDP/IPトランスポートプロトコル経由でのSNMPに対応しています。この環境では、インターネット上から本エージェントにアクセスする全てのシステム(ネットワーク相互接続機器およびPCなど)はそれぞれIPアドレスが設定されている必要があります。

有効なIPアドレスはピリオド(.)で区切られた四つの番号で表されます。各番号はそれぞれ0~255の範囲で設定します。当設定プログラムは、この形式以外の入力は受け付けないようになっています。

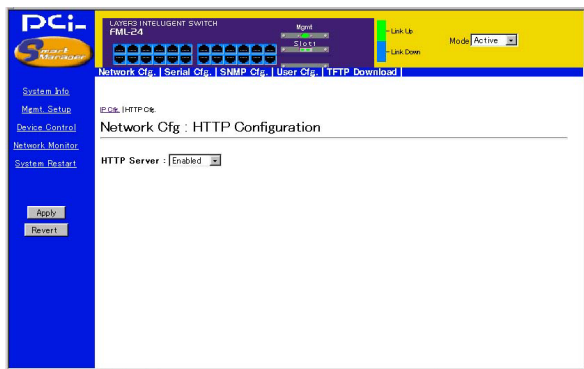
「Subnet Mask」

本製品のサブネットマスクです。当マスクは、特定のサブネットヘルートする際使用されるホストアドレス・ビットを示します。

「Gateway IP」

本製品から管理ステーションにトラップメッセージを渡す際に使用するゲートウェイを指します。なお、管理ステーションが別のIPセグメント上に存在する場合は必ずゲートウェイの指定を行ってください。

HTTP Cfg.



「HTTP Configuration」

Webエージェントを有効にします。

Serial Cfg.

The screenshot shows the web interface for an FML-24 LAYERS INTELLIGENT SWITCH. The main content area is titled "Serial Port Configuration" and contains the following settings:

| | |
|----------------------|--------------|
| Console Baud Rate | 19200 |
| Console Data Bits | 8 |
| Console Stop Bits | 1 |
| Console Parity | None |
| Console Time-Out | 0 minute(s) |
| Console Auto-Refresh | 10 second(s) |

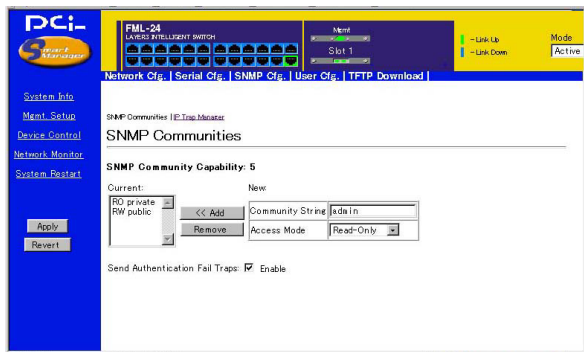
On the left side of the interface, there is a navigation menu with the following items: System Info, Mgmt. Setup, Device Control, Network Monitor, and System Restart. Below the menu are "Apply" and "Revert" buttons. The top of the interface includes the device name "FML-24", a "Mgmt" dropdown menu, "Slot 1", and a "Mode" dropdown menu set to "Active".

「Serial Port Configuration」

シリアルポート用通信パラメータの設定(ボーレート、コンソールタイムアウトおよびスクリーンデータのリフレッシュ間隔)を行います。

SNMP Cfg.

SNMP関連の設定内容を表示・変更する場合はSNMP Configuration スクリーンを使用します。本製品搭載のSNMPエージェントは、本製品ハードウェアの状態ならびにその各ポートを通過するトラフィックを監視します。これらの情報は、ネットワークに接続されているコンピュータ(NMS=ネットワーク管理ステーション)からアクセスすることが可能です。エージェントモジュール(本製品)へのアクセス権はコミュニティストリングにより制限されます。本製品と接続する際、NMSはまず有効なコミュニティストリングを送信して認証を受ける必要があります。コミュニティ名は最大5つまで入力することが可能です。



「SNMP Community Capability」

コミュニティストリングは最大5つまで使用することができます。

「Community String」

管理アクセスが許可されているコミュニティ名(エントリ)です。最大20文字までの文字列が指定可能です。

「Access Mode」

管理アクセスは、Read Only (読み取り専用)か Read/Write (読み書き可)のいずれかにのみ設定可能です。

「Add/Remove」

アクティブリスト上でストリングの追加・削除を行います。

「Send Authentication Fail Traps」

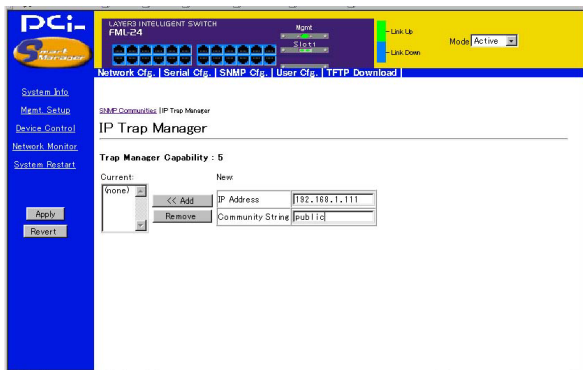
いずれかのSNMP要求の認証に失敗すると、指定IPトラップマネージャに対しトラップメッセージを送信します。(デフォルトでは無効に設定されています)

「Send Link Up/ Down Traps」

スイッチ上ポートのリンク状態が変化するたびに、指定IPトラップマネージャに対しトラップメッセージを送信します。

IP Trap Manager

本製品から認証失敗メッセージや他のトラップメッセージを受信する管理ステーション(Management Station)の設定方法を説明します。トラップマネージャは最大5つまで設定可能となっています。



「Trap Manager」

トラップマネージャは最大5つまで設定可能です。

「IP Address」

トラップマネージャのIPアドレスです。

「Community String」

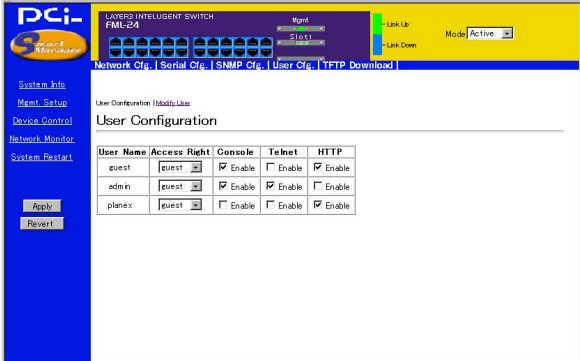
トラップメッセージの受信を許可されているコミュニティです。

「Add/Remove」

アクティブ(使用中)リスト上でストリングの追加・削除を行います。

User Configuration

本製品の管理を許可されているユーザーの名前およびアクセス権限を設定します。



The screenshot shows the web interface for a PCI Layer3 Intelligent Switch FML-24. The top navigation bar includes links for Network Cfg., Serial Cfg., SNMP Cfg., User Cfg., and TFTP Download. The main content area is titled "User Configuration" and contains a table with the following data:

| User Name | Access Right | Console | Telnet | HTTP |
|-----------|--------------|--|--|--|
| guest | guest | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input checked="" type="checkbox"/> Enable |
| admin | guest | <input checked="" type="checkbox"/> Enable | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| planex | guest | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input checked="" type="checkbox"/> Enable |

「User Name」

ユーザー名を指定します。ユーザーは、端末、TelnetおよびHTTP経由で本製品を管理することが許可されます。

「Access Right」

ADMIN：全スクリーンにおいて読み書きを許可
GUEST：全スクリーンにおいて読み取りのみ許可

「Console」

端末経由の管理を許可します。

「Telnet」

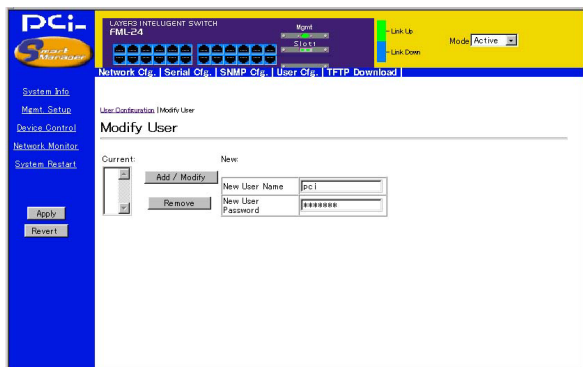
Telnet経由の管理を許可します。

「HTTP」

HTTP (Webブラウザ) 経由の管理を許可します。

Modify User

新規ユーザを登録します。ここで登録された新規ユーザの権限は User Configuration で設定することが可能です。



「New User Name」

新規ユーザ名を入力してください。

「New User Password」

新規ユーザに対応したパスワードを設定してください。

「Add/Modifyボタン」

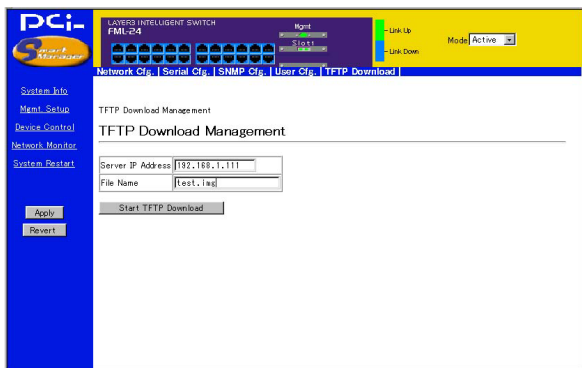
設定された新規ユーザをリストに追加します。

「Removeボタン」

リストからユーザを削除します。

TFTP Download

本製品に最新版ソフトウェアをTFTPサーバ経由でダウンロードすることが可能です。ダウンロードするファイルはバイナリまたはイメージファイルを使用します。(エージェントは他形式のファイルは受け付けません)ダウンロードの成否は、TFTPサーバへの接続性およびネットワーク接続の状態に依存します。最新ソフトウェアをダウンロードすると、本製品は自動的に再起動されます。



「Server IP Address」

TFTPサーバのIPアドレスです。

「Download Mode」

ファームウェアは固定フラッシュROMにダウンロードされます。

「File Name」

ダウンロードするバイナリ/イメージファイルです。

「Start TFTP Download」

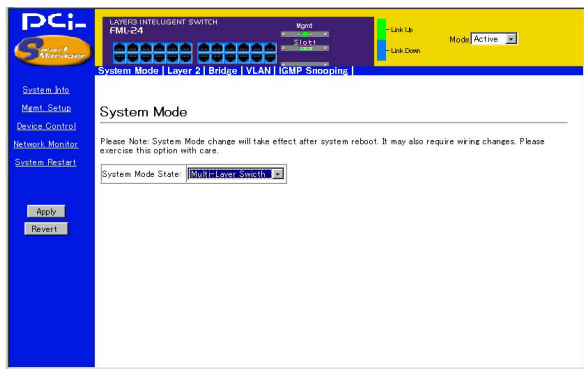
指定ファイルのダウンロードを開始します。

5. Device Control Menu

Device Control メニューからは、ポートモード、ポートミラーリング、ポート・トランキング、スパニングツリー、パーチャルLAN、IP サブネット、マルチキャストフィルタリングおよびルーティングプロトコルなど本製品の多くの機能を設定することが可能です。

System Mode

レイヤ2スイッチ マルチレイヤ・ルーティングスイッチの動作モードを切り替えます



Layer2

各ポートの通信モード、ポートミラーリングおよびポート・トランキングを設定します。

Port Cfg.

現在使用中の通信パラメータを表示/変更します。設定可能なオプションには、管理ステータス、通信速度、通信モードおよびフローコントロールなどがあります。

The screenshot shows the 'Port Configuration' page for a PCI-3000 switch. The interface includes a navigation menu on the left with options like 'System Info', 'Mgmt. Setup', 'Device Control', 'Network Monitor', and 'System Restart'. The main content area displays a table of port configurations. The table has columns for Port, Link Status, Admin Status, Auto Negotiate, Default Type, Current Type, Flow Control, and Jack Type. All 9 ports listed have a red 'X' in the Link Status column, indicating they are not connected. The Admin Status and Auto Negotiate columns are checked for all ports. The Default Type and Current Type are both set to '10M-Half-Duplex' for all ports. The Flow Control column is checked for all ports. The Jack Type is 'RJ,45' for all ports.

| Port | Link Status | Admin Status | Auto Negotiate | Default Type | Current Type | Flow Control | Jack Type |
|------|-------------|---|---|-----------------|-----------------|----------------------------------|-----------|
| 1 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |
| 2 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |
| 3 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |
| 4 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |
| 5 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |
| 6 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |
| 7 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |
| 8 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |
| 9 | ✗ | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled | 10M-Half-Duplex | 10M-Half-Duplex | <input type="checkbox"/> Enabled | RJ,45 |

「Link Status」

ポートと外部機器との間で有効な接続があるかどうかを示します。

「Admin Status」

ポートが有効であるかどうかを示します。

「AutoNegotiate」

オートネゴシエーション機能の有効/無効を設定します。

「Default Type」

ポート速度、通信モードを設定します。

「Current Type」

現在のポート速度(10M、100M、1000M)、通信モード(Half、Full)を示します。

「Flow Control」

フローコントロールを有効/無効に設定します。本製品のバッファが一杯の場合、フローコントロールは、エンドステーションや本製品と直接接続されたセグメントから送られてくるトラフィックを遮断してフレームの損失を防ぎます。有効となっている場合、半二重ではバックプレッシャーを、また全二重ではIEEE802.3xを使用します。なお、ポートがハブに接続されている場合はフローコントロールは使用しないでください。

「Jack Type」

ポートのコネクタの形状を表示します。

Mirror Cfg.

本製品では、本製品のいずれかのポート(ソースポート)から送られるトラフィックを他のポート(ターゲットポート)にコピー(ミラー)して、リアルタイムでトラフィックを解析することが可能です。ターゲットポートにロジックアナライザやRMONプローブなどを接続すると、現状の通信にまったく影響を与えることなく、ソースポートを通過するトラフィックを解析することができます。なお、ポート上のトラフィックをミラーするには、ソース・ターゲットの両ポートとも同じVLANに所属している必要があります。

「Enable Port Mirror」

ポートミラーリングを有効/無効に設定します。

「Tx Mirrored Port」

トラフィック監視の対象となる送信ポートです。

「Rx Mirrored Port」

トラフィック監視の対象となる受信ポートです。

「Monitor Port」

監視対象ポートとして選択されたトラフィックのミラー先ポートを選択します。

「Clean Portsボタン」

Monitor Portとして選択されたポートをクリアします。

Trunk Cfg.

複数のポートを合わせて一つのリンクとして使用することにより、ネットワーク接続の帯域幅を増やしたり、いずれかのポートが使用不可となった場合でも他の予備ルートを使用して接続を維持するなどの冗長化が可能になります。この技術はトランクと呼ばれるもので、本製品同士であればトランク接続を行うことができます。本製品上のRJ-45ポートは、2/4/8ポートをまとめて一本のリンク(トランク)にすることにより、全二重通信時にそれぞれ合計400/800/1600Mbpsまでの帯域幅を提供します。トランク内の各ポート上の負荷を分散する以外にも、実際に二台のスイッチ間でトランク接続を行う前に、Port Trunking Configurationメニューを使って各機器のトランク設定を行う必要があります。なおポート・トランキングを行う際は以下の点にご注意ください。

トランクポートとして追加可能なポートはRJ-45ポートのみ使用可能です。

1つのトランクに割り当てられたポートは、他のトランクに割り当てることは出来ません。

トランクの設定を両方のスイッチで行う必要があります。

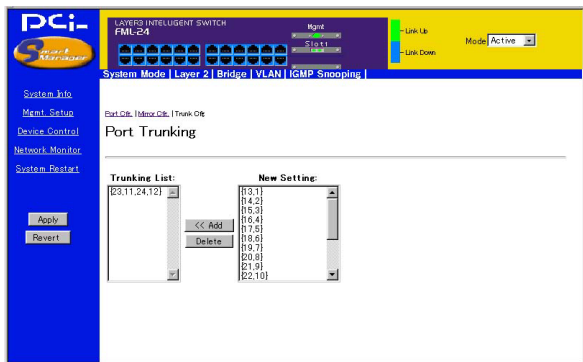
トランクポートは、両方のスイッチで通信モードやVLAN設定などを同じにする必要があります。

トランクに割り当てられたポートはミラー/モニターポートには指定できません。

トランク内のポートを移動したりVLAN上で追加/削除する際は、すべて1グループ単位でまとめて移動/追加/削除を行ってください。

スパニングツリーアルゴリズムは、トランク内の全ポートを1つのリンクとして扱います。

ループの発生を防ぐためにも、スイッチ間を接続する前にトランクを有効にするようにしてください。



「Trunking List」

現在設定されているトランクグループのリストを表示します。

「New Setting」

以下の組み合わせから選択可能です。

- ・2ポートTrunk

< < 13 , 1 > < < 14 , 2 > > < < 15 , 3 > > < < 16 , 4 > >

< < 17 , 5 > > < < 18 , 6 > > < < 19 , 7 > > < < 20 , 8 > >

< < 21 , 9 > > < < 22 , 10 > > < < 23 , 11 > > < < 24 , 12 > >

・ 4ポートTrunk

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

・ 8ポートTrunk

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

トランクを削除する場合は、削除したいするエントリを反転表示させてDeleteボタンをクリックしてください。ポートトランクを切断する場合は、事前に以下の点をご確認ください。

Configuration Menu経由でポートトランクを切断する場合は、最初にトランク内の全ポートを無効にするか、すべてのネットワークケーブルを取り外す必要があります。この操作を行わないとループが発生する恐れがあります。

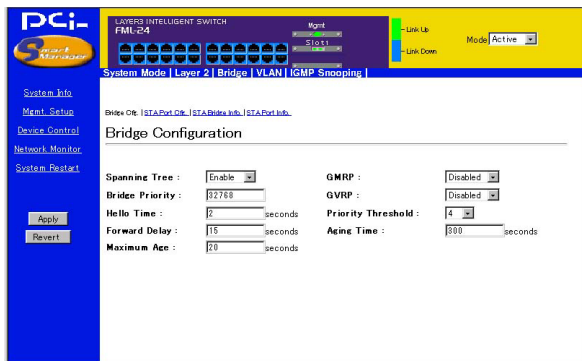
ポートトランク内のいずれか一つのリンクを無効にする場合は、まず該当するネットワークケーブルを外し、そのリンクの両端をそれぞれConfiguration Menu上で無効にする必要があります。この結果リンクを通過するトラフィックは自動的にトランク内の他のリンクに配分されるため、多量のトラフィックを失うことはありません。

Bridge Menu

スパニングツリー・アルゴリズムの設定やブリッジ全体のGMRP (GARP Multicast Registration Protocol)およびGVRP (GART VLAN Registration Protocol) 設定、またトラフィッククラスのプライオリティしきい値やアドレスのエイジングタイムを設定することが可能です。

スパニングツリーアルゴリズム(STA)はネットワークループを検出しこれを無効にするほか、スイッチ・ブリッジおよびルータ間で冗長化を実現できます。本製品はSTAに対応しているため、ネットワーク内の他のSTA対応スイッチ/ブリッジ/ルータと連絡をとりあい、ネットワーク上のどの二つの機器間においても、常にルートが一つだけとなるよう調整します。また通常使用しているリンクが使用不可となっても、代替りのリンクを自動的に提供して通信をそのまま続行することが可能です。

Bridge Configuration



「Spanning Tree」

有効に設定するとSTA対応ネットワークに参加できるようになります。

「Bridge Priority」

ルート機器、ルートポートおよび指定 (designated) ポートを選択します。優先度の最も高い機器がSTAルート機器となります。ただし全機器の優先度が同じ場合は、最も低いIMACアドレスを持ったデバイスがルート機器となります。設定範囲は 0 ~ 65535 となっており、低い数字ほど優先度は高くなります。

「Hello Time」

ルート機器が設定メッセージを送信する間隔を秒で指定します。設定可能な最小値は1となっており、最大値は10秒もしくは $\{(Max. Message Age \div 2) - 1\}$ のうちいずれか低い方となります。

「Forward Delay」

リスニング ラーニング フォワーディングのステート移行を実行する前にルート機器が待機する最大時間を秒単位で設定します。どの機器もフレーム転送を開始する前にトポロジの変更情報を受信する必要があるため、ここで設定するディレイ時間が必要となります。また各ポートも、矛盾する情報がないかどうかリスニングする時間が必要となります。リスニングの結果矛盾する情報が存在する場合はブロッキング状態に移行しますが、リスニングの時間がないとデータがループする恐れがあります。ディレイの設定可能な最大値は30秒です。最小値は4秒もしくは $\{(\text{Max. Message Age} \div 2) + 1 \}$ のうちいずれか大きい方となります。

「Max (Message) Age」

各機器が再設定を試みる前に待機する時間を指定します。この時間の間、設定メッセージが届かない場合は再設定を行います。指定ポート (designated port) を除く全ポートは、一定間隔で設定メッセージを受信します。各ポートとも、最後に受信した設定メッセージに含まれるSTA情報がエージアウトすると、そのポートは接続されたLANの指定ポートとなります。そのポートがルートポートであった場合は、ネットワークに接続されたデバイスポートの中から新しくルートポートが選出されます。最小値は 6秒もしくは $\{ 2 \times (\text{Hello Time} + 1) \}$ のうちいずれか大きい値となるほか、最大値は40秒もしくは $\{ 2 \times (\text{Forward Delay} - 1) \}$ のうちいずれか小さい値となります。

「GMRP」

GMRP(GARP Multicast Registration Protocol)を使用すると、ネットワーク機器側でエンドステーションをマルチキャストグループに登録できるようになります。

本製品全体でGMRPを有効にすると、各ポートごとにGMRPを有効または無効にできるようになります。本製品はIGMPスヌーピングもサポートしているため、マルチキャスト・フィルタリングが行えるようになっています。

「GVRP」

GVRP(GARP VLAN Registration Protocol)は、各スイッチがネットワーク上の必要なVLANメンバーを登録できるよう、互いにVLAN情報を交換する手段を提供します。VLANの自動登録を許可する場合や、ローカルスイッチを超えて広がるVLANを使用する場合などは当機能を有効(Enabled)に設定してください。

「Priority Threshold」

本製品は、2つのプライオリティ・キューを使ったQoSをサポートしており、各ポートではWeighted Fair Queuing(WFQ)を採用しています。IEEE802.1p では最大8個まで別々のトラフィック・クラスを定義することが可能です。このため、プライオリティがこのしきい値と同じかこれより高いパケットは、高いプライオリティ用のキューに移動します。

「(Address)Aging Time」

動的に学習したフォワーディング情報をエージアウトするためのタイムアウト値を秒単位で設定します。設定可能範囲は 10 ~ 415 秒です。

STA Port Cfg.

System Mode | Layer 2 | Bridge | VLAN | IGMP Snooping |

Bridge Ctrl | STA Port Ctrl | STA Bridge Info | STA Port Info.

STA Port Configuration

| Port | Type | Priority | Cost | FastForwarding |
|------|------------|----------------------------------|---------------------------------|---|
| 1 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 2 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 3 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 4 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 5 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 6 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 7 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 8 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 9 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 10 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |
| 11 | 100BASE-TX | <input type="text" value="128"/> | <input type="text" value="19"/> | <input checked="" type="checkbox"/> Enabled |

「Priority」

STAアルゴリズム内での、ポートの使用優先度(プライオリティ)を設定します。スイッチ上の全ポートでパスコストが同じ場合は、プライオリティの最も高い(数値の最も小さい)ポートがスパンニングツリー内でのアクティブリンクとして設定されます。プライオリティが最大のポートが複数存在する場合は、ポートの識別値が最も低いものが有効となります。なお識別値は0~255の範囲で設定可能です。

「(Path) Cost」

スパニングツリーアルゴリズムは、このパスコストをもとに機器間における最適なパスを決定します。このため、より高速なメディアには低い値を、また低速メディアには高い値を設定する必要があります。(パスコストはポート・プライオリティより先に優先されます。)以下に、デフォルトおよび推奨設定を示します。

Ethernet : 100 (50 ~ 600)

Fast Ethernet : 19 (10 ~ 60)

Gigabit Ethernet : 4 (3 ~ 10)

最大レンジは 0 ~ 65535 となっています。

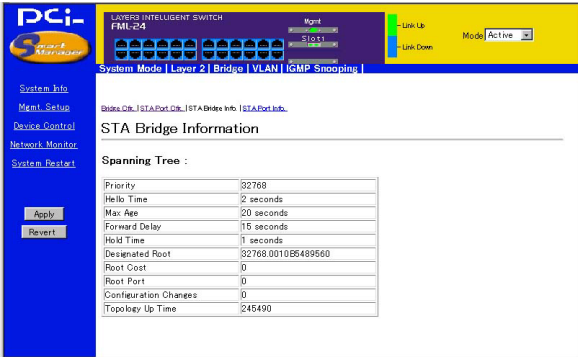
「Fast Forwarding *」

指定ポート上で、ファスト・スパニングツリーモードを有効/無効に設定します。このモードでは、ポートはBlocked、ListeningおよびLearningの各ステートを飛ばして直接Forwardingステートに移行します。

* 末端ノードではフォワーディングループは発生しないため、これらのノードでは、通常の検出(convergence)時間で許されているより高速にスパニングツリーのステート移行を行うことが可能です。ファストフォワーディングは末端ノードおよびサーバ上でより高速に最適経路の検出が行えるほか、他のSTAに関連したタイムアウト問題も克服することが可能です。(重要：ファストフォワードを有効に設定できるポートは、末端デバイスと接続しているポートのみとなっておりますのでご注意ください。)

Spanning Tree Bridge Information

STA Bridge Informationスクリーンには、ブリッジ(本製品)全体のSTA情報の概要が表示されます。



The screenshot shows the configuration page for a PCI switch. The main content area is titled "STA Bridge Information" and displays the "Spanning Tree" configuration. The configuration is presented as a table with the following data:

| | |
|-----------------------|--------------------|
| Priority | 32768 |
| Hello Time | 2 seconds |
| Max Age | 20 seconds |
| Forward Delay | 15 seconds |
| Hold Time | 1 seconds |
| Designated Root | 32768.0010E5489560 |
| Root Cost | 0 |
| Root Port | 0 |
| Configuration Changes | 0 |
| Topology Up Time | 245490 |

「Priority」

本製品は、このプライオリティ値をもとにルート機器、ルートポートおよび指定ポート (designated port) を選出します。プライオリティの最も高いものがSTAルート機器となります。全機器のプライオリティが同じである場合は、最も低いMACアドレスを持つ機器がルート機器に選ばれます。

「Hello Time」

ルート機器が設定メッセージを送信する間隔を秒単位で設定します。

「Max Age」

各機器が再設定を試みる前に、設定メッセージ受信のため待機する時間を秒単位で設定します。

「Forward Delay」

ルート機器がそのステートをリスニング ラーニング フォワーディングと移行する前に待機する時間を秒単位で設定します。

「Hold Time」

連続してConfiguration BPDUを送信する際の、各送信間の最小間隔を設定します。

「Designated Root」

スパニングツリー内で、本製品がルート機器であると認めた機器のプライオリティおよびMACアドレスを示します。

「Root Cost」

本製品上のルートポートからルート機器までのパスコストです。

「Root Port」

本製品上のポートのうち、ルートに最も近いもののポート番号です。本製品は、このポートを通してルート機器との通信を行います。ルートポートが存在しない場合は、本製品自体がスパニングツリーネットワーク内のルート機器として割り当てられています。

「Configuration Changes」

スパニングツリーがこれまで再設定された回数です。

「Topology Up Time」

スパニングツリーが最後に再設定されてから経過した時間です。

Spanning Tree Port Information

The screenshot shows the web interface of a PCi- Layers Intelligent Switch FMT-24. The interface includes a navigation menu on the left with options like System Info, Mgmt Setup, Device Control, Network Monitor, and System Restart. The main content area displays 'STA Port Information' with a table of 14 ports. The table columns are Port, Type, Status, Designated Cost, Designated Bridge, and Designated Port. Most ports are in a 'Disabled' state, while port 14 is 'Forwarding'.

| Port | Type | Status | Designated Cost | Designated Bridge | Designated Port |
|------|------------|------------|-----------------|--------------------|-----------------|
| 1 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.1 |
| 2 | 100BASE-TX | Forwarding | 0 | 32768.0010B5489560 | 128.2 |
| 3 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.3 |
| 4 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.4 |
| 5 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.5 |
| 6 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.6 |
| 7 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.7 |
| 8 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.8 |
| 9 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.9 |
| 10 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.10 |
| 11 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.11 |
| 12 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.12 |
| 13 | 100BASE-TX | Disabled | 0 | 32768.0010B5489560 | 128.13 |
| 14 | 100BASE-TX | Forwarding | 0 | 32768.0010B5489560 | 128.14 |

「Status」

スパンニングツリー内における、ポートの現在の状態を表示します。

「Disabled」

ポート上で何もリンクが確立していないか、ポートがユーザーにより無効に設定されています。もしくは自己診断で不良が認められた可能性があります。

「Blocking」

ポートはSTA設定メッセージを受信しますが、パケットは転送しません。

「Listening」

トポロジ上の変更のため、ポートはブロッキング状態を抜けて設定メッセージの送信を開始します。しかしパケットはまだ転送しません。

「Learning」

ポートは矛盾する情報を受信しておらず、Forward Delayで設定されている時間間隔で設定メッセージを既に送信しました。ポートアドレスはクリアされ、ポートはまたアドレス学習を開始します。

「Forwarding」

ポートはパケットを転送し、アドレス学習を続行します。

ポートステータスは以下のルールにより決定されます。

他にSTA準拠のブリッジ機器が同一セグメント上に存在しない場合、そのポートは常に Forwarding状態となります。

スイッチ上の二つのポートが同一セグメントに接続されており、また他にSTA機器がそのセグメントに接続されていない場合、IDのより小さいポートがパケット転送を行い、他方のポートはブロックされます。

本製品起動時、ポートはすべてブロックされます。この後、ポートのうちいくつかはリスニング、ラーニングそしてフォワーディングへとそれぞれ移行します。

「Designated Cost」

現在のスパニングツリー設定内で、パケットがそのポートからルートに移動する際のコストです。メディアの速度が遅いほどコストは高くなります。

「Designated Bridge (ID)」

このポートがスパニングツリーのルートに到達するため、途中通過しなければならない機器のプライオリティおよびMACアドレスを表示します。

「Designated Port (ID)」

本製品がスパンニングツリーのルートと通信する際、途中通過しなければならない指定 (designated) ブリッジ機器のプライオリティおよびポート番号を表示します。

VLAN

VLAN設定メニューでは、本製品上のどのポートもLANグループに割り当てることができます。本製品では最大256のLANグループが設定可能となっています。従来のルータを使ったネットワークでは、ブロードキャスト・トラフィックは別々のドメインに分けられていました。スイッチは元々ブロードキャストドメインを想定して製造されていないため、IPXやNetBEUIトラフィックを扱う大規模ネットワークではブロードキャスト・ストームが発生する恐れがあります。IEEE802.1Qに準拠した本製品のVLANを使用することにより、複数のネットワーク・ノードを別々のブロードキャストドメインに任意で割り当て、ブロードキャスト・トラフィックを最初のグループ内にものみ制限することが可能です。またVLANは、より安全かつ整然としたネットワーク環境を提供します。

VLAN Table Configuration

新規のVLANグループ作成や既存のVLANグループの設定を変更を行います。

The screenshot shows the 'VLAN Table Configuration' page for a 'LAYERS INTELLIGENT SWITCH FML-24'. The interface includes a navigation menu on the left with options like 'System Info', 'Mgmt. Setup', 'Device Control', 'Network Monitor', and 'System Restart'. The main area displays a table for VLAN configuration. Below the table, there are buttons for 'Add', 'Delete', and 'Modify', and a section for 'VLAN: 2' with a 'Port:' table.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|--------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| VLAN 1 | S | S | S | S | S | N | N | N | N | N | N | N | N | N | N | S | S | S | S | S | S | S | S | S | S |
| VLAN 2 | N | N | N | N | N | N | S | S | S | S | S | S | S | N | N | N | N | N | N | N | N | N | N | N | N |

VLAN: 2 S: Static N: Normal F: Forbidden

| Port: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|-------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |
| 2 | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |
| 3 | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |
| 4 | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |
| 5 | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |
| 6 | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |

「VLAN」

現在設定されているVLANのIDです。

「Port」

ポートエントリの状態を示します。

「S」

ポートを静的(static)エントリとして追加します。

「N」

ポートのGVRPを有効にします(ポートは含みません)。

「X」

ポートのGVRPを無効にします(ポートは含みません)。削除したポートがタグ無しポートとして他のどのグループにも割り当てられていない場合、そのポートは自動的にVLANグループ1にタグ無しポートとして割り当てられます。

「VLAN」

追加、削除、新規したいVLANグループ用の名称および数字の識別番号を指定します。(VLAN名は本製品上での管理でのみ使用します。VLANタグにこの番号は追加されません。)

「Add」

現在のリストに新規VLANグループを追加します。

「Delete」

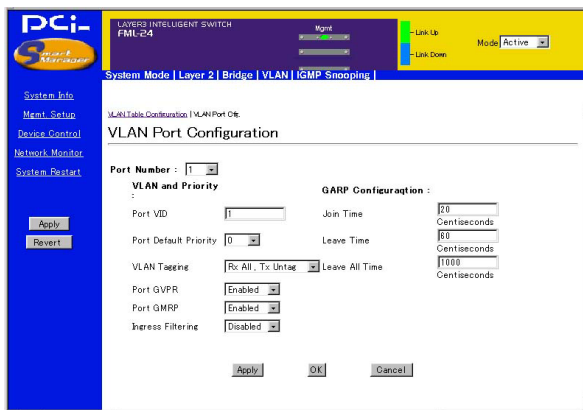
現在のリストからVLANグループを削除します。削除したポートがタグ無しポートとして他のどのグループにも割り当てられていない場合、そのポートは自動的にVLANグループ1に「タグ無し」として割り当てられます。

「Modify」

設定した内容でVLANグループの設定を更新します。

VLAN Port Configuration

GARP、デフォルトVLAN識別子、デフォルトポート・プライオリティ、接続リンクのVLANタグging、GVRPおよびGMRPステータス、ポートが所属していないVLANグループに対して送られてきたフレームのフィルタリングを設定します。



「Port VID」

このポートで受信したタグなしフレームに割り当てられるVLAN IDです。

「Port Default Priority * 1」

イングレス(着信するパケットの)プライオリティ値を設定します。この値より低いものは低プライオリティ用キューに、またこれと同じかより高いプライオリティのものは高プライオリティ用キューに渡します。

「VLAN Tagging *2」

このポートから送信するフレームにVLANタグを追加するかどうかを指定します。

- *1 本製品は二つのプライオリティ・キューを使ったQoSに対応しており、各ポートともWeighted Fair Queuingをサポートしています。着信したフレームのうちVLANタグの無いものは、その着信ポートのデフォルト・イングレス・ユーザープライオリティ情報が追加(タギング)され、出力ポートで適切なプライオリティ・キューに渡されます。どのイングレスポートも、デフォルトのプライオリティ設定は0となっています。このため、着信フレームのうちプライオリティ・タグのないものはすべて低プライオリティ用キューに渡されます。(なお、出力ポートが関連VLANのタグ無しメンバーである場合は、これらのフレームは送信される前にすべてのVLANタグを外されます。)
- *2 1~2台のスイッチのみを使った小規模のポートベースVLANを作成する場合は、ポートを同一のタグ無しVLANに割り当て、これらスイッチ間のVLAN接続には別の接続を使用することが可能です。

しかし本製品を超えて広がっているVLANグループに参加する場合は、そのグループ用のVLAN IDを使用することをおすすめします。なおVLAN IDを使用する方法には1)レイヤ2モードのVLANタギングと、2)マルチレイヤモードの一般PVID使用の二種類があります。本製品をレイヤ2モードでご利用の場合、複数のスイッチをまたがるような大機後VLANグループに割り当てられているポートは、VLANタギングを必ず使用してください。

マルチレイヤモード使用時の制限

ただしマルチレイヤモードをご利用の場合は、現状ではタギングを無効にし、リンクの両側においてPVIDを同じに設定し(接続機器がVLAN対応の場合) このVLANを他グループと接続する場合はさらにIPインターフェースを設定する必要があります。また本製品がマルチレイヤモードで動作している場合は、いずれのVLANも重複させることはできません。(これらの制限は、将来提供されるファームウェア・バージョンからは取り除かれる予定です。)

「GVRP」

このポートのGVRP機能を有効/無効に設定します。無効に設定した場合、このポートで受信されたGVRPパケットは破棄され、他ポートからGVRP登録が(このポートに) 広がることもありません。

注意 この設定を有効とするには、まず本製品全体でGVRPを有効にする必要があります。

「GMRP」

このポート上でGMRPを有効/無効に設定します。有効に設定されていると、当ポートはエンドステーションのマルチキャストグループへの登録を許可します。

注意 この設定を有効とするには、まず本製品上でGMRPを有効にする必要があります。

「Ingress Filtering *3」

有効に設定すると、受信したVLAN宛のフレームのうち、このイングレスポート(Ingress Port)がメンバーセットに含まれていないフレームはイングレスポートで破棄されます。

*3 この制限は、GVRPやSTPといった、VLANに依存しないBPDUフレームに対しては無効となります。ただしGMRPなどのVLANに依存するBPDUフレームは影響を受けます。

「IP Menu *4」

各VLANグループへのIPインターフェイスの設定、VLANのポートグループ設定、システム全体のユニキャストおよびマルチキャスト・ルーティングプロトコル設定、IGMPスヌーピング設定、OSPFエリア設定を行えます。

*4 本製品がマルチレイヤモードで動作中の場合のみ設定可能です。

GARP

GVRPとGMRPは、ブリッジLAN内のクライアント用サービスに対し、クライアント属性を登録/抹消する際にGARP(Group Address Registration Protocol)を使用します。

各GARPタイマのデフォルト値は、データ速度やメディア接続方法に依存しません。GMRPまたはGVRPの登録/抹消において何か不具合が発生していない限り、これらの設定値は変更しないようにしてください。

各ポートのVLAN属性の変更、VLANグループのポート・メンバーシップを設定を設定します。

「Join Time」

グループ内でリクエストまたはクエリーを送る送信間隔を1/100秒単位で設定します。

「Leave Time」

グループから離れる前にポートが待機する時間を1/100秒単位で設定します。Leave Timeは、少なくともJoin Timeの二倍以上に設定する必要があります。このように設定することにより、LeaveまたはLeaveAllメッセージが発信されたあと、参加希望者(applicants)は、ポートが実際にグループを離れる前に再参加できるようになります。

「LeaveAll」

LeaveAllクエリーメッセージをグループ参加者に送信してから、ポートがグループを離れるまでの間隔を1/100秒単位で設定します。グループに再参加するノードから発生するトラフィック量を最小限に止めるためにも、LeaveAllはLeave Timeより相当に大きく設定する必要があります。

IP Menu

本製品がマルチレイヤモードに設定されている場合に本製品上の各VLANのIPサブネットや、IGMPおよびユニキャスト/マルチキャストルーティングプロトコルの設定を行います。

Subnet Configuration

本製品に設定したVLANグループ同士を通信させる場合はそれぞれのVLANグループにIPインターフェースを設定する必要があります。本製品を帯域内(in-band)で使用する場合でも、管理用に最低一つのVLAN用のIPサブネットアドレスを設定する必要があります。

System Mode | Layer 2 | Bridge | VLAN | IP Menu

Subnet Cfg | Protocol Cfg | ICMP Snooping Cfg | OSPF Area Cfg

IP Menu : Subnet Configuration

| IP Address | Subnet Mask | VLAN | RIP | OSPF | DVMRP |
|---------------|---------------|------|-----|------|-------|
| 192.168.1.221 | 255.255.255.0 | 1 | | | |

Modify IP Address: RIP: Advance >>

Add Subnet Mask: OSPF: Advance >>

Cancel VLAN: DVMRP: Advance >>

Apply

Revert

「IP Address」

指定VLANインターフェースと関連づけられるIPアドレスです。

「Subnet Mask」

特定サブネットにルーティングする際に使用されるホストアドレスの、アドレスビットを示すテンプレートです。「1」に対応する各ビットはネットワーク/サブネット番号の一部となっています。また「0」に対応する各ビットはホスト番号の一部となっています。

「VLAN」

IPインターフェイスが追加されているVLANグループを表示します。

「RIP」

設定したインターフェイスに対しユニキャストルーティング用のルーティング情報プロトコルであるRIPが有効または無効に設定されているかを表示します。

「OSPF」

設定したインターフェイスに対しOSPF(Open Shortest Path First)ユニキャスト・ルーティングプロトコルが有効または無効に設定されているかを表示します。

「DVMRP」

設定したインターフェイスに対しDVMRP(Distance-Vector Multicast Routing Protocol)が有効または無効に設定されているかを表示します。

「Modifyボタン」

IPインターフェイスの情報を更新します。

「Addボタン」

設定されたIPインターフェイスを追加します。

「Cancelボタン」

設定されたIPインターフェイスをクリアーします。

「IP Address」

IPアドレスを入力してください。

「Subnet Mask」

特定サブネットにルーティングする際に使用されるホストアドレスの、アドレスビットを示すテンプレートです。「1」に対応する各ビットはネットワーク/ サブネット番号の一部となっています。また「0」に対応する各ビットはホスト番号の一部となっています。

「VLAN」

IPインターフェイスを追加したいVLANグループを入力してください。

「Select」

VLANの作成/編集を行う場合はこのオプションを選択します。

「RIP」

ユニキャストルーティング用のルーティング情報プロトコルの有効/無効を設定します。

「OSPF」

OSPF(Open Shortest Path First)ユニキャスト・ルーティングプロトコルの有効/無効を設定します。

「DVMRP」

DVMRP(Distance-Vector Multicast Routing Protocol)の有効/無効を設定します。

Advanceボタン

RIPのAdvancedオプションでは、複数のルータがお互いにルーティングテーブルの情報を交換する方法を設定します。本製品上でRIPを有効にすると、本製品はネットワーク内の全機器に対し30秒おきにRIPメッセージをブロードキャストし、他のルータからRIPメッセージを受信した際は自身のルーティングテーブルを自動的に更新します。RIPメッセージにはIPアドレスおよび、本製品から各通信先ネットワークまでのメトリック(ホップ数)が含まれます。1)認証タイプの指定、2)指定ポート上でルーティングメッセージ送受信に使用するプロトコル、3)最適パス計算時に使用するデフォルト・メトリックおよび4)Poison Reverseの有効/無効がそれぞれ設定可能です。

「Authentication Type」

認証(authentication)は、ルーティング情報が正当なサイトから送信されたものであることを保証します。

「Authentication Key」

認証を有効にするために必要なパスワードです。認証ストリングは半角英数字で最長16文字まで設定可能です。ストリングは大文字・小文字を区別します。

「Send Type」

このポートから送信されるトラフィックで使用されているプロトコルです。

RIP1 Broadcast : ルート情報は、RIPv1を使ってネットワーク上の他のルータにブロードキャストされます。

RIP2 Broadcast : ルート情報は、RIPv2を使ってネットワーク上の他のルータにブロードキャストされます。

RIP2 Multicast : ルート情報は、RIPv2を使ってネットワーク上の他のルータにマルチキャストされます。

Do Not Send : 本製品は、ネットワークに接続された他のルータから送られてくるルート情報を受動的に監視します。

「Receive Type」

このポートで受信可能なルーティングプロトコルメッセージの種類です。RIP1, RIP2, RIP1/RIP2またはDisabled (受信しない) に設定可能です。

「Default Metric」

メトリックとは、本製品と通信先ネットワークとの間のホップ数を指します。「デフォルトメトリック」は、当インターフェースから発信されたRIP更新(情報)に含まれるデフォルトルートを示します。0と設定すると、デフォルトルートは何も発信されず、他のルータから発信されたデフォルトルートが伝播するようになります。値は0~15の範囲で設定可能です。

「Poison Reverse*」

ルートを最初に入手したインターフェースポートまで、ルートを逆に伝播します。ただし距離のベクター・メトリックは無限大に設定されません。

- * ルーティング情報が送信元までループすることを阻止する方法の一つです。なお、同じ目的のため本製品では「Split Horizon」も有効となっていますのでご注意ください。

IGMP Snooping Configuration

本製品ではIGMP（Internet Group Management Protocol）を使って、本製品と接続されているホストのうち、特定のマルチキャスト・サービスを希望するものを監視することが可能です。IGMPはそのサービスで使用されているIPマルチキャストグループを参照し、同様のリクエストを受信したすべてのポートをこのグループに追加します。

The screenshot shows the web management interface for a PCI Layer 2 Intelligent Switch. The top navigation bar includes 'System Mode | Layer 2 | Bridge | VLAN | IP Menu'. The main content area is titled 'IP Menu : IGMP Snooping Configuration'. It features three configuration options:

- IGMP State:** A dropdown menu currently set to 'Disabled'.
- IGMP Router Timeout:** A text input field containing the value '5', followed by the unit 'minutes'.
- IGMP Group Timeout:** A text input field containing the value '5', followed by the unit 'minutes'.

On the left side of the interface, there is a vertical menu with links for 'System Info', 'Mgmt. Setup', 'Device Control', 'Network Monitor', and 'System Restart'. Below these links are 'Apply' and 'Revert' buttons. The top right corner of the interface shows 'Link Up' and 'Link Down' status indicators, and a 'Mode' dropdown menu set to 'Active'.

「IGMP Status」

有効の場合、本製品はネットワークトラフィックを監視してどのホストがマルチキャストトラフィックの受信を希望しているかを確認します。これを「IGMPスヌーピング」と呼びます。

「IGMP Router Timeout」

スイッチ上のポートで、ここで指定された時間の間マルチキャストプロトコルパケットの受信を停止したものはIGMPフォワーディングリストから除かれます。タイムアウトは3~5分の間で設定可能です。

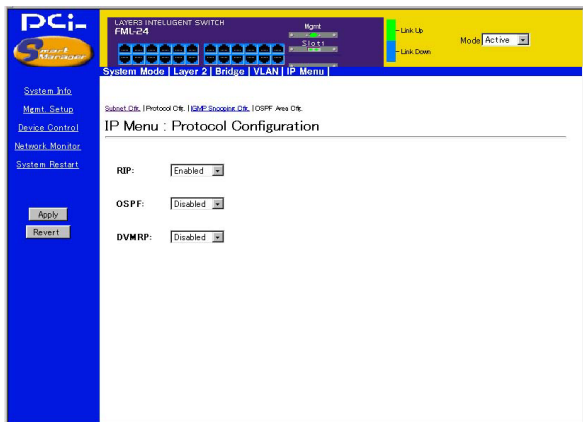
「IGMP Group Timeout」

指定ポート上で、いずれかのIPマルチキャストアドレスに対するIGMP Reportメッセージが検出されてから、本製品がそのエントリをリストから削除するまでの時間を設定します。値は3~5分の間で設定可能です。

注意 IGMPプロトコルセット全体は、DVMRPとともに自動的に有効/無効に設定されます。

Protocol Configuration

本製品上でのルーティングプロトコルの有効/無効を設定します。IPMenuからルーティングプロトコルの設定を行う前に必ず有効または無効に設定してください。



「RIP」

設定したインターフェイスに対しユニキャストルーティング用のルーティング情報プロトコルであるRIPが有効または無効に設定されているかを表示します。

「OSPF」

設定したインターフェイスに対しOSPF(Open Shortest Path First)ユニキャスト・ルーティングプロトコルが有効または無効に設定されているかを表示します。

「DVMRP」

設定したインターフェイスに対しDVMRP(Distance-Vector Multicast Routing Protocol)が有効または無効に設定されているかを表示します。

6. Network Monitor

Network Monitor Menuでは、ポート統計、RMON統計、静的ユニキャスト/マルチキャストアドレステーブルおよびMACアドレス・フィルタテーブルのそれぞれの情報を参照することが可能です。

Port Statistics

Port Statisticsスクリーンでは、各ポートのInterface GroupおよびEthernetMIBに関する主な統計情報が表示されます。これらの情報は、ポート不良や負荷の異常増大など、本製品上で発生する可能性のある問題を識別する際に使用されます。表示される値は、最後にシステムを再起動した時点からの累計です。

The screenshot shows the Network Monitor interface for a Layer3 Intelligent Switch (FML-24). The interface includes a navigation menu on the left with options like System Info, Mgmt. Setup, Device Control, Network Monitor, and System Restart. The main content area displays Port Statistics for a selected Port Number (1). The statistics are organized into two sections: Interfaces and Ethernet. The Interfaces section shows statistics for In Octets, In Unicast Pkts, In Non-Unicast Pkts, In Discards, In Errors, and Alignment Errors, along with corresponding Out statistics. The Ethernet section shows statistics for Single Collisions, Deferred Transmissions, Excess Collisions, Drop Events, and Octets, along with Multiple Collisions, Late Collisions, Carrier Sense Errors, Fragments, and Jabbers. The interface also includes buttons for Refresh, Reset Port Statistics, and Reset All Statistics.

| Interfaces | | | |
|----------------------|---|-----------------------|---|
| In Octets | 0 | Out Octets | 0 |
| In Unicast Pkts. | 0 | Out Unicast Pkts. | 0 |
| In Non-Unicast Pkts. | 0 | Out Non-Unicast Pkts. | 0 |
| In Discards | 0 | Out Discards | 0 |
| In Errors | 0 | Out Errors | 0 |
| Alignment Errors | 0 | CRC Errors | 0 |

| Ethernet | | | |
|------------------------|---|----------------------|---|
| Single Collisions | 0 | Multiple Collisions | 0 |
| Deferred Transmissions | 0 | Late Collisions | 0 |
| Excess Collisions | 0 | Carrier Sense Errors | 0 |
| Drop Events | 0 | Fragments | 0 |
| Octets | 0 | Jabbers | 0 |

「Port Number」

参照したいポートをリストボックスから選択してください。

「Interface In Octets」

このインターフェース上で受信されたオクテット数の合計です。値にはフレーミング・キャラクタも含まれます。

「In Unicast Pkts」

高位層プロトコルに渡されたサブネットワーク-ユニキャストパケットの数です。

「In Non-Unicast Pkts」

高位層プロトコルに渡された、非ユニキャスト(サブネットワーク-ブロードキャストまたはサブネットワーク-マルチキャスト)パケット数を指します。

「In Discards」

高位層プロトコルへ転送するのを防ぐため、なにもエラーが検出されなかったにも関わらず廃棄される受信(インバウンド)パケットの数を指します。これらのパケットを廃棄する理由には、バッファ領域を空ける目的も含まれます。

「In Errors」

エラーが含まれるため高位層プロトコルに転送できない受信(インバウンド)パケット数です。

「Alignment Errors」

アライメントエラー(同期に失敗したデータパケット)数です。

「Out Octets」

このインターフェースから送信されたオクテットの総計です(フレーミングキャラクタも含まれます)。

「Out Unicast Pkts」

高位層プロトコルの要求によりサブネット-ユニキャストアドレスに送信されたパケットの総計です（破棄または送信されなかったパケットも含む）。

「Out Non-Unicast Pkts」

高位層プロトコルの要求により、非ユニキャスト（サブネットワーク-ブロードキャストまたはサブネットワーク-マルチキャスト）アドレスに送信されたパケットの総計です（破棄または送信されなかったパケットも含む）。

「Out Discards」

高位層プロトコルへ転送するのを防ぐため、なにもエラーが検出されなかったにも関わらず廃棄される送信（アウトバウンド）パケットの数を指します。これらのパケットを廃棄する理由には、バッファ領域を空ける目的も含まれます。

「Out Errors」

エラーのため送信できなかったアウトバウンドパケット数です。

「CRC Errors」

当機器で検出された、イーサネットCRC（Cyclic Redundancy Check）エラー数です。

「Ethernet Single Collisions」

正常に送信されたフレームのうち、一回のコリジョンにより送信が禁止されたものの数を示します。

「Deferred Transmissions」

送信メディアがビジー状態のため、特定インターフェース上での一回目の送信試行が失敗したフレームの数です。

「 Excessive Collisions 」

過度のコリジョンのため送信に失敗したフレームの数です。

「 Drop Events 」

リソース不足のためパケットがドロップ(廃棄)されたイベントの総計です。

「 Octets 」

当ポートを通過するオクテット数です。

「 Multiple Collisions 」

正常に送信されたパケットのうち、複数回のコリジョンにより送信が禁止されたものの数を示します。

「 Late Collisions 」

パケット送信中、64オクテット以降に検出されたコリジョン数です。

「 Carrier Sense Errors 」

フレーム送信を試みた際、キャリアセンス状態が失われたか、もしくはこの状態にまったくならなかった回数を示します。

「 Fragments 」

64オクテットより短い受信フレーム(ただしフレーミングビットは除き、FCSオクテットは含む)のうち、FCSもしくはアライメントエラーを起こしたものの総計です。

「 Jabbers 」

1518オクテットより長い受信フレーム(ただしフレーミングビットを除き、FCSオクテットを含む)のうち、FCSまたはアライメントエラーを持ったものの総計です。

■ **注意** 各統計情報の更新はデフォルトで10秒毎におこないます。

「Refreshボタン」

最新のステータス情報に更新します。

「Reset Port Statistics」

選択されたているポートのステータス情報をクリアします。

「Reset All Statistics」

本製品上のポートの全てのステータス情報をクリアします。

RMON Statistics

RMON Statisticsスクリーンでは、RMONグループ1の各ポートの主な統計情報を参照することができます。(RMONグループ2,3および9を参照するにはSNMP管理ソフトウェアを使用してください。)以下のスクリーンでは、各ポートを通過するトラフィックの総合的な統計情報を示しています。RMON Statisticsスクリーンでは、各ポートを通過する異なる種類・サイズのフレームの合計カウントを含む、多くの統計情報にアクセスできるようになっています。なお、表示される値はシステムが最後に再起動された時点からの累計です。

The screenshot shows the 'RMON Statistics' page for a 'LAYER3 INTELLIGENT SWITCH FML-24'. The 'Port Number' is set to 1. The statistics table is as follows:

| | | | |
|-----------------------|---|-----------------------|---|
| Drop Events | 0 | Jabbers | 0 |
| Received Bytes | 0 | Collisions | 0 |
| Received Frames | 0 | 64 Byte Frames | 0 |
| Broadcast Frames | 0 | 65-127 Byte Frames | 0 |
| Multicast Frames | 0 | 128-255 Byte Frames | 0 |
| CRC/Alignments Errors | 0 | 256-511 Byte Frames | 0 |
| Undersize Frames | 0 | 512-1023 Byte Frames | 0 |
| Oversize Frames | 0 | 1024-1518 Byte Frames | 0 |
| Fragments | 0 | 1519-1536 Byte Frames | 0 |

Buttons at the bottom of the table include 'Refresh', 'Reset Port Statistics', and 'Reset All Statistics'.

「Port Number」

参照したいポートをリストボックスから選択してください。

「Drop Events」

リソース不足のためパケットが廃棄されたイベントの総計です。

「Received Bytes」

ネットワーク上で受信したデータの合計バイト数です。この情報は、Ethernetの利用状況を確認する上で有効なデータとなっています。

「Received Frames」

フレーム(不良フレーム、ブロードキャスト/マルチキャストフレーム)の総受信数を示します。

「Broadcast Frames」

受信された有効フレームのうち、ブロードキャストアドレスに転送されたものの総計です。これにはマルチキャストパケットは含まれませんのでご注意ください。

「Multicast Frames」

受信された有効フレームのうち、このマルチキャストアドレスに転送されたものの総計です。

「CRC/Alignment Errors」

CRC/アライメントエラー（FCSまたはアライメントエラー）の総計です。

「Undersize Frames」

受信フレームのうち、長さが64オクテットより短いことを除けば他に問題が検出されなかったフレームの総計です。なおFCSオクテットはこれに含まれますが、フレーミングビットは除きます。

「Oversize Frames」

受信フレームのうち、長さが1518オクテットより長いことを除けば他に問題が検出されなかったフレームの総計です。なおFCSオクテットはこれに含まれますが、フレーミングビットは除きます。

「Fragments」

受信フレームのうち、64オクテットより短かつFCSかアライメントエラーが含まれるものの総計です。なおFCSオクテットはこれに含まれますが、フレーミングビットは除きます。

「 Jabbers 」

受信フレームのうち、1518オクテットより長くかつFCSかアライメントエラーが含まれるものの総計です。なおFCSオクテットはこれに含まれますが、フレーミングビットは除きます。

「 Collisions 」

このEthernetセグメント上で発生するコリジョンの予想発生数です。

「 64 Byte Frames 」

送受信したフレームのうち、長さが64オクテットのものの総計です。これには不良パケットやFCSオクテットが含まれますが、フレーミングビットは除きます。

「 65-127 Byte Frames, 128-255 Byte Frames, 256-511 Byte Frames, 512-1023 Byte Frames, 1024-1518 Byte Frames, 1519-1536 Byte Frames 」

送受信したフレームのうち、長さがこの範囲内のものの総計です。これには不良パケットやFCSオクテットが含まれますが、フレーミングビットは除きます。

注意 デフォルト設定では、各統計は10秒ごとに更新(リフレッシュ)するようになっています。

「 Refreshボタン 」

最新のスタティクス情報に更新します。

「 Reset Port Statistics 」

選択されたているポートのスタティクス情報をクリアします。

「 Reset All Statistics 」

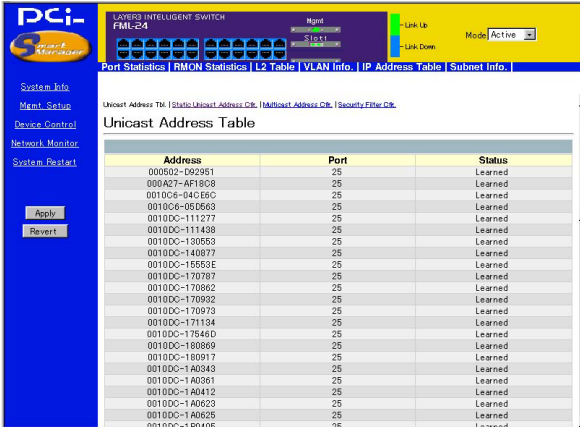
本製品上のポートの全てのスタティクス情報をクリアします。

Layer 2 Address Table

このメニューでは、ユニキャストアドレステーブル、静的ユニキャスト/マルチキャストアドレステーブルおよびセキュリティフィルタテーブルを参照することができます。

Unicast Address Table

ユニキャストアドレステーブルには、各ポートと関連付けられたMACアドレス(これらのアドレスと関連付けられた送信元(ソース)ポート)が含まれます。Address Table内に表示される各情報につき解説します。



The screenshot shows the PCi-Switch Manager interface for a Layer 3 Intelligent Switch FML-24. The main content area displays the Unicast Address Table with the following data:

| Address | Port | Status |
|---------------|------|---------|
| 000502-D92951 | 25 | Learned |
| 000A27-AF18C8 | 25 | Learned |
| 0010C6-04CE6C | 25 | Learned |
| 0010C6-05D663 | 25 | Learned |
| 0010DC-111277 | 25 | Learned |
| 0010DC-111438 | 25 | Learned |
| 0010DC-130553 | 25 | Learned |
| 0010DC-140877 | 25 | Learned |
| 0010DC-15563E | 25 | Learned |
| 0010DC-170787 | 25 | Learned |
| 0010DC-170862 | 25 | Learned |
| 0010DC-170932 | 25 | Learned |
| 0010DC-170973 | 25 | Learned |
| 0010DC-171134 | 25 | Learned |
| 0010DC-17546D | 25 | Learned |
| 0010DC-180869 | 25 | Learned |
| 0010DC-180917 | 25 | Learned |
| 0010DC-1A0343 | 25 | Learned |
| 0010DC-1A0361 | 25 | Learned |
| 0010DC-1A0412 | 25 | Learned |
| 0010DC-1A0623 | 25 | Learned |
| 0010DC-1A0625 | 25 | Learned |
| 0010DC-1B040E | 25 | Learned |

「Address」

本製品上で参照できるノードのMACアドレスです。

「Port」

自身のアドレステーブルにこのMACアドレスを持つポートです。

「Status」

アドレスステータスを表示します。

「Learned」

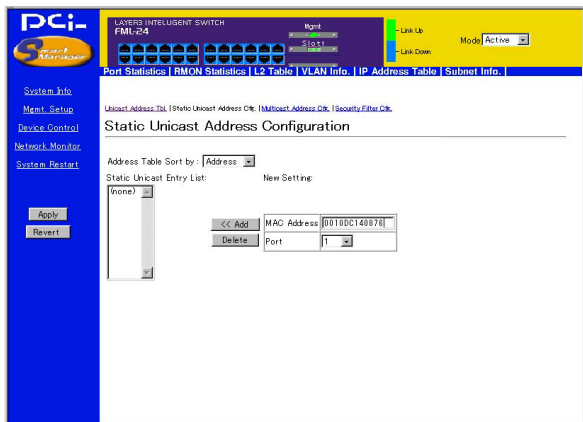
動的(ダイナミック)に学習。

「Static」

SNMPネットワーク管理ソフトウェアにより永久に固定。

Static Unicast Address Cfg.

Static(静的)ユニキャストアドレステーブルを使って、ホスト機器のMACアドレスを本製品上の特定ポートに割り当てることができます。静的ユニキャストアドレスはエージアウトしないほか、他のポート上で学習することはできません。このテーブル内にある送信元アドレスを持ったパケットが他のポートに届いても、このパケットはそこで破棄されます。以下に、Static Unicast Address Table 内の各項目につき解説します。



「MAC Address」

ポートに割当てたいMACアドレスを入力してください。

「Port」

MACアドレスを追加するポートを選択してください。

「Addボタン」

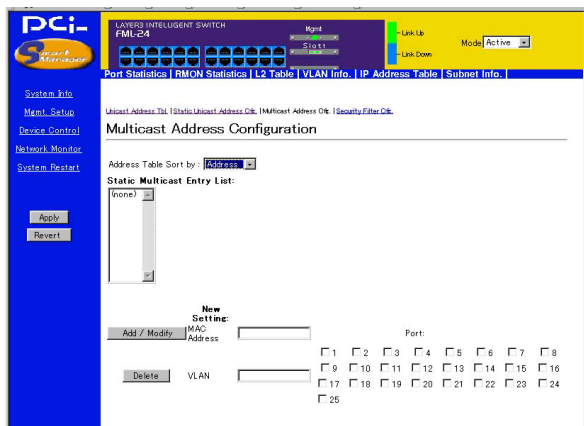
Static Unicast Entry Listに設定されたMACアドレスをリストします。

「Deleteボタン」

Static Unicast Entry Listから選択されたMACアドレスを削除します。

Static Multicast Address Table

Static Multicast Address Tableを使って、特定のマルチキャストサービス用に使用するVLANグループに対し、接続先MACアドレスおよびこれに対応するポートを割り当てることができます。静的マルチキャストアドレスはエージアウトしないほか、これらのアドレスを持ったトラフィックは、このテーブルで指定されているポートにしか転送できないようになっています。



「MAC Address」

マルチキャストサービスの供給先(送信先)MACアドレスを入力してください。

「VLAN」

このマルチキャストサービスに対応するVLANグループを入力してください。

「Port」

マルチキャストトラフィックを転送したいポート番号を入力してください。

「Add/Modifyボタン」

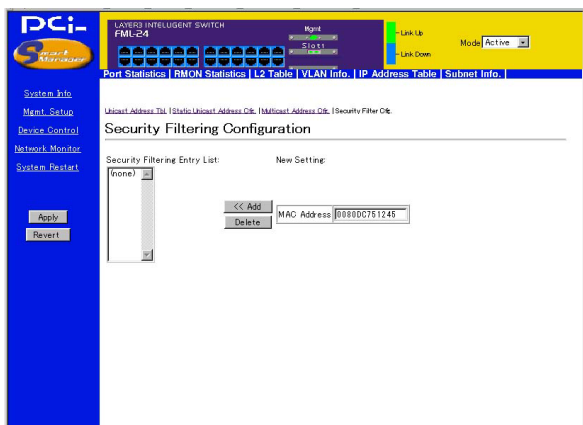
Static Multicast Entry Listに設定されたMACアドレスをリストします。また設定された内容で更新します。

「Deleteボタン」

Static Multicast Entry Listから選択されたMACアドレスを削除します。

Security Filtering Configuration

セキュリティ面でリスクのあるノードや故障中のノードは、本製品上でフィルタする(切り離す)ことができます。セキュリティ・フィルタリングを使って、指定MACアドレスのホストから送信されるトラフィックをすべて破棄することが出来ます。同様に、本製品ではSecurity Filtering Configurationテーブル内で登録されている送信元/送信先アドレスを持つトラフィックをフィルタすることが可能です。



「MAC Address」

フィルタの対象になるMACアドレスを入力します。

「Addボタン」

入力されたMACアドレスをフィルタリングテーブルに追加します。

「Deleteボタン」

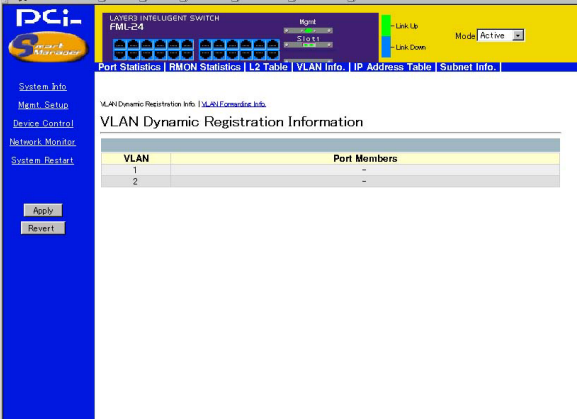
Security Filtering Entry ListにリストされているMACアドレスから選択したアドレスを消去します。

VLAN Information

以下の各メニューは、GVRP経由で自動的に学習されたポートの情報および、動的または静的で設定された、VLANトラフィック転送用ポートの情報を表示します。

VLAN Dynamic Registration Information

GVRPにより自動的に学習されたポートを表示します。

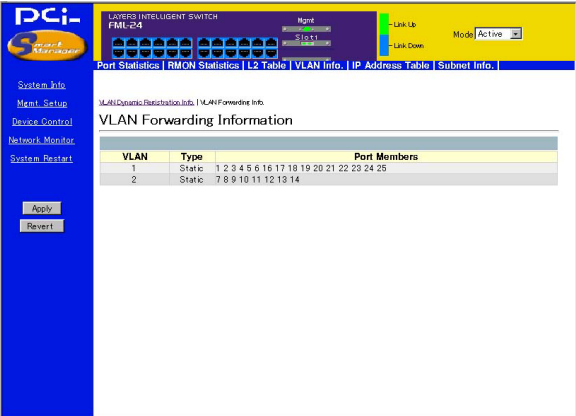


The screenshot displays the web interface for a Layered Intelligent Switch (FML-24). The interface includes a navigation menu on the left with options like System Info, Mgmt. Setup, Device Control, Network Monitor, and System Restart. The main content area shows the VLAN Dynamic Registration Information, which is currently empty.

| VLAN | Port Members |
|------|--------------|
| 1 | - |
| 2 | - |

VLAN Forwarding Information

VLANトラフィック転送用の、動的または静的に設定されたポートを表示します。



The screenshot shows the web interface for a PCI-Switch Management system. The main content area displays the 'VLAN Forwarding Information' table. The table has three columns: 'VLAN', 'Type', and 'Port Members'. There are two rows of data, both for static VLANs.

| VLAN | Type | Port Members |
|------|--------|---|
| 1 | Static | 1 2 3 4 5 6 16 17 18 19 20 21 22 23 24 25 |
| 2 | Static | 7 8 9 10 11 12 13 14 |

IP Address Table

このメニューでは、1)静的ルート、2)動的に学習されたルート、3)未知のネットワークアドレス用のデフォルトルート、4)マルチキャストグループ、および5)セキュリティフィルタの各IPアドレステーブルを表示します。

ARP Table

ARP(Address Resolution Protocol)は、ホストのインターネットアドレスからそのイーサネットアドレスを割り当てる方法を定義します。ARPにより検出されたIPとMACアドレスのキャッシュ情報を表示します。

The screenshot shows the H3C S Series Switch Manager interface. The main content area displays the 'IP Address Table : ARP Table' for a 'LAYERS INTELLIGENT SWITCH FML-24'. The table lists the following data:

| IP Address | Mac Address | VLAN | Port |
|-----------------|----------------|------|------|
| 169.254.185.86 | 0010DC-111438 | 1 | 25 |
| 169.254.189.235 | 00C0CA-8003DE | 1 | 25 |
| 192.168.1.0 | FFFFFF-FFFFFF | 1 | - |
| 192.168.1.1 | 004005-51E45F | 1 | - |
| 192.168.1.10 | 004005-42A031 | 1 | 25 |
| 192.168.1.16 | 004005-A045F8 | 1 | 25 |
| 192.168.1.19 | 00A0AE-00775D | 1 | 25 |
| 192.168.1.20 | 004005-A05D94 | 1 | 25 |
| 192.168.1.25 | 00A0AE-001DC-E | 1 | - |
| 192.168.1.26 | 00A0AE-004AF2 | 1 | 25 |
| 192.168.1.28 | 0010DC-05D563 | 1 | 25 |
| 192.168.1.30 | 008045-12940C | 1 | - |
| 192.168.1.31 | 0010DC-1D0539 | 1 | 25 |
| 192.168.1.33 | 0010DC-15553E | 1 | 25 |
| 192.168.1.34 | 0010DC-04CE9C | 1 | 25 |
| 192.168.1.35 | 0010DC-170862 | 1 | 25 |
| 192.168.1.36 | 008045-10C0D9 | 1 | 25 |
| 192.168.1.37 | 0090CC-A52BD1 | 1 | 25 |
| 192.168.1.40 | 008045-1178FA | 1 | 25 |
| 192.168.1.41 | 008045-117113 | 1 | 25 |
| 192.168.1.42 | 008045-120AEB | 1 | 25 |
| 192.168.1.45 | 008045-1172B7 | 1 | 25 |
| 192.168.1.46 | 000045-131067 | 1 | 25 |

「IP Address」

ブロードキャストメッセージをもとに、ARPはこのIPアドレス用の物理アドレスを検出します。

「MAC Address」

IPアドレスに対応しているMACアドレスが表示されます。

「VLAN」

ホストに割り当てられているVLANグループが表示されます。

「Port」

ホスト機器と接続しているポートが表示されます。

注意 <First page>または<Next Page>にカーソルを移動してEnterキーを押すとアドレステーブルをスクロールさせることができます。

Static Route Table

本製品では、ユニキャストまたはマルチキャスト・ルーティングプロトコルを使用し、他のIPネットワーク/サブネットホストへのルートをダイナミックに学習するよう設定できるようになっています。しかし特定の通信先へのルートがこれらのプロトコルで学習できない場合や、通信先にトラフィックを送信する際指定のパスを使用させたい場合は、Static Route Tableを使って静的パスを設定することも可能です。

静的ルートを定義する前に、本製品上で少なくともIPインターフェースを一つ設定する必要があります。静的ルートは動的(ダイナミック)に学習したルートより優先されるほか、ユーザーがテーブルから削除するか、対応するIPインターフェースを本製品から削除しない限りテーブル内から消えることはありません。

PCi- Search Manager

LAYER3 INTELLIGENT SWITCH
FML-24

Port Statistics | RMON Statistics | L2 Table | VLAN Info. | IP Address Table | Subnet Info.

System Info
Mgmt. Setup
Device Control
Network Monitor
System Restart

Apply
Revert

APB TL | Static Route TL | Routing TL | Default Route | IP Multicast Per. TL | P.P Filter

IP Address Table : Static Route Table

Static Route Entry List:
Destination Network Destination Mask VLAN Next Hop Type Metrics

(none)

New Setting:

<< Add Destination Network: 192.168.10.0 Destination Mask: 255.255.255.0

Delete Next Hop: 192.168.1.11 Routing Metric: 1

「Destination Network」

宛先のネットワークグループ入力してください。

「Destination Mask」

宛先のサブネットマスクを入力してください。

「Next Hop」

次のホップにあたるルータのIPアドレスを入力してください。

「Routing Metric」

Destination networkへのIPルートの種類を入力してください。本製品は以下のルートをサポートしています。

Direct : 直接接続されているサブネットワーク

Indirect : リモートIPサブネットワークまたはリモートホスト
アドレス

Myself : 特定IPサブネットワーク上のスイッチIPアドレス

Bcast : サブネットワーク・ブロードキャストアドレス

Mcast : IPマルチキャストアドレス

Invalid : フィルタ対象となる不正IPアドレス

Routing Table

認識されているすべてのイーサネット・ネットワークおよび対応VLANまでの各ルートを表示します。ルーティングプロトコルで学習されたルートおよび手動設定されたルートは、すべてこのRouting Tableに含まれます。

The screenshot shows the PCI-Switch Manager web interface for a LAYER3 INTELLIGENT SWITCH FML-24. The main content area displays the 'IP Address Table : Routing Table' with the following data:

| Destination Network | Destination Mask | VLAN | Next Hop | Type | Protocol | Route Aging | Routing Metric |
|---------------------|------------------|------|---------------|--------|----------|-------------|----------------|
| 192.9.200.0 | 255.255.255.0 | 2 | 192.9.200.1 | Direct | Local | 0 | 1 |
| 192.168.1.0 | 255.255.255.0 | 1 | 192.168.1.221 | Direct | Local | 0 | 1 |

「Destination Network」

通信先のネットワーク/サブネット/ホストです。

「Destination Mask」

適合するビットを指定するサブネットマスクです。Destination Maskにより設定されたビットがDestination Networkと一致する場合、ルーティングエントリはパケットに使用(適用)されます。

「VLAN」

ゲートウェイまたはDestination AddressはこのVLAN内に存在します。

「Next Hop」

次のホップにあたるルータのIPアドレスです。

「Type」

Destination networkのIPルートの種類です。本製品は以下のルートをサポートしています。

Direct : 直接接続されているサブネットワーク

Indirect : リモートIPサブネットワークまたはリモートホストアドレス

Myself : 特定IPサブネットワーク上のスイッチIPアドレス

Bcast : サブネットワーク・ブロードキャストアドレス

Mcast : IPマルチキャストアドレス

Invalid : フィルタ対象となる不正IPアドレス

「プロトコル」

ルートは以下のいずれかの方法で学習されます。

Local : 手動設定

Mgmt : SNMPで設定

ICMP : ICMPリダイレクト経由で入手

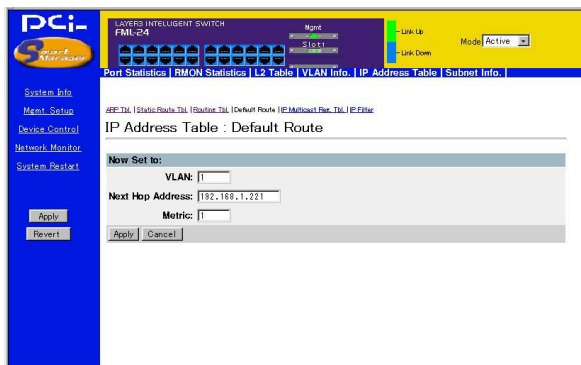
RIP : RIPプロトコルで学習

OSPF : OSPFプロトコルで学習

Other : 他の手段で学習

Default Route

不明なネットワークに宛てられたすべてのトラフィックを本製品から転送するための転送先ルータを設定します。デフォルトルートはRIPプロトコル経由で学習可能なほか、手動で設定することも可能です。本製品上にデフォルトルートが何も存在しない場合、そのルーティングテーブル内のエントリと一致しないパケットは破棄されます。デフォルトルートを手動で設定する場合は、以下のテーブル上でNext Hopを指定してください。



「VLAN」

デフォルトルータへのIPインターフェースを持つVLANグループを入力してください。

「Next Hop Address」

デフォルトルータのIPアドレスを入力してください。

「Metric」

デフォルトルータに到達するまで必要なホップ数を入力してください。

「Applyボタン」

設定された内容を更新します。

「Cancelボタン」

設定された内容をクリアします。

IP Multicast Registration Table

本製品上で活動中のすべてのマルチキャストグループを表示します。表示される情報にはマルチキャストIPアドレスおよびこれに対応するVLANなどが含まれます。

The screenshot shows the web management interface for a PCI-24 Layer 2 Intelligent Switch. The interface includes a navigation menu on the left with options like System Info, Mgmt. Setup, Device Control, Network Monitor, and System Restart. The main content area displays the 'IP Address Table : IP Multicast Registration Table' with a table containing columns for VLAN, Multicast IP, Multicast Group Ports, and Learn By. The table is currently empty.

| VLAN | Multicast IP | Multicast Group Ports | Learn By |
|------|--------------|-----------------------|----------|
| - | - | - | - |

「VLAN」

表示されたマルチキャストサービスの受信を要求した、ホストメンバーの所属するVLANが表示されます。

「Multicast IP」

特定のマルチキャストサービスを表す、送信元(ソース)IPアドレスが表示されます。

「Multicast Group Port Lists」

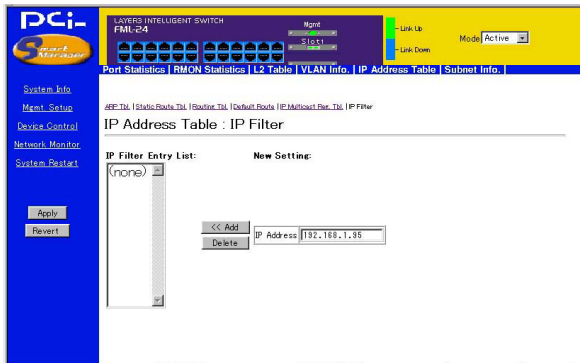
表示されたVLANグループに所属するポートが表示されます。

「Learned by」

このエントリが動的に学習されたのか、IGMPスヌーピング経由で学習されたのかを示します。マルチキャストパケットがポートを通過するのを本製品が検出した場合、エントリは動的(ダイナミック)に学習されます。逆にIGMPレジストレーションパケットがポートを通過するのを検出した場合は、IGMPスヌーピングにより学習します。

IP Filter

いずれかのノード上でセキュリティ上の問題が認められた場合は、そのアドレスをIP Filter に登録し、このノードへのトラフィックをすべてフィルタできるようにになっています。当テーブル上のいずれかのエントリと一致する送信元/送信先IPアドレスを持つパケットは、本製品を通過する際にフィルタされます。



「IP Address」

フィルタリングしたいIPアドレスを入力してください。

「Addボタン」

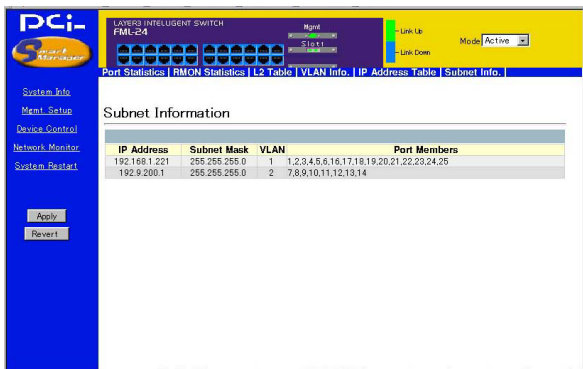
設定されたIPアドレスをIP Filter Entry Listに追加します。

「Deleteボタン」

IP Filter Entry Listから選択されたIPアドレスを削除します。

Subnet Information

本製品上で設定されているすべてのIPインターフェースを表示します。当テーブルにはゲートウェイアドレスおよびこれに対応するVLANのほか、このアドレスを使用するメンバーポートも表示します。



The screenshot shows the web management interface for a Layer 3 Intelligent Switch (FML-24). The page title is "Subnet Information". The interface includes a navigation menu on the left with options like "System Info", "Mgmt. Setup", "Device Control", "Network Monitor", and "System Restart". The main content area displays a table with the following data:

| IP Address | Subnet Mask | VLAN | Port Members |
|---------------|---------------|------|---|
| 192.168.1.221 | 255.255.255.0 | 1 | 1,2,3,4,5,6,16,17,18,19,20,21,22,23,24,25 |
| 192.9.200.1 | 255.255.255.0 | 2 | 7,8,9,10,11,12,13,14 |

「IP Address」

本製品上のIPインターフェースのアドレスです。

「Subnet Mask」

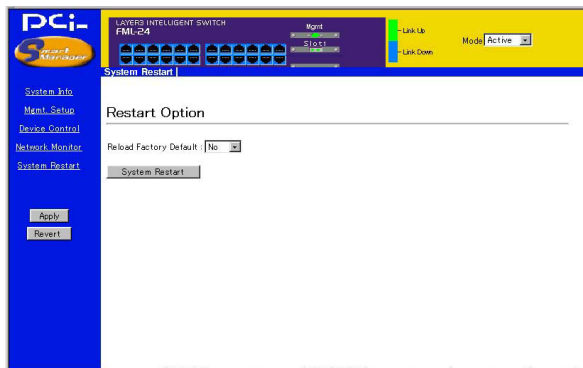
サブネットマスクが表示されます。

「VLAN」

当IPインターフェースと関連づけられているVLANグループが表示されます。

7.System Restart Menu

システムを再起動又は再起動時に工場出荷時の設定に戻すかどうかを設定します。管理エージェントをリセットする場合は、Main MenuでRestartコマンドを実行してください。



「Reload Factory Default」

Yesに設定すると再起動時に工場出荷時のデフォルト設定を読み込みます。

「System Restartボタン」

本製品を再起動します。

注意 本製品は、再起動時に必ずPOST（電源投入時の自己診断）を実行します。また工場出荷時の設定を読み込むよう設定しない限り、それまでのすべてのシステム情報も保持します。

6. 詳細解説

本製品は、機器の物理アドレスに基づくレイヤ2および、IPネットワークアドレスに基づくレイヤ3スイッチングの両者に対応しています。以下に、これらの機能を含めた詳細を説明します。

1. レイヤ2スイッチング

フレームがポートに到達すると、ポートは自身のアドレスデータベース内でこのフレームの送信先MACアドレスを検索し、送信先のポートを確認します。送信先アドレスが他のポート上で見つかった場合、フレームはそのポートに転送され、出力待ちのキューに入れられます。送信先アドレスがアドレスデータベース内で見つからない場合、フレームはタグ付/タグ無しVLANフレームの処理を行った後、一つないし複数の他の出力ポートに送られます。

フレームの送信先MACアドレスがアドレステーブル内で見つからなかった場合、フレームはそれが着信されたポートの番号とともに記録されます。この情報は、後にフレーム転送を決定する際に使用されます。

スイッチングを行う際、本製品は以下に示される複数の処理を実行します。

- VLAN判別 (VLAN Classification)

- ラーニング

- フィルタリング

- フォワーディング

- エージング

ユニキャスト・スイッチング

当セクションでは、ユニキャスト・スイッチングのVLAN判別、ラーニング、フィルタリングおよびフォワーディングについてそれぞれ説明します。

VLAN 判別(VLAN Classification)

本製品上で受信されたフレームは、以下の二種類いずれかに分類されます。

タグ無しフレームの場合、本製品はこのフレームを受信ポートのデフォルトVLANに分類します。

タグ付フレームの場合、本製品はタグ付VLAN IDを使ってフレームのプロードキャストドメインを識別します。

ラーニング

VLAN判別が完了すると、本製品はアドレステーブル内の <source MAC address, VLAN (送信元MACアドレス、VLAN)> ペアを参照し、このペアが既知のものかどうかを確認します。

ペアが未知のものである場合、本製品はこの <source MAC Address, VLAN> ペアを学習しアドレステーブルにこれを追加します。

ペアが既知である場合、本製品はこのペアに間違っただポートIDが与えられていないか確認します。アドレステーブル内の source MAC address, VLAN ペアに関連づけられているポートIDが受信ポート以外のポートである場合、本製品はアドレステーブル内のポートIDを修正し、その管理データベースも同様に修正します。

フィルタリング

アドレスの学習(ラーニング)が完了すると、本製品はフィルタリングを行います。

送信元/送信先ポートがフォワーディング状態以外の状態にないか(例:ブロッキング状態や無効になっていないか)

送信元/送信先MACアドレスがフィルタ(破棄)対象となっていないか

送信元ポートIDと送信先ポートが同じでないか

これらの条件のうちどれか一つでも満たされると、本製品は受信フレームをドロップ(破棄)します。どの条件もあてはまらない場合、本製品は以下のようにフォワーディング処理を続けます。

フォワーディング

フォワーディング処理中、本製品は destination MAC address, VLAN(送信先MACアドレス、VLAN)ペアが既知のものかどうか確認します。

ペアが未知のものである場合、本製品は受信フレームをVLAN内の全ポート(送信元ポートを除く)に一括送信します。

ペアが既知のものである場合、本製品は受信フレームを destination MAC address, VLAN ペアに関連付けられているポートに転送します。同時に本製品は、VLANタグ付/タグ無し設定および出力ポートのVLAN IDの各情報に従って、このフレームにVLANタグを付けるべきか、逆にVLANタグを取り除くべきかを決定します。

2. マルチキャスト・スイッチング

マルチキャスト・スイッチングを行う際、本製品は受信フレームがBPDU(Bridge Protocol Data Unit)かどうかを判断します。BPDUを受信していた場合、本製品はこのフレームがスパニングツリープロトコルに処理されるよう転送します。これ以外の場合、本製品は以下の処理を実行します。

「VLAN判別」

ユニキャスト・スイッチングと同じです。

「ラーニング」

ユニキャスト・スイッチングと同じです。

「フィルタリング」

ラーニング完了後、本製品はフィルタリングを行います。

- ・送信元/送信先ポートがフォワーディング状態以外の状態にないか(例：ブロッキング状態や無効になっていないか)
- ・送信元/送信先MACアドレスがフィルタ対象となっていないか
- ・送信元ポートIDと送信先ポートが同じでないか

これらの条件のうちどれか一つでも満たされると、本製品は受信フレームをドロップ(破棄)します。どの条件もあてはまらない場合、本製品はフォワーディング処理を続けます。

「フォワーディング」

本製品は受信フレームをVLAN内の全ポート(送信元ポートを除く)に一括送信します。同時に本製品は、VLANタグ付/タグ無し設定および出力ポートのVLAN IDの各情報に従って、このフレームにVLANタグを付けるべきか、逆にVLANタグを取り除くべきかを決定します。

「エージング」

本製品はMACアドレステーブル内の< MAC addresses, VLAN >ペアに対しエージング処理を行います。< MAC addresses, VLAN >ペアがエージアウトするたび、アドレステーブルは修正されます。

3. スパニングツリーアルゴリズム

スパニングツリーアルゴリズム(IEEE802.1Dに定められるSTA設定アルゴリズム)はネットワークループを検出しこれを無効にするほか、スイッチ・ブリッジおよびルータ間で予備用(バックアップ)リンクを提供します。本製品はSTAに対応しているため、ネットワーク内の他のSTA対応スイッチ/ブリッジ/ルータと連絡をとりあい、ネットワーク上のどの二つの機器間においても、常にルートが一つだけとなるよう調整します。冗長パスやループを検出した場合、一つまたはそれ以上のポートをブロッキング状態(パケット転送を停止)にして余分なパスを排除します。また安定したスパニングツリートポロジ内で一つ以上のパスが使用不可となっても、これまでブロッキング状態にしてきたポートをフォワーディング状態にして全ネットワークステーションとの接続を復旧します。

STAは分布式的アルゴリズムを使用し、スパニングツリーネットワークのルートとして動作するブリッジ機器(STA対応スイッチ/ブリッジ/ルータ)を選出します。ルート機器を除いた各ブリッジング機器上ではルートポートが選択されます。ルートポートは、その機器からルート機器までパケットを転送する際、パスコストが最も低くなるものを指します。次にSTAは、各LANより指定(designated)ブリッジング機器を選出します。指定ブリッジング機器とは、LANからルート機器までにパケットを送信する際のパスコストが最小となるものを指します。指定ブリッジング行きに接続されたポートはすべて指定(designated)ポートとして割り当てられます。コストが最低となるスパニングツリーが決定されると、STAはすべてのルートポートおよび指定ポートを有効にし、残りのポートをすべて無効に設定します。このためネットワークパケットはルートポートと指定ポートの間でのみ転送されるかたちとなり、ネットワーク・ループの発生を防ぐことが可能となります。

安定したネットワークトポロジがいったん確定すると、全ブリッジはルートブリッジから送信されるHello BPDUを受信するようになります。事前に設定しておいた期間(Maximum Age)が経過してもHello BPDUが受信されない場合、そのブリッジは、ルート・ブリッジとのリンクが使用不可となったものと判断します。この場合、ブリッジは他のブリッジとのネゴシエーションを始め、ネットワークを再設定して使用可能なネットワークトポロジを再度構成します。

以下は、STAがブリッジ機器のポートを割り当てる仕組みを表しています。

Root Bridging Device : ルートブリッジ

Designated Port : 指定ポート

Root Port : ルートポート

Blocking : ブロッキング「FDX LED」

ポートが全二重でリンクが確立したときに点灯します。

4. レイヤ3スイッチング

レイヤ3スイッチの特長は、1)IPスイッチングと2)ルーティングパス管理となっています。本製品は、マルチレイヤモードに設定するとルーティングスイッチとして動作します。このとき本製品では、標準のIPルーティングおよびVLAN間でトラフィックをやりとりする機能が使用可能となります。ただし本製品を初めてマルチレイヤモードに設定した場合、その時点ではまだデフォルトルーティングが設定されていません。従来のルータ同様、この時ルーティング機能の設定を行う必要があります。

5. 初期設定

デフォルトでは、全ポートとも同じVLANに割り当てられているほか、本製品自体もレイヤ2の機能しか使用できないようになっています。このため、まず同一サブネットに所属するポートをVLANグループに分割する必要があります。同一サブネット内のネットワークトラフィックは、以前と同じようにレイヤ2スイッチングによりスイッチされます。またレイヤ3スイッチングを使用することにより、必要な場合に限って複数VLAN間を相互接続することが可能です。

各VLANは、レイヤ3への仮想インターフェースとして機能します。各仮想インターフェースのネットワークアドレスを設定するだけで異なるサブネットワーク間のトラフィックはレイヤ3スイッチングによりルートされるようになります。

サブネット間トラフィック（レイヤ3スイッチング）

Routing : ルーティング

Intra-subnet : サブネット内トラフィック(レイヤ2スイッチング)

注意 マルチレイヤモードでご利用の場合は、ポートはすべてタグ無しに設定する必要があるほか、VLANグループが重複しないようにしてください。またVLANが複数スイッチをまたがる場合は、同じデフォルトPVIDを設定する必要があります。

6. IPスイッチング

IPスイッチング(パケットフォワーディング)は、レイヤ2・レイヤ3両者のパケット転送で必要な処理を指すほか、従来のルーティングも担当します。以下、サポートされている各機能を解説します。

レイヤ2送信先MACアドレスを使ったレイヤ2フォワーディング(スイッチング)

レイヤ3フォワーディング(ルーティング)

- ・レイヤ3送信先アドレスを使ったフォワーディング
- ・各ホップの送信先/送信元MACアドレスの変更
- ・ホップカウントのカウント増加
- ・Time-to-liveの減少
- ・レイヤ3チェックサムの検証および再計算

送信先ノードが送信元ネットワークと同一のサブネットワーク上にある場合は、パケットはルータの助けを借りることなく直接送信することができます。ただし本製品にとって未知のMACアドレスであった場合、送信先アドレスの入ったARP (Address Resolution Protocol) がブロードキャストされ、送信先ノードから送信先MACアドレスを入手します。この時点で、IPパケットを直接送信先MACアドレスに送信することが可能になります。

送信先が本製品上の別のサブネットに所属する場合、パケットは直接送信先ノードまでルートすることができます。ただし本製品に含まれないサブネットに所属するパケットの場合、パケットはルータに送信する必要があります。この場合ルータのMACアドレスを送信先MACアドレスとして使用するほか、送信先ノードの送信先IPアドレス情報も一緒に送られます。ルータはこの時点でパケットを正しいパス経由で送信先ノードに転送します。また必要に応じて、ルータはARPプロトコルを使って次のルータの送信先ノード用MACアドレスを確認します。

注意 IPスイッチングを行う場合、本製品は他ネットワーク上のノードからIPルータとして認識される必要があります。このためには、本製品をデフォルト・ゲートウェイに設定するか、またはICMP処理経由で他のルータからリダイレクトする必要があります。

本製品が自身のMACアドレス宛のIPパケットを受信すると、そのパケットにはレイヤ3のルーティング処理が実行されます。レイヤ3アドレステーブル上にパケットの送信先IPアドレスがないか確認を行い、テーブル上で見つからない場合、本製品は送信先VLAN上の全ポートに対しARPパケットを送信して送信先MACアドレスを探します。MACアドレスが発見されると、パケットは再フォーマットされて送信先に送られます。再フォーマット処理には具体的に、1)IPヘッダのTTL (Time-To-Live)フィールドの減少、2)IPヘッダのチェックサムの再計算および、3)送信先MACアドレスを送信先ノードのMACアドレスまたは次ホップのルータのMACアドレスに変更する作業などが含まれます。

同一ノード行きのパケットが他に届いた場合、送信先MACアドレスはレイヤ3アドレステーブルから直接読み込まれ、パケットは再フォーマットを受けて送信先ポートに送られます。送信先アドレスが既にレイヤ3アドレステーブルに記憶されている場合、IPスイッチングはワイヤースピードで実行することが可能となっています。

7. Routing Path Management (ルーティングパスの管理)

Routing Path Managementを行うには、パケット転送に必要なすべてのルーティング情報の決定および更新が必要となります。以下に、これらの各情報につき解説します。

- ルーティングプロトコルの処理

- ルーティングテーブルの更新

- レイヤ3スイッチングデータベースの更新

8. ICMP Router Discovery

ホストが自身に直接接続されたサブネットを超えてIPデータグラムを送信する場合、このホストはあらかじめ、そのサブネット上で現在動作中の、最低一つのルータのアドレスを発見しておく必要があります。この情報は通常、システム起動時に設定ファイル内のルータアドレスのリストを1~2個参照するだけで入手できるようになっています。マルチキャストリンクの場合、ホストの中には、ルーティングプロトコル・トラフィックを監視してルータアドレスを入手するものもあります。

ICMP Router Discoveryメッセージはこれらに代わるルータの検出方法で、マルチキャストリンク上において一対のICMPメッセージを使用します。この方法では手動でルータのアドレスを設定する必要がないほか、どのルーティングプロトコルにも依存しません。

IGMP Router Discoveryメッセージは「Router Advertisements」および「Router Solicitations」と呼ばれています。各ルータは、そのマルチキャストインターフェースから定期的にRouter Advertisements をマルチキャストして、このインターフェースのIPアドレスを宣言します。各ホストは、Router Advertisements を受信(listen)するだけで自身の近辺のルータを検出できません。マルチキャストリンクに接続されているホストが起動すると、このホストはRouter Solicitationをマルチキャストし、アドバタイズメント定期送信を待たず、即座にアドバタイズメント送信するよう要求します。

Router Discoveryメッセージはルーティングプロトコルを構成するわけではありません。これらのメッセージは各ホストがその周囲のルータを認識できるようにはするものの、特定の送信先に対し、ルータにルートを提供させることはできません。ホストが特定の送信先用として選んだ第一ホップ用ルータが最適のルータでない場合、このホストはルータから、より最適なルータを通知するICMP Redirect (ICMPリダイレクト)を受信します。

9. ルーティングプロトコル

本製品は、静的/動的ルーティングの両方に対応しています。

静的ルーティングでは、ルーティング情報を本製品内に保存する必要があります。これは1)手動設定で行えるほか、2)本製品外部のアプリケーションで接続がセットアップされた際に保存することも可能です。

動的ルーティングはルーティングプロトコルを使って1)ルーティング情報の交換および2)ルーティングテーブルの計算を行うほか、3)ネットワークの状態や負荷の変化にも対応します。

- ・ルーティングプロトコルの処理
- ・ルーティングテーブルの更新
- ・レイヤ3スイッチングデータベースの更新

本製品はRIP、RIP-2およびOSPFv2動的ルーティングプロトコルをサポートしています。

10. RIP/RIP-2動的ルーティングプロトコル

RIPプロトコルは最も広く使用されているルーティングプロトコルです。RIPプロトコルはルーティングを行う際、距離ベクターベース(distance vector-based)の方法を使用します。ルートは、距離ベクターやホップカウントを最小化する方向で決定されます。ホップカウントは、送信コストのたまかな予測手段として利用されています。各ルータは、そのルーティングテーブルの更新情報と一緒に各々の情報を30秒ごとにブロードキャストします。この結果ネットワーク上のすべてのルータにおいて、次ホップへのリンクを示す、(ルータ間で互いに)矛盾しないテーブルを学習することが可能となります。これは最終的に、各サブネットの最適化につながります。

レイヤ2スイッチがスパニングツリーアルゴリズムを使ってループ発生を防いでいるように、ルータもまた、データトラフィックを無限に再送信させてしまうループを阻止するための手段を持っています。RIPでは、以下の3つのループ予防法が使用されています。

「Split horizon (スプリット・ホライゾン)」

ルートを最初に取得したポートインターフェースに対し、そのルートを伝播しなくなります。

「Poison reverse (ポイズン・リバース)」

ルートを最初に取得したポートインターフェースに対しそのルートを伝播しますが、距離ベクター・メトリックを無限大に設定します(最適経路の検出がより高速になります)。

「Triggered updates (トリガ更新)」

ルートが変更されると、ランダムに決定される短時間のディレイのあと更新メッセージをブロードキャストします。ブロードキャストは、定期的なサイクルを待たずに行われます。

RIP-2とRIPは互換性があります。RIP-2は1)通常テキストでの認証、2)複数の独立RIPドメイン、3)可変長のサブネットマスク、4)経路アドバタイズメントのマルチキャスト送信(RFC 1388)を含む便利な機能を提供します。

ご利用ネットワーク上でRIP及びRIP2いずれかの使用を決める前に、それぞれの持ついくつかの特長を確認する必要があります。まずRIP(バージョン1)ではサブネットの概念そのものが利用できず、両RIPバージョンにおいても、リンクやルータの不良が発生するとその間ルーティンググループが発生する可能性があるため新しいルートを検出するまで長時間かかる恐れがあります。またホップカウントも15までとなっているため、利用は小規模ネットワークに限定されます。さらに、RIP(バージョン1)はルーティング情報をブロードキャストするため貴重なネットワーク帯域幅が無駄に消費されてしまいます。同様にRIP(バージョン1)では、ネットワーク上の各パラメータを十分考慮して最適なルーティング(経路)を決定する、ということもありません。

11. OSPFv2 動的ルーティングプロトコル

OSPFではリンクステート・ルーティングプロトコルを使って最短経路のツリーを作成し、自身のルーティングテーブルをこのツリーに基づいて作成します。OSPFは、参加ルータがネットワーク上の変化をほぼ見越してこれに対応するか、もしくはその発生と同時にその対処にあたるため、RIPより素早く最適経路を検出することができます。さらに一つの送信先に対し、同一コストの経路が複数存在する場合でも、これら複数の経路間で平等にトラフィックを配分することも可能です。

OSPFは単純にホップカウントのみ監視するわけではありません。いずれかのノードへの最短経路をツリーに追加する際、遅延、スループットおよび接続性をもとに最適経路が選ばれます。OSPFはIPマルチキャストを使って、ルーティングパスの更新情報の送受信時に必要なルーティングトラフィックの量を削減します。OSPFで採用しているルーティングエリアを分離する方式はルーティングトラフィック量をさらに減らすほか、これ自体、別レベルのルーティング保護手段として機能します。さらに、OSPFアルゴリズムはTCP/IPインターネット上で効率良く動作するように調整されています。

OSPFv2はOSPFと互換性があります。OSPFv2ではプロトコルメッセージ認証が改良されているほか、OSPFを非ブロードキャストネットワーク上で使用するためのポイント・ツー・マルチポイントインターフェースが追加されています。さらにOSPFv2は重複するエリア範囲にも対応するようになりました。

12. 非IPプロトコル・ルーティング

本製品はIPルーティングのみ対応しています。このためIPXやAppletalkなどの非IPプロトコルは本製品上でルートすることは出来ず、別途ルータでブリッジしない限り、これらのプロトコルを使った通信は各々のローカルVLANグループ内に限定されます。

非IPプロトコルサブネットワークをマルチレイヤスイッチ上に構築されたネットワークと共存させる場合、前者には、IPサブネットワークに適用されるものと同じ論理制限を守る必要があります。この条件を満たして初めて、別途マルチプロトコルレイヤを使ってこれらのサブネットワークとリンクすることが可能となります。この場合、ネットワーク上で使用可能な各VLANのいずれか一つのポートをサブネットに接続する必要があります。

13. VLAN

スイッチは元々ブロードキャストドメインを想定して製造されていないため、IPXやNetBEUIトラフィックを扱う大規模ネットワークではブロードキャスト・ストームが発生する恐れがあります。従来のルータを使ったネットワークでは、ブロードキャスト・トラフィックを別々のドメインに分け、このトラフィックを発信元のグループに制限することによりネットワーク環境を整理していました。従来の低速なルータでリンクされた、これらの物理的に分けられたサブネットを使用する代わりに、本製品は簡単に設定が可能なVLANを使って別々のブロードキャストドメインを作成し、これらのVLANを必要に応じて回線速度ルーティングにリンクします。

IEEE802.1Q準拠VLANとは複数のポートをひとまとめに集めたものを指し、これらのポートはネットワーク上のどこに存在するものでもかまいません。またこれらのポートは、あたかも同一の物理セグメント上に存在するかのように通信を行うことができます。VLANはネットワーク管理をより簡単にします。例えば、機器を新しいVLANに追加する場合も、物理的に接続を変更する必要はありません。VLANは「マーケティング用」また「技術開発部用」といったように組織の各部署ごとに作成できるほか、用途別グループ（例：e-mail）やマルチキャストグループ（ビデオ会議などのマルチメディアアプリケーションで使用）ごとに作成することも可能です。

VLANはブロードキャストトラフィックを削減してネットワーク効率を向上させるほか、これを使用することにより、IPアドレスやIPサブネットを更新しなくともネットワークにて変更を加えられるようになります。またVLANでは、トラフィックはあらかじめ設定されたレイヤ3リンクを通過しなければ他のVLANに到達できないようになっているため、VLANは元々高度なネットワークセキュリティ機能を備えていると言えます。

本製品は以下のVLAN機能に対応しています。

- ・ IEEE802.1Q規格に準拠したVLANを最大256グループまでサポート
- ・ 直接/間接タギングおよびGVRPプロトコルを使用し、複数スイッチ間での分散式VLAN学習を実現
- ・ ポート・オーバーラッピング：単一ポートから複数VLANに参加可能（マルチレイヤモードでは非対応）
- ・ エンドステーションは複数のVLANに所属可能

- ・ VLAN対応機器とVLAN非対応機器間のトラフィック移動
- ・ プライオリティ・タギング

14. VLANへのポート割り当て

VLANを本製品上で有効にする前に、まず各ポートを参加したいVLANグループに割り当てる必要があります。デフォルトでは全ポートともVLAN 1にタグ無しポートとして設定されています。ポート上で一つまたは複数のVLAN行きのトラフィックを扱う場合で、かつリンクの反対側の機器もVLANに対応している場合は、ポートをタグ付ポート(VLAN対応機器に接続されたポート)として追加してください。次に、リンクの反対側のポートに対し同じVLANを割り当ててください。ただし、本製品上のポートが一つまたは複数のVLANに参加する場合で、リンクの反対側の機器がVLANに対応していない場合、このポートはタグ無しポート(VLAN非対応機器に接続されたポート)として追加する必要があります。

VLANの分類

本製品は、フレーム受信時にこれを二種類いずれかのVLANに分類します。フレームがタグ無しの場合、本製品はフレームを関連付けられたVLANに割り当てます。逆にフレームがタグ付である場合、本製品はそのタグ上のVLAN IDを使って、フレームのポート・ブロードキャストドメインを確認します。

15. ポート・オーバーラッピング

ポートオーバーラッピングを使用することにより、よく共有されるネットワークリソース(例：ファイルサーバ、プリンターなど)を複数のVLANグループ間で共有することが可能となります。(マルチレイヤモードでは非対応) オーバーラップしないVLANを設定し、これらの中で通信を行わせる場合は、本製品をまずマルチレイヤモードに設定し、別のVLANへのIPインターフェースアドレスを設定します。

16. ポートベースVLAN

ポートベースVLANは、特定ポートに対し手動で設定されます。本製品は、送信先MACアドレスおよび関連づけられたポートをもとに転送の決定を行います。この理由上、本製品が有効な転送/フラッドの決定を行うためには、本製品はMACアドレスとその関連ポート(およびVLAN)との関係を実行時に学習する必要があります。GVRPが有効となっている場合、この処理はすべて自動的に行われます。

17. 自動VLAN登録（GVRP）

GVRPは、各エンドステーションに割り当てるVLANを本製品が自動的に学習できるシステムを構築します。エンドステーション（またはそのネットワークアダプタ）がIEEE802.1Q VLANプロトコルに対応している場合、そのエンドステーションは、自身が参加したいVLANグループを示すメッセージをネットワークに対しブロードキャストするよう設定することが可能です。本製品はこのメッセージを受信すると、自動的に受信ポートを指定VLANに設定し、同メッセージを他のすべてのポートに転送します。他のGVRP対応スイッチにこのメッセージが届くと、そのスイッチもまた、受信ポートを指定VLANに設定し、同メッセージを他のすべてのポートに転送します。VLAN上の各要求条件は、このようにしてネットワーク中に伝播します。この方法では、エンドステーションからの要求を受信するだけでGVRP対応機器を自動的にVLANグループに設定することが可能です。

18. タグ付/タグ無しフレームの転送

ポートは、複数のタグ付またはタグ無しVLANに割り当てられるようになっています。このため、本製品上の各ポートはタグ付およびタグ無しフレームを送ることが可能です。フレームをVLAN対応機器からVLAN非対応機器に転送する場合、本製品はまずフレームをどこに転送するかを決定し、その上でVLANタグを取り外します。ただしフレームをVLAN非対応機器からVLAN対応機器に転送する場合、本製品はフレームの転送先を決定したあと、ポートのデフォルトVIDを示すVLANタグを挿入します。デフォルトPVIDは全ポートともVLAN 1となっていますが、この設定を変更することも可能です。

19. VLANグループの接続

本製品はハードウェアベースのストア&フォワードスイッチングを使用し、同一VLAN内での通信を可能としています。ただし、個別のVLAN間で通信を行う必要があり、また通信する機器をすべて共通のVLANに入れることが難しい場合は、本製品のレイヤ3ルーティングを使って異なるVLAN同士を接続することができます。

従来のルータはルーティングテーブル内で物理ポート番号のみ使用するため、VLANには対応していません。これと対照的に、本製品は論理ポート番号と物理ポート番号の両方を使ったレイヤ3ルーティングをサポートしており、VLANとレイヤ3スイッチングを両者同時に実行することが可能となっています。

同一VLAN内の物理スイッチポートの集まりを、論理ポート番号から抽出したもので表すことにより、一つのVLANと他のVLANとの間でレイヤ3スイッチングを行うことが可能です。レイヤ3スイッチングは、ルーティングプロトコル、IPルーティングソフトウェアのどちらも変更しないためその存在をユーザーに意識されることもありません。一方、レイヤ2スイッチングは現在もVLAN内部のトラフィックで使用されています。

本製品は、RIPやOSPFといった、静的設定プロトコルや動的ルーティングプロトコルで構築された標準のルーティングテーブルを使用します。各ルーティングエントリはネットワークアドレス (IPアドレス + サブネットマスク) および仮想インターフェース番号 (virtual interface number) により構成されます。各仮想インターフェースはそれぞれVLANに対応しているほか、VLAN IDにより識別されます。またさらに、同一仮想インターフェースに対し複数のルーティングエントリを設定することも可能となっております。これは、同一仮想インターフェースに対し希望のルーティングテーブル・エントリを追加することで可能となります。以下に、ルーティング対応VLANの簡単な設定例を示します。

| | |
|-------------------|--------------|
| Network | : ネットワーク |
| Virtual Interface | : 仮想インターフェース |
| Routing Table | : ルーティングテーブル |
| PVID Table | : PVIDテーブル |

20. マルチキャストフィルタリング

マルチキャストイングでは、単一の送信先の代わりに、一グループのノードに対してデータを送信します。最も簡単なマルチキャストイング例は、ネットワーク上の全ポートに対してデータをブロードキャストすることでしょう。しかし送信先グループがブロードキャストドメイン全体から見て小さい場合、この方法では多くの帯域幅を無駄にってしまうことになります。

ビデオ会議やデータ共有が一般的になった今、効率的なマルチキャストイングは必須となっています。よく利用される方法としては、グループ登録プロトコル(Group Registration Protocol)の使用が挙げられます。グループ登録プロトコルは、ノードのマルチキャストグループへの参加およびそこからの撤退を可能にします。スイッチまたはルータは、この時点でどのポートがグループメンバーを持っているかを簡単に割り出し、データをこれらのポートにのみ送信します。この一連の処理はマルチキャスト・フィルタリングと呼ばれています。

IPマルチキャストフィルタリングの使用目的はスイッチネットワーク上のパフォーマンスを最適化することにあります。このためマルチキャストパケットは、サブネット(VLAN)上の全ポートにすべて送信する代わりに、マルチキャストホスト/マルチキャストルータ/スイッチを含むポートにのみ転送されます。

本製品でサポートしているIPマルチキャストフィルタリングは、受動的にIGMPクエリー、ReportメッセージおよびDVMRP Probeメッセージを監視してエンドステーションをマルチキャストグループメンバー(レイヤ2)として登録するだけでなく、積極的にGMRPクエリーメッセージを送信して、各VLAN内部のマルチキャストグループ内のマルチキャストルータ/スイッチおよびメンバーホストの場所を学習します(レイヤ3)。本製品はまた、マルチキャストトラフィックを他のサブネットに転送するのに必要なDVMRPマルチキャスト・ルーティングプロトコルをサポートしています。

21. IGMP スヌーピング

レイヤ2スイッチは、IPマルチキャストルータ/スイッチとIPマルチキャストホストグループとの間で転送されるIGMPクエリーおよびReportパッケージを受動的にスヌープ(調査)してIPマルチキャストグループのメンバーを学習します。このときレイヤ2スイッチは自身を通過するIGMPパッケージをそのまま監視し、グループ登録(registration)情報を引き出して、これに応じてマルチキャストフィルタを設定します。IGMPスヌーピングは余分にネットワークトラフィックを発生させることもないため、ご利用スイッチを通過するマルチキャストトラフィックを著しくカットすることが可能です。

22. IGMPプロトコル

IGMP(Internet Group Management Protocol)は、ホストとその隣接したマルチキャストルータ/スイッチとの間で実行されるマルチキャストホスト登録プロトコルです。IGMPを使用することにより、ホストが指定マルチキャストグループ宛の送信内容の受信を希望している旨、どのホストからもそのローカルルータに対し通知できるようになります。

ルータおよびマルチキャスト対応スイッチでは、そのホストがマルチキャストトラフィックの受信を希望しているかどうかを定期的に確認できるようになっています。IPマルチキャストを実行しているLAN上にルータ/スイッチが複数存在する場合、これらのうち一台が「クエリア」に選ばれ、グループメンバー確認のためのクエリーをLANに送る役目を持つこととなります。クエリアは次に、隣接するいずれかのマルチキャストスイッチ/ルータにサービス要求を伝播して、自身が今後も常にマルチキャストサービスを受信できるようにします。

IGMPで学習したグループメンバーシップ情報をもとに、ルータ/スイッチは、どのマルチキャストトラフィックを(これが存在する場合)その各ポートに転送すべきかを決定します。レイヤ3では、マルチキャストルータはDVMRPなどのマルチキャストルーティングプロトコルと一緒にこの情報を使って、インターネット上でIPマルチキャストを実現します。

なお、IGMPはIPマルチキャストパケットの変更およびルートは行いませんのでご注意ください。異なる複数のサブネットワークを通してIPマルチキャストパケットを送信する場合はマルチキャストルーティングプロトコルが必要となります。このためDVMRPルーティングが本製品上のサブネットで有効になると、本製品は自動的にIGMPを有効にします。

23. GMRPプロトコル

GMRP(GARP Multicast Registration Protocol)を使用することにより、ネットワーク機器側でエンドステーションをマルチキャストグループに登録することが可能となります。GMRPを使用する場合、参加するどのネットワーク機器およびエンドステーションもIEEE802.1p規格に準拠している必要があります。当規格に準拠したエンドステーションは、既知のマルチキャストアドレスを入れたjoinパケットを発信するだけで、マルチキャストグループからトラフィックを受信するよう要求することができます。Joinパケットが本製品上のポートに届くと、joinパケットは、要求されたグループのマルチキャストトラフィックを受信するようこのポートを設定します。次に同様のjoinパケットを本製品上の残りすべてのポートに対して送信し、これらのポートに対し、指定グループ用の受信マルチキャストトラフィックが、要求を行ったポートに転送される旨をそれぞれ通知します。

24. DVMRPルーティングプロトコル

DVMRP(Distance-Vector Multicast Routing Protocol)の動作はRIPといくらか似ています。DVMRP対応ルータは、自身に接続されているネットワークに対し定期的にフラッドを行い、対応しているマルチキャストサービスについての情報を新しいルータおよびホストに連絡します。DVMRPパケットを受信したルータは、送信元に返ってくる経路を除いた全経路に対し、そのコピーを送信します。特定マルチキャストグループからのトラフィック受信を希望しないLANにルータが接続されている場合、これらのルータは次にpruneメッセージを送信元に送ってデータストリームそのものを停止します。ただし、このルーティングスイッチに接続されているホストがIGMPメッセージを送信し、問題のマルチキャストサービスを希望している旨を明らかにした場合、このスイッチはDVMRPを使って送信元をルートとしたマルチキャスト配信ツリーを作成します。このツリーをもとに本製品はマルチキャストトラフィックの送信元までの最短経路を割り出すほか、ループもこれで防止します。

このスイッチがマルチキャストメッセージを受信すると、スイッチはそのユニキャストルーティングテーブルを参照し、送信元までの最短経路を提供するポートを探します。この経路が、マルチキャストメッセージの受信に使用したものと同一ポートを通過する場合、このスイッチは該当マルチキャストグループまでの経路情報をそのルーティングテーブルに記録し、マルチキャストメッセージを隣接するルータに転送します(ただしメッセージ受信に使用したポートは除きます)。この処理は、ツリー上で発生し得るループをすべて除去するほか、いつも最短経路(ホップカウント単位)が使用されることを保証します。

25. CoS(Class-of-Service)サポート

本製品は各ポートで、Weighted Fair Queuing方式に対応した二つの送信キューを提供します。この機能を使用することにより、リアルタイムの動画/音声送信やベスト・エフォートデータなど、様々な種類のデータに対し個別に優先順位(プライオリティ)を設定することが可能となります。

本製品内のパケットには、以下のどの方法でもプライオリティを割り当てることができます。

ベストエフォート型よりプライオリティの高いアプリケーションを備えたエンドステーションにより、直接プライオリティを割り当てることができます。本製品ではIEEE802.1pおよび802.1Qタグ構造を使って、受信パケットのプライオリティ割り当てを決定しています。

ポートは手動でプライオリティを高く設定することができます。この場合、いずれかのポートがプライオリティの高いポートからトラフィックを受信すると、トラフィックは自動的に高プライオリティ出力キューに渡されます。

26. セキュリティ機能

本製品には、管理アクセスおよびネットワークアクセスを制限するためのセキュリティ機能がいくつか搭載されています。以下に各機能の詳細を説明します。

27. SNMPコミュニティストリング

ネットワーク管理ツール(例: HP OpenViewなど)を使った本製品へのアクセスは、SNMPコミュニティストリングにより制限されています。本製品は、最大5つまでのコミュニティストリングをサポートします。本製品にSNMPメッセージを送信する際は、必ず管理コミュニティへのアクセス権を示す文字列を提示する必要があります。各コミュニティはリードオンリー(読み取り専用)またはリード/ライト(読み書き可能)アクセス権を持っています。リードオンリーアクセスのみを持つコミュニティでは、現在の設定内容およびスイッチの状態を表示するためのGETおよびGET-NEXTコマンドしか使用できません。一方、リード/ライトアクセスを持つコミュニティでは、GET、GETNEXTの両コマンドに加え、本製品を設定するためのSETコマンドも使用可能となります。

28. ユーザー名およびパスワード

本製品はコンソールポートに直接接続された端末からアクセス可能であるほか、TelnetまたはWebブラウザを使ってネットワーク経由でも接続できるようになっています。本製品をこれらいずれかの手段で管理する場合は、システムと接続する際にユーザー名とパスワードの入力が必要となります。ユーザー名とパスワードはそれぞれ二種類用意されています。このうち一つは管理者権限を持つもので、システムパラメータの参照および変更が行えます。もう一方はリードオンリーアクセス権限を持っており、システム状態を参照できますがその変更は行えません。

29. MAC アドレスフィルタ

セキュリティ上問題となりうるデータや、ネットワークに悪影響をもたらす可能性のある異常または悪質なデータがいずれかのポートから送信されていることが判明した場合は、このポートのMACアドレスを本製品上でフィルタするよう設定することが可能です。送信先/送信元アドレスがMACアドレスフィルタに登録されているパケットは、着信時に本製品上で破棄されます。

30. IPアドレスフィルタ

IPアドレスも、同様に本製品上でフィルタすることが可能です。送信先/送信元アドレスがIPアドレスフィルタに登録されているIPパケットは、着信時に本製品上で破棄されます。

31. SNMP管理ソフトウェア

SNMP(Simple Network Management Protocol)は、ネットワーク上の管理機器などを管理するために特別に設計された通信プロトコルです。SNMPが通常管理を行うネットワーク機器にはハブ、スイッチ、ブリッジ、ルータおよびホストコンピュータが含まれます。SNMPは主に、これらの機器がネットワーク環境内で正しく動作するよう設定を行うほか、機器を監視してそれぞれの性能を評価し、また何か問題が発生していないか確認も行います。

32. リモート監視(RMON)

ネットワーク中に分布しているネットワーク機器(例：ハブ、スイッチ、ルータなど)に埋込式または外部プローブを使用することにより、RMONは、コスト効率の高い方法で大規模ネットワークを監視することが可能です。ネットワーク管理ソフトウェアはネットワーク機器に埋め込まれているプローブにアクセスしてトラフィック解析、ネットワーク上のトラブル解決および過去の傾向分析を行うほか、積極的に管理ポリシーを実行します。数百にも達する独立セグメントを備え、かつ急速に変化するネットワーク環境を相手にするネットワーク管理者たちにとり、RMONは既に有益なツールとして重宝されています。RMONは、ネットワークの制御を行いつつ、毎秒メガビット単位で動作するアプリケーションを解析することが可能な唯一の方法となっています。またRMONはリアルタイムで重要な統計情報にアクセスすることにより、ネットワーク運転を維持するための反応型および積極的なポリシーを実行する際に必要なツールを提供します。

本製品は、「ミニRMON」に対応しています。ミニRMONは、基本的なりモート監視を行うのに必要な4つのキー・グループを備えています。以下に各グループについて説明します。

「Statistics」

ネットワーク上の一般的なエラーおよび全体のトラフィック速度を監視するのに必要なすべてのツールを備えています。表示する情報には、帯域幅の利用状況、最大利用度、パケットの種類、エラー、コリジョンおよびパケットサイズの分布などが含まれます。

「History」

ネットワーク利用、パケットタイプ、エラーおよびコリジョンの記録を作成します。断続的に発生する問題を分析するには、(ネットワーク上の)動作の過去の記録が必要となります。履歴データはまた、ネットワーク上の動作の通常/基準レベルを割り出す際に使用されます。基準値を割り出すことにより、多大なトラフィック量やブロードキャストストーム、また他の希なイベントなどに関連した問題を検出できる場合があります。さらに履歴情報を使ってネットワーク成長を事前に予測し、ネットワーク上の負担が大きくなりすぎる前に拡張を計画することも可能です。

「Alarms」

指定した時間間隔でデータをテストしたり、絶対値または変化値の監視を行うよう設定することが可能です(例: 特定の値に達するよう設定された統計カウンタや、指定時間内で一定量の変化を追う統計など)。

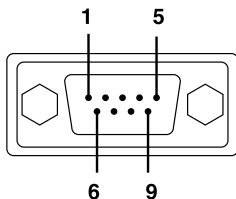
「Events」

アラーム(alarm)が発動した際に実行する動作を設定します。アラーム発動に対する行動には、1)Log Tableへのアラーム発生記録や、2)トラップマネージャへのメッセージ送信などが含まれます。なお重要イベントを記録する場合や重大なネットワーク上の問題に即座に対応する場合は、AlarmとEvent Groupsは一緒に使用するようになっています。

付録A. RS232Cのピンアサイン

シリアルRS-232コネクタのピンアサイン

シリアルRS-232コネクタは9ピンメスD-Subコネクタとなっています。また表B-1はピンアサインを示しています。DSRとCTSの各信号出力端子は互いに接続されません。また、CD、DTR、RTSおよびRI信号入力端子は使用されていません。当コネクタは、管理ステーション(PCまたは端末)側から直接ストレートケーブルを使って本製品に接続できるようになっています。



図B-3 DB-9 サービスポート・コネクタ

| FML-24側 D-sub9ピンオス | コンピュータ側 D-sub9ピンメス |
|-----------------------|-----------------------|
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |
| 8 | 8 |
| 9 | 9 |

表B-1 シリアルケーブルのピンアサイン

付録B. 製品仕様

< 最大ポート数 >

24

< ポート (100BASE-TX) >

24

< ポート (1000BASE-SX拡張用) >

最大1ポートまで拡張可能

< オートネゴシエーション (NWAY) >

全ポート

< LED/インディケータ >

Link, Status, Trunk, Col.Act, FDX, 100M, Utilization%, Port, L2,
ML, Power, RPU, FAN, SNMP, Console

< スイッチング方式 >

ストア・アンド・フォワード

< スイッチングバス速度 >

8.52Gbps

< フィルタ速度 >

各ポートとも148,800パケット/秒

< パケットバッファ容量 >

4MByte

- <フローコントロール (半二重) >
バックプレッシャー
- <フローコントロール (全二重) >
IEEE 802.3x
- <スイッチングデータベース >
MACアドレス32K IPアドレス64K
- <最大VLANグループ数 >
256個までのポートベースVLANを構築可
- <プライオリティ対応 >
2-Level (IEEE 802.1p準拠)
- <SNMP >
MIBII/RMON MIB/RIP2MIB/PrivateMIB
- <RMON >
1、2、3、9(Statistics,History,Alarm,Event)
- <スパニングツリー >
IEEE 802.1d
- <ネットワーク管理 >
VT100、Telnet、WebベースNMS
- <ファームウェア更新 >
TFTP
- <寸法 (W×D×H) >
440 x 285 x 64 mm

< 重量 >

5.1kg

< 消費電力 >

80W

< 動作温度 >

0 ~ 45

< 動作湿度 >

35 ~ 80%(結露しないこと)

< 入力電圧 >

100 ~ 240VAC

< 入力周波数 >

50 ~ 60Hz

< EMI >

FCC Class A, CE, VCCI class A

付録C.用語集

「ブリッジ」

二つ以上のLANを接続するための機器です。MAC(メディアアクセスコントロール)レイヤー2で動作し、異なるLAN間でデータパケットの確認および転送を行います。ほとんどのブリッジがCPUとソフトウェアを使ってデータのチェックおよび転送機能を行っています。

「ハブ」

スター型ネットワークポート内の中心に位置する機器で、信号を増幅または再送することによりネットワークを延長したり、より多くのPCと接続してネットワークを拡張したりします。例えば、一般的にハブは8、12もしくは16個のRJ-45ポートを備えており、その各ポートをPCやワークステーション、またサーバと接続します。またハブのBNCポートを同軸ケーブルと接続することによりネットワークの延長が可能になります。

「JAVA」

クライアント-サーバのプログラミング分野上の問題を解決するため作成されたインターネット上でのプログラムに最適なネットワークプログラム言語です。Javaセキュリティ機能は、Netscape Communicator 4.5以降、またMicrosoft Explorer 4.0以降といった最新のブラウザに組み込まれています。

「JAVAベースのネットワーク管理システム」

JAVAアプレットを使用したネットワーク管理機能です。ネットワーク管理ソフトウェアはJAVA言語で作成され、ネットワーク機器(ハブ、LANスイッチ等)内に格納されています。ユーザはWebブラウザでネットワークを管理することが可能でWebサーバをブラウズする感覚で簡単にネットワーク管理を行う事が出来ます。

「ネットワークインターフェースカード(NIC)」

他のPCとの通信用として、各ネットワークステーション(PC、ワークステーション、サーバ)本体内にインストールされている回路基盤です。使用するコンピュータによって、NICのバスはISA、PCI、EISA、MCA、S-バスなど様々な種類が存在します。

「ネットワーク管理」

ネットワークを制御し機能を管理することです。ネットワーク管理は、1：耐故障管理、2：ユーザーアカウント管理、3：設定管理、4：性能の維持・管理、および5：セキュリティ管理のすべてを実行出来なければいけません。

「RIP」

RIPは内部ゲートウェイプロトコル(Interior Gateway Protocol = IGP)とも呼ばれるルーティングプロトコルで、ただ一人の管理者や技術者により制御される独立ネットワーク(autonomous network)などで使用されます。

「RMON」

ネットワークの性能、エラーおよび他のサマリー情報などを監視する機能です。RMON機能はネットワーク機器(ハブ、LANスイッチ等)やPCなどのステーションに対して実行できるようになっています。

「ルータ」

ネットワークレイヤー(レイヤー3)で動作する機器で、類似した、もしくは異なるネットワーク間のデータをルーティングします。ルータはネットワークプロトコルとアドレス(IP、IPX)を認識する事が出来るため、ブリッジやLANスイッチと比べ高性能になっています。

「SNMP」

インターネットおよびUPP/IPベースのネットワークの管理を行うための標準プロトコルです。

「Telnet」

端末とホストマシン間で汎用の双方向通信を提供します。端末上の操作でホストマシンにアクセスし作業が行えるため、端末側では、ローカルで作業を行っている場合と同様の操作が可能です。

「VLAN」

ブリッジの(物理的)インフラストラクチャー内で、各ステーション(PC)の論理的グループ化を行います。VLANはブロードキャストドメインを制限することが可能でVLANによるPCのグループ化は物理的にハードウェア上の制限を受けないため、簡単にダイナミックなネットワーク構築を行う事が出来ます。

「ブロードキャスト」

全てのネットワーク機器に対して同時に同じデータを転送する方式です。

付録D. 出荷時設定

< IPアドレス >

192.168.1.254/24

< ポート状態 >

全てのポートが使用可能

< オートネゴシエーション >

ON

< ユーザアカウント >

admin(パスワードは、設定されていません。)

< コンソールポート初期設定 >

19200bps、8ビット、ストップビット1、パリティチェック無し、
フロー制御無し

< HTTPサーバ >

ON

< SNMP >

有効

< SNMPリードコミュニティネーム >

public private

< SNMPライトコミュニティネーム >

public

< RMON統計機能 >

全てのポートで可能

<VLAN機能>

デフォルトで一つのVLANグループが作成されています。全てのポートは、デフォルトのVLANグループに所属しています。

<802.1Qタグ>

デフォルトのVLANグループ上の全てのパケットには、タグは付加されません。

<802.1P優先順位>

優先設定されたタグが付加してあるパケットを受け取った場合は、自動的に認識します。

<スパニングツリープロトコル機能>

有効

<フォワーディングデータベースのエージング時間>

300秒

<フローコントロール>

全てのポートで使用しない。

<Telnet サーバ>

ON