24ポート 10M/100M レイヤ3 インテリジェントスイッチングハブ

FML-24NX

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！

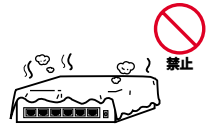
雷が発生している間は、製品各部およびケーブルにさわらないでください。感電するおそれがあります。

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

《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.1.1　Rev.A

No.PCM-01-10-JF-FML-24NX

1.はじめに

1. 概要

FML-24NXはIEEE802.3 10BASE-T, 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・インテリジェント・スイッチです。ASICによるワイヤースピード、IPルーティング機能を可能にし、RIP1、2及びOSPFに対応しています。
Autonegotiation及びAutoMDIに対応したRJ-45 STPポートを24ポートと1ポートのIEEE802.3z 1000BASE-SX/LX、IEEE802.3ab 1000BASE-Tモジュールがインストール可能な拡張スロットを2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、RS-232Cコンソールなどにより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/LX、1000BASE-Tオプションモジュール用拡張用スロットを2スロット装備
●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
●AutoMDI機能によりケーブルの結線タイプ（ストレート、クロス）を自動認識
●合計9.6Gbps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
●IPアドレステーブルを装備し、最高64KのIPアドレスを自動学習可能
●最大26個のIPサブネットを作成可能
●4MByteのパケットバッファを装備
●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
●IEEE802.1QVLANに準拠（Layer2 node時 256グループ、Multilayer mode時 26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、DVMRPマルチキャストプロトコルに対応
●RIP，RIP-2，OSPF-V2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、EthernetMAU、Bridge、Private、RIP2 MIB、IP Forwarding Table、OSPF、IGMP、DVMRP、IP Multicast Router MIBに対応
●Statistics、History、Alarm、Eventの4グループのRMONに対応
●TFTPサーバによるファームウェアのアップデートが可能
●TFTPクライアントによる設定ファイルのアップロード及びダウンロードが可能
●MAC及びIPアドレスフィルタリングに対応
●ネットワーク管理用のRS-232Cコンソールポート（D-SUB25ピン）を装備
●冗長化電源に対応

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-24NX本体
●設定用RS-232C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
●このユーザーズ・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

■前面パネル

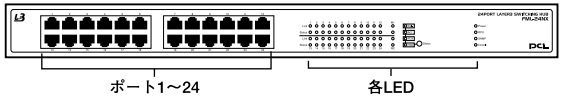


図1-1 前面パネル

「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。

「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。

「Power LED」
ハブに電源が入ると点灯します。

「RPU LED」
本製品に接続された冗長化電源から動作電源が供給されている場合に点灯します。

「SNMP LED」
本製品にSNMPでアクセスしている場合に点灯します。

「Console LED」
シリアルポートから本製品コンソールへアクセスしている場合は点灯します。

■背面パネル

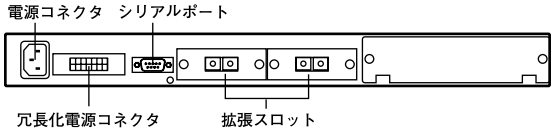


図1-2 背面パネル

「拡張スロット1、2」
1000BASE-SX/LX、1000BASE-T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RS-232C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。

「冗長化電源コネクタ」
冗長化電源ユニットを接続します。

■裏面ステッカー

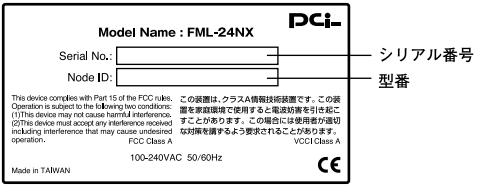


図1-3 裏面ステッカー

「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になります。

2.クイックインストレーション

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-24NXのインストールの概要は、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、ハブおよびスイッチと接続する。

1. 設置場所について

ハブを設置する際には必ず以下の点をお守りくださいますようお願いします。

●湿気の多い場所に設置しないでください。
●チリやほこりの多い場所には設置しないでください。
●直射日光のあたる場所や温度の高い場所には設置しないでください。
●内部に熱がこもる原因となりますので、周囲にはなるべく空間を空けてください。

注意　本体側面の通風口にほこりなどがたまると内部に熱がこもる原因となります。定期的に点検を行い、ほこりがたまっているようでしたら掃除機等でほこりを取り除くようにしてください。

2. 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。

※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。また、本製品のファン取りつけ口にほこり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。

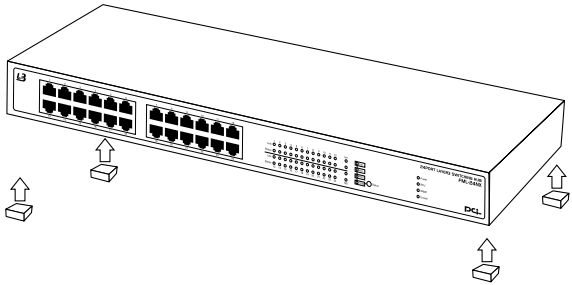


図2-1 ゴム足の取りつけ図

■ラックへの取りつけ

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けてある場合は、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. **付属のネジを使用して、ラックマウント用金具を製品側面にとりつけます。プラスのドライバをお使いください。**
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2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。**

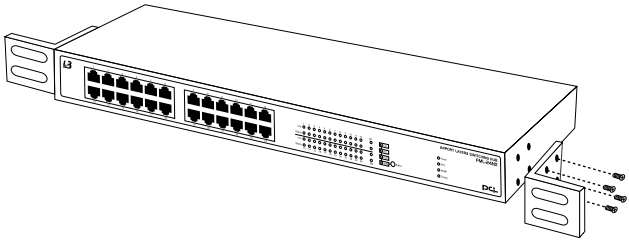


図2-2 ラックマウント用金具の取り付け

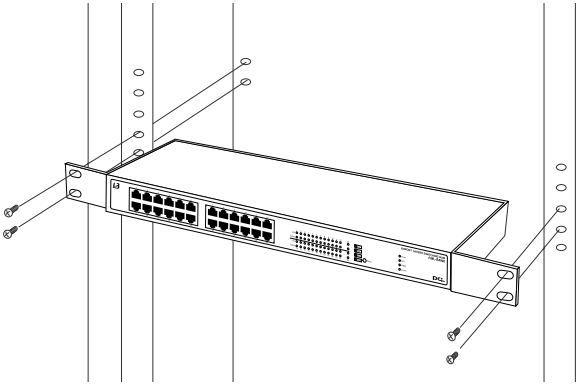


図2-3 ラックマウント用金具をラックに固定

3. 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。

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はしばらく時間がかかります。

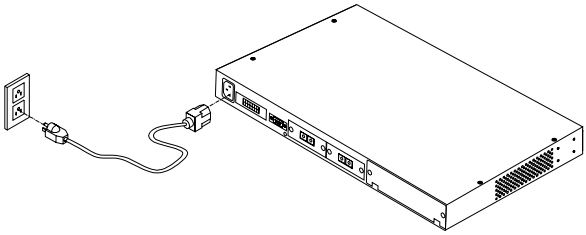


図2-4 電源ケーブルの接続方法

4. ネットワーク機器と本製品の接続

以下の手順で本製品のスイッチポートとコンピュータのLANアダプタまたはスイッチ等のネットワーク機器を通信速度に合わせたケーブルを使用して接続してください。本製品上のポートは全てAutoMDIに対応しているためケーブルの結線タイプを自動で認識することが出来ます。接続先のポートの結線に依存すること無くストレートまたはクロスケーブルのどちらでも使用可能です。

1.ケーブルの一端を本製品のRJ-45 ポートに接続してください。
2.もう一端をコンピュータまたはスイッチ等のネットワーク機器のRJ-45 ポートに接続してください。
3.接続先のポートがAutonegotiationに対応している場合はポートの転送モードが自動的に設定されます。

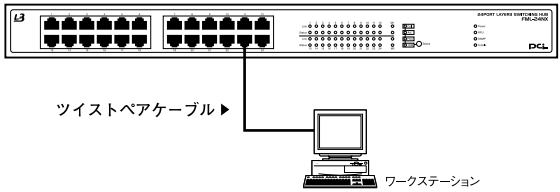


図2-5 ネットワーク機器との接続

注意　●10BASE-Tでの接続にはカテゴリ3以上、100BASE-TXの接続にはカテゴリ5のUTPまたはSTPケーブルを使用してください。ケーブルの最大長は100mです。●1000BASE-T ギガビット・イーサネットの接続にはエンハンスドカテゴリ5またはカテゴリ6のケーブルが必要です。　●1000BASE-T ギガビット・イーサネットのケーブル最大長は、IEEE 802.3ab 1000BASE-T 仕様で100mと定められています。

3.スイッチの管理

1. 設定オプション

本製品は管理エージェントを搭載しており、メニュー形式の設定プログラムを使用して本製品の設定および管理を行えるようになっています。当プログラムは、製品背面のシリアルポートから直接アクセス可能なほか、TelnetまたはWebブラウザ（対応ブラウザ：Internet Explorer 4.0以降、Netscape Navigator 4.0以降）を使用し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
- ●トランクポートの設定
- ●ネットワークVLANへのポート追加
- ●IPインターフェイスの追加
- ●IPルーティングおよびマルチキャストルーティング経路の設定
- ●システム情報および統計の表示
- ●スパニングツリーの設定
- ●システムファームウェアのダウンロード
- ●設定ファイルのアップロード及びダウンロード

2. シリアルポートとの接続

製品背面のシリアル・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出来ます。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　Windows 95/98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。ターミナルユーティリティをアップデートするか、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**
- **フロー制御なし**
- **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RS-232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オス型コネクター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でDB-9オス型コネクタが使用出来ます。）

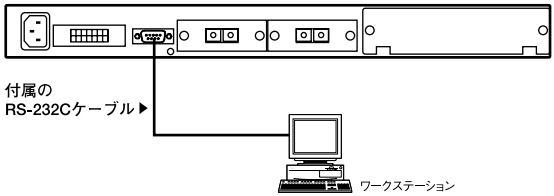


図3-1 RS-232Cケーブルとの接続

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をそれぞれ正しく設定する必要があります。
※本製品は工場出荷状態でレイヤ2モードに設定されています。

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　●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ことが可能です。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。　●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）　●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ース

コンソールインターフェー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。
本マニュアル内の各機能の説明はは全てMultilayer Mode時のメニューツリーをもとに行います。

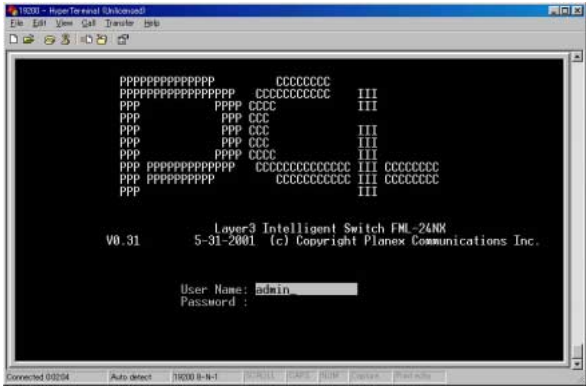
1. 基本操作

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す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）ユーザ名はデフォルトで「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）権限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）権限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。

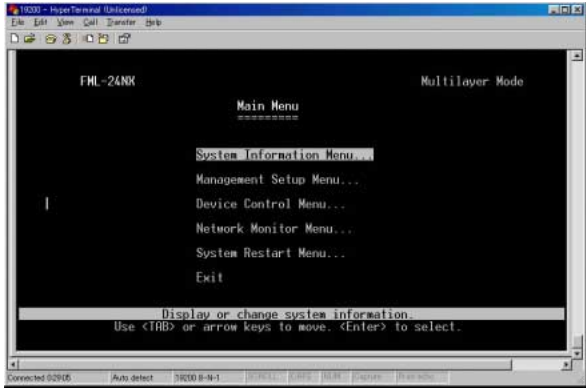
※本製品はデフォルトのユーザ名としてadmin及びguestが用意されていてそれぞれアクセス権がADMIN及びGUESTに設定されています。

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三回まで可能となっています。三度目のパスワードも間違って入力された場合、接続は自動的に切断されます。またログインスクリーン表示後、30秒の間ログインが行われなかった場合も自動的に切断されます。

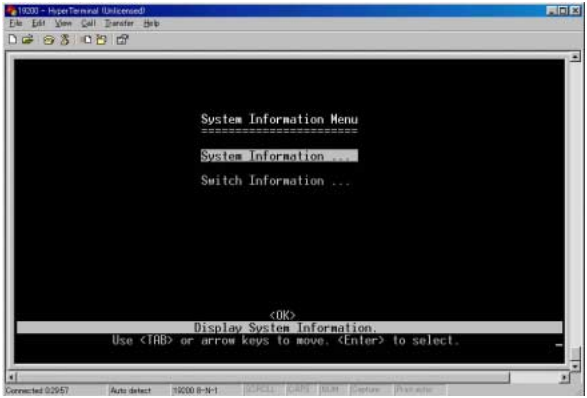
3. Main Menu

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。



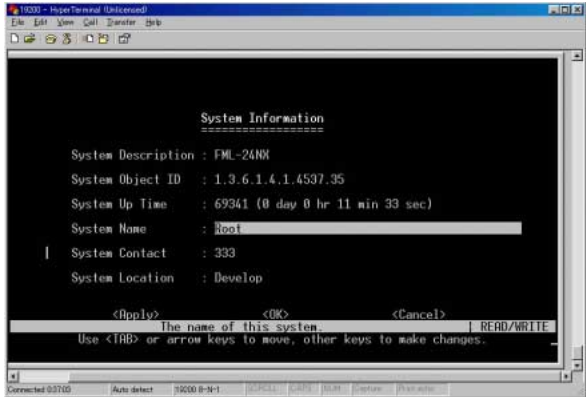
注意　●現在選択されているオプションの説明は画面一番下のハイライト部分に表示されます。　●画面上右端には、本製品がレイヤ2スイッチ/マルチレイヤールーティングスイッチのどちらのモードで動作しているかが文字列で表示されます。

■System Information Menu



◎System Information

システム監理者への連絡先やシステムの稼動時間などのシステム情報を設定及び参照する場合は System Informationを選択してください。



「System Description」

FML-24NXと表示されます。

「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の稼働時間が表示されます。

「System Name＊」

システム名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が、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の供給方法または拡張スロットへインストールされているモジュールのインターフェースタイプなどを参照して確認することが出来ます。

「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/未使用が表示されます。

「Redundant Power Status」
冗長化電源の使用/未使用が表示されます。

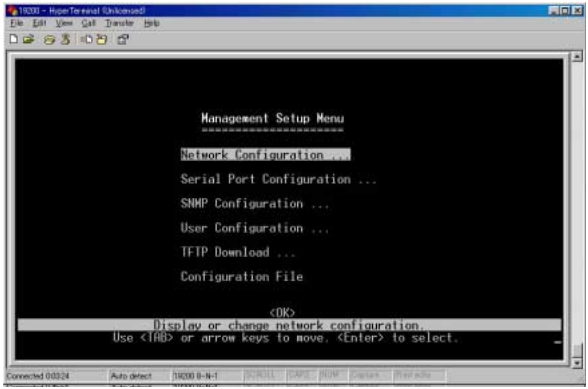
「Fan Power Status」
ファンの動作状態が表示されます。

「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が表示されます。

「Expansion Slot 2」
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が表示されます。

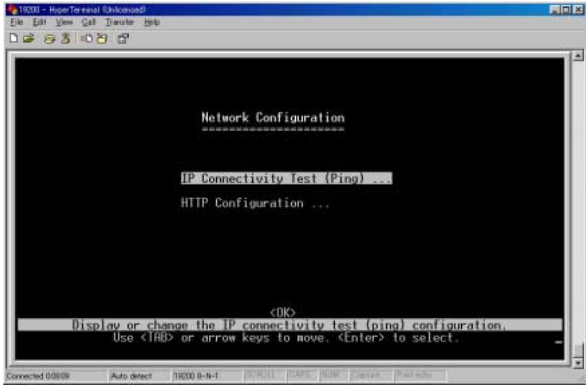
■Management Setup Menu

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（① Serial Port Configuration）。本製品用のIPアドレスを設定し（② Network Configuration / IP Configuration）、管理者およびユーザーのパスワードを設定します（③User 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。またコミュニティ名（SNMPコミュニティ名）の設定も行ってください（④SNMP 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。



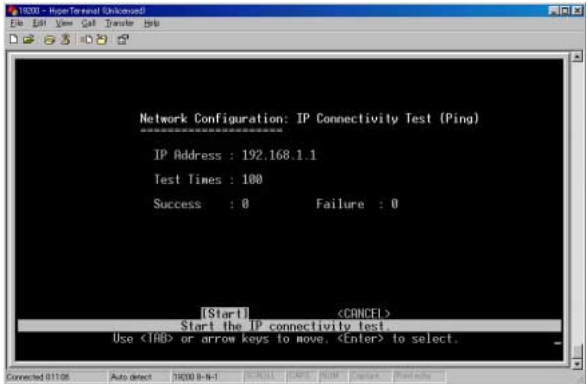
◎Network Configuration

IP設定 PING関連およびHTTP（Webエージェント）を設定します。



◎IP Connectivity Test

ネットワークのデバイスに対して本製品から接続可能か確認する場合はIP Connectivity Testを選択します。トラブルシューティング時などに有効です。



「IP Address」

Pingテストを行う相手先のIPアドレスを入力してください。

「Test Times」

指定サイトに対しICMP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。

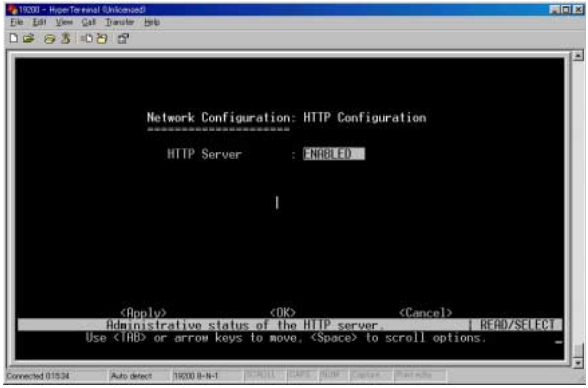
「Success/Failure」

Pingの応答（もしくは失敗）回数を示します。

注意　Pingは10秒間隔で行われます。

◎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。



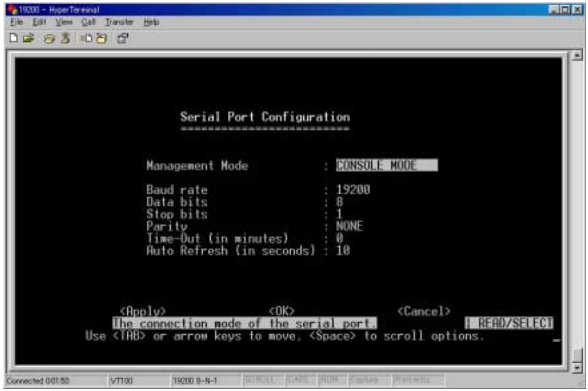
「HTTP Server」

製品上のWebエージェントへのアクセスを有効/無効に設定します。

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ターミナルユーティリティがインストールされたコンピュータを接続することで、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。(当ポートへの接続についての詳細についてはセクション 3-2「シリアルポートとの接続」をご覧ください。) 当ポートの通信パラメータは、以下のSerialPort Configurationスクリーンからアクセス可能となっています。



「Management Mode」：Console Mode

ポート設定は端末との直接接続用です。

※変更できません。

「Baud rate」 ：19200

通信時のデータ転送速度の設定を行います。9600，19200および38400のいずれかが選択可能です。工場出荷時は19200に設定されています。

「Stop bit」：1
ストップビットの設定を行います。1及び2が設定可能です。

「Data bits」：8 bits
データ長の設定を行います。7ビット及び8ビットが選択可能です。

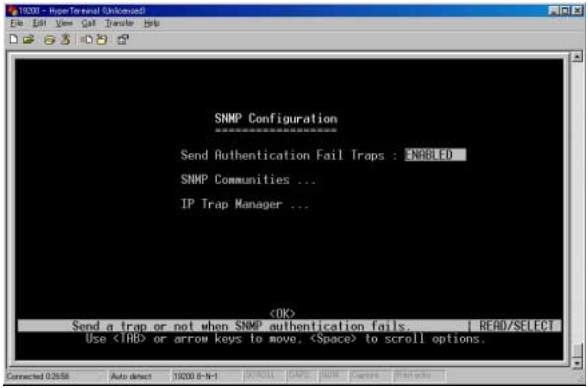
「Parity」：None
パリティチェックの設定をおこないます。none（なし）/ odd （奇数）/even（偶数）が設定可能です。

「Time-Out」：0
本製品に接続した後に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）

「Auto Refresh」：10
コンソールセッション内でコンソール情報を自動的に更新する時間間隔を指定します。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）

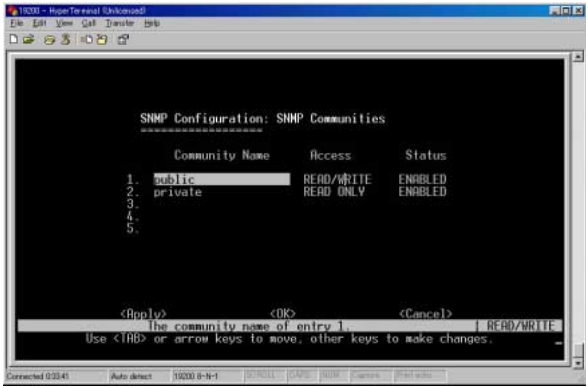
◎SNMP Configuration

SNMP（Simple Network Management Protocol）関連の設定内容を表示・変更する場合は SNMP Configuration スクリーンを選択します。本製品に搭載されているSNMPエージェントは、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。本製品上のエージェントへのアクセス権はコミュニティ名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名を送信して認証を受ける必要があります。以下に、コミュニティ名の設定およびこれと関連するトラップ機能について解説します。



「Send Authentication Fall Traps」
ネットワーク管理ステーションから本製品へのアクセス時に認証に失敗した場合、予め設定した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
アクセスを許可されているコミュニティの設定方法を説明します。

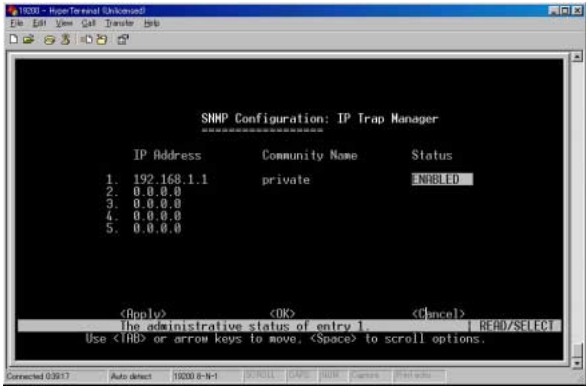


「Community Name」
アクセスが許可されているコミュニティ名（エントリ）です。最大19文字までの文字列が入力可能です。デフォルトでpublicとprivateが設定されています。

「Access」
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。

「Status」
設定したアクセス権をenabled（有効）またはdisabled（無効）に設定します。

◎IP Trap Manager
認証に失敗した場合及び本製品が対応しているトラップメッセージの送信先IPアドレスを設定します。トラップの送信先は最大5つまで指定することが可能です。

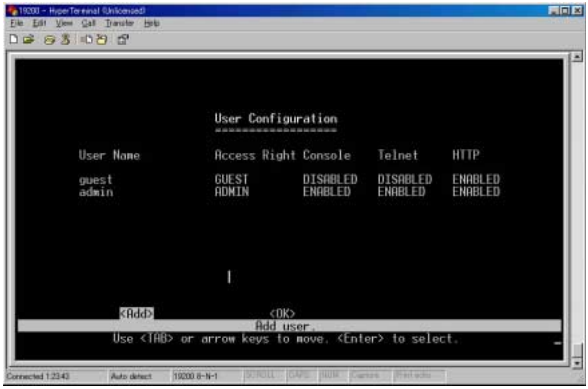


「IP Address」
トラップの送信先IPアドレスです。通常はトラップを受け取るためのネットワークマネージメントソフトウェアがインストールされたコンピュータを指定します。

「Community Name」
トラップの送信先コミュニティを指定します。

「Status」
設定したトラップの設定を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本製品の管理エージェントへのアクセスを制限する場合はUser Configurationメニューを選択してください。ユーザー権限にはにはADMIN （管理者）とGUEST （ゲスト）の二種類があります。管理エージェントのパラメータへの書き込み権限はADMINにのみ与えられています。本製品の設定を開始したら可能な限り早急にADMIN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な場所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」
コンソール、Telnet、HTTP経由で本製品にアクセスすることが出来るユーザ名を設定します。

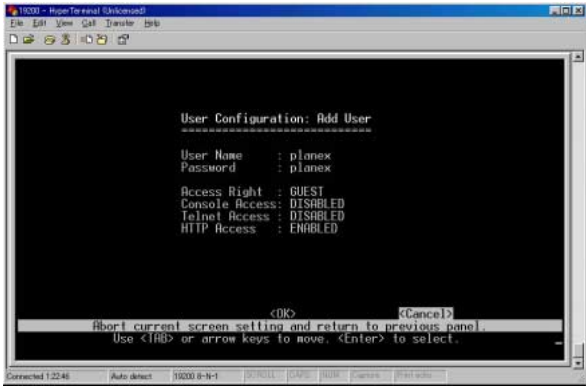
「Access Right」
ADMIN：全スクリーンにおいて読み書きを許可
GUEST：全スクリーンにおいて読み取りのみ許可

「Console」
コンソール経由でのアクセス権を設定します。

「Telnet」
Telnet経由でのアクセス権を設定します。

「HTTP」
HTTP（Webブラウザ）経由でのアクセス権を設定します。

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」
ユーザー名を入力します。

「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。

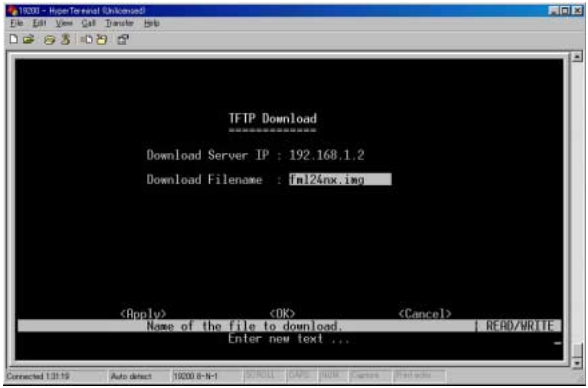
「Access Right」
ADMIN：全スクリーンにおいて読み書きを許可
GUEST：全スクリーンにおいて読み取りのみ許可

「Console Access」
コンソール経由でのアクセスを許可する場合はEnableに、禁止する場合はDisableに設定してください。

「Telnet Access」
Telnet経由でのアクセスを許可する場合はEnableに、禁止する場合はDisableに設定してください。

「HTTP Access」
HTTP（Webブラウザ）経由でのアクセスを許可する場合はEnableに、禁止する場合はDisableに設定してください。

◎TFTP Download
本製品のフラッシュROM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。（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。最新ソフトウェアのダウンロードが完了すると、エージェントは自動的に再起動します。

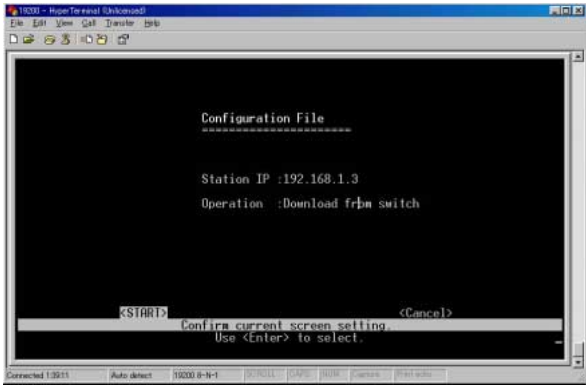


「Download Server IP」
TFTPサーバのIPアドレスを入力してください。

「Download Filename」
ダウンロードするバイナリまたはイメージファイルを指定します。

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。

◎Configuration File
本製品上の設定をTFTPクライアントにアップロードまたはTFTPクライアントからダウンロードすることが可能です。設定ファイルの保存または書き戻し機能を使用することで各設定を短時間で行えるほか、トラブルシューティング時など完全に設定を復元することが出来ます。



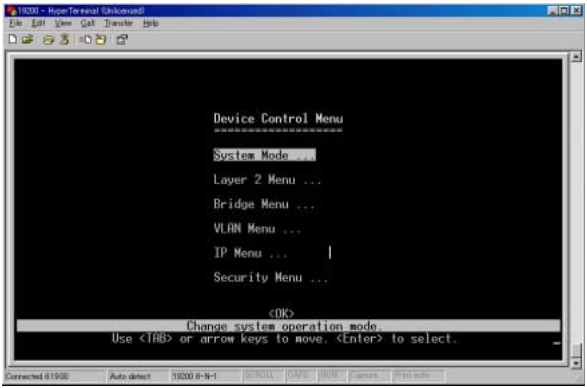
「Station IP」
TFTPクライアントのIPアドレスを入力してください。

「Operation」
本製品の設定を書き出す場合はDownload from switchを、書き戻す場合はUpload to switchを選択してください。

STARTを選択すると設定ファイルの書き出し及び書き戻しを開始します。
次にTFTPクライアント側で送受信の操作を行って下さい。

■Device Control Menu

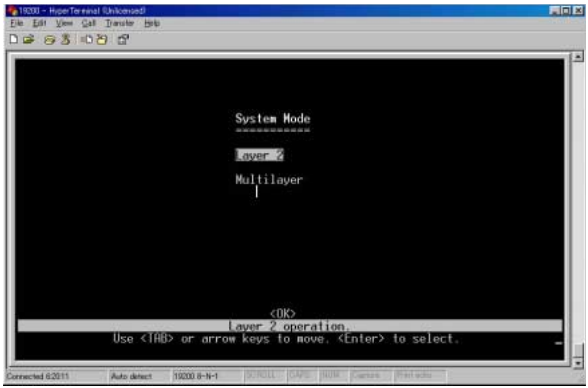
Device Control メニューからは、ポートの転送モード、ポートミラーリング、トランクポート、スパニングツリー、VLAN、IP、マルチキャストおよびルーティングプロトコルなど設定を行うことが可能です。



◎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、IPパケットのみ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。

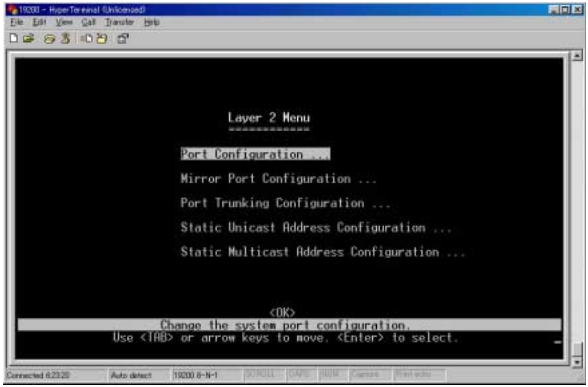


「Layer 2」
全てのプロトコルのトラフィックからフィルタリングおよびフォワーディングの決定をMACアドレスベースで実行します。

「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。

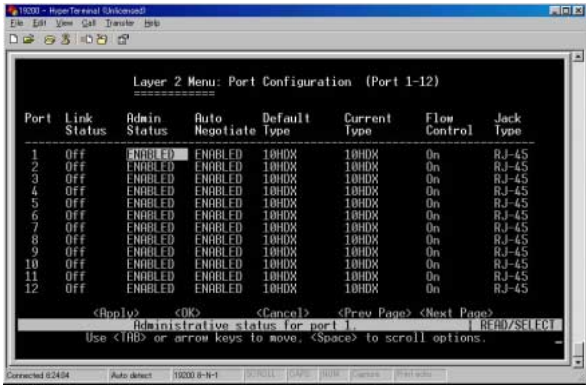
注意　マルチレイヤモードで動作している場合、IPメニューが有効になるかわりに「IP設定（レイヤ2モード）」メニューが無効になります。マルチレイヤモードで動作中にVLANグループ同士で通信を行う必要がある場合はすべてVLANグループにIPインターフェースを設定する必要があります。

◎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・トランキングを設定します。



◎Port Configuration

本製品上の全てのポート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、AutoNegotiation、転送モードの固定、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。



「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、転送モード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Autonegotiationを行いますが、速度は1000Mps固定となります。

「Default Type」
Autonegotiation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ています。

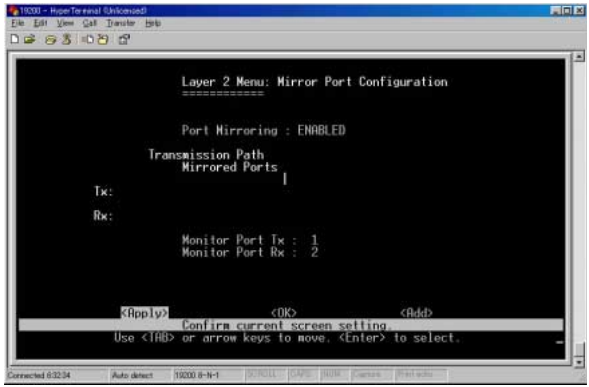
「Current Type」
現在の転送速度および転送モードを表示します。

「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 25-26：SC/RJ-45

◎Mirror Port Configuration

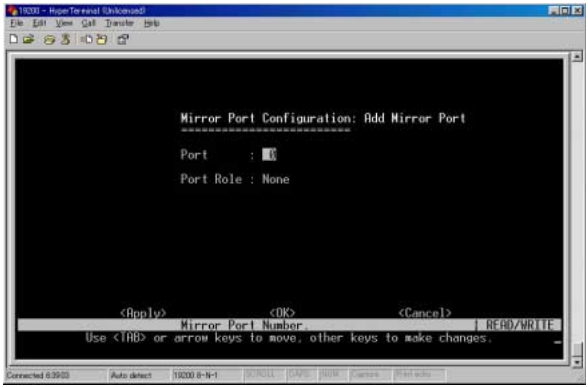
本製品上のいずれかのポート（ソースポート）から送られるトラフィックを他のポート（ターゲットポート）にコピー（ミラー）してリアルタイムでトラフィックを解析することが可能です。ターゲットポートにロジックアナライザやRMONプローブなどを接続すると、現状の通信にまったく影響を与えることなく、ソースポートを通過するトラフィックを解析することができます。なお、ポート上のトラフィックをミラーするには、ソース・ターゲットの両ポートとも同じVLANに所属している必要があります。



「Port Mirroring」

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。
追加されたミラーポートを削除する場合は削除したいポート番号にカーソルを移動しエンターキーを押してください。メニューの一番下にAre you sure you want to perform this operation？ (y/n)と表示されたら削除する場合はYを、削除しない場合はNを入力してエンターキーを押してください。



「Port」
ミラーしたいポート番号を入力してください。

「Port Role」
ポートの送信をミラーする場合はTx Mirroredを、受信の場合はRX Mirroredを、送受信をミラーしたい場合はAll Monitoredを選択してください。

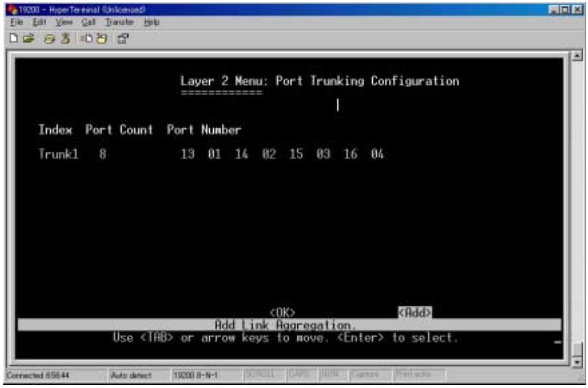
注意　ポートトランクを通過するトラフィックを調べる場合など、複数のポートを一つのポートにミラーすることは可能となっています。ただし、トラフィックの負荷が通常～最大の場合、いくつかパケットが失われる場合があります。

◎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メニューを使用し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。

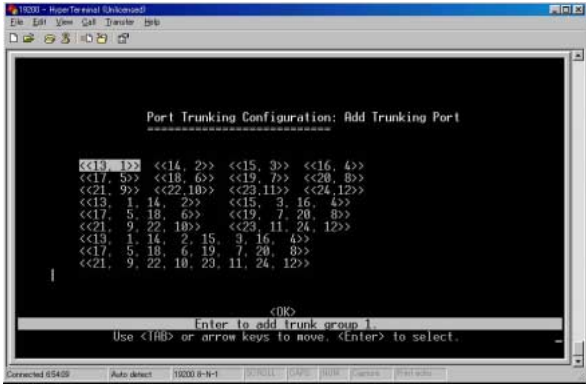
- **１つのトランクに割り当てられたポートは、他のトランクに割り当てることは出来ません。**
- **トランクの設定を両方(対向)のスイッチで行う必要があります。**
- **トランクポートは、両方のスイッチで通信モードやVLAN設定などを同じにする必要があります。**
- **トランクに割り当てられたポートはモニターポートには指定できません。**

●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。
●ギガビットポートはトランクできません。



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。



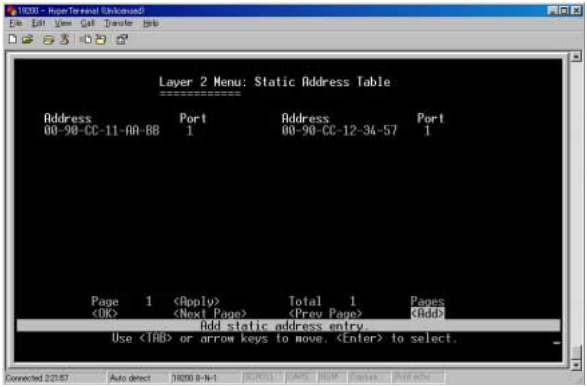
トランクを削除する場合は、削除したいトランクグループにカーソルを移動して反転表示させてEnterキーを押してください。メニューの一番下にAre you sure you want to perform this operation ? (y/n) と表示されたら削除する場合はYを、削除しない場合はNを、入力してエンターキーを押してください。ポートトランクを切断する場合は、事前に以下の点をご確認ください。

●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。

◎Static Unicast Address Configuration

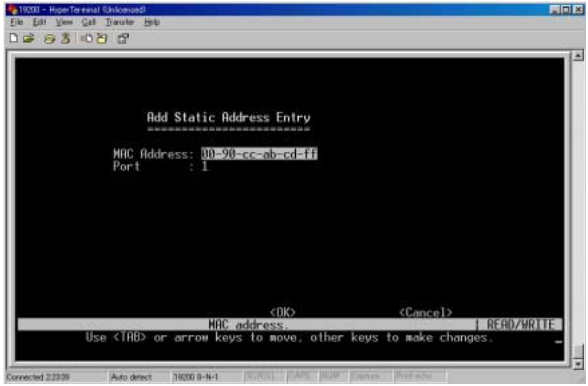
静的ユニキャストアドレスをアドレステーブルに追加することが出来ます。



「Address」
静的に入力したMACアドレスが表示されます。

「Port」
静的に入力されたMACアドレスを持つネットワークデバイスが接続されているポート番号が表示されます。

静的ユニキャストアドレスをテーブルに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。

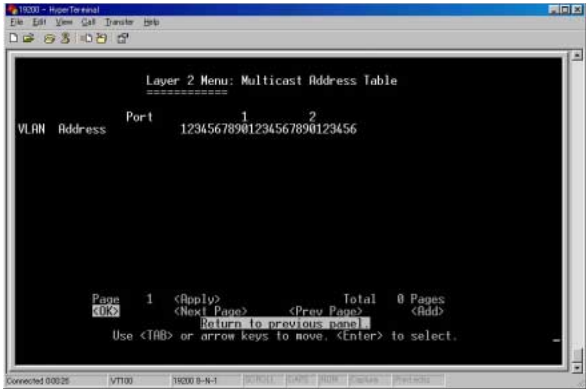


「MAC Address」
ユニキャストテーブルに追加したいMACアドレスを入力します。

「Port」
追加したMACアドレスが接続されているポート番号を入力してください。

◎Static Multicast Address Configuration

Static Multicast Address Tableを使用して、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。



「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。

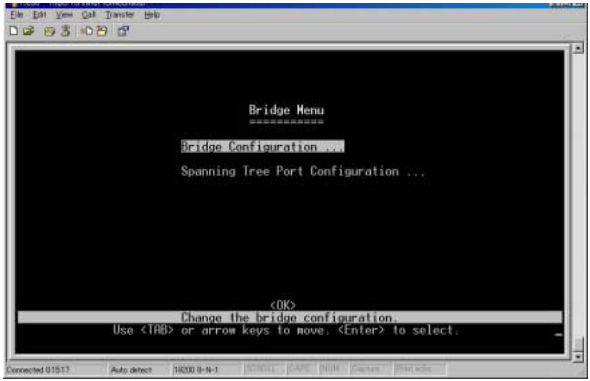
「Port」

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。

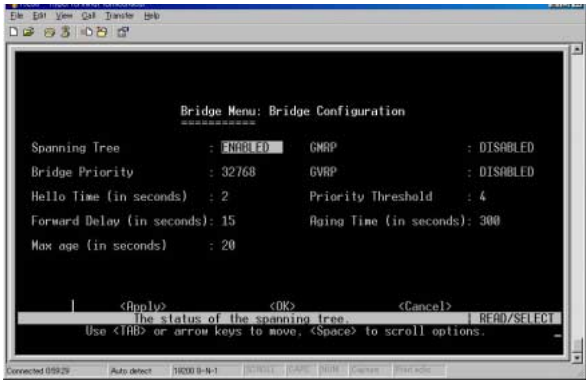
◎Bridge Menu

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（GARP 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、代わ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」
Enable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MAC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 ÷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{(Max. Message Age÷2) ＋1} のうちいずれか大きい方になります。

「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の指定ポートになります。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×（Hello Time ＋1）} のうちいずれか大きい値になるほか、最大値は40秒もしくは {2×（Forward Delay －1）} のうちいずれか小さい値になります。

「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。

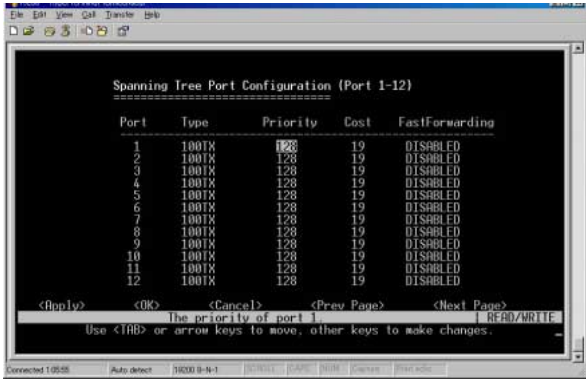
「Priority Threshold」

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



「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。

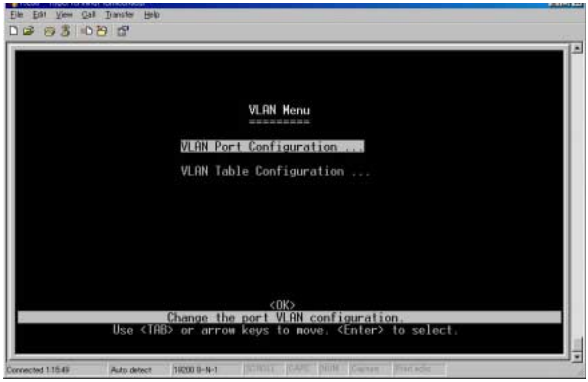
Ethernet　　：100（50～600）
Fast Ethernet　：19（10～60）
Gigabit Ethernet：4（3～10）
最大レンジは 0～65535となっています。

「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です。）

◎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になっています。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設計されていないため、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。マルチレイヤモードではVLANのオーバーラップは出来ません。ルーティングを正しく実行できない原因になります。
※Multilayer Modeの時は、最大26グループが設定可能です。

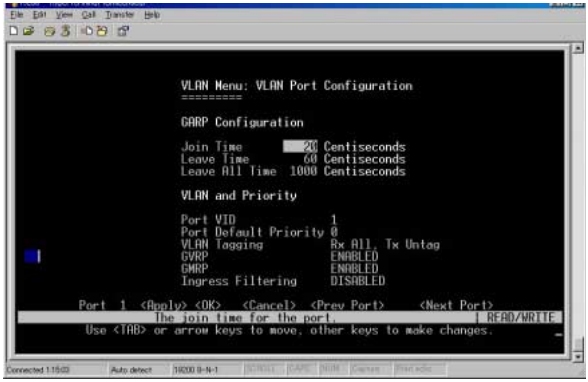


◎VLAN Port Configuration

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タギング、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 Configuration

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LeaveTimeより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無しフレームに割り当てられるVLAN IDを設定します。

「Port Default Priority＊」
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。

＊ 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規模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

マルチレイヤモードでご利用の場合は、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。

「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。

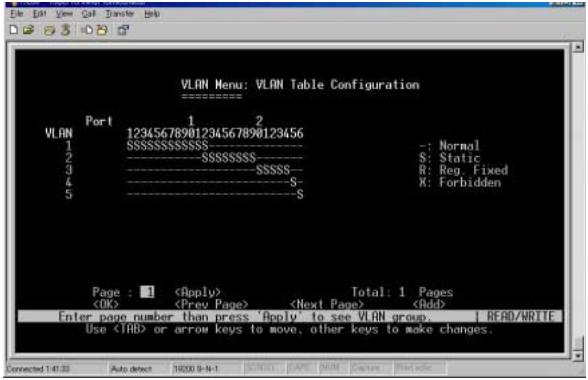
「Ingress Filtering ＊4」

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。

＊4 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。

◎VLAN Table Configuration

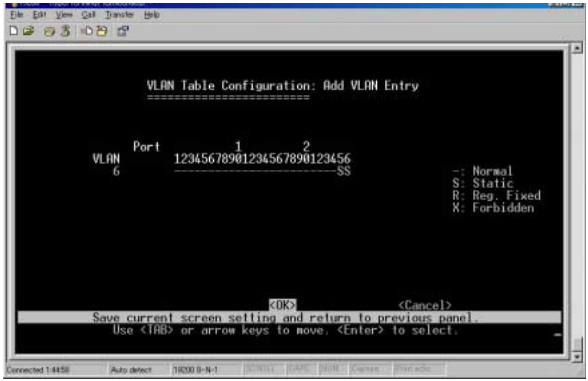
新規のVLANグループ作成や既存のVLANグループの設定を変更を行います。



「VLAN」
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。
R ：GVRPによって追加されたポートメンバーシップを固定します。
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。

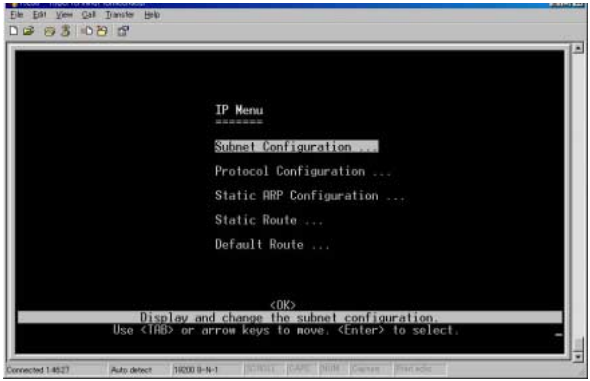


「VLAN」
VLANIDを入力してください。

「Port　1 - 26」
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。

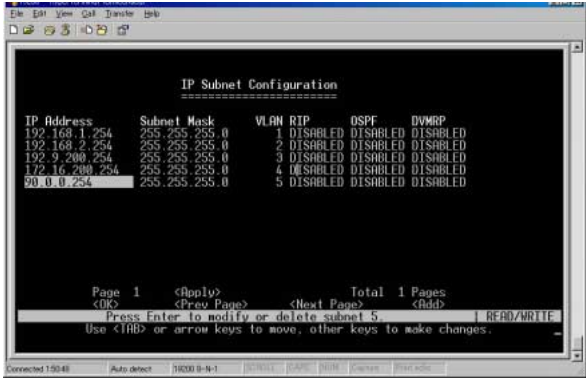
注意　カーソルを<Next Page>　または　<Prev Page>に合わせてエンターキーを押すと、テーブル内容をスクロールできます。特定ページを表示する場合はPage Fieldに希望のページ番号を入力し、カーソルを<Apply>に移動してエンターキーを押します。いずれかのVLANグループを変更する場合は、テーブル内の該当するエントリにカーソルを移動してEnterキーを押してください。VLANグループを追加する場合は カーソルを<Add>に移動してEnterキーを押してください。

◎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。

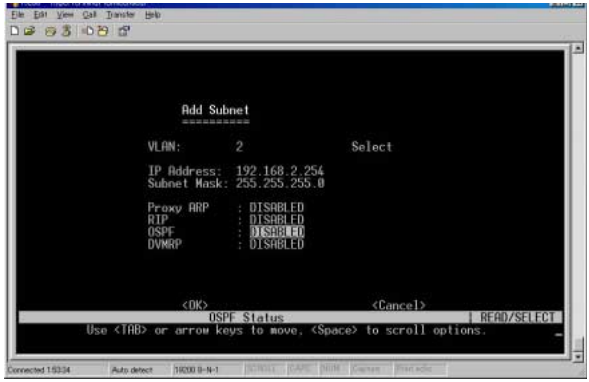
IPインターフェースを新しく追加する場合は、Subnet Configurationメニューの＜Add＞にカーソルを移動してエンターキーを押してください。Add Subnetスクリーンが表示されます。インターフェィスを追加したいVLANグループを選択した後、IPアドレスの設定、必要なルーティングプロトコルを有効にしてください。本メニューからVLANグループの作成および編集を行うことも可能です。

「DVMRP」
設定したインターフェィスに対しマルチ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DVMRPが有効または無効に設定されているかを表示します。

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、AddSubnetスクリーンでSelectを選択します。



「VLAN」

IPインターフェースを追加したい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。

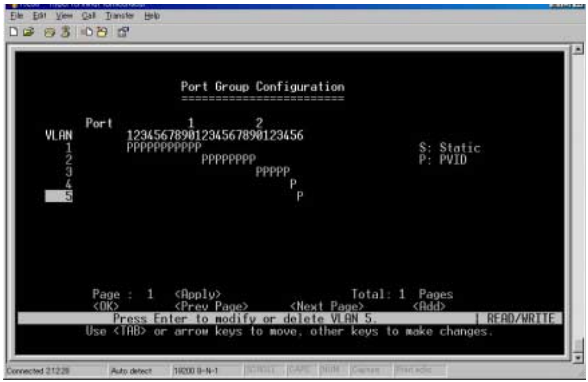
「Subnet Mask」

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になっています。

「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。

「DVMRP」
設定したインターフェイスに対しマルチ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DVMRPが有効または無効に設定されているかを表示します。

◎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を使用し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を使用し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を使用し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。

DVMRPのAdvancedオプションでは、DVMRPに対応したルータがお互いにマルチキャストルーティングテーブルを交換するための詳細設定を行えます。本製品上でDVMRPプロトコルを有効に設定するとPruneメッセージを10秒おきに送信しプルーニングの状態が失効するまでの時間が35秒に設定されます。

「Metrics」
本製品のメトリック(コスト)を設定することができます。DVMRPに対応したルータでは冗長リンクを作成することが可能です。この場合、受信したデータの重複を防ぐためにメトリック値の少ないルータがメインルータになります。

「Probe Interval (in seconds）」
プルーンメッセージを送信する間隔を設定します。

「Neighbor Timeout (in seconds）」
プルーニングの効力が失効するまで時間を設定します。

◎Protocol Configuration

本製品全体でARP、DHCPリレー、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。

「ARP」

ARPのタイムアウトまでの時間を設定します。

「ProxyARP」

ProxyARPの有効/無効を設定します。

「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。

「RIP Update Time」

RIP情報を更新する時間間隔を設定します。

「Default Route Advertisement」

有効に設定するとRIPパケットにデフォルトルートアドレスを追加します。

「Static Route Advertisement」
有効（Enable）に設定するとスタティックで設定されたルート情報をRIPパケットに追加します。

「Ignore Host Route」
有効（Enable）に設定するとRIPパケット内にホストへのルート情報を追加しません。

「DHCP Relay」
DHCPリレー機能の有効/無効を設定します。DHCPリレー機能を有効に設定する場合はAdvancedを選択します。続いて表示されるスクリーンでAddボタンを選択しDHCPサーバのIPアドレスを入力します。設定が完了したらApplyを選択してください。

「IGMP Snooping」
IGMPスヌーピング機能の有効/無効を設定します。IGMPスヌーピングの機能の詳細を設定する場合はAdvancedを選択します。

「IGMP Router Timeout」
IGMPスヌーピングによって取得したマルチキャストルータ情報を消去するまでの時間を設定します。

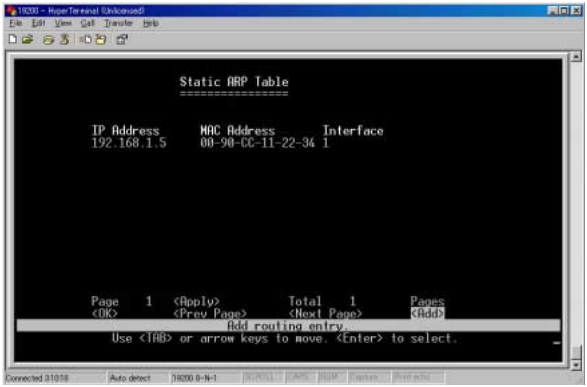
「IGMP Group Timeout」
IGMPスヌーピングによって取得したマルチキャストグループ情報を消去するまでの時間を設定します。

「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 メニューを使用して、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。

◎Static ARP Configuration

本製品では送信先MACアドレスが不明な場合にARPプロトコルを使用して送信先MACアドレスを学習しようとしますがARPパケットから送信先MACアドレスを学習することが出来ない場合にStatic ARP Configurationを使用して送信先IPアドレスとMACアドレスをテーブルに固定することが可能です。



「IP Address」

送信先IPアドレスが表示されます。

「MAC Address」

送信先IPアドレスが持つMACアドレスが表示されます。

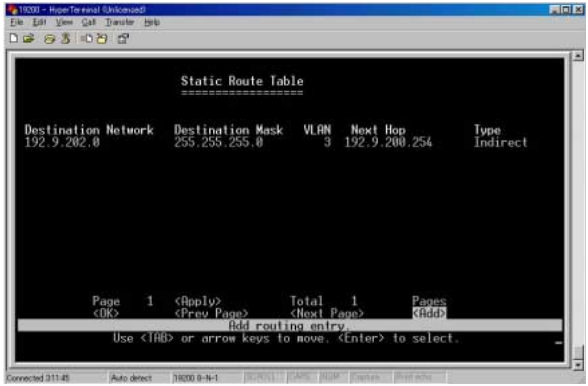
「Interface」

本製品上の接続されているポート番号を表示します。

◎Static Route Configuration

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。



「Destination Network」
通信先のネットワークグループが表示されます。

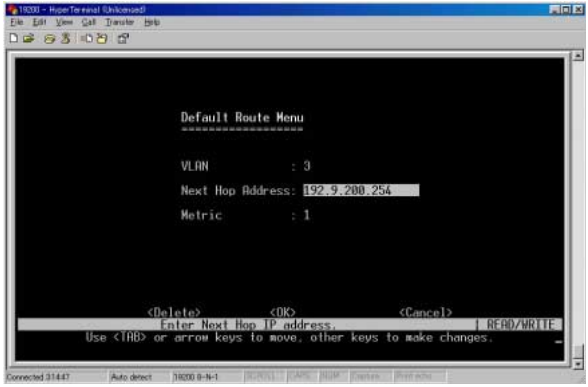
「Destination Mask」
サブネットマスクが表示されます。

「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

◎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。

◎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）を使用して、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」

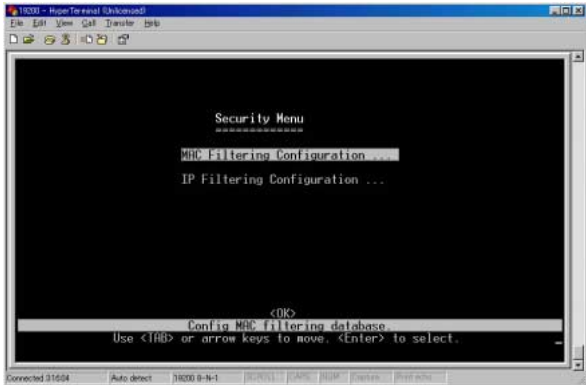
有効の場合、本製品はネットワークトラフィックを監視してどのホストがマルチキャストトラフィックの受信を希望しているかを確認します。これを「IGMPスヌーピング」と呼びます。

「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。

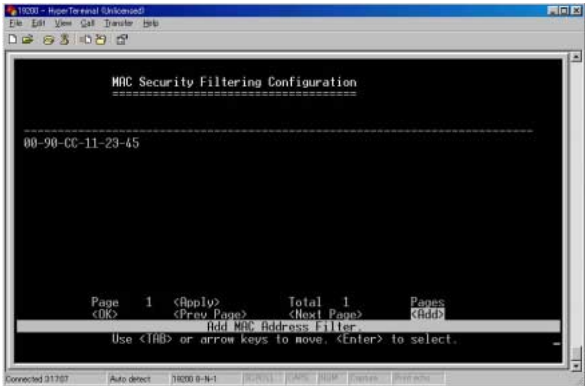
注意　IGMPプロトコルセット全体は、DVMRPとともに自動的に有効/無効に設定されます。

◎Security Menu
本製品は特定のMACアドレスまたはIPアドレスを持つノードに対してフィルタリングすることが可能です。



◎MAC Security Filtering Configuration

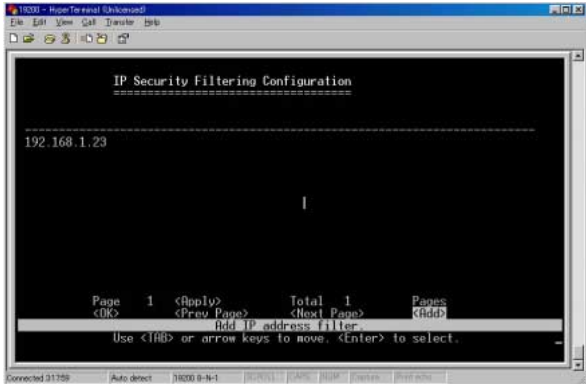
セキュリティュリ面でリスクのあるノードや故障中のノードは、本製品上でフィルタする（切り離す）ことができます。セキュリティ・フィルタリングを使用して、指定MACアドレスのホストから送信されるトラフィックをすべて破棄することが出来ます。同様に、本製品ではSecurity Filtering Configurationテーブル内で登録されている送信元/送信先アドレスを持つトラフィックをフィルタすることが可能です。



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。

◎IP Security Filtering Configuration

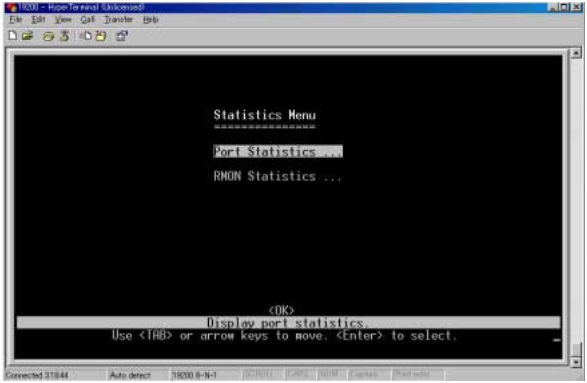
いずれかのノード上でセキュリティ上の問題が認められた場合は、そのアドレスをIP Security Filterに登録し、このノードへのトラフィックをすべてフィルタできるようになっています。当テーブル上のいずれかのエントリと一致する送信元/送信先IPアドレスを持つパケットは、本製品を通過する際にフィルタされます。



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。

■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、何もエラーが検出されなかったにも関わらず破棄される受信（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破棄する理由には、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みます）

「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、何もエラーが検出されなかったにも関わらず破棄される送信（アウトバウンド）パケットの数を指定します。これらのパケットを破棄する理由には、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。

「Defered 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。

「Excess 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（破棄）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、512ビットタイム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。

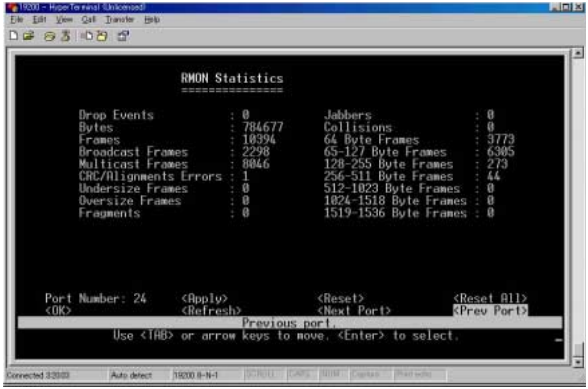
「Fragments」
64オクテットより短い受信フレーム（ただしフレーミングビットは除き、FCSオクテットは含む）のうち、FCSもしくはアライメントエラーを起こしたものの総計です。

「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され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。

「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。

「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。

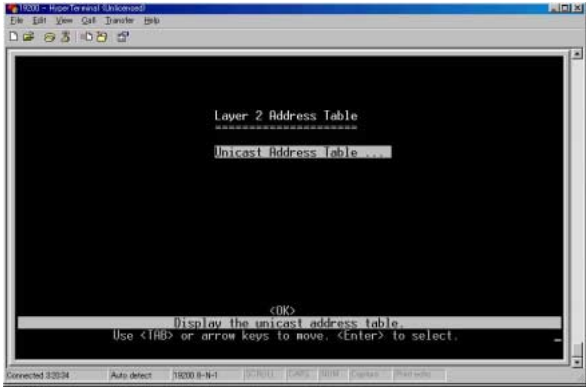
「65-127 Byte Frames」
送受信したフレームのうち、長さがこの範囲内のものの総計です。これには不良パケットやFCSオクテットが含まれますが、フレーミングビットは除きます。

128-255 Byte Frames　：（同上）
256-511 Byte Frames　：（同上）
512-1023 Byte Frames　：（同上）
1024-1518 Byte Frames　：（同上）
1519-1536 Byte Frames　：（同上）

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。

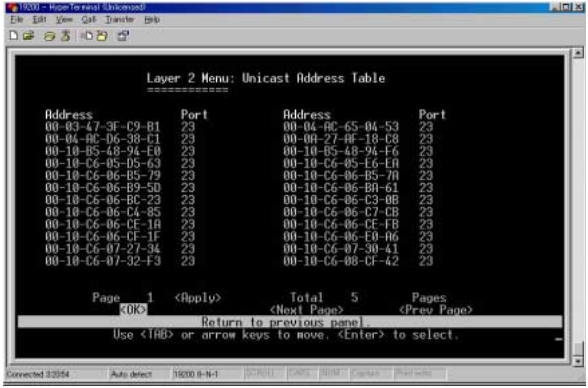
◎Layer 2 Address Table

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。



「Address」

本製品上で参照できるノードのMACアドレスです。

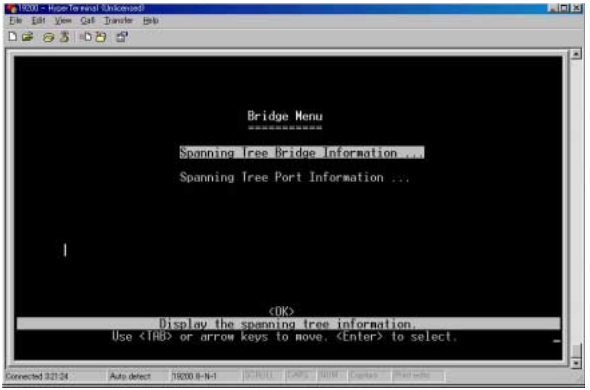
「Port」

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。

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PageField 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。

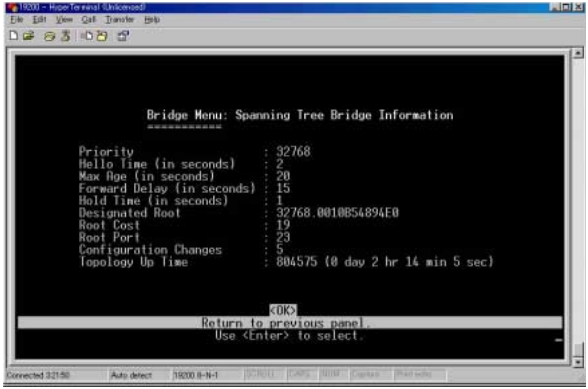
◎Bridge Menu

スパニングツリー・アルゴリズムの状態を参照することが可能です。



◎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表示します。

「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表示します。

「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表示します。

「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表示します。

「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。

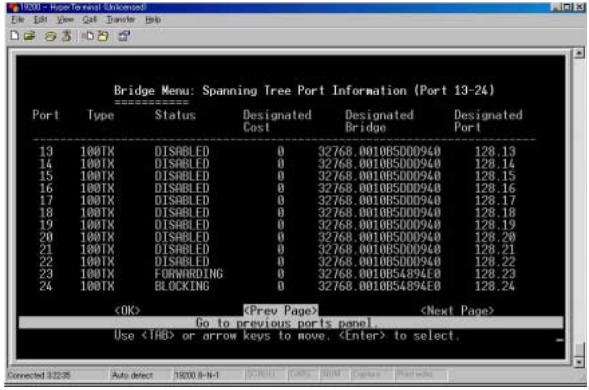
「Root Cost」
本製品上のルートポートからルート機器までのパスコストです。

「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



「Status」

スパ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ステート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。

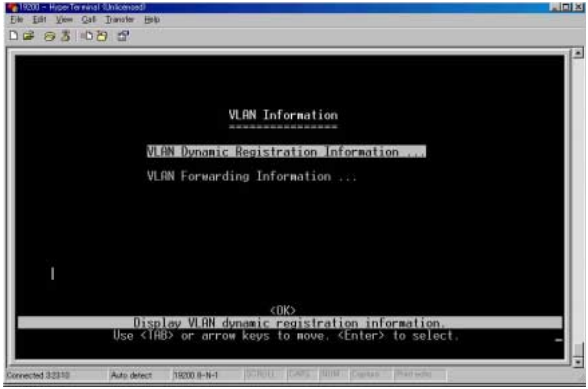
「Designated Bridge（ID）」
このポートがスパニングツリーのルートに到達するため、途中通過しなければならない機器のプライオリティおよびMACアドレスを表示します。

「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。

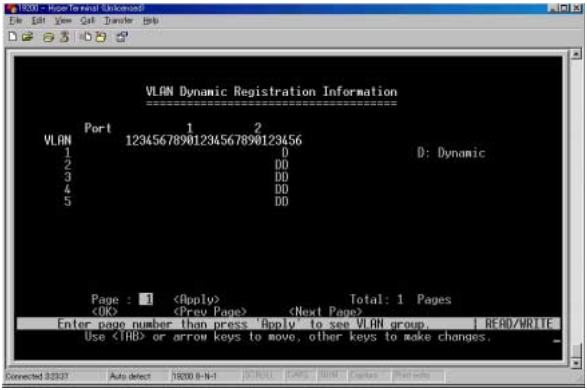
◎VLAN Information

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

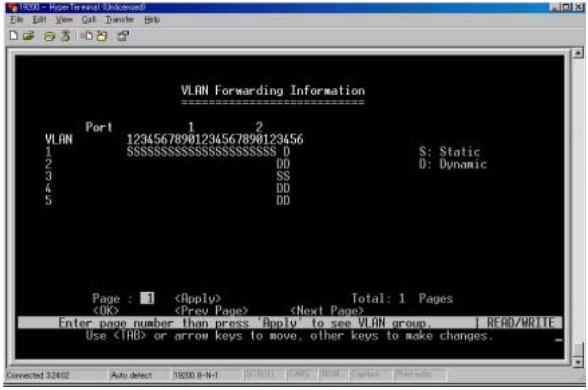
GVRPにより自動的に学習されたポートを表示します。



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

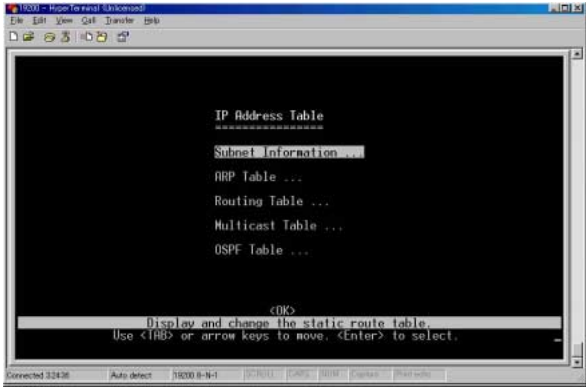
VLANトラフィック転送用の、動的または静的に設定されたポートを表示します。



注意　画面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。

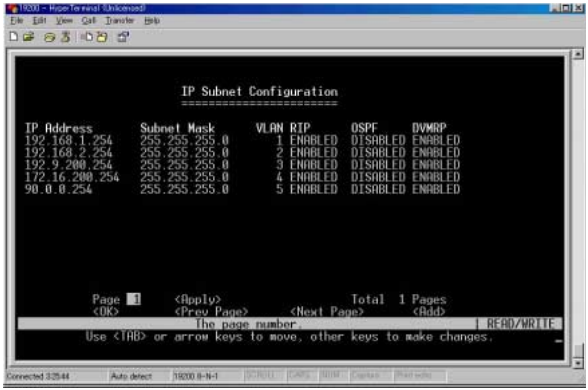
◎IP Address Table

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。



◎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」

本製品上のIPインターフェースのアドレスです。

「Subnet Mask」

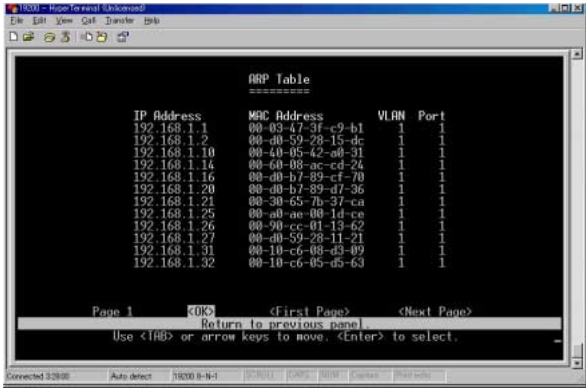
サブネットマスクが表示されます。

「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。

◎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」

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。

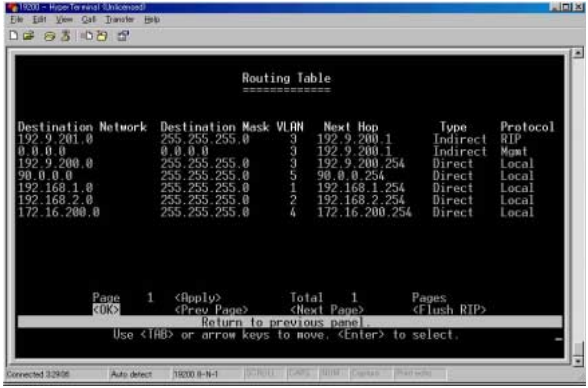
「Port」

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。

◎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。



「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。

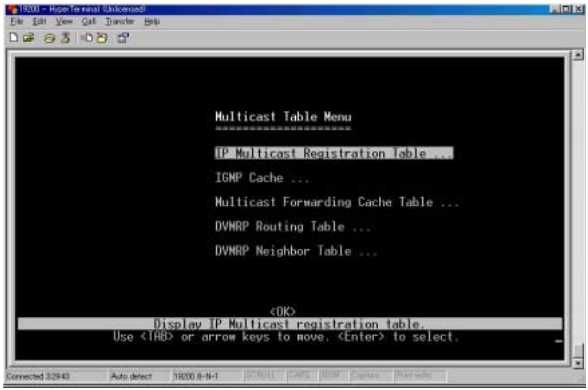
「Next Hop」
次のホップにあたるルータのIPアドレスです。

「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

「Protocol」
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

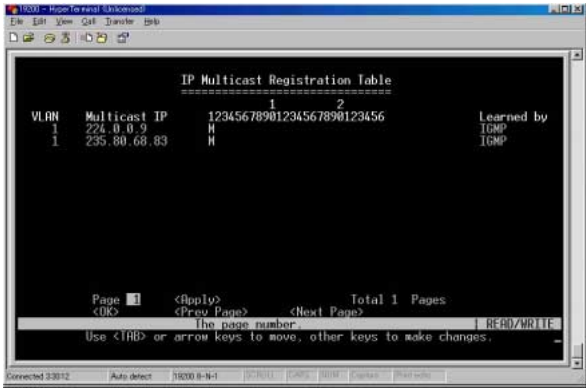
注意　<Next Page>または<Prev Page>にカーソルを移動してEnterキーを押すとルーティングテーブルをスクロールできます。特定ページを表示する場合は、Page Fieldにページ番号を入力して<Apply>にカーソルを移動してEnterキーを押してください。

◎Multicast Table



◎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。



「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。

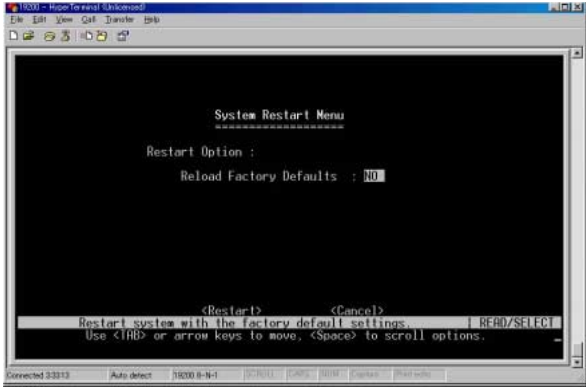
「Learned by 」

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。

■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。

■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。(Internet Explorer4.0以降およびNetscape Navigator4.0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ー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Webインターフェースからは、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で本製品に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エージェントもコンソールからのアクセス時と同じ管理者用ユーザー名およびパスワードを使用してログインします。

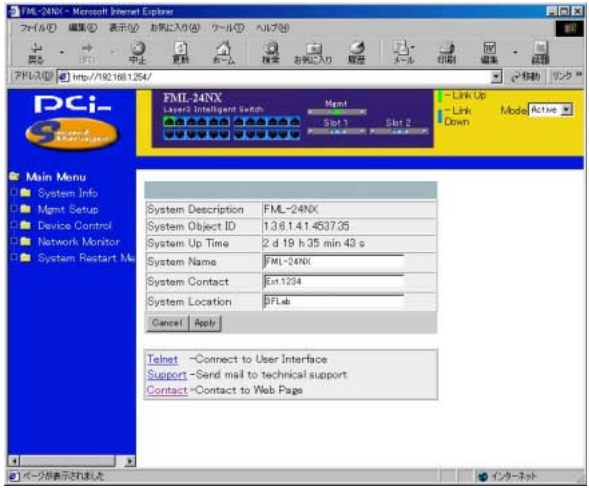
2. Webブラウザインターフェースを操作する

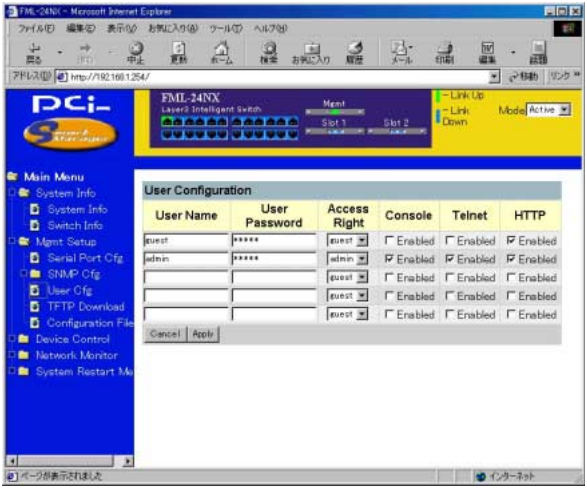
Webブラウザインターフェースにアクセスするには、まずユーザー名とパスワードを入力する必要があります。デフォルトのユーザー名はadminとなっており、パスワードは設定されていません。管理者は、すべての設定パラメータおよび統計において読み書きアクセスが実行できるようになっています。

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。ウィンドウ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。

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。


FML-24NX
Layer2 Intelligent Switch
Mgmt
Slot 1
Slot 2
Link Up
Link Down
Mode
Active
Main Menu
System Info
Mgmt Setup
Device Control
Network Monitor
System Restart
System Description
FML-24NX
System Object ID
1.3.6.1.4.1.4537.35
System Up Time
2 d 19 h 35 min 43 s
System Name
FML-24NX
System Contact
Ext.1234
System Location
BFLab
Cancel
Apply
Telnet -Connect to User Interface
Support -Send mail to technical support
Contact -Contact to Web Page



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

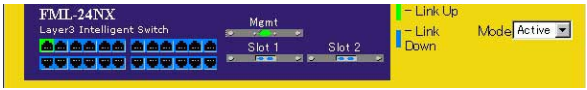
◎設定可能オプション

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。
Cancel　：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または転送モードを切り替えることで状況を色で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通信モードを変更する事が出来ます。



◎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。

Port 1 state summary	
Name	
Type	100BASE-TX
Admin Status	Enabled
Link Status	Up
Speed Status	100M
Duplex Status	Full
Flow Control Status	Enabled
VLAN ID	1

Port StatisticsPort 1 Statistics			
In Octets	354543	Out Octets	377848
In Unicast Pkts.	1463	Out Unicast Pkts.	1358
In Non-Unicast Pkts.	1875	Out Non-Unicast Pkts.	777
In Discards	0	Out Discards	0
In Errors	0	Out Errors	0
Alignment Errors	0	CRC Errors	0
Single Collisions	0	Multiples Collisions	0
Defered Transmissions	0	Late Collisions	0
Excess Collisions	0	Carrier Sense Errors	0
Drop Events	0	Fragments	0
Octets	732391	Jabbers	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。

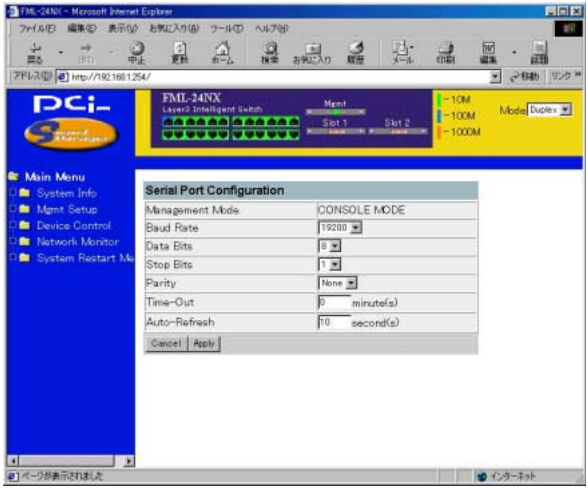
「Speed Status」
現在のポート速度を表示します。

「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 ID」
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。



「Baud Rate」：19200
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」：10分
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」：8ビット
RS-232Cポートのデータビットを設定します。設定範囲：7,8

「Stop bits」：1ビット
RS-232Cポートのストップビットを設定します。設定範囲：1,2

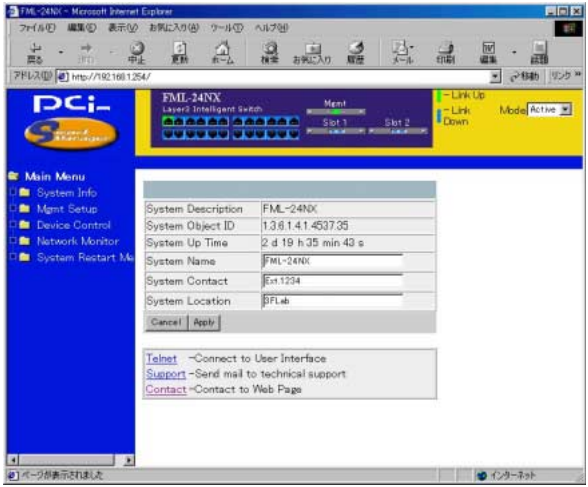
「Parity」：none
RS-232Cポートのパリティを設定します。設定範囲：none（なし）/odd/even

■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。



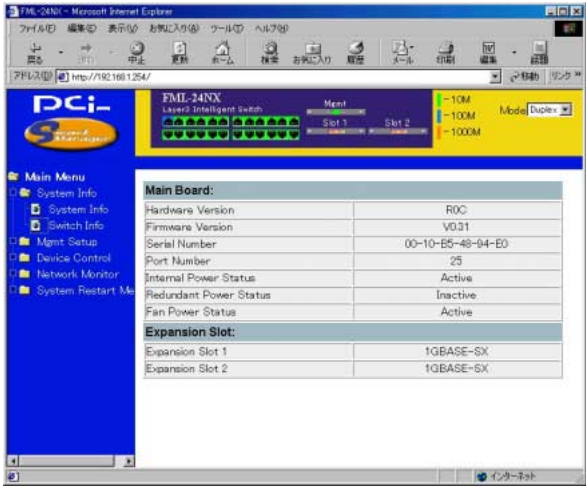
「System Name＊」
本製品に割り当てられている名称です。

「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が、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

「Hardware Version」

マザーボードのハードウェアバージョンです

「Firmware Version」

ROM内システムファームウェアのバージョンです

「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

「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。

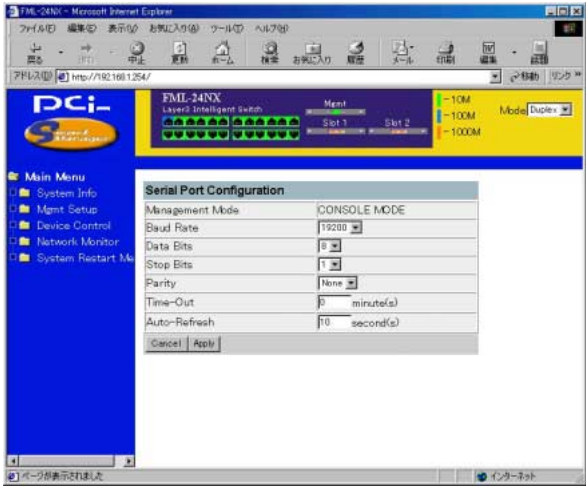
「Fan Power Status」
ファン電源の使用/非使用を表示します。

Expansion Slot
「Expansion Slot 1」及び「Expansion slot 2」
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。Management Setup Menuで使用可能なオプションを以下に示します。

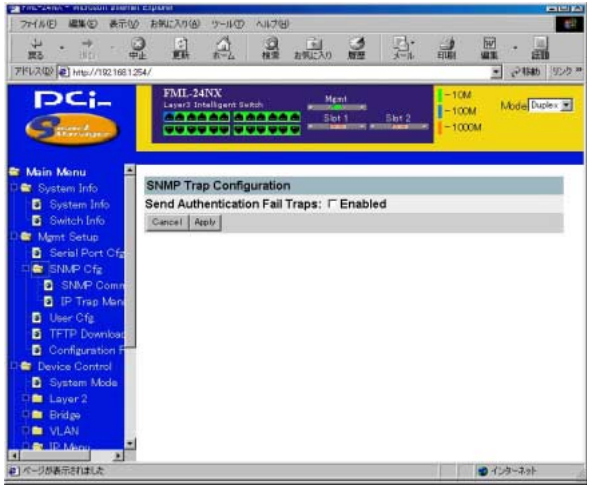
◎Serial Port Cfg.



「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。

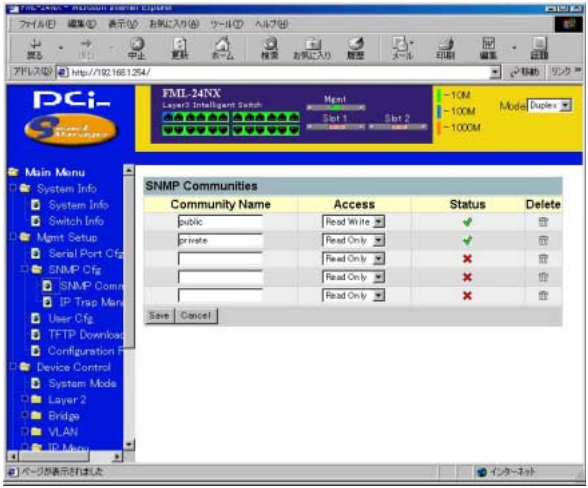
◎SNMP Cfg.

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。



「Send Authentication Fail Traps」
ネットワーク管理ステーションから本製品へのアクセス時に認証に失敗した場合、予め設定した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)

「SNMP Communities」
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。



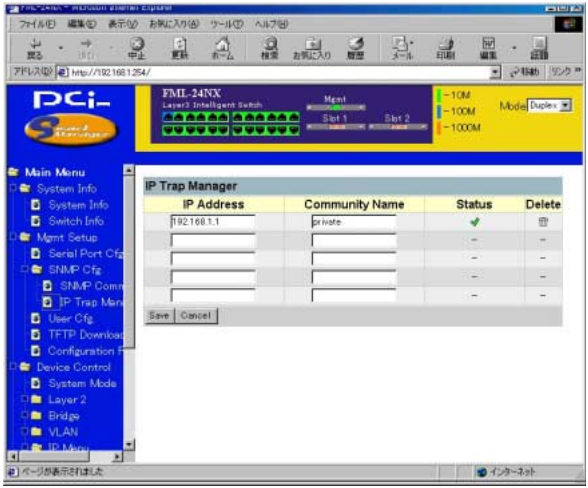
「Community Name」
管理アクセスが許可されているコミュニティ名(エントリ)です。最大20文字までの文字列が指定可能です。

「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（使用中）リスト上でストリングの追加・削除を　行います。

「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。



「IP Address」

トラップマネージャのIPアドレスです。

「Status」

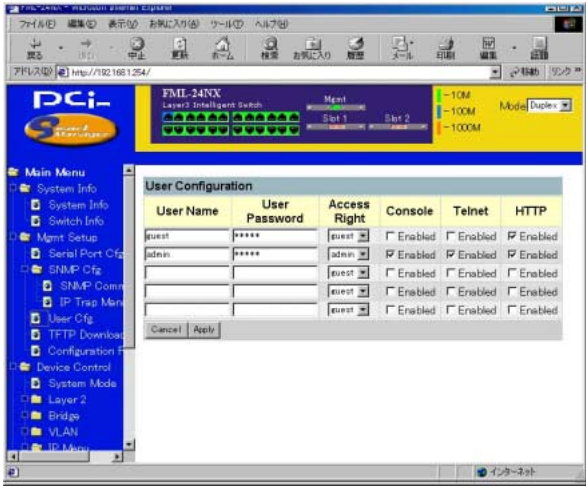
トラップ送信の有効無効を行います。

「Delete」

リスト上で設定のストリングの追加・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。



「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

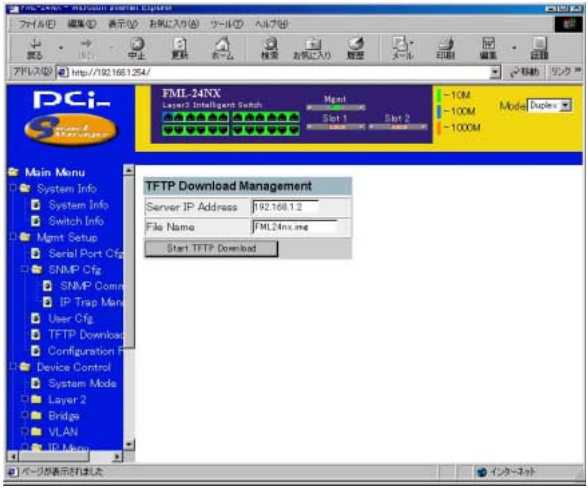
「Console」

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。

◎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。

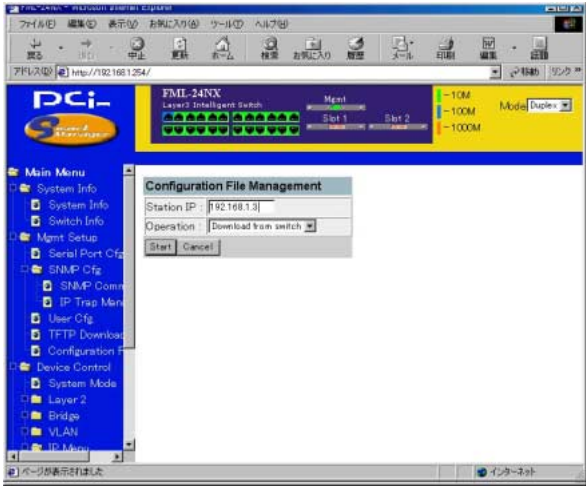


「Server IP Address」
TFTPサーバのIPアドレスです。

「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。

◎Configration File
本製品上の設定をTFTPクライアントにアップロードまたはTFTPクライアントからダウンロードすることが可能です。設定ファイルの保存または書き戻し機能を使用することで各設定を短時間で行行える他トラブルシューティング時など完全に設定を復元することが出来ます。



「Station IP」
TFTPクライアントのIPアドレスを入力してください。

「Operation」
本製品の設定を書き出す場合はDownload from switchを書き戻す場合はUpload to switchを選択してください。

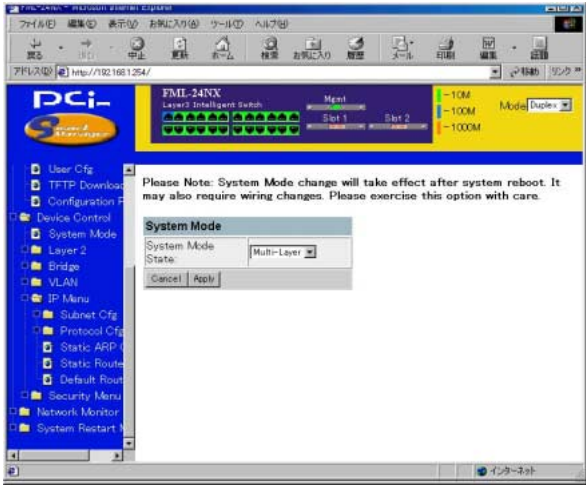
STARTを選択すると設定ファイルの書き出し及び書き戻しを開始します。
次にTFTPクライアント側で送受信の操作を行って下さい。

■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、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

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

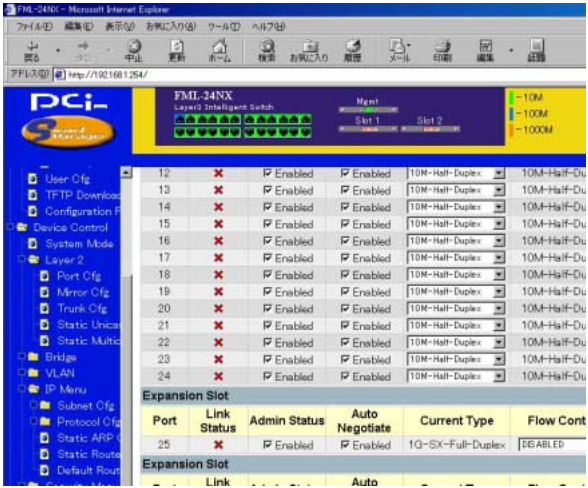


◎Layer2

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。



「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。

「AutoNegotiation」
Autonegotiation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。

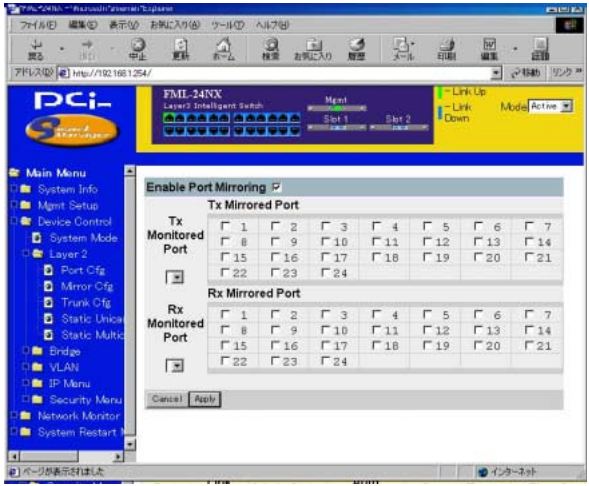
「Current Type」
現在のポート速度（10M, 100M, 1000M）、通信モード（Half, Full）を示します。

「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。

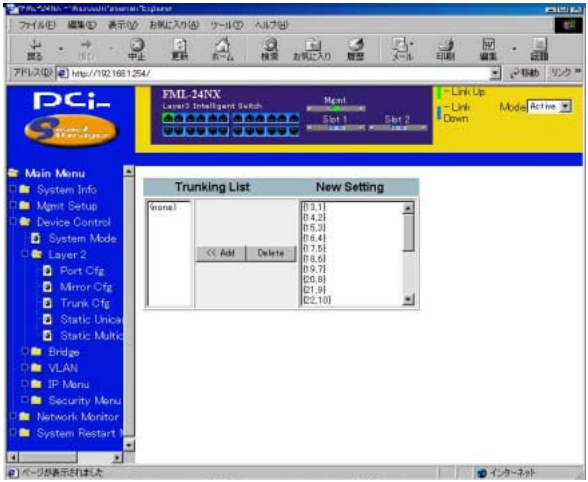
「Rx Mirrored Port」
トラフィック監視の対象となる受信ポートです。

「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ーします。

◎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メニューを使用し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。

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

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

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

<<13, 1, 14, 2>>　　<<15, 3, 16, 4>>

<<17, 5, 18, 6>>　　<<19, 7, 20, 8>>

<<21, 9, 22, 10>>　　<<23, 11, 24, 12>>

<<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。

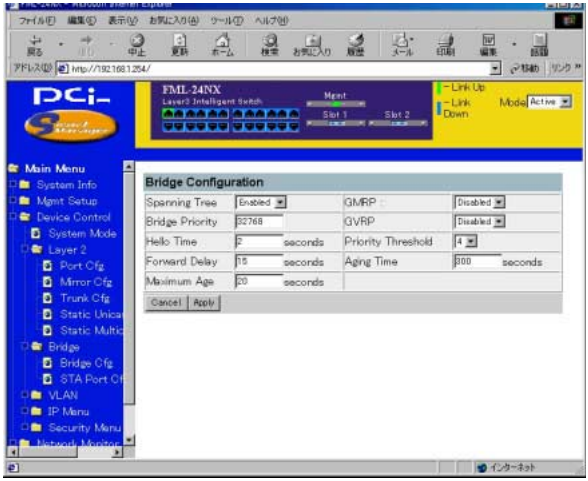
●ポートトランク内のいずれか一つのリンクを無効にする場合は、まず該当するネットワークケーブルを外し、そのリンクの両端をそれぞれConfiguration Menu上で無効にする必要があります。この結果リンクを通過するトラフィックは自動的にトランク内の他のリンクに配分されるため、多量のトラフィックを失うことはありません。

◎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 (GARP 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、代わ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MAC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 ÷2)-1}のうちいずれか低い方になります。

「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{(Max. Message Age ÷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×(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×（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。

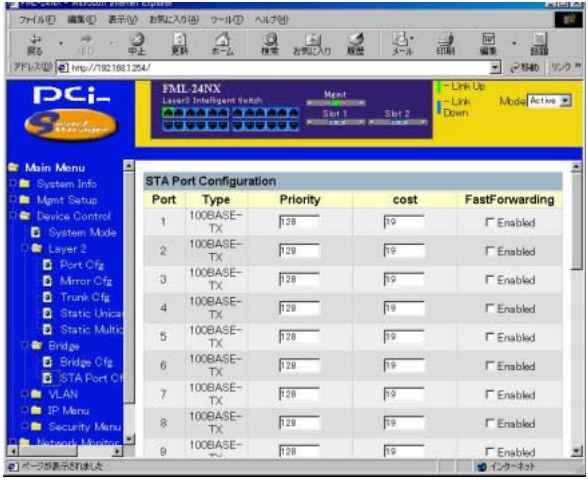
「GVRP」
GVRP (GARP VLAN Registration Protocol) は、各スイッチがネットワーク上の必要なVLANメンバーを登録できるよう、互いにVLAN情報を交換する手段を提供します。VLANの自動登録を許可する場合や、ローカルスイッチを超えて広がるVLANを使用する場合などは当機能を有効(Enabled)に設定してください。

「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



「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。

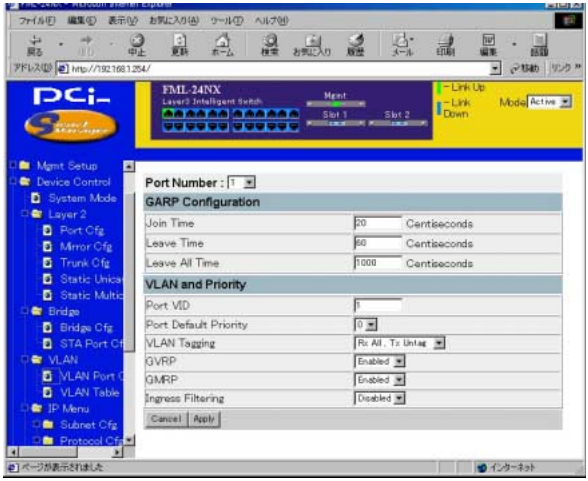
＊末端ノードではフォワーディングループは発生しないため、これらのノードでは、通常の検出(convergence)時間で許されているより高速にスパニングツリーのステート移行を行うことが可能です。ファストフォワーディングは末端ノードおよびサーバ上でより高速に最適経路の検出が行えるほか、他のSTAに関連したタイムアウト問題も克服することが可能です。(重要：ファストフォワードを有効に設定できるポートは、末端デバイスと接続しているポートのみとなっておりますのでご注意ください。)

◎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。



「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。

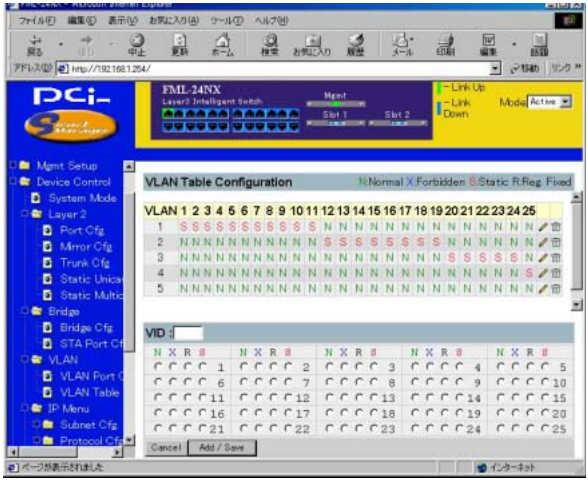
「VLAN」
追加、削除、新規したいVLANグループ用の名称および数字の識別番号を指定します。(VLAN名は本製品上での管理でのみ使用します。VLANタグにこの番号は追加されません。)

「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タギング、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＊2」
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赤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 ＊3」
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。

＊2 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。）

＊3 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。

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を使用することを推奨します。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規模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

マルチレイヤモードでご利用の場合は、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。

「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 ＊4」
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。

*4 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。

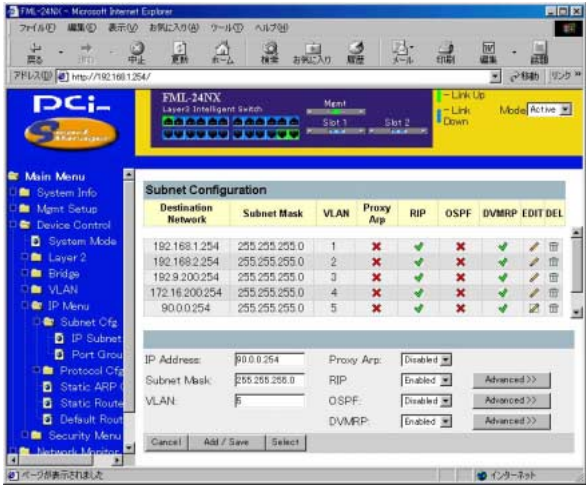
※GARP
GVRPとGMRPは、ブリッジLAN内のクライアント用サービスに対し、クライアント属性を登録/抹消する際にGARP（Group Address Registration Protocol)を使用します。
各GARPタイマのデフォルト値は、データ速度やメディア接続方法に依存しません。GMRPまたはGVRPの登録/抹消において何か不具合が発生していない限り、これらの設定値は変更しないようにしてください。
各ポートのVLAN属性の変更、VLANグループのポート・メンバーシップを設定を設定します。

「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
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。

◎IP　Subnet Cfg.

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ー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ースに対し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ースに対し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）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インターフェースの情報を更新します。

「Addボタン」
設定されたIPインターフェースを追加します。

「Cancelボタン」
設定されたIPインターフェー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インターフェースを追加したい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。

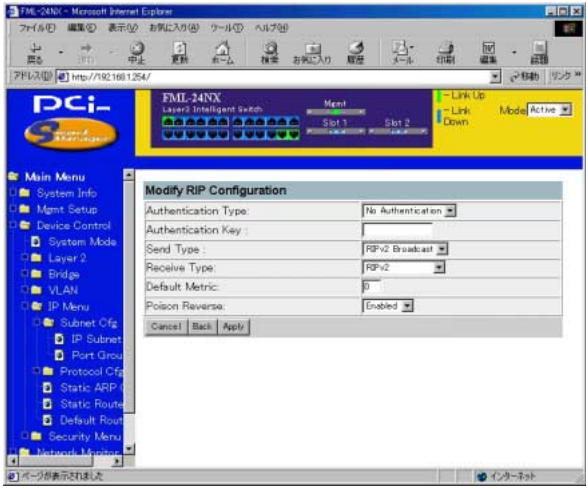
「RIP」
ユニキャストルーティング用のルーティング情報プロトコルの有効/無効を設定します。

「OSPF」
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の有効/無効を設定します。

「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）の有効/無効を設定します。

◎Advanceボタン
RIP、OSPF、DVMRPそれぞれに詳細設定を選択することが可能です。

RIP
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を使用し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を使用し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を使用し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。

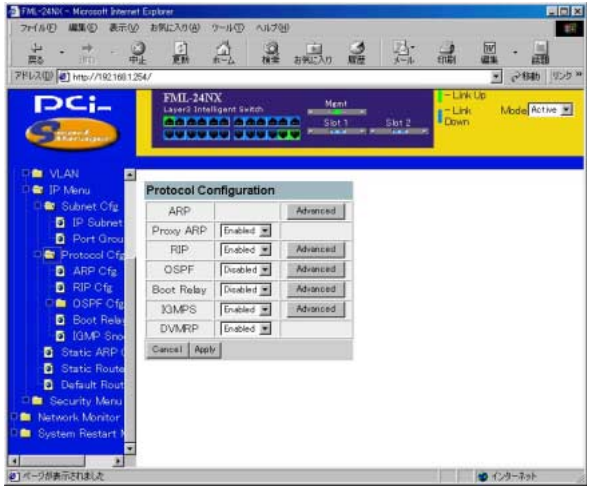
「Default Metric」
メトリックとは、本製品と通信先ネットワークとの間のホップ数を指します。「デフォルトメトリック」は、当インターフェースから発信されたRIP更新（情報）に含まれるデフォルトルートを指します。0と設定すると、デフォルトルートは何も発信されず、他のルータから発信されたデフォルトルートが伝播するかたちになります。値は0～15の範囲で設定可能です。

「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下さい。

◎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。IP Menu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」

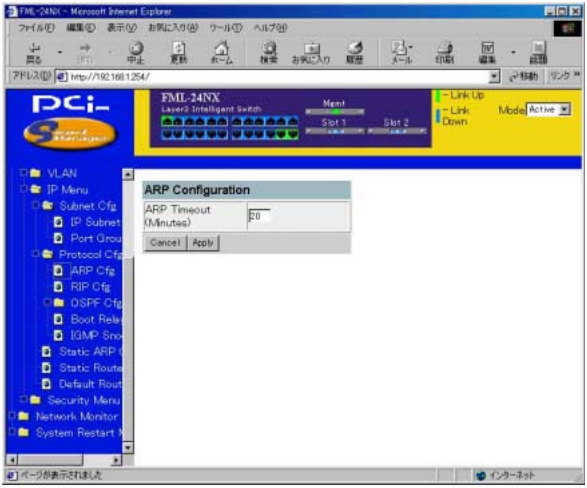
設定したインターフェースに対しユニキャストルーティング用のルーティング情報プロトコルであるRIPが有効または無効に設定されているかを表示します。

「OSPF」

設定したインターフェースに対し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ースに対し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）が有効または無効に設定されているかを表示します。

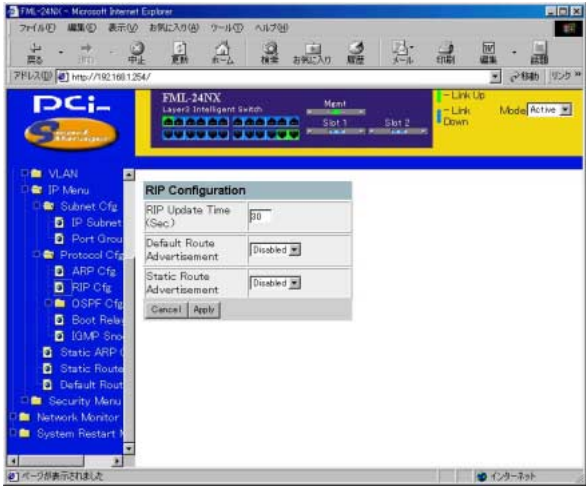
◎ARP Cfg.
ARPパケット送信後、ネットワークでデバイスからの応答を待つ間のタイムアウト値を設定することができます。



「ARP Timeout」
応答を待時間を入力します。

◎RIP Cfg

RIPパケットの設定を行います。



「RIP Update Time」

RIP情報をアップデートする時間間隔を入力してください。

「Default Route Advertisement」

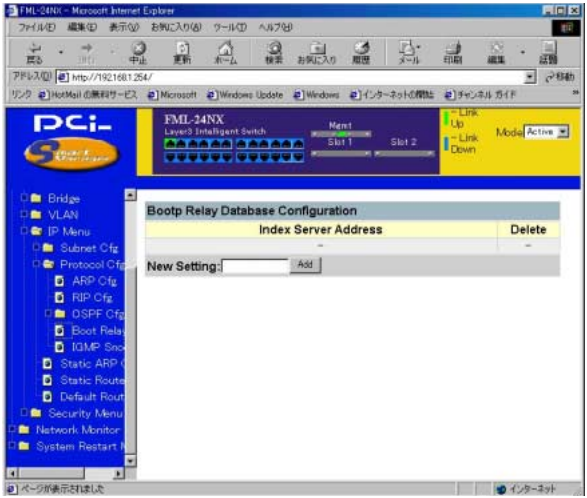
RIPパケット内に本製品上に設定されているデフォルトルートアドレスを入れて送信するかどうかを設定します。

「Static Route Advertisement」

RIPパケット内に本製品上に設定されているスタティックルートアドレスを入れて送信するかどうかを設定します。

◎Boot Relay Cfg.

本製品はBootPまたはDHCPリレー機能に対応しています。リレー機能を有効にすることによりIPサブネットを越えてDHCPサーバからIPアドレスを動的に取得することが可能になります。

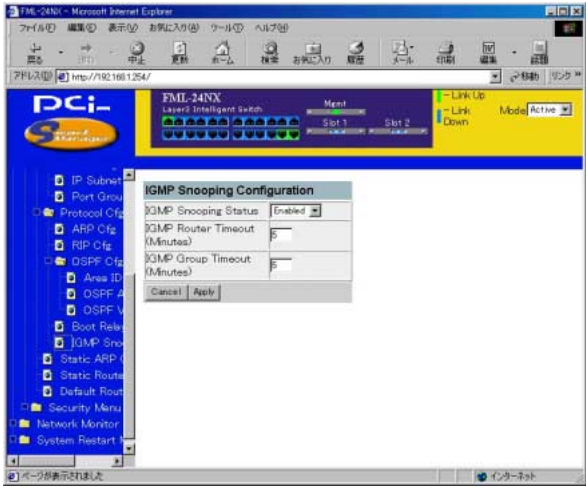


「Index Server Address」

DHCPサーバのIPアドレスが表示されます。

◎IGMP Snooping Configuration

本製品ではIGMP（Internet Group Management Protocol）を使用して、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」：Disabled

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」：5

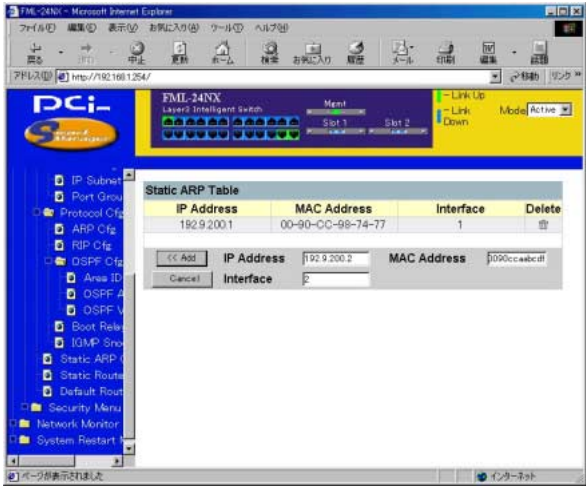
スイッチ上のポートで、ここで指定された時間の間マルチキャストプロトコルパケットの受信を停止したものはIGMPフォワーディングリストから除かれます。　タイムアウトは 3～5分の間で設定可能です。

「IGMP Group Timeout」: 5

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。

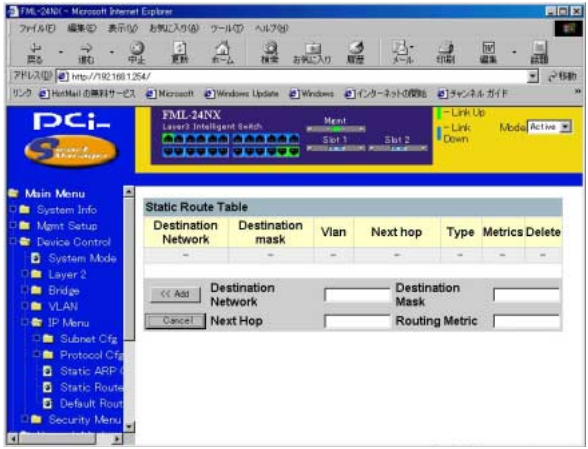
◎Static ARP Cfg



◎Static Route

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を使用し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。



「Destination Network」
宛先のネットワークグループ入力してください。

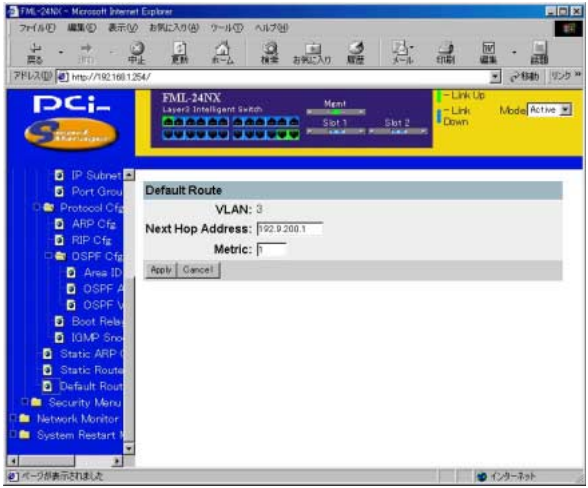
「Destination Mask」
宛先のサブネットマスクを入力してください。

「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。

◎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ーします。

◎IGMP Snooping Configuration（レイヤ2モードのみ）
本製品ではIGMP (Internet Group Management Protocol)を使用して、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。

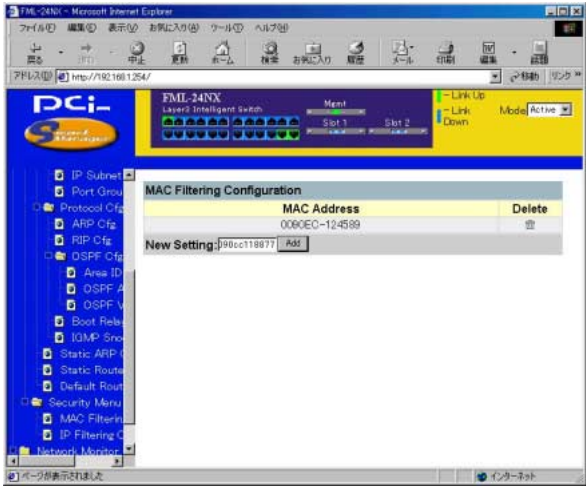
「IGMP Status」：Disabled
有効の場合、本製品はネットワークトラフィックを監視してどのホストがマルチキャストトラフィックの受信を希望しているかを確認します。これを「IGMPスヌーピング」と呼びます。

「IGMP Router Timeout」：5
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」：5
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。

◎MAC Filtering Cfg.
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用して、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。



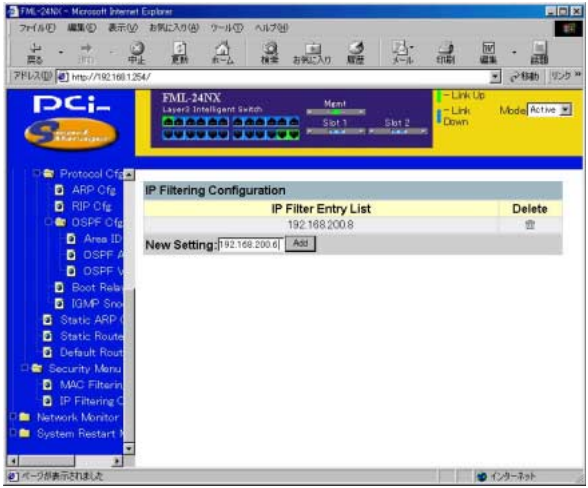
「MAC Address」
フィルタの対象になるMACアドレスを入力します。

「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から選択したアドレスを消去します。

◎IP Filtering Cfg.

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用して、指定IP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。



「IP Filter Entry List」

フィルタの対象になるIPアドレスを入力します。

「Addボタン」
入力されたIPアドレスをフィルタリングテーブルに追加します。

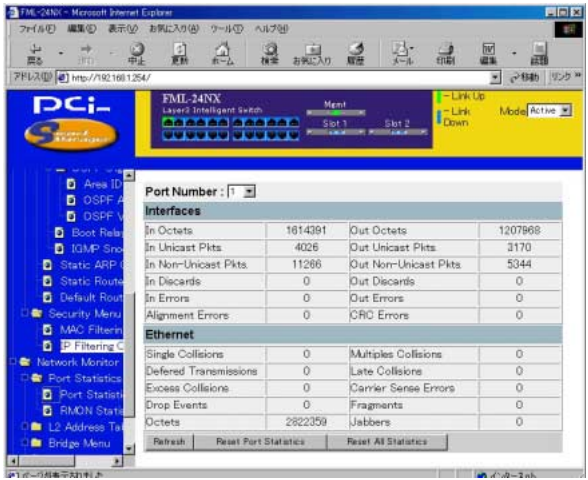
「Deleteボタン」
Security Filtering Entry Listから選択したアドレスを消去します。

■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。



「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破棄される受信（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破棄する理由には、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みます）

「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破棄される送信（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破棄する理由には、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（破棄）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、512ビットタイム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。

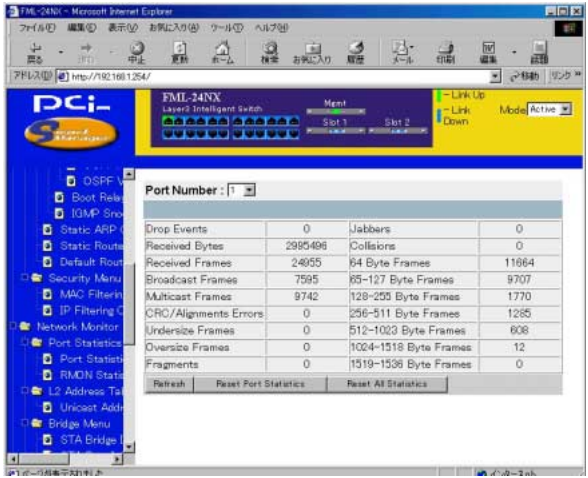
「Jabbers」
1518オクテットより長い受信フレーム（ただしフレーミングビットを除き、FCSオクテットを含む）のうち、FCSまたはアライメントエラーを持ったものの総計です。

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。

◎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。



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破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。
128-255 Byte Frames　: (同上)
256-511 Byte Frames　: (同上)
512-1023 Byte Frames　: (同上)
1024-1518 Byte Frames : (同上)
1519-1536 Byte Frames : (同上)

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。

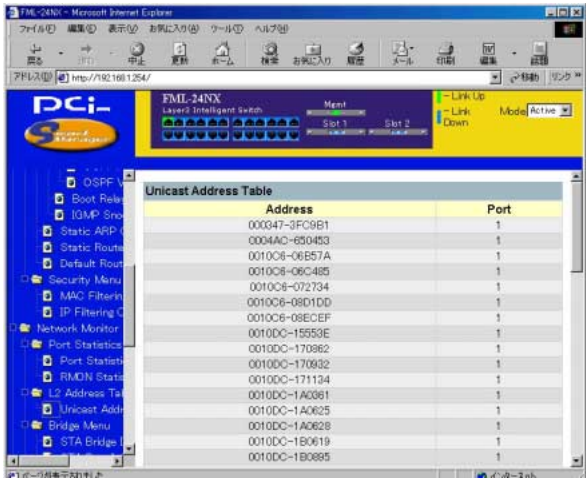
「Refreshボタン」
最新のスタティクス情報に更新します。

「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。



「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。

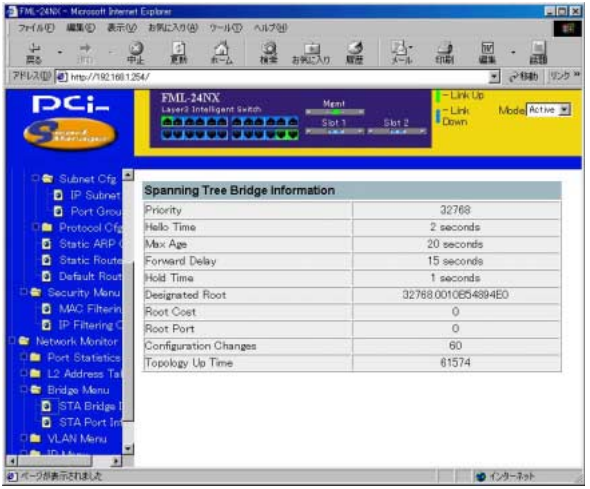
「Status」
アドレスステータスを表示します。

「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

◎ 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。

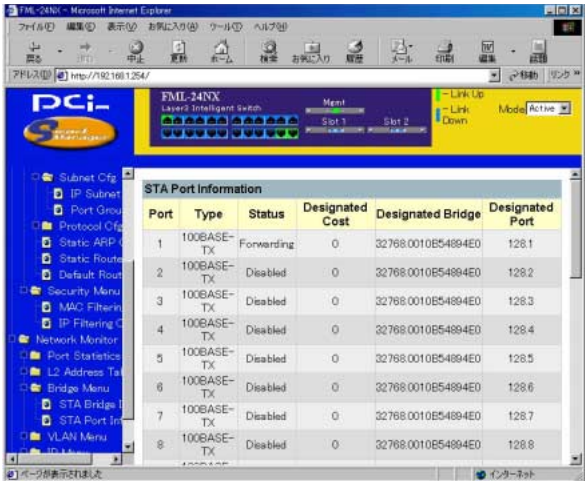
「Root Cost」
本製品上のルートポートからルート機器までのパスコストです。

「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



「Status」
スパ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ステート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。

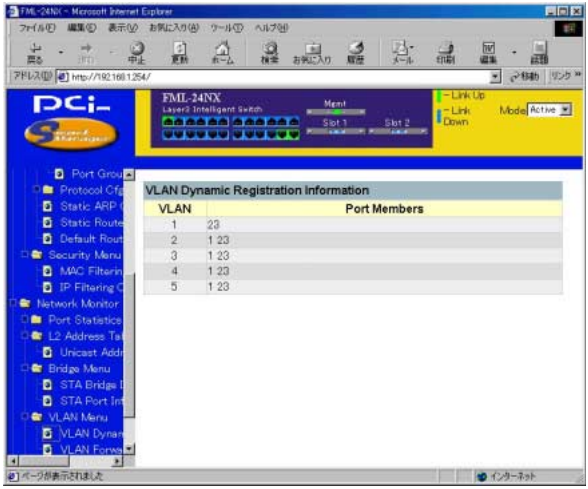
「Designated Bridge（ID）」
このポートがスパニングツリーのルートに到達するため、途中通過しなければならない機器のプライオリティおよびMACアドレスを表示します。

「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 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。

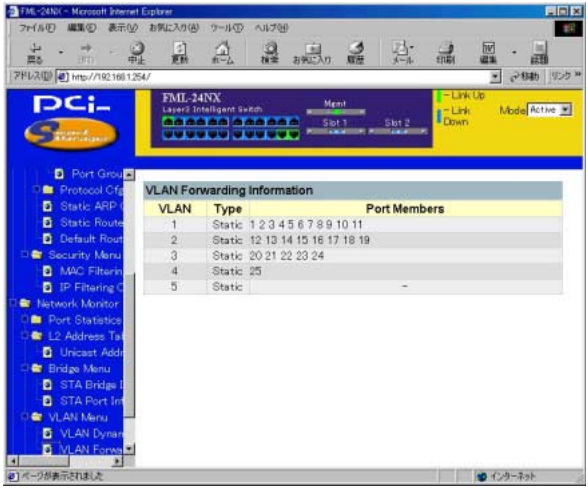
◎VLAN Dynamic Registration Information

GVRPにより自動的に学習されたポートを表示します。



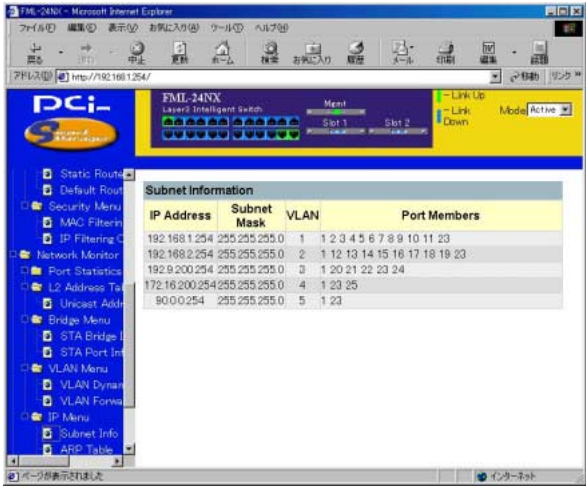
◎VLAN Forwarding Information

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。



◎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」

本製品上のIPインターフェースのアドレスです。

「Subnet Mask」

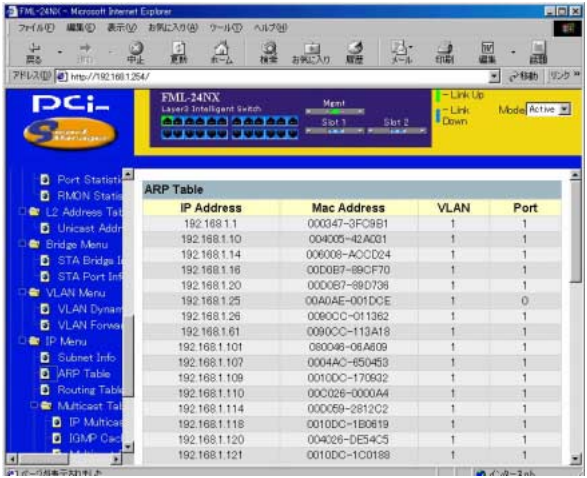
サブネットマスクが表示されます。

「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。

◎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」

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。

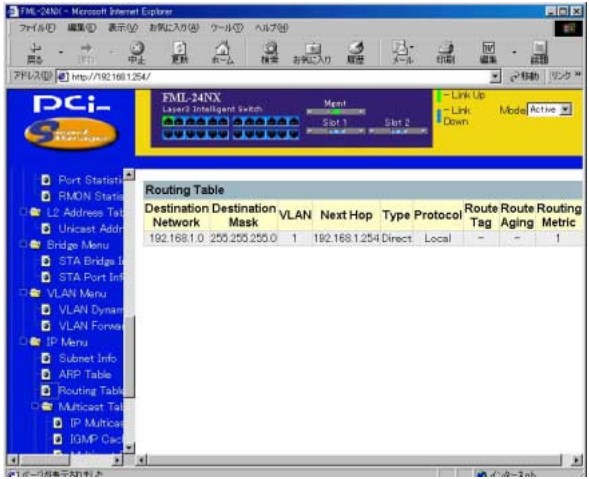
「Port」

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。

◎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。



「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。

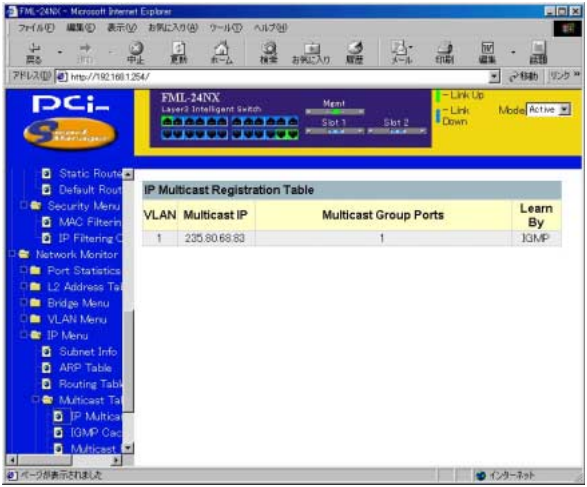
Direct　：直接接続されているサブネットワーク
Indirect　：リモートIPサブネットワークまたはリモートホストアドレス
Myself　：特定IPサブネットワーク上のスイッチIPアドレス
Bcast　：サブネットワーク・ブロードキャストアドレス
Mcast　：IPマルチキャストアドレス

「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

◎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。



「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」

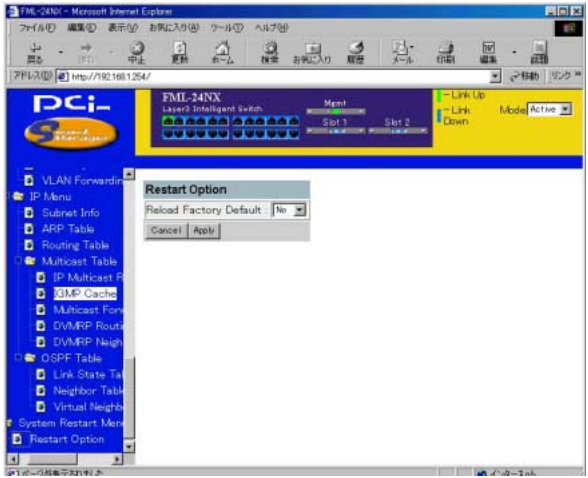
表示されたVLANグループに所属するポートが表示されます。

「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。

■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、ネットワーク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、ポートは自分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の識別
- 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識別、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 識別（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を使用してフレームのブロードキャストドメインを識別します。

「ラーニング」

VLANの識別が完了すると、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＜desitination 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＜desitination 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分別」
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（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 address，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は分布式の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。

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

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です。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。
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になります。ただし本製品を初めてマルチレイヤモードに設定した時点ではまだルーティングに必要な機能が設定されていません。従来のルータ同様、使用開始前に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、レイヤ2スイッチング機能によりスイッチされます。またレイヤ3スイッチング機能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、各ポートはすべてタグ無しパケットを送信します。VLANグループが重複するような設定をした場合、レイヤ3スイッチング機能が正しく動作しない原因になります。また同一VLAN内で通信を行うためには、VLAN内の全てのポートを同じPVIDを設定する必要があります。

6. IPスイッチング

IPスイッチングには、レイヤ2・レイヤ3両方の処理が必要になります。以下、対応し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、パケットはルータ機能を必要とすることなく直接送信先に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パケット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、パケットは次の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プロトコルを使用し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です。

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）するだけで自身の周辺のルータを検出できます。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、広告の定期送信を待たず、即座に広告を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用して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。

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、送信コストの大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用し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
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
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
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）経路広告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用し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、ディレイ、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用して、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用し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、本製品は簡単に設定が可能なVLANを使用し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で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を使用して、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VAN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、これらの間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る場合は、本製品のレイヤ3ルーティングを使用して異なる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。

20. マルチキャストフィルタリング

マルチキャスティングでは、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ティング例は、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し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ティ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対してのみ転送されます。

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パケット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パケットをそのまま監視し、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になります。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用して、インターネット上でのIPマルチキャスティングを実現します。

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を使用して送信元をルートとしたマルチキャスト配送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じ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、Weigted 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タグ構造を使用して、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GETNEXT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ブラウザを使用し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（除去）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、基本的なリ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。

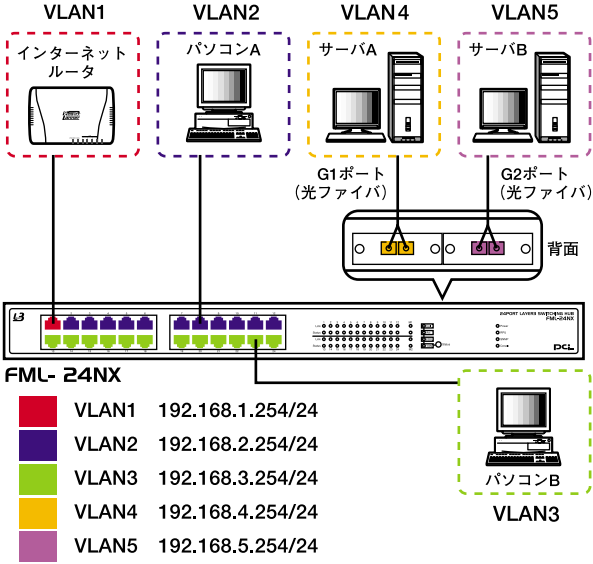
◎Statistics
ネットワーク上の一般的なエラーおよび全体のトラフィック速度を監視するのに必要なすべてのツールを備えています。表示する情報には、帯域幅の利用状況、最大利用度、パケットの種類、エラー、コリジョンおよびパケットサイズの分布などが含まれます。
◎History
ネットワーク利用、パケットタイプ、エラーおよびコリジョンの記録を作成します。断続的に発生する問題を分析するには、(ネットワーク上の) 動作の過去の記録が必要となります。履歴データはまた、ネットワーク上の動作の通常/基準レベルを割り出す際に使用されます。基準値を割り出すことにより、多大なトラフィック量やブロードキャストストーム、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用し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. レイヤ3アプリケーション

本製品を使用したベーシックなネットワークを構成する場合の設定例を説明します。
設定例はあくまでも参考構成です。また設定を明記していない項目は全てMultiLayrモード時のデフォルトです。



◎インターネットルータ

IP：192.168.1.1

Subnet：255.255.255.0

◎パソコンA
IP：192.168.2.100
Subnet：255.255.255.0

◎パソコンB
IP：192.168.3.100
Subnet：255.255.255.0

◎サーバーA
IP：192.168.4.100
Subnet：255.255.255.0

◎サーバーB
IP ：192.168.5.100
Subnet：255.255.255.0

■FML-24NX設定
●VLAN1 Port1
PVID 1
IP：192.168.1.254
Subnet：255.255.255.0

●VLAN2 Port2～12
PVID 2
IP：192.168.2.254
Subnet：255.255.255.0

●VLAN3　Port13～24
PVID 3
IP：192.168.3.254
Subnet：255.255.255.0

●VLAN4　PortGi1
PVID 4
IP：192.168.4.254
Subnet：255.255.255.0

●VLAN5　PortGi2
PVID 5
IP：192.168.5.254
Subnet：255.255.255.0

●Default Route
IP：192.168.1.1
Subnet：255.255.255.0

●RIP
Send Type RIP2 Broadcast
Receive Type RIP2

付録B. トラブルシューティング

■症状：パスワードを忘れた/紛失してしまった

◎対処

・弊社テクニカルサポートまでご連絡ください。

■症状：シリアルポートを使用してコンソールにアクセスしているがログインスクリーンが表示されないまたはキー入力が効かない。

◎対処

・使用されているターミナルユーティリティのシリアルポートの設定を確認してください。

■症状：シリアルポートを使用してコンソールにアクセスしているがキーボードの矢印キーが効かない。

◎対処

・Windows標準のターミナルユーティリティでは矢印キーを使用することが出来ません。ユーティリティをアップデートするか他のユーティリティを使用してください。

■症状：設定した内容が正しく動作に反映されない。

◎対処

・設定を追加、削除または変更した場合は必ず各設定スクリーン上のApplyを実行して設定内容を更新してください。

■症状：デフォルトルートのIPアドレスが表示されない。

◎対処

・デフォルトルートが接続されているポートのリンクを確認してください。ポートのリンクが確立していない場合、本製品はデホルトルートのIPアドレスを表示しません。

■症状：スタティックでルートを入力したがルーティングテーブルに表示されない。

◎対処

・スタティックで設定したポートのリンクを確認してください。ポートのリンクが確立していない場合、本製品はスタティックルートのIPアドレスを表示しません。

■症状：ルーティング出来ない。

◎対処：

・コンピュータのIPアドレスが接続先のVLANグループのIPインターフェィスと同一のグループに設定されているか確認してください。

・コンピュータのデフォルトゲートウェイアドレスに接続先のVLANグループのIPインターフェィスアドレスが指定されていることを確認してください。

■症状：Multi Layreモードに設定した場合にタグを付加したパケットを送信するための設定ができない。

◎対処：

・本製品はMulti Layreモード時にパケットにタグを付加して送信することが出来ません。またタグ付のパケットを受信してもタグをフィルタリングして送信します。

■症状：ルーティングは出来るが同一VLAN内の通信ができない。

◎対処：

・ポートのPVID（ポートVID）が所属しているVLANグループのVIDと同じ番号になっているかどうかを確認してください。

■症状：ルーティングが不安定だ。

◎対処：

・Multi Layreモード時のVLANのオーバライド（ポートが複数のVLANに属している状態）はルーティングが不安定になる原因になります。

■症状：Pingを実行して異なるサブネットと通信テストをすると最初のリプライが遅い。

◎対処：

・本製品はハードウェアルーティング処理によりワイヤースピードでのルーティングが可能ですが送信先のネットワーク機器のIPアドレスがルーティングテーブル上に存在しない場合は、アドレス検索のために最初のパケット処理に遅れが生じます。

付録C ファームウェアアップデートと設定ファイルのアップロード/ダウンロード

■シリアルポート経由でファームウェアを更新する

本製品のシリアルポートにお使いのコンピュータを接続し、Xmodemプロトコル対応の端末インターフェースパッケージを使用することにより、本製品のファームウェアを更新することが可能となります。

1. Restart Systemコマンドを実行してシステムをリセットします。もしくは、電源コードをコンセントから外して5秒ほど待ち、またコードを接続してください。本製品はこの方法でもリセット可能です。
2. システムの初期化スクリーンが以下のように表示されますので、Dキーを押してファームウェアのダウンロードを行ってください。またこのとき、コードの種類も r （Runtime image）か d（Diagnostic image）のいずれかを選択してください。
3. ボーレートを115200bpsに変更してEnterキーを押すとダウンロードが有効となります。お使いのターミナルエミュレーションプログラム上で、ダウンロードするファイルを選択し、プロトコルをXmodemに設定してダウンロードを開始してください。

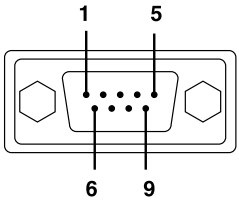
注意　●Windows用ハイパーターミナルをお使いの場合は、いったん切断（切断アイコンを挿入）してボーレートを設定してから再度接続（接続アイコンを挿入）してください。　●ダウンロードファイルは、バイナリファイルかイメージファイルを指定してください。これら以外のファイル形式は本製品で受け付けられないようになっています。

4. ファイルのダウンロードが完了すると、端末画面には以下のような情報が表示されます（下図参照）。Enterキーを押して固定メモリにダウンロードし、ボーレートをまた19200に戻してください。次にEnterキーを押して最新ファームウェアを解凍し、再度Enterキーを押してログオンスクリーンを表示してください。

付録D. コネクタとピンアサインについて

●コンソールポートのピンアサイン設定

本製品背面上のDB-9シリアルポートを使用して本製品と接続し、帯域外コンソール設定が行えます。製品内蔵のメニュー式設定プログラムは、ターミナルまたはターミナルエミュレーションプログラムが実行可能なPCからアクセス可能なほか、モデム接続経由で遠隔地からも接続できるようになっています。以下に、上記シリアルポートに接続する際使用されるピンアサインを示します。



図D-1. DB9 ポートピンアサイン

FML-24側	コンピュータ側
D-sub9ピンオス	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D-1 シリアルケーブルのピンアサイン

付録E 仕様

＜最大ポート数＞
24

＜ポート（100BASE-TX）＞
24

＜ポート（1000BASE-SX、LX、T拡張用）＞
最大2ポートまで拡張可能

＜Autonegotiation（NWAY）＞
全ポート

＜AutoMDI＞
全ポート

＜LEDインディケータ＞
Link，Status，Col.Speed，FDX，Speed，Power，RPU，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＞
9.6Gbps

＜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＞
4MB

＜MAC アドレス＞
32K

＜IP アドレス＞
64k

＜フローコントロール＞
半二重：バックプレッシャー
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 を構築可能

＜最大IP サブネット数＞
32 までのIP サブネットグループを構築可能

＜プライオリティ対応＞
2‐Level （IEEE 802.1p 準拠）

＜MIB＞
MIB

＜RMON＞
1、2、3、9 （Statistics，History，Alarm，Event）

＜SNMP＞
対応

＜スパニングツリー＞
対応

＜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 × 285 × 44 mm

＜重量＞
3.85kg

＜消費電力＞
60W

＜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 1

＜安全規格＞
cUL

付録F.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用してで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トポロジ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）内に格納されるています。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。

付録G 工場出荷設定

＜機能＞
初期設定値

＜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

＜Autonegotiation＞
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＞
19200ボーレート、8ビット、ストップビット1、パリティチェック無し、ハンドシェイク無し

＜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＞
優先設定た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