



**USER'S  
MANUAL**

インテリジェントスイッチングハブ

**FMX-0248K**

**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う誤動作や火災につながるおそれがあります。



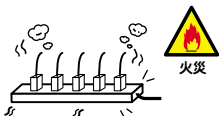
### 通気口をふさがないで！

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！

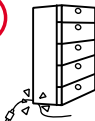
製品内部に液体や異物が入ると、ショートして火災が発生したり、誤動作したりする可能性があります。万一異物や液体が入ってしまった場合は、電源コードをコンセントから外して弊社サポートセンターまでご連絡ください。



## 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してください。

- コードの上に物を載せない
- 熱源の側にコードを置かない
- コードをかじる癖のあるペットは隔離する  
(かじった部分からショートし発火する危険があります)



## 設置・保管場所をもう一度確認して！

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

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



## おねがい

本製品のお手入れ

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

# 目次

## 第1章 はじめに

- 1. 概要 ..... 7
- 2. 特長 ..... 8
- 3. 梱包内容の確認 ..... 9
- 4. 各部の名称 ..... 10

## 第2章 クイックインストール

- 1. インストールの手順 ..... 20
- 2. 設置場所について ..... 21
- 3. 本製品の設置 ..... 21
- 4. 電源ケーブルの接続 ..... 24
- 5. 冗長化電源ユニットの接続 ..... 25
- 6. miniGBICモジュールの接続 ..... 30
- 7. 本製品とネットワーク機器の接続 ..... 32

## 第3章 スイッチの管理

- 1. 設定オプション ..... 35
- 2. シリアルポートとの接続 ..... 36
- 3. Telnet・ウェブブラウザの接続 ..... 38

## 第4章 ウェブインターフェース

- 1. ウェブインターフェースについて ..... 39
- 2. ウェブインターフェースの操作 ..... 39
- 3. ウェブインターフェースのログイン ..... 40
- 4. メニュー階層 ..... 41
- 5. Home ..... 44
- 6. ポート画面 ..... 45
- 7. System Information ..... 46
- 8. IP ..... 48
- 9. Passwords ..... 50
- 10. Radius ..... 51
- 11. Firmware ..... 52
- 12. Configuration ..... 57

13. Reset	62
14. Bridge Extension	63
15. Switch Information	64
16. Port Information	66
17. Trunk Information	68
18. Port Configuration	70
19. Trunk Configuration	73
20. Port Broadcast Control	76
21. Mirror	77
22. Static Addresses	79
23. Dynamic Addresses	81
24. Address Aging	83
25. STA Information	84
26. STA Configuration	86
27. STA Port Information	89
28. STA Trunk Information	91
29. STA Port Configuration	93
30. STA Trunk Configuration	96
31. VLAN Base Information	99
32. VLAN Current Table	100
33. VLAN Static List	102
34. VLAN Static Table	104
35. VLAN Static Membership by Port	106
36. VLAN Port Configuration	108
37. VLAN Trunk Configuration	111
38. Port Priority Configuration	114
39. Trunk Priority Configuration	116
40. Traffic Classes	117
41. Queue Scheduling	119
42. IP Precedence/DSCP Priority Status	120
43. IP Precedence Priority	121
44. IP DSCP Priority	122
45. IP Port Priority Status	124
46. IP Port Priority	125
47. LACP Configuration	127

48. Trunk Configuration	129
49. SNMP Configuration	131
50. IGMP Configuration	134
51. Multicast Router Port Information	136
52. Static Multicast Router Port Configuration	137
53. IP Multicast Registration Table	139
54. IGMP Member Port Table	140
55. Port Statistics	142

## 第5章 技術解説

1. レイヤ2スイッチ ( Layer 2 Switch )	150
2. マルチキャストスイッチング ( Multicast Switching )	153
3. スパニングツリーアルゴリズム ( Spanning Tree Algorithm : STA )	154
4. レイヤ3スイッチ ( Layer 3 Switch )	156
5. IPスイッチング	156
6. ICMP Router Discovery	159
7. ルーティングプロトコル	160
8. RIP ( Routing Information Protocol ) / RIP-2動的ルーティングプロトコル	161
9. OSPF v2動的ルーティングプロトコル ( Open Shortest Path First )	163
10. 非IPルーティング	171
11. VLAN	171
12. VLANへのポート割り当て	173
13. ポートオーバーラッピング	174
14. ポートベースVLAN	174
15. 自動VLAN登録 : GVRP ( GARP VLAN Registration Protocol )	175
16. タグ付/タグ無しフレームの転送	176
17. VLANグループの接続	178
18. マルチキャストフィルタリング	179
19. IGMPスヌーピング ( IGMP Snooping )	180
20. IGMP ( Internet Group Management Protocol )	181
21. GMRP ( GARP Multicast Registration Protocol )	182
22. DVMRP ( Distance-Vector Multicast Routing Protocol )	183
23. CoS ( Class-of-Service )	184
24. SNMPコミュニティストリング	184
25. ユーザー名およびパスワード	184
26. MACアドレスフィルタ	185

27. IPアドレスフィルタ	185
28. SNMP管理ソフトウェア ( Simple Network Management Protocol )	185
29. リモート監視 : RMON ( Remote Network Monitoring )	186
付録A 管理ユーティリティで設定できる項目	188
付録B トラブルシューティング	191
付録C 用語集	193
付録D 工場出荷設定	205
付録E 仕様	206

#### 《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 Ver.1.0

No.PCM-02-09-JF-FMX-0248NX

# 1.はじめに

## 1.概要

FMX-0248KはIEEE 802.3 10BASE-T、IEEE 802.3u 100BASE-TX、IEEE 802.3ab 1000BASE-T規格に準拠したラックマウントサイズのギガビットインテリジェントスイッチングハブです。AutonegotiationおよびAuto MDI/MDI-Xに対応したRJ-45 STPポートを48ポートと、IEEE 802.3z 1000BASE-SX/LX対応miniGBICポートとIEEE 802.3ab 1000BASE-Tに対応したRJ-45 STPポートのコンポポートを2ポート装備しています。

本製品はIEEE802.1Q VLAN機能、IEEE802.1pプライオリティ制御、IEEE802.1dスパニングツリー、IEEE802.3ad Link Aggregationに対応しています。これらの規格に準拠したハブであれば他メーカーのハブとの接続も可能です。VLAN機能はIEEE802.1Q VLANで最大255グループまで構成することができます。

ネットワークの管理は、SNMP、ウェブベースマネジメント、Telnet、RS-232Cコンソールなどの機能で実現できます。また、RMONを使ったネットワークの監視機能も備え、遠隔からの通信状況の把握ができ、システム管理者の負担を軽減します。



## 2.特長

IEEE 802.3 10BASE-T、IEEE 802.3u 100BASE-TX、IEEE 802.3ab 1000BASE-T規格準拠

100BASE-TX、10BASE-TのRJ-45 STPポートを48ポート装備  
miniGBIC、1000BASE-Tコンボポートを2つ装備

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

AutoMDI/MDI-X機能によってケーブルの結線タイプ(ストレート/クロス)自動認識

合計9.6Gbpsの帯域幅に対応

MACアドレステーブルを装備し、最大8000個のMACアドレス  
を自動学習可能

64Mバイトの packetsバッファ装備

フロー制御対応(全二重:IEEE 802.3x/半二重: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

IEEE 802.1Q VLANに準拠(最大255グループ)

IEEE 802.1Q/p準拠により4レベルのプライオリティ管理

IEEE 802.1dスパンニングツリー準拠

IEEE 802.1ad LinkAggregationに準拠。

2/3/4ポートTrunk対応。最大6グループ作成可能。

IGMP(v1/v2) Snooping対応

SNMP、ウェブ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

P-Bridge、Q-Bridge、Ether-Link、Interfaces、RMON(1,2,3,9)とSNMP-MIB2、EntityMIB対応

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

TFTPサーバでファームウェアのアップデート可能  
ネットワーク管理用のシリアルポート装備( D-SUB9ピンメス )  
MACアドレスフィルタリング対応  
冗長化電源対応

### 3. 梱包内容の確認

パッケージは、以下の付属品が含まれます。

- ・ FMX-0248K本体
- ・ 設定用RS-232Cストレートケーブル( D-SUB9ピンオス/メス )
- ・ 電源ケーブル
- ・ ラックマウント用金具 x 2個
- ・ ネジ
- ・ ゴム足 x 4個
- ・ ユーザーズマニュアル( CD-ROM )
- ・ 保証書

付属品が足りないときは、販売店または弊社テクニカルサポートまで連絡してください。

## 4. 各部の名称

### 前面パネル

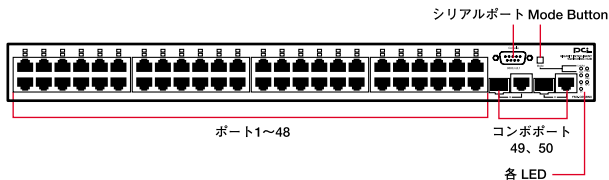


図1-1 前面パネル

#### 【ポート1～48】

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。

#### 【コンボポート49、50】

miniGBICまたは1000BASE-Tツイストペアケーブル接続用のコンボポートです。

#### 【シリアルポート】

コンピュータを付属のRS-232Cケーブルを使い接続します。

#### 【Mode Button】

Port Status LEDに表示させる項目を選択します。解除するとLink/Act、押すとFDXになります。

## 【Mode LED】

Port Status LEDに表示させる項目を選択します。解除するとLink/Act、押すとFDXになります。

LED	状態	記述
FDX	消灯 点灯(緑)	電源が入っていないか、Mode Buttonが解除されています。 電源が投入されており、Mode Buttonが押されています。
Link/Act	消灯 点灯(緑)	電源が入っていないか、Mode Buttonが押されている。 電源が投入されており、Mode Buttonが押されています。

表1-1 Mode LED

## 【System LED】

システム上の状態を表すLEDです。

LED	状態	記述
Power	消灯 点灯(緑)	電源がOFFの状態 電源がONの状態
Diag	消灯 点滅(緑) 点灯(緑)	異常が 電源が投入され、自己診断モードに入っている時または自己診断モード中エラーが検出された時に点滅します。 自己診断モードが終了後、正常に起動しています。
RPU	消灯 点灯(緑)	

表1-2 System LED

## 【Port Status LED】

ポートごとの状態を表すLEDです。

LED	状態	記述
Port Status LED(1～48)	消灯 [ Mode Buttonを押している状態 ]	電源が供給されていないか、ポートのリンクが確立していないまたは、100/10Halfで接続しているときに消灯します
	点灯(緑) [ Mode Buttonを押している状態 ]	100Fullで接続しているときに点灯します
	点灯(赤) [ Mode Buttonを押している状態 ]	10Fullで接続しているときに点灯します
	消灯 [ Mode Buttonを解除している状態 ]	電源が供給されていないか、ポートのリンクが確立
	点灯(緑) [ Mode Buttonを解除している状態 ]	100Mbpsでポートのリンクが確立すると点灯します
	点滅(緑) [ Mode Buttonを解除している状態 ]	100Mbpsでポートがデータの送受信中に点滅します
	点灯(赤) [ Mode Buttonを解除している状態 ]	10Mbpsでポートのリンクが確立すると点灯します
	点滅(赤) [ Mode Buttonを解除している状態 ]	10Mbpsでポートがデータの送受信中に点滅します

表1-3-1 Port Status LED

LED	状態	記述
Port Status LED(49~50)	消灯 [ Mode Buttonを押している状態 ]	電源が供給されていないか、ポートのリンクが確立していないまたは、10Full・100/10Halfで接続しているときに消灯します
	点灯(緑) [ Mode Buttonを押している状態 ]	1000/100Fullで接続しているときに点灯します
	消灯 [ Mode Buttonを解除している状態 ]	電源が供給されていないか、ポートのリンクが確立
	点灯(緑) [ Mode Buttonを解除している状態 ]	1000Mbpsでポートのリンクが確立すると点灯します
	点滅(緑) [ Mode Buttonを解除している状態 ]	1000Mbpsでポートがデータの送受信中に点滅します
	点灯(橙) [ Mode Buttonを解除している状態 ]	100/10Mbpsでポートのリンクが確立すると点灯します
	点滅(橙) [ Mode Buttonを解除している状態 ]	100/10Mbpsでポートがデータの送受信中に点滅します

表1-3-2 Port Status LED

## 背面パネル

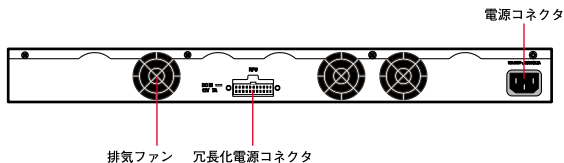


図1-2 背面パネル

### 【電源コネクタ】

電源ケーブルを接続します。

### 【排気ファン】

本製品内の熱を排出するファンです。

本製品のファン取り付け口にほこりなどがたまらないように注意してください。十分な冷却ができないときは、誤動作、故障などの原因になります。

### 【冗長化電源コネクタ】

冗長化電源ユニット (FMK-RPU) を接続します。

## 裏面ステッカー

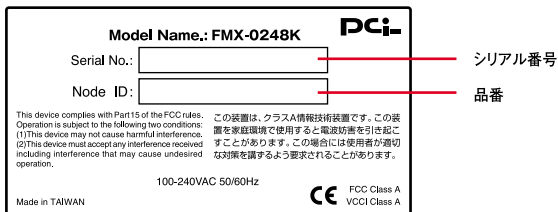


図1-3 裏面ステッカー

### 【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。ユーザ登録時または製品故障などでサポートを受けるとき必要になります。

### 【Node番号】

本製品のMACアドレスです。製品外箱に記載されているものと同じ番号です。ユーザ登録時または製品故障などでサポートを受けるとき必要になります。



## 冗長化電源ユニット(FMK-RPU) 前面パネル

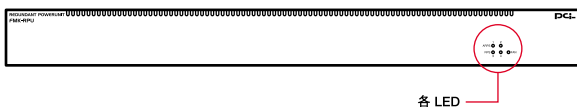


図1-4 冗長化電源ユニット前面パネル

LED	状態	記述
RPS	点灯 (緑)	電源がONの状態。 本体 (FMX-0248K) と接続し正常に動作しています。
	点滅 (緑)	電源がONの状態。 本体 (FMX-0248K) と接続が確立していない状態
	消灯	電源がOFFの状態。または異常により停止しています。
FAN	点灯 (緑)	排気ファンが正常に動作しています。
	点滅 (赤)	排気ファンの異常停止等の故障が発生しています。
	消灯	電源がOFFの状態。

表1-4 RPSおよびFAN LED

## 背面パネル



図1-5 冗長化電源ユニット背面パネル

### 【電源コネクタ】

電源ケーブルを接続します。

### 【排気ファン】

冗長化電源ユニット内の熱を排出するファンです。

重要:本製品のファン取り付け口にほこりなどがたまらないように注意してください。十分な冷却ができないときは、誤動作、故障などの原因になります。

### 【冗長化電源コネクタ】

FMX-0248Kに接続します。

## 冗長化電源ユニット（FMK-RPU）専用ケーブル

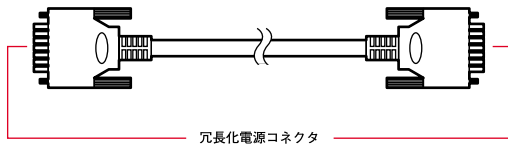


図1-6 冗長化電源ユニット専用ケーブル

### 【冗長化電源コネクタ】

FMX-0248Kまたは冗長化電源ユニットに接続します。

## miniGBIC ( miniGBIC-SXC/LXC )



図1-7 miniGBIC

### 【LCポート】

1000BASE-SXまたは1000BASE-LXファイバケーブル接続用のLCポートです。

### 【接続コネクタ】

miniGBICコネクタに接続します。

## 2. クイックインストール

### 1. インストールの手順

FMX-0248K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へ設置して使ってください。他のハブとカスケード接続するときは、19インチラックに設置して使うことをおすすめします。本製品のインストールの概要は、以下のとおりです。

1. 本製品をパッケージから取り出す
2. 本製品本体を設置する
3. 電源ケーブルを接続する
4. 各コンピュータ、ハブおよびスイッチと接続する
5. 冗長化電源ユニットの接続
6. miniGBICモジュールの接続

## 2.設置場所について

本製品の設置は、必ず以下の点を守ってください。

- ・湿気の多い場所に設置しない
- ・チリやほこりの多い場所に設置しない
- ・直射日光のあたる場所や温度の高い場所に設置しない
- ・設置する周囲の隙間を空ける

本製品のファン取り付け口にほこりなどがたまらないように注意してください。十分な冷却ができないときは、誤動作、故障などの原因になります。

1、2か月に1度点検し、ほこりがたまっているようでしたら掃除機などで取り除いてください。

## 3.本製品の設置

本製品は、デスクトップなどの平らな場所に設置して使ってください。他のハブとカスケード接続するときは、19インチラックへ設置して使うことをおすすめします。

本製品の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設置してください。また、本製品のファン取り付け口にほこりなどがたまらないように注意してください。十分な冷却ができないときは、誤動作、故障などの原因になります。

## デスクトップへの設置

デスクトップなどの平らな場所へ設置する手順です。

- 1.本製品の底面の4隅に、付属のゴム足を取り付けます。
- 2.本製品を平らな場所に設置します。

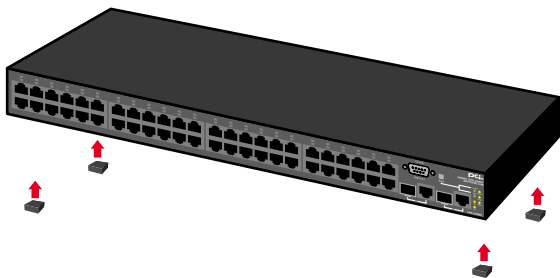


図2-1 ゴム足の取り付け図

## ラックへの取り付け

本製品を19インチラックに取り付ける手順です。プラスのドライバーと19インチラックに付属しているマウント用ネジを4つ用意してください。

- 1.本製品の底面にゴム足を取り付けているときは、すべてのゴム足を取り外します。
- 2.本製品の側面にある、ラックマウント用のネジ穴の位置を確認します。
- 3.本製品の付属のネジを使い、ラックマウント用金具を側面に取り付けます。

- 4.本製品をラック内に配置します。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つ使い、ラックマウント用金具に差し込んで固定します。

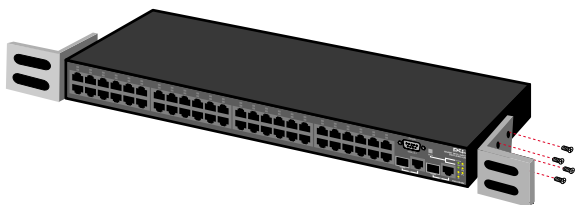


図2-2 ラックマウント用金具の取り付け

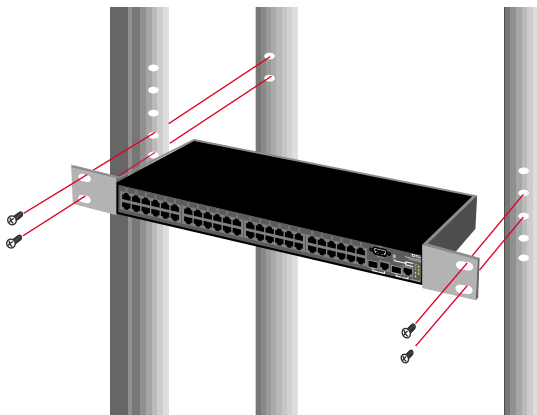


図2-3 ラックマウント用金具をラックに固定



## 4.電源ケーブルの接続

電源ケーブルを取り付ける手順です。以下の手順で確実に接続してください。

- 1.電源ケーブルを本製品背面の電源コネクタに接続します。
- 2.電源ケーブルの3芯タイプのプラグを、アース対応した電源コンセントに接続します。
- 3.Power LEDが点灯していれば正常です。

本製品は電源投入時に自己診断テストおよび設定の読み込みをします。  
このため、電源投入から使用開始までしばらく時間がかかります。

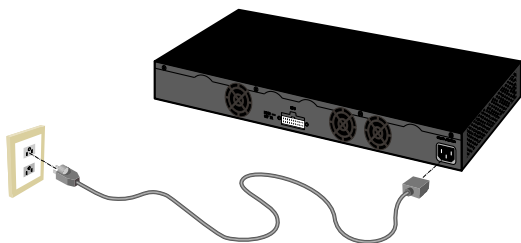


図2-4 電源ケーブルの接続方法

## 5.冗長化電源ユニットの接続

本製品に冗長化電源ユニット( FMK-RPU )を接続する手順です。

本製品で使用できる冗長化電源ユニットは [ FMK-RPU ] だけです。他の冗長化電源ユニットを使用しないでください。

本製品( FMX-0248 )を一台のみ接続する

- 1.本製品の電源を切ります。
- 2.本製品の冗長化電源コネクタに冗長化電源用ケーブルのコネクタを接続します。

**重要** コネクタを接続するときは「カチッ」と音がするまで置くに押し込んでください。コネクタの接続が不十分だと漏電する恐れがあります。

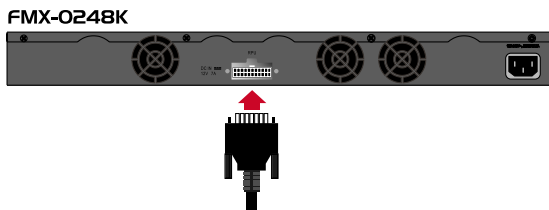


図2-5 本体へのコネクタ取り付け

- 3.冗長化電源用ケーブルのコネクタのもう片方を冗長化電源ユニットの冗長化電源コネクタに接続します。

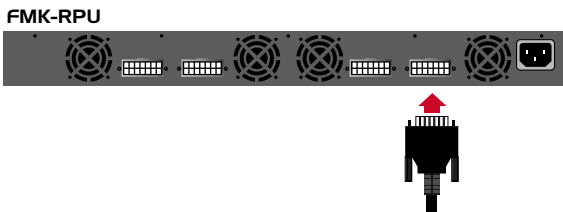


図2-6 冗長化電源ユニットへのコネクタ取り付け

- 4.本製品の電源を投入します。
- 5.電源ケーブルを冗長化電源ユニット背面の電源コネクタに接続します。

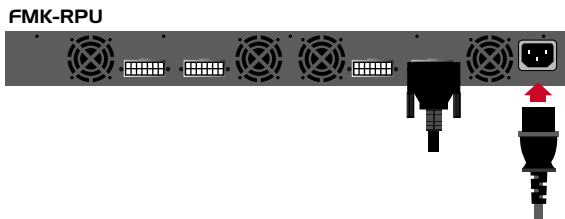


図2-7 冗長化電源ユニットの電源ケーブル接続方法

- 冗長化電源ユニットに接続した電源ケーブルの3芯タイプのプラグを、アース対応した電源コンセントに接続します。
- 冗長化電源ユニット前面のRPS LEDが点灯（緑）になっていることを確認します。



図2-8 RPS LEDの点灯（緑）

冗長化電源ユニットがすでに稼動している時に本製品 (FMX-0248) を追加する

1. 稼動している本製品 (FMX-0248) が冗長化電源ユニットを使用せず主電源で稼動していることを確認します。
2. 冗長化電源ユニットの電源を切ります。
3. 追加する本製品の冗長化電源コネクタに冗長化電源用ケーブルのコネクタを接続します。

**重要** コネクタを接続するときは「カチッ」と音がするまで置くに押し込んでください。コネクタの接続が不十分だと漏電する恐れがあります。

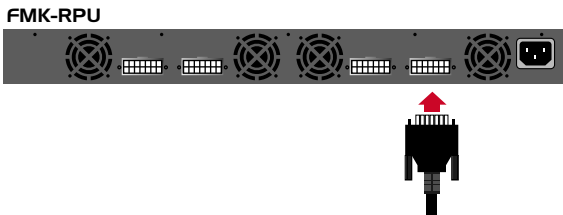


図2-9 本体へのコネクタ取り付け

4. 冗長化電源用ケーブルのコネクタのもう片方を冗長化電源ユニットの冗長化電源コネクタに接続します。

## FMK-RPU

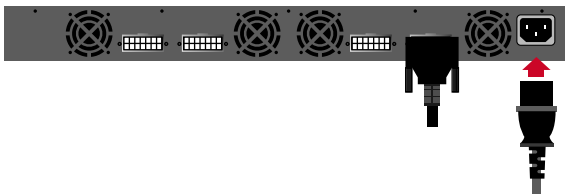


図2-10 冗長化電源ユニットへのコネクタ取り付け

- 5.追加する本製品の電源を投入します。
- 6.冗長化電源ユニットの電源を投入します。
- 7.冗長化電源ユニット前面のRPS LEDが点灯(緑)になっていることを確認します。



図2-11 RPS LEDの点灯 (緑)

## 6.miniGBICモジュールの接続

本製品のコンポポートにminiGBICモジュールを接続する手順です。

miniGBICモジュールを接続する時は、「49」,「50」ポートと兼用になるため、miniGBICモジュールのコネクタを使用しているときは「49」,「50」ポートの1000Base-Tのコネクタは使用できません。

- 1.本体の「49」,「50」ポートを使用しているときは使用していない状態にします。
- 2.「49」,「50」ポートのminiGBICコネクタにminiGBICモジュールを奥まで差し込みます。

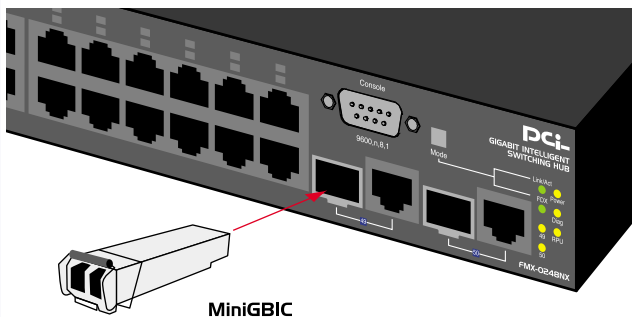


図2-12 miniGBICモジュールの取り付け位置

### 3. シリアル接続画面でminiGBICコネクタの自己診断が開始されます。

```
=====
Username : admin
```

```
Password :
```

```
CLI session with the FMX-0248K is opened.
```

```
To end the CLI session, enter [ Exit ].
```

```
Console#
```

```
Console#
```

```
GBIC 1 be removed!!
```

```
GBIC status is ff
```

```
GBIC 0 be inserted!!
```

```
GBIC status is f8
```

```
Serial transceiver : [ SFP ] ...
```

```
Gigabit ethernet Compliance Codes : [ 1000BASE-SX ] ...
```

```
GBIC 0 Vendor Name : FINISAR CORP.
```

```
GBIC 0 Vendor Part Number : FTRJ-8519-7D
```

```
GBIC 0 Vendor Revision Number :
```

```
GBIC 0 Vendor Serial Number : H11C3JC
```

```
Console#
=====
```



## 7.本製品とネットワーク機器の接続

本製品のポートとコンピュータのLANアダプタまたはハブなどのネットワーク機器を接続する手順です。接続先のネットワーク機器の通信速度に合ったLANケーブルを用意してください。

### RJ-45ポートを利用したネットワーク機器との接続

本製品のポートは全てAutoMDI/MDI-Xに対応していますので、LANケーブルの結線タイプを自動で認識できます。接続先のネットワーク機器のポートに依存することなく、ストレートまたはクロス結線のLANケーブルどちらでも使うことができます。

- 1.LANケーブルの一端を本製品のRJ-45ポートに接続します。
- 2.LANケーブルの一端をコンピュータまたはハブなどのネットワーク機器のRJ-45ポートに接続します。
- 3.接続先のネットワーク機器がAutonegotiationに対応しているとき、ポートの転送モードが自動的に設定されます。

10BASE-Tの接続はカテゴリ3以上、100BASE-TXの接続はカテゴリ5のUTPまたはSTPケーブルを使ってください。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。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ケーブル最大長は、IEEE 802.3ab 1000BASE-Tの仕様で100mと定められています。

## FMX-0248K

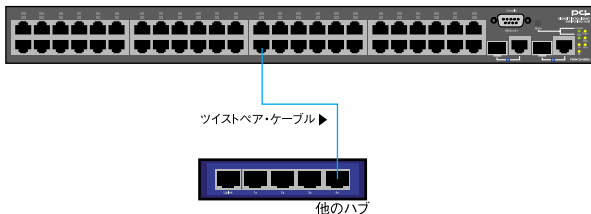


図2-9 ネットワーク機器との接続[ RJ-45 ]

ファイバーポートを利用したネットワーク機器との接続  
本製品のファイバーポートとコンピュータのファイバーコネクタ  
またはネットワーク機器のファイバーコネクタをLCコネクタ  
タイプファイバケーブルで接続します。

1. ケーブルの一端を本製品の光ファイバポートに接続し、もう一端を接続先機器の光ファイバポートに接続します。
2. ケーブルの接続は、RXとTXをそれぞれ接続します。接続が正常な時は、LinkLEDが点灯します。LinkLEDが消灯した場合は、正常に接続されていないのでコネクタの接続を確認してください。

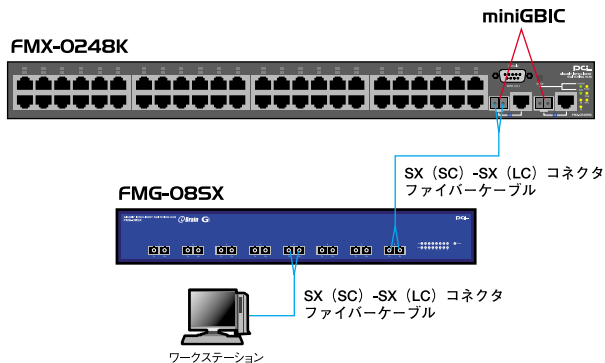


図2-10 ネットワーク機器との接続[ ファイバー ]

1000BASE-SXでのファイバケーブルの最大長は、IEEE 802.3z 1000BASE-SXは仕様で定められている550mです。1000BASE-LXでのファイバケーブルの最大長は、IEEE 802.3z 1000BASE-LXは仕様で定められている5000mです。

# 3. スイッチの管理

## 1. 設定オプション

FMX-0248Kは管理エージェントを搭載しています。管理エージェントは、SNMPを採用し、本製品の設定と管理をします。SNMPエージェントは、マネージメントモジュールのシリアルポートへコンピュータを接続、Telnet接続、またはウェブブラウザ\*から起動することができます。SNMPエージェントとSNMPマネージャを使うことで、本製品はネットワークのどのコンピュータからでも管理ができます。

SNMPエージェントは、以下の管理機能を提供します。

- ・各ポートの有効または無効を設定
- ・各ポートの通信モードを設定
- ・SNMPパラメータの設定
- ・トランクポートの設定
- ・ネットワークVLANのポート追加
- ・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およびダウンロード

■ 対応ブラウザ: Internet Explorer 4.0以降/Netscape Navigator 4.0以降

## 2.シリアルポートの接続

本製品前面のシリアルポートにコンピュータを接続し、本製品の設定および管理ができます。シリアルポートは、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またはVT-100互換のターミナルを接続します。Windows 95/98/98 SE/Me/2000/XPがインストールされたコンピュータでは、ハイパーターミナルなどの通信ユーティリティを使います。

■ *Macintoshは、本製品のシリアルポートに接続した設定はできません。*

### ターミナルユーティリティの設定

シリアルポートに接続する機器のターミナルユーティリティを、以下のように設定します。

- ・9600bps
- ・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、なしに設定
- ・Terminal Preferences でFunction、Arrow、Controlキーはすべて有効に設定

## シリアルケーブルの接続

ご利用のコンピュータにD-SUB9ピンオス型の形状をしたシリアルポートが装備されているか確かめてください。付属の設定用RS-232Cケーブルは、D-SUB9ピンのメス/メス型のコネクタ形状をしています。設定用RS-232Cケーブルを使い、本製品背面のシリアルポート(D-SUB9ピンメス)とご利用のコンピュータ(D-SUB9ピンオス)と接続します。

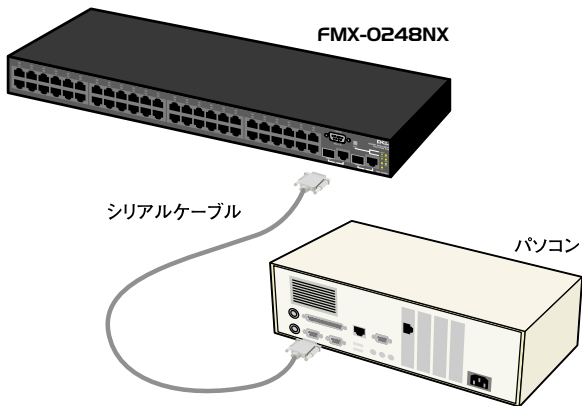


図3-1 RS232Cケーブルとの接続

### 3. Telnet・ウェブブラウザの接続

管理エージェントはTelnetまたはウェブブラウザで起動することができます。

本製品は工場出荷時状態でマネージメントIPアドレスとして「192.168.0.1/24」が設定され、ウェブインターフェースが有効に設定されているので、ネットワークに接続されたコンピュータから管理エージェントを起動できるようになります。

VLANグループは、1つのVLANグループにIPインターフェースアドレスを割り当てることができます。ネットワーク管理ステーションに接続しているポートが複数のVLANに所属しているときは、設定した1つのVLANグループからのみ管理ができます。

本製品で使えるTelnetのセッションは4セッションまでです。

本製品の設定プログラムは基本管理機能だけ設定できます。すべてのSNMP管理機能を使うときは、別途、SNMP対応のネットワーク管理ソフトウェアをご用意ください。

# 4. ウェブインターフェース

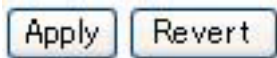
## 1. ウェブインターフェースについて

本製品は管理エージェントとして、ウェブインターフェースを搭載しています。ウェブインターフェースは、ネットワークに接続されたコンピュータのウェブブラウザ\* から起動できます。

■ \*対応ブラウザ : Internet Explorer 4.0以降/Netscape Navigator 4.0以降

## 2. ウェブインターフェースの操作

設定できる項目は、ダイアログボックス、リストボックスが用意されています。項目の設定を変更したときは、必ず画面下の [ Apply ] (適用) をクリックし、変更内容を更新します。一部の設定を除き、適用された内容はすぐに本製品に反映されます。



### 【Apply】

指定した値を管理エージェントにセットします。

### 【Revert】

指定した値を適用しません。



### 3. ウェブインターフェースのログイン

本製品に設定したIPアドレスをコンピュータのウェブブラウザから入力すると、以下のログイン画面が表示されます。工場出荷状態のユーザ名は、「admin」と「guest」が設定されています。パスワードはそれぞれ「admin」と「guest」が設定されています。「admin」は管理者権限を持ち、すべての設定・統計の読み込みと書き込みができます。「guest」はゲスト権限を持ち、設定の読み込みだけです。



パスワードは、[ Home ] [ System ] [ Passwords ](xxページ)から設定できます。

工場出荷状態では、ログイン時のパスワードは3回まで入力できます。3回目のパスワード入力を間違えたとき、接続は切断されます。

はじめて管理エージェントを使うときは、新たな管理者名とパスワードを設定し、「admin」を無効にしておくことをおすすめします。

## 4. メニュー階層

ウェブインターフェースのメニューは以下のようになっています。  
各メニューの説明は、それぞれのページから参照ください。

### Home

#### System

System Information .....	46ページ
IP .....	48ページ
Passwords .....	50ページ
Radius .....	51ページ
Firmware .....	52ページ
Configuration .....	57ページ
Reset .....	62ページ
Bridge Extension .....	63ページ
Switch Information .....	64ページ

#### Port

Port Information .....	66ページ
Trunk Information .....	68ページ
Port Configuration .....	70ページ
Trunk Configuration .....	73ページ
Port Broadcast Control .....	76ページ
Mirror .....	77ページ

## Address Table

Static Addresses	79ページ
Dynamic Addresses	81ページ
Address Aging	83ページ

## Spanning Tree

STA Information	84ページ
STA Configuration	86ページ
STA Port Information	89ページ
STA Trunk Information	91ページ
STA Port Configuration	93ページ
STA Trunk Configuration	96ページ

## VLAN

VLAN Base Information	99ページ
VLAN Current Table	100ページ
VLAN Static List	102ページ
VLAN Static Table	104ページ
VLAN Static Membership	106ページ
VLAN Port Configuration	108ページ
VLAN Trunk Configuration	111ページ

## Priority

Default Port Priority .....	114ページ
Default Trunk Priority .....	116ページ
Traffic Classes .....	117ページ
Queue Scheduling .....	119ページ
IP Precedence/DSCP Priority Status .....	120ページ
IP Precedence Priority .....	121ページ
IP DSCP Priority .....	122ページ
IP Port Priority Status .....	124ページ
IP Port Priority .....	125ページ

## Trunk

LACP Configuration .....	127ページ
Trunk Configuration .....	129ページ

## SNMP

SNMP Configuration .....	131ページ
--------------------------	--------

## IGMP

IGMP Configuration .....	134ページ
Multicast Router Port Information .....	136ページ
Static Multicast Router Port Configuration .....	137ページ
IP Multicast Registration Table .....	139ページ
IGMP Member Port Table .....	140ページ

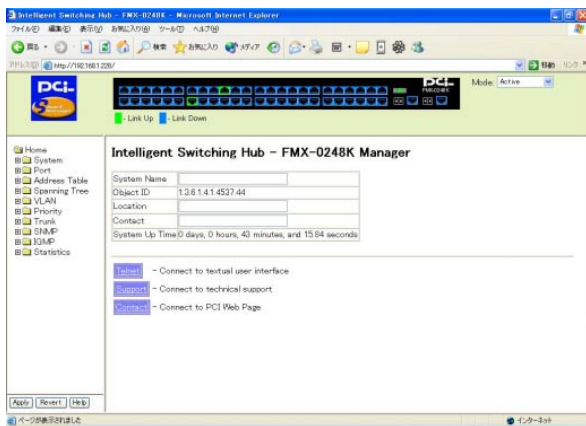
## Statistics

Port Statistics .....	142ページ
-----------------------	--------

## 5. Home

ウェブブラウザからウェブインターフェースにログインすると、以下の画面が表示されます。

画面の左側にメニュー一覧、右上にパネル画面、右下にシステム情報がそれぞれ表示されます。メイン一覧の各リンクを使い、他のメニューの表示、パラメータの設定、および統計データが表示されます。



## 6. ポート画面

ポート画面は、本製品の各ポートの状態が表示されます。各ポートをクリックすると、統計および設定情報が表示されます。



### ポート図

各ポートの状態が色で表示されます。クリックすると、[ Port Configuration ] ( xxページ )が表示されます。

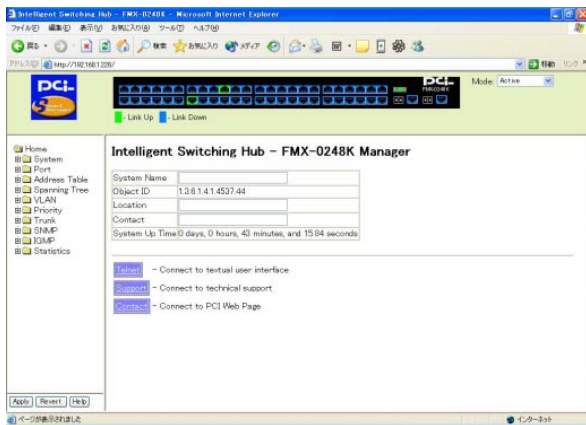
### Mode

ポート図で表示する内容を選びます。

- ・Active: ネットワーク機器の接続状態が表示されます。
  - ・緑: ネットワーク機器が接続され、リンクが確立している
  - ・青: リンクが確立されていない
- ・Duplex: 転送モードが表示されます。
  - ・緑: 半二重
  - ・青: 全二重
- ・Flow Control: フロー制御の状態が表示されます。
  - ・緑: 無効
  - ・青: 有効

## 7. System Information

項目メニューから「Home」「System」「System Information」を選択すると、以下の画面が表示されます。システム監理者の連絡先、システムの稼動時間などのシステム情報の設定と参照ができます。



### 【System Name】

システム名を設定します。

### 【Object ID】

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「1.3.6.1.4.1.4537.44」が表示されます。

### \* 【Location】

システムの設置場所を設定します。

**\*【Contact】**

管理者の情報を設定します。

**\*【System Up Time】**

起動している管理エージェントの稼働時間を表示します。

**【telnet】**

ターミナルユーティリティを使用してTelnetを接続します。

**【Support】**

弊社テクニカルサポートまで連絡するメールアドレスを表示します。

**【Contact】**

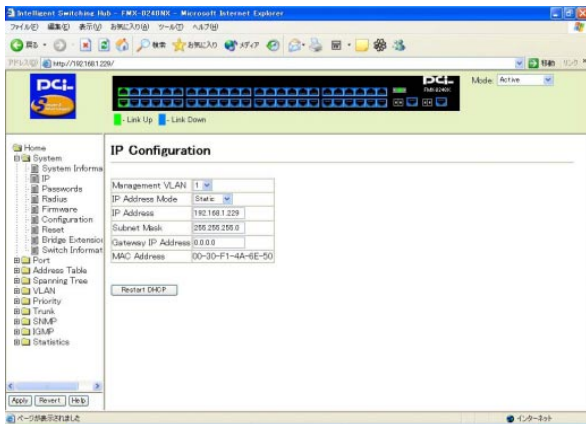
弊社WEBサイトを表示します。

\* 無し、または最小1文字から最大99文字の半角英数字で設定します。



## 8. IP

項目メニューから「Home」「System」「IP」を選択すると、以下の画面が表示されます。管理用にIPサブネットアドレスを設定します。



### 【Management VLAN】

本製品にアクセスするVLANグループを設定します。

### 【IP Address Mode】

本製品に振り当てるIPアドレスの取得方法を設定します。

- ・Static : 手動でIPアドレスを設定
- ・BOOTP : BootPサーバからIPアドレスを取得
- ・DHCP : DHCPサーバからIPアドレスを取得

### 【IP Address】

Staticに設定した時に、本製品のIPアドレスを設定します。

**【Subnet Mask】**

Staticに設定した時に、サブネットマスクを設定します。

**【Gateway IP Address】**

Staticに設定した時に、ゲートウェイのIPアドレスを設定します。

**【MAC Address】**

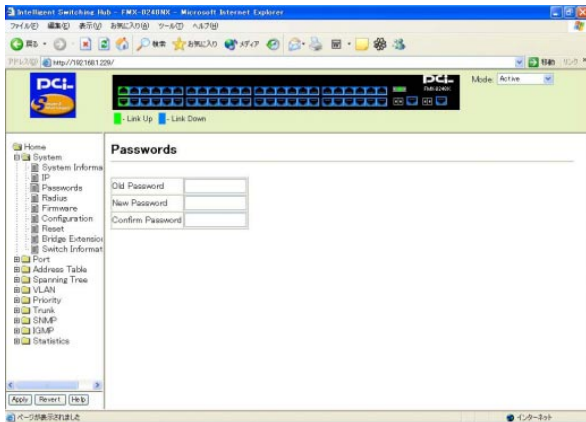
本製品のMACアドレスを表示します。

**【ReStart DHCP】**

BOOTPまたはDHCPに設定した時に、IPアドレスを再取得します。

## 9 .Passwords

項目メニューから「Home」「System」「Passwords」を選択すると、以下の画面が表示されます。管理用のパスワードを変更できます。



### 【Old Password】

現在のパスワードを入力します。最大15文字の半角英数字で設定します。大文字・小文字の区別はありません。

### 【New Password】

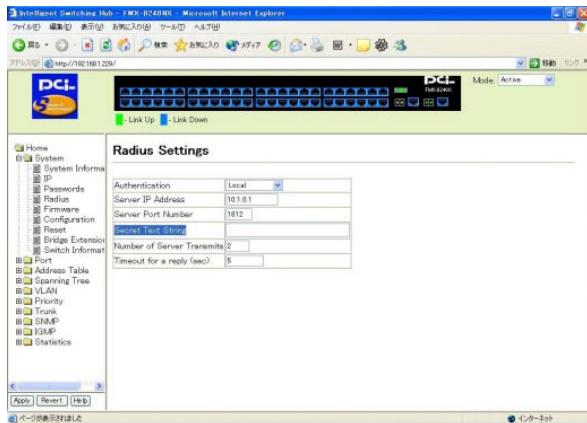
新しいパスワードを入力します。最大15文字の半角英数字で設定します。大文字・小文字の区別はありません。

### 【Confirm Password】

確認のため、もう一度パスワードを入力します。最大15文字の半角英数字で設定します。大文字・小文字の区別はありません。

## 10. Radius

項目メニューから「Home」「System」「Radius」を選択すると、以下の画面が表示されます。Radiusサーバを使用してユーザ認証を提供するための設定をします。



### 【Authentication】

認証をする方式を設定します。

- local : 本製品内の認証を使用
- Radius : Radiusサーバを使用して認証
- Radius,local : Radiusサーバを使用して認証後、必要であれば本製品内の認証を使用
- local,Radius : 本製品内の認証を使用後、必要であればRadiusサーバを使用して認証

### 【Server IP Address】

RadiusサーバのIPアドレスを設定します。

#### 【Server Port Number】

Radiusサーバのポート番号を設定します。

#### 【Secret Text String】

Radiusサーバの設定値を必要であれば入力します。

#### 【Number of Server Transmits】

Radiusサーバに送信する数を設定します。

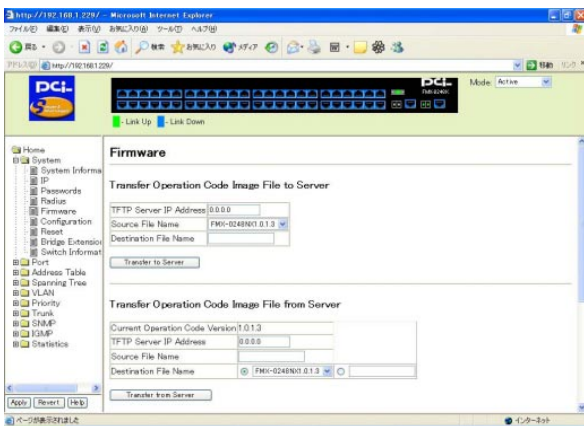
#### 【Timeout for a reply ( sec )】

Radiusサーバにアクセス後、再接続する時の間隔を設定します。

## 11 Firmware

項目メニューから「Home」「System」「Firmware」を選択すると、以下の画面が表示されます。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・現在のソフトウェアをアップロードします。

ダウンロードするファイルは、バイナリ形式またはイメージファイルです。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、本製品とコンピュータの接続やネットワークの状況に依存します。



Transfer Operation Code Image File to Server  
TFTPサーバにイメージファイル等をアップロードします。

### Transfer Operation Code Image File to Server

TFTP Server IP Address	0.0.0.0
Source File Name	FMX-0248NX1.0.1.3
Destination File Name	
<input type="button" value="Transfer to Server"/>	

#### 【TFTP Server IP Address】

アップロードする相手先のTFTPサーバのIPアドレスを設定します。

### 【Source File Name】

アップロードするイメージファイルを指定します。

### 【Destination File Name】

アップロードするイメージファイルにファイル名を設定します。

### 【Transfer to Server】

設定する項目を全て入力し終わったらクリックします。

## Transfer Operation Code Image File from Server

TFTPサーバから最新のファームウェア、イメージファイル等をダウンロードします。

### Transfer Operation Code Image File from Server

Current Operation Code Version	1.0.1.3	
TFTP Server IP Address	<input type="text" value="0.0.0.0"/>	
Source File Name	<input type="text"/>	
Destination File Name	<input type="button" value="⊕"/> FMX-0248NX1.0.1.3 <input type="button" value="⊖"/>	<input type="text"/>

### 【Current Operation Code Version】

現在のファームウェアのバージョンが表示されます。

### 【TFTP Server IP Address】

ダウンロードする相手先のTFTPサーバのIPアドレスを設定します。

### 【Source File Name】

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。

### 【Destination File Name】

ダウンロードするバイナリまたはイメージファイルを書き込むファイル名を設定します。

### 【Transfer from Server】

設定する項目を全て入力し終えたらクリックします。

### Remove Operation Code Image File

保存しているイメージファイル(ファームウェア)を削除します。

## Remove Operation Code Image File

File Name	FMX-0248NX1.0.1.3 ▼
-----------	---------------------

Remove File

### 【File Name】

削除したいイメージファイル(ファームウェア)を設定します。

### 【Remove file】

削除したいファイル名を設定後、クリックします。



## Start-Up Operation Code Image File

システム起動時に起動するイメージファイル(ファームウェア)を設定します。

### Start-Up Operation Code Image File

File Name	FMX-0248NX1.0.1.3	▼
-----------	-------------------	---

Apply Changes

#### 【File Name】

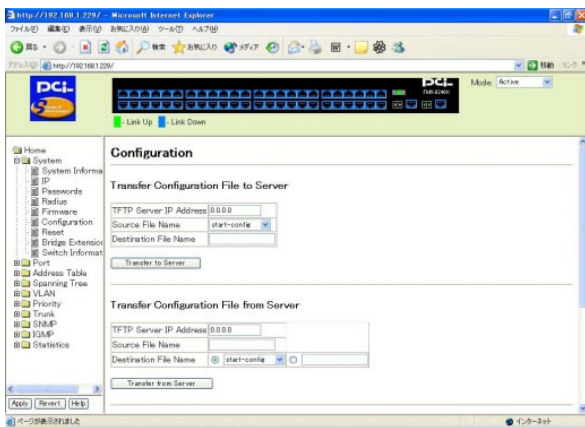
システム起動時に使用するイメージファイル(ファームウェア)を指定します。

#### 【Apply Changes】

システム起動時に使用するファイル名を指定後、クリックします。

## 12. Configuration

項目メニューから「Home」「System」「Configuration」を選択すると、以下の画面が表示されます。本製品の設定情報をTFTPサーバにダウンロード・アップロードできます。設定ファイルの保存、書き戻し機能を使うことで、各設定を短時間で変更、トラブルシューティング時の設定復元などできるようになります。



### Transfer Configuration File to Server

TFTPサーバにコンフィグレーションファイルをアップロードします。

## Transfer Configuration File to Server

TFTP Server IP Address	<input type="text" value="0.0.0.0"/>
Source File Name	<input type="text" value="start-config"/> ▼
Destination File Name	<input type="text"/>

### 【TFTP Server IP Address】

アップロードする相手先のTFTPサーバのIPアドレスを設定します。

### 【Source File Name】

アップロードするコンフィグレーションファイルを指定します。

### 【Destination File Name】

アップロードするコンフィグレーションファイルをTFTPサーバに保存するとき使用するファイル名を設定します。

### 【Transfer to Server】

設定する項目を全て入力し終わったらクリックします。

## Transfer Configuration File from Server

TFTPサーバからコンフィグレーションファイルをダウンロードします。

### Transfer Configuration File from Server

TFTP Server IP Address	<input type="text" value="0.0.0.0"/>
Source File Name	<input type="text"/>
Destination File Name	<input type="text" value="start-config"/> <input type="radio"/>

#### 【TFTP Server IP Address】

ダウンロードする相手先のTFTPサーバのIPアドレスを設定します。

#### 【Source File Name】

ダウンロードするコンフィグレーションファイルを指定します。

#### 【Destination File Name】

ダウンロードするコンフィグレーションファイルを書き込むファイル名を指定するか新たに名前を設定します。

#### 【Transfer from Server】

設定する項目を全て入力し終えたらクリックします。

## Remove Configuration File

コンフィグレーションファイルを削除します。

### Remove Configuration File

File Name	start-config	▼
-----------	--------------	---

Remove File

#### 【File Name】

削除したいコンフィグレーションファイルを設定します。

#### 【Remove file】

削除したいファイル名を設定後、クリックします。

## Start-Up Configuration File

システム起動時に使用するコンフィグレーションファイルを設定します。

### Start-Up Configuration File

File Name	startup-config	▼
-----------	----------------	---

Apply Changes

## 【File Name】

システム起動時に使用するコンフィグレーションファイルを指定します。

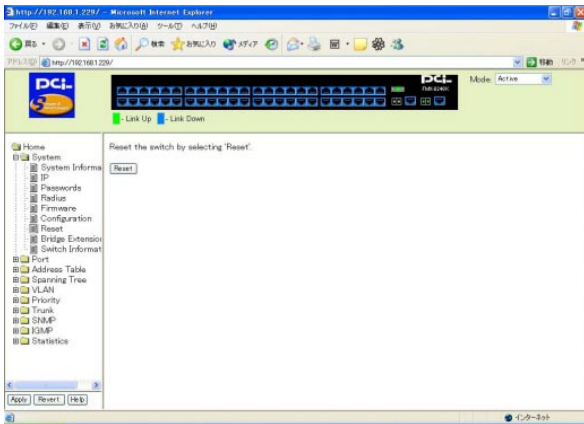
## 【Apply Changes】

コンフィグレーションファイルを指定後、クリックします。

### Copy Running Config to File

設定した内容をコンフィグレーションファイルに保存します。

設定した内容は「Copy Running Config to File」を使用して保存しないと、再起動後に変更した設定内容が消去されます。



## 【File Name】

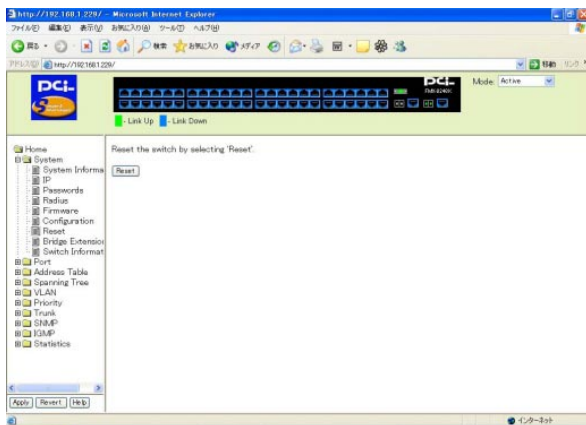
保存先となるコンフィグレーションファイルを指定します。

## 【Apply Changes】

コンフィグレーションファイル名を指定後、クリックします。

## 13. Reset

項目メニューから「Home」「System」「Reset」を選択すると、以下の画面が表示されます。本製品を再起動するか設定します。



### 【Reset】

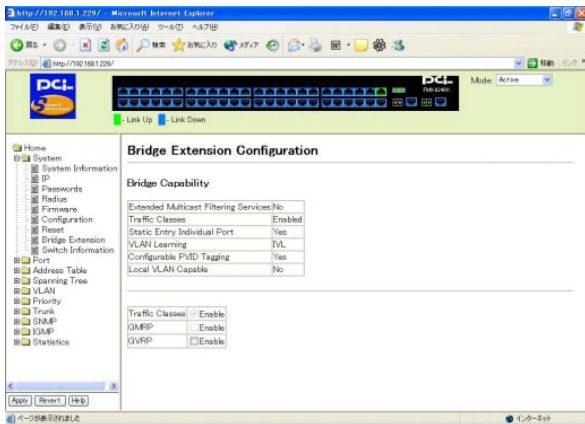
再起動する時にクリックします。



再起動するときは[ OK ]を中止するときは[ キャンセル ]をクリックします。

## 14. Bridge Extension

項目メニューから「Home」「System」「Bridge Extension」を選択すると、以下の画面が表示されます。本製品のブリッジに関する状態と設定ができます。



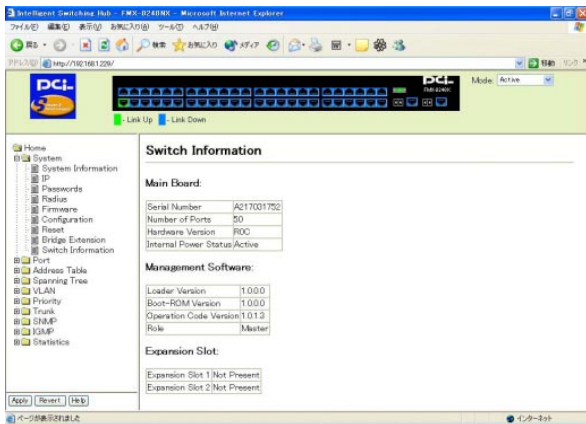
### 【GVRP】

GVRPの有効/無効を設定します。GVRPを有効にするときは、チェックを付けます。



## 15. Switch Information

項目メニューから「Home」「System」「Switch Information」を選択すると、以下の画面が表示されます。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などを参照できます。



### 【Serial Number】

本製品のシリアル番号を表示します。

### 【Number of Ports】

本製品のポート数を表示します。

### 【Hardware Version】

ハードウェアバージョンを表示します。

### 【Internal Power Status】

主電源の状況を表示します。

- ・Active : 使用
- ・Inactive : 未使用

### 【Loader Version】

ローダーバージョンを表示します。

### 【Boot-ROM Version】

ROMのバージョンを表示します。

### 【Operation Code Version】

ROMに保存されているファームウェアのバージョンを表示します。

### 【Role】

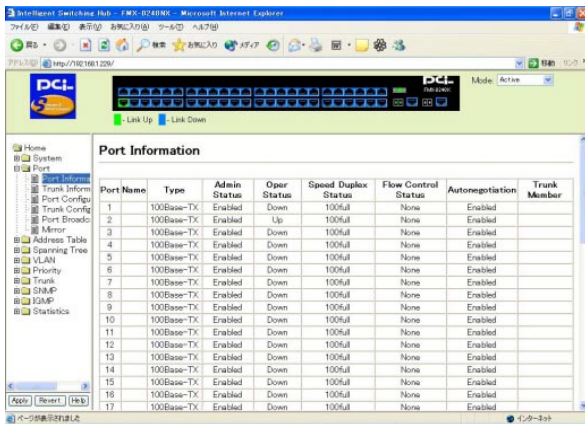
本製品の状態を表示します。

### 【Expansion Slot 1、Expansion Slot 2】

現段階では使用しません。

## 16. Port Information

項目メニューから「Home」「Port」「Port Information」を選択すると、以下の画面が表示されます。本製品のすべてのポートの通信パラメータを表示します。



The screenshot shows the web interface of an Intelligent Switching Hub. The browser address bar indicates the URL is http://192.168.1.220/. The page title is "Port Information". A navigation menu on the left includes Home, System, Port, Port Inform, Trunk Inform, Port Config, Trunk Config, Port Broad, Mirror, Address Table, Spanning Tree, VLAN, Priority, Trunk, SHMP, QMMP, and Statistics. The main content area displays a table with the following data:

Port Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Trunk Member
1	100Base-TX	Enabled	Down	100full	None	Enabled	
2	100Base-TX	Enabled	Up	100full	None	Enabled	
3	100Base-TX	Enabled	Down	100full	None	Enabled	
4	100Base-TX	Enabled	Down	100full	None	Enabled	
5	100Base-TX	Enabled	Down	100full	None	Enabled	
6	100Base-TX	Enabled	Down	100full	None	Enabled	
7	100Base-TX	Enabled	Down	100full	None	Enabled	
8	100Base-TX	Enabled	Down	100full	None	Enabled	
9	100Base-TX	Enabled	Down	100full	None	Enabled	
10	100Base-TX	Enabled	Down	100full	None	Enabled	
11	100Base-TX	Enabled	Down	100full	None	Enabled	
12	100Base-TX	Enabled	Down	100full	None	Enabled	
13	100Base-TX	Enabled	Down	100full	None	Enabled	
14	100Base-TX	Enabled	Down	100full	None	Enabled	
15	100Base-TX	Enabled	Down	100full	None	Enabled	
16	100Base-TX	Enabled	Down	100full	None	Enabled	
17	100Base-TX	Enabled	Down	100full	None	Enabled	

### 【Port】

ポート番号を表示します。

### 【Name】

ポートに指定した名前を表示します。

### 【Type】

ポートのタイプを表示します。

- ・100Base-TX : 10/100Base対応RJ-45ポート
- ・1000Base-TX : 10/100/1000Base対応RJ-45ポート
- ・1000Base-SFP : 1000Base対応LCコネクタポート

### 【Admin Status】

ポートの状態を表示します。

- ・Enabled : 有効
- ・Disabled : 無効

### 【Oper Status】

ポートとネットワーク機器間の接続状態を表示します。

- ・Up : ネットワーク機器が接続され、リンクが確立している
- ・Down : リンクが確立されていない

### 【Speed Duplex Status】

転送速度および転送モードを表示します。

### 【Flow Control Status】

フロー制御が表示されます。

- ・On : 有効
- ・None : 無効

### 【Autonegotiation】

オートネゴシエーション機能を表示します。

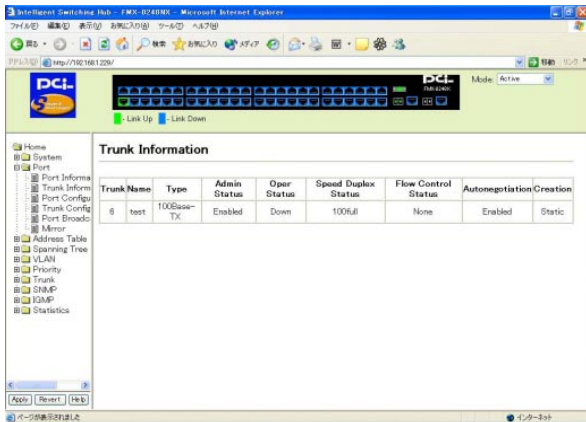
- ・Enabled : 有効
- ・Disabled : 無効

### 【Trunk Member】

ポートが登録しているトランクグループ番号を表示します。

## 17. Trunk Information

項目メニューから「Home」「Port」「Trunk Information」を選択すると、以下の画面が表示されます。トランクの設定状態を表示します。



### 【Trunk】

現在作成されているトランクグループの番号を表示します。

### 【Name】

トランクグループに指定している名前を表示します。

### 【Type】

トランクポートのタイプを表示します。

- ・100Base-TX : 10/100Base対応RJ-45ポート
- ・1000Base-TX : 10/100/1000Base対応RJ-45ポート
- ・1000Base-SFP : 1000Base対応LCコネクタポート

### 【Admin Status】

トランクポートの状態を表示します。

- ・Enabled : 有効
- ・Disabled : 無効

### 【Oper Status】

トランクポートとネットワーク機器間の接続状態を表示します。

- ・Up : ネットワーク機器が接続され、リンクが確立している
- ・Down : リンクが確立されていない

### 【Speed Duplex Status】

トランクポートの転送速度および転送モードを表示します。

### 【Flow Control Status】

フロー制御が表示されます。

- ・On : 有効
- ・None : 無効

### 【Autonegotiation】

オートネゴシエーション機能を表示します。

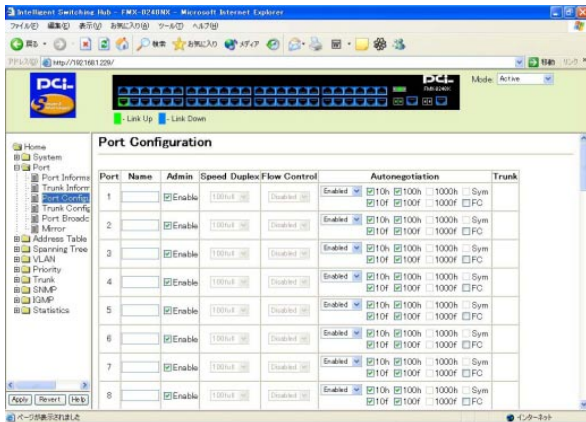
- ・Enabled : 有効
- ・Disabled : 無効

### 【Creation】

トランクグループの作成状況を表示します。

## 18. Port Configuration

項目メニューから「Home」「Port」「Port Configuration」を選択すると、以下の画面が表示されます。各ポートの通信速度、フローコントロール、名前等を設定することができます。



### 【Port】

ポート番号を表示します。

### 【Name】

ポートに名前を設定します。

- ・無しまたは最小1文字から最大64文字の半角英数字で設定します。

### 【Admin】

ポートの状態を表示します。

- ・チェック有り：有効
- ・チェック無し：無効

### 【Speed Duplex】

ポートの転送速度および通信モードを設定します。

「Autonegotiation」を無効にしたときに表示されます。

- ・10Half : 10Mbps/半二重
- ・10Full : 10Mbps/全二重
- ・100Half : 100Mbps/半二重
- ・100Full : 100Mbps/全二重
- ・1000Full : 1000Mbps/全二重

### 【Flow Control】

フロー制御を設定します。

「Autonegotiation」を無効にしたときに表示されます。

- ・Enabled : 有効
- ・Disabled : 無効

### 【Autonegotiation】

オートネゴシエーション機能の有効/無効とオートネゴシエーション機能の詳細設定をします。

- ・Enabled : 有効
- ・Disabled : 無効

オートネゴシエーション機能の有効時に以下の項目にチェックを入れるとチェックを入れた設定は有効になります。

- ・10h : オートネゴシエーションで接続時に10Mbps/半二重を有効にします。
- ・10f : オートネゴシエーションで接続時に10Mbps/全二重を有効にします。



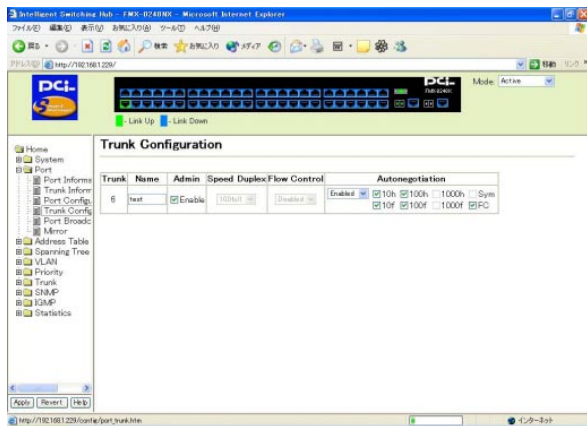
- ・100h : オートネゴシエーションで接続時に100Mbps/半二重を有効にします。
- ・100f : オートネゴシエーションで接続時に100Mbps/全二重を有効にします。
- ・1000f : オートネゴシエーションで接続時に1000Mbps/全二重を有効にします。
- ・FC : オートネゴシエーションで接続時にフロー制御を有効にします。

#### 【Trunk】

ポートが登録しているトランクグループ番号を表示します。

## 19. Trunk Configuration

項目メニューから「Home」「Port」「Trunk Configuration」を選択すると、以下の画面が表示されます。作成されているトランクグループの通信速度、フローコントロール、名前等を設定することができます。



### 【Trunk】

現在作成されているトランクグループの番号を表示します。

### 【Name】

トランクグループに名前を設定します。

- ・無しまたは最小1文字から最大64文字の半角英数字で設定します。

### 【Admin】

トランクグループの有効/無効を設定します。

- ・チェック有り：有効
- ・チェック無し：無効

### 【Speed Duplex】

トランクグループの転送速度および通信モードを設定します。

「Autonegotiation」を無効にしたときに表示されます。

- ・10Half : 10Mbps/半二重
- ・10Full : 10Mbps/全二重
- ・100Half : 100Mbps/半二重
- ・100Full : 100Mbps/全二重
- ・1000Full : 1000Mbps/全二重

### 【Flow Control】

フロー制御を設定します。

「Autonegotiation」を無効にしたときに表示されます。

- ・Enabled：有効
- ・Disabled：無効

### 【Autonegotiation】

オートネゴシエーション機能の有効/無効とオートネゴシエーション機能の詳細設定をします。

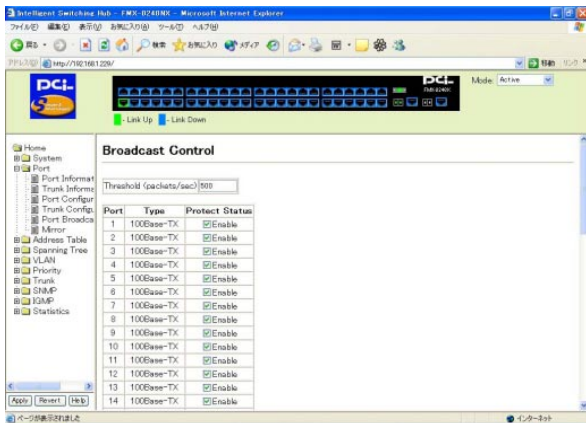
- ・Enabled：有効
- ・Disabled：無効

オートネゴシエーション機能の有効時に以下の項目にチェックを入れるとチェックを入れた設定は有効になります。

- ・10h: オートネゴシエーションで接続時に10Mbps/半二重を有効にします。
- ・10f: オートネゴシエーションで接続時に10Mbps/全二重を有効にします。
- ・100h: オートネゴシエーションで接続時に100Mbps/半二重を有効にします。
- ・100f: オートネゴシエーションで接続時に100Mbps/全二重を有効にします。
- ・1000f: オートネゴシエーションで接続時に1000Mbps/全二重を有効にします。
- ・FC: オートネゴシエーションで接続時にフロー制御を有効にします。

## 20. Port Broadcast Control

項目メニューから「Home」「Port」「Port Broadcast Control」を選択すると、以下の画面が表示されます。ブロードキャストコントロールの設定をします。



### 【Threshold ( packets/sec )】

ブロードキャストコントロールのしきい値を設定します。

- ・設定値：1 ~ 99999

### 【Port】

ポート番号を表示します。

### 【Type】

ポートのタイプを表示します。

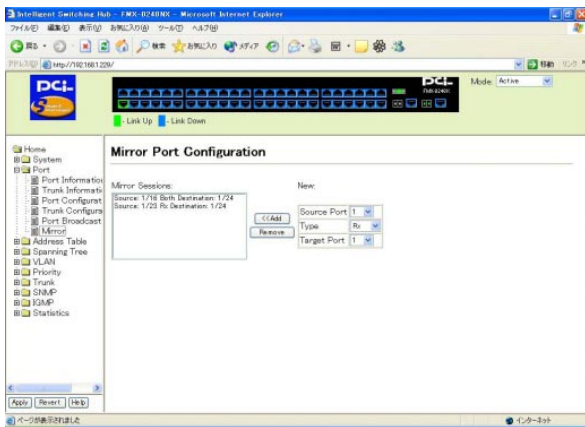
- ・100Base-TX：10/100Base対応RJ-45ポート
- ・1000Base-TX：10/100/1000Base対応RJ-45ポート
- ・1000Base-SFP：1000Base対応LCコネクタポート

## 【Protect Status】

ポートごとのブロードキャストコントロールの有効/無効を設定します。

## 21. Mirror

項目メニューから「Home」「Port」「Mirror」を選択すると、以下の画面が表示されます。特定ポート(ソースポート)のトラフィックを他のポート(ターゲットポート)にコピーします。ターゲットポートにロジックアナライザなど接続し、ソースポートの通信に影響を与えることなくトラフィックを解析できます。



## 【Mirror Sessions】

作成したミラーリング設定を表示します。

複数のミラーリング設定を作成することが可能です。

### 【Source Port】

送信、受信または送受信したトラフィックをミラーリングするポートします。

### 【Type】

ミラーリングする方法を設定します。

- ・Rx: 受信トラフィックのみ取得
- ・Tx: 送信トラフィックのみ取得
- ・Both: 送受信トラフィックともに取得

### 【Target Port】

「Source Port」ミラーリングするポートを選択します。

### 【<<Add】

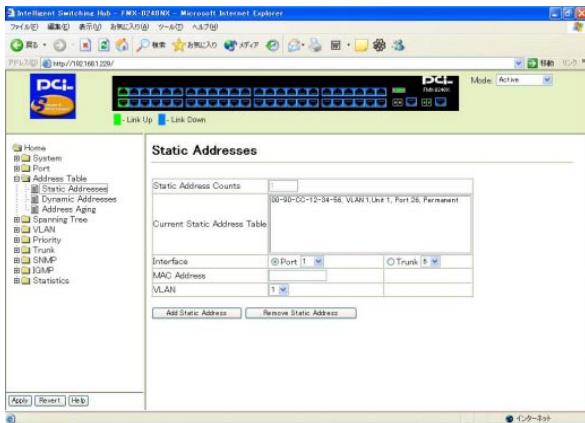
「Source Port」, 「Type」, 「Target Port」を設定して「Add」をクリックすることでミラーリングするポート設定を追加します。

### 【Remove】

「Mirror Sessions」から削除したいミラーリング設定を選択して「Remove」をクリックすることでミラーリングするポート設定を削除します。

## 22. Static Addresses

項目メニューから「Home」「Address Table」「Static Addresses」を選択すると、以下の画面が表示されます。静的MACアドレスをポートに設定します。



### 【Static Address Counts】

静的に設定したMACアドレスの総数を表示します。

### 【Current Static Address Table】

作成した静的MACアドレスの一覧を表示します。

### 【Interface】

静的MACアドレスを登録するポート番号またはトランク番号を設定します。

- ・Port : ポート番号を指定します。
- ・Trunk : トランク番号を指定します。



### 【MAC Address】

指定する静的MACアドレスを設定します。

### 【VLAN】

静的MACアドレスを登録するVLAN IDを設定します。

### 【Add Static Address】

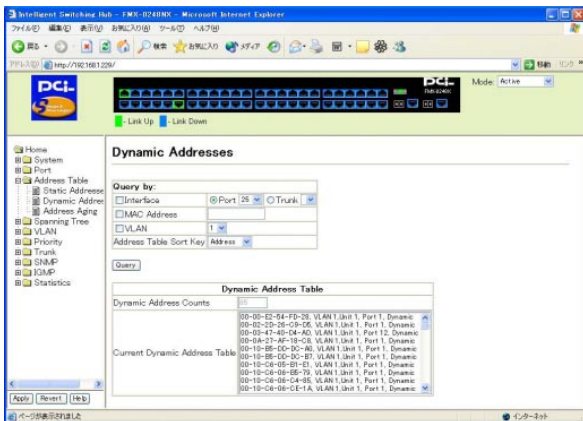
静的MACアドレスを登録するときにクリックします。「Interface」、「MAC Address」、「VLAN」を設定後クリックすると「Current Static Address Table」に静的MACアドレスが登録されます。

### 【Remove Static Address】

静的MACアドレスを削除するときにクリックします。「Current Static Address Table」から削除したい静的MACアドレスを指定後、クリックをすると削除されます。

## 23. Dynamic Addresses

項目メニューから「Home」「Address Table」「Dynamic Addresses」を選択すると、以下の画面が表示されます。動的に学習したMACアドレスを表示します。



### 【Query by】

動的に学習したMACアドレスを表示する条件を設定します。

- Interface: どのインターフェイスで学習したMACアドレスかを選択します。  
1ポートごとまたは1トランクグループごとを選択します。
- MAC Address: 表示させたい動的MACアドレスを設定します。
- VLAN: VLAN IDを指定し、表示させたい動的MACアドレスを設定します。
- Address Table Sort Key: Address、VLAN、Interfaceから選択します。

### 【Query】

指定した条件を表示させるときにクリックします。「Query by」の各項目の左側にチェックを入れ、Queryをクリックすると指定した条件を表示します。

### 【Dynamic Address Counts】

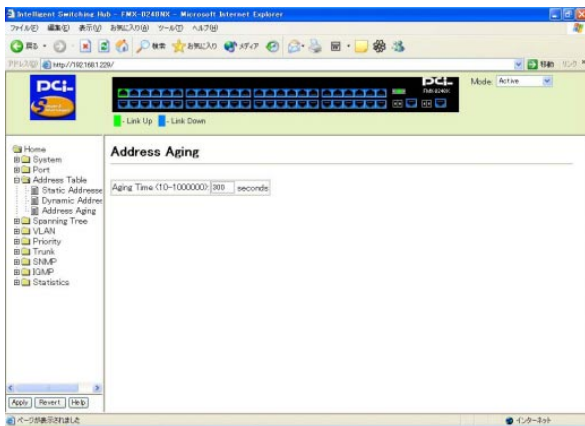
動的に学習したMACアドレスの総数を表示します。

### 【Current Dynamic Address Table】

動的に学習したMACアドレスの一覧を表示します。

## 24. Address Aging

項目メニューから「Home」「Address Table」「Address Aging」を選択すると、以下の画面が表示されます。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タイムアウト値を設定します。



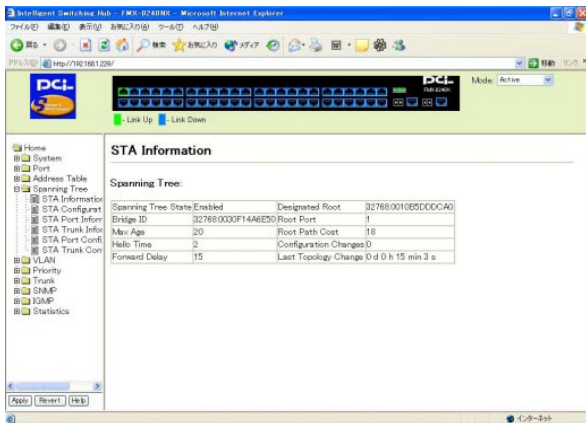
### 【Aging Time】

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タイムアウト値を設定します。

- ・10～1000000：エージアウトするタイムアウト値を設定します。  
単位は秒

## 25. STA Information

項目メニューから「Home」「Spanning Tree」「STA Information」を選択すると、以下の画面が表示されます。スパンニングツリー情報の概要を表示します。



### 【Spanning Tree State】

スパンニングツリーの有効/無効の状態を表示します。

- ・ENABLED: スパンニングツリーアルゴリズム (STA) 対応ネットワークに参加します。
- ・DISABLED: STAを無効にします。

### 【Designated Root】

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アドレスを表示します。

### 【Bridge ID】

本製品がルート機器との間で認識させるためのIDを表示します。

### 【Root Port】

本製品のポートのうちルートに最も近いポート番号を表示します。本製品は、このポートを通してルート機器と通信します。ルートポートが存在しないときは、本製品がスパンニングツリーネットワーク内のルート機器になります。

### 【Max Age】

各機器が再設定を試みる前に、待機する時間を表示します。

### 【Root Path Cost】

本製品のルートポートからルート機器までのパスコストを表示します。

### 【Hello Time】

連続してConfiguration BPDUを送信するときの、各送信間の最小間隔を表示します。

### 【Configuration Changes】

スパンニングツリーが再設定された回数が表示されます。

### 【Forward Delay】

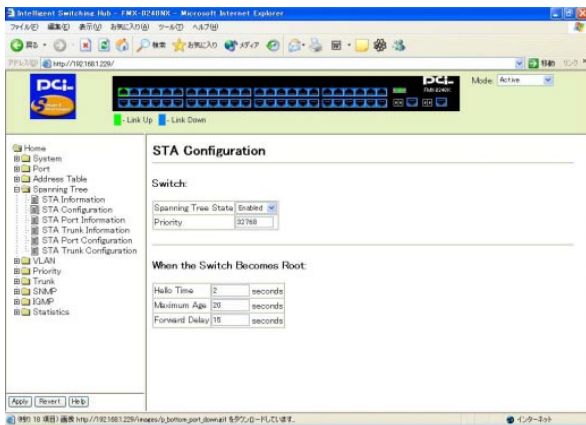
リスニング ラーニング フォワーディングのステート移行を実行する前の、ルート機器が待機する最大時間が表示されます。

### 【Last Topology Change】

スパンニングツリーが最後に再設定されてから経過した時間が表示されます。

## 26. STA Configuration

項目メニューから「Home」「Spanning Tree」「STA Configuration」を選択すると、以下の画面が表示されます。スパニングツリーの概要を設定します。



### 【Spanning Tree State】

スパニングツリーを設定します。

- ・ENABLED: スパニングツリーアルゴリズム( STA )対応ネットワークに参加します。
- ・DISABLED: STAを無効にします。

### 【Priority】

スパンニングツリーを形成しているネットワークで、ルート機器、ルートポート、および指定ポートを設定します。優先度の最も高い機器がSTAルート機器になります。全機器の優先度が同じ場合は、最も低いIMACアドレスを持ったデバイスがルート機器になります。工場出荷状態は「32768」に設定されています。

・0～65535：優先度を設定。値が低いほど、優先度は高くなります

### 【Hello Time】

ルート機器の設定メッセージ送信間隔を設定します。単位は秒。最小値は「1」、最大値は「4」または次の計算式の値と比べ、低い値になります。工場出荷状態は「2」に設定されています。

$$\text{最大値} = \{ (\text{Max. Message Age} \div 2) - 1 \}$$

### 【Maximum Age】

各機器が再設定を試みる前に、待機する時間を設定します。この時間の間、設定メッセージが届かない場合は再設定します。指定ポートを除く全ポートは、一定間隔で設定メッセージを受信します。各ポートは、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のときは、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ばれます。工場出荷状態は「20」に設定されています。

・6～40：待機時間を設定します。単位は秒。最小値は「6」または次の計算式の値と比べ、高い値になります。最大値は「40」または次の計算式の値と比べ、低い値になります

$$\text{最小値} = \{ 2 \times (\text{Hello Time} + 1) \}$$

$$\text{最大値} = \{ 2 \times (\text{Forward Delay} - 1) \}$$



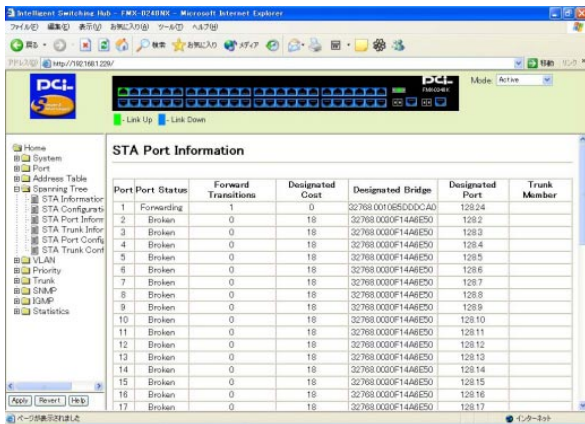
## 【Forward Delay】

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、ディレイ時間が必要です。また、各ポートも矛盾する情報があるかリスニングする時間が必要になります。リスニングの結果矛盾する情報があるときは、ブロッキング状況に移行しますが、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。工場出荷状態は「15」に設定されています。

- ・4～30：ルート機器が待機する最大時間を設定します。単位は秒。  
最大値は「30」、最小値は「4」または次の計算式の値と比べ、高い値になります  
最小値 = { ( Max. Message Age ÷ 2 ) + 1 }

## 27. STA Port Information

項目メニューから「Home」「Spanning Tree」「STA Port Information」を選択すると、以下の画面が表示されます。スパンニングツリー内の、ポートの現在の状態を表示します。



The screenshot shows the web interface for an Intelligent Switching Hub. The main content area displays the 'STA Port Information' table. The table has the following columns: Port, Port Status, Forward Transitions, Designated Cost, Designated Bridge, Designated Port, and Trunk Member. The data in the table is as follows:

Port	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Trunk Member
1	Forwarding	1	0	32768.0010E5D000CA0	128.24	
2	Broken	0	18	32768.0000F14A6E50	128.2	
3	Broken	0	18	32768.0000F14A6E50	128.3	
4	Broken	0	18	32768.0000F14A6E50	128.4	
5	Broken	0	18	32768.0000F14A6E50	128.5	
6	Broken	0	18	32768.0000F14A6E50	128.6	
7	Broken	0	18	32768.0000F14A6E50	128.7	
8	Broken	0	18	32768.0000F14A6E50	128.8	
9	Broken	0	18	32768.0000F14A6E50	128.9	
10	Broken	0	18	32768.0000F14A6E50	128.10	
11	Broken	0	18	32768.0000F14A6E50	128.11	
12	Broken	0	18	32768.0000F14A6E50	128.12	
13	Broken	0	18	32768.0000F14A6E50	128.13	
14	Broken	0	18	32768.0000F14A6E50	128.14	
15	Broken	0	18	32768.0000F14A6E50	128.15	
16	Broken	0	18	32768.0000F14A6E50	128.16	
17	Broken	0	18	32768.0000F14A6E50	128.17	

### 【Port】

ポート番号を表示します。

### 【Port Status】

スパンニングツリー内の、ポートの現在の状態を表示します。

- Broken: 何もリンクが確立していないか、ユーザによって無効に設定されています。
- Listening: トポロジの変更のため、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、パケットは転送しません

- ・ Bloking : 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
- ・ 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送信しました。ポートアドレスはクリアされ、再びアドレス学習を開始します
- ・ Forwarding : パケットを転送し、アドレス学習を続けます

#### 【Forward Transitions】

トポロジーチェンジを起こし、Forwardingになった回数を表示します。

#### 【Designated Cost】

パケットがポートからルートに移動するときのコストを表示します。メディアの速度が遅いほどコストは高くなります。

#### 【Designated Bridge】

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】

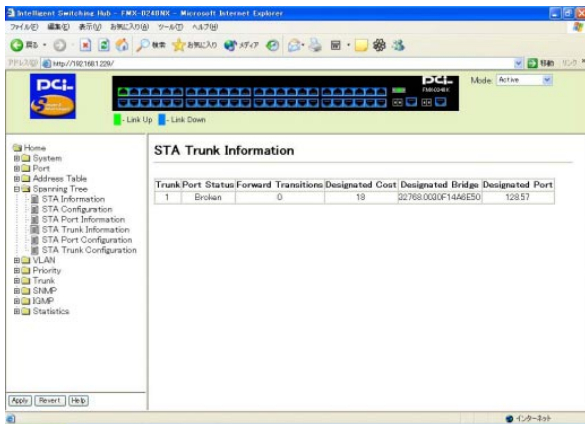
スパニングツリーのルートと通信するとき、途中通過しなければならない指定ブリッジ機器のプライオリティおよびポート番号を表示します。

#### 【Trunk Member】

トランクグループに属しているときにトランク番号を表示します。

## 28. STA Trunk Information

項目メニューから「Home」「Spanning Tree」「STA Trunk Information」を選択すると、以下の画面が表示されます。スパンニングツリー内の、トランクグループの現在の状態を表示します。



The screenshot shows a web browser window displaying the configuration page for an Intelligent Switching Hub. The page title is "Intelligent Switching Hub - FMC-B240NK - Microsoft Internet Explorer". The browser address bar shows "http://192.168.1.229/". The page features a navigation menu on the left with options like Home, System, Port, Address Table, Spanning Tree, STA Information, STA Configuration, STA Port Information, STA Trunk Information, STA Port Configuration, STA Trunk Configuration, VLAN, Priority, Trunk, STMP, IGMP, and Statistics. The main content area is titled "STA Trunk Information" and contains a table with the following data:

TrunkPort	Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port
1	Broken	0	19	02768.0030F14A6E50	128/57

### 【Trunk】

トランクグループ番号を表示します。

### 【Port Status】

スパニングツリー内の、トランクグループの現在の状態を表示します。

- ・ Bloken : 何もリンクが確立していないか、ユーザによって無効に設定されています。
- ・ Bloking : 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送信しました。ポートアドレスはクリアされ、再びアドレス学習を開始します
- ・ Forwarding : パケットを転送し、アドレス学習を続けます

### 【Forward Transitions】

トポロジチェンジを起こし、Forwardingになった回数を表示します。

### 【Designated Cost】

パケットがポートからルートに移動するときのコストを表示します。メディアの速度が遅いほどコストは高くなります。

### 【Designated Bridge】

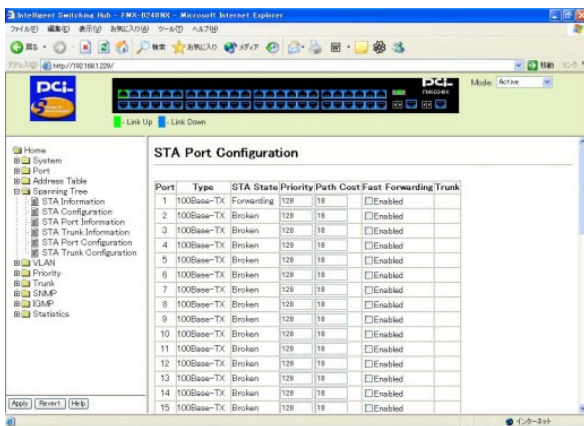
スパニングツリーのルートに到達するため、途中通過しなければならない機器のプライオリティおよびMACアドレスを表示します。

## 【Designated Port】

スパンニングツリーのルートと通信するとき、途中通過しなければならない指定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。

## 29. STA Port Configuration

項目メニューから「Home」「Spanning Tree」「STA Port Configuration」を選択すると、以下の画面が表示されます。スパンニングツリアルゴリズムのポート設定します。



The screenshot shows the web interface of an Intelligent Switching Hub. The main content area is titled "STA Port Configuration" and contains a table with the following data:

Port	Type	STA State	Priority	Path Cost	Fast Forwarding	Trunk
1	100Base-TX	Forwarding	129	19	<input type="checkbox"/>	Enabled
2	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
3	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
4	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
5	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
6	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
7	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
8	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
9	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
10	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
11	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
12	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
13	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
14	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled
15	100Base-TX	Broken	129	19	<input type="checkbox"/>	Enabled

## 【Port】

ポート番号を表示します。

## 【Type】

転送速度および転送モードを表示します。

## 【STA State】

スパンニングツリー内の、ポートの現在の状態を表示します。

- ・Blocken : 何もリンクが確立していないか、ユーザによって無効に設定されています。
- ・Bloking : 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送信しました。ポートアドレスはクリアされ、再びアドレス学習を開始します
- ・Forwarding : パケットを転送し、アドレス学習を続けます

## 【Priority】

STAアルゴリズム内の、ポートの優先度(プライオリティ)を設定します。スイッチの全ポートでパスコストが同じときは、プライオリティの最も高いポートがスパンニングツリー内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になります。工場出荷状態は「128」に設定されています。

- ・0~255 : ポートのプライオリティを設定します。値が低いほど、プライオリティは高くなります

### 【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。より高速なメディアに低い値を、低速メディアに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優先されます。工場出荷状態は「18」に設定されています。

- ・0～65535：パスコストを設定します

### 【Fast Forwarding】

指定ポートで、ファストスパニングツリーモードを設定します。このモードでは、ポートはBlocking、Listening、およびLearningの各ステートを飛ばして直接Forwardingステータに移行します。

- ・チェック有り：有効
- ・チェック無し：無効

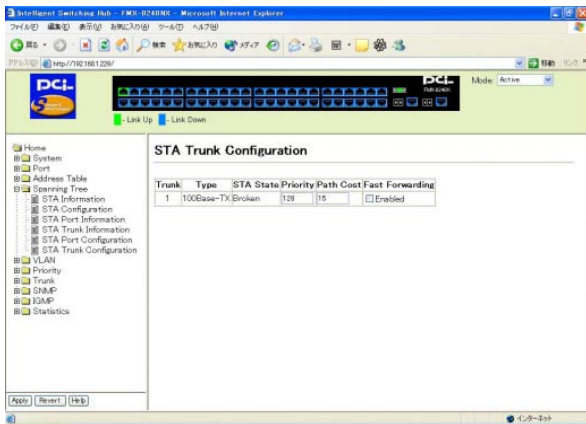
### 【Trunk】

トランクグループに属しているときにトランク番号を表示します。



## 30. STA Trunk Configuration

項目メニューから「Home」「Spanning Tree」「STA Trunk Configuration」を選択すると、以下の画面が表示されます。スパニングツリーアルゴリズムのトランクグループの設定をします。



### 【Trunk】

トランクグループ番号を表示します。

### 【Type】

転送速度および転送モードを表示します。

## 【STA State】

スパンニングツリー内の、トランクグループの現在の状態を表示します。

- ・ Bloken : 何もリンクが確立していないか、ユーザによって無効に設定されています。または、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送信しました。ポートアドレスはクリアされ、再びアドレス学習を開始します
- ・ Forwarding : パケットを転送し、アドレス学習を続けます

## 【Priority】

STAアルゴリズム内の、トランクグループの優先度(プライオリティ)を設定します。スイッチの全ポートでパスコストが同じときは、プライオリティの最も高いポートがスパンニングツリー内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になります。工場出荷状態は「128」に設定されています。

- ・ 0 ~ 255 : ポートのプライオリティを設定します。値が低いほど、プライオリティは高くなります

### 【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。より高速なメディアに低い値を、低速メディアに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優先されます。工場出荷状態は「18」に設定されています。

- ・0～65535：パスコストを設定します

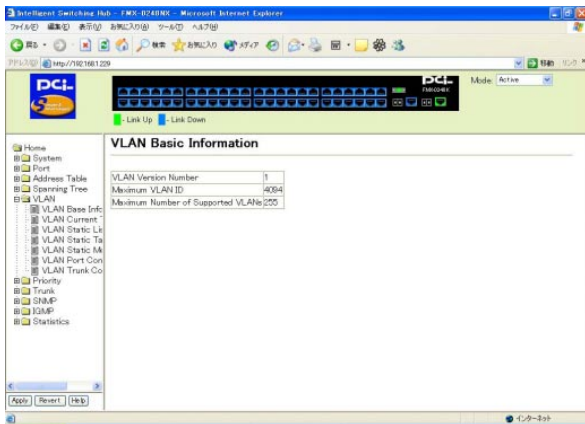
### 【Fast Forwarding】

指定トランクグループで、ファストスパニングツリーモードを設定します。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。

- ・チェック有り：有効
- ・チェック無し：無効

## 31. VLAN Base Information

項目メニューから「Home」「VLAN」「VLAN Base Information」を選択すると、以下の画面が表示されます。IEEE802.1Q VLANの基本的な情報を表示します。



### 【VLAN Version Number】

使用可能なVLANバージョンを表示します。

### 【Maximum VLAN ID】

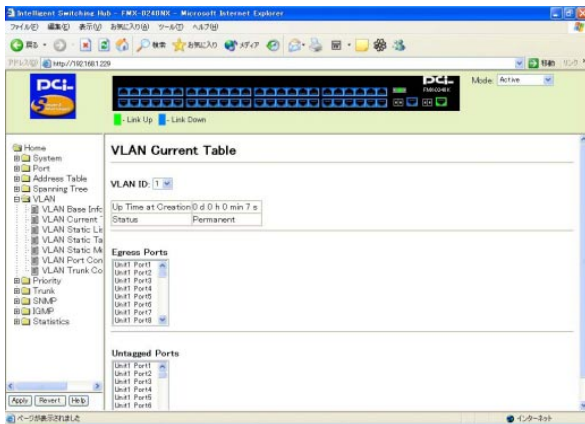
使用可能なVLAN ID数を表示します。

### 【Maximum Number of Supported VLANs】

本製品上で設定可能なVLANグループ数を表示します。

## 32. VLAN Current Table

項目メニューから「Home」「VLAN」「VLAN Current Table」を選択すると、以下の画面が表示されます。VLANグループごとの情報を表示します。



### 【VLAN ID】

表示したいVLAN IDを選択します。

### 【Up Time at Creation】

指定したVLAN IDが起動何時間後に作成されたか表示します。

### 【Status】

VLAN IDが本製品にどのように作成されたか表示します。

- ・Dynamic GVRP : 動的に作成されたVLANグループ
- ・Permanent : 静的に作成したVLANグループ

**【Egress Ports】**

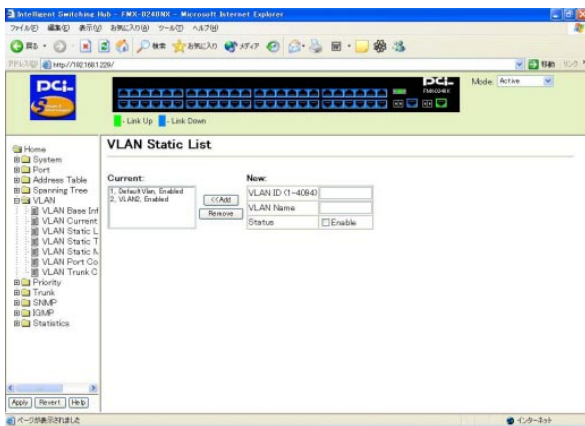
VLANメンバー送受信するフレームにVLANタグを追加して送受信するポートを表示します。

**【Untagged Ports】**

フレームにVLANタグを付けずに送受信するポートを表示します。

### 33. VLAN Static List

項目メニューから「Home」「VLAN」「VLAN Static List」を選択すると、以下の画面が表示されます。VLANグループの作成、削除をします。本製品は最大256個のVLANが設定できます。



#### 【Current】

現在作成されているVLANグループを表示します。

#### 【VLAN ID】

作成するVLAN IDを選択します。

\* 2 ~ 4094まで設定可能

VLAN ID「1」は工場出荷時から設定されているため、選択することはできません。

### 【VLAN Name】

作成したVLAN IDに管理しやすい名前を設定します。

\* 無し、または最小1文字から最大半角英数22文字まで可能

### 【Status】

VLANグループの有効/無効を設定します。

- ・チェック有り：有効
- ・チェック無し：無効

### 【<<Add】

「VLAN ID」, 「VLAN Name」, 「VLAN Name」を設定して「<<Add」をクリックするとVLANグループが追加されます。

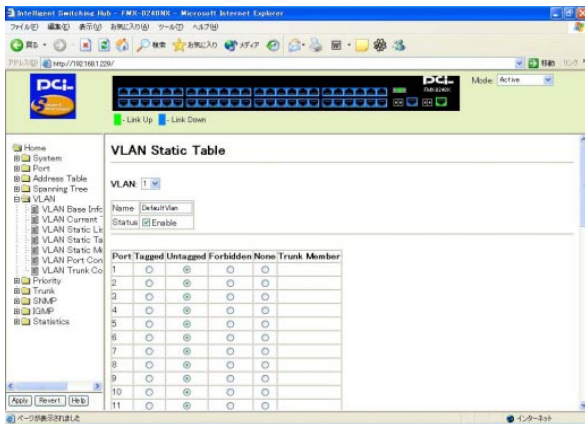
### 【Remove】

「Current」から削除したいVLANグループを選択して「Remove」をクリックするとVLANグループを削除します。



## 34. VLAN Static Table

項目メニューから「Home」「VLAN」「VLAN Static List」を選択すると、以下の画面が表示されます。各VLANグループに属させるポートを設定します。



### 【VLAN】

設定したいVLAN IDを選択します。

### 【Name】

選択したVLAN IDの名前を表示します。名前の変更を行うことができます。無し、または最小1文字から最大半角英数22文字まで可能

### 【Status】

VLANグループの有効/無効を設定します。

- ・チェック有り：有効
- ・チェック無し：無効

**【Port】**

ポート番号を表示します。

**【Tagged】**

選択したVLAN IDにタグ付でポートを属させたいときに選択します。

**【Untagged】**

選択したVLAN IDにタグ無しでポートを属させたいときに選択します。

**【Forbidden】**

GVRPの有効/無効に関わらずVLAN間の通信を行わないように設定したポートを属させたいときに選択します。

**【None】**

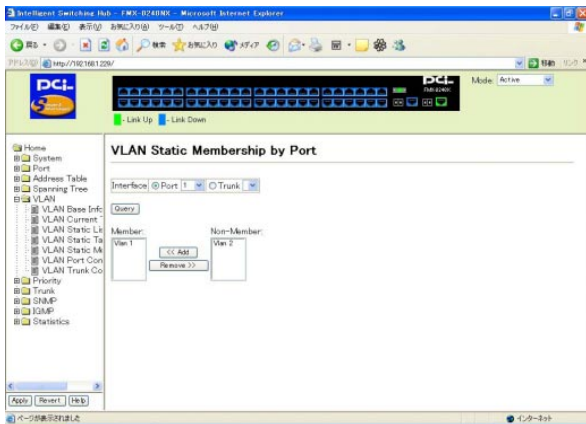
選択したVLAN IDに属させないようにします。

**【Trunk Member】**

ポートがトランクグループに属しているときはトランク番号が表示されます。

## 35. VLAN Static Membership by Port

項目メニューから「Home」「VLAN」「VLAN Static List」を選択すると、以下の画面が表示されます。各ポートまたは各トランクグループに属させるVLANグループを設定します。



### 【Interface】

設定を行うインターフェイスを選択します。

- ・Port: ポート単位で設定するときに選択します。
- ・Trunk: トランクグループを設定するときに選択します。

### 【Query】

Interfaceを選択した後に「Query」をクリックすると現在のインターフェイス状態を表示します。

### 【Member】

選択したインターフェイスが所属しているVLANグループが表示されます。

### 【Non-Member】

作成はされているが選択したインターフェイスが所属していないVLANグループが表示されます。

### 【<<Add】

「Non-Member」に表示されているVLANグループ選択して「<<Add」をクリックするとMemberに所属できます。

VLANグループを追加したときはタグ付で所属するため、タグ無しに変更するときは「VLAN Static Table」で変更をしてください。

### 【Remove】

「Member」に表示されているVLANグループ選択して「Remove」をクリックすると所属を解除できます。

## 36. VLAN Port Configuration

項目メニューから「Home」「VLAN」「VLAN Port Configuration」を選択すると、以下の画面が表示されます。各ポートの詳細設定を変更できます。

Port	PVID	Acceptable Frame Type	Ingress Filtering	QVRP Status	GARP Join Timer	GARP Leave Timer	GARP LeaveAll Timer	Trunk Member	Mode
1	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
2	2	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
3	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
4	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
5	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
6	2	Tagged	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		10 Trunk
7	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
8	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
9	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
10	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
11	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
12	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
13	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid

### 【Port】

ポート番号を表示します。

### 【PVID】

各ポートに設定するPVIDを指定します。

VLANグループにポートを属させるときにタグ付に設定したときは「Acceptable Frame Type」で「tagged」にタグ無し等に設定したときは「ALL」にします。

### 【Acceptable Frame Type】

設定したいIPVIDを選択したときにVLANスタティックテーブルで指定した送受信方法に合わせます。

- ・ALL: 「Untagged」、「Forbidden」を選択したときに設定します。
- ・tagged: 「Tagged」を選択したときに設定します。

### 【Ingress Filtering】

イングレスフィルタリングを設定します。有効にするときはチェックを付けます。

- ・チェック有り: 有効
- ・チェック無し: 無効

### 【GVRP Status】

GVRPを設定します。有効にするときは、本製品全体のGVRPが有効になっている必要があります。

- ・チェック有り: 有効
- ・チェック無し: 無効

### 【GARP Join Timer】

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。工場出荷状態は「20」に設定されています。

### 【GARP Leave Timer】

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2倍以上の値に設定します。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び参加できるようになります。工場出荷状態は「60」に設定されています。

### 【GARP LeaveAll Timer】

LeaveAllクエリ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。グループに再び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、LeaveAllはLeaveTimeより大きい値を設定します。工場出荷状態は「1000」に設定されています。

### 【Trunk Member】

ポートがトランクグループに属しているときはトランク番号が表示されます。

## 37. VLAN Trunk Configuration

項目メニューから「Home」「VLAN」「VLAN Trunk Configuration」を選択すると、以下の画面が表示されます。各トランクグループの詳細設定を変更できます。

Trunk PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer	GARP Leave Timer	GARP Leave All Timer	
3	1	ALL	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	20	60	1000

### 【Trunk】

トランクグループ番号を表示します。

### 【PVID】

各ポートに設定するPVIDを指定します。

VLANグループにポートを属させるときにタグ付に設定したときは「Acceptable Frame Type」で「tagged」にタグ無し等に設定したときは「ALL」にします。



### 【Acceptable Frame Type】

設定したいPVIDを選択したときにVLANスタティックテーブルで指定した送受信方法に合わせます。

- ・ALL：「Untagged」、「Forbidden」を選択したときに設定します。
- ・tagged：「Tagged」を選択したときに設定します。

### 【Ingress Filtering】

イングレスフィルタリングを設定します。有効にするときはチェックを付けます。

- ・チェック有り：有効
- ・チェック無し：無効

### 【GVRP Status】

GVRPを設定します。有効にするときは、本製品全体のGVRPが有効になっている必要があります。

- ・チェック有り：有効
- ・チェック無し：無効

### 【GARP Join Timer】

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。工場出荷状態は「20」に設定されています。

### 【GARP Leave Timer】

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2倍以上の値に設定します。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び参加できるようになります。工場出荷状態は「60」に設定されています。

### 【GARP LeaveAll Timer】

LeaveAllクエリ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。グループに再び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、LeaveAllはLeaveTimeより大きい値を設定します。工場出荷状態は「1000」に設定されています。

## 38. Port Priority Configuration

項目メニューから「Home」「Priority」「Default Port Priority」を選択すると、以下の画面が表示されます。各ポートの着信するパケットのイングレスプライオリティ値を設定します。プライオリティ値より低いものは低プライオリティ用キューに、プライオリティ値と同じまたは高いものは高プライオリティ用キューに渡します。

Port	Default Priority	Number of Egress Traffic Classes	Trunk
1	0 (0-7)	4	
2	0 (0-7)	4	
3	0 (0-7)	4	
4	0 (0-7)	4	
5	0 (0-7)	4	
6	0 (0-7)	4	
7	0 (0-7)	4	
8	0 (0-7)	4	
9	0 (0-7)	4	
10	0 (0-7)	4	
11	0 (0-7)	4	
12	0 (0-7)	4	
13	0 (0-7)	4	
14	0 (0-7)	4	
15	0 (0-7)	4	

### 【Port】

ポート番号を表示します。

### 【Default Priority】

着信するパケットのイングレスプライオリティ値を設定します。工場出荷状態は「0」に設定されています。

**【Number of Egress Traffic Classes】**

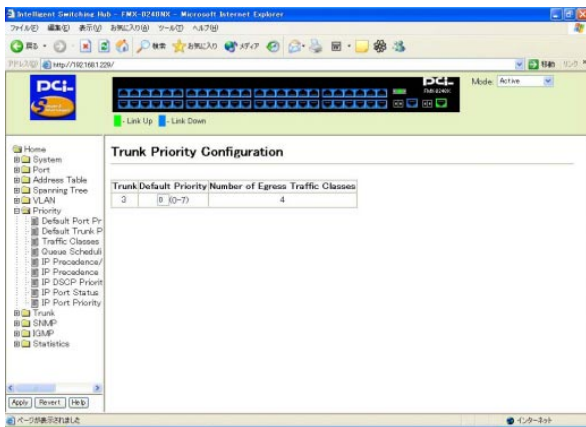
各ポートに供給されるキュー・バッファーの数です。

**【Trunk】**

ポートがトランクグループに属しているときはトランク番号が表示されます。

## 39. Trunk Priority Configuration

項目メニューから「Home」「Priority」「Default Trunk Priority」を選択すると、以下の画面が表示されます。各トランクグループの着信するパケットのイングレスプライオリティ値を設定します。プライオリティ値より低いものは低プライオリティ用キューに、プライオリティ値と同じまたは高いものは高プライオリティ用キューに渡します。



### 【Trunk】

トランクグループ番号を表示します。

### 【Default Priority】

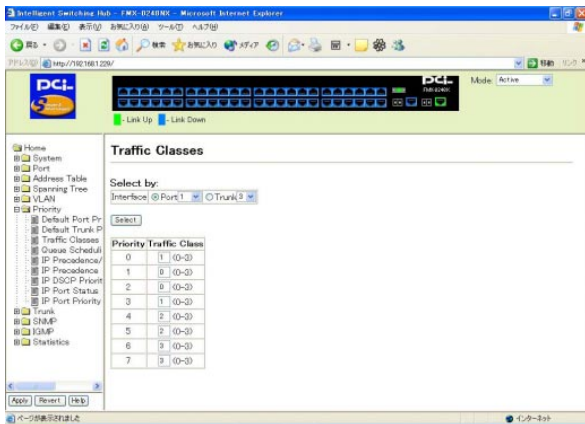
着信するパケットのイングレスプライオリティ値を設定します。工場出荷状態は「0」に設定されています。

### 【Number of Egress Traffic Classes】

各ポートに供給されるキュー・バッファの数です。

## 40. Traffic Classes

項目メニューから「Home」「Priority」「Traffic Classes」を選択すると、以下の画面が表示されます。インターフェイスごとのプライオリティ値のトラフィッククラスを設定します。



### 【Interface】

設定を行うインターフェイスを選択します。

- ・Port: ポート単位で設定するときを選択します。
- ・Trunk: トランクグループを設定するときを選択します。

### 【Priority】

プライオリティ値のレベルが表示されます。

## 【Traffic Class】

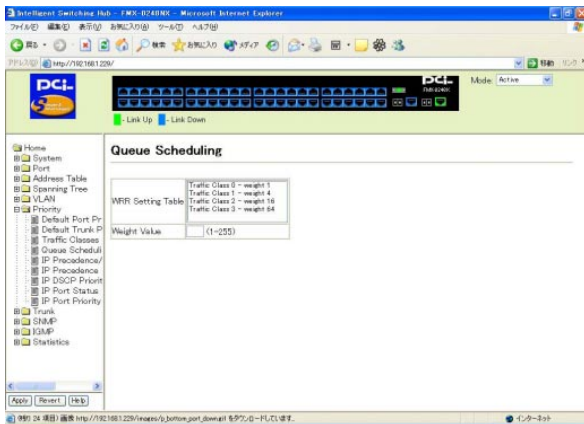
トラフィッククラスを設定します。工場出荷状態は以下のように設定されています。

	キュー			
	0	1	2	3
プライオリティ	1 2	0  3	  4 5	   6 7

表4-1 トラフィッククラス

## 41. Queue Scheduling

項目メニューから「Home」「Priority」「Queue Scheduling」を選択すると、以下の画面が表示されます。各キューのウェイトを設定します。



### 【WRR Setting Table】

現在の各キューのウェイトが表示されます。工場出荷状態は以下のように設定されています。

- ・トラフィッククラス0：ウェイト1
- ・トラフィッククラス1：ウェイト4
- ・トラフィッククラス2：ウェイト16
- ・トラフィッククラス3：ウェイト64

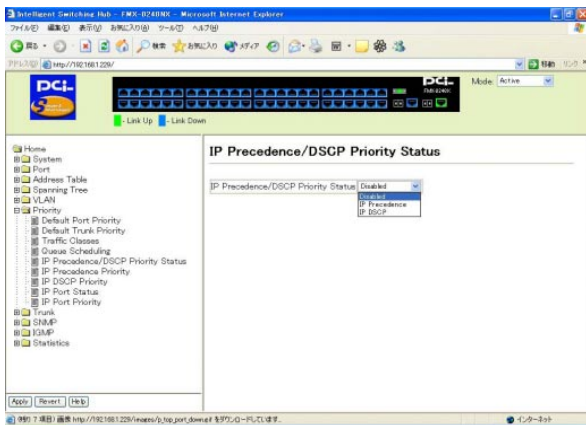
### 【Weight Value】

変更するウェイト値を設定します。WRR Setting Tableで変更したいトラフィッククラスを指定してWeight Valueにウェイト値を入力します。



## 42. IP Precedence/DSCP Priority Status

項目メニューから「Home」「Priority」「IP Precedence/DSCP Priority Status」を選択すると、以下の画面が表示されます。トラフィックの優先事項を使用するのにIP PrecedenceとDSCPのどちらを使用するか設定します。



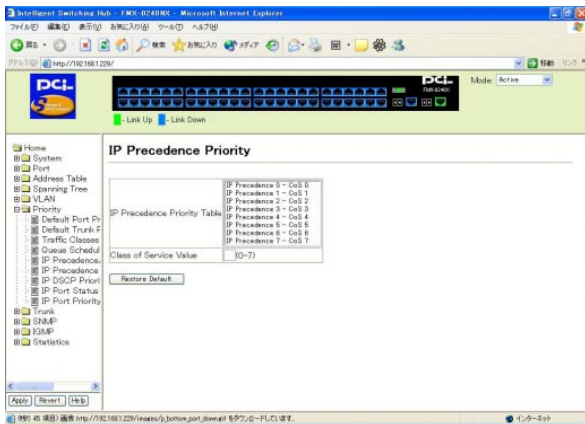
### 【IP Precedence/DSCP Priority Status】

使用する優先事項を設定します。

- IP Precedence : IP Precedenceを使用します。
- DSCP : DSCPを使用します。
- Disabled : IP Precedence、DSCPの両方とも使用しません。

## 43. IP Precedence Priority

項目メニューから「Home」「Priority」「IP Precedence Priority」を選択すると、以下の画面が表示されます。IP Precedenceのプライオリティを表示、設定します。



### 【IP Precedence Priority Table】

各IP PrecedenceクラスのCoSプライオリティレベルが表示されます。

### 【Class of Service Value】

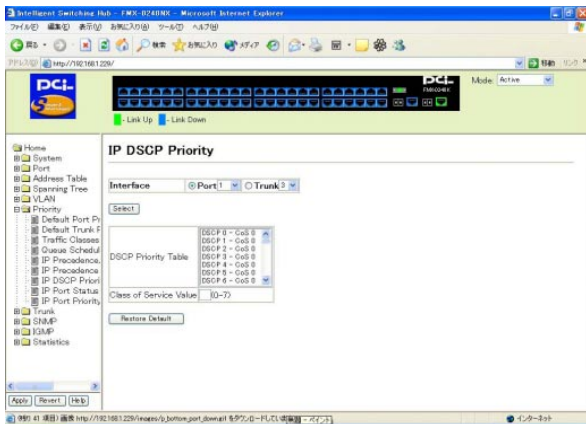
「IP Precedence Priority Table」で指定したIP Precedenceクラスのプライオリティレベルを設定します。

### 【Restore Default】

IP Precedenceクラスのプライオリティレベルを工場出荷状態に戻します。

## 44. IP DSCP Priority

項目メニューから「Home」「Priority」「IP DSCP Priority」を選択すると、以下の画面が表示されます。DSCPプライオリティを表示、設定します。



### 【Interface】

DSCPを設定するインターフェイスを選択します。

- ・Port: ポート単位で設定します。
- ・Trunk: トランク単位で設定します。

### 【DSCP Priority Table】

各DSCPクラスのCoSプライオリティレベルが表示されます。

### 【Class of Service Value】

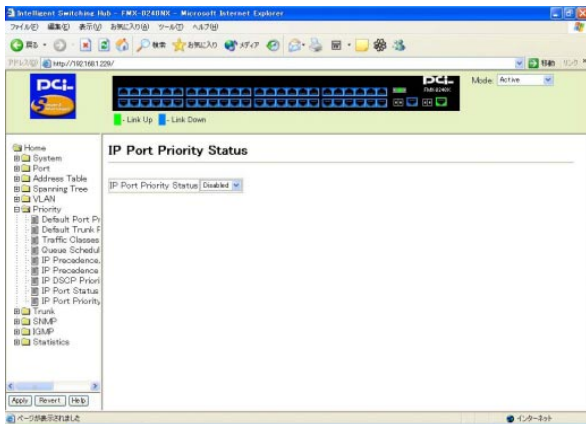
「DSCP Priority Table」で指定したDSCPクラスのプライオリティレベルを設定します。

### 【Restore Default】

DSCPクラスのプライオリティレベルを工場出荷状態に戻します。

## 45. IP Port Priority Status

項目メニューから「Home」「Priority」「IP Port Priority Status」を選択すると、以下の画面が表示されます。IPポート・プライオリティの有効/無効を設定します。



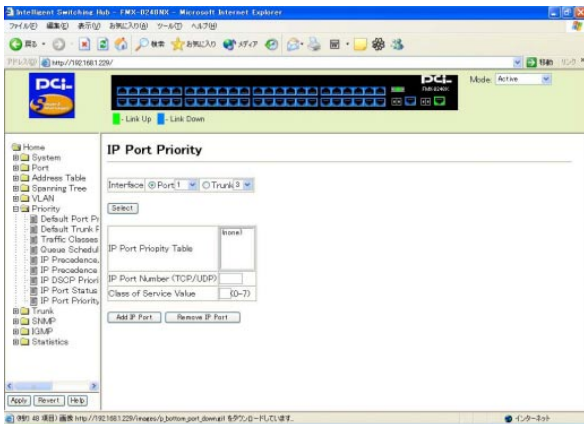
### 【IP Port Priority Status】

IPポート・プライオリティの有効/無効を設定します。

- ・ENABLED : 有効
- ・DISABLED : 無効

## 46. IP Port Priority

項目メニューから「Home」「Priority」「IP Port Priority」を選択すると、以下の画面が表示されます。各ポートのIPポートおよびCoSプライオリティレベルを表示、設定します。



### 【Interface】

IPポートを設定するインターフェイスを選択します。

- ・Port : ポート単位で設定します。
- ・Trunk : トランク単位で設定します。

### 【IP Port Priopity Table】

作成したIPポート番号に対してのCoSプライオリティレベル

### 【IP Port Number ( TCP/UDP )】

IPポート番号を指定します。

### 【Class of Service Value】

指定したIPポート番号に対してのCoSプライオリティレベルを設定します。

### 【Add IP Port】

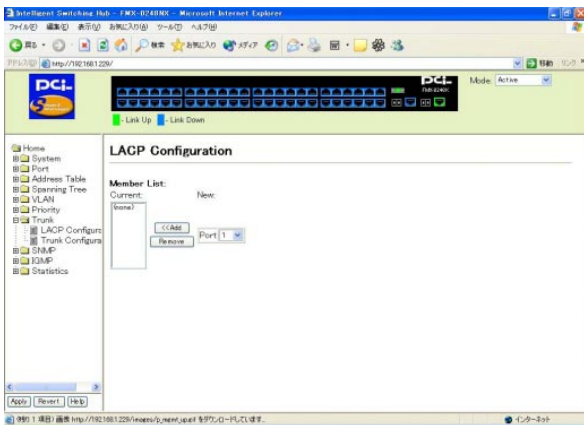
IPポート番号とCoSプライオリティレベルを設定後、クリックすると「IP Port Priopity Table」に作成したIPポートのプライオリティレベルが表示されます。

### 【Remove IP Port】

「IP Port Priopity Table」に現在登録されているIPポートのプライオリティレベルを選択して、クリックをすると選択したIPポートのプライオリティレベルは削除されます。

## 47 LACP Configuration

項目メニューから「Home」「Trunk」「LACP Configuration」を選択すると、以下の画面が表示されます。Link Aggregation (LACP)グループのポートの追加、削除の設定をします。



### 【Current】

Link Aggregation (LACP)グループに現在登録されているポートを表示します。

### 【New】

Link Aggregation (LACP)グループに追加したいポート番号を指定します。

### 【<<Add】

「New」で指定したポートをLink Aggregation (LACP)グループに追加するときにクリックします。

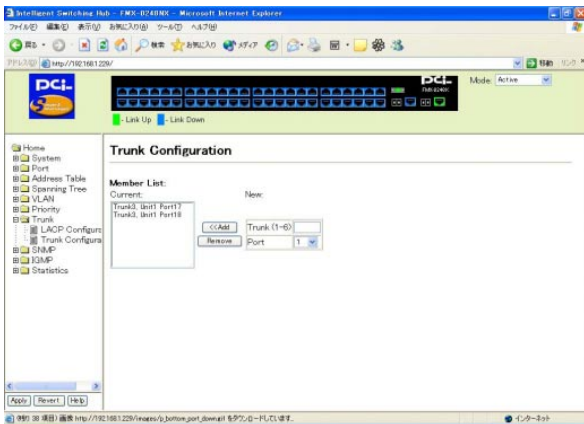


### 【Remove】

Link Aggregation( LACP )グループに現在登録されているポートを削除するときに「Current」で削除したいポートを選択してクリックします。

## 48. Trunk Configuration

項目メニューから「Home」「Trunk」「Trunk Configuration」を選択すると、以下の画面が表示されます。トランクグループのポートの追加、削除の設定をします。



### 【Current】

トランクグループに現在登録されているトランク番号とポート番号を表示します。

### 【New】

トランクグループに追加したいトランク番号とポート番号を指定します。

### 【<<Add】

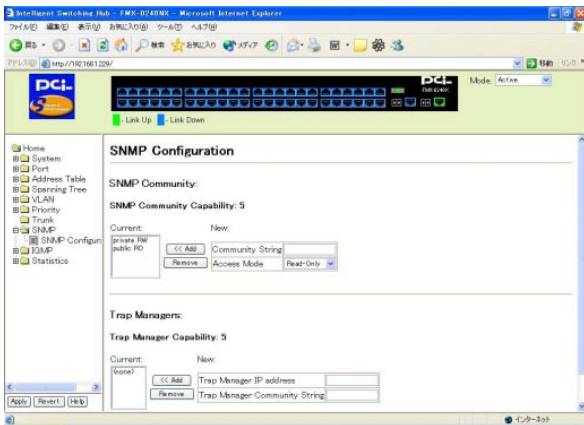
「New」で指定したトランク番号とポート番号をトランクグループに追加するときをクリックします。

## 【Remove】

トランクグループに現在登録されているトランク番号とポート番号の組み合わせを削除するときに「Current」で削除したいトランク番号とポート番号の組み合わせを選択してクリックします。

## 49 SNMP Configuration

項目メニューから「Home」「SNMP」「SNMP Configuration」を選択すると、以下の画面が表示されます。SNMPエージェントの接続を許可するコミュニティの設定と認証に失敗したときなどのトラップメッセージの設定をします。



### SNMP Community

コミュニティ名の設定をします。

#### 【Current】

現在作成されているコミュニティ名とアクセスレベルを表示します。

- ・RW：読み込みと書き込み可能
- ・RO：読み込み専用

### 【New】

追加したいコミュニティ名を設定します。

- ・Community String: 接続を許可するコミュニティ名を設定します。最大32文字の半角英数字で設定します。工場出荷状態は「private」と「public」が設定されています。
- ・Access Mode: Read Only(読み込み専用)とRead/Write(読み込みと書き込み可能)があります。

### 【<<Add】

「New」で指定したコミュニティ名を追加するときにクリックします。

### 【Remove】

「Current」に現在登録されているコミュニティ名を削除するときに「Current」で削除したいコミュニティ名を選択してクリックします。

#### Trap Managers

トラップメッセージを送信するIPアドレスを設定します。

### 【Current】

現在作成されているトラップメッセージを送信するIPアドレスを表示します。

### 【New】

追加したいトラップメッセージを送信するIPアドレスの設定をします。

- ・Trap Manager IP address  
：トラップメッセージを送信するIPアドレスを設定します。
- ・Trap Manager Community String  
：トラップメッセージを送信するときに使用するコミュニティ名を設定します。

#### 【<<Add】

「New」で指定したトラップの送信IPアドレスを追加するときにクリックします。

#### 【Remove】

「Current」に現在登録されている送信IPアドレスを削除するときに「Current」で削除したい送信IPアドレスを選択してクリックします。

#### 【Enable Authentication Traps】

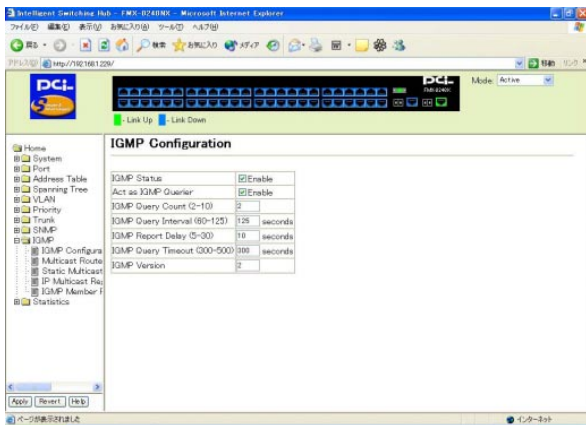
認証時のトラップを設定します。

本製品にネットワーク管理ステーションから接続したとき、認証に失敗すると、あらかじめ設定した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。工場出荷状態は「チェック有り」に設定されています。

- ・チェック有り：認証トラップを有効
- ・チェック無し：認証トラップを無効

## 50. IGMP Configuration

項目メニューから「Home」「IGMP」「IGMP Configuration」を選択すると、以下の画面が表示されます。IGMPスヌーピングの基本設定をします。



### 【IGMP Status】

IGMPスヌーピングの有効/無効が設定をします。

- ・チェック有り：有効
- ・チェック無し：無効

### 【Act as IGMP Querier】

IGMPクエリーの有効/無効が設定をします。

- ・チェック有り：有効
- ・チェック無し：無効

### 【IGMP Query Count】

接続するクエリーの数を設定します。工場出荷状態は「2」に設定されています。

- ・設定範囲：2～10

### 【IGMP Query Interval】

クエリーを再構築する間隔を設定します。工場出荷状態は「125」に設定されています。

- ・設定範囲：60～125

### 【IGMP Report Delay】

クエリーの再構築情報を送り、そのリストからエントリーを取り除く前に、ポート上のIPマルチキャストアドレスのIGMP情報を受け取る間隔を設定します。工場出荷状態は「10」に設定されています。

- ・設定範囲：5～30

### 【IGMP Query Timeout】

接続中のクエリーが切断した後、次のクエリーに接続するまでの待機時間を設定します。工場出荷状態は「300」に設定されています。

- ・設定範囲：300～500

### 【IGMP Version】

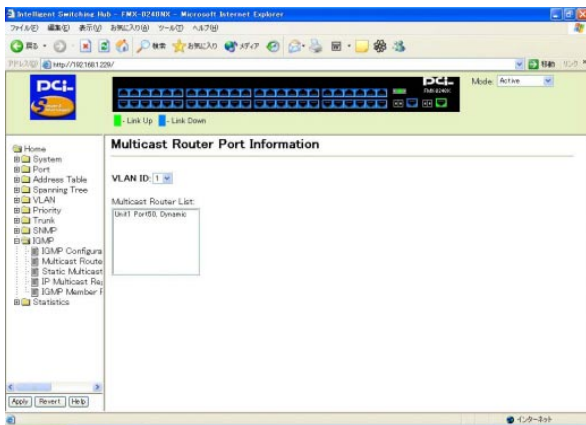
ネットワーク上のIGMPスヌーピングのバージョンを合わせるためにバージョンを設定します。工場出荷状態は「2」に設定されています。

- ・1：IGMP-v1
- ・2：IGMP-v2



## 51. Multicast Router Port Information

項目メニューから「Home」「IGMP」「Multicast Router Port Information」を選択すると、以下の画面が表示されます。VLANグループごとにマルチキャストルータポートに指定されているポートを表示します。



### 【VLAN ID】

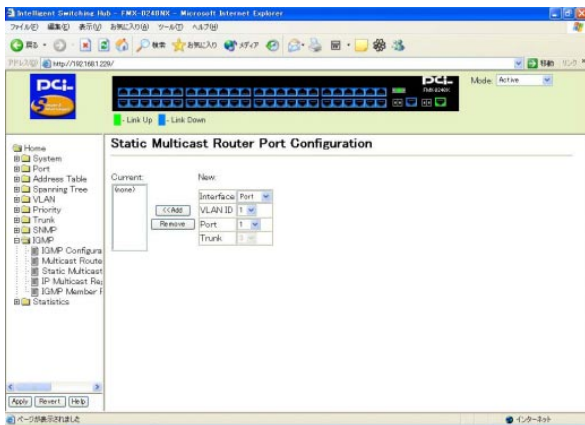
ルータポートを表示したいVLAN IDを設定します。

### 【Multicast Router List】

設定したVLAN IDのルータポートに指定したポートの状態を表示します。

## 52. Static Multicast Router Port Configuration

項目メニューから「Home」「IGMP」「Static Multicast Router Port Configuration」を選択すると、以下の画面が表示されます。静的にルータポートを設定します。



### 【Current】

現在作成されている静的ルータポートを表示します。

### 【Interface】

ルータポートを作成するインターフェイスを設定します。

- ・Port: ポート単位でルータポートを設定するときに選択します。
- ・Trunk: トランクグループでルータポートを設定するときに選択します。

**【VLAN ID】**

設定するVLAN IDを指定します。

**【Port】**

InterfaceでPortを選択したときは設定したいポートを指定します。

**【Trunk】**

InterfaceでTrunkを選択したときは設定したいトランクグループを指定します。

**【<<Add】**

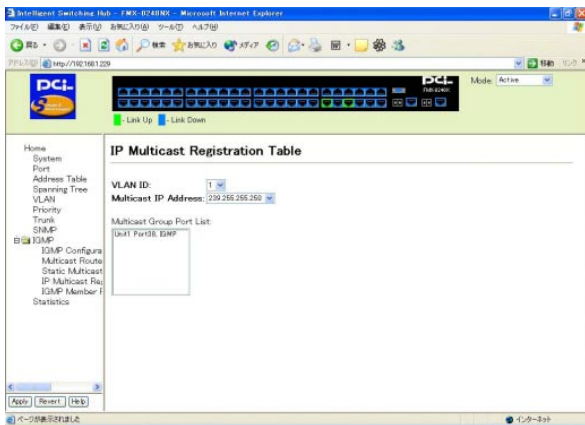
「New」で指定した静的ルータポートを追加するときにクリックします。

**【Remove】**

「Current」に現在登録されている静的ルータポートを削除するときに「Current」で削除したい静的ルータポートを選択してクリックします。

## 53. IP Multicast Registration Table

項目メニューから「Home」「IGMP」「IP Multicast Registration Table」を選択すると、以下の画面が表示されます。マルチキャストIPアドレスごとのルータポートを表示します。



### 【VLAN ID】

ルータポートを表示するVLAN IDを指定します。

### 【Multicast IP Address】

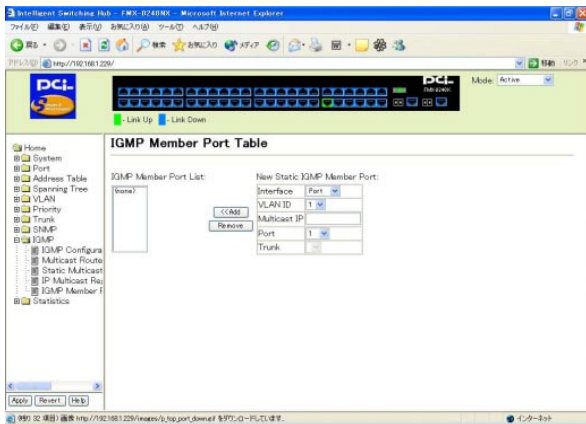
指定したVLAN ID内で取得しているマルチキャストIPアドレスを表示します。マルチキャストIPアドレスを指定します。

### 【Multicast Group Port List】

指定したマルチキャストIPアドレスのルータポートを表示します。

## 54. IGMP Member Port Table

項目メニューから「Home」「IGMP」「IGMP Member Port Table」を選択すると、以下の画面が表示されます。静的にマルチキャストを配布するポートを設定します。



### 【IGMP Member Port List】

現在作成されている静的マルチキャストポートを表示します。

### 【Interface】

静的マルチキャストポートを作成するインターフェイスを設定します。

- ・Port: ポート単位で静的マルチキャストポートを設定するときに選択します。
- ・Trunk: トランクグループで静的マルチキャストポートを設定するときに選択します。

**【VLAN ID】**

設定するVLAN IDを指定します。

**【Multicast IP】**

静的マルチキャストポートに配布するマルチキャストIPアドレスを設定します。

**【Port】**

InterfaceでPortを選択したときは設定したいポートを指定します。

**【Trunk】**

InterfaceでTrunkを選択したときは設定したいトランクグループを指定します。

## 55. Port Statistics

項目メニューから「Home」「Statistics」「Port Statistics」を選択すると、以下の画面が表示されます。各ポートのInterface GroupおよびEthernet MIBに関する統計情報が表示されます。表示される値は、システムを再起動した時点からの累計です。ポートの不良や負荷の異常状態などの問題を判断するときに使います。

The screenshot shows a web browser window displaying the DCI network management interface. The main content area is titled 'Port Statistics'. Below this title, there are dropdown menus for 'Interface' and 'Port', and a 'Query' button. The 'Interface Statistics' section contains a table with the following data:

Interface Statistics:	
Received Octets	23125
Received Multicast Packets	0
Received Discarded Packets	0
Received Errors	0
Transmit Unicast Packets	548
Transmit Broadcast Packets	8813
Transmit Errors	0

The 'Etherlike Statistics' section contains a table with the following data:

Etherlike Statistics:	
Alignment Errors	0
FCS Errors	0
Single Collision Frames	0

## Interface Statistics

### Interface Statistics:

Received Octets	13870204	Received Unicast Packets	15593
Received Multicast Packets	64837	Received Broadcast Packets	58017
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	2385448
Transmit Unicast Packets	15604	Transmit Multicast Packets	4
Transmit Broadcast Packets	0	Transmit Discarded Packets	0
Transmit Errors	0		

#### 【Received Octets】

インターフェース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。

#### 【Received Unicast Packets】

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数です。

#### 【Received Multicast Packets】

受信された有効フレームのうち、マルチキャストアドレスに転送された数です。

#### 【Received Broadcast Packets】

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数です。マルチキャストパケットは除きます。

#### 【Received Discarded Packets】

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パケット数です。パケットを破棄する理由は、バッファ領域を空ける目的も含まれます。

#### 【Received Unknown Packets】

受信された有効フレームのうち、マルチキャストアドレス、ブロードキャストアドレス以外に転送された数です。

#### 【Received 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パケット数です。



#### 【Transmit Octets】

インターフェースから送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。

#### 【Transmit Unicast Packets】

高位層プロトコルの要求によって、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数です。破棄または送信されなかったパケットも含まれます。

#### 【Transmit Multicast Packets】

送信した有効フレームのうち、マルチキャストアドレスに転送した数です。

#### 【Transmit Broadcast Packets】

送信し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した数です。マルチキャストパケットは除きます。

#### 【Transmit Discarded Packets】

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パケット数です。パケットを破棄する理由は、バッファ領域を空ける目的も含まれます

#### 【Transmit Errors】

エラーが含まれるため送信できなかった送信パケット数です。

## Etherlike Statistics

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

### 【Alignment Errors】

アライメントエラー(同期に失敗した)のパケット数です。

### 【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。

### 【FCS Errors】

64オクテットより短い受信フレームのうち、FCSまたはアライメントエラーを持った数です。また1518オクテットより長い受信フレームのうち、FCSまたはアライメントエラーを持った数です。ただし、フレーミングビットは除き、FCSオクテットは含まれます。

### 【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。

### 【Single Collision Frames】

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数です。

#### 【Internal MAC Transmit Errors】

スイッチ内部でMACアドレスエラーにより転送に失敗したフレームの数を表示します。

#### 【Multiple Collision Frames】

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数です。

#### 【Carrier Sense Errors】

フレーム送信を試みたとき、キャリアセンス状態が失われたか、またはこの状態にならなかった数です。

#### 【SQE Test Errors】

PLS層でSQEテストエラーメッセージが発生した場合の総数を表示します。

#### 【Frames Too Long】

許可された最大フレーム数を超えた受信済みフレームの総数を表示します。

#### 【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の一回目の送信試行が失敗したフレームの数です。

#### 【Internal MAC Receive Errors】

受け入れの失敗により内部のMAC層で受信エラーになったフレームの総数を表示します。

## RMON Statistics

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	20204502	Collisions	0
Received Frames	184548	64 Bytes Frames	129544
Broadcast Frames	61629	85-127 Bytes Frames	24432
Multicast Frames	66402	128-255 Bytes Frames	13796
CRC/Alignment Errors	0	256-511 Bytes Frames	15567
Undersize Frames	0	512-1023 Bytes Frames	511
Oversize Frames	0	1024-1518 Bytes Frames	698
Fragments	0		

### 【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合計です。

### 【Jabbers】

受信フレームのうち、1518オクテットより長く、かつFCSまたはアライメントエラーが含まれる数です。ただし、フレーミングビットは除き、FCSオクテットは含まれます。

### 【Received Bytes】

高位層プロトコルに渡されたバイト数です。

### 【Collisions】

このEthernetセグメントで発生するコリジョンの予想発生数です。

### 【Received Frames】

高位層プロトコルに渡されたフレーム数です。

### 【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数です。マルチキャストパケットは除きます。

#### 【Multicast Frames】

受信された有効フレームのうち、マルチキャストアドレスに転送された数です。ブロードキャストパケットは除きます。

#### 【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 )の合計です。

#### 【Undersize Frames】

受信フレームのうち、64オクテットより短いことを除き、他に問題が検出されなかったフレームの数です。ただし、フレーミングビットは除き、FCSオクテットは含まれます。

#### 【Oversize Frames】

受信フレームのうち、1518オクテットより長いことを除き、他に問題が検出されなかったフレームの数です。ただし、フレーミングビットは除き、FCSオクテットは含まれます。

#### 【Fragments】

受信フレームのうち、64オクテットより短く、かつFCSまたはアライメントエラーが含まれる数です。ただし、フレーミングビットは除き、FCSオクテットは含まれます。

#### 【64 Bytes Frames】

送受信したフレームのうち、長さが64オクテットの数です。ただし、フレーミングビットは除き、不良パケットやFCSオクテットは含まれます。

**【65-127 Bytes Frames】**

送受信したフレームのうち、長さが範囲内の数です。ただし、フレームングビットは除き、不良パケットやFCSオクテットは含まれません。

**【128-255 Bytes Frames】**

(同上)

**【256-511 Bytes Frames】**

(同上)

**【512-1023 Bytes Frames】**

(同上)

**【1024-1518 Bytes Frames】**

(同上)

# 5. 技術解説

FMX-0248Kは、ネットワーク機器の物理アドレスに基づくレイヤ2スイッチに対応します。これらの機能、技術解説について説明します。

## 1. レイヤ2スイッチ ( Layer 2 Switch )

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テーブル内でフレームの送信先MACアドレスを検索し、送信先ポートを確かめます。

送信先MACアドレスが他のポートで見つかったとき、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MACアドレスがアドレステーブル内で見つからないとき、フレームはタグ付またはタグ無しVLANの処理の後、ひとつまたは複数の他の出力ポートに転送されます。

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とき、フレームは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、フレーム転送を決定する際に使われます。

スイッチングの際、本製品は以下の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

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)

受信されたフレームは、以下の2種類に分類されます。

タグ無しフレームのとき、フレームを受信ポートのデフォルトVLANに分類します

タグ付フレームのとき、タグ付VLAN IDを使い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、アドレステーブル内の送信元MACアドレスとVLANの対を参照し、既知のものが確かめます。

対が未知のとき、送信元MACアドレスとVLANの対を学習し、アドレステーブルに追加します

対が既知のとき、間違っただポートIDが与えられているか確かめます。アドレステーブル内の送信元MACアドレスとVLANの対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のとき、アドレステーブル内のポートIDと、管理データベースを修正します



## フィルタリング

アドレスの学習が完了すると、フィルタリングを行います。これらの条件のうち、どれかひとつでも満たされると、受信フレームは破棄されます。どの条件もあてはまらないとき、フォワーディング処理を続けます。

送信元ポートまたは送信先ポートが、ブロッキング状態などのフォワーディング状態以外になっているか

送信元MACアドレスまたは送信先MACアドレスはフィルタ対象になっているか

送信元ポートIDと送信先ポートが同じか

## フォワーディング

フォワーディング処理中、本製品は送信先MACアドレスとVLANの対を参照し、既知のものか確かめます。

対が未知のとき、受信フレームは送信元ポートを除くVLAN内の全ポートに一括送信されます

対が既知のとき、受信フレームを送信先MACアドレスとVLANの対に関連づけられているポートに転送します。同時に、VLANタグ付またはタグ無しの設定、および出力ポートのVLAN IDの各情報に従い、フレームにVLANタグを付けるか、またはタグを取り除くか設定します。

## 2. マルチキャストスイッチング ( Multicast Switching )

マルチキャストスイッチングを行うとき、受信フレームがBPDUが判断します。

BPDUを受信したときは、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。

これ以外は、以下の処理を実行します。

VLAN識別 : ユニキャストスイッチングと同じ

ラーニング : ユニキャストスイッチングと同じ

フィルタリング : ラーニング完了後、フィルタリングする

以下の条件のうち、どれかひとつでも満たされると、受信フレームは破棄されます。どの条件もあてはまらないとき、フォワーディング処理を続けます。

送信元ポートまたは送信先ポートが、ブロッキング状態などのフォワーディング状態以外になっているか

送信元MACアドレスまたは送信先MACアドレスはフィルタ対象になっているか

送信元ポートIDと送信先ポートが同じか

### フォワーディング

受信フレームは送信元ポートを除くVLAN内の全ポートに一括送信されます。

同時に、VLANタグ付またはタグ無しの設定、および出力ポートのVLAN IDの各情報に従い、フレームにVLANタグを付けるか、またはタグを取り除くか設定します。

## エージング

MACアドレステーブル内のMACアドレスとVLANの対に対し、エージング処理します。MACアドレスとVLANの対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 ( Spanning Tree Algorithm : STA )

IEEE 802.1dで制定される、スパニングツリーアルゴリズム( STA ) は、ネットワークのループを検出すると、ループしないようにポートを無効にするなど、スイッチ・ブリッジ・ルータ間で冗長化を実現できます。本製品はSTAに対応しており、ネットワーク内の他のSTA対応機器と連絡をとり、ネットワークのどの二つの機器間においても、常にルートが一つだけになるよう調整します。

STAは、冗長パスやループを検出したとき、ひとつまたはそれ以上のポートの packets 転送を停止し、余分なパスを排除します。通常使っているリンクが使用不可になったとき、代替のリンクを自動で提供し、そのまま通信を続行できます。

また、安定したスパニングツリートポロジ内でひとつ以上のパスが使用不可になったとき、これまでブロッキングしていたポートをフォワーディングにし、全ネットワークステーションとの接続を復旧します。

STAは分布式的アルゴリズムを使い、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(ルートブリッジ機器: Root Bridging Device)を選びます。ルートブリッジ機器を除く各ブリッジ機器はルートポート(Root Port)が選ばれます。ルートポートは、その機器からルートブリッジ機器までパケットを転送するとき、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より指定ブリッジ機器を選びます。指定ブリッジ機器は、LANからルートブリッジ機器までパケットを送信するとき、パスコストが最小となるものを指します。指定ブリッジ行きに接続されたポートは、すべて指定ポート(Designated Port)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間だけ転送されるようになり、ネットワークループの発生を防げます。

安定したネットワークトポロジがいったん確定すると、すべてのブリッジ機器はルートブリッジ機器から送信されるBPDUを受信するようになります。事前に設定した期間(Maximum Age)が経過してもBPDUが受信されないとき、そのブリッジ機器は、ルートブリッジ機器とのリンクが使用不可となったと判断します。このとき、ブリッジ機器は他のブリッジ機器とネゴシエーションをはじめ、ネットワークを再設定し、使用可能なネットワークトポロジを再度構成します。

## 4. レイヤ3スイッチ ( Layer 3 Switch )

レイヤ3スイッチの特長は、IPスイッチングとルーティングパス管理があります。本製品は、マルチレイヤモードに設定すると、ルーティングスイッチとして動作し、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えるようになります。

ただし、本製品をはじめてマルチレイヤモードに設定したときは、ルーティングに必要な機能が設定されていません。マルチレイヤモードで使うとき、ルーティング機能を設定する必要があります。

## 5. IPスイッチング

IPスイッチングは、レイヤ2またはレイヤ3の処理が必要になります。以下に対応している各機能を説明します。

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は必要なく直接送信先に送信できます。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アドレスに送信できます。

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。

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できます。

## 6. 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しません。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リダイレクトを受信します。

## 7. ルーティングプロトコル

### 静的ルーティング

静的ルーティングは、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。これは手動設定および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ときも保存できます。

### 動的ルーティング

動的ルーティングはルーティングプロトコルを使い、ルーティング情報の交換、ルーティングテーブルの計算、およびネットワークの状態や負荷の変化に対応します。

本製品はRIP、RIP-2、およびOSPF v2動的ルーティングプロトコルに対応します。

## 8. RIP ( Routing Information Protocol )/ RIP-2 動的ルーティングプロトコル

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

## 9. OSPF v2動的ルーティングプロトコル (Open Shortest Path First)

### 概要

OSPFはRIPと同じIGP(内部ルーティングプロトコル群)の一種です。RIPは距離ベクトル型プロトコル(Distance Vector)アルゴリズムを使用しますが、OSPFはリンク状態型プロトコル(Link State)アルゴリズムを使用します。このLink Stateアルゴリズムでは同一エリア内にある全てのルータが同じデータベースを持ち、その中にはAS全体のトポロジーが記述されていて、到達可能なルータ、経路、そしてそれに伴うコストがわかるようになっています。それにより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。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の配分もできます。OSPFはシステムのトポロジーを正確に知っているため、トポロジーの動的変更に対応でき、収束に要する時間を大幅に減らすことができます。ASをいくつかのエリアに分割すると、より早く収束でき、ネットワークの障害に対する防御力を高めます。また、このことによりルーティングプロトコルが生成するトラフィック(つまりOSPF自身がルーティングに使用するパケット)を少なくできます。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。RIPなどの多くのルーティン

グプロトコルではホップ数をカウントする方式をとっていますが、OSPFでは実際のリンク速度に基づいてコストを計算するため、より大きなスループットをもたらすルートを選択できます。ただし、リンクコストに基づいてルートを選択する場合にはルータの性能や、リンクの信頼性は考慮されないため、必要なら管理者が手動でコストを割り当てる必要があります。

### OSPFのネットワークの構成

他のルーティングプロトコルと同じように、ルーティング情報が交換されるのは隣接するインターフェースルータとの間です。他のルーティングプロトコルと違うのは、OSPFインターフェースルータがIPマルチキャストパケットをこの交換に使い、交換とは関係のないホストの負荷を軽くすることです。ただし、これらの交換から生じるトラフィックをどう軽減するかなど、別の問題が生じることになります。

同じブロードキャストネットワーク上に多数のルータが接続されていると交換によって生じるトラフィックが大きくなるため、情報を交換するルータを制限します。OSPFではどのルータも最大で2台の隣接ルータとだけ隣接関係 (Adjacency) を結びます。

隣接関係を作る相手のルータは指名ルータ (Designated Router, DR)、およびバックアップ指名ルータ (Backup Designated Router, BDR) と呼ばれこれらのルータは特別な責任を負うもので、同じネットワーク上の全てのルータにルーティング情報を配布するのはこれらのルータの仕事となります。OSPFはネットワーク上で次のような隣接関係を形成するようになっています。

#### ・ポイントトゥポイントリンク

これは、1対のルータを専用線などで結ぶネットワークで、これらのネットワークにはIPアドレスを割り当てなくても良く。その場合このリンクは無番号といわれます。

#### ・ブロードキャストネットワーク

ブロードキャストネットワークでは、多数のルータが接続され、ブロードキャストできるようになっています。実際にはOSPFはマルチキャストを用いて隣接装置間の通信を行っていますが、複数の装置と同時に通信する原理は同じで、イーサネットもこのようなタイプのネットワークの一例です。

#### ・非ブロードキャストネットワーク

ISDN、X.25、フレームリレーなど、非ブロードキャストのマルチアクセスネットワークで、複数ルータの同時接続は可能ですが、ブロードキャストとマルチキャストの機能はありません。これらのネットワークでは全ての隣接装置に同時にパケットを送ることができず、その代わりにそれぞれの隣接装置にユニキャストで送ることになります。したがって、何かの方法で事前に設定することがこのタイプのネットワークでは必要となります。

## エリア

OSPFでは連続したいくつかのネットワークをまとめて、エリアを作ります。エリアを構成するのはネットワークとそれを接続するルータで、ネットワーク内のホストもこれに含まれます。

それぞれのエリアでは独自のルーティングアルゴリズムが使われ、その結果エリアを利用する場合には、同一AS内のルータが全て同じデータベースを持つとは言えなくなります。実際、エリアのトポロジはエリア外からでは見えません。同様にエリアの内部ルータはそのエリアの外のトポロジに付いての情報は持ちません。エリアを利用する利点はASを分割し、ルーティングトラフィックを大きく軽減できず。また、ルーティング障害などに対しての防護策にもなります。

エリアはバックボーンエリアという特別なエリアに接続されていなければなりません。エリア間のトラフィックはすべてバックボーンエリアを通して配信されます。ネットワークの接続携帯の問題で直接接続ができない場合には、仮想リンク (Virtual Link) という特別なパスを使用します。

### ・内部ルータ (Internal Router)

ルータが直接しているどのネットワークも同じエリアに属する時、このルータを内部ルータと言います。したがって、エリアに分割しなければどのルータもこれに該当します。

- ・エリア境界ルータ( Area Border Router )

複数のエリアに接続しているルータです。これらのルータには接続先のエリアの数だけデータベースが存在します。ABRは直接または仮想リンクを通してバックボーンエリアに接続している必要があります。

- ・バックボーンルータ( Backbone Router )

バックボーンエリアへのインタフェースを持つルータで、ABRはすべてバックボーンルータです。ただし、バックボーンエリアの内部ルータもバックボーンルータに属すると言えます。

- ・自律システム境界ルータ( Autonomous System Border Router )

ASBRが担当するのは、他のASにあるルータとの情報交換です。このルータにはABRでも内部ルータでもなることが可能です。また、バックボーンルータでも、そうでなくてもASBRになることができます。一般にこれらのルータは、接続先エリアのそれぞれに付いての情報を収めたデータベースを持ち、他のASとの間で別のルーティングプロトコルを実行します。

- ・スタブネットワーク

OSPFルータが1台だけ接続されているネットワークのことを言います。



### ・スタブエリア

ABRが1台だけの場合と、2台以上でもスタブエリア内の同じネットワークに繋がれ、バックボーン内の同じネットワークに接続されている場合のことを言います。スタブエリアの制限の一つはASBRを置けないことで、外部ルート広告のFloodingがこのエリアでは行えないからです。エリアをこのように設定する利点は、データベースを小さくでき、ルータに必要なメモリも少なくなります。

### ・バックボーンエリア(Backbone Area)

ASをエリアに分割する場合には、1つのエリアに特別な設定を行い、ルーティング情報とエリア間のトラフィックの配信を行わせなければなりません。このエリアがバックボーンと呼ばれるもので、それを構成しているのは他のどのエリアにも属さないネットワーク、それを接続するルータ、これらのネットワーク上のホスト、および複数のエリアに接続されているABRです。全てのエリア間データが通過するようになっているから、どのABRも当然バックボーンエリアに接続されています。エリアを設定していない場合は、全てのネットワーク、ルータ、ホストはこのバックボーンエリアに属します。

## ・仮想リンク (Virtual Link)

バックボーンエリアが他のエリアと異なるのは、このエリアが物理的に連続している必要がないことです。つまりバックボーンエリアを2つの物理エリア内に置き、仮想リンク (Virtual Link) と呼ばれるもので論理的にリンクさせることができます。

この機能が重要なのは、単に地理的な制約によってエリアをバックボーンに接続できないことがあるからです。

バックボーンに直接接続されたABRは仮想リンクの遠端のABRに接続性を提供でき、このとき仮想リンクは、ポイントトゥポイントリンクとして扱われます。バックボーンを通じてFloodingされたエリア間ルートは、バックボーンに直接接続されているのと同様に、遠端のABRに送られます。次にこのABRはそのエリアの内部で広告されたルート情報を要約し、それをバックボーンに送り返します。仮想リンクはすべてABR間に設定しなければならないが、通常これは手動で行われます。どのABRもインターフェースのIPアドレスではなくルータIDで識別します。ABRには制限が一つあり、バックボーンに接続されているものを除いて、どれも最低1つの非バックボーンエリアに属していなければなりません。このエリアは仮想リンク通過エリアと呼ばれます。

## 他のルーティングプロトコルとの結合

ASBRは他のASにあるルータとの結合に使用されます。したがってこれらのルータは、OSPF以外に少なくとも1つ、他のルーティングプロトコルを実行する必要があります。他のプロトコルには、EGPやBGPなどのEGPsが使用されることがあります。あるいは、OSPFの考えではASとは共通のルーティングポリシーを使うインターネットワークなので、RIPなどのIGPsも他のプロトコルになることができます。

ASBRはAS外部リンク広告をOSPF AS内に送るが、この広告は外部プロトコルから作られ、OSPF ASの外にあるネットワークへのルートを記述するものです。他のLSAと同じように、到達可能ネットワークのそれぞれに1つの広告が作成されます。ただし、他のLSAとは異なり、AS外部リンク広告は、エリアとは関係なく、スタブエリアを除くAS全体にFloodingされます。

AS外部LSAはスタブエリアにはFloodingされないため、ASBRをこの中に置くことはできません。このとき、スタブエリアを動作させるには、要約リンク広告を使い、ABRがスタブエリアにデフォルトルートを広告しなければなりません。このデフォルトルートの広告は、次にこのエリア全体にFloodingされるが、それ以上は広がりません。スタブエリアに置かれたホストとルータは、外部ネットワークにデータを送りたい場合、このデフォルトルートを使用します。

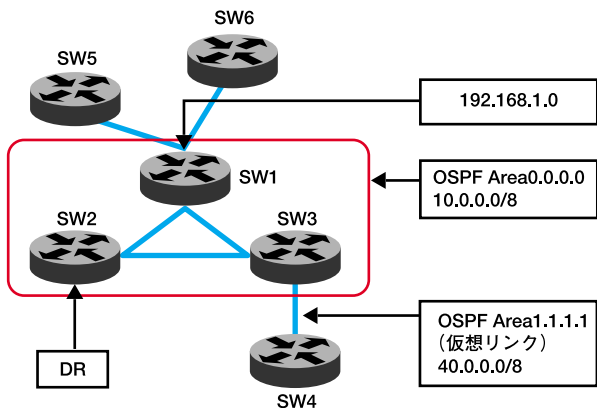


図5-1 OSPF構成図

## 10. 非IPルーティング

本製品はIPのルーティングだけ対応します。IPXやAppletalkなどの非IPはルーティングできず、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とき、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い、これらのサブネットワークとリンクできます。

このとき、ネットワークで使うことができるVLANのいずれかひとつのポートを、サブネットに接続する必要があります。

## 11. 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。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し、ネットワーク環境を整理していました。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うかわりに、本製品は簡単に設定が可能なVLANを使います。VLANは別々のブロードキャストドメインを作成し、必要に応じて回線速度ルーティングにリンクします。

IEEE 802.1Q準拠VLAN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）ごとに作成できます。

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、これを使うことで、IPアドレスやIPサブネットを更新しなくともネットワークにて変更を加えられるようになります。またVLANでは、トラフィックはあらかじめ設定されたレイヤ3リンクを通過しなければ他のVLANに到達できないようになっているため、VLANは元々高度なネットワークセキュリティ機能を備えていると言えます。本製品は以下のVLAN機能に対応します。

- IEEE 802.1Q規格に準拠したVLANを最大256グループに対応
- 直接または間接タギング、およびGVRPを使用し、複数スイッチ間の分散式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

## 12. 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に対応しているときは、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に対応しないとき、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。

## 13 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うことで、よく使わ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グループ間で共有できます。(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。

## 14 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/フラッドを決定するには、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。

## 15. 自動VLAN登録：GVRP ( GARP VLAN Registration Protocol )

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IEEE 802.1Q VLANプロトコルに対応しているとき、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できます。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グループに設定できます。



## 16. 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、この設定も変更できます。

## 17. 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間で通信する必要があり、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の場合は、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だけ使うため、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ルーティングに対応しており、VLANとレイヤ3スイッチングを両者同時に実行できます。

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はありません。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、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も設定できます。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・エントリを追加します。

## 18. マルチキャストフィルタリング

マルチキャストイングでは、単一の送信先の代わりに、一グループのノードに対してデータを送信します。最も簡単なマルチキャストイング例は、ネットワーク上の全ポートに対してデータをブロードキャストすることでしょう。しかし送信先グループがブロードキャストドメイン全体から見て小さい場合、この方法では多くの帯域幅を無駄にしまうこととなります。ビデオ会議やデータ共有が一般的になった今、効率的なマルチキャストイングは必須となっています。よく利用される方法としては、グループ登録プロトコル( Group Registration Protocol )の使用が挙げられます。グループ登録プロトコルは、ノードのマルチキャストグループへの参加およびそこから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の最適化にあります。このためマルチキャストパケットは、サブネット(VLAN)上の全ポートにすべて送信する代わりに、マルチキャストホスト/マルチキャストルータ/スイッチを含むポートにのみ転送されます。

本製品が対応している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に対応します。

## 19. IGMPスヌーピング ( IGMP Snooping )

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

## 20. IGMP ( Internet Group Management Protocol )

IGMP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を使うことで、ホストが指定マルチキャストグループ宛の送信内容の受信を希望している旨、どのホストからもそのローカルルータに対し通知できるようになります。

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

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

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

## 21. GMRP ( GARP Multicast Registration Protocol )

GMRPを使うことで、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IEEE 802.1p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。

## 22. DVMRP ( Distance-Vector Multicast Routing Protocol )

DVMRPの動作はRIPと似ています。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と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一ポートを通過する場合、このスイッチは該当マルチキャストグループまでの経路情報をそのルーティングテーブルに記録し、マルチキャストメッセージを隣接するルータに転送します(ただしメッセージ受信に使用したポートは除きます)。この処理は、ツリー上で発生し得るループをすべて除去するほか、いつも最短経路(ホップカウント単位)が使用されることを保証します。

## 23. CoS ( Class-of-Service )

本製品は各ポートで、Weighted Fair Queuing方式に対応した二つの送信キューを提供します。この機能を使うことで、リアルタイムの動画/音声送信、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)を設定できます。本製品内のポケットには、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IEEE 802.1p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。



## 24. 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に対応します。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。

## 25. 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またはウェブ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。

## 26. 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)するよう設定できます。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。

## 27. IPアドレスフィルタ

IPアドレスをフィルタできます。送信先または送信元アドレスがIPアドレスフィルタに登録されているIPパケットは、本製品で破棄されます。

## 28. SNMP管理ソフトウェア ( Simple Network Management Protocol )

SNMP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が通常管理する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するほか、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。

## 29. リモート監視：RMON ( Remote Network Monitoring )

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うことで、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できます。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のほか、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と、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できる唯一の方法です。またRMONはリアルタイムで重要な統計情報にアクセスし、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」に対応します。ミニRMONは、基本的なリモート監視するのに必要な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できます。

## 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を監視するように設定できます(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 . 管理ユーティリティで設定できる項目

各管理ユーティリティで設定できる項目の一覧です。

表A-1 設定項目

	CLI	Web	SNMP	HP OpenView
Ping	Yes	No	No	No
Reload	Yes	Yes	Yes	No
test SNMP trap	No	No	No	No
Copy	Yes	Yes	Yes	Yes
( upload/download )				
copy, delete, dir	Yes	No	No	No
( local files )				
copy to running,	Yes	No	No	No
save running-config				
select boot file	Yes	Yes	Yes	No
enable password,	Yes	No	No	No
add username				
Logging	Yes	No	No	No
MIB-2 system group	Yes	Yes	Yes	Yes
MIB-2 protocol groups	No	No	Yes	No
HTTP enable/port	Yes	No	Yes	No
Radius config	Yes	Yes	Yes	No

	CLI	Web	SNMP	HP OpenView
GVRP, GARP	Yes	Yes	Yes	No
LACP ( 802.3ad )	Yes	Yes	Yes	No
SNMP config	Yes	Yes	No	No
max-telnet-sessions	No	No	No	No
Console config	Yes	No	No	No
Interface config	Yes	Yes	Yes	Yes
clear counters ( in CLI )	Yes	No	No	No
Etherlike statistics	Yes	Yes	Yes	No
RMON-like statistics ( power up = 0 )	Yes	Yes	No	No
RMON functions	No	No	Yes	No
trunk config	Yes	Yes	Yes	Yes
MAC address table display	Yes	Yes	Yes	Yes
MAC static addresses add	Yes	Yes	Yes	No
clear bridge address	Yes	No	No	No
IP address, subnet mask, default gateway	Yes	Yes	Yes	No
DHCP client enable	Yes	Yes	Yes	No

	CLI	Web	SNMP	HP OpenView
port monitor	Yes	Yes	Yes	Yes
spanning tree	Yes	Yes	Yes	Yes
bridge extension basic	Yes	No	Yes	No
priority ( 802.1P )	Default priority	Default priority	Default priority	No
priority ( IP prec )	Yes CLI	Yes Web	Yes SNMP	Yes HP OpenView
priority ( IP DSCP, IP port )	Yes	Yes	Yes	Yes
VLAN	Yes	Yes	Yes	Yes
management VLAN	Yes	Yes	Yes	No
IGMP snooping	Yes	Yes	Yes	No
port security	No	No	No	No
broadcast control	Yes	Yes	Yes	Yes

## 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、または紛失してしまった

### 対処

- ・弊社テクニカルサポートまで連絡してください。

### 症状

シリアルポートを使いコンソールにアクセスしているがログイン画面が表示されない、またはキー入力できない

### 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設定を確かめてください。

### 症状

シリアルポートを使い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うことはできません。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ってください。



### 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、変更、または削除したときは、必ず各設定画面の【Apply Chenges】を実行し、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とき、本製品はデフォルトルートのIPアドレスは表示されません。

### 症状

VLAN間の通信が行えない

### 対処

- ・ 本製品はレイヤー2スイッチングハブのため、VLAN間の通信は行えません。VLAN間でVLAN IDの情報を受け渡しするためにはGVRPを使用してください。

## 付録C.用語集

本製品に接続した機器間の通信ができない場合は以下の点を確認してください。それでも解決しない場合は、弊社テクニカルサポートまでご連絡ください。

### A

ABR( Area Border Router )

エリア境界ルータ。OSPFの境界に設置されるルータ。

ARP( Address Resolution Protocol )

IPアドレスからMACアドレスを調べるプロトコル。

AS( Autonomous System )

OSPF自律システム。

ASBR( Autonomous System Bounday Router )

自律システム境界ルータ。OSPF自律システム( AS )と非OSPFネットワーク間をつなぐエリア境界ルータ。

ASIC( Application Specific Integrated Circuit )

特定の用途のために作られるICの名称。

## B

BGP( Border Gateway Protocol )  
経路制御に使われるプロトコル。

BPDU( Bridge Protocol Data Unit )  
スパンニングツリーの情報交換するHelloパケット。

## D

DVMRP( Distance Vector Multicast Routing Protocol )  
マルチキャストをルーティングさせるプロトコル。

## G

GARP( Group Address Registration Protocol )  
ネットワーク機器間で、優先度などの情報をやり取りするプロトコル。IEEE 802.1pで制定。

GMRP( GARP Multicast Registration Protocol )  
ネットワーク危機感で、マルチキャストの情報をやり取りするプロトコル。

GVRP( GARP VLAN Registration Protocol )  
ネットワーク機器間で、VLANタグなどの情報をやり取りするプロトコル。IEEE 802.1Qで制定。

## I

IEEE( Institute Electrical and Electronic Engineers )

米国電気電子学会。コンピュータのインターフェースやLANの規格を制定している。

IETF( Internet Engineering Task Force )

Internetで開発される技術の標準化を促進するために設立されたコンソシアム。

IGMP( Internet Group Management Protocol )

単一のIPマルチキャストアドレスで識別されるグループにマルチキャストするプロトコル。

## L

LANアダプタ

コンピュータとネットワークをつなぐための基板。ネットワークインターフェースカードやLANボードなどとも呼ばれる。LANアダプタは使用するコンピュータによって、さまざまな種類が存在する。

## M

MACアドレス( Media Access Control Address )

LANアダプタ固有の6バイトからなる物理アドレス。先頭の3バイトはベンダーコードとしてIEEEが管理している。後ろ3バイトはベンダ独自に重複しないように管理している。

MD5( Message Digit 5 )

暗号化のアルゴリズムのひとつ。暗号化されたものから原文を得ることができない手法。認証や改ざんされていないことの確認に使われる。

MIB( Management Information Base )

SNMPによって管理される項目を定義したもの。ネットワーク機器が自製品の状態を保持する変数で、基本的なMIBはRFCで定められている。

## N

NMS( Network Management System )

ネットワーク管理システム。ネットワークに接続される機器の監視や制御をする。

## O

OSPF( Open Shortest Path First )

RIPの制約を解消するため、IETFによって定義された大規模ネットワークに対応するルーティングプロトコル。帯域や混雑度を元に経路を決定する。

## P

Proxy ARP

ルータがホストの代わりにARP要求に対し、返答すること。

## Q

QoS( Quality of Service )

サービスの品質。通信の目的に応じて、優先度の高い通信に最適な帯域を割り当て、レスポンスやスループットを確保する技術。

## R

RFC( Request For Comments )

IETFが公式に発行するドキュメント。

RIP( Routing Information Protocol )

UDP/IPで動作するルーティングプロトコル。内部ゲートウェイプロトコル( Interior Gateway Protocol : IGP )とも呼ばれる。ルータを経由するホップ( Metric )数をもとに最小で到達できる経路を決定する。

RMON( Remote Network Monitoring )

ネットワークのトラフィックや障害などの情報を監視する機能。

## S

SNMP( Simple Network Management Protocol )

IETFで標準化されたTCP/IPネットワークで使われる管理プロトコル。管理する側を「SNMPマネージャ」といい、管理される側を「SNMPエージェント」という。ふたつの間は、MIBを交換することで、機器の管理をする。

SNMPエージェント( SNMP Agent )

SNMPに対応したスイッチングハブなどのネットワーク機器が備えているプログラム。自製品のMIBを管理する。

## T

Telnet

遠隔地のネットワーク接続されたコンピュータやネットワーク機器に接続する仕組み。

## V

VLAN( Virtual LAN )

物理的なケーブルやコンピュータの接続に依存せず、特定のノードだけで仮想的なグループを作る技術。VLANはブロードキャストの制限ができ、ダイナミックにネットワーク構築できる。

## W

WFQ( Weighted Fair Queuing )

データの優先順位を変える技術。

## あ行

### イングレスフィルタリング( Ingress Filtering )

レイヤ3スイッチなどのネットワーク機器で、不要だとわかっているパケットを事前に破棄する機能です。外部へ送信するパケットは、LAN内部に接続されたIPアドレスだけと判断し、内部ネットワークではないIPアドレスをフィルタします。

偽装したIPアドレスなどが外部へ送信されないようフィルタすることを推奨します。

## さ行

### サブネット( Subnet )

IPアドレスはネットワークアドレスとホストアドレスのふたつに分けられる。そのうち、ホストアドレスをさらに分割したものをサブネットという。

### スイッチングハブ( Switching Hub )

データリンク層(レイヤ2)で動作するネットワーク機器。それぞれのポートがブリッジ機能を持ち、接続されたネットワーク機器のMACアドレスを学習する。データは通信に必要なポート間だけでやり取りをする。スイッチングハブは、レイヤ3スイッチと対して、レイヤ2スイッチとも呼ばれる。

### スパニングツリー( Spanning Tree )

ループが存在しないブリッジネットワーク。スパニングツリーアルゴリズムや、スパニングツリープロトコルのことを指すこともある。



スパニングツリーアルゴリズム( Spanning Tree Algorithm : STA )  
スパニングツリーを形成するアルゴリズム。IEEE 802.1dで制定。

スパニングツリープロトコル( Spanning Tree Protocol )  
スパニングツリーアルゴリズムを使い、ネットワークループを検出・解除するプロトコル。ループが検出されたとき、対象のポートを無効にする。

静的ルーティング( Static Routing )  
あらかじめルーティング情報をネットワーク機器に設定し、パケットをルーティングする。

## た行

動的ルーティング( Dynamic Routing )  
ネットワーク機器間でネットワーク接続を監視し、通信の時点で最適な経路を選び、パケットをルーティングする。

トラフィック( Traffic )  
ネットワークで送受信されるデータや情報。ネットワーク回線を道路、情報の流れを車の交通にたとえ、トラフィックと呼ばれる。

## な行

ネットワーク管理  
ネットワークを制御し、機能を維持・管理すること。性能、構成、課金、障害、機密の5つを管理する。

ノード(Node)

ネットワークに接続されるコンピュータやハブなどの機器。

## は行

パケット(Packet)

一定の大きさに区切られたデータの集合。

ハブ(Hub)

LANのケーブルを集中して接続するネットワーク機器。ハブを中心に、スター状にネットワークを構築する。

ブリッジ(Bridge)

データリンク層(レイヤ2)で動作するネットワーク機器。LANのセグメント間を接続し、それぞれのネットワーク機器のMACアドレスを学習する。データは登録されたテーブルを参照し、やり取りをする。

フロー制御(Flow Control)

データ通信において、主に受信側のバッファがいっぱいになったとき、データ転送速度を下げたり、停止したりして、データの損失を防ぐこと。

ブロードキャスト(Broadcast)

ネットワーク内の全ノードに対し、データを送信する通信方式。

## ま行

マルチキャスト(Multicast)

パケット通信技術のひとつ。単一のパケットで複数のノードに対し、同じデータを送信する通信方式。

## や行

ユニキャスト(Unicast)

1対1で通信する方式。

## ら行

ルータ(Router)

ネットワーク層(レイヤ3)で動作するネットワーク機器。異なるネットワーク間を接続し、データをルーティングする。レイヤ3スイッチに比べ、ルーティング速度が遅い。

ルーティング(Routing)

ルータやレイヤ3スイッチで、ネットワークと別のネットワークを接続し、パケットを中継する。

レイヤ3スイッチ(Layer three Switch)

ネットワーク層(レイヤ3)でルーティング処理をするネットワーク機器。レイヤ2スイッチに専用のハードウェアASICを追加し、IPのルーティングを高速に処理する。

## わ行

ワイヤスピード (Wire speed)

スイッチングハブは、その機能のためパケット処理に遅延が出ることがある。遅延が最小で、ワイヤが直結されているときのパフォーマンスに近い状態を、ワイヤスピードと呼ぶ。

# 付録 D. 工場出荷設定

機能	初期設定値
IPアドレス	192.168.0.1/24
ポート状態	全てのポートが使用可能
Autonegotiation	有効
ユーザアカウント	admin、guest（パスワードはそれぞれ admin、guest）
コンソールポート	通信速度:9600bps
初期設定	データ長: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 フロー制御:なし
HTTPサーバ	有効
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	private security
RMON統計機能	全てのポートで可能
VLAN機能	ひとつのVLANグループ (VLAN ID1) 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	VLANグループの全てのバケットには、タグは付加されない
802.1P優先順位	優先設定されたタグが付加してあるバケットを受け取ったときは、自動認識
スパンニングツリー プロトコル機能	有効
フォワーディングデータベース エージング時間	300秒
フロー制御	全てのポートで使用しない
Telnet サーバ	有効

# 付録 E. 製品仕様

< 品名 >

ギガビットインテリジェントスイッチ

< 型番 >

FMX-0248K

< 最大ポート数 >

48( 10/100BASE RJ-45 )

2 ( 1000BASE コンポポート )

< ポート >

10/100BASE-TX×24

1000BASE-SX、LX、Tx 2( RJ-45、miniGBICコンポポート )

< Autonegotiation >

全ポート対応

< AutoMDI >

全ポート対応

< LEDインジケータ >

FDX、Link/Act、Power、Diag、RPU、Port Status

< 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 >

13.6Gbps

<フィルタ速度>

各ポート14880パケット/秒

148800パケット/秒

1488000パケット/秒

<パケットバッファ容量>

64Mバイト

<フロー制御>

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:8000個

<VLANグループ数>

最大255個のVLANグループを構築可能

<プライオリティ対応>

4 Level(IEEE 802.1p 準拠)

<MIB>

MIB-2、Interface MIB、Ether-Link MIB、Bridge MIB、Extended Bridge MIB、RMON MIB、Entity MIB、RADIUS 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、ウェブベースNMS

< ファームウェア更新 >

TFTP

< 寸法 ( W x D x H ) >

440 x 324 x 43 mm

< 重量 >

4.36kg

< 消費電力 >

48W

< 動作温度 >

0 ~ 45

< 動作湿度 >

35 ~ 80% ( 結露しないこと )

< 入力電圧 >

100 ~ 240VAC

< 入力周波数 >

50 ~ 60Hz

< EMI >

FCC Class A、CE、VCCI Class A