

USER'S MANUAL

シャーシタイプ10M/100M/1000M
レイヤ3 インテリジェントスイッチングハブ

FML-1200

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すると誤動作や火災につながるおそれがあります。



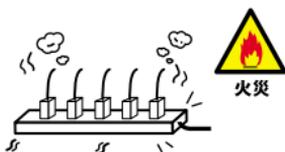
通気口をふさがないで！

内部に熱がこもり、誤動作や火災につながるおそれがあります。



タコ足配線・無理な配線はダメ！

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



電源コードをつけて移動しないで！

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



液体・異物は入れないで！

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



電源コードは傷つけないで！

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

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



設置・保管場所をもう一度確認して！

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

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



◎おねがい

本製品のお手入れ

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

目次

第1章 はじめに

- 1. 概要 7
- 2. 特長 8
- 3. 梱包内容の確認 12
- 4. 各部の名称 13

第2章 クイックインストール

- 1. インストールの手順 43
- 2. 設置場所について 44
- 3. 本製品の設置 45
- 4. マネージメントモジュールの接続 51
- 5. FML-1200専用モジュールの接続 54
- 6. 電源ユニットの接続 57
- 7. 電源ケーブルの接続 60
- 8. 本製品とネットワーク機器の接続 61

第3章 スイッチの管理

- 1. 設定オプション 67
- 2. シリアルポートの接続 68
- 3. Telnet・ウェブブラウザの接続 70

第4章 ウェブインターフェイス

- 1. ウェブインターフェイスについて 71
- 2. ウェブインターフェイスの操作 72
- 3. ウェブインターフェイスのログイン 73
- 4. メニュー階層 74
- 5. Summary Menu 78
- 6. Device View Menu 79
- 7. ポート画面 80
- 8. Setup(Console) 90
- 9. Initialize(Control) 91
- 10. Reboot(Control) 92
- 11. Software Upgrade(Control) 93

12. Setup(Management)	95
13. Connect(Telnet)	96
14. Getting Started	97
15. Add(Address Database)	104
16. Aging Time(Address Database)	106
17. Find(Address Database)	107
18. Remove(Address Database)	108
19. Summary(Address Database)	109
20. Setup(Broadcast Storm Control)	112
21. AddPort(Link Aggregation)	113
22. Admin State(Link Aggregation)	114
23. Remove Port(Link Aggregation)	115
24. Summary(Link Aggregation)	116
25. IGMP Mode(Multicast Filter)	117
26. SnoopMode(Multicast Filter)	118
27. Setup(Spanning Tree)	119
28. Create(VLAN)	121
29. Delete(VLAN)	122
30. Modify(VLAN)	123
31. Setup(Ethernet)	128
32. Statistics(Ethernet)	131
33. Summary(Ethernet)	139
34. Aging(ARP)	142
35. Display/Edit(ARP)	143
36. Flush(ARP)	146
37. Display/Edit(INTERFACE)	147
38. ASBR Summary(OSPF)	153
39. Display areas(OSPF)	160
40. Interface(OSPF)	170
41. LSAs Database Summary(OSPF)	177
42. LSAs Summary(OSPF)	179
43. LSAs AsSummary(OSPF)	181
44. LSAs router(OSPF)	183
45. LSAs network(OSPF)	185
46. LSAs external(OSPF)	187

47. LSAs NssaExternal(OSPF)	189
48. Display Neighbors(OSPF)	191
49. Modify Router ID(OSPF)	193
50. Virtual links modify(OSPF)	196
51. Display/Edit(RIP)	204
52. Mode(RIP)	207
53. Neighbors(RIP)	208
54. Statistics(RIP)	209
55. Default Gateway(ROUTE)	210
56. Display(ROUTE)	211
57. Flush(ROUTE)	216
58. Display/Edit(UDP Helper)	217
59. Setup(IP)	222
60. Modify(User)	227
61. Port Security(Access)	228

第5章 技術解説

1. レイヤ2スイッチ	233
2. マルチキャストスイッチング	236
3. STA(Spanning Tree Algorithm)	238
4. レイヤ3スイッチ	240
5. IPスイッチング	241
6. ICMP Router Discovery	244
7. ルーティングプロトコル	246
8. RIP(Routing Information Protocol)/RIP-2動的ルーティングプロトコル	247
9. OSPF v2動的ルーティングプロトコル(Open Shortest Path First)	249
10. 非IPルーティング	259
11. VLANの初期設定	260
12. VLAN	261
13. VLANへのポート割り当て	263
14. ポートオーバーラッピング	264
15. ポートベースVLAN	265
16. 自動VLAN登録：GVRP(GARP VLAN Registration Protocol)	266
17. タグ付/タグ無しフレームの転送	267
18. VLANグループの接続	268
19. マルチキャストフィルタリング	269

20. IGMPスヌーピング(IGMP Snooping)	271
21. IGMP(Internet Group Management Protocol)	272
22. GMRP(GARP Multicast Registration Protocol)	274
23. DVMRP(Distance-Vector Multicast rRouting Protocol)	275
24. CoS(Class-of-Service)	276
25. SNMPコミュニティストリング	277
26. ユーザー名およびパスワード	278
27. MACアドレスフィルタ	279
28. IPアドレスフィルタ	280
29. SNMP管理ソフトウェア(Simple Network Management Protocol)	281
30. リモート監視 : RMON(Remote Network Monitoring)	282
付録A 本体構成	284
付録B IPルーティングネットワーク構成例	288
付録C トラブルシューティング	291
付録D ファームウェアのアップデートと設定ファイルのアップデート/ダウンロード	295
付録E 用語集	297
付録F 工場出荷時設定	305
付録G 仕様	307

《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.1.1

No.PCM-02-10-SK-FML-1200

1.はじめに

1 概要

FML-1200は、さまざまなネットワークの規格に準拠したシャーシタイプのレイヤ3 インテリジェントスイッチングハブです。シャーシ本体に12個のスロットを持ち、専用モジュールを取り付けることで多種多様なネットワークに柔軟に対応します。本製品と専用のモジュールを使うことで、8ポートのスイッチングハブから、ギガビット24ポートのレイヤ3スイッチまで、お客様の利用環境にあわせ、組替えることができます。

ASICによるワイヤスピード、IPルーティング、VLAN、プライオリティ制御、スパニングツリーなどの機能を持ち、RIP、RIP2、およびOSPFに対応しています。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

本体(FML-1200)の特徴

IEEE 802.3i 10BASE-T、IEEE 802.3u 100BASE-TX/FX、
IEEE 802.3ab 1000BASE-T、IEEE 802.3z 1000BASE-SX/LX
規格準拠

冗長化可能なマネージメントモジュール用スロットを2個装備

FML-1200専用モジュール用スロットを12個装備

冗長化可能な電源ユニット用スロットを2個装備

排気用大型ファンを4機搭載

軽量なアルミボディーを採用

標準19インチラックにマウント可能

全高で7U(309mm)分使用します。

冗長化電源ユニット

300W ACの大電流

冗長化電源ユニットを2台使用することにより負荷分散が可能

非常時の冗長電源として2台目をインストールすることも可能

マネージメントモジュール(F120-MGT)の特徴

MACアドレステーブルを装備し、最大32768個のMACアドレスを自動学習可能

IPアドレステーブルを装備し、最大65536個のIPアドレスを自動学習可能

最大64個のIPサブネットを作成可能

8Mバイトのパケットバッファ装備

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)

IEEE 802.1Q VLANに準拠。最大2046グループ作成可能

IEEE 802.1Q/p準拠により2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。最大12グループ作成可能。2/3/4ポートTrunk対応

IGMP、DVMRPマルチキャストプロトコル(対応予定)に対応

RIP-v1、RIP-v2、OSPF-V2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

MIB2、EthernetMAU MIB、Bridge MIB、Private MIB、RIP2 MIB、IP Forwarding MIB、OSPF MIB、IGMP MIB、DVMRP MIB、IP Multicast Router MIB対応

RMONのStatistics、History、Alarmの3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)
バックアップ用としてもう1枚インストールされている場合は、1枚目が故障したりこれを取り外した場合でも2枚目のマネージメントモジュールが動作を引き継ぐかたちとなります。

F120-8TXの特徴

IEEE 802.3i 10BASE-T、IEEE 802.3u 100BASE-TX規格準拠
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
100BASE-TX、10BASE-T接続用のRJ-45 STPポートを8ポート装備

F120-1TE/F120-2TEの特徴

IEEE 802.3i 10BASE-T、IEEE 802.3u 100BASE-TX規格準拠、IEEE 802.3ab 1000BASE-T規格準拠
Autonegotiation機能によって、転送速度(1000/100/10Mbps)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
1000BASE-T、100BASE-TX、10BASE-T接続用のRJ-45 STPポートを1ポートまたは2ポート装備

F120-1SXの特徴

IEEE 802.3z 1000BASE-SX規格準拠
Autonegotiation機能によって、転送速度および転送モードを自動認識可能
1000BASE-SX接続用のSCファイバーポートを1ポート装備

F120-1GBIC/F120-2GBICの特徴

IEEE 802.3z 1000BASE-SX1LX規格準拠

Autonegotiation機能によって、転送速度および転送モードを自動認識可能

1000BASE-SX/LX用GBIC対応スロットを1スロットまたは2スロット装備

F120-8MT

IEEE 802.3u 100BASE-FX規格準拠

Autonegotiation機能によって、転送速度および転送モードを自動認識可能

100BASE-FXマルチモード用のMT-RJポートを8ポート装備

F120-8MT-S

IEEE 802.3u 100BASE-FX規格準拠

Autonegotiation機能によって、転送速度および転送モードを自動認識可能

100BASE-FXシングルモード用のMT-RJポートを8ポート装備

F120-2GMT

IEEE 802.3z 1000BASE-SX規格準拠

Autonegotiation機能によって、転送速度および転送モードを自動認識可能

1000BASE-SX用のMT-RJポートを2ポート装備

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。

FML-1200本体

F120-MGT(マネージメントモジュール) × 1

設定用RS-232Cストレートケーブル(D-SUB9ピンオス/メス・
ストレートタイプ)

冗長化電源ユニット × 1

ファンユニット × 1

電源ケーブル

ラックマウント用金具 × 2

ケーブル収束用金具 × 1

ネジ × 8

ゴム足 × 4

ユーザーズマニュアル(CD-ROM)

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

本体(FML-1200)

前面パネル

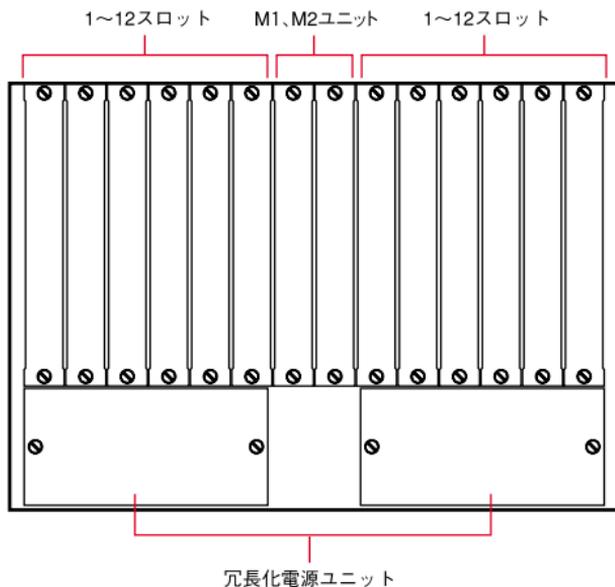


図1-1 前面パネル

【M1、M2スロット】

マネージメントモジュール(F120-MGT)の接続用スロットです。

【1~12スロット】

FML-1200専用モジュールの接続用スロットです。

【冗長化電源スロット】

冗長化電源ユニットの接続用スロットです。

背面パネル

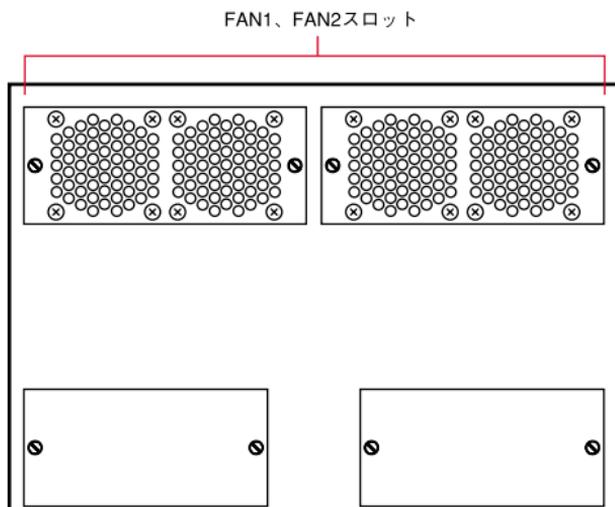


図1-2 背面パネル

【FAN 1、FAN 2スロット】

ファンユニットの接続用スロットです。

側面パネル

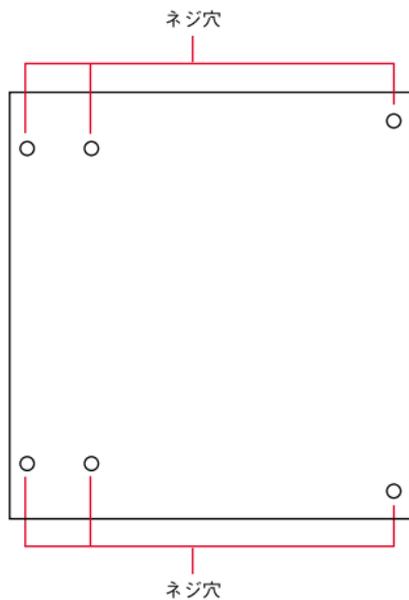


図1-3 側面パネル

【ネジ穴】

ラックマウント用金具を取り付けるネジ穴です。

裏面ステッカー

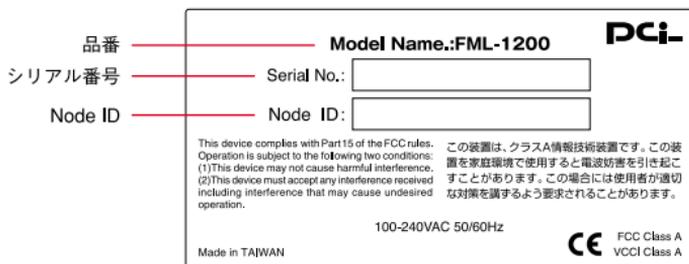


図1-6 裏面ステッカー

【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 ID】

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 前面パネル

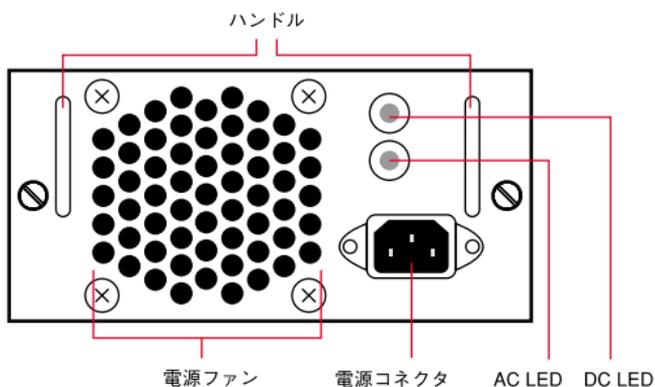


図1-4 前面パネル

【電源コネクタ】

電源ケーブルを接続します。

【ハンドル】

電源ユニットを取り外す際にはハンドルを持ち作業を行いません。

【AC LED】

AC電源から供給している時に点灯します。

【DC LED】

DC電源を供給している時に点灯します。

【電源ファン】

本体内部の熱および電源ユニット内部の熱を放出します。

背面パネル

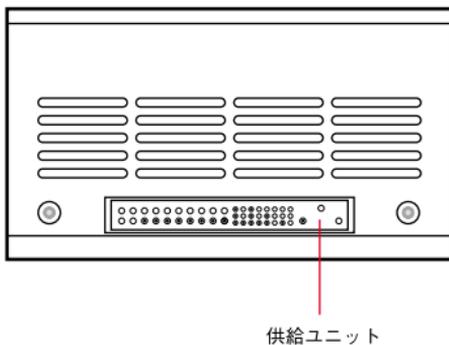


図1-5 前面パネル

【供給コネクタ】

シャーシ本体に接続します。

ファンユニット

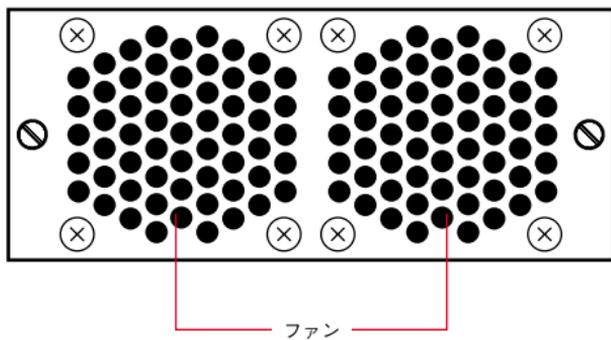


図1-7 ファンユニット

【ファン】

本体内部の熱を放出します。

マネージメントモジュール(F120-MGT)

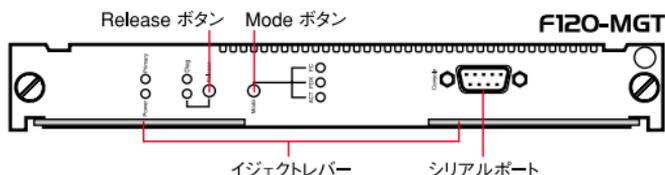


図1-8 マネージメントモジュール

LED	状態	記述
Power	消灯	電源がOFFの状態の時は消灯します。
	点灯(緑)	電源がONの状態の時に点灯します。
Primary	消灯	* 1電源がOFFまたはスタンバイ状態の時は消灯します。
	点灯(青)	本製品の管理を行なっている状態の時に点灯します。
Diag	点滅(緑)	自己診断モード及びFirmWare等を読み込んでいる時に点滅します。
	点灯(緑)	自己診断モード及びFirmWare等の読み込みが正常終了し正常に稼動している時に点灯します。
Release	点滅(橙)	マネージメントモジュールの取り外しの準備をしています。
	点灯(橙)	マネージメントモジュールの取り外し可能な状態です。

表1-1 マネージメントステータスLED

*1 マネージメントモジュールを二枚使い、冗長化を行なった場合 Primaryとして使用されていない時はスタンバイ状態となります。

【Release ボタン】

マネージメントモジュールを取り外す時に押します。

【Mode ボタン】

Mode LEDに表示させる項目を選択します。ACT、FDX、FCから選びます。

LED	状態	記述
ACT (Activity)	点灯(緑)	すべてのモジュール上のMode LEDがデータの送受信中に点滅します。
	消灯	FDX、FCが選択されている時の状態または電源がOFFの状態です。
FDX (Full Duplex)	点灯(緑)	すべてのモジュール上のMode LEDが全二重で通信中に点灯します。
	消灯	すべてのモジュール上のMode LEDがフローコントロール有効時に点灯します。
FC (Flow Control)	点灯(緑)	すべてのモジュール上のMode LEDがフローコントロール有効時に点灯します。
	消灯	ACT、FDXが選択されている時の状態または電源がOFFの状態です。

表1-2 Mode LED

【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。

【イジェクトレバー】

本体に接続したモジュールを外す時に、レバーを起します。

F120-8TX

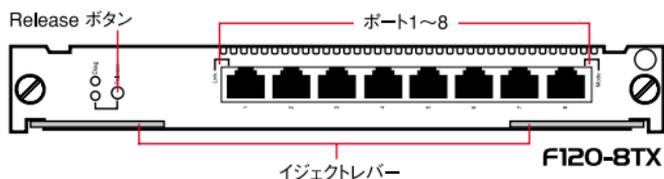


図1-9 F120-8TX

【ポート1~8】

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。

LED	状態	記述
Diag	点滅(緑)	自己診断モード及びFirmWare等を読み込んでいる時に点滅します。
	点灯(緑)	自己診断モード及びFirmWare等の読み込みが正常終了し正常に稼動している時に点灯します。
	消灯	モジュールを挿入するかモジュール・リセット後に、LEDが、およそ3秒間消灯します。その他の時は、自己診断の失敗を示します。
Release	点滅(橙)	マネージメントモジュールの取り外しの準備をしています。
	点灯(橙)	マネージメントモジュールの取り外し可能な状態です。
	消灯	正常作動中
Link	点灯(橙)	10BASE-Tでポートのリンクが確立されると点灯(橙)します。
	点灯(緑)	100BASE-TXでポートのリンクが確立されると点灯(緑)します。
	点滅(橙)	ポートを無効にすると点滅します。
	消灯	ポートが有効時にケーブルを接続していないと消灯します。
Mode	点滅(橙) [F120-MGT上でFC LEDが点灯している時]	フローコントロールが有効になっている時に点滅します。

Mode	消灯 [F120-MGT上で FC LEDが点灯 している時]	フローコントロールが無効になっている、もしくはLinkしていない時に消灯します。
	点灯(橙) [F120-MGT上で FDX LEDが点灯 している時]	ポートが全二重で通信中に点灯します。
	消灯 [F120-MGT上で FDX LEDが点灯 している時]	ポートが半二重で通信中に消灯します。
	点滅(橙) [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信中に点滅します
	消灯 [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信を行っていない時に消灯します。

表1-3 マネージメントLED

【Release ボタン】

マネージメントモジュールを取り外す時に押します。

【イジェクトレバー】

本体に接続したモジュールを外す時に、レバーを起します。

F120-1TE/F120-2TE

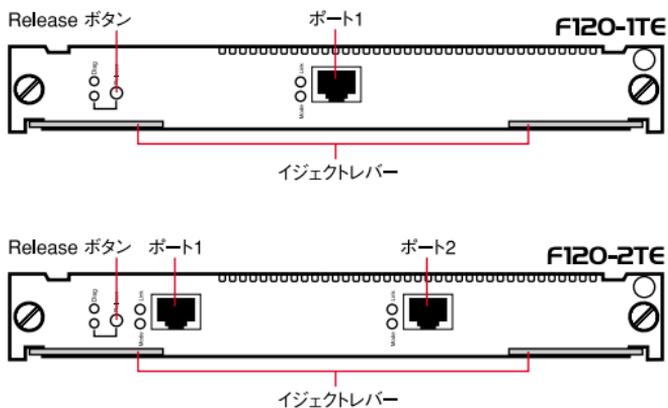


図1-10 F120-1TE/F120-2TE

【ポート1/1～2】

1000BASE-T/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。

LED	状態	記述
Diag	点滅(緑)	自己診断モード及びFirmWare等を読み込んでいる時に点滅します。
	点灯(緑)	自己診断モード及びFirmWare等の読み込みが正常終了し正常に稼働している時に点灯します。
	消灯	モジュールを挿入するかモジュール・リセット後に、LEDが、およそ3秒間消灯します。その他の時は、自己診断の失敗を示します。
Release	点滅(橙)	マネージメントモジュールの取り外しの準備をしています。
	点灯(橙)	マネージメントモジュールの取り外し可能な状態です。
	消灯	正常作動中
Link	点灯(橙)	10BASE-Tでポートのリンクが確立されると点灯(橙)します。
	点灯(緑)	100BASE-TXでポートのリンクが確立されると点灯(緑)します。
	点滅(緑)	1000BASE-Tでポートのリンクが確立されると点滅(緑)します。
	点滅(橙)	ポートを無効にすると点滅します。
	消灯	ポートが有効時にケーブルを接続していないと消灯します。
Mode	点滅(橙) [F120-MGT上でFC LEDが点灯している時	フローコントロールが有効になっている時に点滅します。

Mode	消灯 [F120-MGT上で FC LEDが点灯 している時]	フローコントロールが無効になっている、もしくはLinkしていない時に消灯します。
	点灯(橙) [F120-MGT上で FDX LEDが点灯 している時]	ポートが全二重で通信中に点灯します。
	消灯 [F120-MGT上で FDX LEDが点灯 している時]	ポートが半二重で通信中に消灯します。
	点滅(橙) [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信中に点滅します
	消灯 [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信を行っていない時に消灯します。

表1-4 マネージメントLED

【Release ボタン】

マネージメントモジュールを取り外す時に押します。

【イジェクトレバー】

本体に接続したモジュールを外す時に、レバーを起します。

F120-1SX

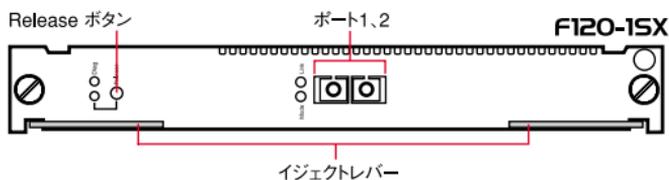


図1-11 F120-1SX

【ポート1】

1000BASE-SXファイバーケーブル接続用のSCポートです。

LED	状態	記述
Diag	点滅(緑)	自己診断モード及びFirmWare等を読み込んでいる時に点滅します。
	点灯(緑)	自己診断モード及びFirmWare等の読み込みが正常終了し正常に稼動している時に点灯します。
	消灯	モジュールを挿入するかモジュール・リセット後に、LEDが、およそ3秒間消灯します。その他の時は、自己診断の失敗を示します。
Release	点滅(橙)	マネージメントモジュールの取り外しの準備をしています。
	点灯(橙)	マネージメントモジュールの取り外し可能な状態です。
	消灯	正常作動中
Link	点滅(緑)	1000BASE-SXでポートのリンクが確立されると点滅(緑)します。
	点滅(橙)	ポートを無効にすると点滅します。
	消灯	ポートが有効時にケーブルを接続していないと消灯します。
Mode	点滅(橙) [F120-MGT上でFC LEDが点灯している時]	フローコントロールが有効になっている時に点滅します。

Mode	消灯 [F120-MGT上で FC LEDが点灯 している時]	フローコントロールが無効になっている、もしくはLinkしていない時に消灯します。
	点灯(橙) [F120-MGT上で FDX LEDが点灯 している時]	ポートが全二重で通信中に点灯します。
	消灯 [F120-MGT上で FDX LEDが点灯 している時]	ポートが半二重で通信中に消灯します。
	点滅(橙) [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信中に点滅します
	消灯 [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信を行っていない時に消灯します。

表1-5 マネージメントLED

【Release ボタン】

マネージメントモジュールを取り外す時に押します。

【イジェクトレバー】

本体に接続したモジュールを外す時に、レバーを起します。

F120-1GBIC/F120-2GBIC

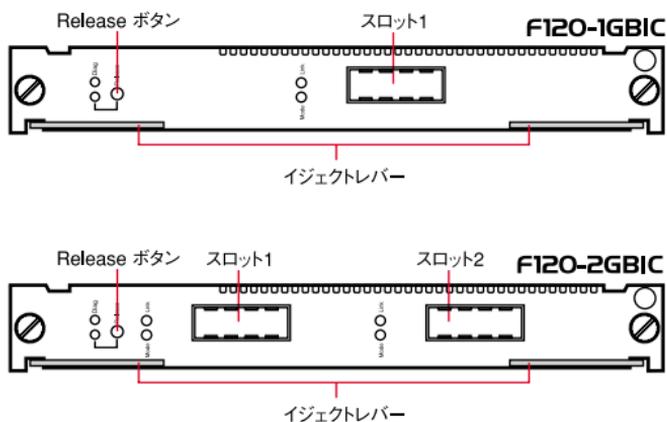


図1-12 F120-1GBIC/F120-2GBIC

【スロット1/1～2】

1000BASE-SX/LX用GBIC対応スロットです。

LED	状態	記述
Diag	点滅(緑)	自己診断モード及びFirmWare等を読み込んでいる時に点滅します。
	点灯(緑)	自己診断モード及びFirmWare等の読み込みが正常終了し正常に稼動している時に点灯します。
	消灯	モジュールを挿入するかモジュール・リセット後に、LEDが、およそ3秒間消灯します。その他の時は、自己診断の失敗を示します。
Release	点滅(橙)	マネージメントモジュールの取り外しの準備をしています。
	点灯(橙)	マネージメントモジュールの取り外し可能な状態です。
	消灯	正常作動中
Link	点滅(緑)	1000BASE-SX/LXでポートのリンクが確立されると点滅(緑)します。
	点滅(橙)	ポートを無効にすると点滅します。
	消灯	ポートが有効時にケーブルを接続していないと消灯します。
Mode	点滅(橙) [F120-MGT上でFC LEDが点灯している時]	フローコントロールが有効になっている時に点滅します。

Mode	消灯 [F120-MGT上で FC LEDが点灯 している時]	フローコントロールが無効になっている、もしくはLinkしていない時に消灯します。
	点灯(橙) [F120-MGT上で FDX LEDが点灯 している時]	ポートが全二重で通信中に点灯します。
	消灯 [F120-MGT上で FDX LEDが点灯 している時]	ポートが半二重で通信中に消灯します。
	点滅(橙) [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信中に点滅します
	消灯 [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信を行っていない時に消灯します。

表1-6 マネージメントLED

【Release ボタン】

マネージメントモジュールを取り外す時に押します。

【イジェクトレバー】

本体に接続したモジュールを外す時に、レバーを起します。

F120-8MT

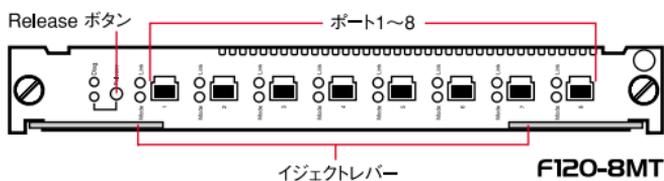


図1-13 F120-8MT

【ポート1~8】

100BASE-FXマルチモード用のMT-RJポートです。

LED	状態	記述
Diag	点滅(緑)	自己診断モード及びFirmWare等を読み込んでいる時に点滅します。
	点灯(緑)	自己診断モード及びFirmWare等の読み込みが正常終了し正常に稼動している時に点灯します。
	消灯	モジュールを挿入するかモジュール・リセット後に、LEDが、およそ3秒間消灯します。その他の時は、自己診断の失敗を示します。
Release	点滅(橙)	マネージメントモジュールの取り外しの準備をしています。
	点灯(橙)	マネージメントモジュールの取り外し可能な状態です。
	消灯	正常作動中
Link	点灯(緑)	100BASE-FXでポートのリンクが確立されると点灯(緑)します。
	点滅(橙)	ポートを無効にすると点滅します。
	消灯	ポートが有効時にケーブルを接続していないと消灯します。
Mode	点滅(橙) [F120-MGT上でFC LEDが点灯している時]	フローコントロールが有効になっている時に点滅します。

Mode	消灯 [F120-MGT上で FC LEDが点灯 している時]	フローコントロールが無効になっている、もしくはLinkしていない時に消灯します。
	点灯(橙) [F120-MGT上で FDX LEDが点灯 している時]	ポートが全二重で通信中に点灯します。
	消灯 [F120-MGT上で FDX LEDが点灯 している時]	ポートが半二重で通信中に消灯します。
	点滅(橙) [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信中に点滅します
	消灯 [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信を行っていない時に消灯します。

表1-7 マネージメントLED

【Release ボタン】

マネージメントモジュールを取り外す時に押します。

【イジェクトレバー】

本体に接続したモジュールを外す時に、レバーを起します。

F120-8MT-S

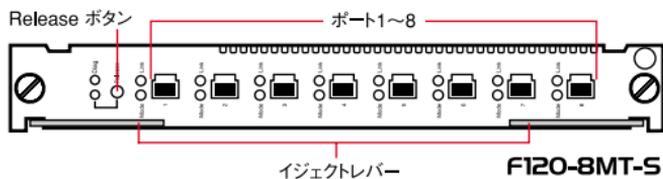


図1-14 F120-8MT-S

【ポート1～8】

100BASE-FXシングルモード用のMT-RJポートです。

LED	状態	記述
Diag	点滅(緑)	自己診断モード及びFirmWare等を読み込んでいる時に点滅します。
	点灯(緑)	自己診断モード及びFirmWare等の読み込みが正常終了し正常に稼働している時に点灯します。
	消灯	モジュールを挿入するかモジュール・リセット後に、LEDが、およそ3秒間消灯します。その他の時は、自己診断の失敗を示します。
Release	点滅(橙)	マネージメントモジュールの取り外しの準備をしています。
	点灯(橙)	マネージメントモジュールの取り外し可能な状態です。
	消灯	正常作動中
Link	点灯(緑)	100BASE-FXでポートのリンクが確立されると点灯(緑)します。
	点滅(橙)	ポートを無効にすると点滅します。
	消灯	ポートが有効時にケーブルを接続していないと消灯します。
Mode	点滅(橙) [F120-MGT上でFC LEDが点灯している時]	フローコントロールが有効になっている時に点滅します。

Mode	消灯 [F120-MGT上で FC LEDが点灯 している時]	フローコントロールが無効になっている、もしくはLinkしていない時に消灯します。
	点灯(橙) [F120-MGT上で FDX LEDが点灯 している時]	ポートが全二重で通信中に点灯します。
	消灯 [F120-MGT上で FDX LEDが点灯 している時]	ポートが半二重で通信中に消灯します。
	点滅(橙) [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信中に点滅します
	消灯 [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信を行っていない時に消灯します。

表1-8 マネージメントLED

【Release ボタン】

マネージメントモジュールを取り外す時に押します。

【イジェクトレバー】

本体に接続したモジュールを外す時に、レバーを起します。

F120-2GMT

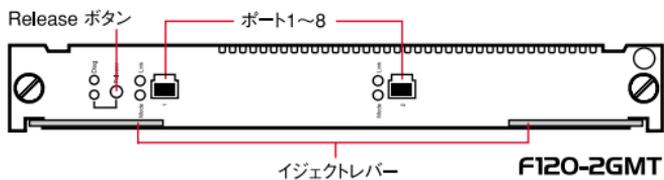


図1-15 F120-2GMT

【ポート1～2】

1000BASE-SX用のMT-RJポートです。

LED	状態	記述
Diag	点滅(緑)	自己診断モード及びFirmWare等を読み込んでいる時に点滅します。
	点灯(緑)	自己診断モード及びFirmWare等の読み込みが正常終了し正常に稼動している時に点灯します。
	消灯	モジュールを挿入するかモジュール・リセット後に、LEDが、およそ3秒間消灯します。その他の時は、自己診断の失敗を示します。
Release	点滅(橙)	マネージメントモジュールの取り外しの準備をしています。
	点灯(橙)	マネージメントモジュールの取り外し可能な状態です。
	消灯	正常作動中
Link	点滅(緑)	1000BASE-SXでポートのリンクが確立されると点滅(緑)します。
	点滅(橙)	ポートを無効にすると点滅します。
	消灯	ポートが有効時にケーブルを接続していないと消灯します。
Mode	点滅(橙) [F120-MGT上でFC LEDが点灯している時]	フローコントロールが有効になっている時に点滅します。

Mode	消灯 [F120-MGT上で FC LEDが点灯 している時]	フローコントロールが無効になっている、もしくはLink [F120-MGT上でして いない時に消灯します。
	点灯(橙) [F120-MGT上で FDX LEDが点灯 している時]	ポートが全二重で通信中に点灯します。
	消灯 [F120-MGT上で FDX LEDが点灯 している時]	ポートが半二重で通信中に消灯します。
	点滅(橙) [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信中に点滅します
	消灯 [F120-MGT上で ACT LEDが点灯 している時]	ポートがデータの送受信を行っていない時に消灯します。

表1-9 マネージメントLED

【Release ボタン】

マネージメントモジュールを取り外す時に押します。

【イジェクトレバー】

本体に接続したモジュールを外す時に、レバーを起します。

2. クイックインストール

1 インストールの手順

FML-1200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. マネージメントモジュールを接続する
4. FML-1200専用モジュールを接続する
5. 電源ユニットを接続する
6. 電源ケーブルを接続する
7. 各コンピュータ、ハブおよびスイッチと接続する

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

注意 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。

注意

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。

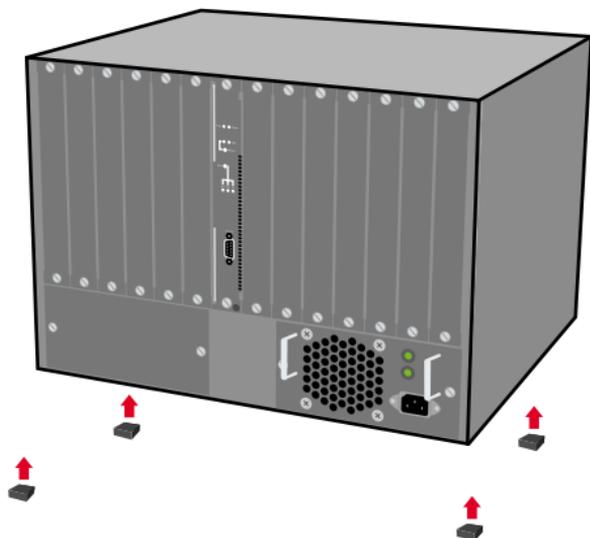


図2-1 ゴム足の取り付け図

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かめます。
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4つ使い、ラックマウント用金具に差し込んで固定します。

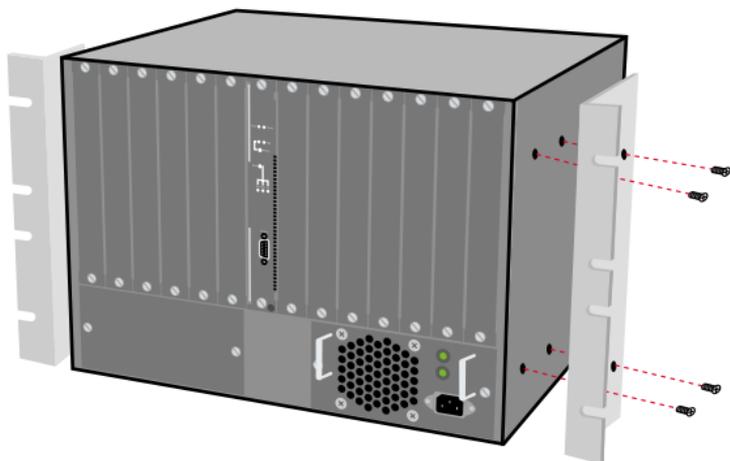


図2-2 ラックマウント用金具の取り付け

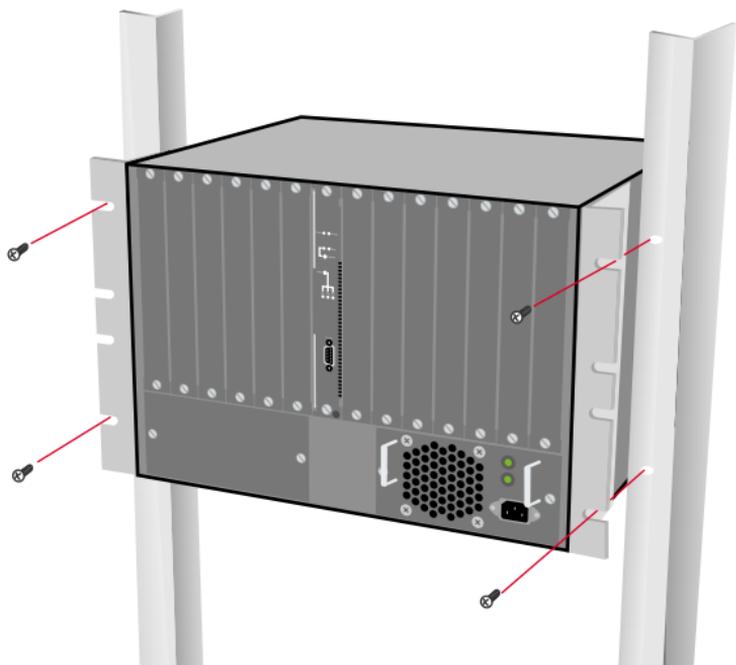


図2-3 ラックマウント用金具をラックに固定

6. 本製品の付属のケーブル収束用金具を本製品の下の側に配置してください。19インチラックのシャーシ上の穴に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、ケーブル収束用金具に差し込んで固定します。

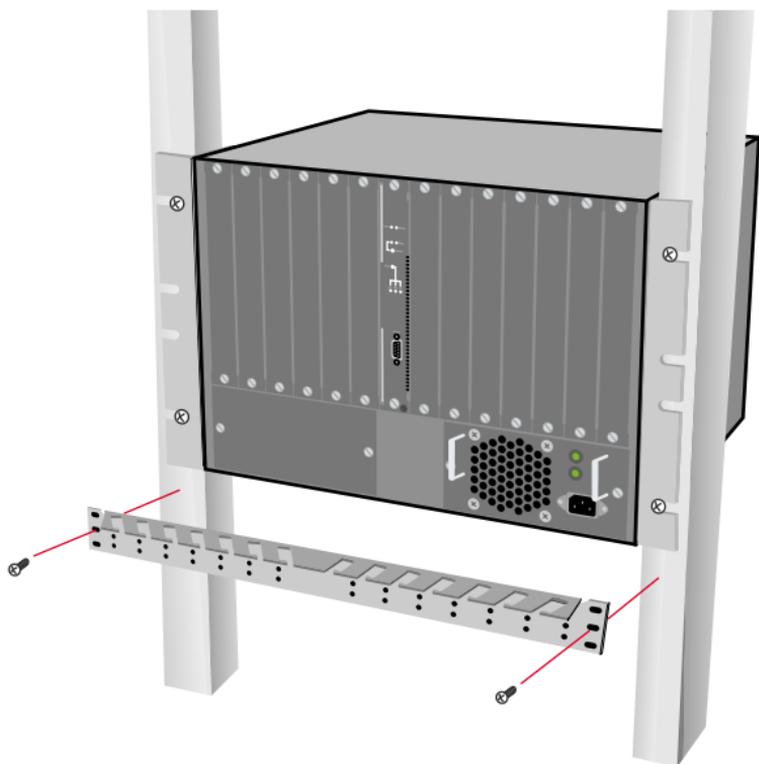


図2-4 ケーブル収束用金具をラックに固定

4 マネージメントモジュールの接続

本製品にマネージメントモジュールを接続する手順です。

重要 マネージメントモジュールを接続する時は、「M1」、「M2」と表記されているスロットを使用してください。

1. 本体の「M1」または「M2」の使用するスロットのスロットカバーを外します。

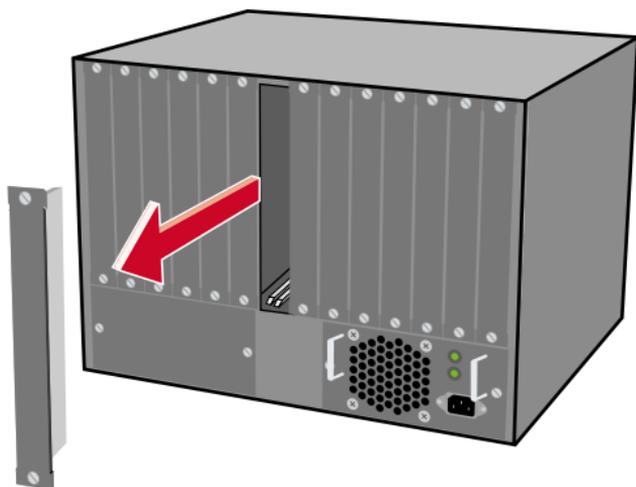


図2-5 スロットカバー取り外し

2. マネージメントモジュールの基盤の側面を本体の「M1」または「M2」のモジュール・ガイドラインに合わせます。
3. マネーメントモジュールのイジェクトレバーを起します。

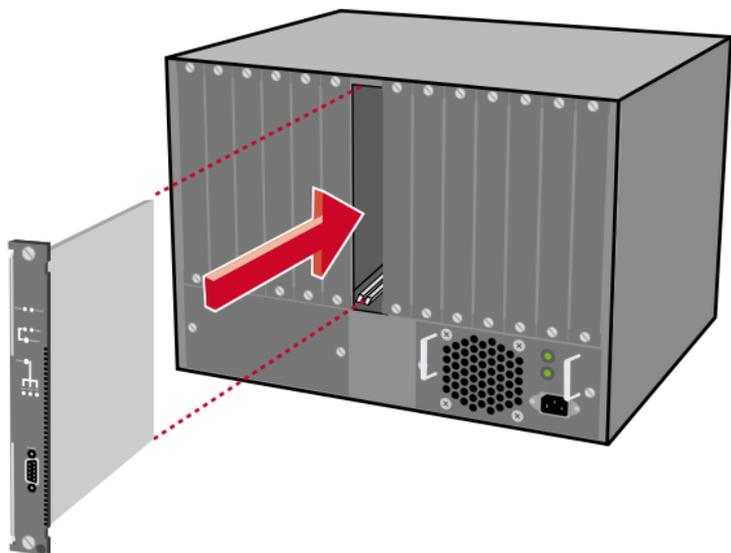


図2-6 マネージメントモジュールの取り付け位置

4. イジェクトレバー近くのフロントパネル部分を押し、マネージメントモジュールを本体の奥に滑り込ませます。

注意 本体にマネージメントモジュールを挿入する時はねじったり曲げたりはしないでください。

5. スロットの奥までしっかり押し込んだら、マネージメントモジュールの上下に付いているネジで本体にしっかりと固定します。

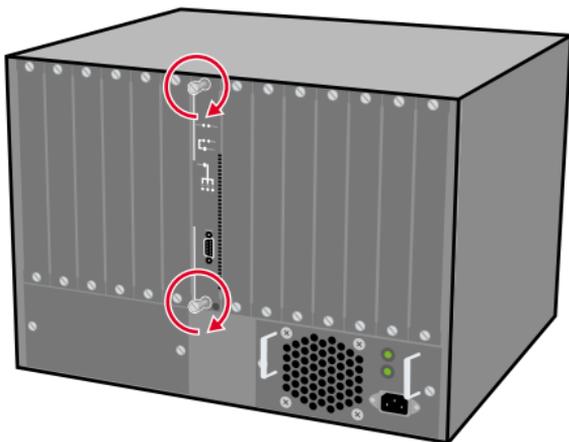


図2-7 ネジの取り付け

5 FML-1200専用モジュールの接続

本製品にFML-1200専用モジュールを接続する手順です。

重要 FML-1200専用モジュールを接続する時は、「1」～「12」と表記されているスロットを使用してください。

1. 本体の「1」～「12」の使用するスロットのスロットカバーを外します。

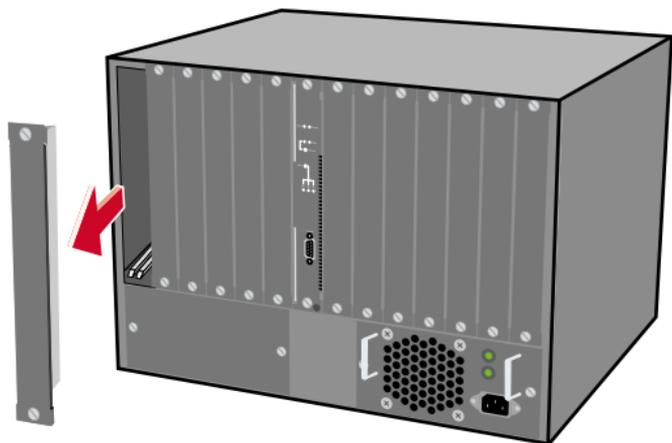


図2-8 スロットカバー取り外し

2. FML-1200専用モジュールの基盤の側面を本体の使用するスロットのモジュール・ガイドラインに合わせます。

3.FML-1200専用モジュールのイジェクトレバーを起します。

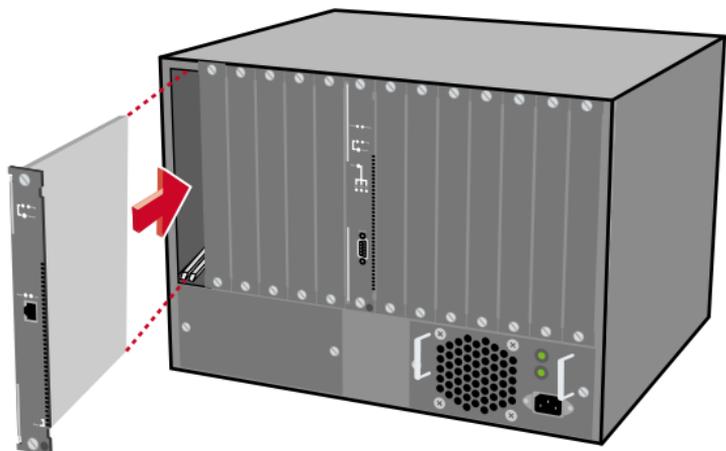


図2-9 FML-1200専用モジュールの取り付け位置

4.イジェクトレバー近くのフロントパネル部分を押し、FML-1200専用モジュールを本体の奥に滑り込ませます。

注意 本体にマネージメントモジュールを挿入する時はねじったり曲げたりはしないでください。

5. スロットの奥までしっかり押し込んだら、FML-1200専用モジュールの上下に付いているネジで本体にしっかりと固定します。

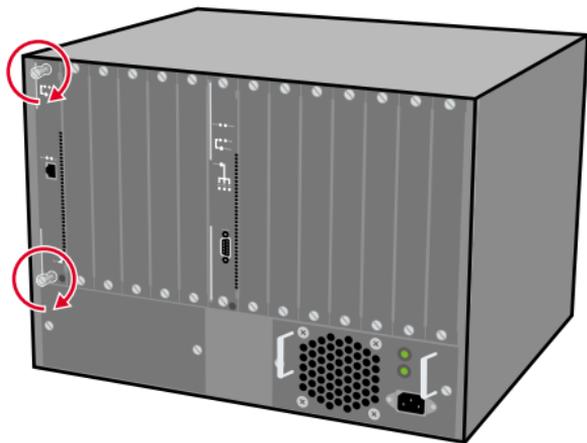


図2-10 ネジの取り付け

6 電源ユニットの接続

本製品に電源ユニットを接続する手順です。

重要：電源ユニットを接続する時は、「PWR1」,「PWR2」と表記されているスロットを使用してください。

1. 本体の「PWR1」,「PWR2」の使用するスロットのスロットカバーを外します。

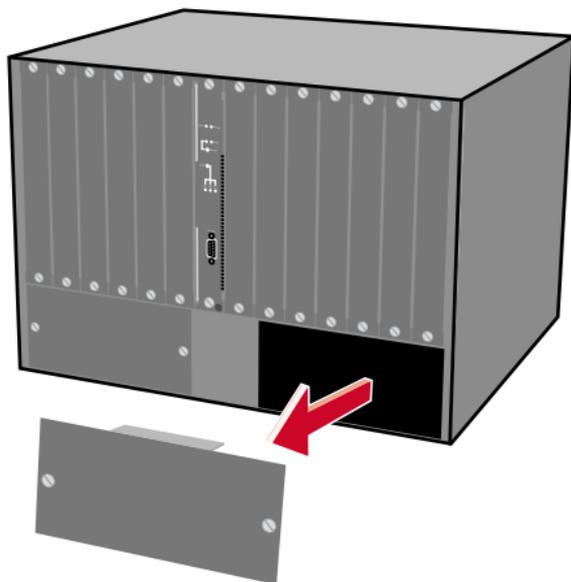


図2-11 スロットカバー取り外し

2.電源ユニットのハンドルを持ち、スロットの奥に滑り込ませます。

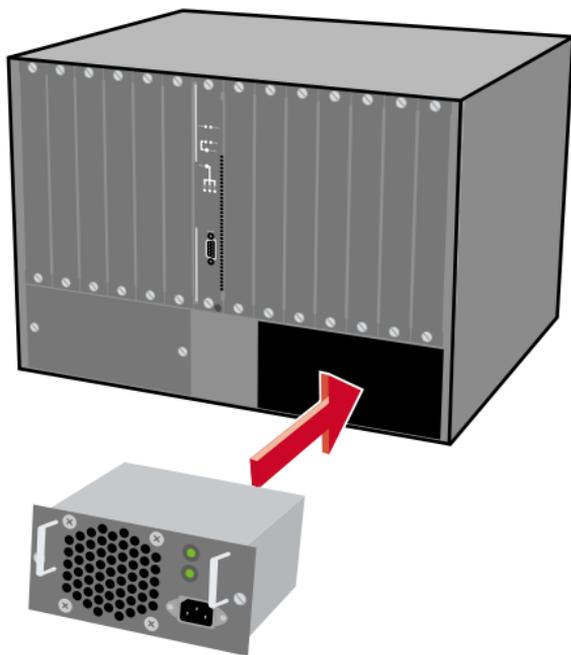


図2-12 電源ユニットの取り付け

3. スロットの奥までしっかり押し込んだら、電源ユニットの左右に付いているネジで本体にしっかりと固定します。

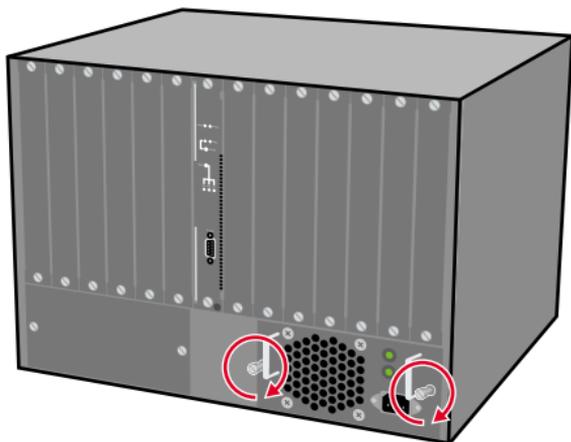


図2-13 ネジの取り付け

7 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.電源ケーブルを電源ユニット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。

注意 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。

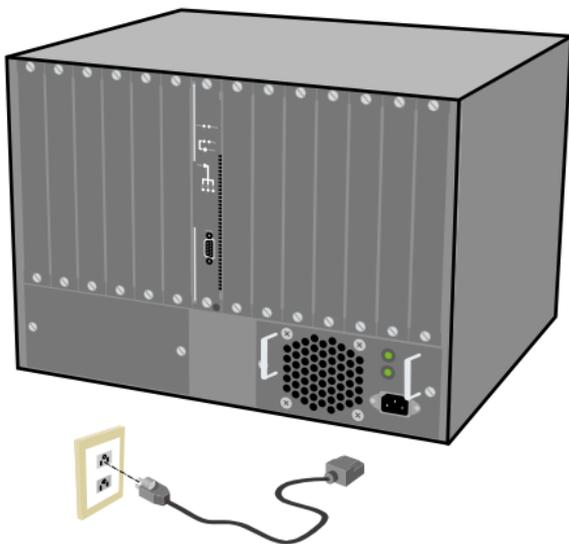


図2-14 電源ケーブルの接続方法

8 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。

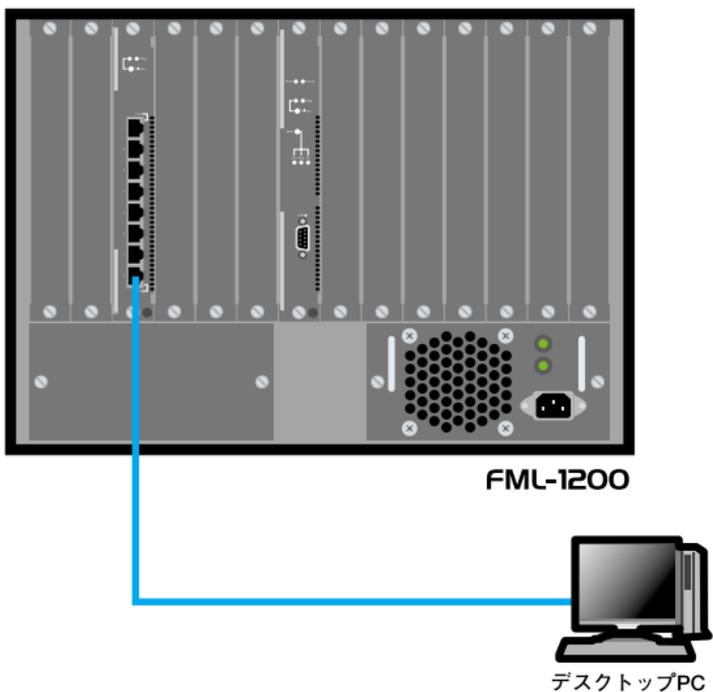


図2-15 ネットワーク機器との接続[RJ-45]

重要 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。

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
ポートまたはネットワーク機器のファイバーコネクタポートを
SC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。

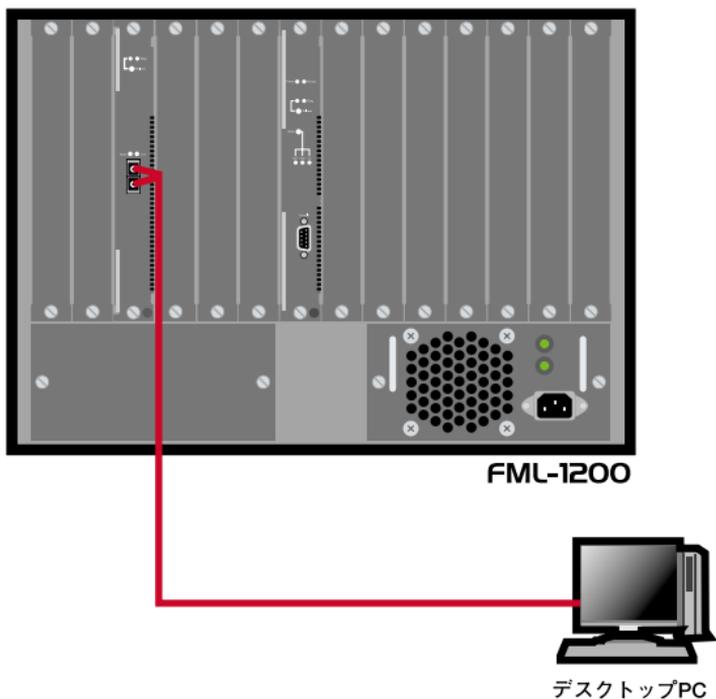


図2-16 ネットワーク機器との接続[ファイバー]

重要 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。

MT-RJポートを利用したネットワーク機器との接続

本製品のMT-RJポートとコンピュータのMT-RJコネクタまたはネットワーク機器のMT-RJコネクタをMT-RJ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MT-RJポートに接続し、もう一端を接続先機器のMT-RJポートに接続します。
2. 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。

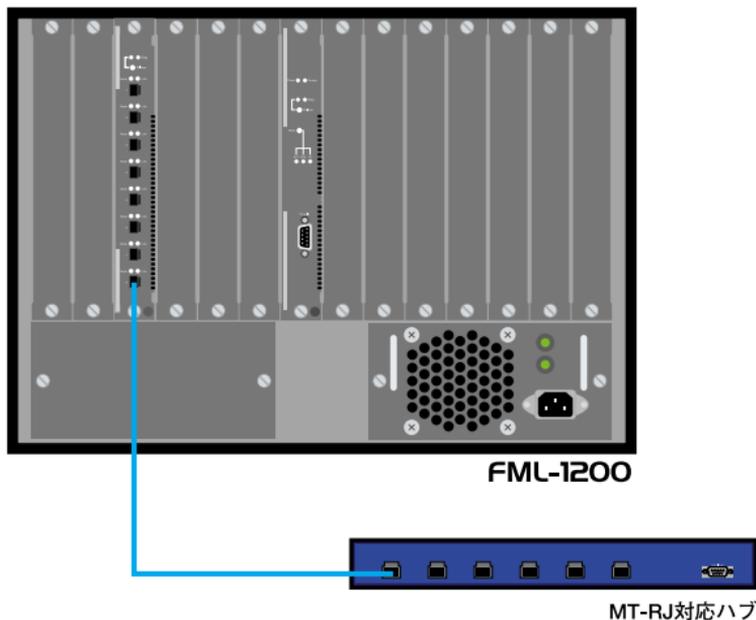


図2-17 ネットワーク機器との接続[MT-RJ]

重要 100BASE-FXマルチモードでのファイバケーブルの最大長は、IEEE 802.3u 100BASE-FXマルチモードは仕様で定められている2000mです。100BASE-FXシングルモードでのファイバケーブルの最大長は、IEEE 802.3z 100BASE-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

FML-1200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*¹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

LAポートの設定

ネットワークVLANのポート追加

IPインターフェースの追加

IPルーティングおよびマルチキャストルーティング経路の設定

システム情報および統計の表示

スパニングツリーの設定

システムファームウェアのダウンロード

設定ファイルのアップロードおよびダウンロード

注意 *¹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

マネージメントモジュール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。

注意 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(NO)」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(ストレートタイプ)を使い、マネージメントモジュールのシリアルポート(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。

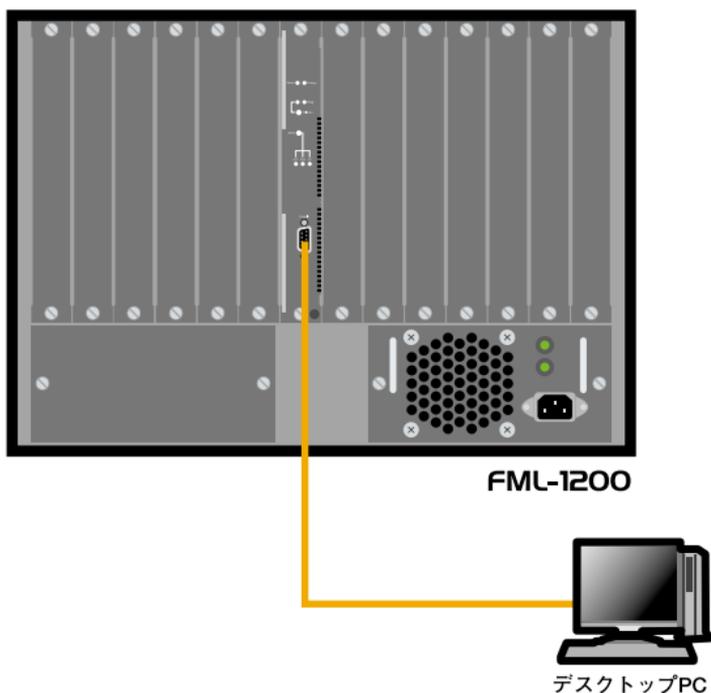


図3-1 RS-232Cケーブルの接続

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できますが、設定前に以下の作業が終わっている必要があります。設定後は、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。

シリアルポート接続のコンソールインターフェースの作業内容

- ・本製品のIPアドレス、サブネットマスク、およびデフォルトゲートウェイが設定されていること
- ・ウェブインターフェースが有効に設定されていること

注意 VLANグループは、それぞれ固有のIPインターフェースアドレスを割り当てることができます。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、本製品はどのIPアドレスからでも管理ができます。

本製品で使えるセッション数は、コンソールインターフェース×1、Telnet×4、webアクセス×8を同時に使えます。

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*1ウェブブラウザから起動できます。

注意 *1 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[OK] (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。



[OK]

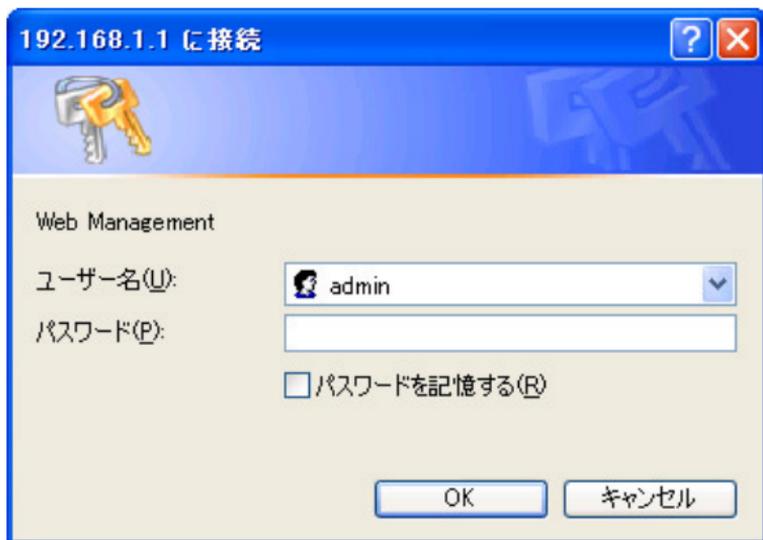
指定した値を管理エージェントにセットします。

[Cancel]

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(security権限)」が設定されています。「admin」はパスワードの設定はされていません。「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。



192.168.1.1 に接続

Web Management

ユーザー名(U): admin

パスワード(P):

パスワードを記憶する(R)

OK キャンセル

- 注意** ・パスワードの変更はシリアル接続の管理エージェント内の security [device] [user] [modify X 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。

System	78ページ
Console	
Setup	90ページ
Control	
Initialize	91ページ
Reboot	92ページ
Software Upgrade	93ページ
Management	
Setup	95ページ
Telnet	
Connect	96ページ
Getting Started	97ページ
Bridge	
Address Database	
Add	104ページ
Aging Time	106ページ
Find	107ページ
Remove	108ページ
Summary	109ページ
Broadcast Storm Control	
Setup	112ページ

Link Aggregation	
Modify	
AddPort	113ページ
Admin State	114ページ
Remove Port	115ページ
Summary	116ページ
Multicast Filter	
ICMP Mode	117ページ
Snooper Mode	118ページ
Spanning Tree	
Setup	119ページ
VLAN	
Create	121ページ
Delete	122ページ
Modify	123ページ
Physical Interface	
Ethernet	
Setup	128ページ
Statistics	131ページ
Summary	139ページ
Protocol	
IP	
ARP	
Aging	142ページ
Display/ Edit	143ページ
Flush	146ページ

INTERFACE

Display/ Edit 147ページ

OSPF

ASBR Summary 153ページ

Display areas 160ページ

Interface 170ページ

LSAs Database Summary 177ページ

LSAs Summary 179ページ

LSAs AsSummary 180ページ

LSAs router 183ページ

LSAs network 185ページ

LSAs external 187ページ

LSAs NssaExternal 189ページ

Display Neighbors 191ページ

Modify Router ID 193ページ

Virtual links modify 196ページ

RIP

Display/ Edit 204ページ

Mode 207ページ

Neighbors 208ページ

Statistics 209ページ

ROUTE

Default Gateway 210ページ

Display 211ページ

Flush 216ページ

UDP Helper	
Display/Edit	217ページ
Setup	222ページ
Security	
Device	
User	
Modify	227ページ
Network	
Access	
Port Security	228ページ

5 Summary Menu

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。画面の上側に項目メニュー一覧、左側にメニュー一覧、右側に簡単なシステム情報、各スロットのタイプ・各バージョン情報が表示されます。

PCI Web Management - Microsoft Internet Explorer

http://192.168.1.1/

FML-1200

Summary Device View Help View

System

System Summary	
System Name:	DEFAULT SYSTEM NAME
Location:	DEFAULT SYSTEM LOCATION
Contact:	DEFAULT SYSTEM CONTACT
Up Time:	0 d 0 h 50 min 0 s
Software Version:	V1.1
Ip address:	192.168.1.1

Device Summary Slot 1	
Type:	PCI-GBTH module
Microcode Version:	V5.5
Hardware Version:	V1.0

Device Summary Slot 4	
Type:	PCI-GBTH module
Microcode Version:	V5.5
Hardware Version:	V1.0

Device Summary Slot 5

6 Device View Menu

「Summary Menu」の状態から項目メニュー一覧の「Device View」を選択すると、以下の画面が表示されます。画面内容として、画面の上側に項目メニュー一覧、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。

The screenshot shows the FCL Web Management interface for device FML-1200. The browser window title is 'FCL Web Management - Microsoft Internet Explorer'. The address bar shows 'http://192.168.1.1/'. The page title is 'FML-1200'. The navigation tabs are 'Summary', 'Device View', and 'Help View'. The left sidebar menu includes 'System', 'Bridge', 'Physical Interface', 'Protocol', and 'Security'. The main display area shows a grid of device status indicators for 'PCI FML-1200'. The grid has columns for ports 0-12 and rows for various status indicators. Below the grid are buttons for 'Polling Interval', 'Poll Now', and 'Color Key'. The 'Device Summary' panel at the bottom right displays the following information:

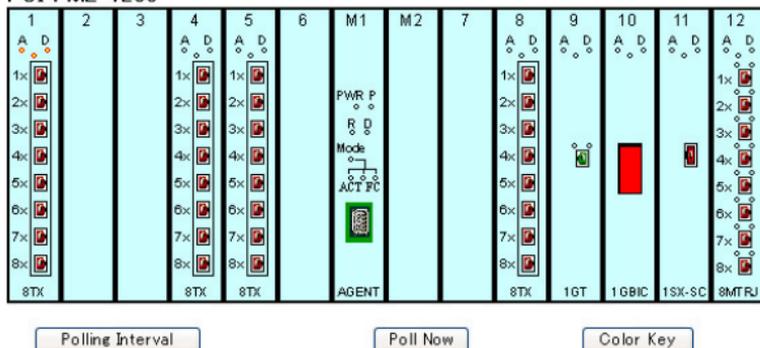
Device Summary	
Name:	DEFAULT SYSTEM NAME
Type:	FML-1200
Software Version:	V3.1
Hardware Version:	V3.0 (800 CPU)
MAC Address:	00:00:00:00:00:00

7 ポート画面

ポート画面は、本製品のマネージメントモジュールの設定・状態、各ポートの設定・状態が表示されます。各ポートおよびマネージメントモジュールをクリックすると、統計および設定情報が表示されます。各ポートは色によって状態を判断することができます。

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

PCI FML-1200



【Polling Interval】

自動更新を行なう時間を設定します。

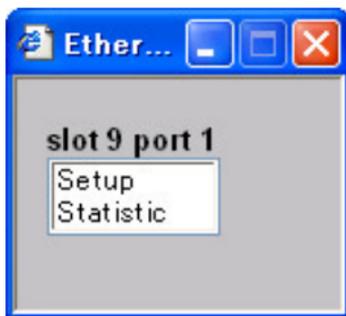
初期状態：[180] 単位は秒。

【Polling Now】

すぐに更新をします。

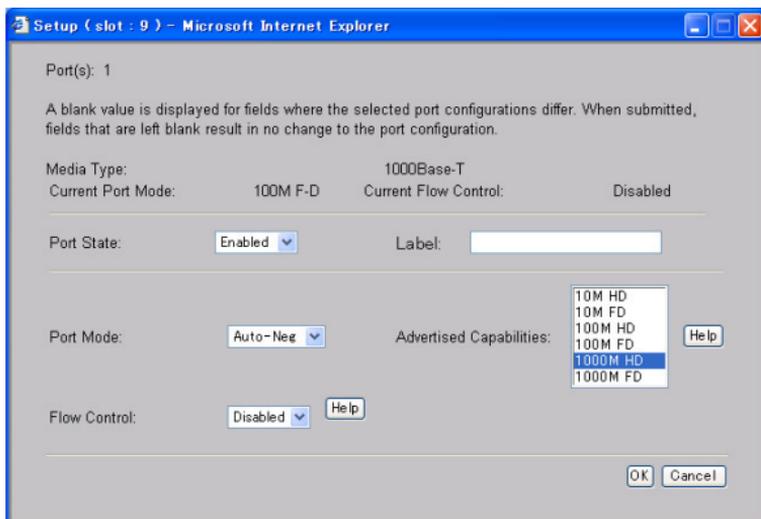
各ポート

色でリンクの状態が表示されます。クリックすると、「Ethernet Port」が表示され設定と統計情報が参照できます。



【Setup】

「Ethernet Port」から「Setup」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等を設定することができます。



【Port State】

ポートの有効/無効を選択します。

- ・ Enabled : 有効
- ・ Disabled : 無効

【Port Mode】

ポートの通信速度を選択します。

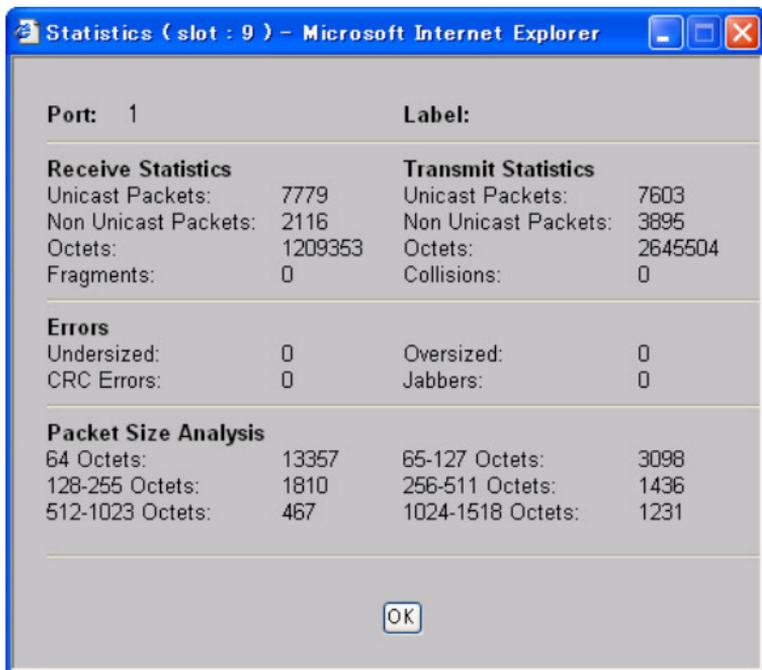
【Flow Control】

フロー制御を設定します。

- ・ Enabled : 有効
- ・ Disabled : 無効

Statistic

「Ethernet Port」から「Statistic」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EthernetMIBに関する統計情報が表示されます。表示される情報は、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。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。



Port:	1	Label:	
Receive Statistics		Transmit Statistics	
Unicast Packets:	7779	Unicast Packets:	7603
Non Unicast Packets:	2116	Non Unicast Packets:	3895
Octets:	1209353	Octets:	2645504
Fragments:	0	Collisions:	0
Errors			
Undersized:	0	Oversized:	0
CRC Errors:	0	Jabbers:	0
Packet Size Analysis			
64 Octets:	13357	65-127 Octets:	3098
128-255 Octets:	1810	256-511 Octets:	1436
512-1023 Octets:	467	1024-1518 Octets:	1231

OK

【Port Number】

ポート番号を選びます。

Receive Statistics

【Unicast Pkts】

高位層プロトコルに渡されたサブネットワーク - ユニキャストパケット数です。

【Non-Unicast Pkts】

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

【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。

【Fragments】

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。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。

Transmit Statistics

【Unicast Pkts】

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。

【Non-Unicast Pkts】

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

【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。

【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。

Errors

【Undersized】

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。

【Oversized】

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。

【CRC 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。

【Jabbers】

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。

Packet Size Analysis

【64 Octets】

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せん。

【65-127 Octets】

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せん。

【128-255 Octets】

(同上)

【256-511 Octets】

(同上)

【512-1023 Octets】

(同上)

【1024-1518 Octets】

(同上)

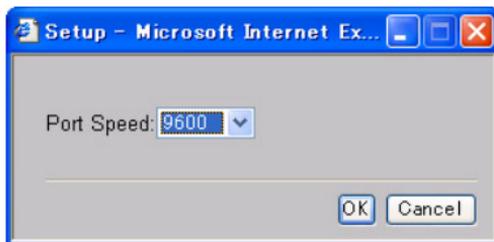
AGENT

[AGENT]のシリアルポート図をクリックすると、[Device Body]が表示されます。シリアルポートの通信パラメータの設定、参照ができます。



【Setup】

[Device Body]から[Setup]をクリックすると、以下の[Setup]が表示されます。通信時のデータ転送速度を設定します。



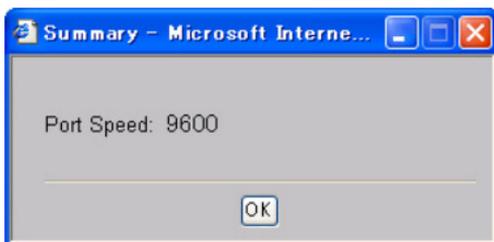
【Port Speed】

通信時のデータ転送速度を設定します。

- ・ 2400 : 2400 bps
- ・ 4800 : 4800 bps
- ・ 9600 : 9600 bps
- ・ 19200 : 19200 bps
- ・ AUTO : 自動識別

【Summary】

[Device Body]から[Summary]をクリックすると、以下の[Summary]が表示されます。現在の通信時のデータ転送速度を表示します。



8 Setup(Console)

[System] [Console] [Setup]をクリックすると、以下の画面が表示されます。通信時のデータ転送速度を設定します。



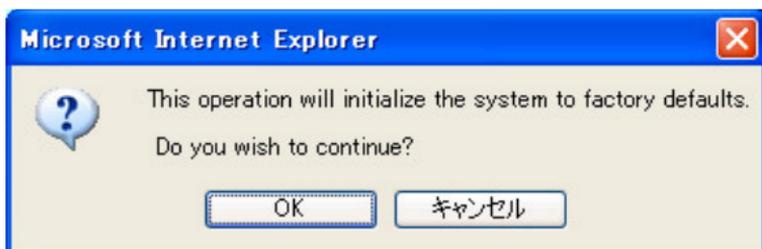
【Port Speed】

通信時のデータ転送速度を設定します。

- 2400 : 2400 bps
- 4800 : 4800 bps
- 9600 : 9600 bps
- 19200 : 19200 bps
- AUTO : 自動識別

9 Initialize(Control)

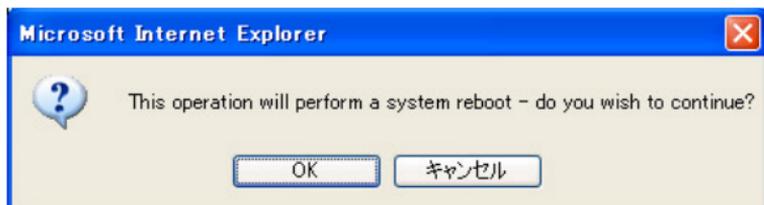
[System] [Control] [Initialize]をクリックすると、以下の画面が表示されます。本製品を再起動時に工場出荷状態の設定に戻すか設定します。



工場出荷状態に戻すときは[OK]を、中止するときは[キャンセル]をクリックします。

10 Reboot(Control)

[System] [Control] [Reboot]をクリックすると、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。



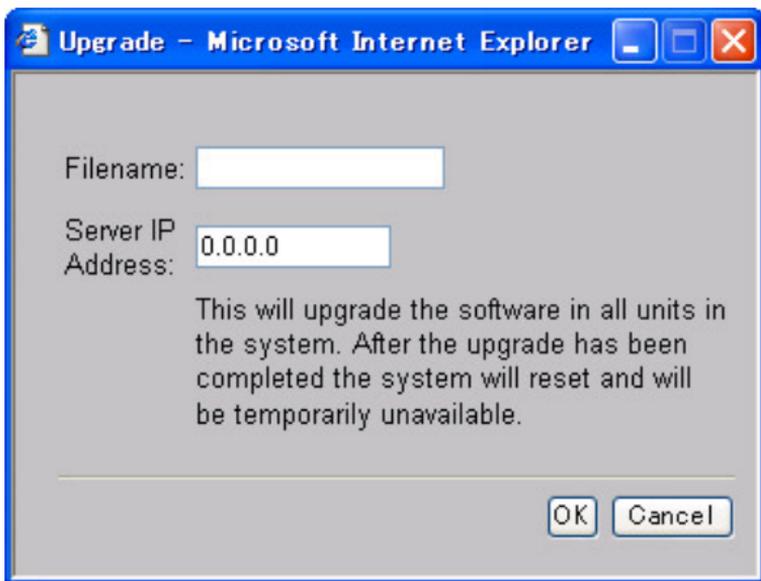
再起動するときは[OK]を、中止するときは[キャンセル]をクリックします。

11 Software Upgrade(Control)

[System] [Control] [Software Upgrade]をクリックすると、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。ダウンロード終了後、本製品は自動で再起動します。



【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。

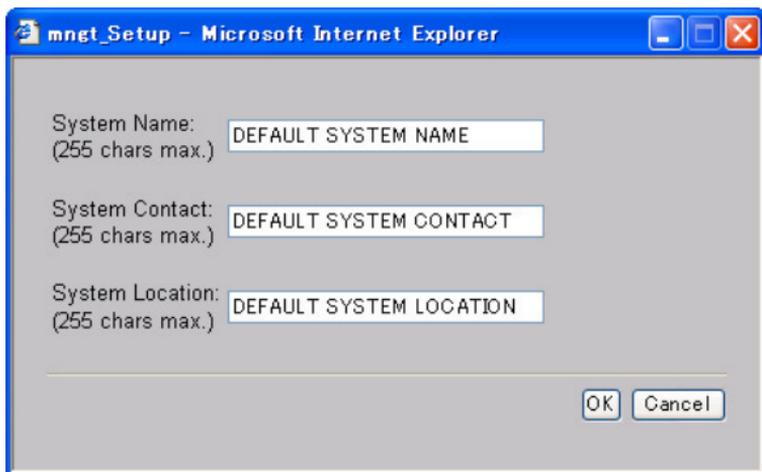
【Server IP Address】

TFTPサーバのIPアドレスを設定します。

選択終了後[OK]をクリックすると、指定ファイルのダウンロードを開始します。

12 Setup(Management)

[System] [Management] [Setup]をクリックすると、以下の画面が表示されます。システム監理者の情報、連絡先などのシステム情報の設定と参照ができます。



mngt_Setup - Microsoft Internet Explorer

System Name: (255 chars max.)

System Contact: (255 chars max.)

System Location: (255 chars max.)

【 *1System Name 】

システム名を設定します。

【 *1System Contact 】

管理者の情報を設定します。

【 *1System Location 】

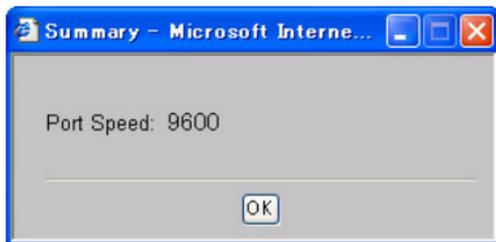
システムの設置場所を設定します。

*1 各項目とも最大255文字の半角英数字で設定します。

13 Connect(Telnet)

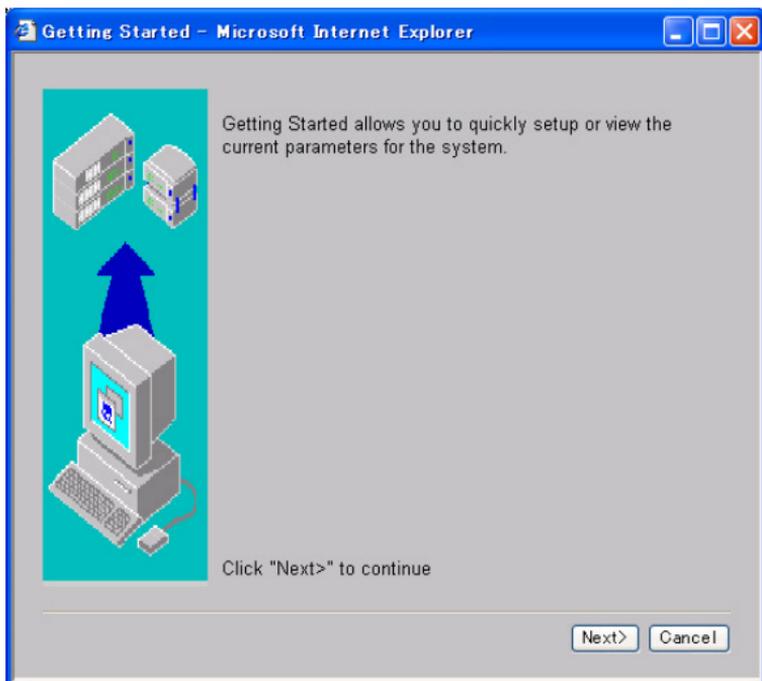
[System] [Telnet] [Connect]をクリックすると、以下の画面が表示されます。

ターミナルユーティリティを使用してTelnetを接続します。



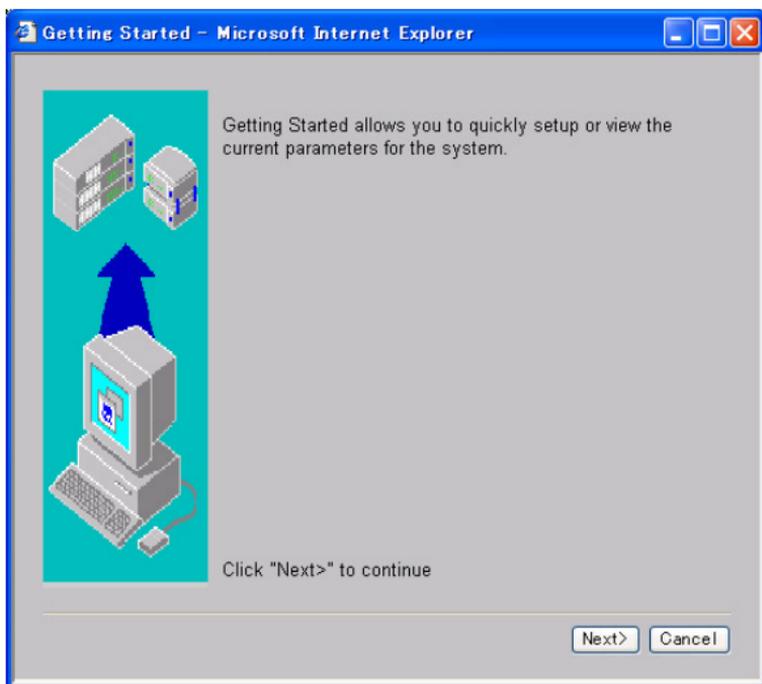
14 Getting Started

[System] [Getting Started]をクリックすると、以下の画面が表示されます。本製品の基本的な初期設定ができます。

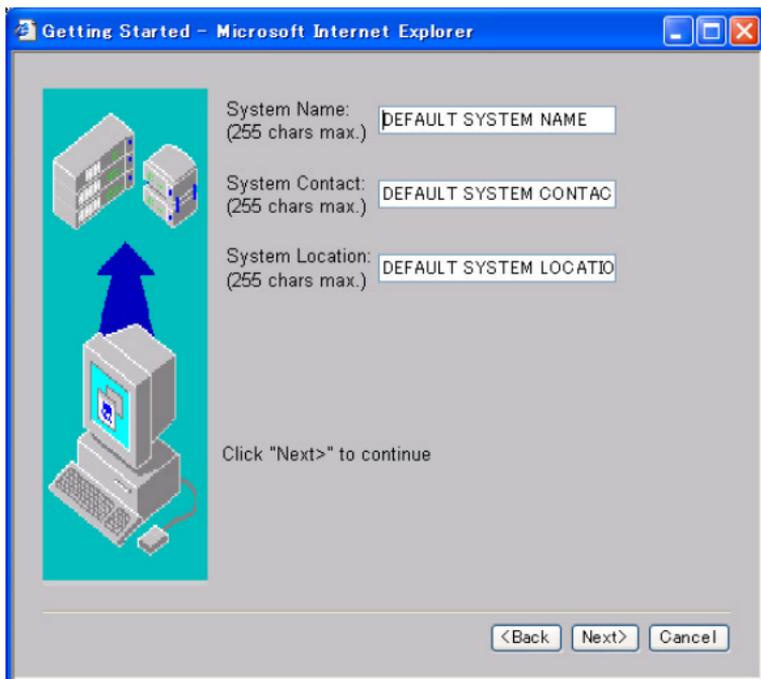


設定方法

1. [System] [Getting Started]をクリックすると、以下の画面が表示されます。[NEXT >]をクリックします。



2. System Name、 System Contact、 System Locationを入力して
[NEXT >]をクリックします。



Getting Started - Microsoft Internet Explorer

System Name: (255 chars max.)

System Contact: (255 chars max.)

System Location: (255 chars max.)

Click "Next>" to continue

< Back Next > Cancel

【 *1System Name 】

システム名を設定します。

【 *1System Contact 】

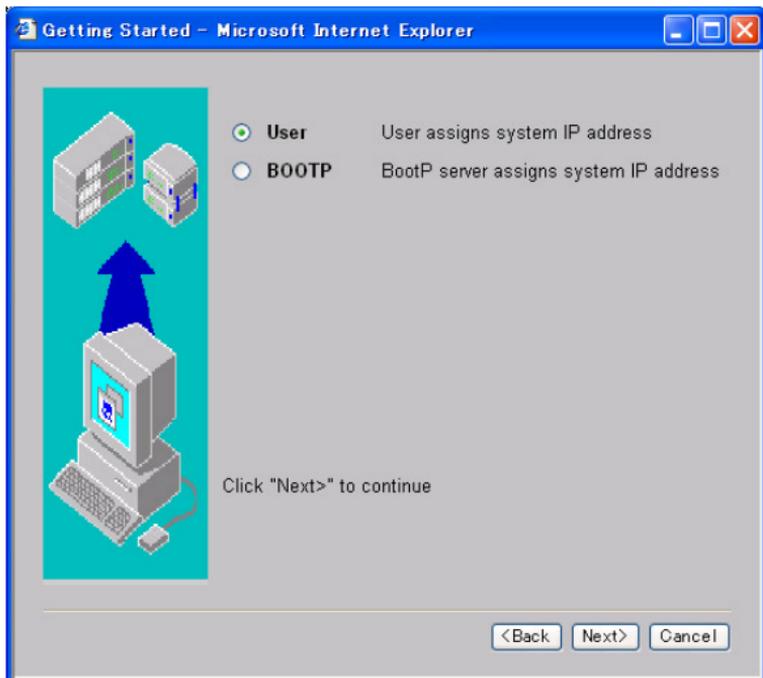
管理者の情報を設定します。

【 *1System Location 】

システムの設置場所を設定します。

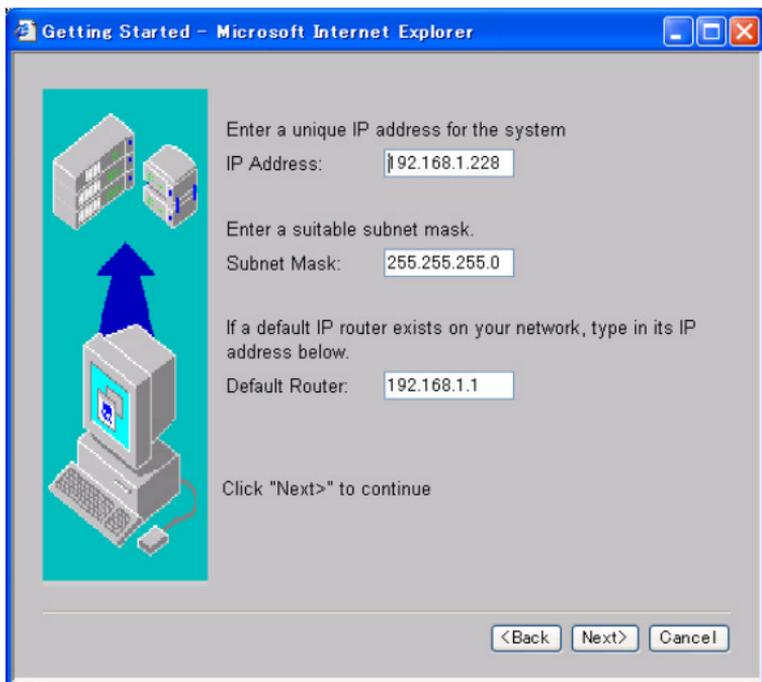
*1 各項目とも最大255文字の半角英数字で設定します。

- 3.本製品の管理用にIPサブネットアドレスを設定するため、手動設定かBootPを選択して[NEXT >]をクリックします。



- ・ User : 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

- 4.上記の項目で[User]を選択したときは以下の画面が表示されます。[BOOTP]を選択したときは「5.」へ進んでください。IP アドレス、サブネットマスク、デフォルトゲートウェイに入力して[NEXT>]をクリックします。



Getting Started - Microsoft Internet Explorer

Enter a unique IP address for the system
IP Address:

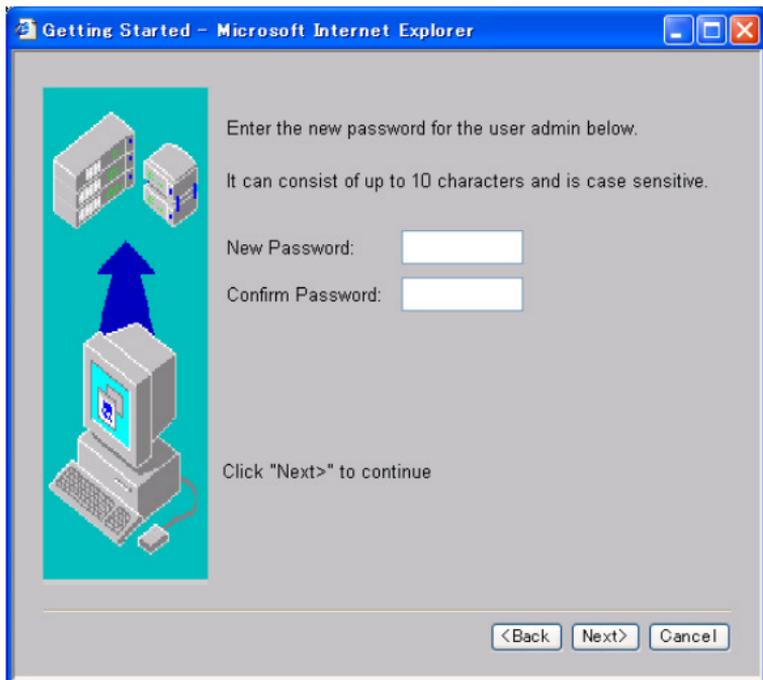
Enter a suitable subnet mask.
Subnet Mask:

If a default IP router exists on your network, type in its IP address below.
Default Router:

Click "Next>" to continue

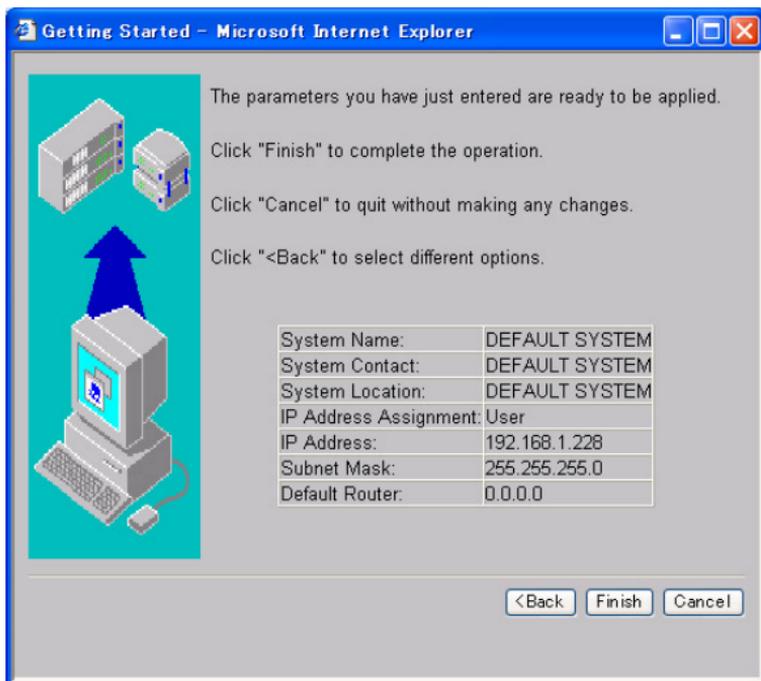
< Back Next> Cancel

5. ログインネーム「admin」のパスワードを設定する画面が表示されます。パスワードを設定して[NEXT >]をクリックします。



- ・ New Password : 新しいパスワードを入力します。
- ・ Confirm Password : 確認のため、もう一度パスワードを入力します。

6. 設定の確認画面が表示されます。設定内容に間違いがないことを確認して[Finish]をクリックします。訂正は[Back]をクリックします。



15 Add(Address Database)

[Bridge] [Address Database] [Add]をクリックすると、以下の画面が表示されます。静的にMACアドレスを設定できます。

Add - Microsoft Internet E...

Select an option below:

Add address on a Port

Add address on an Aggregated Link

Select a Slot and then a Port:

Slot 1 Port 1

MAC Address:
(for example 08-00-15-de-3d-42)

VLAN number: (1-2047)

OK Cancel

【Slot】

静的に入力するMACアドレスが接続されているスロット番号を設定します。

注意 接続されているスロットのスロット番号が表示されます。

【Port】

静的に入力するMACアドレスが接続されているポート番号を設定します。

注意 選択したスロットのポート番号が表示されます。

【MAC Address】

ユニキャストテーブルに静的に入力したいMACアドレスを設定します。

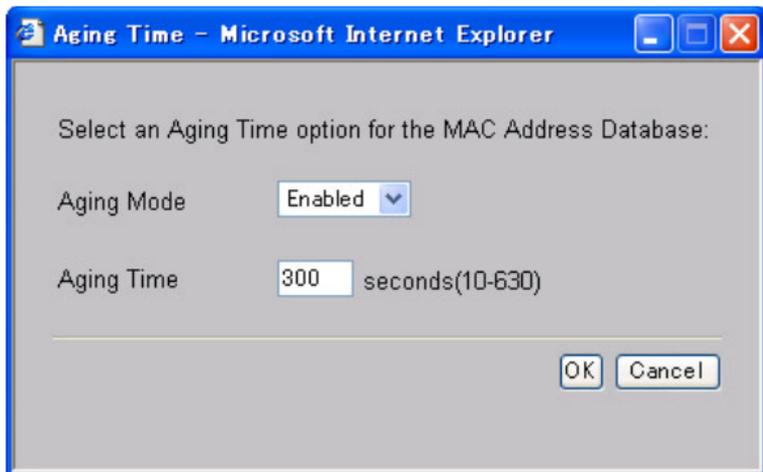
【VLAN number】

静的に入力するMACアドレスが接続されているVLAN IDを設定します。

注意 現在、作成されているVLAN IDを指定します。

16 Aging Time(Address Database)

[Bridge] [Address Database] [Aging Time]をクリックすると、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。



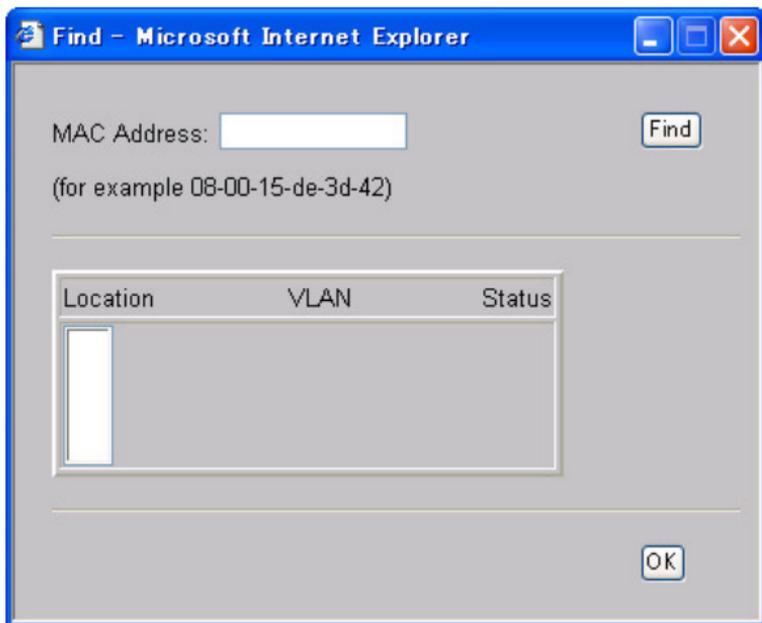
【Aging Mode】

フォワーディング情報をエージアウトの有効/無効を設定します。

- ・ Enabled : 有効
- ・ Disabled : 無効

17 Find(Address Database)

[Bridge] [Address Database] [Find]をクリックすると、以下の画面が表示されます。MACアドレスの情報からスロット番号とポート番号を検索します。



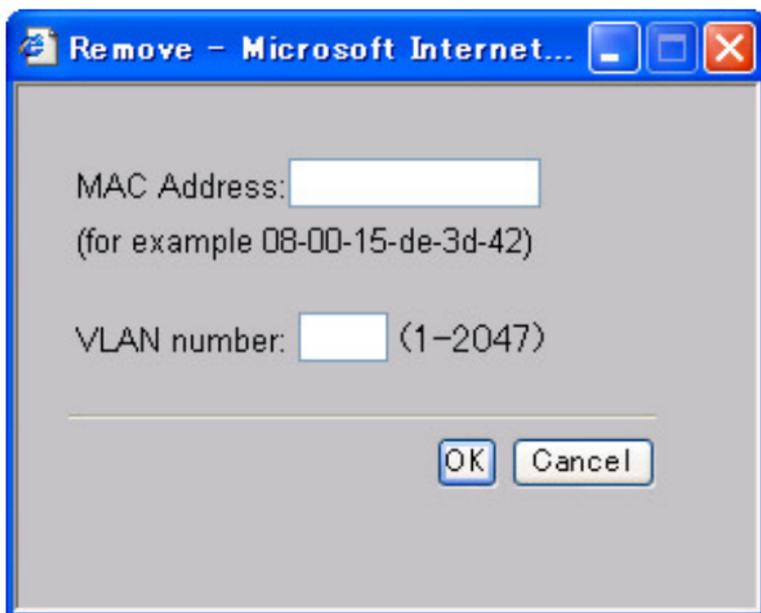
【MAC Address】

検索したい動的または静的に学習したフォワーディング情報のMACアドレスを入力します。MACアドレスを指定してから「Find」をクリックします。

*下側に検索結果が表示されます。

18 Remove(Address Database)

[Bridge] [Address Database] [Remove]をクリックすると、以下の画面が表示されます。設定した静的MACアドレスを削除します。



【MAC Address】

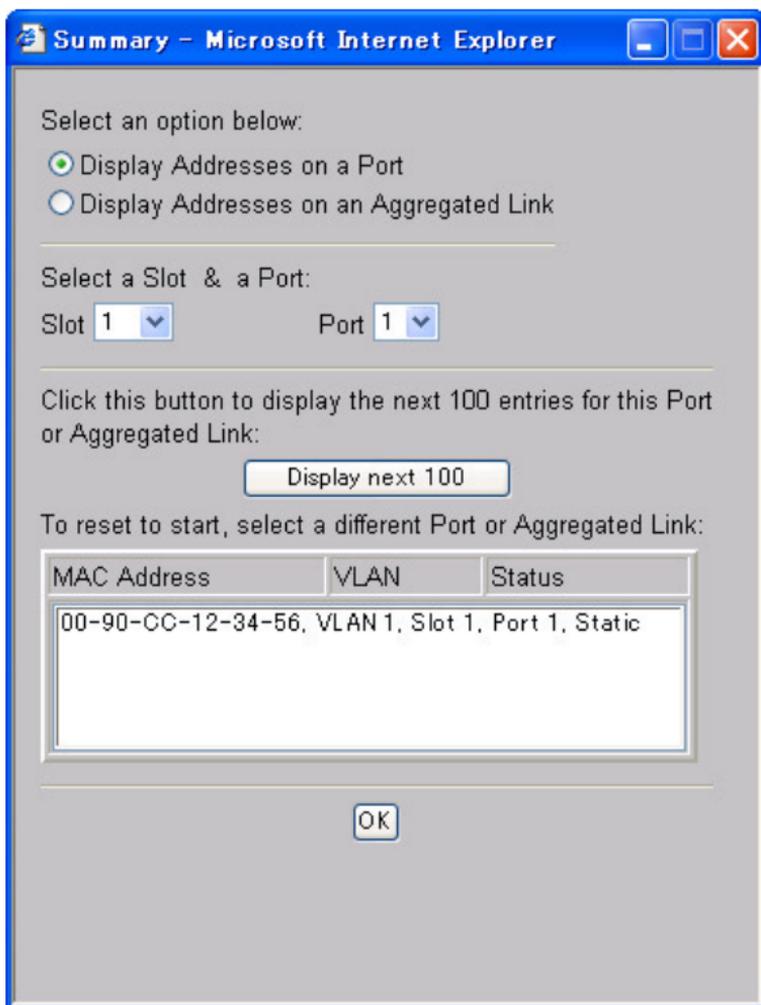
削除する静的MACアドレスを設定します。

【VLAN number】

削除する静的MACアドレスが所属するVLAN IDを設定します。

19 Summary(Address Database)

[Bridge] [Address Database] [Remove]をクリックすると、以下の画面が表示されます。MACアドレス・テーブルを参照できます。



Display Addresses on a Port

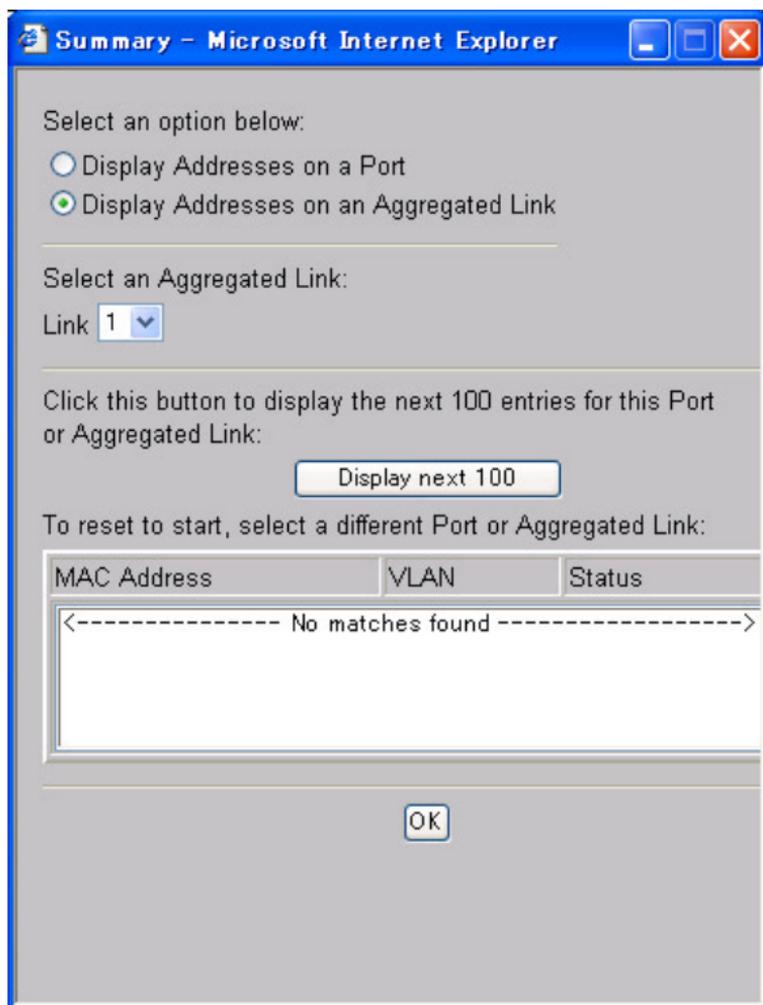
【Slot】

MACアドレス・テーブルを表示させたいスロット番号を設定します。

【Port】

MACアドレス・テーブルを表示させたいポート番号を設定します。

Display Addresses on a Aggregated

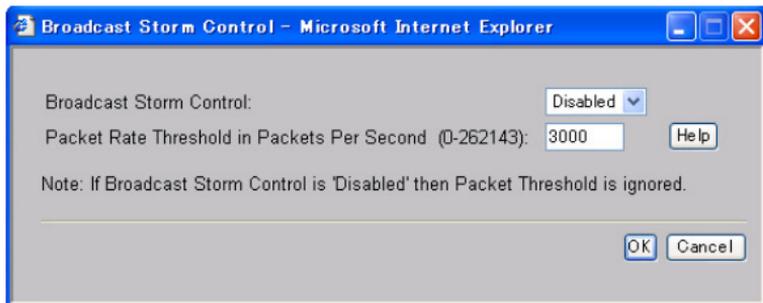


【Link】

現在、作成されているLink Aggregationのグループ番号を設定します。

20 Setup(Broadcast Storm Control)

[Bridge] [Broadcast Storm Control] [Setup]をクリックすると、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ができます。



【Broadcast Storm Control】

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。

- ・ Enabled : 有効
- ・ Disabled : 無効

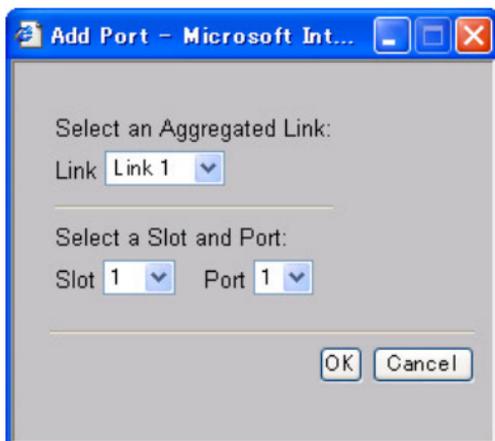
【Packet Rate Threshold in Packets Per Second】

連続したブロードキャスト(マルチキャスト)フレームは破棄させる設定値を設定します。

- ・ 0 ~ 262143 : 設定値を設定

21 AddPort(Link Aggregation)

[Bridge] [Link Aggregation] [modify] [AddPort]をクリックすると、以下の画面が表示されます。link Aggregationグループの追加ができます。



【Link】

link Aggregationのグループ番号を設定します。

* グループ1～グループ12が表示されます。

【Slot】

選択したグループに含みたいスロット番号を選択します。

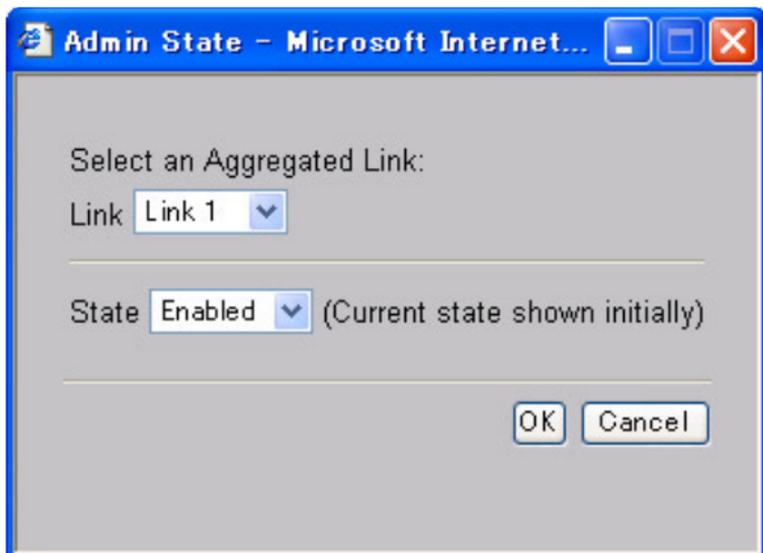
【Port】

選択したスロットで登録したいポート番号を選択します。

重要 Link Aggregationは最大ポート数4ポート、最大グループ数12グループ作成することが出来ます。

22 Admin State(Link Aggregation)

[Bridge] [Link Aggregation] [modify] [Admin State]をクリックすると、以下の画面が表示されます。Link Aggregationの有効/無効ができます。



【Link】

現在作成されているLink Aggregationグループを選択します。

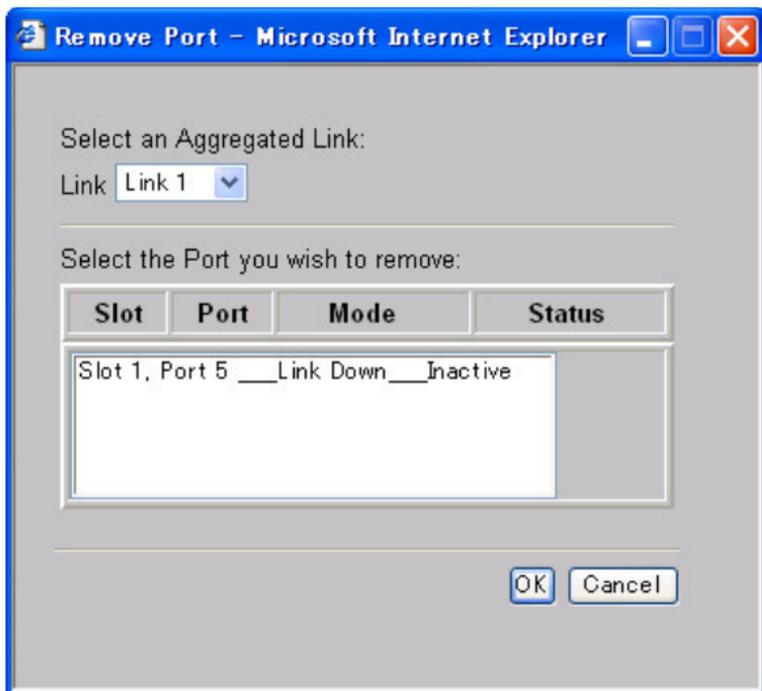
【State】

選択したグループの有効/無効を選択します。

- ・ Enabled : 有効
- ・ Disabled : 無効

23 Remove Port(Link Aggregation)

[Bridge] [Link Aggregation] [modify] [Remove Port]をクリックすると、以下の画面が表示されます。Link Aggregationグループ内のポートを削除することができます。



【Link】

現在作成されているlink Aggregationグループを選択します。

下側に登録されているポート情報が表示されます。削除するポートを選択して[OK]をクリックします。

24 Summary(Link Aggregation)

[Bridge] [Link Aggregation] [Summary]をクリックすると、以下の画面が表示されます。各グループの詳細が参照できます。



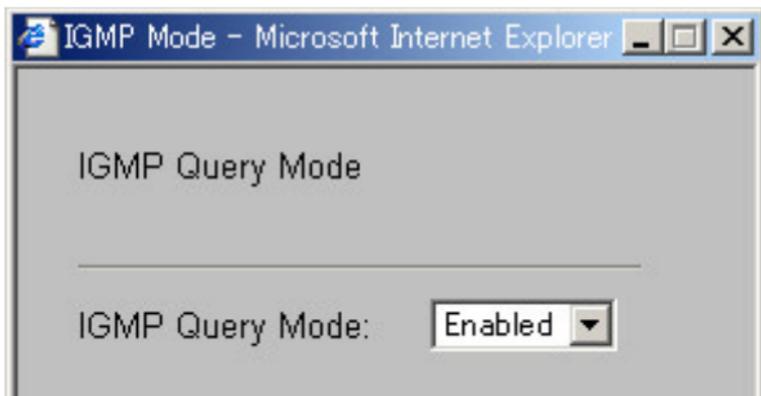
【Link】

現在作成されているlink Aggregationグループを選択します。

下側に登録されているポート情報が表示されます。

25 IGMP Mode(Multicast Filter)

[Bridge] [Multicast Filter] [IGMP Mode]をクリックすると、以下の画面が表示されます。IGMPスヌーピングを有効にしたときのクエリーの設定をします。



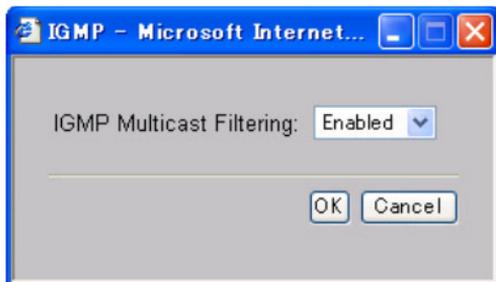
【IGMP Query Mode】

IGMPクエリ応答を設定します。IGMPはマルチキャストルータに、どのマルチキャストグループが何台関心があるか判断するため、クエリ受信を行います。

- ・ ENABLED : 有効
- ・ DISABLED : 無効

26 SnoopMode(Multicast Filter)

[Bridge] [Multicast Filter] [SnoopMode]をクリックすると、以下の画面が表示されます。IGMPスヌーピングの有効/無効が設定できます。



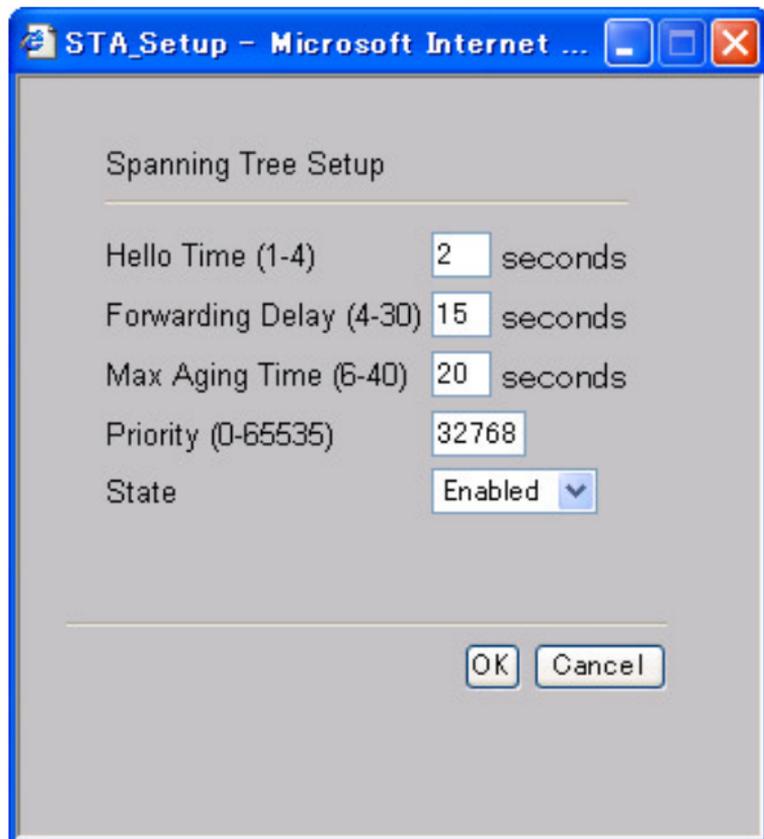
【IGMP Multicast Filtering】

IGMPスヌーピングの有効/無効が設定をします。

- Enabled : 有効
- Disabled : 無効

27 Setup(Spanning Tree)

[Bridge] [Spanning Treer] [Setup]をクリックすると、以下の画面が表示されます。スパニングツリーの設定ができます。



The image shows a dialog box titled "STA_Setup - Microsoft Internet ...". The dialog is titled "Spanning Tree Setup" and contains the following settings:

Hello Time (1-4)	<input type="text" value="2"/>	seconds
Forwarding Delay (4-30)	<input type="text" value="15"/>	seconds
Max Aging Time (6-40)	<input type="text" value="20"/>	seconds
Priority (0-65535)	<input type="text" value="32768"/>	
State	<input type="text" value="Enabled"/>	<input type="button" value="v"/>

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

【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。

- ・最大値 = { (Max. Message Age ÷ 2) - 1 }

【Forwarding Delay】

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 }

【Max Aging Time】

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。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。

- ・最小値 = { 2 × (Hello Time + 1) }

- ・最大値 = { 2 × (Forward Delay - 1) }

【Priority】

スパニングツリーを形成しているネットワークでの優先度を設定します。

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。

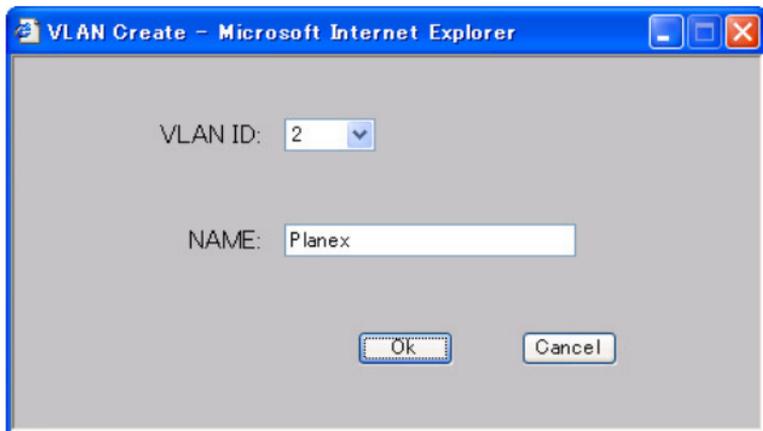
【State】

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/非参加を設定します。

- ・Enabled：参加
- ・Disabled：非参加

28 Create(VLAN)

[Bridge] [VLAN] [Create]をクリックすると、以下の画面が表示されます。VLANグループを作成することができます。



【VLAN ID】

作成するVLAN IDを選択します。

* 2 ~ 2046まで設定可能

注意 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。

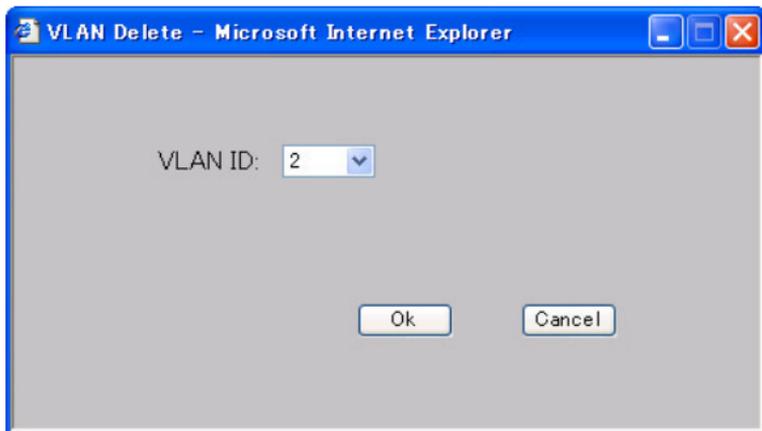
【NAME】

作成したVLAN IDに管理しやすい名前を設定します。

* 最大数：半角英数16文字まで可能

29 Delete(VLAN)

[Bridge] [VLAN] [Delete]をクリックすると、以下の画面が表示されます。作成したVLANグループを削除することができます。



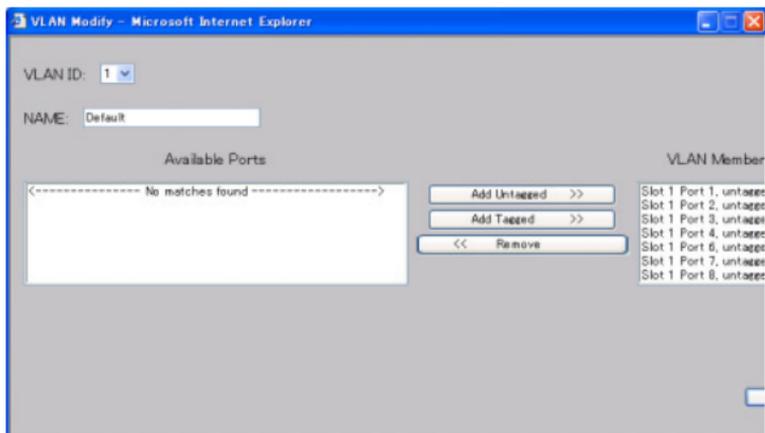
【VLAN ID】

削除するVLANグループを選択します。

注意 VLAN ID「1」はデフォルトVLANのため削除することはできません。

30 Modify(VLAN)

[Bridge] [VLAN] [Modify]をクリックすると、以下の画面が表示されます。VLANグループにポートの振り当て、削除およびVLAN名の変更ができます。



【VLAN ID】

ポートを追加するVLANグループを選択します。

* 現在、作成されているVLAN IDのみ表示されます。

【NAME】

変更する名前を指定します。

* 最大数：半角16文字まで可能

【Available Port】

選択したVLAN IDに登録されていないスロット番号およびポート番号が表示されます。

【add Untagged】

タグ無しパケットで通信したい時に選択します。

【add Tagging】

タグ付きパケットで通信したい時に選択します。

【Remove】

VLANグループに振り当てられたポートを削除します。

【VLAN Members】

振り当てられているスロット番号およびポート番号が表示されます。

ポートの追加(タグ無しパケット)

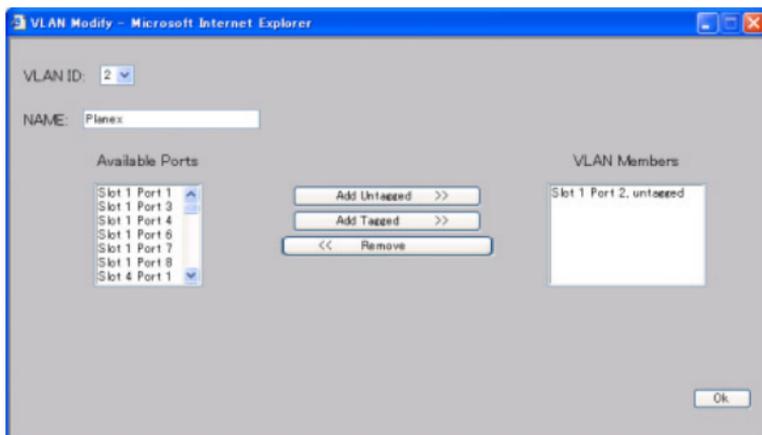
1. 「VLAN ID」でポートを追加したいVLAN IDを選択します。
2. 「Available Port」で追加したいスロット番号とポート番号の組み合わせを選択します。
3. 「add Untagged」をクリックします。
4. 「This operation will change the port's untagged membership」が表示されるので「OK」をクリックします。



5. 「Are you sure you wish to continue」が表示されるので、「OK」をクリックします。

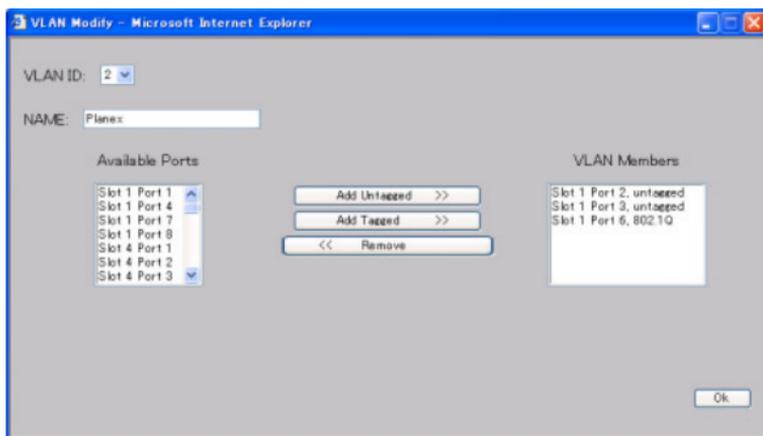


6. 「VLAN Members」にスロット番号とポート番号が「Slot * Port * , untagged」と表示されます。「 」は選択したスロット番号とポート番号が表示されます。



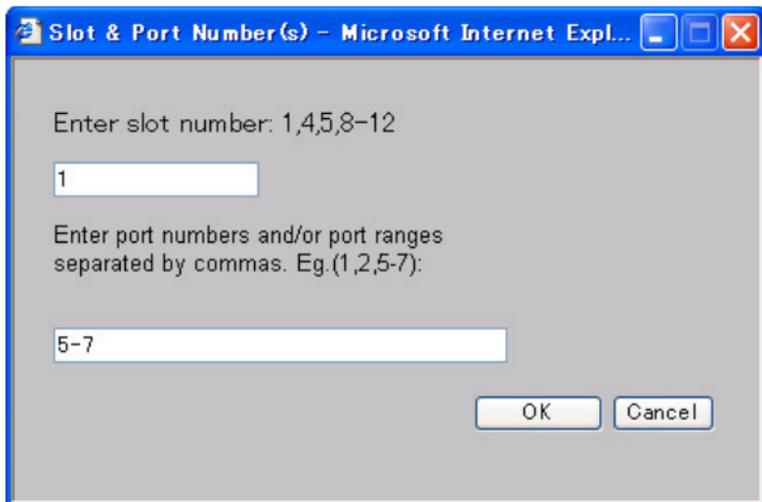
ポートの追加(タグ付きパケット)

1. 「VLAN ID」でポートを追加したいVLAN IDを選択します。
2. 「Available Port」で追加したいスロット番号とポート番号の組み合わせを選択します。
3. 「add Tagging」をクリックします。
4. 「VLAN Members」にスロット番号とポート番号が「Slot * Port * , 802.1Q」と表示されます。「 」は選択したスロット番号とポート番号が表示されます。



31 Setup(Ethernet)

[Physical Interface] [Ethernet] [Setup]をクリックすると、以下の画面が表示されます。ポートの通信パラメータを変更できます。



Slot & Port Number(s) - Microsoft Internet Expl...

Enter slot number: 1,4,5,8-12

1

Enter port numbers and/or port ranges separated by commas. Eg.(1,2,5-7):

5-7

OK Cancel

【Ether slot numberv】

パラメータを変更するスロットを選択します。

注意 接続されているスロット番号が表示されます。

【Enter port numbers and/or port ranges separated by commas.】

選択したスロットのポート範囲を入力してください。

上記項目を選択後、「OK」をクリックします。以下の画面が表示されます。

Setup (slot : 1) - Microsoft Internet Explorer

Port(s): 1,2

A blank value is displayed for fields where the selected port configurations differ. When submitted, fields that are left blank result in no change to the port configuration.

Media Type: 10Base-T / 100Base-TX

Current Port Mode: Link Down Current Flow Control: Disabled

Port State: Enabled Label: [text box]

Port Mode: Auto-Neg Advised Capabilities: 10M HD, 10M FD, 100M HD, 100M FD Help

Flow Control: Disabled Help

OK Cancel

【Media Type】

選択したポートの通信速度の情報が表示されます。

【Current Port Mode】

現在のLinkUP状況が表示されます。

【Current Flow Control】

現在のフローコントロールの有効/無効状況が表示されます。

【Port State】

選択したポートの有効/無効を設定します。

- ・ Enabled : 有効
- ・ Disabled : 無効

【Port Mode】

転送速度および転送モードを設定します。

- ・ Auto-Neg : autoNegotiation
- ・ 10M H-D : 10BASE-T 半二重
- ・ 10M F-D : 10BASE-T 全二重
- ・ 100M H-D : 100BASE-TX 半二重
- ・ 100M F-D : 100BASE-TX 全二重
- ・ 1000M F-D : 1000BASE-T 全二重

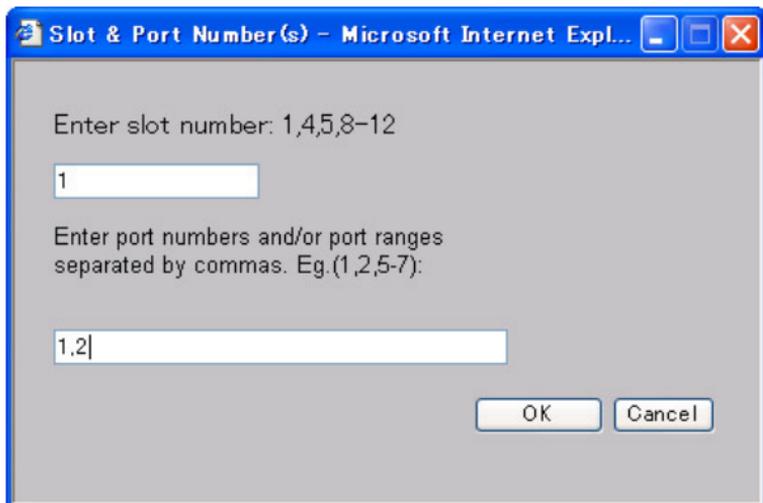
【Flow Control】

フロー制御を設定します。

- ・ Enabled : 有効
- ・ Disabled : 無効

32 Statistics(Ethernet)

[Physical Interface] [Ethernet] [Statistics]をクリックすると、以下の画面が表示されます。各ポートのInterface GroupおよびEthernetMIBに関する統計情報が表示されます。表示される情報は、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。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。



【Ether slot number】

パラメータを参照するスロットを選択します。

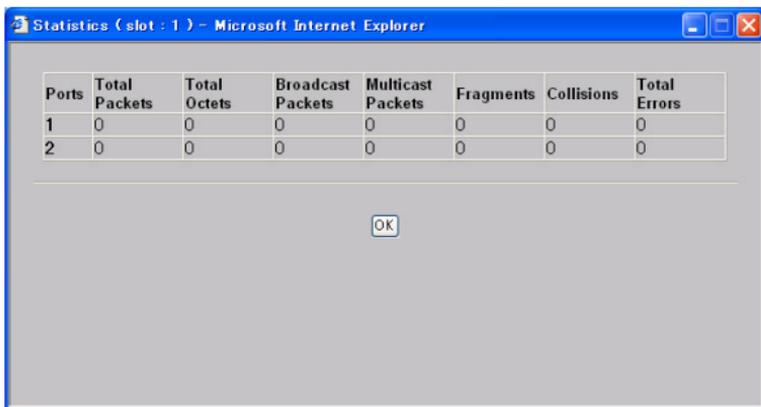
* 接続されているスロット番号が表示されます。

【Enter port numbers and/or port ranges separated by commas.】

選択したスロットのポート範囲を入力してください。

上記項目を選択後、「OK」をクリックします。

複数のポートを指定した時は、以下の画面が表示されます。



Ports	Total Packets	Total Octets	Broadcast Packets	Multicast Packets	Fragments	Collisions	Total Errors
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0

OK

【Total Packets】

高位層プロトコルに渡された非ユニキャスト(サブネットワーク - ブロードキャストまたはサブネットワーク - マルチキャスト)およびサブネットワーク - ユニキャストパケットの総パケット数です。

【Total 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。

【Broadcast Packets】

高位層プロトコルに渡された、ブロードキャストパケットの総パケット数です。

【Multicast Packets】

高位層プロトコルに渡された、マルチキャストキャストパケットの総パケット数です。

【Fragments】

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。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

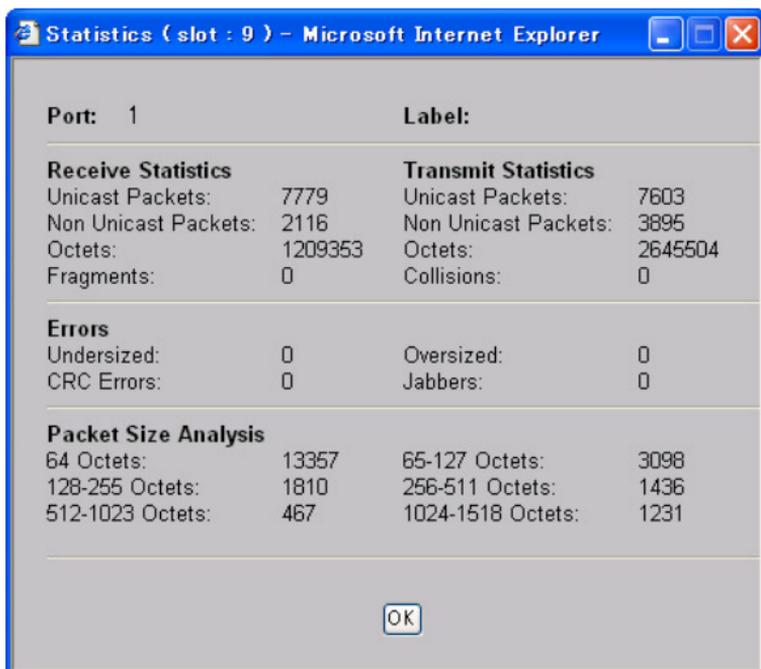
【Collisions】

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。

【Total Errors】

Undersized、Oversized、CRC Errorsの総エラー数です。

1ポートのみを選択した時は、以下の画面が表示されます。



Port: 1	Label:		
Receive Statistics		Transmit Statistics	
Unicast Packets:	7779	Unicast Packets:	7603
Non Unicast Packets:	2116	Non Unicast Packets:	3895
Octets:	1209353	Octets:	2645504
Fragments:	0	Collisions:	0
Errors		Errors	
Undersized:	0	Oversized:	0
CRC Errors:	0	Jabbers:	0
Packet Size Analysis			
64 Octets:	13357	65-127 Octets:	3098
128-255 Octets:	1810	256-511 Octets:	1436
512-1023 Octets:	467	1024-1518 Octets:	1231

OK

【Port Number】

ポート番号を選びます。

Receive Statistics

【Unicast Pkts】

高位層プロトコルに渡されたサブネットワーク - ユニキャストパケット数です。

【Non-Unicast Pkts】

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

【Octets】

インターフェースで受信されたオクテットの合計です。値はフレーミングキャラクタも含まれます。

【Fragments】

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。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。

Transmit Statistics

【Unicast Pkts】

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。

【Non-Unicast Pkts】

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

【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。

【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。

Errors

【Undersized】

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。

【Oversized】

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。

【CRC 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。

【Jabbers】

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。

Packet Size Analysis

【64 Octets】

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せん。

【65-127 Octets】

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せん。

【128-255 Octets】

(同上)

【256-511 Octets】

(同上)

【512-1023 Octets】

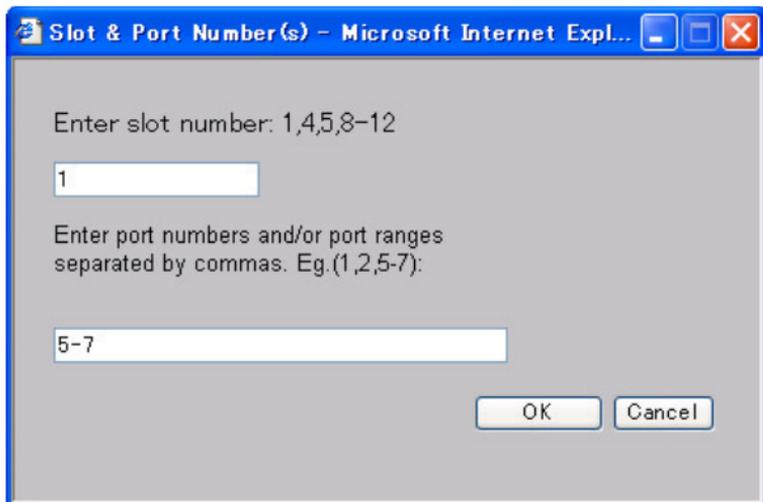
(同上)

【1024-1518 Octets】

(同上)

33 Summary(Ethernet)

[Physical Interface] [Ethernet] [Summary]をクリックすると、以下の画面が表示されます。各スロット内の全ポートの通信パラメータを表示します。



【Enter slot numbers and/or slot ranges separated by commas.】

パラメータを参照するスロットを選択します。

* 接続されているスロット番号が表示されます。

上記項目を選択後、「OK」をクリックします。複数のポートを指定した時は以下の画面が表示されます。



Slot	Port	Port State	Port Mode	Flow Control	Auto-Negotiation	Security	MAC address
1	1	Enabled	Link Down	Disabled	Enabled	No Security	
1	2	Enabled	Link Down	Disabled	Enabled	No Security	
1	3	Enabled	Link Down	Disabled	Enabled	No Security	
1	4	Enabled	Link Down	Disabled	Enabled	No Security	
1	5	Enabled	Link Down	Disabled	Enabled	No Security	
1	6	Enabled	Link Down	Disabled	Enabled	No Security	
1	7	Enabled	Link Down	Disabled	Enabled	No Security	
1	8	Enabled	Link Down	Disabled	Enabled	No Security	
4	1	Enabled	Link Down	Disabled	Enabled	No Security	
4	2	Enabled	Link Down	Disabled	Enabled	No Security	
4	3	Enabled	Link Down	Disabled	Enabled	No Security	
4	4	Enabled	Link Down	Disabled	Enabled	No Security	
4	5	Enabled	Link Down	Disabled	Enabled	No Security	
4	6	Enabled	Link Down	Disabled	Enabled	No Security	
4	7	Enabled	Link Down	Disabled	Enabled	No Security	
4	8	Enabled	Link Down	Disabled	Enabled	No Security	

【Slot】

スロット番号を表示します。

【Port】

ポート番号を表示します。

【Port State】

ポートの有効/無効を表示します。

- ・ Enabled : 有効
- ・ Disabled : 無効

【Port Mode】

ポートのLink状況を表示します。

- ・ Link Down : Link無し
- ・ 10M H-D : 10BASE-T 半二重で接続
- ・ 10M F-D : 10BASE-T 全二重で接続
- ・ 100M H-D : 100BASE-TX 半二重で接続
- ・ 100M F-D : 100BASE-TX 全二重で接続
- ・ 1000M F-D : 1000BASE-T 全二重で接続

【Flow Control】

フロー制御の有効/無効を表示します。

- ・ Enabled : 有効
- ・ Disabled : 無効

【Auto-Negotiation】

オートネゴシエーションの有効/無効を表示します。

- ・ Enabled : 有効
- ・ Disabled : 無効

【Security】

セキュリティ方法を表示します。

- ・ No Security : ポート・セキュリティを無効
- ・ Continuous Learning : アドレスを連続的に学習
- ・ Automatic Learning : 指定したアドレス数を学習

【MAC address】

本製品で参照できるノードのMACアドレスです。

34 Aging(ARP)

[Protocol] [IP] [ARP] [Aging]をクリックすると、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。



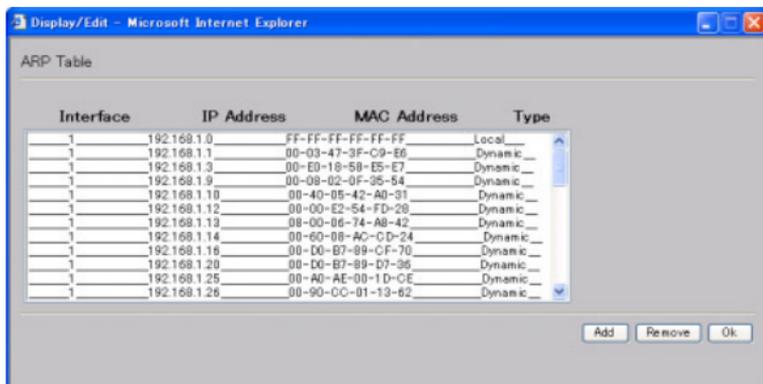
【ARP Aging Time】

ARP情報のエージアウトするタイムアウト値を設定します。

- ・ 0 ~ 1440 : 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

35 Display/Edit(ARP)

[Protocol] [IP] [ARP] [Display/Edit]をクリックすると、以下の画面が表示されます。ARP(Address Resolution Protocol)は、ホストのインターネットアドレスからイーサネットアドレスを割り当てる方法を定義します。ARPにより検出されたIP <-> MACアドレスのキャッシュ情報が表示されます。



Interface	IP Address	MAC Address	Type
1	192.168.1.0	FF-FF-FF-FF-FF-FF	Local
1	192.168.1.1	00-03-47-3F-C9-E6	Dynamic
1	192.168.1.3	00-E0-18-58-E5-E7	Dynamic
1	192.168.1.9	00-08-02-0F-35-54	Dynamic
1	192.168.1.10	00-40-05-42-A0-31	Dynamic
1	192.168.1.12	00-00-E2-54-FD-28	Dynamic
1	192.168.1.13	08-00-06-74-A8-42	Dynamic
1	192.168.1.14	00-60-08-AC-0D-24	Dynamic
1	192.168.1.16	00-D0-B7-89-CF-70	Dynamic
1	192.168.1.20	00-D0-B7-89-D7-36	Dynamic
1	192.168.1.25	00-A0-AE-00-1D-CE	Dynamic
1	192.168.1.26	00-90-CC-01-13-62	Dynamic

【Interface】

ホストに割り当てられているVLANグループが表示されます。

【IP Address】

IPアドレスが表示されます。

【MAC Address】

IPアドレスに対応しているMACアドレスが表示されます。

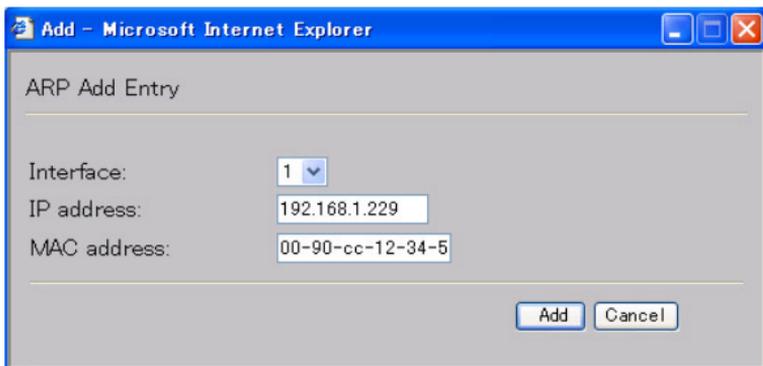
【Type】

ホスト機器と接続しているポートが表示されます。

- ・ Dynamic : 動的に学習したARP
- ・ Local : 本製品に割り当てられているARP
- ・ Static : 手動で設定したARP

手動でARP情報を追加する

「Display/Edit」の画面内の「Add」をクリックすると、以下の画面が表示されます。手動でARPを追加することができます。



ARP Add Entry

Interface: 1

IP address: 192.168.1.229

MAC address: 00-90-cc-12-34-5

Add Cancel

【Interface】

ホストに割り当てるVLANグループを設定します。

【IP address】

IPアドレスを設定します。

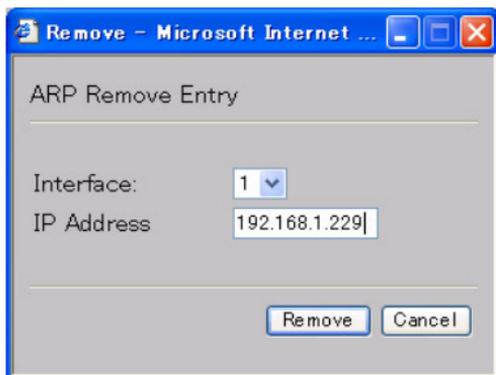
【MAC address】

IPアドレスに対応しているMACアドレスを設定します。

上記の項目を設定したら「Add」をクリックします。「Display/Edit」の画面内の「Type」に「Static」で登録します。

手動または動的に学習したARP情報の削除

「Display/Edit」の画面内の「Remove」をクリックすると、以下の画面が表示されます。手動または動的に学習したARPを削除することができます。



【Interface】

ホストに割り当てられているVLANグループを設定します。

【IP address】

IPアドレスを設定します。

上記の項目を設定したら「Remove」をクリックします。

36 Flush(ARP)

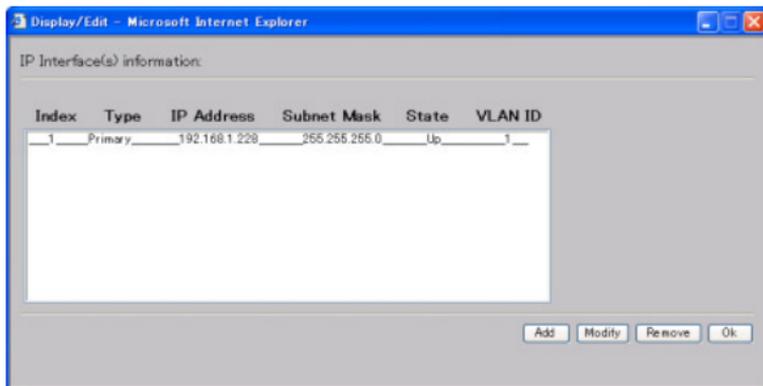
[Protocol] [IP] [ARP] [Flush]をクリックすると、以下の画面が表示されます。動的に学習したARP情報をすべて削除します。



「This operation will remove all dynamic entries from the ARP table Do you wish to continue?」と表示されるので、「OK」をクリックします。

37 Display/Edit(INTERFACE)

[Protocol] [IP] [INTERFACE] [Display/Edit]をクリックすると、以下の画面が表示されます。割り当てたVLANグループのIPアドレス、タイプ、ステータスの追加、変更、参照ができます。



【Type】

作成したVLANグループのタイプを表示します。

- ・ Primary : 作成したVLANグループの主体となるグループ
- ・ Secondary : 作成したVLANグループのセカンドグループ

【IP Address】

作成したVLANグループのIPインターフェースのアドレスが表示されます。

【Subnet Mask】

サブネットマスクが表示されます。

【State】

VLANグループの状況が表示されます。

- ・ Up : VLANグループにノードが接続されている
- ・ Down : 未接続

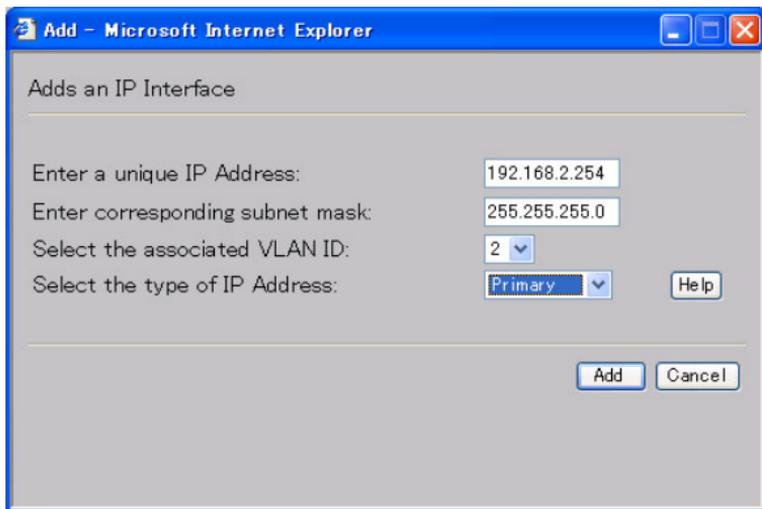
【VLAN ID】

作成したVLANグループのVLAN IDが表示されます。

IPインターフェースの追加

「Display/Edit」の画面内の「Add」をクリックすると、以下の画面が表示されます。

IPインターフェースを追加できます。



The screenshot shows a web browser window titled "Add - Microsoft Internet Explorer". The main content area displays a form titled "Adds an IP Interface". The form contains the following fields and controls:

- Enter a unique IP Address:
- Enter corresponding subnet mask:
- Select the associated VLAN ID:
- Select the type of IP Address:
- Buttons: "Add", "Cancel", and "Help"

【Enter a unique IP Address】

追加するIPアドレスを設定します。Enter corresponding subnet

【mask】

IPアドレスに対応しているサブネットマスクを設定します。

【Select the associated VLAN ID】

IPアドレスを設定するVLAN IDを指定します。

【Select the type of IP Address】

作成したVLANグループのタイプを設定します。

- ・ Primary : 作成したVLANグループの主体となるグループ
- ・ Secondary : 作成したVLANグループのセカンドグループ

上記の項目を設定したら「Add」をクリックします。

IPインターフェースの変更

「Display/Edit」の画面内の変更をしたいグループを選択し、「Modify」をクリックすると、以下の画面が表示されます。IPインターフェースの変更ができます。

Modify any of the parameters for Interface 2

Enter a unique IP Address: 192.168.2.254

Enter corresponding subnet mask: 255.255.255.0

Select the associated VLAN ID: 2

Select the type of IP Address: Primary Help

Modify Cancel

【Enter a unique IP Address】

変更するIPアドレスを設定します。

【Enter corresponding subnet mask】

IPアドレスに対応しているサブネットマスクを設定します。設定が反映されます。

【Select the associated VLAN ID】

変更するVLAN IDを指定します。

【Select the type of IP Address】

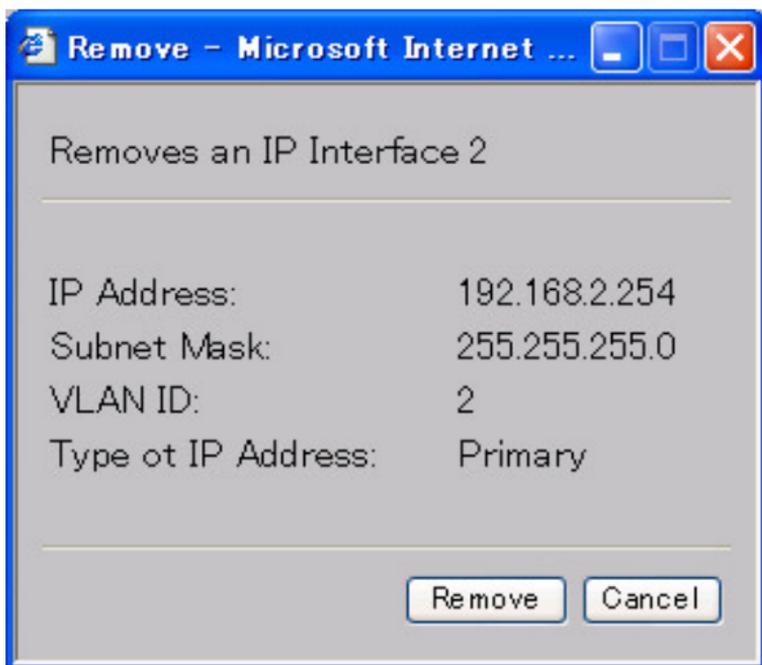
変更したVLANグループのタイプを設定します。

- ・ Primary : 作成したVLANグループの主体となるグループ
- ・ Secondary : 作成したVLANグループのセカンドグループ

上記の項目を設定したら「Modify」をクリックします。設定が反映されます。

IPインターフェースの削除

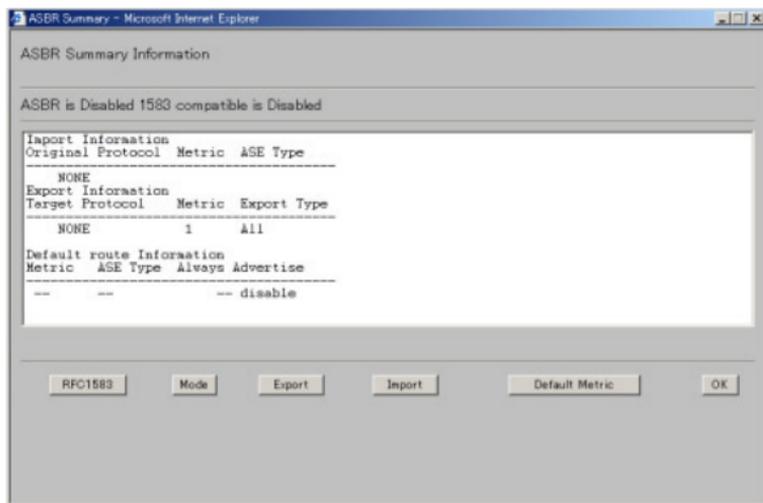
「Display/Edit」の画面内の削除をしたいグループを選択し、「Remove」をクリックすると、以下の画面が表示されます。IPインターフェースの削除ができます。



「Remove」をクリックします。

38 ASBR Summary(OSPF)

[Protocol] [IP] [OSPF] [ASBR Summary]をクリックすると、以下の画面が表示されます。本製品が他のルーティングプロトコルとの境界ルータとして機能するときの詳細を設定します。



【ASBR is Enabled 1583 compatible is Enabled】

現在、設定および指定してあるASBRの状態が表示されます。

RFC1583

本製品でOSPF-V2との境界を行うとき、設定します

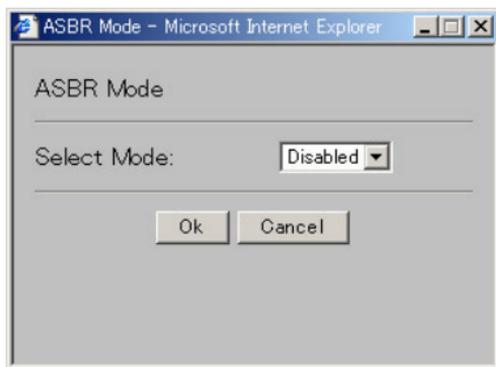


【Select Mode】

- Enabled : 有効
- Disabled : 無効

Mode

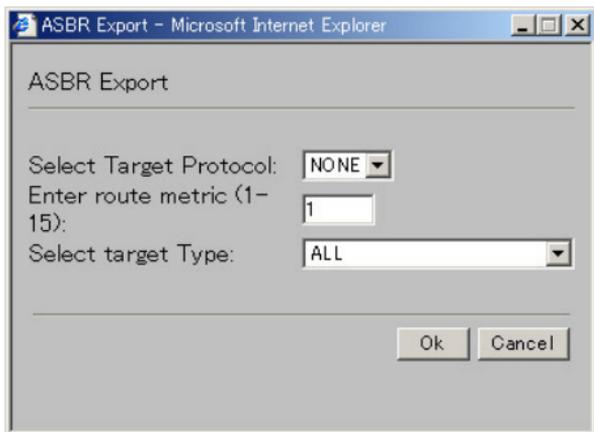
本製品が境界ルータとして機能するときの詳細を設定します。



- Enabled : 有効
- Disabled : 無効

Export

境界ルータとして、ブリッジ相手へ送信する際の設定をします。



【Select Target Protocol】

ブリッジ相手のルーティングプロトコルを設定します。

- ・ NONE : ルーティングプロトコルを使用しない。
- ・ RIP : RIPのみを使用します。
- ・ ALL : すべてのルーティングプロトコルタイプを対応します。

【Enter route metric (1-15)】

ルータへの到達メトリックを指定します。

- ・ 1-15 : 設定可能範囲

【Select target Type】

ブリッジ相手のタイプを設定します。

- ・ ALL : すべてのタイプを有効にします。
- ・ INTERNAL : 内部で設定したのと同じ物を使用します。
- ・ EXTERNAT(type1/type2) : タイプ1とタイプ2を使用します。
- ・ TYPE1 : タイプ1のみ使用します。

Import

境界ルータとして、ブリッジ相手から受信する際の設定をします。

ASBR Import

Select Origin Protocol: NONE

Enter RIP route metric (1-65535): 20

Select RIP ASE Type: Type 2

Enter static route metric (1-65535): 20

Select static ASE Type: Type 2

Ok Cancel

【Select Origin Protocol】

ブリッジ相手のルーティングプロトコルを設定します。

- ・ NONE : ルーティングプロトコルを使用しない。
- ・ Static : 手動で設定したルーティング情報のみ使用します。
- ・ RIP : RIPのみ使用します。
- ・ ALL : すべてのルーティングプロトコルタイプを対応します。

【Enter RIP route metric (1-65535)】

RIP使用時のルータへの到達メトリックを指定します。

- ・ 1-65535 : 設定可能範囲

【Select RIP ASE Type】

RIP使用時のブリッジ相手のタイプを設定します。

- ・ Type1 : タイプ1のみ使用します。
- ・ Type2 : タイプ2のみ使用します。

【Enter static route metric (1-65535)】

手動設定したルーティング情報のルータへの到達メトリックを指定します。

- ・ 1-65535 : 設定可能範囲

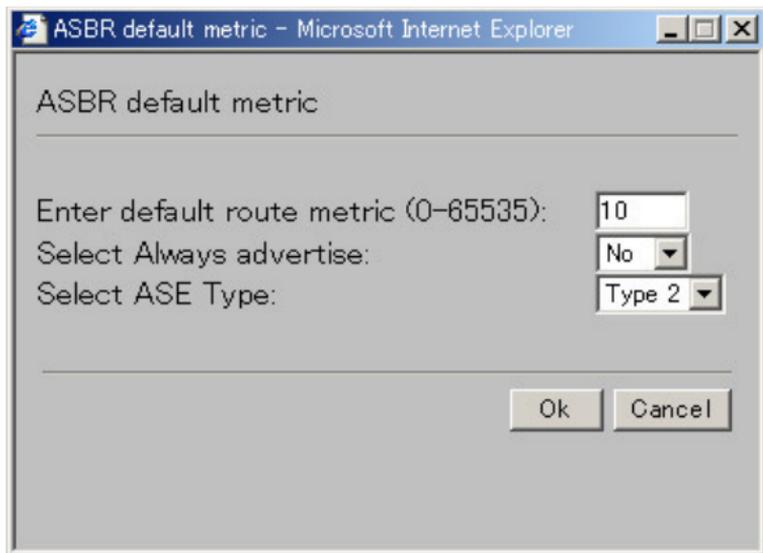
【Select static ASE Type】

手動設定したルーティング情報使用時のブリッジ相手のタイプを設定します。

- ・ Type1 : タイプ1のみ使用します。
- ・ Type2 : タイプ2のみ使用します。

Default Metric

デフォルトメトリックの設定をします。



【Enter default route metric (0-65535)】

デフォルトメトリックの到達メトリックを指定します。

- ・ 1-65535 : 設定可能範囲

【Select Always advertise】

常にデフォルトメトリックを配布し続けるか設定します。

- ・ Yes : 配布し続けます。
- ・ No : 要求があったときのみ配布します。

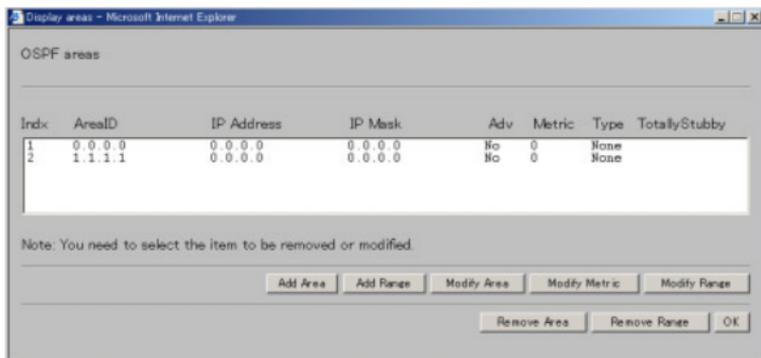
【Select ASE Type】

ASEのタイプを設定します。

- ・ Type1 : タイプ1のみ使用します。
- ・ Type2 : タイプ2のみ使用します。

39 Display areas(OSPF)

[Protocol] [IP] [OSPF] [Display areas]をクリックすると、以下の画面が表示されます。作成されているエリアの状況およびエリアを作成します。



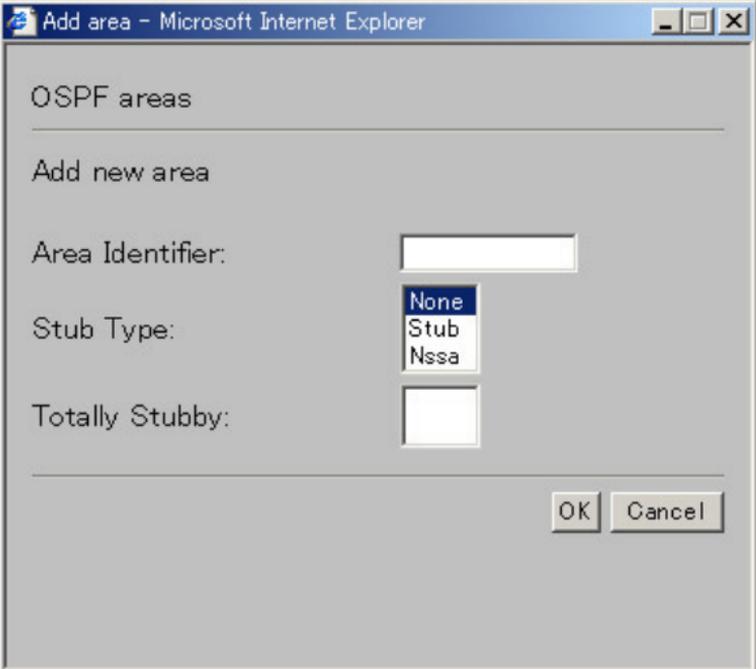
【OSPF areas】

現在、作成されているエリアを表示します。

- ・ Indx : 作成したエリアの数を表示します。
- ・ AreaID : エリアIDを表示します。
- ・ IP Address : 集約するとき使用するIPアドレスを表示します。
- ・ IP Mask : 集約するとき使用するサブネットマスクを表示します。
- ・ Adv : 集約情報を広告するか表示します。
- ・ Metric : 到達メトリックを表示します。
- ・ Type : スタブエリアのタイプを表示します。
- ・ TotallyStubby : 指定エリアに存在するスタブルータの総数を表示します。

Add Area

新たにエリアを作成します。



OSPF areas

Add new area

Area Identifier:

Stub Type:

Totally Stubby:

OK Cancel

【Area Identifier】

エリア番号を入力します。

バックボーンエリア(0.0.0.0)は初期状態で設定されています。

【Stub Type】

スタブエリアにするか設定します。

- ・ None : スタブエリアに設定しないときに設定します。
- ・ Stub : スタブエリアに設定する場合に選択します。
- ・ Nssa : 準スタブエリアに設定する場合に選択します。

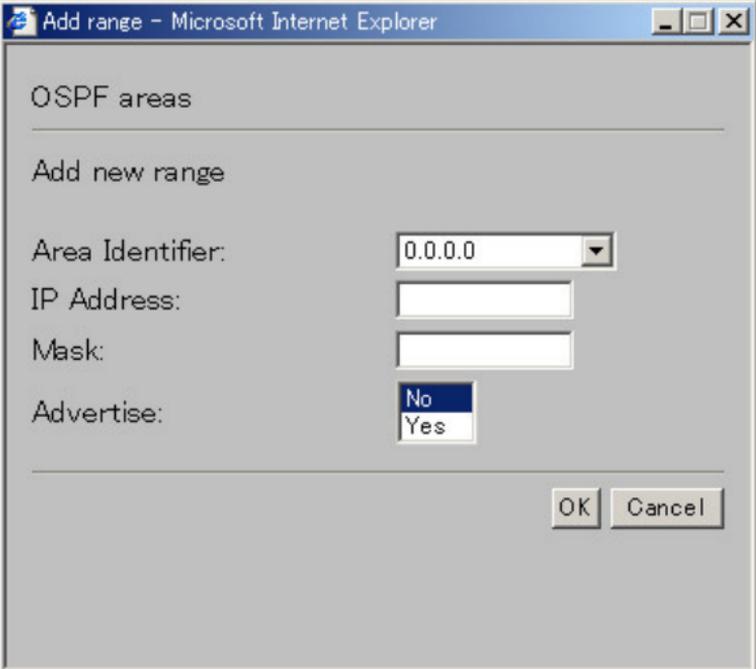
【Totally Stubby】

スタブエリアに設定したことを広告するか設定します。

- ・ Yes : 広告します。
- ・ No : 広告しません。

Add Range

新たにエリア情報を集約を作成します。



OSPF areas

Add new range

Area Identifier: 0.0.0.0

IP Address:

Mask:

Advertise: No

Yes

OK Cancel

【Area Identifier】

エリア情報を集約するエリアを指定します。

- ・ 選択肢 : 現在作成されているエリアを表示します。

【IP Address】

集約したエリア情報を送るIPアドレスを設定します。

【Mask】

集約したエリア情報を送るIPアドレスのサブネットマスクを設定します。

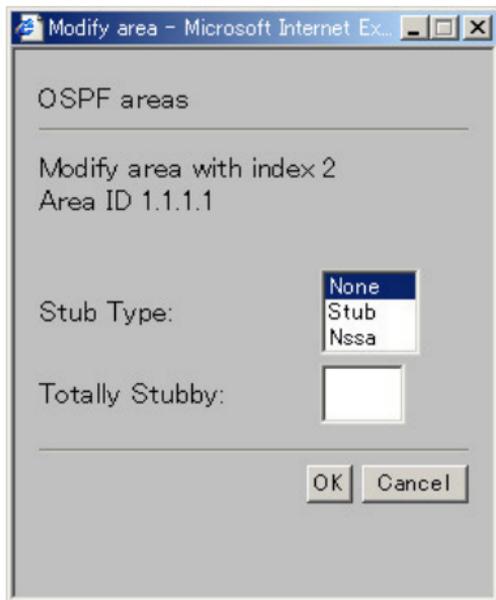
【Advertise】

集約したエリア情報を広告するか設定します。

- ・ Yes : 広告します。
- ・ No : 広告しません。

Modify Area

作成されているエリアの編集をします。「OSPF areas」で編集したいエリアを指定して「Modify Area」をクリックします。



【Stub Type】

スタブエリアの設定をします。

- ・ None : スタブエリアに設定しないときに設定します。
- ・ Stub : スタブエリアに設定する場合に選択します。
- ・ Nssa : 準スタブエリアに設定する場合に選択します。

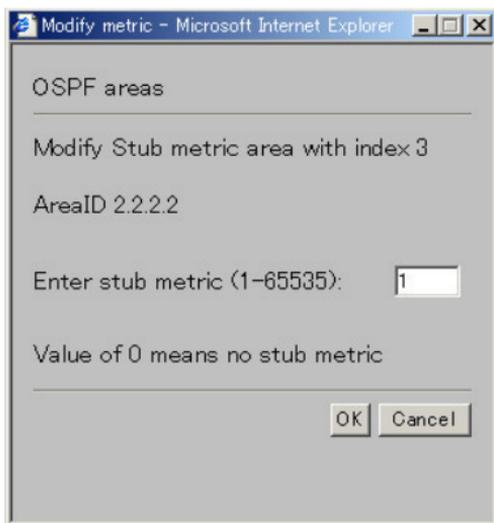
【Totally Stubby】

スタブエリアに設定したことを広告するか設定します。

- ・ Yes : 広告します。
- ・ No : 広告しません。

Modify Metric

スタブエリアに設定した際の到達メトリック範囲を設定します。
「OSPF areas」で設定したいエリアを指定して「Modify Metric」をクリックします。

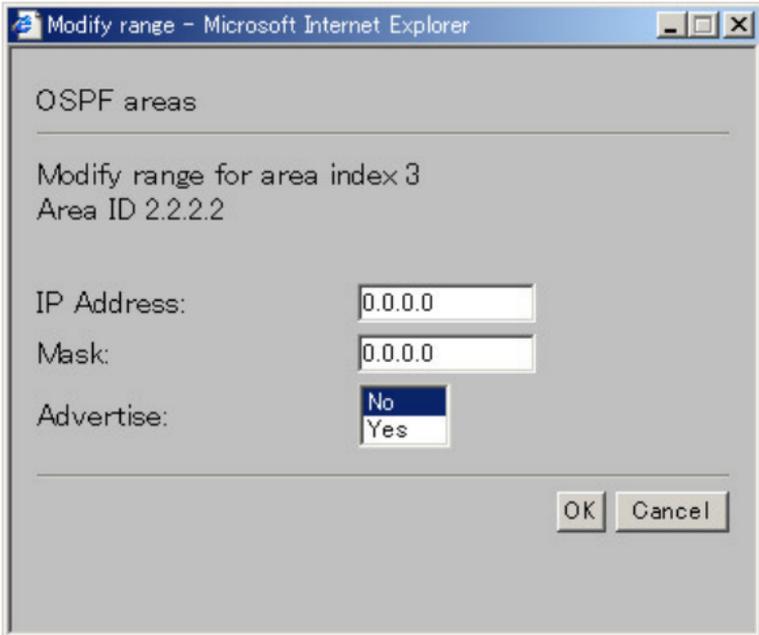


【Enter stub metric (1-65535)】

- ・ 1-65535 : 設定可能範囲

Modify Range

エリア情報を集約する設定を編集します。「OSPF areas」で編集したいエリアを指定して「Modify Range」をクリックします。



Modify range - Microsoft Internet Explorer

OSPF areas

Modify range for area index 3
Area ID 2.2.2.2

IP Address:

Mask:

Advertise:

【IP Address】

集約したエリア情報を送るIPアドレスを設定します。

【Mask】

集約したエリア情報を送るIPアドレスのサブネットマスクを設定します。

【Advertise】

集約したエリア情報を広告するか設定します。

- ・ Yes : 広告します。
- ・ No : 広告しません。

Remove Area

作成したエリアを削除します。



【Area Identifier】

削除したいエリアを選択します。削除するエリアを指定後、「OK」をクリックします。

Remove Range

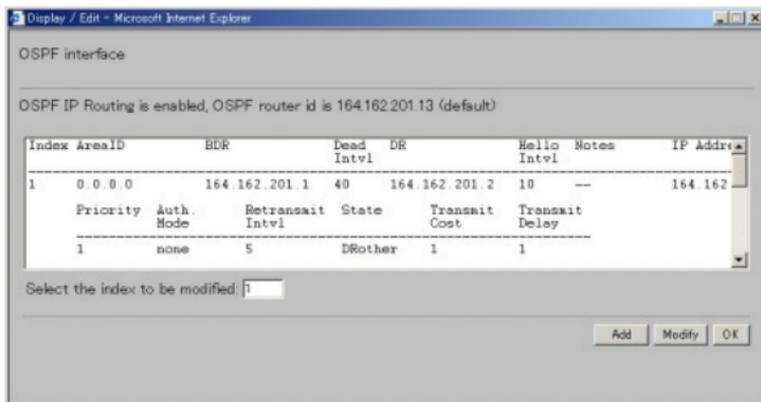
作成したエリア集約情報設定を削除します。「OSPF areas」で削除したいエリア集約情報設定を指定して「Remove Range」をクリックします。

以下の画面が表示されるので、「OK」をクリックします。



40 Interface(OSPF)

[Protocol] [IP] [OSPF] [Interface]をクリックすると、以下の画面が表示されます。各インタフェースのOSPF使用状況や追加・編集などの設定をします。



【OSPF IP Routing is enabled, OSPF router id is xxx.xxx.xxx.xxx (default)】

現在選択されているルータIDの設定方法とルータIDを表示します。

【表】

現在作成されているインターフェイスの設定内容を表示します。

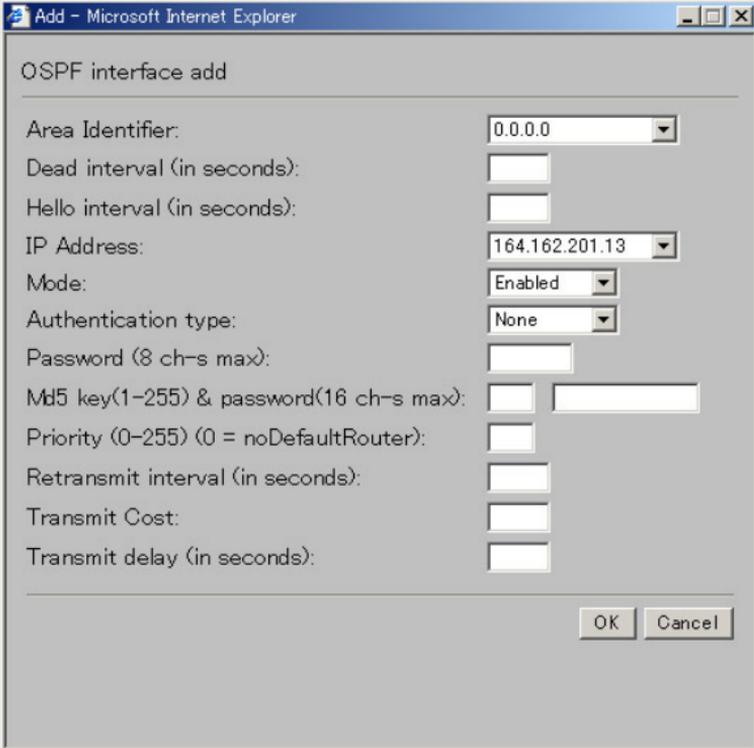
【Select the index to be modified】

OSPFインデックスを指定します。

Add

インターフェイスへOSPFインデックスの設定を作成します。

OSPFインデックス設定をする前にインターフェイスを作成してください。



OSPF interface add

Area Identifier:	0.0.0.0
Dead interval (in seconds):	<input type="text"/>
Hello interval (in seconds):	<input type="text"/>
IP Address:	164.162.201.13
Mode:	Enabled
Authentication type:	None
Password (8 ch-s max):	<input type="text"/>
Md5 key(1-255) & password(16 ch-s max):	<input type="text"/> <input type="text"/>
Priority (0-255) (0 = noDefaultRouter):	<input type="text"/>
Retransmit interval (in seconds):	<input type="text"/>
Transmit Cost:	<input type="text"/>
Transmit delay (in seconds):	<input type="text"/>

OK Cancel

【Area Identifier】

設定するエリアIDを指定します。

- ・ 指定項目 : 現在作成されているエリアIDが表示されます。

【Dead interval(in seconds)】

ルータ間の情報のやり取りの最中に、隣接するルータから返答が無くなったときの待機する時間を設定します。単位は秒です。

【Hello interval (in seconds)】

ルータ間の情報をやり取りする時間を設定します。単位は秒です。

【IP Address】

OSPFインデックスを設定するIPアドレスを設定します。

- ・ 指定項目 : 現在作成されているインターフェイスIPアドレスが表示されます。

【Mode】

OSPFの有効/無効を設定します。

- ・ Enabled : 有効
- ・ Disabled : 無効

【Authentication type】

認証タイプを設定します。認証タイプは、ルーティング情報が正当なサイトから送信されたものであることを保証します。

- ・ None : 認証を使わない
- ・ Password : パスワードを使用
- ・ Md5 : MD5パスワードを使用。

【Password(8 ch-s max)】

認証パスワードを設定します。パスワードは最小1文字～最大8文字の半角英数字で設定します。大文字・小文字を区別します。

【Md5 key(1-255)& password(16 ch-s max)】

暗号化認証パスワードを設定します。キーは最小1文字～最大255文字の半角英数字で設定します。パスワードは最小1文字～最大16文字の半角英数字で設定します。大文字・小文字を区別します。

【Priority(0-255)(0 = noDefaultRouter)】

OSPFインデックスのプライオリティ(優先度)を設定します。プライオリティ(優先度)によって代表ルータが決定されます。代表ルータに立候補しないときは「0」を設定します。

【Retransmit interval(in seconds)】

LSAを再送信する時間を設定します。単位は秒です。

【Transmit Cost】

送信コストを設定します。

【Transmit delay(in seconds)】

LSAの遅延時間を設定します。単位は秒です。

Modify

OSPFインデックスの編集をします。「Select the index to be modified」で編集したいOSPFインデックスを指定して「Modify」をクリックします。

OSPF interface modify

Modifying interface 1

Area Identifier:	0.0.0.0
Dead interval (in seconds):	40
Hello interval (in seconds):	10
IP Address:	164.162.201.13
Mode:	Enabled
Authentication type:	None
Password (8 ch-s max):	
Md5 key(1-255) & password(16 ch-s max):	
Priority (0-255) (0 = noDefaultRouter):	1
Retransmit interval (in seconds):	5
Transmit Cost:	1
Transmit delay (in seconds):	1

OK Cancel

【Area Identifier】

変更するエリアIDを指定します。

- ・ 指定項目 : 現在作成されているエリアIDが表示されます。

【Dead interval(in seconds)】

ルータ間の情報のやり取りの最中に、隣接するルータから返答が無くなったときの待機する時間を変更します。単位は秒です。

【Hello interval(in seconds)】

ルータ間の情報をやり取りする時間を変更します。単位は秒です。

【IP Address】

OSPFインデックスのIPアドレスを変更します。

- ・ 指定項目 : 現在作成されているインターフェイスIPアドレスが表示されます。

【Mode】

OSPFの有効/無効を変更します。

- ・ Enabled : 有効
- ・ Disabled : 無効

【Authentication type】

認証タイプを変更します。認証タイプは、ルーティング情報が正当なサイトから送信されたものであることを保証します。

- ・ None : 認証を使わない
- ・ Password : パスワードを使用
- ・ Md5 : MD5パスワードを使用。

【Password (8 ch-s max)】

認証パスワードを変更します。パスワードは最小1文字～最大8文字の半角英数字で設定します。大文字・小文字を区別します。

【Md5 key(1-255)& password(16 ch-s max)】

暗号化認証パスワードを変更します。キーは最小1文字～最大255文字の半角英数字で設定します。パスワードは最小1文字～最大16文字の半角英数字で設定します。大文字・小文字を区別します。

【Priority(0-255)(0 = noDefaultRouter)】

OSPFインデックスのプライオリティ(優先度)を変更します。プライオリティ(優先度)によって代表ルータが決定されます。代表ルータに立候補しないときは「0」を設定します。

【Retransmit interval (in seconds)】

LSAを再送信する時間を変更します。単位は秒です。

【Transmit Cost】

送信コストを変更します。

【Transmit delay (in seconds)】

LSAの遅延時間を変更します。単位は秒です。

41 LSAs Database Summary(OSPF)

[Protocol] [IP] [OSPF] [LSAs Database Summary]をクリックすると、以下の画面が表示されます。Link State Databaseの状態を確認できます。



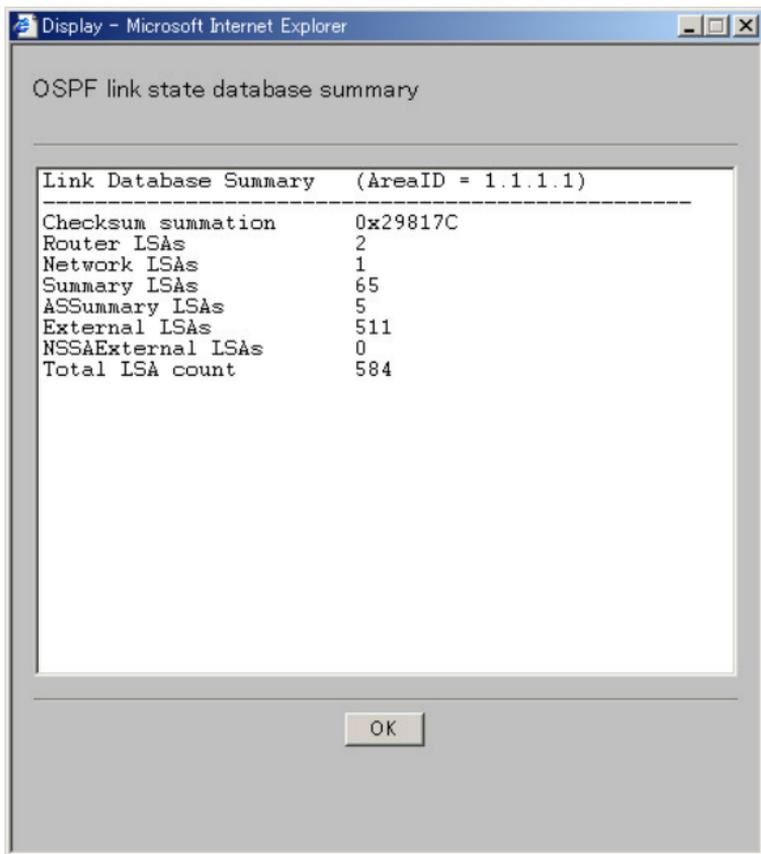
【All AreaID】

全エリアの状態を確認するときはチェックを入れます。

【AreaID】

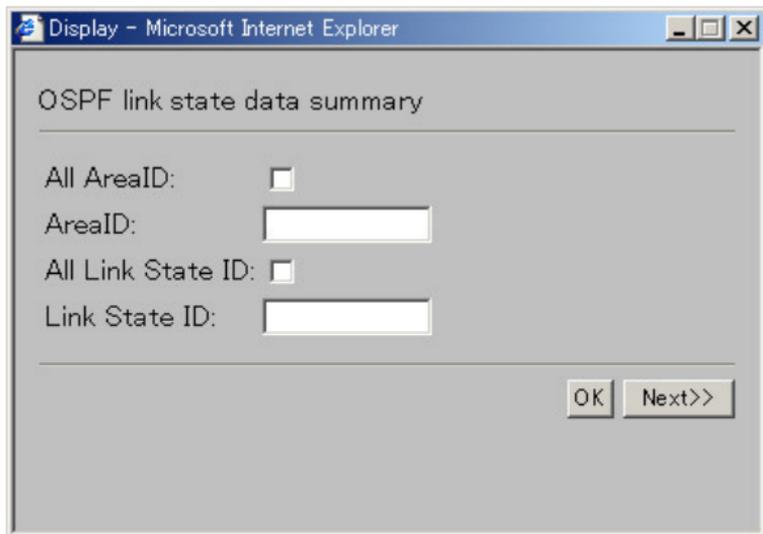
確認したいエリアIDを指定します。

上記のどちらかを指定後「Next >>」をクリックすると、以下の画面が表示されます。



42 LSAs Summary(OSPF)

[Protocol] [IP] [OSPF] [LSAs Summary]をクリックすると、以下の画面が表示されます。Link State Databaseの状態を確認できます。



【All AreaID】

全エリアの状態を確認するときはチェックを入れます。

【AreaID】

確認したいエリアIDを指定します。

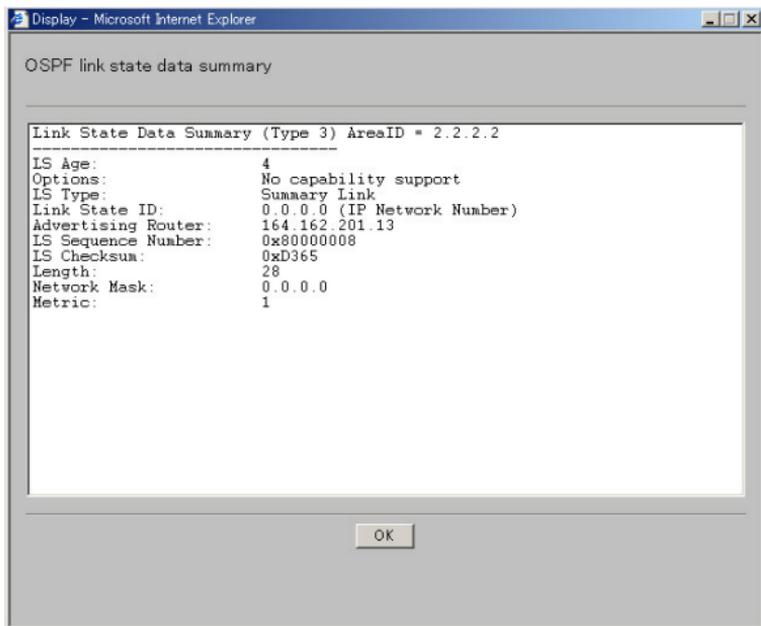
【All Link State ID】

全リンクステータスの状態を確認するときはチェックを入れます。

【Link State ID】

確認したいリンクステータスのIDを指定します。

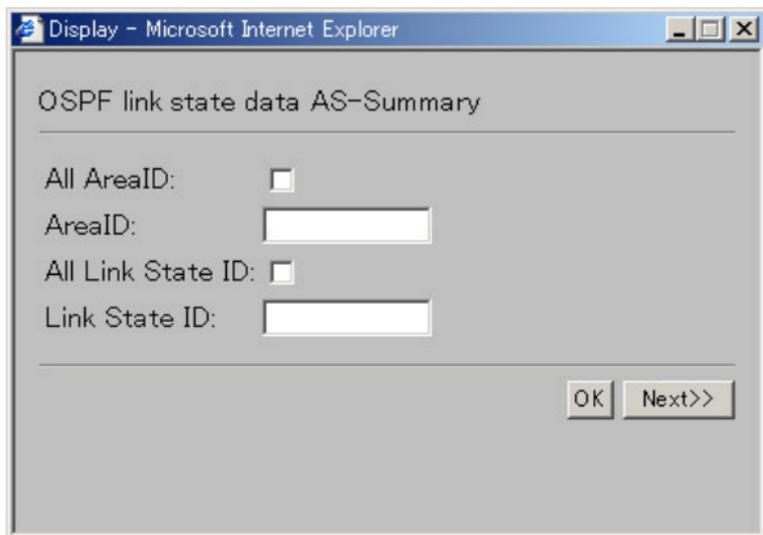
上記の項目を指定後「Next >>」をクリックすると、以下の画面が表示されます。



LSAが一つも正常に取得ができない時は「Could not get summary link data - no records found」と表示されます。

43 LSAs AsSummary(OSPF)

[Protocol] [IP] [OSPF] [LSAs AsSummary]をクリックすると、以下の画面が表示されます。AsSummaryの状態を確認できます。



【All AreaID】

全エリアの状態を確認するときはチェックを入れます。

【AreaID】

確認したいエリアIDを指定します。

【All Link State ID】

全リンクステータスの状態を確認するときはチェックを入れます。

【Link State ID】

確認したいリンクステータスのIDを指定します。

上記の項目を指定後「Next > >」をクリックすると、AsSummaryの
情報画面が表示されます。

LSAが一つも正常に取得ができない時は「Could not get as summary link data - no records found」と表示されます。

44 LSAs router(OSPF)

[Protocol] [IP] [OSPF] [LSAs router]をクリックすると、以下の画面が表示されます。router LSAの状態を確認できます。

OSPF link state data router

All AreaID:

AreaID:

All Link State ID:

Link State ID:

OK Next>>

【All AreaID】

全エリアの状態を確認するときはチェックを入れます。

【AreaID】

確認したいエリアIDを指定します。

【All Link State ID】

全リンクステータスの状態を確認するときはチェックを入れます。

【Link State ID】

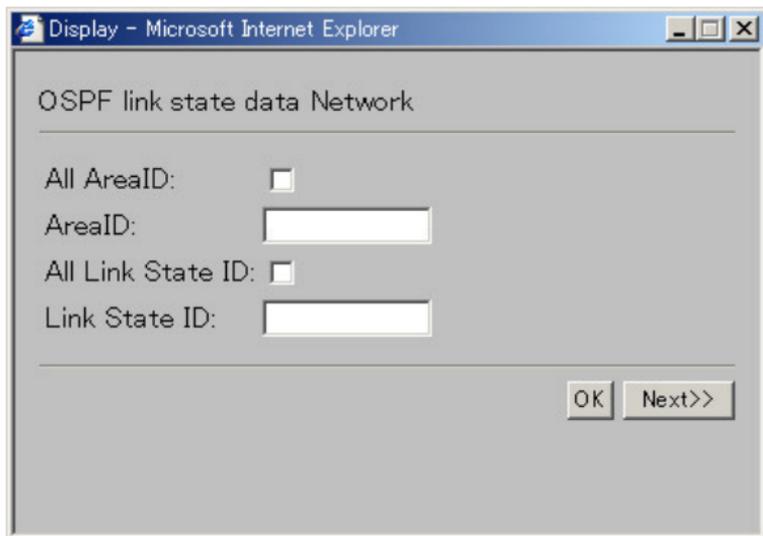
確認したいリンクステータスのIDを指定します。

上記の項目を指定後「Next > > 」をクリックすると、ルータLSAの情報画面が表示されます。

LSAが一つも正常に取得ができない時は「Could not get router link data - no records found」と表示されます。

45 LSAs network(OSPF)

[Protocol] [IP] [OSPF] [LSAs network]をクリックすると、以下の画面が表示されます。network LSAの状態を確認できます。



【All AreaID】

全エリアの状態を確認するときはチェックを入れます。

【AreaID】

確認したいエリアIDを指定します。

【All Link State ID】

全リンクステータスの状態を確認するときはチェックを入れます。

【Link State ID】

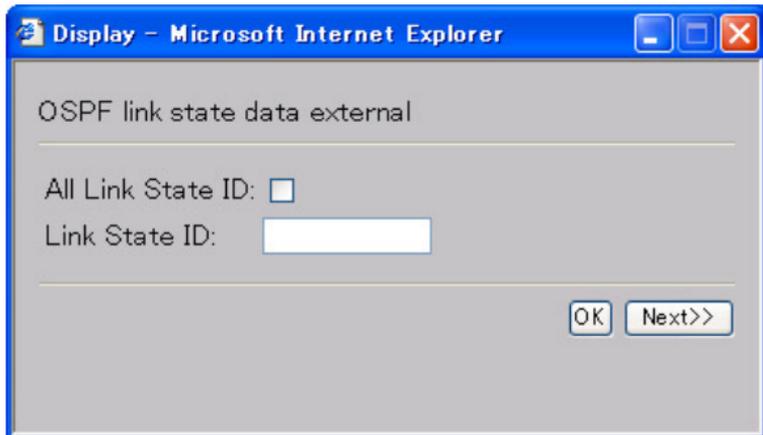
確認したいリンクステータスのIDを指定します。

上記の項目を指定後「Next>>」をクリックすると、ネットワークLSAの情報画面が表示されます。

LSAが一つも正常に取得ができない時は「Could not get network link data - no records found」と表示されます。

46 LSAs external(OSPF)

[Protocol] [IP] [OSPF] [LSAs external]をクリックすると、以下の画面が表示されます。externalの状態を確認できます。



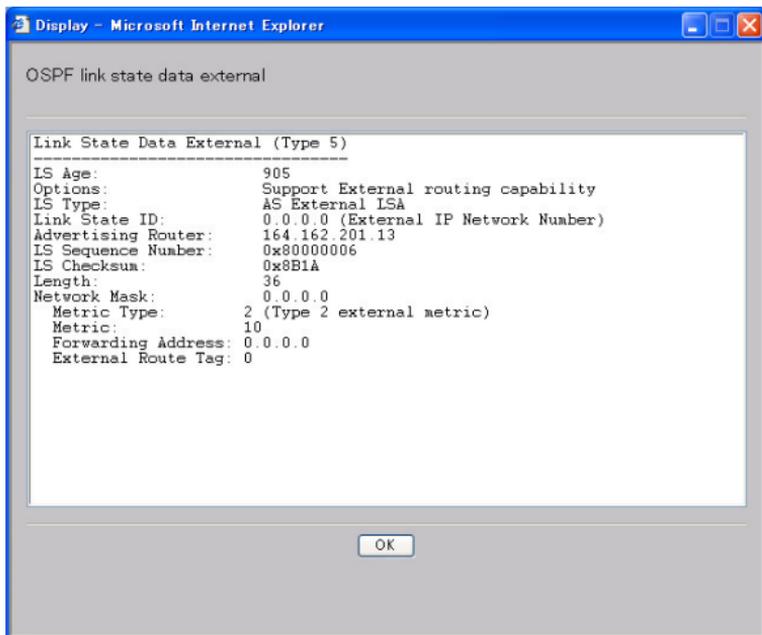
【All Link State ID】

全リンクステータスの状態を確認するときはチェックを入れます。

【Link State ID】

確認したいリンクステータスのIDを指定します。

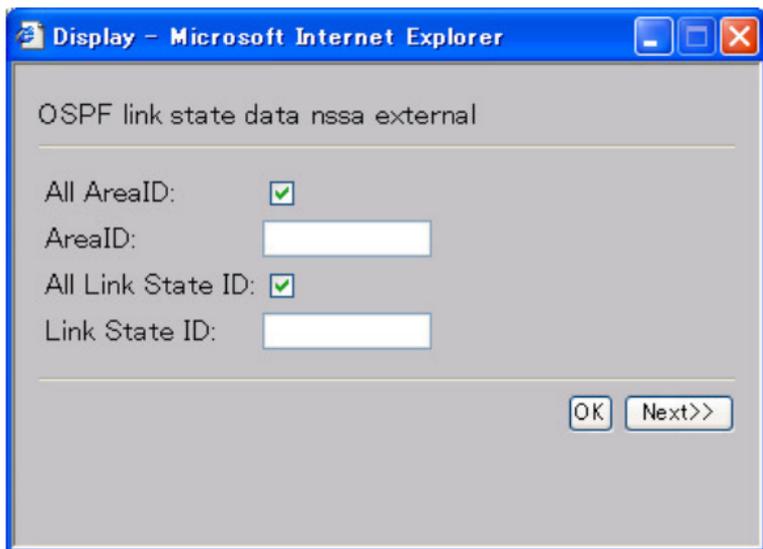
上記のどちらかを指定後「Next > >」をクリックすると、以下の画面が表示されます。



LSAが一つも正常に取得ができない時は「Could not get external link data - no records found」と表示されます。

47 LSAs NssaExternal (OSPF)

[Protocol] [IP] [OSPF] [LSAs external]をクリックすると、以下の画面が表示されます。NssaExternalの状態を確認できます。



【All AreaID】

全エリアの状態を確認するときはチェックを入れます。

【AreaID】

確認したいエリアIDを指定します。

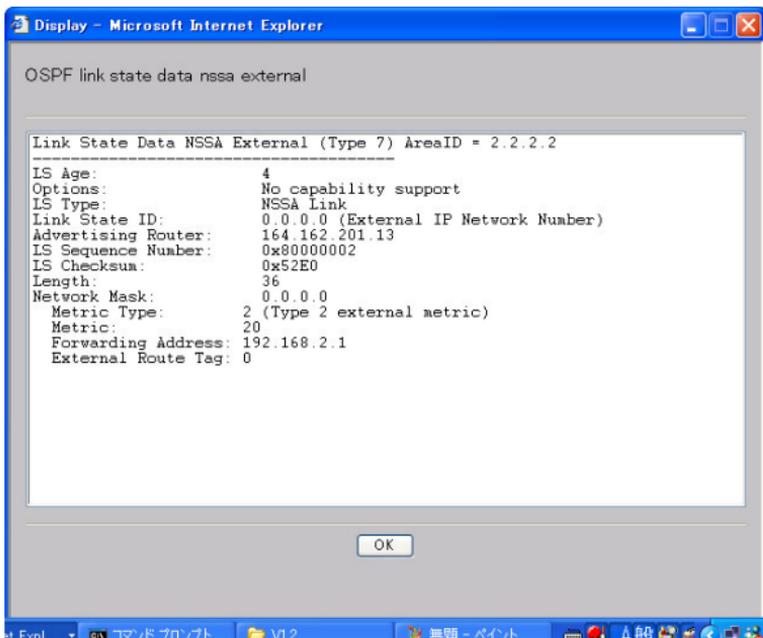
【All Link State ID】

全リンクステータスの状態を確認するときはチェックを入れます。

【Link State ID】

確認したいリンクステータスのIDを指定します。

上記の項目を指定後「Next >>」をクリックすると、以下の画面が表示されます。



LSAが一つも正常に取得ができない時は「Could not get nssa external link data - no records found」と表示されます。

48 Display Neighbors(OSPF)

[Protocol] [IP] [OSPF] [Display Neighbors]をクリックすると、以下の画面が表示されます。隣接関係のルータ情報を表示します。

Flags	Index	Neighbor Address	Priority	ReqD	RouterID	RxQ	State	SumQ
	1	164.162.201.252	1	0	164.162.201.252	0	Full	

【Flags】

隣接ルータとの関係を表示します。

- ・ DRouter : 指名ルータ
- ・ BDRouter : バックアップ指名ルータ

【Index】

本製品に接続されているOSPFインデックス番号を表示します。

【Neighbor Address】

隣接しているルータのIPアドレスを表示します。

【Priority】

隣接しているルータのプライオリティ(優先度)を表示します。

【ReqQ】

隣接しているルータに同期をとるためにリクエストをしたキューの総数を表示します。

【RouterID】

隣接しているルータのルータIDを表示します。

【RxQ】

隣接しているルータから再送達されて受信したキューの総数を表示します。

【State】

隣接ルータとの接続状況を表示します。

【SumQ】

隣接ルータへ送信した本製品のデータベースの総数を表示します。

49 Modify Router ID(OSPF)

[Protocol] [IP] [OSPF] [Modify Router ID]をクリックすると、以下の画面が表示されます。本製品のルータIDを変更できます。



【OSPF current router id is xxx.xxx.xxx.xxx】

現在のルータIDが表示されます。

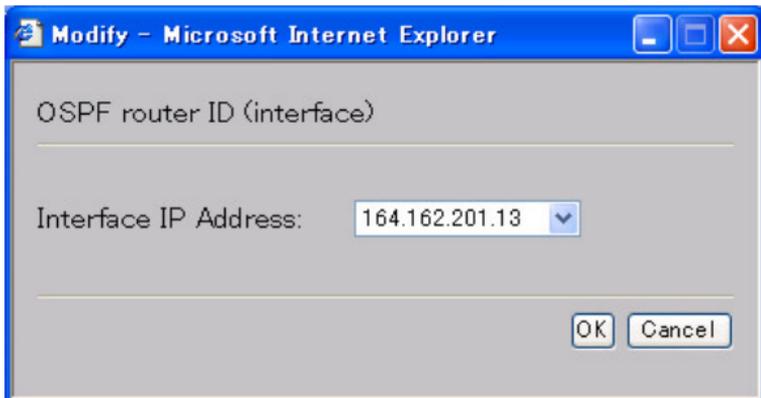
【Router ID】

- ・ default : 動的に設定されたルータIDを使用します。
- ・ interface : インターフェイスに設定されているIPアドレスをルータIDとして使用します。
- ・ address : 手動でルータIDを設定します。

「Router ID」で「interface」と「address」を選択したときは「Next >>」をクリックします。「default」を選択したときは「OK」をクリックします。

interfaceを選択した場合

interfaceを選択した場合は以下の画面が表示されます。



【Interface IP Address】

ルータIDに指定したいインターフェイスのIPアドレスを設定します。

- ・ 選択範囲 : 現在作成されているインターフェイスのIPアドレスが表示されます。

addressを選択した場合

addressを選択した場合は以下の画面が表示されます。



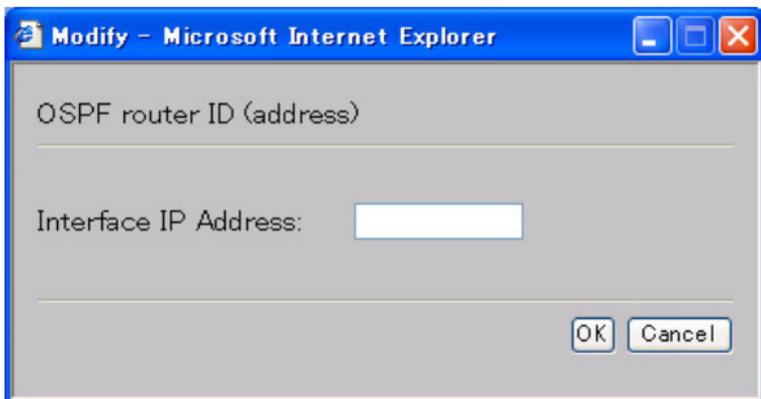
【Interface IP Address】

ルータIDに指定したいIPアドレスを設定します。

インターフェイスまたはネットワーク上で使用していないIPアドレスを設定してください。

50 Virtual links modify(OSPF)

[Protocol] [IP] [OSPF] [Virtual links modify]をクリックすると、以下の画面が表示されます。本製品をバックボーンルータとしたとき、別のスタンダードエリアを超えて存在するスタンダードエリアルータとの通信を確立する場合に設定します。エリアを超えてバックボーンに接続するスタンダードエリアルータにもVirtual Linkを設定してください。



Modify - Microsoft Internet Explorer

OSPF router ID (address)

Interface IP Address:

OK Cancel

表(上段)

【Index】

仮想リンクを行っているOSPFインデックス番号を表示します。

【Target Router】

仮想リンクを行っている相手先エリアルータのルータIDを表示します。

【Transit Area】

仮想リンクを行っている通過エリアのエリアIDが表示されます。

【Hello Intv1】

ルータ間の情報をやり取りする時間を変更します。単位は秒です。

【Dead Intv1】

ルータ間の情報のやり取りの最中に、隣接するルータから返答が無くなったときの待機する時間を設定します。単位は秒です。

【Rxmit Intv1】

LSAを再送信する時間を設定します。単位は秒です。

【Auth Mode】

認証タイプを表示します。認証タイプは、ルーティング情報が正当なサイトから送信されたものであることを保証します。

- ・ None : 認証を使わない
- ・ Password : パスワードを使用
- ・ Md5 : MD5パスワードを使用。

表(下段)

【Index】

仮想リンクを行っているOSPFインデックス番号を表示します。

【LocalAddr】

仮想リンクを行っている本製品のインターフェイスIPアドレスを表示します。

【RemoteAddr】

仮想リンクを行っている相手先ルータのインターフェイスIPアドレスを表示します。

【State】

現在の仮想リンクの状態が表示されます。

- ・ Full : 相手先エリアとの仮想リンクが確立しています。
- ・ Loading : 相手先エリアとの仮想リンクを確立させるため準備しています。
- ・ Init : 相手先エリアとの仮想リンクが確立していません。
- ・ NULL : 仮想リンクを行っている相手先ルータとのリンクが確立していません。

【RxQ】

仮想リンク先ルータから再送達されて受信したキューの総数を表示します。

【SumQ】

隣接ルータへ送信した本製品のデータベースの総数を表示します。

Add

Virtual Linkの設定を作成します。

注意 Virtual Linkの設定を作成する前に隣接ルータとのOSPFを確立させておく必要があります。

The screenshot shows a web browser window titled "Add - Microsoft Internet Explorer" displaying a configuration form for "OSPF Virtual Link". The form contains the following fields:

- Target Area: 0.0.0.0 (dropdown menu)
- Target Router: (text input field)
- Dead interval (in seconds): (text input field)
- Hello interval (in seconds): (text input field)
- Authentication type: None (dropdown menu)
- Password (8 ch-s max): (text input field)
- Md5 key(1-255) & password(16 ch-s max): (two text input fields)
- Retransmit interval (in seconds): (text input field)
- Transmit delay (in seconds): (text input field)

At the bottom right of the form are "OK" and "Cancel" buttons.

【Target Area】

仮想リンクを行っている通過エリアのエリアIDを設定します。

- ・ 指定項目 : 現在作成されているエリアIDが表示されます。

【Target Router】

仮想リンクを行っている相手先エリアルータのルータIDを設定します。

【Dead interval(in seconds)】

ルータ間の情報のやり取りの最中に、隣接するルータから返答が無くなったときの待機する時間を設定します。単位は秒です。

【Hello interval(in seconds)】

ルータ間の情報をやり取りする時間を設定します。単位は秒です。

【Authentication type】

認証タイプを設定します。認証タイプは、ルーティング情報が正当なサイトから送信されたものであることを保証します。

- ・ None : 認証を使わない
- ・ Password : パスワードを使用
- ・ Md5 : MD5パスワードを使用。

【Password(8 ch-s max)】

認証パスワードを設定します。パスワードは最小1文字～最大8文字の半角英数字で設定します。大文字・小文字を区別します。

【Md5 key(1-255)& password(16 ch-s max)】

暗号化認証パスワードを設定します。キーは最小1文字～最大255文字の半角英数字で設定します。パスワードは最小1文字～最大16文字の半角英数字で設定します。大文字・小文字を区別します。

【Retransmit interval(in seconds)】

LSAを再送信する時間を設定します。単位は秒です。

【Transmit delay(in seconds)】

LSAの遅延時間を設定します。単位は秒です。

Remove

作成したVirtual Link設定を削除します。「表(上段)」で削除するVirtual Link設定を選択後、「Remove」をクリックします。

Modify

作成したVirtual Link設定を編集をします。「表(上段)」で編集するVirtual Link設定を選択後、「Modify」をクリックすると、以下の画面が表示されます。

Modify - Microsoft Internet Explorer

OSPF Virtual Link

Modifying Virtual Link 1

Target Area: 1.1.1.1

Target Router: 192.168.2.2

Dead interval (in seconds): 40

Hello interval (in seconds): 10

Authentication type: None

Password (8 ch-s max):

Md5 key(1-255) & password(16 ch-s max):

Retransmit interval (in seconds): 5

Transmit delay (in seconds): 1

OK Cancel

【Target Area】

仮想リンクを行っている通過エリアのエリアIDの設定を変更します。

- ・ 指定項目 : 現在作成されているエリアIDが表示されます。

【Target Router】

仮想リンクを行っている相手先エリアルータのルータIDの設定を変更します。

【Dead interval(in seconds)】

ルータ間の情報のやり取りの最中に、隣接するルータから返答がなくなったときの待機する時間を変更します。単位は秒です。

【Hello interval(in seconds)】

ルータ間の情報をやり取りする時間を変更します。単位は秒です。

【Authentication type】

認証タイプを変更します。認証タイプは、ルーティング情報が正当なサイトから送信されたものであることを保証します。

- ・ None : 認証を使わない
- ・ Password : パスワードを使用
- ・ Md5 : MD5パスワードを使用。

【Password(8 ch-s max)】

認証パスワードを変更します。パスワードは最小1文字～最大8文字の半角英数字で設定します。大文字・小文字を区別します。

【Md5 key(1-255)& password(16 ch-s max)】

暗号化認証パスワードを変更します。キーは最小1文字～最大255文字の半角英数字で設定します。パスワードは最小1文字～最大16文字の半角英数字で設定します。大文字・小文字を区別します。

【Retransmit interval(in seconds)】

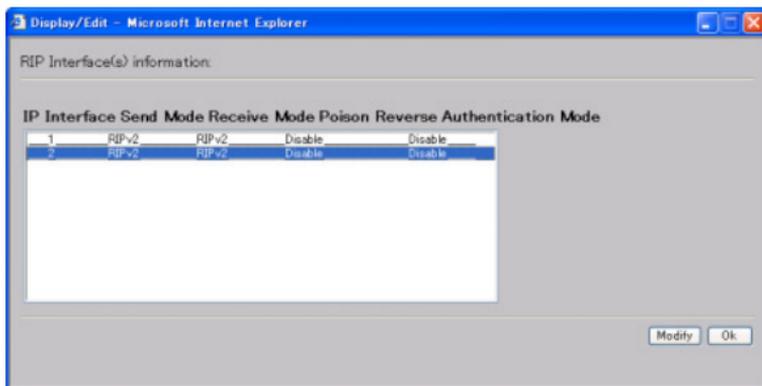
LSAを再送信する時間を変更します。単位は秒です。

【Transmit delay(in seconds)】

LSAの遅延時間を変更します。単位は秒です。

51 Display/Edit(RIP)

[Protocol] [IP] [RIP] [Display/Edit]をクリックすると、以下の画面が表示されます。RIP(Routing Information Protocol)の変更、参照ができます。



【IP Interface】

VLANグループが表示されます。

【Send Mode】

ポートで送信可能なルーティングプロトコルメッセージの種類を表示します。

【Receive Mode】

ポートで受信可能なルーティングプロトコルメッセージの種類を表示します。

【Poison Reverse】

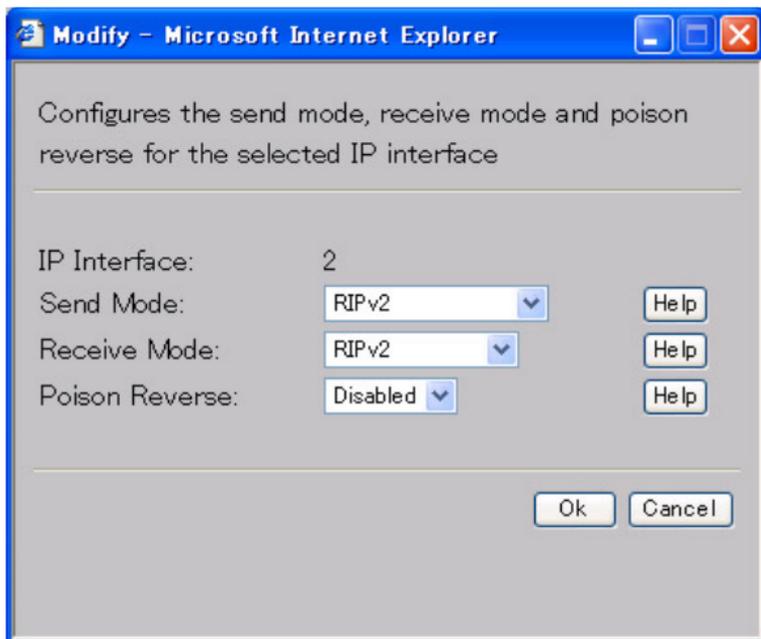
ポイズンリバーの有効/無効が表示されます。

【Authentication Mode】

RIPの認証の有効/無効が表示されます。

IPインターフェースの変更

「Display/Edit」の画面内の変更をしたいグループを選択し、「Modify」をクリックすると、以下の画面が表示されます。RIPの設定の変更ができます。



【IP Interface】

VLANグループが表示されます。

【Send Mode】

ポートで送信可能なルーティングプロトコルメッセージの種類を設定します。

- ・ do NotSend : 無効
- ・ RIPv1 : RIPv1のみ有効
- ・ RIPv1 Compatible : RIPv1とその互換性があるルーティングプロトコルとが有効
- ・ RIPv2 : RIPv2のみ有効

【Receive Mode】

ポートで受信可能なルーティングプロトコルメッセージの種類を設定します。

- ・ RIPv1 : RIPv1のみ有効
- ・ RIPv2 : RIPv2のみ有効
- ・ RIPv1OrRIPv2 : RIPv1とRIPv2の両方が有効

【Poison Reverse】

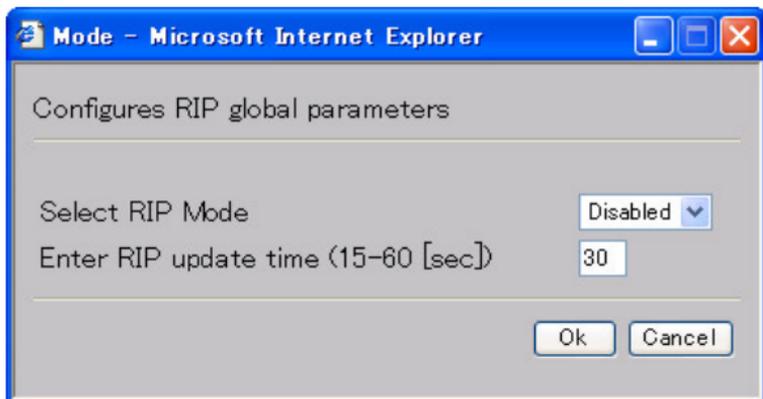
ルートを最初に入手したインターフェースポートまで、ルートを逆に伝播します。ただし、距離のベクターメトリックは無限大に設定されます。

- ・ Enabled : 有効
- ・ Disabled : 無効

上記の項目を設定したら「OK」をクリックします。設定が反映されます。

52 Mode(RIP)

[Protocol] [IP] [RIP] [Display/Edit]をクリックすると、以下の画面が表示されます。RIPの有効/無効を設定します。



【Select RIP Mode】

RIPの有効/無効を設定します。

- ・ Enabled : 有効
- ・ Disabled : 無効

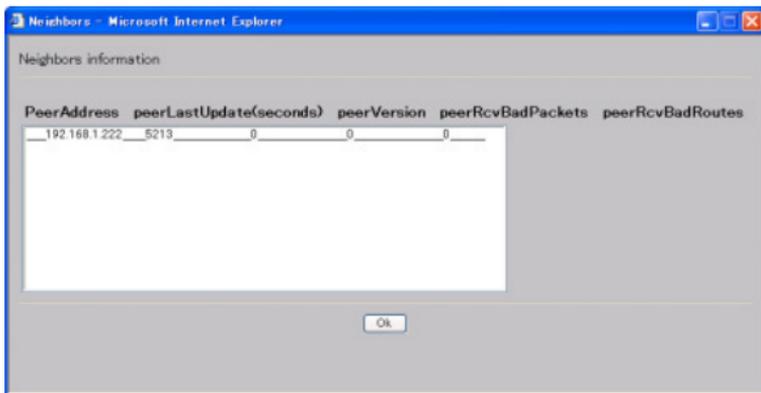
【Enter RIP update time (15-60 [sec])】

ネットワークの全機器に対し数秒に1回RIPメッセージをブロードキャストします。RIPメッセージを送る時間を設定します。

- ・ 15 ~ 60 : RIPメッセージを送る時間を設定します。単位は秒

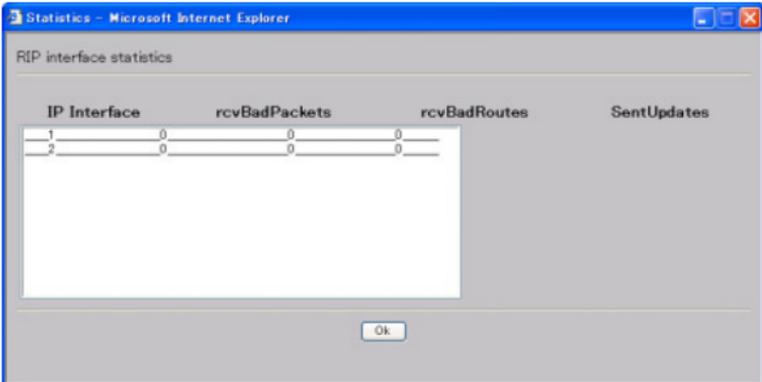
53 Neighbors(RIP)

[Protocol] [IP] [RIP] [Neighbors]をクリックすると、以下の画面が表示されます。隣接するRIPルータの情報が表示されます。



54 Statistics(RIP)

[Protocol] [IP] [RIP] [Statistics]をクリックすると、以下の画面が表示されます。本製品内でのRIP状況の情報が表示されます。



IP Interface	rcvBadPackets	rcvBadRoutes	SentUpdates
1	0	0	0
2	0	0	0

55 Default Gateway(ROUTE)

[Protocol] [IP] [ROUTE] [Default Gateway]をクリックすると、以下の画面が表示されます。アクセス先のIPアドレスについて特定のゲートウェイを指定していない場合に、デフォルトゲートウェイに指定されているホストにデータが送信されます。

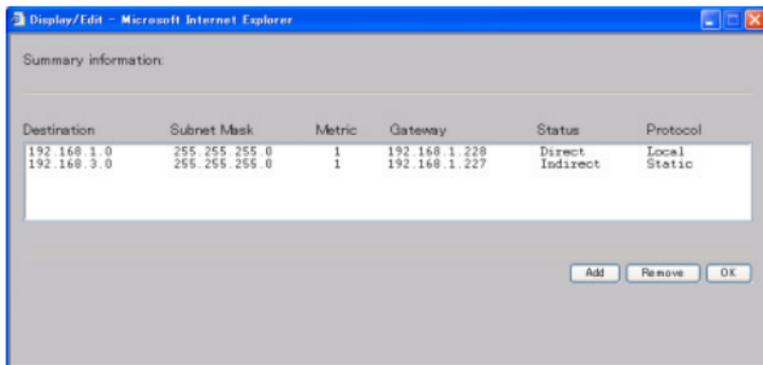


【Default Gateway IP Address】

デフォルトゲートウェイに指定されているホストのIPアドレスを設定します。

56 Display(ROUTE)

[Protocol] [IP] [ROUTE] [Display]をクリックすると、以下の画面が表示されます。ルート情報の表示、静的ルートの追加・削除ができます。



The screenshot shows a web browser window titled 'Display/Edit - Microsoft Internet Explorer'. The main content area is titled 'Summary information:' and contains a table with route data. At the bottom right of the window, there are three buttons: 'Add', 'Remove', and 'OK'.

Destination	Subnet Mask	Metric	Gateway	Status	Protocol
192.168.1.0	255.255.255.0	1	192.168.1.228	Direct	Local
192.168.3.0	255.255.255.0	1	192.168.1.227	Indirect	Static

【Destination】

通信先のネットワークグループが表示されます。

【Subnet Mask】

サブネットマスクが表示されます。

【Metric】

Destination NetworkのIPルートまでのホップ数が表示されます。

【Gateway】

次のホップにあたるルータのIPアドレスが表示されます。

【Status】

Destination NetworkへのIPルートの種類が表示されます。本製品は以下のルートに対応します。

- ・ Direct : 直接接続されているサブネットワーク
- ・ Indirect : リモートIPサブネットワークまたはリモートホストアドレス
- ・ Myself : 特定IPサブネットワークのスイッチIPアドレス
- ・ Bcast : サブネットワーク・ブロードキャストアドレス
- ・ Mcast : IPマルチキャストアドレス
- ・ Invalid : フィルタ対象となる不正IPアドレス

【Protocol】

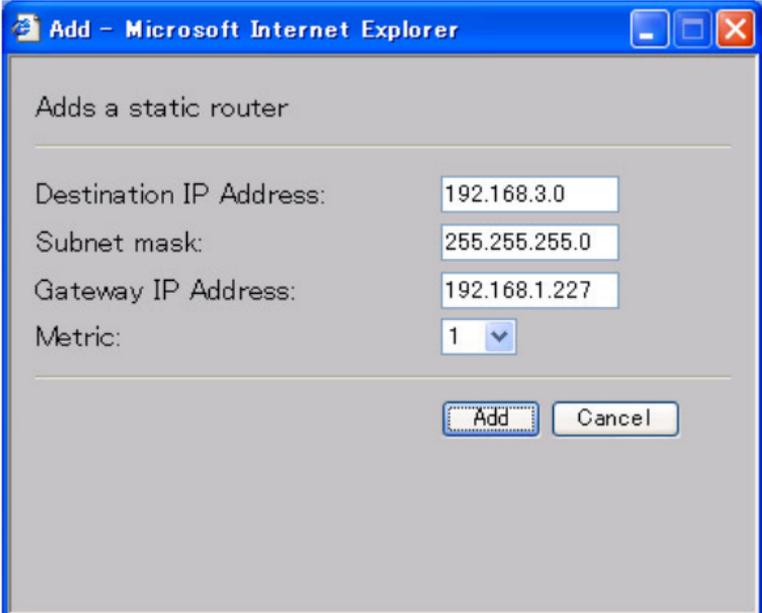
ルートは以下のいずれかの方法で表示されます。

- ・ Local : 本製品のインターフェイスに設定している時
- ・ Static : 手動で設定
- ・ RIP : RIPで学習

静的ルートの追加

「Display」の画面内の「Add」をクリックすると、以下の画面が表示されます。

静的ルートを追加できます。



The screenshot shows a dialog box titled "Add - Microsoft Internet Explorer". The main text inside the dialog is "Adds a static router". Below this, there are four input fields and a dropdown menu:

Destination IP Address:	192.168.3.0
Subnet mask:	255.255.255.0
Gateway IP Address:	192.168.1.227
Metric:	1

At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

【Destination IP Address】

通信先のネットワークグループを設定します。

【Subnet mask】

サブネットマスクを設定します。

【Gateway IP Address】

次のホップにあたるルータのIPアドレスを設定します。

【Metric】

Destination NetworkのIPルートまでのホップ数を指定します。

上記の項目を設定したら「Add」をクリックします。

静的ルートの削除

「Display」の画面内の削除をしたいグループを選択し、「Remove」をクリックすると、以下の画面が表示されます。静的ルートの削除ができます。



【Destination IP Address】

通信先のネットワークグループを設定します。

【Subnet mask】

サブネットマスクを設定します。

「Remove」をクリックします。

57 Flush(ROUTE)

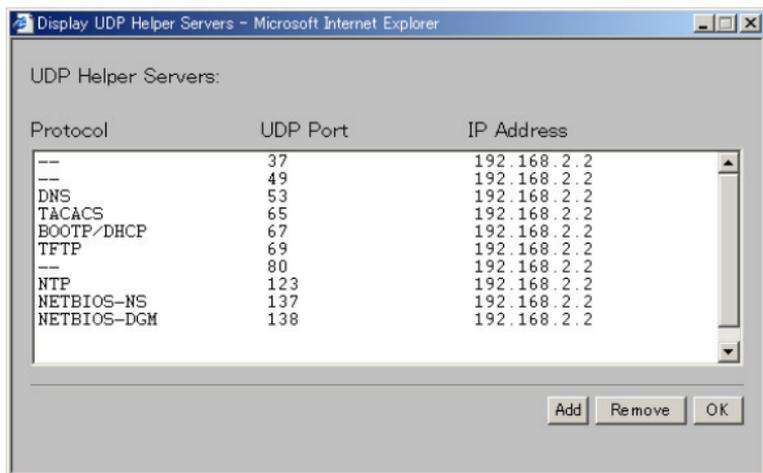
[Protocol] [IP] [ROUTE] [Flush]をクリックすると、以下の画面が表示されます。動的に学習したルーティング情報を削除します。



「This operation will remove all learned routes from the routing table.」が表示されるので「OK」をクリックします。

58 Display/Edit(UDP Helper)

[Protocol] [IP] [UDP Helper] [Display/Edit]をクリックすると、以下の画面が表示されます。特定サービスポート宛でのUDPブロードキャストを、指定したIPアドレスに転送します。



【Protocol】

特定サービスポートの名称を表示します。

【UDP Port】

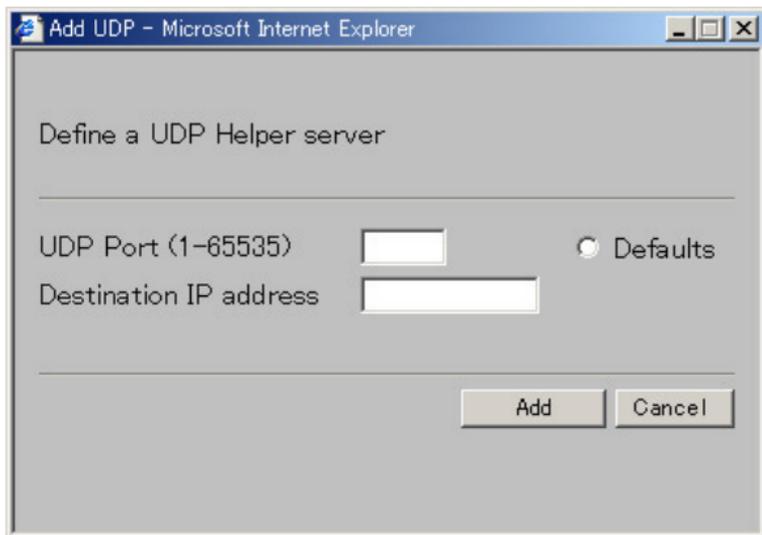
特定サービスポート番号を表示します。

【IP Address】

指定したIPアドレスを表示します。

Add

UDPヘルパーの設定を作成・追加します。



Define a UDP Helper server

UDP Port (1-65535) Defaults

Destination IP address

Add Cancel

【UDP Port(1-65535)】

特定サービスポート番号を設定します。

【Defaults】

「UDP Port(1-65535)」を設定せずに「Defaults」にチェックを入れて設定すると以下の項目の特定サービスポート番号すべてを追加します。

- ・ DNS : ポート番号53
- ・ TACACS : ポート番号65
- ・ BOOTP/DHCP : ポート番号67
- ・ TFTP : ポート番号69
- ・ NTP : ポート番号123
- ・ NETBIOS-NS : ポート番号137
- ・ NETBIOS-DGM : ポート番号138

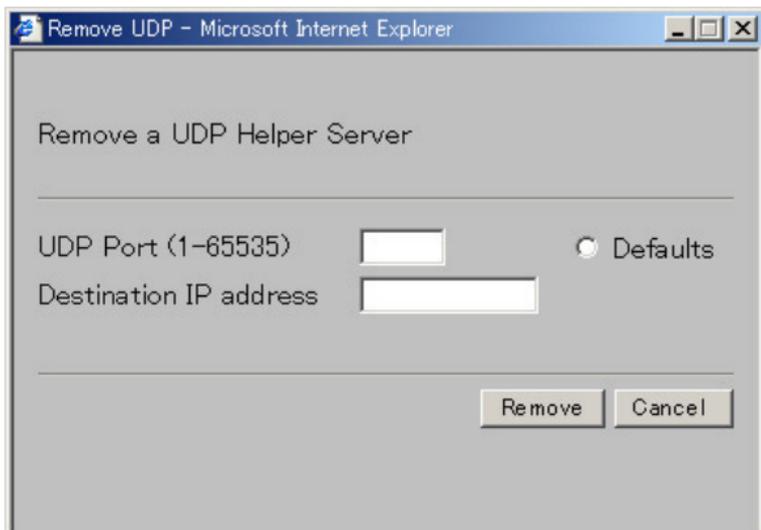
【Destination IP address】

転送するIPアドレスを設定します。

すべての項目を設定後「Add」をクリックします。

Remove

設定してあるUDPヘルパーの設定を削除します。



【UDP Port(1-65535)】

削除する特定サービスポート番号を設定します。

【Defaults】

「Defaults」の設定で作成されているときは「Defaults」にチェックを入れて設定すると以下の項目の特定サービスポート番号すべてを削除します。

- ・ DNS : ポート番号53
- ・ TACACS : ポート番号65
- ・ BOOTP/DHCP : ポート番号67
- ・ TFTP : ポート番号69
- ・ NTP : ポート番号123
- ・ NETBIOS-NS : ポート番号137
- ・ NETBIOS-DGM : ポート番号138

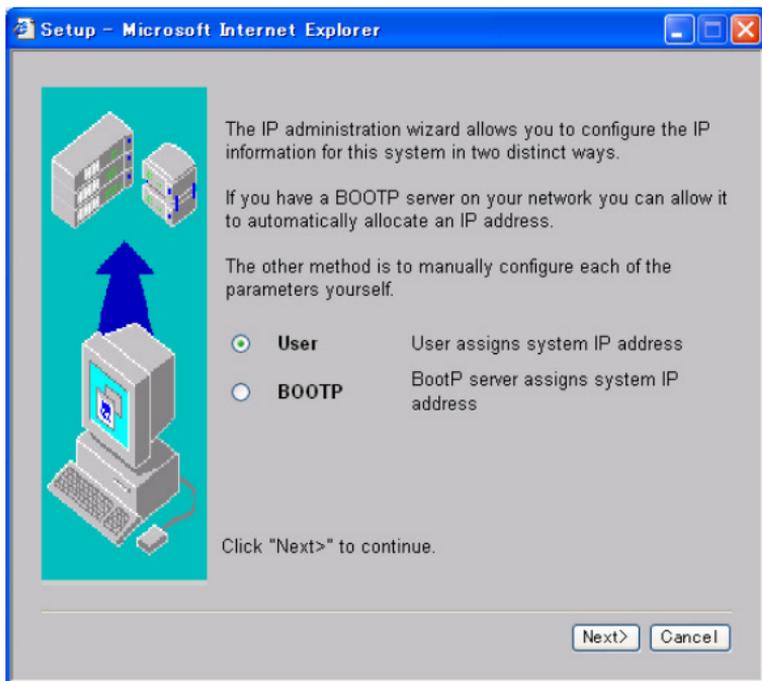
【Destination IP address】

削除する転送するIPアドレスを設定します。

すべての項目を設定後「Remove」をクリックします。

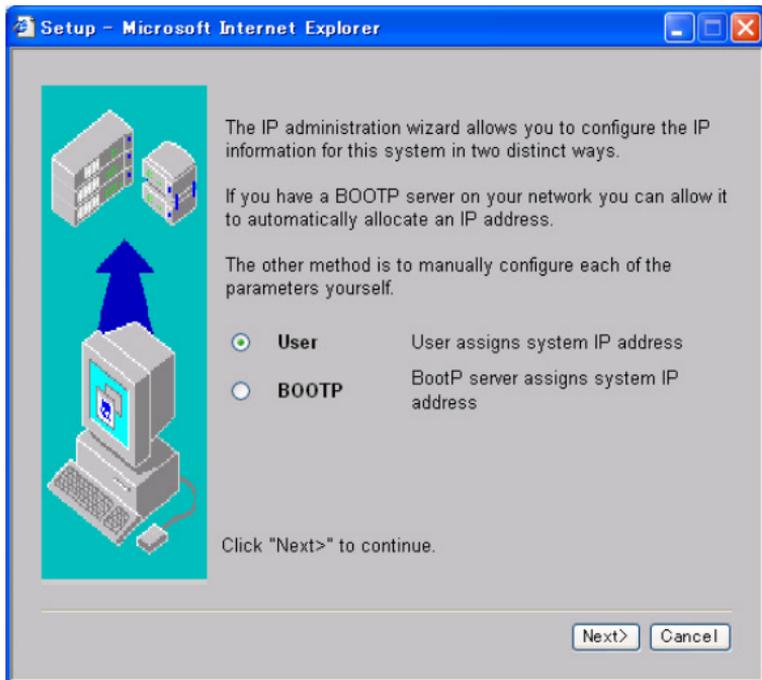
59 Setup(IP)

[Protocol] [IP] [Setup]をクリックすると、以下の画面が表示されます。本製品の管理用にIPサブネットアドレスを設定できます。



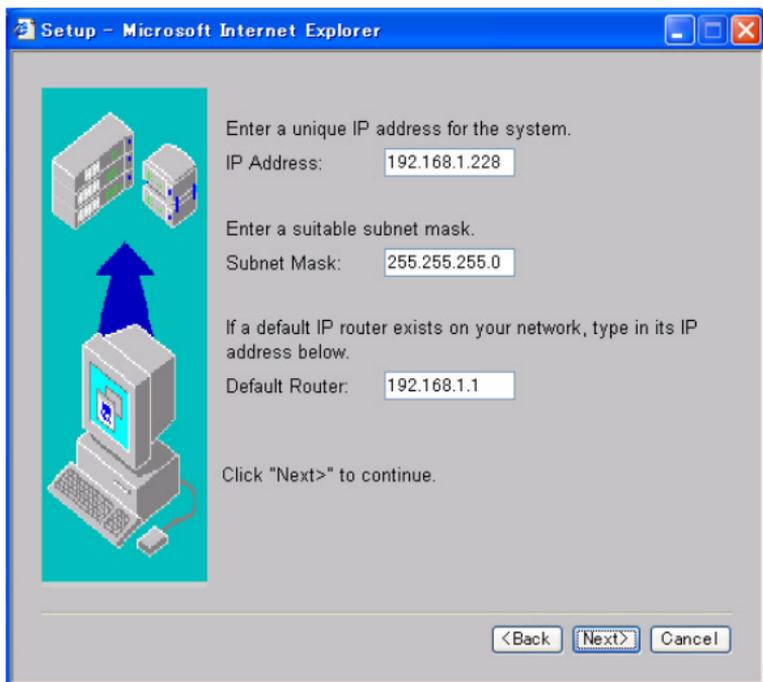
IPサブネットアドレスの設定方法

1. 本製品の管理用にIPサブネットアドレスを設定するため、手動設定かBootPを選択して[NEXT >]をクリックします。

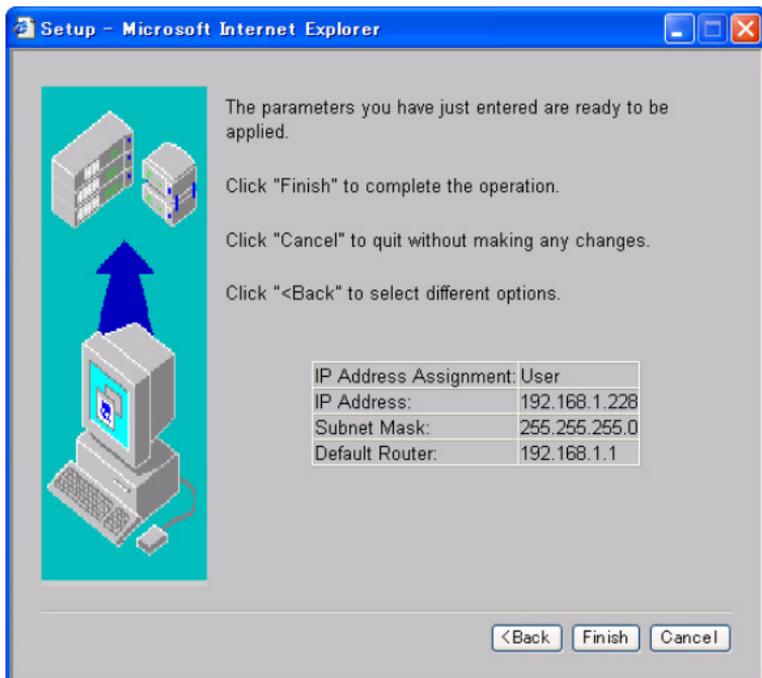


- ・ User : 手動でIPアドレスを設定
- ・ BOOTP : BootPサーバからIPアドレスを取得

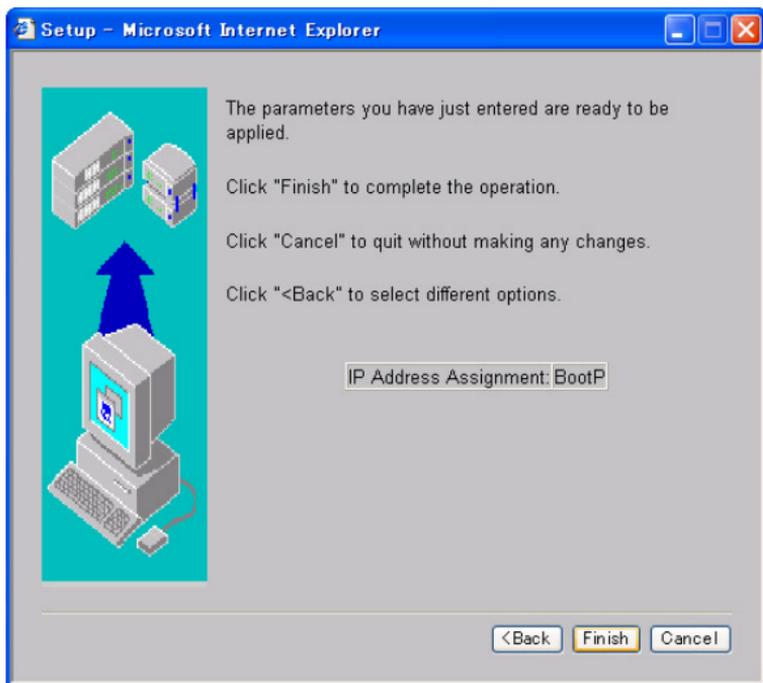
- 2.上記の項目で[User]を選択したときは以下の画面が表示されます。[BOOTP]を選択したときは「4.」へ進んでください。IPアドレス、サブネットマスク、デフォルトゲートウェイに入力して[NEXT >]をクリックします。



3. 設定の確認画面が表示されます。設定内容に間違いがないことを確認して[Finish]をクリックします。

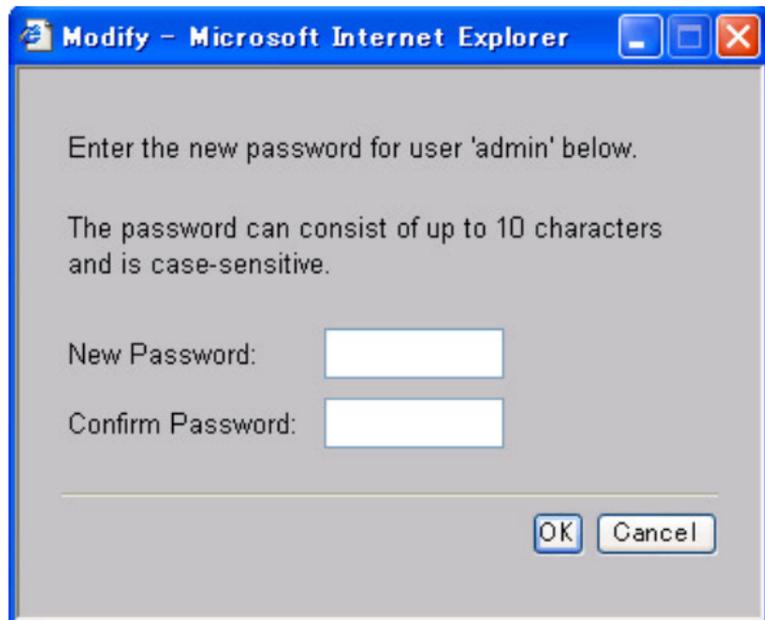


4. 設定の確認画面が表示されます。設定内容に間違いがないことを確認して[Finish]をクリックします。訂正は[Back]をクリックします。



60 Modify(User)

[Security] [Device] [User] [Modify]をクリックすると、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。



The screenshot shows a dialog box titled "Modify - Microsoft Internet Explorer". The background is light gray. The text inside reads: "Enter the new password for user 'admin' below." followed by "The password can consist of up to 10 characters and is case-sensitive." Below this, there are two input fields. The first is labeled "New Password:" and the second is labeled "Confirm Password:". At the bottom right, there are two buttons: "OK" and "Cancel".

【New Password】

新しいパスワードを入力します。

【Confirm Password】

確認のため、もう一度パスワードを入力します。

* 最大数：半角英数10文字まで可能

61 Port Security(Access)

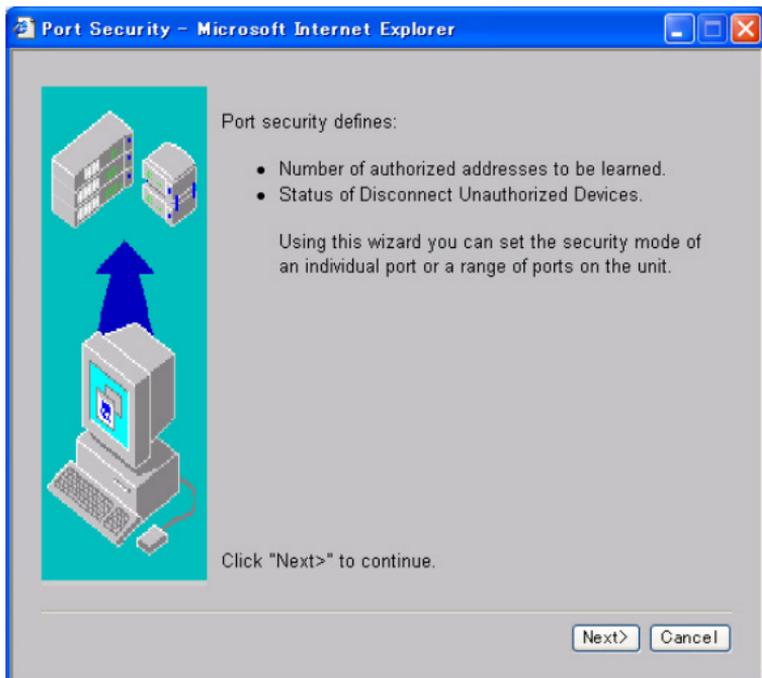
[Security] [Network] [Access] [Port Security]をクリックすると、以下の画面が表示されます。ポートセキュリティを設定します。



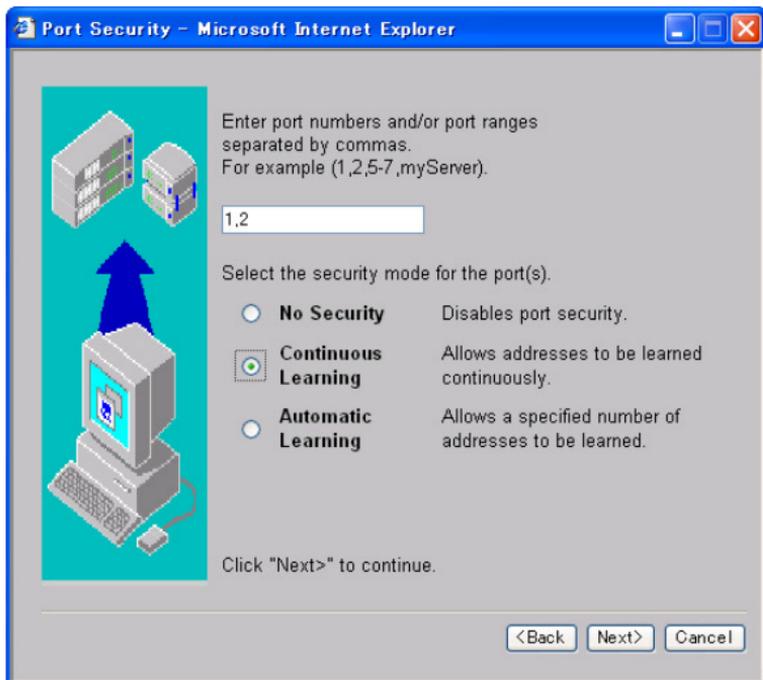
【Ether a slot number】

ポートセキュリティを設定するスロット番号を設定します。

上記の項目を入力したら「OK」をクリックします。以下の画面が表示されるので「Next >」をクリックします。



ポート範囲とセキュリティ方法を設定して「Next >」をクリックします。



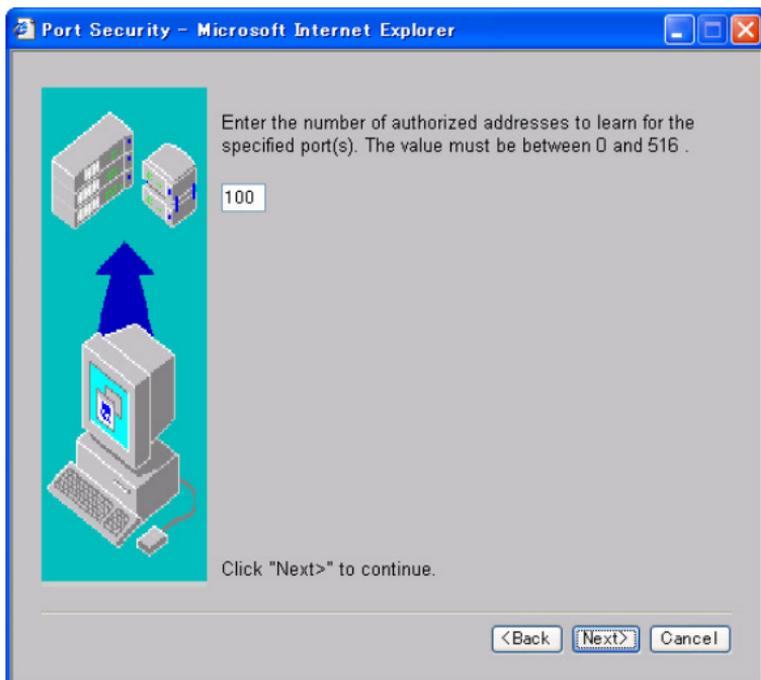
【Enter port numbers and/or port ranges separated by commas.】
ポート範囲を設定します。

【Select the security mode for the port(s).】

セキュリティ方法を設定します。

- ・ No Security : ポート・セキュリティを無効
- ・ Continuous Learning : アドレスを連続的に学習
- ・ Automatic Learning : 設定したアドレス数が学習

学習するアドレス数を設定して「Next>」をクリックします。

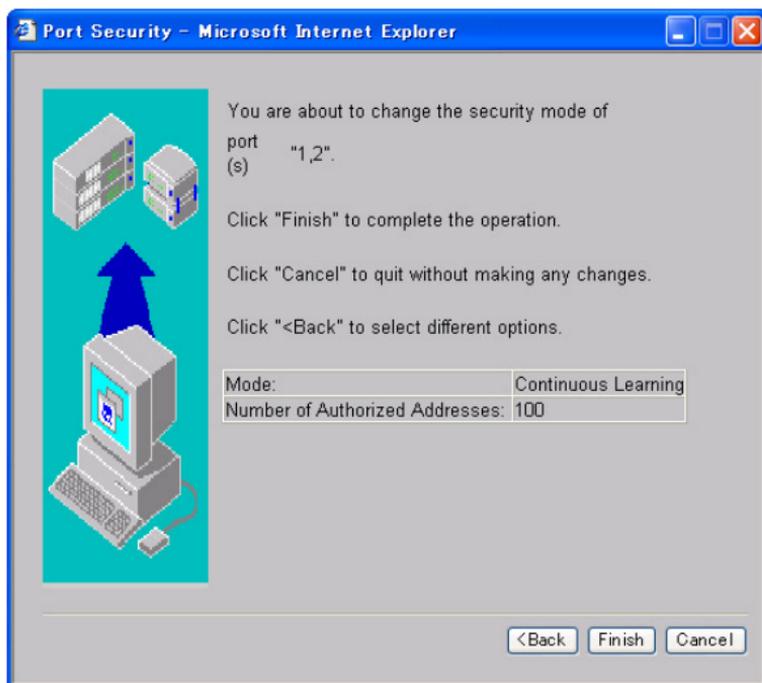


【Enter the number of authorized addresses to learn for the specified port(s).】

学習するアドレス数を設定します。

- ・ 0 ~ 516 : 指定するアドレス数の範囲

設定の確認画面が表示されます。設定内容に間違いがないことを確認して[Finish]をクリックします。訂正は[Back]をクリックします。



5. 技術解説

FML-1200は、ネットワーク機器の物理アドレスに基づくレイヤ2、およびIPネットワークアドレスに基づくレイヤ3スイッチに対応します。これらの機能を説明します。

1 レイヤ2スイッチ

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、既知のものか確かめます。

- ・ 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

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か判断します。

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 STA(Spanning Tree Algorithm)

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は分布式の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

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。

注意 IPスイッチングを行う場合、本製品は他ネットワーク上のノードからIPルータとして認識される必要があります。このためには、本製品をデフォルトゲートウェイに設定するか、またはICMP処理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次の作業などが含まれます。

- 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
- 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

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

本製品は、静的および動的ルーティングに対応します。

【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、エリアのトポロジー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ー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ます。また、ルーティング障害などに対する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。

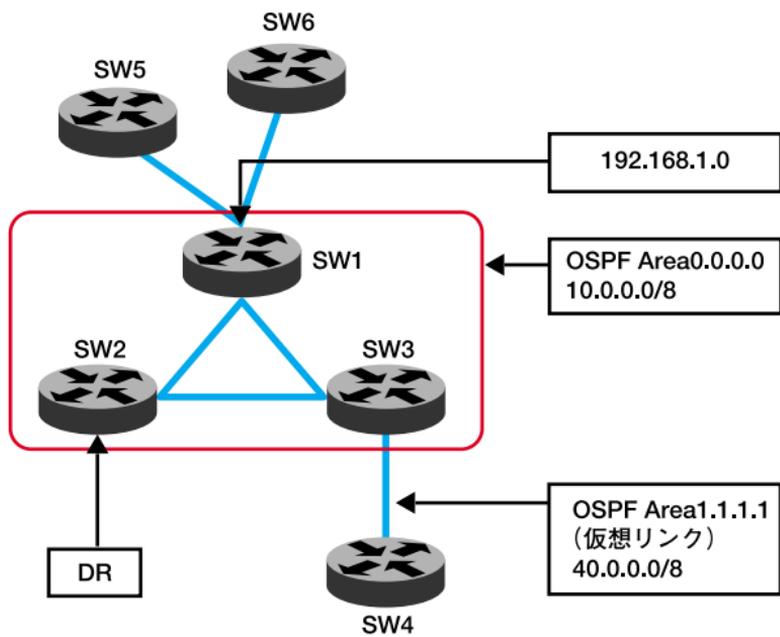


図5-1 OSPF構成図

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の初期設定

本製品のVLAN初期設定は、すべてのポートが同じVLANグループのため、レイヤ2の機能だけが使えます。このため、まず同一サブネットに所属するポートをVLANグループに分割する必要があります。同一サブネット内のネットワークトラフィックは、レイヤ2スイッチ機能によってスイッチされます。

また、レイヤ3スイッチ機能を使うことで、必要な場合に限り、複数VLAN間を相互接続できます。各VLANは、レイヤ3への仮想インターフェースとして機能します。各仮想インターフェースのネットワークアドレスを設定するだけで、異なるサブネットワーク間のトラフィックはレイヤ3スイッチによりルートされるようになります。

注意 マルチレイヤモードで使うとき、各ポートはすべてタグ無しパケットを送信します。VLANグループが重複するような設定は、レイヤ3スイッチング機能が正しく動作しない原因になります。また、同一VLAN内で通信するためには、VLAN内のすべてのポートを同じPVIDに設定する必要があります。

12 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作られていないため、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内で変更を加えられるようになります。またVLANでは、トラフィックはあらかじめ設定されたレイヤ3リンクを通過しなければ他のVLANに到達できないようになっているため、VLANは元々高度なネットワークセキュリティ機能を備えていると言えます。本製品は以下のVLAN機能に対応します。

- 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

13 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。

14 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VLAN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、これらの中で通信を行わせる場合は、本製品をまずマルチレイヤモードに設定し、別のVLANへのIPインターフェースアドレスを設定します。

15 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。

16 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。

17 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。

18 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もありません。一方、レイヤ2スイッチングは現在もVLAN内部のトラフィックで使用されています。

本製品は、RIPやOSPFといった、静的設定プロトコルや動的ルーティングプロトコルで構築された標準のルーティングテーブルを使用します。各ルーティングエントリはネットワークアドレス(IPアドレス+サブネットマスク)および仮想インターフェース番号(virtual interface number)により構成されます。各仮想インターフェースはそれぞれVLANに対応しているほか、VLAN IDにより識別されます。また、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。

19 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て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。

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

21 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。

22 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。

23 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。

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

- ・ベストエフォート型よりプライオリティの高いアプリケーションを備えたエンドステーションにより、直接プライオリティを割り当てることができます。本製品では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。

25 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。

26 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。

27 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。

28 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。

29 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。

30 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. 本体構成

最低限必要な構成

FML-1200の通常動作に最低限必要なコンポーネントは以下の通りです。

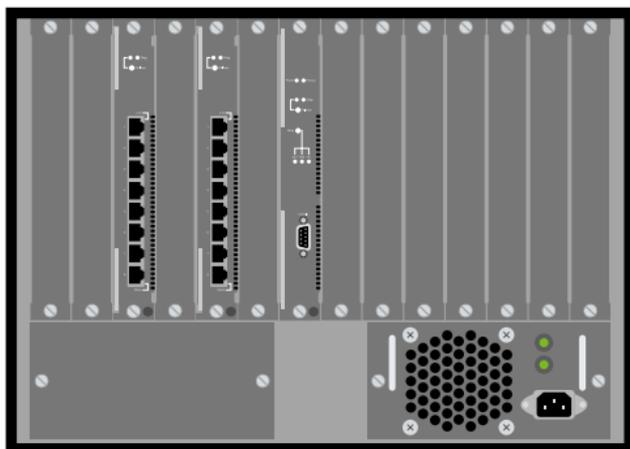
本体 (FML-1200)

マネージメントモジュール(システムソフトウェアで動作)×1

ファンユニット×2 (合計ファン数=4)

冗長化電源ユニット×1

ご使用ネットワークに必要な数量・種類のインタフェースモジュール
ブランク・フェイスプレート(未使用モジュールスロットおよび、第2電源用ベイを使用しない場合は同ベイにはめます)



図A-1 必要最低限

搭載可能な最大構成

FML-1200の最大限に拡張できるコンポーネントは以下の通りです。

本体(FML-1200)

マネージメントモジュール(システムソフトウェアで動作)×2

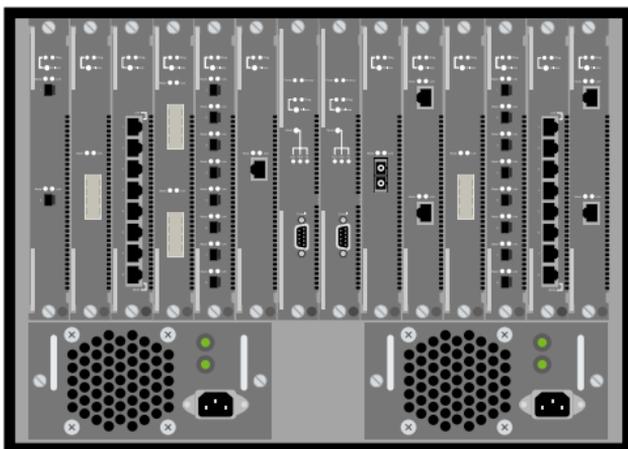
*一つはバックアップ用として使用

ファンユニット×2(合計ファン数=4)

冗長化電源ユニット×2

*通常使用時には負荷分散にて使用

全12スロットにインタフェースモジュールを装着



図A-2 最大構成

最大ポート数構成

FML-1200でポートを最大限に接続するには以下の通りです。

本体(FML-1200)

マネージメントモジュール(システムソフトウェアで動作)×1

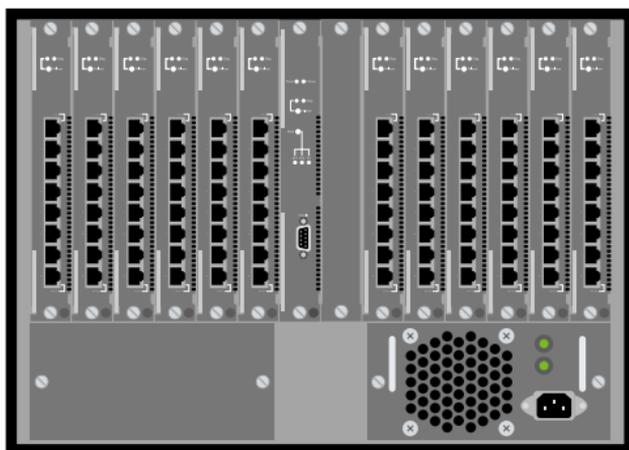
ファンユニット×2 (合計ファン数=4)

冗長化電源ユニット×2

*通常使用時には負荷分散にて使用

全12スロットにF120-8TXまたはF120-8MTを装着

*合計96ポート



図A-3 最大ポート数構成

最大ギガポート数構成

FML-1200でギガポートを最大限に接続するには以下の通りです。

本体(FML-1200)

マネージメントモジュール(システムソフトウェアで動作)×1

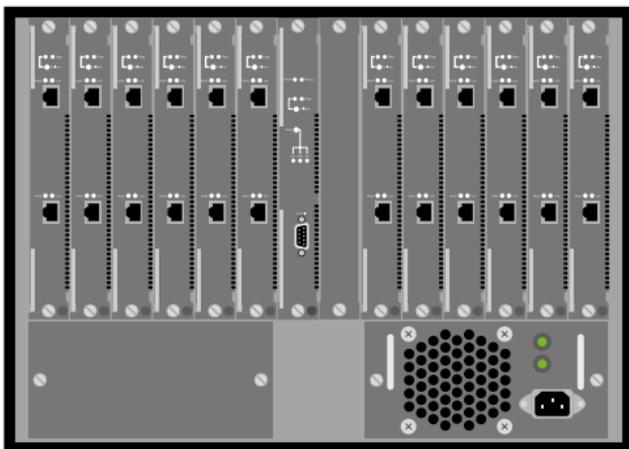
ファンユニット×2 (合計ファン数=4)

冗長化電源ユニット×2

*通常使用時には負荷分散にて使用

全12スロットにF120-2TE、F120-2GBIC、F120-2GMTのいずれかを装着

*合計24ポート



図A-4 最大ギガポート数構成

付録 B. IPルーティングネットワーク構成例

本製品を使った、ネットワーク構成例を説明します。設定例は参考構成です。また、設定を明記していない項目はすべてデフォルト設定です。

ネットワークを構成する機器

【インターネットルータ】

IP : 192.168.1.1

Subnet : 255.255.255.0

【パソコンA】

IP : 192.168.2.100

Subnet : 255.255.255.0

【パソコンB】

IP : 192.168.3.100

Subnet : 255.255.255.0

【サーバA】

IP : 192.168.4.100

Subnet : 255.255.255.0

【サーバB】

IP : 192.168.5.100

Subnet : 255.255.255.0

FML-1200の設定

【VLAN1 Slot1 Port1 ~ 8】

PVID 1

IP : 192.168.1.254

Subnet : 255.255.255.0

【VLAN2 Slot2 Port1 ~ 8、 Slot3 Port1 ~ 8】

PVID 2

IP : 192.168.2.254

Subnet : 255.255.255.0

【VLAN3 Slot4 Port1 ~ 8、 Slot5 Port1 ~ 8】

PVID 3

IP : 192.168.3.254

Subnet : 255.255.255.0

【VLAN4 Slot8 Port1】

PVID 4

IP : 192.168.4.254

Subnet : 255.255.255.0

【VLAN5 Slot9 Port1】

PVID 5

IP : 192.168.5.254

Subnet : 255.255.255.0

【Default Route】

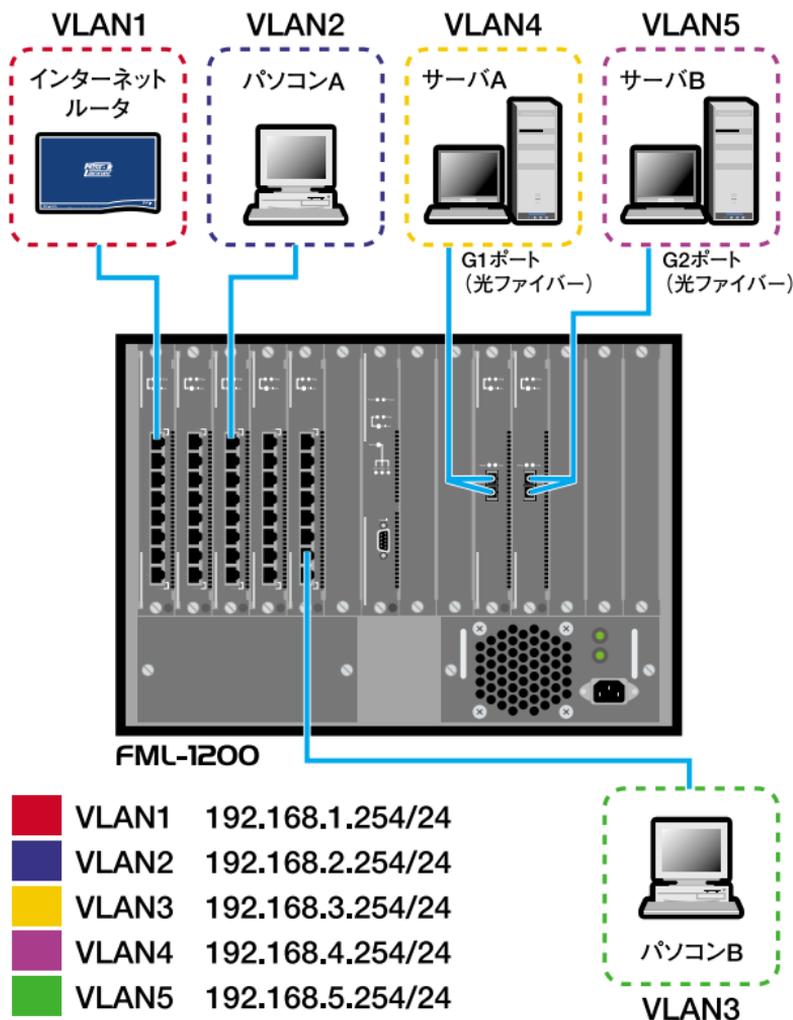
IP : 192.168.1.1

Subnet : 255.255.255.0

【RIP】

Send Type RIP2

Receive Type RIP2



図B-1 レイヤ3 ネットワーク構成図

付録 C. 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 > 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

スタティックでルートを入力したがルーティングテーブルに表示されない

対処

- ・ スタティックで設定したポートのリンクを確認してください。ポートのリンクが確立していないとき、本製品はスタティックルートのIPアドレスは表示されません。

症状

ルーティングできない

対処

- ・ コンピュータのIPアドレスが接続先のVLANグループのIPインターフェースと同一のグループに設定されているか確かめてください。
- ・ コンピュータのデフォルトゲートウェイアドレスに接続先のVLANグループのIPインターフェースアドレスが指定されているか確かめてください。

症状

マルチレイヤモードに設定したとき、タグを付加したパケットを送信するための設定ができない

対処

- ・ 本製品のマルチレイヤモードは、パケットにタグを付加して送信できません。またタグ付のパケットを受信してもタグをフィルタリングして送信します。

症状

ルーティングはできるが同一VLAN内の通信ができない

対処

- ・ ポートのPVID（ポートVID）が所属しているVLANグループのVIDと同じ番号になっているか確かめてください。

症状

ルーティングが不安定

対処

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

症状

Pingを実行して異なるサブネットと通信テストをすると最初のリプライが遅い

対処

- ・本製品はハードウェアルーティング処理によりワイヤースピードでルーティングができます。しかし、送信先のネットワーク機器のIPアドレスがルーティングテーブルに存在しないとき、アドレス検索のために最初のパケット処理に遅れが生じます。

付録 D. ファームウェアのアップデートと 設定ファイルのアップデート/ダウンロード

シリアルポート経由でファームウェアを更新する

本製品のシリアルポートにお使いのコンピュータを接続し、Xmodemプロトコル対応の端末インターフェースパッケージを使うことで、本製品のファームウェアが更新できます。

1. 本製品をリセットします。Restart Systemコマンドを実行するか、電源ケーブルをコンセントから取り外して5秒間待ち、再び電源コードを取り付けます。
2. システムの初期化スクリーンが以下のように表示されますので、Dキーを押してファームウェアのダウンロードを行ってください。またこのとき、コードの種類も1 (Runtime) か2 (POST) か9 (MicroCode) のいずれかを選択してください。
3. ボーレートを115200bpsに変更してEnterキーを押すとダウンロードが有効となります。お使いのターミナルエミュレーションプログラム上で、ダウンロードするファイルを選択し、プロトコルをXmodemに設定してダウンロードを開始してください。

注意 ・Windows用ハイパーターミナルをお使いの場合は、いったん切断（切断アイコンを挿入）してボーレートを設定してから再度接続（接続アイコンを挿入）してください。

・ダウンロードファイルは、バイナリファイルかイメージファイルを指定してください。これら以外のファイル形式は本製品で受け付けられないようになっています。

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

```
XModem Download to DRAM buffer area 0x00200000: ...  
... SUCCESS !  
Verifying image in DRAM download buffer 0x00200000...  
SUCCESS !  
Update FlashROM Image at 0x03140000 ... |
```

付録E.用語集

【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。

【BGP】(Border Gateway Protocol)

経路制御に使われるプロトコル。

【BPDU】(Bridge Protocol Data Unit)

スパニングツリーの情報交換するHelloパケット。

【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。

【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。

【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。

【LACP】(Link Aggregation Control Protocol)

低速なリンクを複数束ねてひとつのリンクとして使う技術。IEEE 802.3adで制定。

【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。

【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。

【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。

【OSPF】(Open Shortest Path First)

経路制御のプロトコルのひとつ。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【WFQ】(Weighted Fair Queuing)

データの優先順位を変える技術。

【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。

【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。

【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。

【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。

【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、ら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。

【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。

【ユニキャスト】(Unicast)

1対1で通信する方式。

【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。

【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の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F. 工場出荷時設定

機能	初期設定値
Pアドレス	0.0.0.0
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(パスワードは、設定されていません)
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
HTTPサーバ	有効
SNMP	有効
SNMPリード	public private manager security
コミュニティネーム	
SNMPライト	private security
コミュニティネーム	
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	LANグループの全てのパケットには、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パケットを受け取ったときは、自動認識
スパニングツリー	有効
プロトコル機能	
フォワーディングデータベース	300秒
エージング時間	
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G.仕様

項目	説明
品名	シャーシタイプ10M/100M/1000M レイヤ3 インテリジェントスイッチングハブ
型番	FML-1200
最大ポート数	96全ポート対応
ポート	100BASE-TX (1モジュール最大8ポート) 1000BASE-SX、LX、T (1モジュール最大2ポート) 100BASE-FX (1モジュール最大8ポート)
Autonegotiation	全ポート対応
AutoMDI	全ポート対応
LEDインジケータ	Link、Mode、ACT、FDX、FC、Power Primary、Diag、Release、AC、DC
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	12Gbps
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	8M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 :32768個 IPアドレス :65536個
VLANグループ数	最大2000個のVLANグループを構築可能
IPサブネット数	最大64個のIPサブネットグループを構築可能
プライオリティ対応	2-Level (IEEE 802.1p 準拠)

項目	説明
MIB	MIB2、EthernetMAU、Bridge、Private、RIP2 IP Forwarding OSPF、IGMP DUMRP (対応予定) IP Multicast Router (対応予定)
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 300 x 308.6 mm
重量	20.62kg
消費電力	200W
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
安全規格	cUL