CentreCOM 9100/8500 シリーズ
ユーザーガイド

ファームウェア V4.1

アライドテレシス株式会社
J613-M6673-00 Rev.B 990908

ご注意

- 本書に記載されている情報は、当社（アライドテレシス株式会社）が保有しています。無断で本書の一部または全体をコピー、転載することを禁じます。
- 当社は、予告なく本書の全体または一部を修正、改訂することがあります。
- 当社は、改良のため製品の仕様を予告なく変更することがあります。
- 本製品の内容またはその仕様に関連して発生した結果に関しては、いかなる責任も負いかねますのであらかじめご了承ください。

商標について

- CentreCOM はアライドテレシス株式会社の登録商標です。
- NetWare、Novell、IPX は、Novell, Inc の登録商標です。
- AppleTalk は、Apple Computer, Inc. の登録商標です。
- PACE は、3Com Corporation の商標です。
- その他、本書に記載されている商品名等は、各メーカーの商標または登録商標です。

マニュアルバージョン

- 1998 年 2 月　J613-M0348-00 Rev.A　初版（英語版、ファームウェア Ver.1）
- 1998 年 10 月　J613-M0348-01 Rev.A　第 2 版（日本語版、ファームウェア Ver.1）
- 1999 年 2 月　J613-M0348-02 Rev.A　全改版（ファームウェア Ver.2）
- 1999 年 6 月　J613-M6673-00 Rev.A　加筆訂正（ファームウェア Ver.2）
- 1999 年 9 月　J6130M6673-00 Rev.B　全改版（ファームウェア Ver4.1）

使用および取り扱い上の注意

本製品を安全に使用するために、以下の事項は必ず守ってください。
守られていない場合、感電や怪我、火災、故障の原因となります。

ケースを外さないでください。
本装置の内部には高電圧の箇所が存在します。感電の恐れがありますので、絶対にケースを外さないでください。ユーザーに必要な部品は内包されていません。

稲妻危険
稲妻が発生しているとき、ケーブルの配線などの作業を行わないでください。落雷により、感電する恐れがあります。

光ファイバーケーブル・コネクタを直視しない
光ファイバーケーブルの端面や機器側のコネクタなどを目で直視しないでください。強い光を通している場合、目に障害が発生する恐れがあります。

正しい電源を使ってください。
本装置は、AC100-120/200-240Vで動作します。ご使用の前に必ずご確認ください。なお、本装置に付属の電源ケーブルは100-120V用ですので、ご注意ください。

正しい電源ケーブルおよびコンセントを使用してください。
本装置に電源を供給する場合には、必ず電源電圧に適合した電源ケーブルをご使用ください。日本国内などで100Vでご使用になる場合は、本装置に付属の 電源ケーブルをご使用ください。電源ケーブルのプラグは、接地端子付きの3ピン電源コンセントに接続してください。不適切な 電源ケーブルや電源コンセントをご使用になった場合にお客様が被った損害についてはいかなる責任も負いかねます。

電源ケーブルは無理に折り曲げたり、引っ張ったり、ねじったりしないでください。また、圧力がかかりコードがつぶれてしまうような箇所に 電源ケーブルを敷設しないでください。

たこ足配線をしないでください。
テーブルタップをご使用になる場合、たこ足配線をしないでください。たこ足配線は、火災の原因になります。

通気口をふさがないでください。
本装置の通気口をふさがないでください。通気口をふさいだ状態で本装置を使用すると、加熱などにより故障、火災の恐れがあります。

取り扱いは丁寧に
落としたり、ぶつけたり、強いショックを与えないでください。

動作温度
本装置は、周囲温度 0 ～40 ℃の範囲でご使用ください。特に、本装置をラックなどに組み込んでご使用になる場合、換気には十分ご注意ください。

異物を入れないでください。
通気口から金属や液体などの異物を入れないでください。本体内部に異物が入ると火災、感電などの恐れがあります。

設置、ケーブル配線、移動は電源を抜いて
本装置の設置や移動、ケーブル配線などを行う場合は、必ず電源ケーブルを抜いた状態で行ってください。

次のような場所での使用や保管はしないでください。
- 直射日光の当たる場所
- 暖房器具の近くなどの高温になる場所
- 急激な温度変化のある場所 (結露するような場所)
- 湿気の多い場所や、水などの液体がかかる場所 (湿度 80 %以下の環境でご使用ください)
- 振動の激しい場所
- ほこりの多い場所や、ジュータンを敷いた場所 (静電気障害の原因になります)
- 腐食性ガスの発生する場所

日常のお手入れ
本装置の汚れは、乾いたやわらかい布でふきとってください。ベンジン、シンナーなどは使用しないでください。変形や変色の原因になります。

目次

10 ルーティングプロトコル

図目次

表目次

0　このマニュアルについて

このたびは、CentreCOM 9100/8500 シリーズをお買い上げいただき、誠にありがとうございます。

このマニュアルには、本製品の設置と設定に必要な情報が記載されています。よくお読みになり、適切な設置・設定を行った上で正しくご使用ください。また、お読みになった後も、本製品活用のためのリファレンスとしてご利用いただけますようお願い申し上げます。

なお、本書はバージョン 4.1 系のファームウェアに共通のことがらについて説明しています。各マイナーバージョン（4.1.10 など）に固有の情報については、製品付属の「リリースノート」をご覧ください。「リリースノート」の情報は、本書よりも優先されます。

0.1 対象読者と前提知識

本書は、ネットワーク機器の設置や設定を担当するネットワーク管理者を対象に書かれています。そのため、本書では下記の事柄に関する基本的な知識を前提としています。

- ローカルエリアネットワーク（LAN）
- イーサネット
- イーサネットにおけるスイッチングとブリッジング
- ルーティング
- IP（Internet Protocol）
- RIP と OSPF
- IP マルチキャスト
- DVMRP（Distance Vector Multicast Routing Protocol）
- PIM-DM（Protocol Independent Multicast-Dense Mode）
- Novell IPX
- SNMP

0.2 マニュアルの構成

本書は次のような構成になっています。

1　本製品の概要

2　設置と初期設定

3　基本的な管理操作

4　ポートの設定

5　バーチャル LAN（VLAN）

6　フォワーディングデータベース（FDB）

7　スパニングツリープロトコル（STP）

8　QoS（Quality of Service）

9　IP **ユニキャストルーティング**

10　ルーティングプロトコル

11　IP **マルチキャストルーティング**

12　IPX **ルーティング**

13　ERRP

14　アクセスポリシー

15　ステータス表示と統計機能

16　ファームウェアのアップグレードと設定の保存

A　トラブルシューティング

B　Web **インタフェース**

C　CentreCOM RPS1000 **接続時の補足事項**

D　出荷時の設定

E　製品仕様

F　ユーザーサポート

0.3 表記規則

本書では、次のような記号やマーク、表記規則を使用しています。

マーク類

このマークは、より詳細に知りたい方のためのポインタ、知っておくと便利な情報を示します。

このマークは、けがや機器の障害につながるおそれがあることを示します。

このマークは、けがや死亡につながるおそれがあることを示します。

画面表示 / 入力例

```
C9100:13# show fdb

Index    Mac                Vlan           Flags  Port List
-----------------------------------------------------------
0ff0: 0  ff:ff:ff:ff:ff:ff  Default(0001)   sm    CPU,1,19
1823: 0  08:00:4e:2b:f3:00  Default(0001)   sm    CPU
2bfb: 0  00:80:c7:01:cb:bd  Default(0001)   dm    1
373d: 0  01:80:c2:00:00:00    (0000)        sm    CPU

Total: 5 Static: 4 Perm: 0 Dyn: 1 Dropped: 0
FDB Aging time: 300 seconds
```

- **ユーザーが実際に入力する文字は、太字のタイプライタ体（Courier-Bold）で示します。**
- **画面に表示される文字は、タイプライタ体（**Courier**）で示します。**
- **入力例では、ほとんどの場合コマンドプロンプトを省略しています。**

キー表示

- **キーは、「**Esc**」のようにかぎかっこで囲んで表します。**
- **複数のキーを同時に押す場合は、「**Ctrl**」＋「**Alt**」＋「**Del**」のように表します。**

コマンド構文

コマンドの構文の表記法については、3-4 **ページの「記号について」で説明します。**

製品名

本書では、説明事項が CentreCOM 9100/8500 **シリーズの特定機種にのみ当てはまる場合は、**C9108**、**C8518**、**C8525**、**C8550 **のように製品の略称を明記しています。シリーズ全機種共通の事柄については、単に本製品と表記します。**

0.4 設定例について

本書では、本製品の多様な機能をわかりやすく説明するため、さまざまな設定例を掲載しています。これらの設定例では、IP **アドレスや** VLAN **名などに具体的な値を使用している場合がありますが、これらはあくまでも説明のためのサンプルです。本書の設定例を参考にしながら、実際にはお客様の環境における適切な値をご使用ください。**

1　本製品の概要

CentreCOM 9100/8500 シリーズは、ギガビットイーサネットに対応したレイヤー 3・インテリジェントスイッチです。本製品を導入することにより、既存のイーサネット / ファーストイーサネット環境の資産を活かしたまま、スムーズにギガビット環境を構築できます。

1.1 製品ラインナップ

本シリーズは、次の各モデルで構成されています。

表 1-1：製品ラインナップ

	SX モデル		LX モデル	
	レイヤー 3	レイヤー 2	レイヤー 3	レイヤー 2
C9108 シリーズ	C9108SX	なし	C9108LX	なし
C8518 シリーズ	C8518SX	なし	C8518LX	なし
C8525 シリーズ	C8525SX-L3	C8525SX-L2	C8525LX-L3	C8525LX-L2
C8550 シリーズ	C8550SX-L3	C8550SX-L2	C8550LX-L3	C8550LX-L2

SX モデルと LX モデルでは、モジュラーポートに装着されている GBIC モジュールが異なります。さらに、C8525 と C8550 にはレイヤー 2（L2）モデルとレイヤー 3（L3）モデルが用意されています。レイヤー 2 モデルは「ベーシック L3」モデルとも呼ぶべきもので、レイヤー 3 機能は基本的なもの（スタティックルーティングと RIP）に限られています。ただし、別売のライセンスキー（L3Key-85）をご購入いただくことで、レイヤー 3 モデル（「フル L3 モデル」）にアップグレードできます。

各モデルのポート構成については、1-9 ページの「ポート構成」をご覧ください。

ライセンスキーの使用方法については、キー付属のドキュメントをご覧ください。

1.2 特徴

本製品には次のような特徴があります。

- ノンブロッキングアーキテクチャによる全ポートワイヤスピードでのパケット送受信
- リダンダントパワーサプライ（RPS1000、オプション）による電源の二重化
- リダンダントギガビットポートによる冗長的なバックボーン構成（C9108 を除く）
- オートネゴシエーションによるフルデュプレックス / ハーフデュプレックス自動認識（10/100M ポートのみ）
- 複数のポートを束ねて使用できるロードシェアリング機能
- 任意のトラフィックを指定ポートにコピーするポートミラーリング機能
- ポート、プロトコル、802.1Q タグによるバーチャル LAN（VLAN）
- GVRP による VLAN 自動登録機能
- スパニングツリープロトコル（IEEE 802.1D）－ 複数の STPD を設定可能
- QoS（Quality of Service）－ IP アドレス、MAC アドレス、パケットプライオリティ、ポート、VLAN 単位で送出トラフィックにサービス品質レベルの設定が可能
- サブネット内 QoS（IQS）－ 同一 VLAN 内のスイッチドトラフィックにも IP QoS を適用可能
- ワイヤスピードの IP ユニキャストルーティング
- 同一物理ポート上に複数の論理 IP サブネットを作成する IP マルチネット機能
- DHCP/BOOTP リレー機能
- UDP ブロードキャストフォワーディング
- RIP バージョン 1 および 2
- OSPF（Open Shortest Path First）－ NSSA（準スタブエリア）、ASBR（AS 境界ルータ）にも対応
- ワイヤスピードの IP マルチキャストルーティング
- IGMP スヌーピングによるレイヤー 2 レベルでの IP マルチキャストトラフィック制御
- DVMRP（Distance Vector Multicast Routing Protocol）
- PIM-DM（Protocol Independent Multicast-Dense Mode）
- IPX ルーティング － Ethernet Ver2、IEEE 802.2、802.3、SNAP の各フレームタイプに対応。IPX/RIP、IPX/SAP にも対応
- アクセスポリシーによるルーティング情報の制御
- コンソール端末から使用可能なコマンドラインインタフェース（CLI）を装備
- Telnet による CLI へのアクセスが可能

- Web ベースの管理インタフェースを内蔵
- SNMP（Simple Network Management Protocol）による管理が可能
- RMON によるリモートモニタリング機能
- ERRP（Enterprise Router Redundancy Protocol）によるデフォルトゲートウェイ（ルータ）の多重化
- 複数のサブVLAN 間でデフォルトゲートウェイアドレスを共有し、IP アドレススペースの有効活用をはかる VLAN アグリゲーション機能
- RADIUS サーバを利用したリモート認証に対応（RADIUS クライアント機能）
- DNS クライアント機能により、一部コマンドでホスト名による指定が可能
- タイムサーバを利用してシステムクロックを自動修正する SNTP クライアント機能
- CLI からの設定変更をログに記録することが可能
- TFTP によるファームウェアのアップグレード
- TFTP による設定ファイルのアップロード / ダウンロード

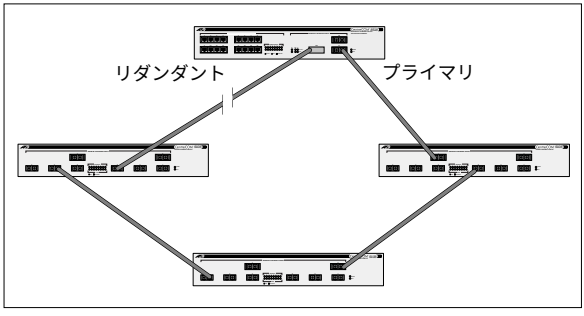
フルデュプレックス

本製品は、すべてのポートでフルデュプレックス通信が可能です。フルデュプレックスモードでは、フレームの送信と受信を同時に行うことができるため、事実上帯域幅が 2 倍になります。10/100Mbps ポートはすべて、オートネゴシエーションによるフルデュプレックス / ハーフデュプレックスの自動認識が可能です。

リダンダントギガビットポート

C8518、C8525、C8550 は、オプションのリダンダントギガビットポートを備えています。リダンダントポートに GBIC モジュール（別売）を装着することにより、図 1-1 のようなデュアルホーム構成が可能です。

図 1-1：デュアルホーム構成



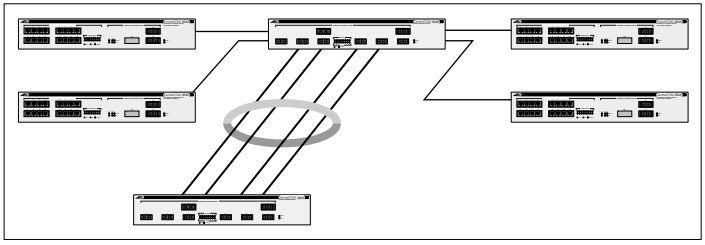
通常、リダンダントポートは待機状態にあり使用されませんが、プライマリポートのリンクがダウンすると、リダンダントポートが自動的にアクティブになります。プライマリポートで通信が再開されると、リダンダントポートは再び待機状態になります。

ただし、プライマリポートとリダンダントポートを同時に使用することはできません。ロードシェアリンググループに参加しているプライマリポートが通信できない状態になると、リダンダントポートがアクティブになります。

ロードシェアリング

ロードシェアリングは、複数の物理ポートを束ねて使用することにより、スイッチ間の帯域幅を拡大する機能です。また、束ねたポート（ロードシェアリンググループ）のいずれかに障害が発生した場合でも、残りのポートで通信を継続できるため、耐障害性の向上にもつながります。このアルゴリズムを使用すると、複数の物理ポートを単一の論理ポートとして使用することができます。これにより、ロードシェアリンググループは VLAN から単一の仮想ポートとして認識されます。また、パケットの順序もこのアルゴリズムによって保証されます。

図 1-2：ロードシェアリング構成



ロードシェアリング機能の詳細については、4-4 ページの「ロードシェアリング機能」をご覧ください。

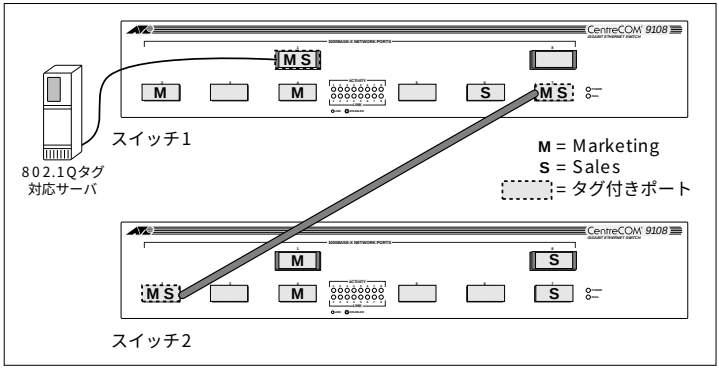
バーチャル LAN（VLAN）

VLAN 機能とは、スイッチの設定によって論理的にブロードキャストドメインを分割する機能です。VLAN 導入の利点としては、次のようなものが挙げられます。

- **ブロードキャストトラフィックの抑制** ― ある VLAN に所属する機器が送出したブロードキャストフレームは、同じ VLAN にしか届きません。
- **セキュリティの向上** ― VLAN 間ルーティングの設定を行わない限り、異なる VLAN 間の通信はできません。
- **ネットワーク機器の取り替えや移動が容易に** ― ある VLAN（たとえば *marketing*）に所属するデバイスを地理的に離れた別のポートにつなぎかえた場合でも、設定コマンドを使って新しいポートの所属を VLAN *marketing* に変更するだけですみます。

本製品では、ポートおよびプロトコルベースの設定に加え、802.1Q タグを利用したタグ VLAN も設定可能です。さらに、サブ VLAN 間でデフォルトゲートウェイアドレスを共用し、IP アドレススペースの有効活用をはかる VLAN アグリゲーション機能や、同一ポート上に複数の IP サブネットを作成する IP マルチネット機能にも対応しています。

図 1-3：タグ VLAN



VLAN の詳細については、第 5 章「バーチャル LAN（VLAN）」をご覧ください。IP マルチネットについては、第 9 章「IP ユニキャストルーティング」をご覧ください。

スパニングツリープロトコル（STP）

本製品は、IEEE 802.1D 準拠のスパニングツリープロトコル（STP）に対応しています。STP は、ネットワーク経路を二重化して耐障害性を高めるブリッジベースのメカニズムで、次のような働きをします。

- メイン経路の稼働中は、バックアップ経路をブロックする。
- メイン経路の障害発生時には、バックアップ経路を使用する。

さらに、本製品ではスパニングツリードメイン（STPD）を 64 個まで作成できます。

スパニングツリープロトコルの詳細については、第 7 章「スパニングツリープロトコル（STP）」をご覧ください。

QoS（Quality of Service）

QoS は、ポートから送出されるトラフィックに最小 / 最大帯域幅や優先度といったサービス品質レベルを設定する機能です。サービスレベルは、QoS プロファイルという形で定義し、宛先 IP アドレスや送信元ポートといった各種トラフィックグループに対して適用します。デフォルトでは、すべてのトラフィックに QoS プロファイル *qp1* が割り当てられていますが、各トラフィックの要件にあわせて QoS プロファイルは修正や追加が可能です。

QoS の詳細については、第 8 章「QoS（Quality of Service）」をご覧ください。

IP ユニキャストルーティング

本製品では、それぞれ仮想的なルータインタフェースとして設定された VLAN 間の IP ルーティングが可能です。ルーティング方式としては、スタティックルーティングとダイナミックルーティングの両方をサポートします。対応しているルーティングプロトコルは、以下のとおりです。

- RIP バージョン 1
- RIP バージョン 2
- OSPF

IP ユニキャストルーティングの詳細については、第 9 章「IP ユニキャストルーティング」をご覧ください。

IP マルチキャストルーティング

IP マルチキャストは、単一のホストから特定多数のホスト（ホストグループ）に IP パケットを送信する一対多通信機能です。本製品では、スタティックルーティングとダイナミックルーティング（DVMRP または PIM-DM）の両方をサポートしています。

IP マルチキャストルーティングの詳細については、第 11 章「IP マルチキャストルーティング」をご覧ください。

IPX ルーティング

本製品では、IPX ネットワーク番号を割り当てた VLAN 間のルーティングが可能です。Ethernet Version2、IEEE 802.3、IEEE 802.2、SNAP の各フレームタイプに対応しており、次のような機能をサポートしています。

- IPX / RIP
- IPX / SAP

IPX ルーティングはソフトウェアによって処理されるため、IP のようなワイヤスピードルーティングは実現できません。IPX ルーティングの詳細については、第 12 章「IPX ルーティング」をご覧ください。

アクセスポリシー

アクセスポリシーとは、ルーティング情報の広告および学習にフィルタをかけることで、セキュリティの向上（または帯域の制御）をはかる機能です。アクセスポリシーは、制御対象の IP アドレスとアクセスの許可 / 拒否をアクセスプロファイルに定義し、ルーティングプロトコルの機

能に割り当てることによって形成されます。アクセスポリシーは、RIP、OSPF、DVMRP、PIM-DM に対して適用できます。

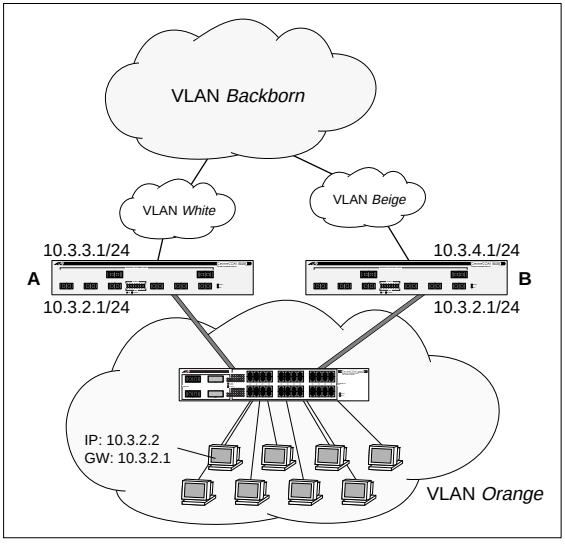
アクセスポリシーの詳細については、第 14 章「アクセスポリシー」をご覧ください。

ERRP（Enterprise Router Redundancy Protocol）

ERRP は、複数の C9100/8500 を連携させることにより、インターネットワーク上での通信に不可欠なデフォルトゲートウェイ（ルータ）を多重化し、冗長性のある信頼性の高いネットワークを構築するためのプロトコルです。ERRP ルータは、IP/IPX アドレスと MAC アドレスを共有し、クライアントホストに対して 1 台のルータであるかのように見せかけます。マスタールータに障害が発生すると、待機状態のスレーブルータが役割を引き継ぎ、ネットワークを切れ目なく運用させます。連携する複数の ERRP ルータはアドレスを共有しているため、クライアントのデフォルトゲートウェイアドレスを変更したり、ARP キャッシュを更新したりする手間がありません。また ERRP ルータの配下にレイヤー 2 の C9100/8500 を配置すると、ERRP Awareness という機能により、より高速なマスター・スレーブの切り替えを実現できます。

ERRP の詳細については、第13 章「ERRP」をご覧ください。

図 1-4：ERRP 設定例

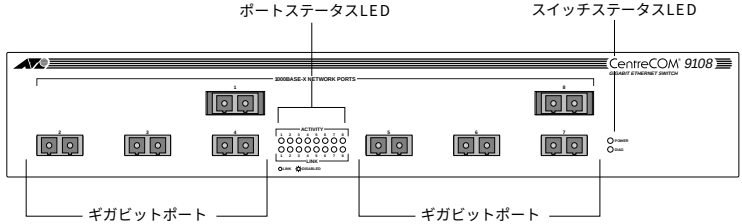


1.3 各部の名称と機能

前面図

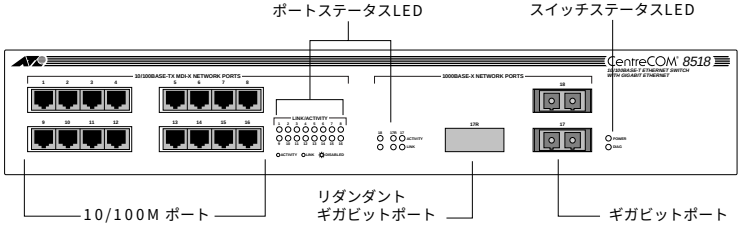
C9108 **は、ギガビットポートを** 8 **ポート装備したバックボーンスイッチです。ポート** 2 **〜** 7 **は固定式の** SC **コネクタ、ポート** 1 **と** 8 **はモジュラー式の** GBIC **スロットです。**

図 1-5：C9108 前面図



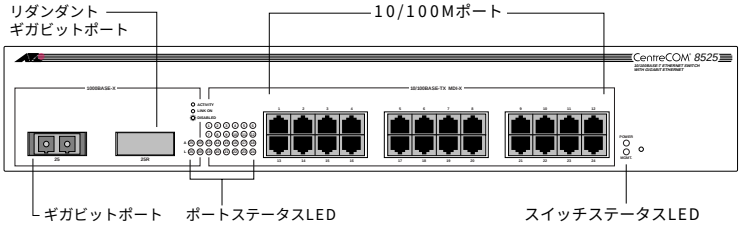
C8518 **は、**10BASE-T / 100BASE-TX **自動認識ポート** 16 **個とギガビットポート** 2 **個（うち** 1 **つはリダンダントポート付き）を装備したセグメントスイッチです。**

図 1-6：C8518 前面図



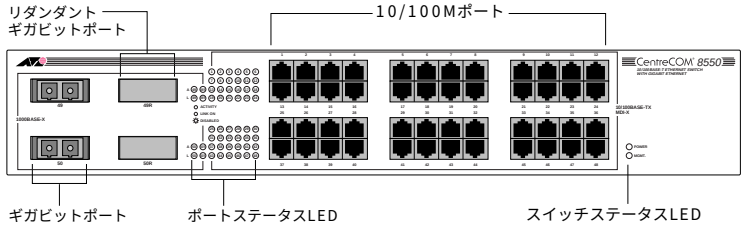
C8525 **は、**10BASE-T / 100BASE-TX **自動認識ポート** 24 **個とギガビットポート** 1 **個（リダンダントポート付き）を装備したワークグループスイッチです。**

図 1-7：C8525 前面図



C8550 は、10BASE-T / 100BASE-TX 自動認識ポート 48 個とギガビットポート 2 個（リダンダントポート付き）を装備したエンタープライズデスクトップスイッチです。

図 1-8：C8550 前面図



対応するケーブルと伝送距離については、2-4 ページの「ネットワークケーブルと最長伝送距離」をご覧ください。

ポート構成

本製品のポート構成を表 1-2 に示します。

表 1-2：本製品のポート構成

	ギガビットポート			
モデル名	**固定式 1000BASE-SX**	**GBIC ポート**	**リダンダント GBIC ポート**	**10BASE-T/ 100BASE-TX**
C9108SX	6	2（GBIC-SX）		
C9108LX	6	2（GBIC-LX）		
C8518SX		2（GBIC-SX）	1（GBIC 未装着）	16
C8518LX		2（GBIC-LX）	1（GBIC 未装着）	16
C8525SX		1（GBIC-SX）	1（GBIC 未装着）	24
C8525LX		1（GBIC-LX）	1（GBIC 未装着）	24
C8550SX		2（GBIC-SX）	2（GBIC 未装着）	48
C8550LX		2（GBIC-LX）	2（GBIC 未装着）	48

LED

表 1-3 **に、本製品の** LED **表示をまとめます。**

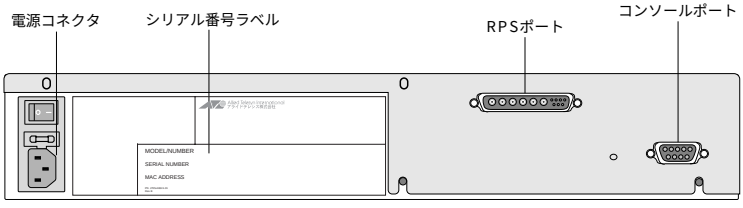
表 1-3：LED 表示

LED	色	意味
POWER	緑（点灯）	電源が正常に供給されている。
	橙（点灯）	電源 / ファンの障害または過熱を示す。
DIAG(MGMT)	緑（点滅）	
	• ゆっくり	正常に動作している。
	• はやい	電源投入時テスト（POST）の実行中、またはファームウェアのダウンロード中であることを示す。
	橙（点灯）	POST エラーが発生した。
10/100M ポート		
LINK/ACTIVITY	橙（点灯）	フレームが送受信されている。
	緑（点灯）	正常にリンクされている。ポートはイネーブル状態。
	緑（点滅）	正常にリンクされている。ポートはディセーブル状態。
	消灯	リンクされていない。
ギガビットポート		
ACTIVITY(A)	橙（点灯）	フレームが送受信されている。
	消灯	無通信状態。
LINK(L)	緑（点灯）	正常にリンクされている。ポートはイネーブル状態
	緑（点滅）	正常にリンクされている。ポートはディセーブル状態。
	消灯	リンクされていない。

背面図

図 1-9 **に本製品の背面図を示します。**

図 1-9：本製品の背面図



- **電源コネクタ** ― AC 電源ケーブルを接続します。本製品は、AC 100-120 / 200-240 V で動作しますが、同梱のケーブルは AC 100-120V 用ですのでご注意ください。
- **シリアル番号ラベル** ― 本製品のシリアル番号、MAC アドレス、MODEL No が記載されています。
- **コンソールポート** ― 本製品の管理に使うコンソールを接続します。コネクタは、RS232C の 9 ピンオス D タイプです。本製品には、PC / AT 互換機などとの接続に使用する 9 ピンメス ― 9 ピンメスのクロスケーブルが付属しています。
- **RPS ポート** ― 別売のリダンダントパワーサプライ（二重化電源装置）、CentreCOM RPS1000 を接続します。RPS1000 は、AC 供給源の停電、電源ケーブルの断線・接触不良、電源ユニットの故障といった電源障害による本製品の機能停止を防ぎます。また、負荷分散により電源ユニットの長寿命化を実現します。接続には、RPS1000 付属の専用ケーブルを使用します。

C8525 と C8550 の RPS ポートは、図 1-9 よりも低い位置（コンソールポートと水平になる位置）にあります。

RPS1000 の接続時は、SNMP やコマンドラインインタフェース、Web インタフェースを通じて、RPS の動作状態（電源およびファン。Web インタフェースでは電源状態のみ）を監視できます。詳細については、付録 C「CentreCOM RPS1000 接続時の補足事項」をご覧ください。

2　設置と初期設定

この章では、本製品の設置および初期設定の方法について説明します。

2.1 同梱品一覧

最初に以下の同梱品を確認してください。万が一欠品や不良品などがございましたら、お買い求めの販売店までご連絡ください。

- CentreCOM 9100/8500 シリーズ本体
- GBIC モジュール（GBIC モジュールの個数については、1-9 ページの「本製品のポート構成」の「GBIC ポート」欄をご覧ください）
- AC 電源ケーブル
- RS232C ケーブル（9 ピンメス－9 ピンメス、クロスケーブル）
- ゴム脚
- CentreCOM 9100/8500 シリーズ ユーザーガイド（本書）
- CentreCOM 9100/8500 シリーズ クイックリファレンスガイド
- CentreCOM 9100/8500 シリーズ リリースノート
- 19 インチラックマウントキット
- 製品保証書
- ユーザー登録はがき

2.2 設置するときの注意

本製品は安定した水平な場所に設置するか、EIA 規格の標準 19 インチラックに収納します。ラックに取り付けるときは、付属のラックマウントキットを使用してください。

設置に際しては、以下の点にご注意ください。

- 手が届きやすくケーブルの接続が容易な場所に設置してください
- 本製品はオフィスなど室内での使用を前提として設計されています。屋外には設置しないでください

- 電源ケーブルやメディアケーブルに無理な力が加わるような配置は避けてください
- テレビ、ラジオ、無線機のそばには設置しないでください
- 水分や湿気が機器内に入る恐れがない場所を選んでください
- 周囲に通気を妨げるものがないか、通気口がふさがれていないか確認してください。本体の周りには最低 25mm のスペースを確保してください
- 本体の上に物を置かないでください
- 水平な場所に設置する場合は、5 台以上積み重ねないでください

本製品の設置や保守を始める前に、必ず iii ページの「使用および取り扱い上の注意」をよくお読みください。

2.3 設置

ラックに取り付ける場合

本製品は EIA 規格の 19 インチラックに取り付けることができます。高さは 2U です。

ラックマウントキットを使って、本製品を机の下にぶらさげたり、壁に取り付けたりしないでください。

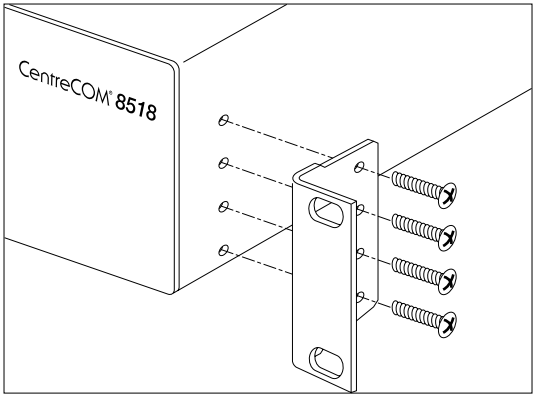
1 上下が正しいことを確認し、前面が見えるようにして水平な場所に置きます。

2 本体側面のネジを取り外します。取り外したネジは、手順4 で使用するのでなくさないようにしてください。

3 マウンティングブラケットを本体側面のネジ穴にあわせます。

4 図 2-1 を参考に、4 個のネジをしっかりと締めます。ネジ溝にあったネジまわしを使用してください。

図 2-1：マウンティングブラケットの取り付け



5 反対側のネジに対して、手順 2 〜手順 4 を繰り返します。

6 本体を 19 インチラックに挿入し、別途用意した適切なネジでしっかりと固定します。このとき、通気口がふさがれないように注意してください。

マウンティングブラケットを取り付けるときは必ず本体付属のネジを使用し、19 インチラックには適切なネジを用いて確実に固定してください。固定が不十分な場合、落下などにより重大な事故が発生する恐れがあります。

本製品を設置するときは、必ずケーブル類を抜いた状態で行ってください。

水平な場所に設置する場合

本体下面の四隅の印にあわせて、ゴム脚を取り付けてください。ゴム脚は、衝撃を吸収するクッションの役割を果たします。設置場所は、水平な安定した場所で、通気口がふさがれないような場所を選んでください。

積み重ねる場合

本製品は最高 4 台まで積み重ねて設置できます。

積み重ねて使用するときは、本体下面四隅の印にあわせてゴム脚を取り付けてください。積み重ねるときは、各機器の角がきちんと揃うようにしてください。

2.4 接続

ネットワークケーブルと最長伝送距離

表 2-1 に、本製品で使用可能なネットワークケーブルと伝送距離の一覧を示します。

表 2-1：ネットワークケーブルと最長伝送距離

標準	ケーブルタイプ	周波数帯域 (Mhz/Km)	最長伝送距離 (m)
1000BASE-SX	50/125µm マルチモード光ファイバー	400	500
	50/125µm マルチモード光ファイバー	500	550
	62.5/125µm マルチモード光ファイバー	160	220
	62.5/125µm マルチモード光ファイバー	200	275
1000BASE-LX	50/125µm マルチモード光ファイバー	400	550
	50/125µm マルチモード光ファイバー	500	550
	62.5/125µm マルチモード光ファイバー	500	550
	10µm シングルモード光ファイバー		5000*
100BASE-TX	UTP ケーブル（カテゴリ 5）		100
10BASE-T	UTP ケーブル（カテゴリ 3 以上 **）		100

* IEEE802.3z clause 38.11 の規格をすべて満たした接続条件下では、10000m まで延長可能。

** 100BASE-TX にアップグレードするときに、余分な経費やトラブルが発生するのを避けるため、最初からカテゴリ 5 のケーブルをご使用になることをお勧めします。

1000BASE-SX および 1000BASE-LX の詳細については、IEEE 802.3z をご参照ください。

コンソールの接続

コンソールポートには、本製品の管理に使用する VT100 互換のコンソール（または端末エミュレータ）を接続します。コンソールポートの設定は、次のとおりです。

表 2-2：コンソールポートの設定

通信速度	9600 ボー
データビット	8
ストップビット	1
パリティ	なし
フロー制御	XON/XOFF

コンソールポートに接続する端末は、スイッチ側と同じ設定にしてください。端末の設定方法については、端末付属のマニュアルをご覧ください。

本製品には、9 ピンメス－ 9 ピンメスのクロスケーブルが同梱されています。ケーブルを自作するときは、表 2-3 のピン配置を参考にしてください。

表 2-3：コンソールコネクタのピン配置

機能	ピン番号
TXD (データ送信)	3
RXD (データ受信)	2
GND (接地)	5

図 2-2 に、9 ピン－ 25 ピンクロスケーブルの結線図を示します。

図 2-2：9 ピン－ 25 ピン クロスケーブルの結線

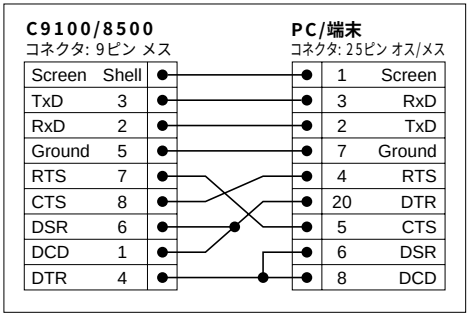
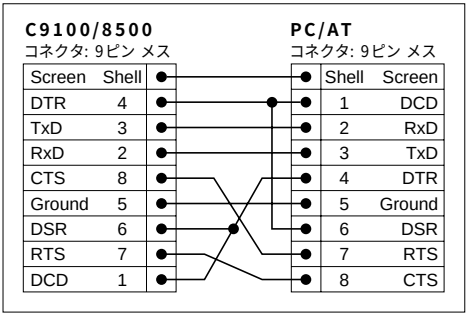


図 2-3 に、9 ピン－ 9 ピン クロスケーブルの結線図を示します。

図 2-3：9 ピン－ 9 ピン クロスケーブルの結線



電源ケーブルの接続

必要に応じ、オプションのリダンダントパワーサプライ RPS1000 を接続します。接続方法については、RPS1000 のマニュアルを参照してください。

AC 電源ケーブルを本体背面の電源コネクタに接続します。

AC 電源ケーブルをアース付きの電源コンセントに接続します。なお、付属の電源ケーブルは AC100-120V 用ですのでご注意ください。

2.5 起動

電源投入

AC 電源ケーブルが正しく接続されていることを確認し、on/off スイッチを on の位置にセットします。

電源投入時テスト（POST）による確認

電源を投入すると、電源投入時テスト（POST）が実行されます。

POST の実行中は、すべてのポートが一時的にディセーブル状態になり、ACTIVITY LED が消灯、POWER LED が点灯、DIAG（MGMT）LED は速い（毎秒約 2 回）点滅状態になります。

POST が正常に終了すると、DIAG LED の点滅がゆっくりになります（毎秒約 1 回）。POST エラーが発生した場合は、DIAG LED が橙色に点灯します。

LED の詳細については、1-10 ページの「LED」をご覧ください。

最初のログイン

POST が完了すると、本製品は動作状態となりログインできるようになります。最初のログインでは、あらかじめ定義されている VLAN *default* の IP アドレスを設定します。IP アドレスを設定することにより、Telnet による CLI へのアクセス、Web インタフェースへのアクセス、SNMP マネージャによるアクセスができるようになります。

IP アドレスを手動で設定するには、次の手順にしたがいます。

1 コンソールポートに端末（または端末エミュレータがインストールされたPCまたはワークステーション）を接続します。

2 端末画面にログインプロンプトが現れるまで、「Return」キーを数回押します。

3 **ログインプロンプトが表示されたら、デフォルトで用意されている管理者レベルのユーザ名** *admin* **でログインします。**

```
login: admin
```

管理者レベルのユーザは、本製品のすべての機能を使用できます。

ユーザレベルの詳細については、3-7 ページの「ユーザアカウント」をご覧ください。

4 **パスワードプロンプトで「**Return**」キーを押します。**

デフォルトユーザの *admin* **にはパスワードが設定されていません。ログインに成功すると、コマンドラインの先頭にスイッチの識別名（例：**C9100**）が表示されます。**

5 VLAN *default* **の** IP **アドレスとサブネットマスクを設定します。**

```
config vlan default ipaddress 123.45.67.8 255.255.255.0
```

変更は直ちに有効となります。

6 **変更が再起動後も有効になるよう、設定内容を保存します。**

```
save
```

設定内容の保存方法については、16-1 ページの「再起動」をご覧ください。

7 **設定が完了したら、ログアウトします。**

```
logout（または quit）
```

3 回ログインに失敗すると、ログインの受け付けが一時的に停止されます。ログインプロンプトが再び表示されるまで、数分間お待ちください。

3　基本的な管理操作

この章では、本製品の管理インタフェースの概要とコマンドラインインタフェースによる基本的な管理操作について説明します。

3.1 管理インタフェース

本製品は次の管理インタフェースを持っています。

- **コマンドラインインタフェース(CLI)** － UNIX のシェルや MS-DOS / Windows のコマンドプロンプトとよく似たキャラクタユーザインタフェース（CUI）で、もっとも基本的な管理インタフェースです。コンソールまたは Telnet 経由でアクセスします。
- **Web インタフェース** － HTML および HTTP プロトコルを利用したグラフィカルユーザインタフェース（GUI）です。頻繁に使用される管理コマンドを直感的な操作で実行できます。Netscape Navigator や Microsoft Internet Explorer などの Web ブラウザを使ってアクセスします。
- **SNMP** － SNMP エージェントを介して本製品内の MIB 変数にアクセスし、さまざまな設定や状態確認を行います。SNMP 対応のネットワークマネージャソフトウェアを使ってアクセスします。

管理セッションは、同時に複数開くことができます（コンソールセッション× 1、Web セッション× 1、Telnet セッション× 8）。

Telnet、HTTP、SNMP 経由で本製品の管理機能にアクセスするには、事前に本製品の IP アドレスやコミュニティ名などを設定しておく必要があります。そのため、初めて本製品を使用する場合は必ずコンソールからアクセスすることになります。詳しくは、2-6 ページの「最初のログイン」をご覧ください。

本製品のもっとも基本的な管理インタフェースは CLI です。したがって、本書では CLI コマンドを中心に、各種機能の設定方法を説明していきます。Web インタフェースの設定および使用方法については、3-15 ページの「Web インタフェース」および付録 B「Web インタフェース」を、SNMP の基本設定については3-16 ページの「SNMP による管理」をそれぞれをご覧ください。

3.2 コマンドラインインタフェースの基本操作

コマンドの入力方法

ここでは、CLI におけるコマンド入力の手順について説明します。

コマンドの入力方法は次のとおりです。

1 コマンド入力前に、適切なユーザレベルでログインしているかどうかを確認してください。

設定コマンドを実行するには、通常管理者レベルでログインする必要があります。

2 コマンド名を入力します。

コマンドにオプションやパラメータが必要な場合は手順 a へ、必要ない場合は手順 3 に進んでください。

a: コマンドラインオプションは、コマンド名の後に記述します。

b: コマンドにパラメータを渡すときは、パラメータ名とその値をペアで指定します。値の部分には、数値、文字列、アドレスなどが入ります。

3 コマンドをすべて入力したら、「Return」キーを押します。

コマンドラインの先頭にアスタリスク（*）が表示されることがあります。これは、まだ保存していない変更点があることを示しています。設定内容の保存方法については、16-2 ページの「設定の保存」をご覧ください。

構文ヘルパー

コマンドラインインタフェースには、ユーザのコマンド入力を補助する構文ヘルパーが用意されています。コマンドの構文を思い出せないときは、覚えている範囲でコマンドを入力して「Return」キーを押せば、構文ヘルパーが足りないオプションの候補を示してくれます。

また、コマンドを間違って入力した場合も、構文ヘルパーの補助が受けられます。

コマンド名ヘルプ機能

コマンドラインインタフェースでは、コマンド名の補完機能を利用できます。コマンド名の先頭部分だけを入力して「Tab」キーを押すと、入力途中のコマンド名が補完され、使用可能なオプションの一覧が表示されます。コマンド名の補完後、カーソルはコマンドラインの末尾に移動します。

コマンドの短縮形

コマンド名、パラメータおよびその値は、一意に識別可能な範囲で短縮可能です。たとえば、`show switch` コマンドは、`sh sw` と略記することができます。

本書では、基本的にコマンド名やキーワードを完全な形で表記していますが、config(ure) コマンドのように省略形で表記しているものもあります。あらかじめご了承ください。

コマンドショートカット

create コマンドで作成するコンポーネント（VLAN やユーザアカウント）には、一意に識別可能な名前を付ける必要があります。こうすることにより、作成したコンポーネントの設定を行うときに、コンポーネントの種類を示すキーワード（vlan や account）を省略できるようになります。たとえば、新しい VLAN を作成するときは、次のようにして他と重複しないような名前を付けます。

```
create vlan engineering
```

いったん名前（この例では *engineering*）を付けたら、それ以降キーワード vlan は省略できます。たとえば、

```
config vlan engineering delete ports 1-3,6
```

と入力する代わりに、次のような指定が可能です。

```
config engineering delete ports 1-3,6
```

ポートの指定方法

ポート番号を示す <portlist> パラメータには、複数のポートを一度に指定できます。たとえば、ポート 1 ～ 3 を指定するには、次のようにハイフンを使います。

```
ports 1-3
```

6 と 8 のように連続していない数は、次のようにカンマで区切って指定します。

```
ports 1-3,6,8
```

ネットマスクの指定方法

ネットマスクを示す <mask> パラメータは、255.255.255.0 のような 10 進ドット表記とマスク長の両方による指定が可能です。マニュアル中で <mask> と記述されている部分には、どちらの形式を使ってもかまいません。たとえば、VLAN *default* に IP アドレスとサブネットマスクを設定する場合、以下の例のどちらも有効となります。マスク長を指定する場合は、IP アドレスとマスク長の間をスラッシュ（/）で区切ることに注意してください。

```
config vlan default ipaddress 123.45.67.8 255.255.255.0
config vlan default ipaddress 123.45.67.8 / 24
```

命名規則

設定に使用するコンポーネントには、他と重複しないような名前を付ける必要があります。コンポーネント名に使用できる文字は基本的に英数字のみです。また、名前の先頭はアルファベットでなくてはなりません。

記号について

表 3-1 にコマンド解説に使用する記号の一覧を示します。

表 3-1：コマンド解説の記号

記号	意味
< >	変数を示します。たとえば、次の例では、 `config vlan <name> ipaddress <ipaddress>` <name>の部分に VLAN 名を、<ipaddress>の部分には IP アドレスを指定します。カッコそのものは入力しないでください。
[ ]	カッコで囲まれた値やキーワードのうち、必ずどれか一つを指定しなくてはならないことを示します。 `disable ports [<portlist> | all]` この例では、[<portlist> | all] の部分に、ポート番号かキーワード all のどちらかを指定します。カッコそのものは入力しないでください。
|	| で区切られた選択肢のうち、どれか一つだけを入力します。 `config snmp community [readonly | readwrite] <string>` この例では、readonly か readwrite のどちらかを指定します。| そのものは入力しないでください。
{ }	省略可能な値またはキーワードを示します。 `show vlan {<name>}` この例では、VLAN 名 <name> を省略することができます。省略時の動作はコマンドによって異なりますが、多くのコマンドでは関連するすべてのコンポーネントに対して処理が行われます。カッコそのものは入力しないでください。

コマンドライン編集キー

表 3-2 にコマンドライン編集に使うキーの一覧を示します。

表 3-2：コマンドライン編集キー

キー	機能
「Backspace」	カーソルの直前にある文字を削除し、カーソル位置以降の文字を 1 つずつ左に移動します。

表 3-2：コマンドライン編集キー

キー	機能
「Ctrl」＋「D」	カーソル位置の文字を削除し、カーソル位置より後ろの文字を 1 つずつ左に移動します。
「Ctrl」＋「K」	カーソル位置から行末までを削除します。
「←」	カーソルを左に移動します。
「→」	カーソルを右に移動します。
「Ctrl」＋「A」	カーソルを行の先頭に移動します。
「Ctrl」＋「E」	カーソルを行末に移動します。
「Ctrl」＋「L」	画面を消去し、カーソルを行の先頭に移動します。
「Ctrl」＋「U」	カーソル位置から行の先頭までを削除します。
「Ctrl」＋「W」	カーソル位置の直前にある単語を削除します。
「↑」	コマンド履歴内の直前のコマンドを表示し、カーソルをコマンドラインの末尾に移動します。
「↓」	コマンド履歴内の次のコマンドを表示し、カーソルをコマンドラインの末尾に移動します。

ページャー機能

CLI コマンドの出力量が多いときは、ページャー機能の働きにより、画面表示がページ単位で一時停止します。コマンド出力をキャプチャしたいときなどは、次のコマンドでページャー機能をディセーブルにします（デフォルトはイネーブル）。

```
disable clipaging
```

再度ページャー機能をイネーブルにするには、次のコマンドを実行します。

```
enable clipaging
```

コマンド履歴

入力したコマンドはコマンドバッファに 49 個まで記憶されます。コマンド履歴を表示するには、次のコマンドを実行します。

```
history
```

3.3 一般的なコマンド

表 3-3 に一般的な管理コマンドを示します。各機能に対応する特殊なコマンドについては、後の各章で解説します。

表 3-3：一般的な管理コマンド

コマンド名	機能
create account [admin | user] <username> {encrypted} {<password>}	ユーザアカウントを作成します。`encrypted` オプションは、ASCII 設定ファイルのアップロード / ダウンロード時に本製品が使用するもので、ユーザが指定するものではありません。
create vlan <name>	VLAN を作成します。
config account <username> {encrypted} {<password>}	指定したユーザアカウントのパスワードを変更します。パスワードは 4 ～ 12 文字で指定します。ユーザアカウントとパスワードは大文字小文字が区別されますのでご注意ください。
config banner	ログインプロンプト画面の前に表示されるバナー文字列を設定します。設定中は、行の先頭で「Return」キーを押すと設定が完了し、新しいバナーが有効になります。バナーの大きさは 80 × 24 文字までです。バナーを削除したいときは、何も入力せずに 1 行目の先頭で「Return」キーを押します。
config ports [<portlist> | all] auto off {speed [10 | 100]} duplex [half | full]	ポートの通信速度と通信モード（フルデュプレックス / ハーフデュプレックス）を設定します。
config time <date> <time>	システムの日付と時刻を設定します。書式は次のとおりです。 `mm/dd/yyyy hh:mm:ss` 時刻は 24 時間形式で指定します。日付を 2036 年以降に設定することはできません。
config timezone <gmt_offset> {autodst | noautodst}	タイムゾーンの設定を行います。`<gmt_offset>` には、グリニッジ標準時（GMT）とローカル時間の差を分で指定します。GMT より早い場合は + を、遅い場合は - を付けてください。夏時間（Daylight Saving TIme）の自動調整を行いたい場合は `autodst` オプション（デフォルト）を、行わない場合は `noautodst` オプションを指定します。
config vlan <name> ipaddress <ipaddress> {<mask>}	指定した VLAN の IP アドレスとサブネットマスクを設定します。
enable bootp vlan [<name> | all]	指定した VLAN の IP アドレスを BOOTP サーバから取得するよう設定します。
enable idletimeouts	無通信状態が 20 分間続いた場合に Telnet およびコンソールからの接続を自動的に切断するよう設定します。デフォルトでは、この機能はオフになっています。
enable clipaging	CLI コマンドの出力が多いときに画面表示を一時停止させるページャー機能をイネーブルにします。デフォルトはイネーブルです。
disable clipaging	ページャー機能をディセーブルにします。
clear session <number>	Telnet セッションを終了させます。

表 3-3：一般的な管理コマンド

コマンド名	機能
disable bootp vlan [<name> | all]	指定した VLAN の IP アドレス設定に BOOTP を使わないよう設定します。
disable idletimeouts	Telnet およびコンソールからの接続を自動的に切断しないようにします。この場合、コンソールからのセッションは、スイッチを再起動するまで継続されます。Telnet セッションは、クライアントが終了するまで継続されます。
disable ports [<portlist> | all]	指定したポートをディセーブルにします。
enable telnet	Telnet アクセスをイネーブルにします。
disable telnet	Telnet アクセスをディセーブルにします。
enable web	Web アクセスをイネーブルにします。
disable web	Web アクセスをディセーブルにします。
enable rmon	RMON 機能をイネーブルにします。
disable rmon	RMON 機能をディセーブルにします。
telnet [<ipaddress> | <hostname>] {<tcp_port>}	CLI セッションから他のホストに Telnet 接続します。TCP ポート番号を指定しなかった場合は、23 番ポートが使用されます。端末タイプは、VT100 のみサポートされます。
delete account <username>	ユーザアカウントを削除します。
delete vlan <name>	VLAN を削除します。
unconfig switch {all}	ユーザアカウントと日付/時刻を除くすべての設定項目を出荷時の内容に戻します。キーワード `all` を指定した場合は、ユーザアカウント情報も出荷時の状態に戻ります。
help	コマンドの簡単な説明を表示します。
history	コマンド履歴を表示します（最大 49 個）。
show banner	ユーザ定義のバナーを表示します。

3.4 ユーザアカウント

ユーザアカウントは、権限によって 2 つのレベルにわけられます。

- 一般ユーザ（user）レベル
- 管理者（admin）レベル

一般ユーザレベルのユーザは、管理パラメータの大部分を見ることができます。ただし、次の情報にはアクセスできません。

- ユーザアカウントデータベース
- SNMP コミュニティ名

また、一般ユーザには ping コマンドの実行権と自身のパスワードを変更する権限があります。一般ユーザレベルでログインした場合、コマンドプロンプトは次のように > 記号で表されます。

```
C9100:2>
```

管理者レベルのユーザは、すべてのパラメータにアクセスする権限を持ち、パラメータの変更、ユーザの追加と削除、パスワードの変更などを行うことができます。また、管理者は Telnet による管理セッションを強制的に切断することもできます。この場合、Telnet でログインしているユーザには、セッションの切断が通知されます。

管理者レベルでログインした場合、コマンドプロンプトは次のように # 記号で表されます。

```
C9100:18#
```

プロンプトの先頭には、SNMP の sysName 変数で定義された文字列が表示されます。コロンの後の数字は、当該セッションにおけるコマンドの通し番号です。

次のように、コマンドラインの先頭にアスタリスク（*）が表示される場合は、まだ保存していない変更内容があることを示しています。

```
*C9100:19#
```

変更した設定内容を保存する方法については、14-2 ページの「設定の保存」をご覧ください。

出荷時のユーザアカウント

出荷時には、表 3-4 に示すユーザが登録されています。

表 3-4：出荷時のユーザアカウント

アカウント名	権限
admin	すべての管理パラメータにアクセスできます。*admin* アカウントを削除することはできません。
user	ほとんどのパラメータを読み出すことができますが、変更はできません。また、次の情報にはアクセスできません。 • ユーザアカウントデータベース • SNMP コミュニティ名 *user* ユーザは、ping コマンドを実行できます。

パスワードの設定

出荷時には、ユーザアカウントにパスワードが設定されていません。以下の手順にしたがってパスワードを設定してください。パスワードは 4 〜 12 文字の間で設定します。

ユーザ名とパスワードは、大文字と小文字が区別されますのでご注意ください。

admin アカウントにパスワードを設定するには、以下の手順にしたがいます。

1 ユーザ名 *admin* でログインします。

2 パスワードプロンプトで「Return」キーを押します。

3 次のコマンドで *admin* アカウントにパスワードを設定します。

```
config account admin
```

4 新しいパスワードを入力します。

5 確認のため、もう一度新しいパスワードを入力します。

user アカウントにパスワードを設定するには、次の手順にしたがいます。

1 ユーザ名 *admin* でログインします。

2 パスワードプロンプトで「Return」キーを押します。

3 次のコマンドを使って *user* アカウントにパスワードを設定します。

```
config account user
```

4 新しいパスワードを入力します。

5 確認のため、もう一度新しいパスワードを入力します。

万が一パスワードを忘れてしまったときは、ご購入先の販売店にご相談ください。

ユーザアカウントの作成

ユーザアカウントは 16 個まで設定できます。

ユーザアカウント情報は、ユーザアカウントデータベースに保存されます。また、RADIUS 認証サーバを利用したアカウントの一元管理も可能です（詳しくは、3-24 ページの「RADIUS クライアント」をご覧ください）。

新しいユーザアカウントを作成するには、次の手順にしたがってください。

1 ユーザ名 *admin* でログインします。

2 パスワードプロンプトで *admin* アカウントのパスワードを入力し、「Return」キーを押します。

3 次のコマンドを使って、新しいアカウントを追加します。[admin | user] の部分で、作成するユーザのレベル（admin ＝管理者 /user ＝一般ユーザ）を指定します。

```
create account [admin | user] <username>
```

4 新しいアカウントのパスワードを入力します。

5 確認のため、もう一度パスワードを入力します。

ユーザアカウントの一覧を表示する

登録されているユーザアカウントの一覧を表示するには、管理者レベルで次のコマンドを実行します。

```
show accounts
```

次に出力例を示します。

```
C9100:617 # show accounts

   User Name     Access LoginOK Failed Session
---------------- ------ ------- ------ -------
           admin   R/W       6      0
            user   RO        0      0
```

ユーザアカウントの削除

ユーザアカウントを削除するには、管理者レベルで次のコマンドを実行します。

```
delete account <username>
```

admin アカウントを削除することはできません。

3.5 IP パラメータの設定

Telnet や Web インタフェース、SNMP 対応ネットワークマネージャによる管理を行う場合は、あらかじめ本製品の IP 関連パラメータを設定しておく必要があります。

IP アドレスの設定は、BOOTP を利用して起動時に自動設定する方法と、管理者が手動で設定する方法があります。以下、それぞれの手順について説明します。

BOOTP による IP アドレスの自動設定

BOOTP による IP アドレスの自動設定を行う場合は、以下の情報を BOOTP サーバに登録しておきます。

- 本製品の MAC アドレス
- IP アドレス
- サブネットマスク（省略可能）

MAC アドレスは、本体背面のラベルに記載されています。また、`show switch` コマンドでも確認できます。

登録後、本製品の IP アドレスとサブネットマスクは、起動時に BOOTP サーバからダウンロードされ自動的に設定されます。そのため、IP アドレスを手動で設定しなくても、本製品の管理機能を使用できるようになります。

VLAN ごとに BOOTP の使用 / 非使用を設定するには、次のコマンドを使います。

```
enable bootp vlan [<name> | all]
```

出荷時には、VLAN *default* が BOOTP を使用する設定になっています。

BOOTP を使用する設定になっているときは、`save` コマンドを実行しても IP アドレスは保存されません。IP アドレスの設定を保存するには、CLI、Telnet、Web インタフェースのいずれかを使って、手動で IP アドレスを設定します。

BOOTP を使って IP アドレスを取得するすべての VLAN は、同じ MAC アドレスを使用します。そのため、ルータの BOOTP リレー機能を使って BOOTP サーバにアクセスする場合は、BOOTP サーバが、BOOTP 要求パケット のゲートウェイ IP アドレスから、BOOTP 応答パケットの返送先を識別できる必要があります。

DHCP/BOOTP リレーの詳細については、9-11 ページの「DHCP/BOOTP リレーの設定」をご覧ください。

IP アドレスの手動設定

BOOTP を使用しない場合、SNMP 対応ネットワークマネージャや Telnet、Web インタフェースを使って本製品にアクセスするには、あらかじめ手動で IP アドレスなどの設定を行っておく必要があります。IP アドレスの設定は、以下の手順で行います。

1 管理者レベルでログインします。

2 VLAN に IP アドレスとサブネットマスクを割り当てます。

Telnet や SNMP 対応ネットワークマネージャを使って本製品にアクセスするには、少なくとも 1 つの VLAN を作成し、IP アドレスとサブネットマスクを割り当てておく必要があります。本製品の出荷時には、「*default*」という名前の VLAN が設定されていますので、最初はこれを使うと便利です。IP アドレスの設定は、つねに VLAN 単位で行います。本製品自体は、複数の IP アドレスを持つことができます。

VLAN の作成と設定に関する詳細については、第 5 章「バーチャル LAN（VLAN）」をご覧ください。

IP アドレスを手動で設定するには、以下の手順にしたがいます。

1 **コンソールポートに端末（または端末エミュレータがインストールされたPC またはワークステーション）を接続します。**

2 **端末画面にログインプロンプトが表示されるまで、「Return」キーを数回押します。**

3 **管理者レベルでログインします。ログイン名とパスワードは、大文字と小文字が区別されるのでご注意ください。**

初めてログインするときは、管理者レベルの *admin* アカウントを使います。出荷時には、このアカウントにはパスワードが設定されていません。

```
login: admin
```

管理者レベルのユーザは、すべての管理機能にアクセスできます。

管理者用アカウントを追加した場合は、ログインプロンプトでそのユーザ名とパスワードを入力します。

4 **パスワードプロンプトが表示されたら、パスワードを入力して「Return」キーを押してください。**

ログインに成功すると、コマンドラインの先頭にスイッチ名（sysName）が表示されます。

5 VLAN *default* **に** IP **アドレスとサブネットマスクを設定します。**

```
config vlan <name> ipaddress <ipaddress> {<mask>}
```

例

```
config vlan default ipaddress 123.45.67.8 255.255.255.0
```

設定内容は直ちに有効となります。

6 **デフォルトルートを設定します。**

```
config iproute add default <gateway> {<metric>}
```

例

```
config iproute add default 123.45.67.1
```

7 **変更が再起動後にも有効となるよう、設定内容を保存します。**

```
save
```

設定の変更内容を保存する方法については、14-2 ページの「設定の保存」をご覧ください。

8　設定が完了したら、ログアウトします。

```
logout（または quit）
```

表 3-5 に、基本的な IP パラメータの設定コマンドを示します。

表 3-5：IP 設定コマンド

コマンド名	機能
config iparp add <ipaddress> <mac_address>	ARP テーブルにパーマネントエントリを追加します。IP アドレスと MAC アドレスをペアで指定してください。
config iparp delete <ipaddress>	ARP テーブルから、指定した IP アドレスを持つエントリを削除します。
clear iparp {<ipaddress> | vlan <name>}	ARP テーブルから、ダイナミックエントリを削除します。パーマネントエントリは削除されません。
config iproute add <ipaddress> <mask> <gateway> {<metric>}	ルーティングテーブルにスタティックルートを追加します。ホストエントリの場合は、<mask> に 255.255.255.255（32 ビットマスク）を指定してください。
config iproute delete <ipaddress> <mask> <gateway>	ルーティングテーブルからスタティックルートを削除します。
config iproute add default <gateway> {<metric>}	デフォルトルートを設定します。デフォルトルートは、設定済みの IP インタフェース上になくてはなりません。<metric> が指定されていない場合は、デフォルトの 1 が使用されます。
config iproute delete default <gateway>	ルーティングテーブルからデフォルトルートを削除します。
show ipconfig {vlan <name>}	指定した VLAN の設定情報を表示します。
show ipstats {vlan <name>}	CPU が処理した IP パケットの統計を表示します。
show iparp {<ipaddress> | vlan <name> | permanent | proxy {<ipaddress> <mask>} }	ARP テーブルを表示します。IP アドレス、VLAN、パーマネントエントリ単位で、表示内容のフィルタリングが可能です。
show iproute {priority | vlan <name> | permanent | <ipaddress> <mask>}	IP ルーティングテーブルを表示します。

3.6 Telnet によるアクセス

TCP/IP ネットワーク上では、Telnet クライアントを使って、PC やワークステーションからコマンドラインインタフェースにアクセスすることができます。

同時に開くことのできるTelnetセッションは8つまでです。idletimeoutsパラメータがイネーブル（デフォルト）の場合、Telnetセッションは、無通信状態が20分間続くと自動的にタイムアウトします。Telnetセッションがロックアップしてしまった場合、2時間以内にスイッチ側からセッションが切断されます。

Telnetで管理機能にアクセスするには、あらかじめ本製品のIPアドレスを設定しておかなくてはなりません。詳細は、3-10ページの「IPパラメータの設定」をご覧ください。Telnet機能はデフォルトで使用可能になっています。

Telnetセッションを開始するには、クライアント側で本製品のIPアドレスを指定します。詳細は、Telnetクライアントのマニュアルをご覧ください。

Telnetセッションが確立されると、ログインプロンプトが表示され、ログイン可能な状態になります。3回連続してログインに失敗すると、セッションが切断されます。

本製品からTelnetで他のホストに接続する

次のコマンドを使用して、本製品のコマンドラインから他のホストにTelnetで接続することができます。

```
telnet [<ipaddress> | <hostname>] {<tcp_port>}
```

TCPポート番号を指定しなかった場合は、Telnetのデフォルトポートである23番ポートが使用されます。サポートされる端末タイプは、VT100のみです。

ホスト名を指定するには、DNSクライアント機能の設定が必要です。DNSクライアントの設定については、3-19ページの「DNSクライアントの設定」をご覧ください。

Telnetセッションの強制切断

管理者レベルのユーザは、Telnetによる管理セッションを強制的に切断することができます。この場合、Telnetで接続中のユーザにはセッションの切断が通知されます。

Telnetセッションを強制的に切断するには、以下の手順にしたがいます。

1 管理者レベルでログインします。

2 show sessionコマンドを使って、現在開かれているセッションを確認します。

次にshow sessionコマンドの出力例を示します。アスタリスク（*）は、現在使用中のセッションを示しています。

```
C9100:618 # show session

   # Login Time                  User    Type    Auth    Location
==========================================================================
*  0 Wed Aug 18 14:06:10 1999 admin     console local   serial
   4 Wed Aug 18 16:52:16 1999 admin     telnet  local   192.208.37.26
```

3　次のコマンドを使って、任意のセッションを強制終了します。

```
clear session <number>
```

Telnet サービスのディセーブル

Telnet サービスは、デフォルトで使用可能になっています。Telnet による管理機能へのアクセスをディセーブルにするには、次のコマンドを実行します。

```
disable telnet
```

Telnet サービスを再開するには、コンソールポートに接続した端末から次のコマンドを実行します。

```
enable telnet
```

Telnet サービスの停止 / 開始を行うには、管理者レベルでログインする必要があります。

3.7 Web インタフェース

本製品には、Web ベースの管理ソフトウェアが組み込まれており、Netscape Navigator 3.0 以上や Microsoft Internet Explorer 3.0 以上など、HTML フレーム対応の Web ブラウザを使って管理が可能です。

Web インタフェースにアクセスするには、少なくとも 1 つの VLAN を作成し、IP アドレスを割り当てておく必要があります。

IP アドレスの設定方法については、3-10ページの「IP パラメータの設定」をご覧ください。

Web インタフェースには、以下の URL でアクセスできます。<ipaddress> には、VLAN に割り当てた本製品の IP アドレスを指定してください。

```
http://<ipaddress>
```

Web インタフェースにアクセスすると、ログイン画面が表示されます。

Web インタフェースの使用方法については、付録 B「Web インタフェース」をご覧ください。

Web サービスのディセーブル

Web サービスは、デフォルトで使用可能になっています。Web アクセスをディセーブルにするには、次のコマンドを実行します。

```
disable web
```

Web サービスを再開するには、次のコマンドを実行します。

```
enable web
```

変更は再起動後から有効になります。

再起動の方法については、16-1 ページの「再起動」をご覧ください。

3.8 SNMP による管理

本製品は、SNMP（Simple Network Management Protocol）対応のネットワークマネージャによる管理が可能です。その場合は、管理ステーションに適切な MIB（Management Information Base）をインストールしておく必要があります。管理用のユーザインタフェースは、ネットワークマネージャによって異なります。

以降の節では、SNMP による管理を行う上で必要な設定について説明します。ここでは、読者の皆様が SNMP によるネットワーク管理に精通しているものと仮定して話を進めます。SNMP についてよくご存じない方は、市販の参考書等を参照してください。

SNMP エージェントへのアクセス

本製品内の SNMP エージェントにアクセスするには、少なくとも 1 つの VLAN を作成し、IP アドレスを割り当てておく必要があります。

IP アドレスの設定方法については、3-10ページの「IP パラメータの設定」をご覧ください。

サポートされる MIB

SNMP による管理を行うには、管理ステーションに適切な MIB がインストールされている必要があります。本製品は、プライベート MIB のほかに表 3-6 に示す標準 MIB をサポートしています。.

表 3-6：サポートされる MIB

名称	RFC 番号
MIB II	1213
IP Forwarding Table MIB	1354
Bridge MIB	1493
Interfaces MIB	1573
RIP2 MIB	1724
RMON MIB（Statistics、History、Alarms、Events グループ）	1757
RMON II Probe Configuration	2021
802.3 MAU MIB	2239

Bridge MIB の dot1dTpPortEntry、dot1dTpPortInDiscards、dot1dBasePortEntry はカウントアップされません。

SNMP 設定

本製品では、以下の SNMP パラメータを設定することができます。

- **トラップレシーバ** － SNMP トラップを受信する管理ステーションを指定します。本製品は、ここで設定されたすべてのトラップレシーバに対して、SNMP トラップを送信します。トラップレシーバは、本製品 1 台につき 16 個まで設定できます。このパラメータのエントリは、RFC 2021 で規定されている RMON2 MIB オブジェクトの `trapDestTable` を操作することによって、作成や修正、削除が可能です。
- **ネットワーク管理ステーション** － ネットワーク管理ステーションを指定します。管理ステーションの IP アドレスを直接指定する方法と、IP アドレスとサブネットマスクを使って一定範囲のアドレス（サブネット全体など）を指定する方法があります。ネットワーク管理ステーションは、8 個まで登録できます。管理ステーションの IP アドレスが 1 つも登録されていない場合、SNMP コミュニティ名による認証をパスしたすべてのステーションから本製品にアクセスできます。
- **コミュニティ名** － SNMP エージェント（本製品）と SNMP マネージャが認証を行う際に使用するコミュニティ名を指定します。コミュニティ名には、本製品にリードオンリーでアクセスする場合に使用する Read-only コミュニティ名と、読み書き権限でアクセスする場合に使用する Read-write コミュニティ名の 2 種類があります。デフォルトの Read-only コミュニティ名は *public*、Read-write コミュニティ名は *private* です。コミュニティ名は 8 個まで設定

できます。トラップレシーバが本製品の SNMP トラップを受信できるようにするには、本製品上でトラップレシーバ用のコミュニティ名を設定しておかなくてはなりません。

- **sysContact（省略可能）** ― 本製品の管理責任者名を設定します。
- **sysName** ― 本製品を識別するための名前を設定します。出荷時には、各モデルにそれぞれ次の値が設定されています。

表 3-7：出荷時の sysName

モデル名	sysName
C9108	C9100
C8518	C8500
C8525	C8525
C8550	C8550

- **sysLocation（省略可能）** ― 本製品の設置場所を設定します。

表 3-8 に SNMP 設定コマンドの一覧を示します。

表 3-8：SNMP 設定コマンド

コマンド名	機能
enable snmp access	SNMP 機能をイネーブルにします。
enable snmp traps	SNMP トラップ機能をイネーブルにします。
config snmp add <ipaddress> {<mask>}	SNMP 管理ステーションの IP アドレスをアクセスリストに追加します。管理ステーションは、8 個まで登録できます。
config snmp add trapreceiver <ipaddress> community <string>	トラップレシーバの IP アドレスを追加します。指定できる IP アドレスは、ユニキャスト、マルチキャスト、ブロードキャストのいずれかです。トラップレシーバは 16 個まで登録できます。
config snmp community [readonly | readwrite] <string>	Read-only および Read-write コミュニティ名を設定します。コミュニティ名は 126 文字以内で指定します。
config snmp delete [<ipaddress> | all]	指定した IP アドレスを持つ SNMP 管理ステーションをアクセスリストから削除します。キーワード all を指定すると、すべての管理ステーションがアクセスリストから削除され、あらゆる機器が SNMP を通じて本製品にアクセスできるようになります。
config snmp delete trapreceiver [<ipaddress> {community <string>} | all]	指定したトラップレシーバの IP アドレスを削除します。キーワード all を指定した場合は、すべてのエントリが削除されます。
config snmp sysContact <string>	本製品の管理責任者を示す sysContact 変数を設定します。255 文字以内で指定してください。

表 3-8：SNMP 設定コマンド

コマンド名	機能
config snmp sysName <string>	本製品の識別名を示す sysName 変数を設定します。255 文字以内で指定してください。出荷時には、スイッチのモデル名（C9100、C8500、C8525、C8550）が設定されています。この変数の内容は、コマンドラインの先頭に表示されます。
config snmp sysLocation <string>	本製品の設置場所を示す sysLocation 変数を設定します。255 文字以内で指定してください。

SNMP 設定の確認

SNMP の設定を確認するには、次のコマンドを実行します。

```
show management
```

出力される情報は次のとおりです。

- Telnet、SNMP、Web アクセスのイネーブル / ディセーブル
- SNMP コミュニティ名
- 登録されている SNMP 管理ステーション
- 登録されている SNMP トラップレシーバ
- ログイン統計

SNMP のディセーブルとリセット

SNMP 設定をリセットしたり SNMP 機能を停止したりするには、表 3-9 に示すコマンドを使用します。

表 3-9：SNMP のディセーブル / リセット用コマンド

コマンド名	機能
disable snmp access	SNMP 機能をディセーブルにします。
disable snmp traps	SNMP トラップの送信機能をディセーブルにします。ただし、登録済みのトラップレシーバは削除されません。
unconfig management	SNMP 関連の設定項目をデフォルト値に戻します。

3.9 DNS クライアントの設定

本製品は、DNS クライアント（リゾルバ）の機能を持っています。ネームサーバアドレスとデフォルトドメイン名を設定することにより、以下のコマンド使用時に IP アドレスだけでなくホ

スト名による指定が可能になります。ホスト名を指定した場合は、リゾルバがネームサーバに問い合わせてホスト名に対応する IP アドレスを取得します。

- telnet
- download [image | configuration | bootrom]
- upload configuration
- ping
- traceroute

DNS クライアントの設定を行うには、以下の手順にしたがいます。

1 自ドメイン名を設定します。ドメインは、1 筐体あたり 1 つだけ設定できます。

```
config dns-client default-domain <domain_name>
```

例

```
config dns-client default-domain birds.or.jp
```

2 ネームサーバ (DNS サーバ) の IP アドレスを設定します。ネームサーバは 3 つまで登録可能です。

```
config dns-client [add | delete] <ipaddress>
```

例

```
config dns-client add 192.168.1.1
```

3 nslookup コマンドを使用して、DNS の検索が正しく行われることを確認します。

```
nslookup <hostname>
```

例

```
c9100:67# nslookup orange.birds.or.jp
Answer 0: 192.168.1.5
```

4 DNS クライアントの設定を確認するには、次のコマンドを使用します。

```
show dns-client
```

表 3-10 に、DNS クライアント機能の設定コマンド一覧を示します。

表 3-10：DNS クライアント設定コマンド

コマンド名	機能
config dns-client default-domain <domain_name>	本製品のデフォルトドメインを設定します。DNS クライアントは、FQDN でないホスト名を受け取った場合、ホスト名にデフォルトドメインを付加した上で DNS を検索します。

表 3-10：DNS クライアント設定コマンド

コマンド名	機能
config dns-client add <ipaddress>	名前解決に使用するネームサーバ（DNS サーバ）の IP アドレスを設定します。DNS は 3 つまで登録できます。
config dns-client delete <ipaddress>	ネームサーバの登録を削除します。
nslookup <hostname>	指定したホスト名に対応する IP アドレスを表示します。
show dns-client	DNS クライアント機能の設定を表示します。

3.10 SNTP クライアントの設定

本製品は、ネットワーク上のタイムサーバ（NTP サーバ）を利用して、システムクロックを自動調整する SNTP（Simple Network Time Protocol）クライアント機能を備えています。SNTP 機能を有効にすると、本製品は定期的にタイムサーバに問い合わせを行い、システムクロックを修正します。また、NTP サーバからのブロードキャストを受信した場合も時刻合わせを行います。

SNTP クライアントの設定を行うには、以下の手順にしたがいます。

1 NTP ではGMT（グリニッジ標準時）を使用するため、GMT オフセットと夏時間を設定します。

```
config timezone <gmt_offset> {autodst | noautodst}
```

<gmt_offset> には、ローカル時間と GMT（グリニッジ標準時）との差を分で指定します。GMT より進んでいる場合は + を、遅れている場合は - を付けてください。夏時間の自動調整を行う場合は autodst オプションを、行わない場合は noautodst オプションを指定します。デフォルトは autodst です。

日本時間（GMT+9、夏時間なし）の設定例

```
config timezone +540 noautodst
```

表 3-11 に、GMT オフセットの一覧を示します。

表 3-11：GMT オフセット

GMT オフセット（時）	GMT オフセット（分）	タイムゾーン	代表的な都市
+0:00	+0	GMT（グリニッジ標準時） UT（世界時） UTC（協定世界時） WET（西ヨーロッパ標準時）	ロンドン（イギリス） ダブリン（アイルランド） リスボン（ポルトガル） レイキャビク（アイスランド） カサブランカ（モロッコ）
-1:00	-60	WAT（西アフリカ標準時）	
-2:00	-120	AT（アゾレス標準時）	

表 3-11：GMT オフセット

GMT オフセット（時）	GMT オフセット（分）	タイムゾーン	代表的な都市
-3:00	-180		ブラジリア（ブラジル）、ブエノスアイレス（アルゼンチン）、ジョージタウン（ギアナ）
-4:00	-240	AST（大西洋標準時）	カラカス（ベネズエラ）、ラパス（ボリビア）
-5:00	-300	EST（東部標準時）	ボゴタ（コロンビア）、リマ（ペルー）、ニューヨーク（米国）
-6:00	-360	CST（中部標準時）	メキシコシティ（メキシコ）
-7:00	-420	MST（山地標準時）	
-8:00	-480	PST（太平洋標準時）	ロサンゼルス、シアトル（米国）
-9:00	-540	YST（ユーコン標準時）	
-10:00	-600	AHST（アラスカハワイ標準時） CAT（中央アラスカ標準時） HST（ハワイ標準時）	
-11:00	-660	NT（ノーム標準時）	
-12:00	-720	IDLW（国際日付変更線西）	
+1:00	+60	CET（中央ヨーロッパ標準時） FWT（フランス冬時間） MET（中欧時間） MEWT（中欧冬時間） SWT（スウェーデン冬時間）	パリ（フランス）、ベルリン（ドイツ）、アムステルダム（オランダ）、ブリュッセル（ベルギー）、ウィーン（オーストリア）、マドリード（スペイン）、ローマ（イタリア）、ベルン（スイス）、ストックホルム（スウェーデン）、オスロ（ノルウェー）
+2:00	+120	EET（東部ヨーロッパ標準時） ロシア・ゾーン 1	アテネ（ギリシャ）、ヘルシンキ（フィンランド）、イスタンブール（トルコ）、エルサレム（イスラエル）、ハラレ（ジンバブエ）
+3:00	+180	BT（バグダッド標準時） ロシア・ゾーン 2	クウェート、ナイロビ（ケニア）、リヤド（サウジアラビア）、モスクワ（ロシア）
+4:00	+240	ZP4（ロシア・ゾーン 3）	アブダビ（アラブ首長国連邦）、マスカット（オマーン）、トビリシ（グルジア）、ボルゴグラード（ロシア）、カブール（アフガニスタン）
+5:00	+300	ZP5（ロシア・ゾーン 4）	
+5:30	+330	IST（インド標準時）	ニューデリー（インド）
+6:00	+360	ZP6（ロシア・ゾーン 5）	

表 3-11：GMT オフセット

GMT オフセット（時）	GMT オフセット（分）	タイムゾーン	代表的な都市
+7:00	+420	WAST（西部オーストラリア標準時）	
+8:00	+480	CCT（中国沿岸部標準時） ロシア・ゾーン 7	
+9:00	+540	JST（日本標準時） ロシア・ゾーン 8	東京（日本）
+10:00	+600	EAST（東部オーストラリア標準時） GST（グアム標準時） ロシア・ゾーン 9	
+11:00	+660		
+12:00	+720	IDLE（国際日付変更線東） NZST（ニュージーランド標準時） NZT（ニュージーランド時間）	ウェリントン（ニュージーランド）、フィジー、マーシャル諸島

2 SNTP クライアント機能を有効にします。

```
enable sntp-client
```

SNTP を有効にすると、本製品は NTP サーバからのブロードキャストメッセージを受信して、クロックを調整するようになります。

3 特定の NTP サーバに定期的に問い合わせを行いたい場合は、次のコマンドを使って NTP サーバを登録します。NTP サーバは、プライマリとセカンダリの 2 つを登録できます。ホスト名を指定するには、DNS クライアント機能の設定が必要です。

```
config sntp-client [primary | secondary] server [<ipaddress> | <host-
name>]
```

例

```
config sntp-client primary 192.168.1.1
config sntp-client secondary 192.168.1.2
```

本製品は、まずプライマリサーバに NTP クエリーを送信します。1 秒以内にプライマリサーバから応答がなかった場合は、セカンダリサーバを試します（セカンダリサーバが設定されている場合）。時刻を取得できなかった場合はただちにクエリーを繰り返します。取得できた場合は、update-interval に指定された時間間隔でクエリーを繰り返します。

4 NTP サーバへの問い合わせ間隔を指定するには、次のコマンドを使います。

```
config sntp-client update-interval <second>
```

間隔は秒で指定します。デフォルトは 64 秒です。

5 SNTP クライアント機能の設定を確認するには、次のコマンドを使います。

- `show sntp-client`

  SNTP クライアント機能の設定と統計情報を表示します。

- `show switch`

  GMT オフセット、夏時間設定、現在時刻（ローカル時間）を表示します。

表 3-12 に、SNTP クライアント設定コマンドの一覧を示します。

表 3-12：SNTP クライアント設定コマンド

コマンド名	機能
config timezone <gmt_offset> {autodst | noautodst}	タイムゾーンの設定を行います。`<gmt_offset>` には、グリニッジ標準時（GMT）とローカル時間の差を分で指定します。GMT より早い場合は + を、遅い場合は - を付けてください。夏時間（Daylight Saving Time）の自動調整を行いたい場合は `autodst` オプション（デフォルト）を、行わない場合は `noautodst` オプションを指定します。
enable sntp-client	SNTP クライアント機能をイネーブルにします。
disable sntp-client	SNTP クライアント機能をディセーブルにします。
config sntp-client [primary | secondary] server [<ipaddress> | <hostname>]	時刻情報を取得するタイムサーバ（NTP サーバ）を設定します。タイムサーバは、プライマリとセカンダリの 2 つを登録できます。プライマリサーバから 1 秒以内に応答がない場合は、セカンダリサーバに問い合わせます。
config sntp-client update-interval <second>	NTP サーバへの問い合わせ間隔を秒で指定します。デフォルトは 64 秒です。
show sntp-client	SNTP クライアント機能の設定と統計情報を表示します。

3.11 RADIUS クライアント

本製品では、RADIUS（Remote Authentication Dial In User Service）サーバを利用したユーザアカウントの一元管理が可能です。RADIUS 認証の対象となるのは、CLI（コンソールおよび Telnet 経由）と Web インタフェースへのアクセスです。

RADIUS 使用時にユーザがログインしようとすると、本製品は登録されている RADIUS サーバに認証要求をリレーします。プライマリサーバから応答がない場合はセカンダリサーバを試し、それでも応答がない場合は、自身が持つユーザアカウントデータベースを使ってユーザを認証します。RADIUS サーバに登録されているアカウント情報とローカルのユーザアカウントデータベースに登録されている情報が食い違っている場合は、RADIUS サーバ側の情報が優先されます。

RADIUS クライアントの設定

RADIUS サーバの設定は以下の手順で行います。

1 RADIUS クライアント機能を有効にします。

```
[enable | disable] radius
```

2 認証に使用する RADIUS サーバを指定します。RADIUS サーバは、プライマリとセカンダリの 2 台を指定することができます。client-ip <ipaddress> には、本製品の IP アドレスを指定します。また、オプションとして RADIUS サーバのポート番号を指定することもできます。デフォルトでは 1645 番ポートを使用します。

```
config radius [primary | secondary] server [<ipaddress> | <hostname>]
{<radius_port_number>} client-ip <ipaddress>
```

3 必要に応じて、RADIUS サーバとの通信に用いる共有秘密鍵を設定します。

```
config radius [primary | secondary] shared-secret <password>
```

RADIUS クライアント機能の設定を確認するには、次のコマンドを使います。

```
show radius
```

RADIUS サーバの登録を抹消するには、次のコマンドを使います。

```
unconfig radius {server [primary | secondary]}
```

表 3-13 に RADIUS クライアント設定コマンドの一覧を示します。

表 3-13：RADIUS クライアント設定コマンド

コマンド名	機能
enable radius	ログイン認証に RADIUS 認証サーバを使用します。
disable radius	RADIUS クライアント機能をディセーブルにします。
config radius [primary | secondary] server [<ipaddress> | <hostname>] {<radius_port_number>} client-ip <ipaddress>	RADIUS サーバを指定します。RADIUS サーバは、プライマリとセカンダリの 2 台を登録できます。client-ip <ipaddress> には、本製品の IP アドレスを指定します。また、オプションとして RADIUS サーバのポート番号も指定できます。デフォルトでは 1645 番ポートを使用します。
config radius [primary | secondary] shared-secret <password>	RADIUS サーバとの通信に用いる共有秘密鍵を設定します。
unconfig radius {server [primary | secondary]}	RADIUS サーバの登録を抹消します。
show radius	RADIUS クライアント機能の設定を表示します。

サポートしている属性

RFC2138 で規定されている諸属性のうち、本製品でサポートされているのは以下のとおりです。

- User-Name
- User-Password

- Service-Type
- Login-IP-Host

3.12 接続確認

本製品には、以下の接続確認用コマンドが用意されています。

- `ping`
- `traceroute`

Ping

`ping` **は、**ICMP（Internet Control Message Protocol）**のエコーメッセージを使って、リモートホストへの到達性を調べるコマンドです。**`ping` **コマンドは、一般ユーザと管理者の双方が使用できます。**

`ping` **コマンドの構文は次のとおりです。**

```
ping {continuous} {size <value>} [<ipaddress> | <hostname>]
```

表 3-14 **に** `ping` **コマンドのパラメータを示します。**

表 3-14：Ping コマンドのパラメータ

パラメータ	機能
`continuous`	ICMP エコーメッセージを断続的に送信します。パケットの送信を中止するには、いずれかのキーを押してください。
`size <value>`	送信するパケットのサイズを指定します。
`<ipaddress>`	リモートホストの IP アドレスを指定します。
`<hostname>`	リモートホストのホスト名を指定します（DNS クライアント機能の設定が必要）。

`ping` **コマンドは、エコー要求に対する応答がないと明示的に中断されるまでパケットの送信を続けます。その場合は、いずれかのキーを押して送信を中断させてください。**

Traceroute

`traceroute` **は、**ICMP **エコー要求メッセージと** TTL **超過メッセージを利用して、リモートホストまでの経路を調べるコマンドです。**`traceroute` **コマンドの構文は次のとおりです。**

```
traceroute [<ipaddress> | <hostname>]
```

`[<ipaddress> | <hostname>]` **には、リモートホストの** IP **アドレスまたはホスト名を指定します。ホスト名を指定する場合は、**DNS **クライアント機能の設定が必要です。**

4　ポートの設定

この章では、ポートの設定方法について説明します。

4.1 ポートのイネーブル / ディセーブル

デフォルトでは、すべてのポートがイネーブルになっています。ポートのイネーブル / ディセーブルを切り替えるには、次のコマンドを使用します。

```
[enable | disable] ports [<portlist> | all]
```

たとえば、C8518 のポート 3、5、12 〜 15 をディセーブルにするには、次のようにします。

```
disable ports 3,5,12-15
```

ポートをディセーブルに設定しても、診断のためリンクは維持されます。

4.2 ポートの通信速度と通信モード

デフォルトでは、各ポートの通信速度と通信モードはオートネゴシエーションによって自動的に選択されますが、手動で設定することも可能です。10 / 100M ポートでは通信速度と通信モード、ギガビットポートでは通信モードの手動選択が可能です。

10 / 100M ポートは、10Base-T ネットワークか 100Base-TX ネットワークと接続できます。デフォルトでは、オートネゴシエーションによる通信速度の自動選択機能が有効になっていますが、手動で各ポートの通信速度（10Mbps / 100Mbps）を設定することも可能です。

ギガビットポートの通信速度は 1Gbps で固定されており、変更することはできません。

出荷時には、通信モードもオートネゴシエーションによって自動選択される設定になっています。通信モードの手動設定はすべてのポートに対して行えます。

ポートの通信速度と通信モードを設定するには、次のコマンドを使います。

```
config ports [<portlist> | all] auto off {speed [10 | 100]} duplex [half |
full]
```

指定したポートでオートネゴシエーションを有効にするには次のコマンドを使います。

```
config ports [<portlist> | all] auto on
```

フロー制御はギガビットポートでのみサポートされています。フロー制御のイネーブル / ディセーブルは、オートネゴシエーションのオン / オフと連動しています。

ギガビットポートのオートネゴシエーションをオフにする

対向機器の種類によっては、ギガビットポートのオートネゴシエーションをオフにする必要があるかもしれません。オートネゴシエーションをオフにするときは、下の例のように通信モードを明示的に指定しなくてはなりません。

C8518 のポート 18（ギガビットポート）のオートネゴシエーションをオフにするには、次のコマンドを実行します。

```
config ports 18 auto off duplex full
```

4.3 ポート設定コマンド

表 4-1 にポート設定コマンドの一覧を示します。

表 4-1：ポート設定コマンド

コマンド名	機能
enable learning ports <portlist>	指定したポートの MAC アドレス学習機能をイネーブルにします。デフォルトはイネーブルです。
enable ports [<portlist> | all]	ポートをイネーブルにします。
enable sharing <master_port> grouping <portlist>	ロードシェアリンググループを定義します。グループに参加するポートを <portlist> に指定してください。他のコマンド中でロードシェアリンググループを参照するときは、<master_port> に指定したポートを使います。
enable smartredundancy <portlist>	C8518、C8525、C8550 において、リダンダントギガビットポートのスマートリダンダンシー機能をイネーブルにします。この機能がイネーブルの場合、プライマリポートが利用可能なときは、つねにプライマリポートが使用されます。デフォルトはイネーブルです。
config ports [<portlist> | all] auto on	オートネゴシエーションをオンにします。10/100 M ポートでは IEEE 802.3u、ギガビットポートでは 802.3z準拠のオートネゴシエーションが有効となります。
config ports [<portlist> | all] auto off {speed [10 | 100]} duplex [half | full]	指定したポートの通信速度と通信モードを変更します。以下の項目を設定できます。 • auto off − オートネゴシエーションをオフにします。 • speed − 通信速度を設定します（10/100M ポートのみ）。 • duplex − 通信モード（フルデュプレックス/ハーフデュプレックス）を指定します。
config ports <portlist> display-string <string>	show ports info コマンドなどで表示されるポート名を設定します。15 文字以内で指定してください。

表 4-1：ポート設定コマンド

コマンド名	機能
unconfig ports <portlist> display-string <string>	ポート名を削除します。
config ports [<portlist> | all] qosprofile [<qosname> | none]	指定したポートに QoS プロファイルを割り当てます。
disable learning ports <portlist>	指定したポートの MAC アドレス学習機能をディセーブルにします。MAC アドレス学習機能がディセーブルの場合は、パーマネント MAC エントリ宛てのフレームのみ転送されます。デフォルトはイネーブルです。
restart ports <portlist>	指定したポートのリンクをいったんダウンした後、再度アップします。ポートに接続されたケーブルの抜き差しと同様の効果があります。
disable ports [<portlist> | all]	ポートをディセーブルにします。ただし、ポートをディセーブルに設定しても、診断のためリンクは維持されます。
disable sharing <master_port>	ロードシェアリンググループをディセーブルにします。
disable smartredundancy <portlist>	スマートリダンダンシー機能をディセーブルにします。この機能がディセーブルのときは、現在アクティブなポートが使用不可能になったときだけ、リンクの切り替えが行われます。
show ports {<portlist>} collisions	コリジョン統計をリアルタイムに表示します。
show ports {<portlist>} configuration	以下に示すポートの設定内容を表示します。 • ポートの状態 • リンクの状態 • オートネゴシーエションの状態 • 通信速度 • 通信モード • フロー制御 • ロードシェアリング情報 • リンクメディア情報
show ports {<portlist>} info	ポートに関する詳細な情報を表示します。表示される項目は以下のとおりです。 • ポートの状態 • リンクの状態 • オートネゴシーエションの状態 • 通信速度 • 通信モード • STP 情報 • リダンダントポートの状態 • ロードシェアリング情報 • VLAN 情報 • QoS 情報
show ports {<portlist>} packet	パケットの分布統計を表示します。

表 4-1：ポート設定コマンド

コマンド名	機能
show ports {<portlist>} qosmonitor	QoS に関する統計情報をリアルタイムに表示します。QoS 機能の詳細については、第 8 章「QoS（Quality of Service）」をご覧ください。
show ports {<portlist>} rxerrors	受信エラー統計をリアルタイムに表示します。エラー統計の詳細については、15-6 ページの「ポートエラー統計」をご覧ください。
show ports {<portlist>} stats	ポート統計をリアルタイムに表示します。ポート統計の詳細については、15-6 ページの「ポート統計機能」をご覧ください。
show ports {<portlist>} txerrors	送信エラー統計をリアルタイムに表示します。エラー統計の詳細については、15-6 ページの「ポートエラー統計」をご覧ください。
show ports {<portlist>} utilization	ポートの使用状況をリアルタイムに表示します。表示単位をパケット、バイト、パーセントの間で切り替えるには、「Space」キーを押します。

4.4 ロードシェアリング機能

ロードシェアリング機能は、複数の物理ポートを束ねて使用することにより、スイッチ間の帯域幅を拡大する機能です。束ねたポート（ロードシェアリンググループ）のいずれかに障害が発生した場合でも、残りのポートで通信を継続できるため、耐障害性の向上にもつながります。このアルゴリズムを使用すると、複数の物理ポートを単一の論理ポートとして使用することができます。これにより、ロードシェアリンググループは、VLAN から単一の仮想ポートとして認識されます。また、パケットの順序もこのアルゴリズムによって保証されます。

グループ内のポートが使用できなくなった場合、トラフィックは残りのポートに再配分されます。使用できなかったポートが復旧すると、負荷の再配分が行われ、再びグループ内の全ポートを使って通信が行われるようになります。

ロードシェアリング機能がもっとも有効に働くのは、ロードシェアリンググループを通じて送信されるトラフィックの量が、ロードシェアリンググループの帯域幅と同じかそれ以上の場合です。たとえば、2 ポートでロードシェアリンググループを構成する場合、このグループを通じて送り出すトラフィックの受信元ポート数は 2 ポート以上であることが望まれます。

本機能は当社の独自仕様であり、C9100/8500 シリーズ間でしか使用できませんのでご注意ください。ただし、他社の「トランキング」機能と互換性がある可能性もあります。詳細については、ご購入先の販売店までお問い合わせください。

ロードシェアリングの設定

ポート間で負荷分散を行うには、ロードシェアリンググループを作成する必要があります。ロードシェアリンググループの作成にあたっては、以下のルールが適用されます。

- **ポートは、2 つずつまたは 4 つずつのグループに分けられます。**
- **ロードシェアリンググループを構成するポートは、互いに隣接していなければなりません。**
- **有効なポートの組み合わせについては、下の表を参照してください。**
- **ロードシェアリンググループを構成するポートのうち、ポート番号がもっとも若いものを「マスター」ポートに設定します。ロードシェアリンググループ全体に対して設定を行うときは、設定コマンド中でこのマスターポートを指定します。**

表 4-2 ～表 4-5 に、C9108、C8518、C8525、C8550 でロードシェアリンググループを構成する際の有効なポートの組み合わせを示します。

表 4-2：C9108 におけるポートの組み合わせ

ロードシェアリンググループ	2	3	4	5	6	7	1	8
4 ポート構成			x	x	x	x		
2 ポート構成	x	x	x	x	x	x	x	x

表 4-3：C8518 におけるポートの組み合わせ

ロードシェアリンググループ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
4 ポート構成	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
2 ポート構成	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

表 4-4：C8525 におけるポートの組み合わせ

ロードシェアリンググループ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
4 ポート構成	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
2 ポート構成	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	

表 4-5：C8550 におけるポートの組み合わせ

ロードシェアリンググループ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
4 ポート構成	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2 ポート構成	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

ロードシェアリンググループ	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
4 ポート構成	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2 ポート構成	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

ロードシェアリンググループ	49	50
4 ポート構成		
2 ポート構成	x	x

ロードシェアリンググループを定義するときは、グループを構成するポートと、グループを代表するマスターポートを指定します。ロードシェアリンググループの定義と削除を行うには、次のコマンドを使用します。

```
enable sharing <master_port> grouping <portlist>
disable sharing <master_port>
```

ポート 9 ～ 12 **でロードシェアリングを行うには、次のようにします。ここでは、グループ内でもっともポート番号が若いポート** 9 **をマスターポートに指定しています。**

```
enable sharing 9 grouping 9-12
```

この例では、ポート 9 **がポート** 9 ～ 12 **を代表します。**

ロードシェアリングの使用中に VLAN の設定や表示を行うときは、コマンド中でグループ内のマスターポート（先ほどの例ではポート 9）を指定します。VLAN がグループ内のマスターポート以外のポートを使用する設定になっている場合、ロードシェアリングが有効になった時点で、マスターポート以外のポートは VLAN から削除されます。

ロードシェアリンググループ内のポートをディセーブルにしないでください。ポートをディセーブルにすると、そのポートはフォワーディング状態ではなくなりますが、リンクはアップのままとなります。そのため、対向機器はそのポートがフォワーディング状態でないことを検知できずにパケットの送信を継続してしまいます。

ロードシェアリングを使用するときは、ループの形成を防ぐため、必ずリンクの両側ともロードシェアリングをイネーブルにしてください。

ロードシェアリング設定の確認

ロードシェアリンググループの構成ポートとマスターポートの情報を確認するには、`show ports configuration` コマンドを実行します。

4.5 ポートミラーリング

ポートミラーリングとは、一定の基準にしたがってフィルタリングされたすべてのトラフィックを、あらかじめ指定したミラーポートにコピーする機能です。ミラーポートには、ネットワークアナライザや RMON プローブを接続してパケット解析を行うことができます。どのトラフィックをミラーポートにコピーするかは、以下の基準にしたがって定義されるミラーリングフィルタによって決定されます。

- **送信元MACアドレス/宛先MACアドレス** ― 特定の送信元MACアドレス、または宛先MACアドレスを持つすべてのトラフィックをミラーポートにコピーします。

MAC ミラーリングを正しく機能させるには、希望する MAC アドレスエントリがあらかじめフォワーディングデータベース（FDB）に登録されていなければなりません。FDB の詳細については、第 6 章「フォワーディングデータベース（FDB）」をご覧ください。

- **物理ポート** ― 特定のポートを通過するすべてのトラフィックをミラーポートにコピーします。
- **VLAN** ― 特定の VLAN から送受信されるすべてのトラフィックをミラーポートにコピーします。
- **バーチャルポート** ― あるポート上に設定された特定の VLAN から送受信されるすべてのトラフィックをミラーポートにコピーします。

ミラーポートは 1 つ、ミラーリングフィルタは 8 つまで定義できます。ミラーポートとして設定したポートは、監視以外の目的には使用できません。

エラーフレームはミラーリングされません。

ポートミラーリングコマンド

表 4-6 にポートミラーリング設定コマンドの一覧を示します。

表 4-6：ポートミラーリングコマンド

コマンド名	機能
enable mirroring to port <port>	指定したポートをミラーポートとして設定します。

表 4-6：ポートミラーリングコマンド

コマンド名	機能
config mirroring add [<mac_address> | vlan <name> | port <port> | vlan <name> port <port>]	ミラーリングフィルタを定義します。フィルタは8 つまで定義できます。VLAN とポートの組み合わせ（バーチャルポート）、MAC アドレス単位、VLAN 単位、物理ポート単位でのフィルタリングが可能です。
config mirroring delete [<mac_address> | vlan <name> | port <port> | vlan <name> port <port>]	ミラーリングフィルタを削除します。
disable mirroring	ポートミラーリングをディセーブルにします。
show mirroring	ポートミラーリング関連の設定を表示します。

ポートミラーリングの設定例

次の例では、ポート 1 **を通過するすべてのトラフィックを、ミラーポートであるポート** 3 **にコピーします。**

```
enable mirroring to port 3
config mirroring add port 1
```

次の例では、ポート 1 **を通過するトラフィックのうち、**VLAN *default* **に属するものだけをミラーポートにコピーします。**

```
config mirroring add port 1 vlan default
```

5　バーチャル LAN（VLAN）

この章では、バーチャル LAN（VLAN）の概要と設定方法について説明します。

5.1 概要

VLAN 機能とは、スイッチの設定によって論理的にブロードキャストドメインを分割する機能です。同じ VLAN に所属する機器同士は、あたかも同じ物理セグメントに属しているかのように通信できます。本製品では、ポートベース、プロトコルベース、タグベースなど、物理的なネットワーク構成にとらわれない柔軟な VLAN 設定が可能です。

VLAN のメリット

VLAN 導入には、次のようなメリットがあります。

- **ブロードキャストトラフィックの抑制 ー** 従来のネットワークでは、受信側の機器がそれを必要としているかどうかに関係なく、ネットワーク内のすべての機器に対して送信されるブロードキャストトラフィックが混雑発生の原因になっていました。互いに通信の必要がある機器だけを集めて VLAN を構成することにより、無駄なトラフィックを減らし、ネットワークの効率を高めることができます。
- **セキュリティの向上 ー** VLAN 内の機器は、同じ VLAN に所属する機器としか通信できません。たとえば、VLAN *Marketing* 内の機器と VLAN *Sales* 内の機器が通信するには、VLAN 間ルーティングの設定を行う必要があります。
- **機器の取り替えや移動が容易に ー** 従来のネットワークでは、機器の移動や取り替えに費やされる時間と労力が無視できないものとなっていました。ユーザが別のサブネットに移動したときは、端末ごとにアドレスを手動で変更する必要がありました。

  VLAN を導入すれば、このような手間が軽減されます。たとえば、VLAN *Marketing* に所属する機器を別のポートに移動することを考えます。この機器は移動後も同じサブネットに属するものとします。この場合、新しいポートの所属を VLAN *Marketing* に変更するだけで作業が完了します。

5.2 VLAN の種類

VLAN は 256 個まで作成できます。本製品では、次に挙げる種類の VLAN をサポートしています。

- **ポート** VLAN

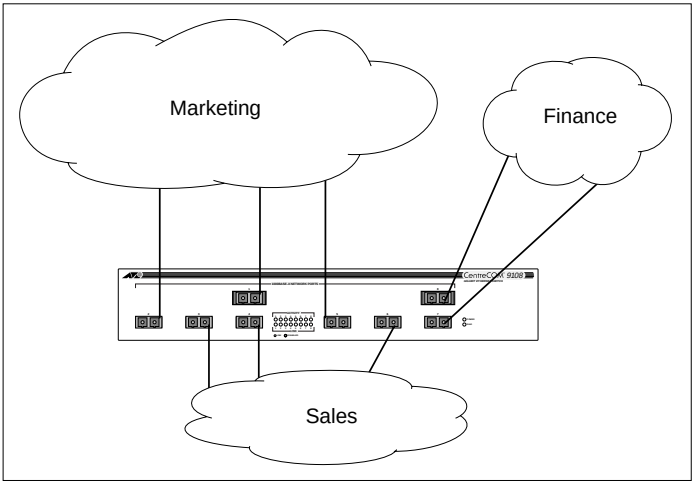
- IEEE 802.1Q タグ VLAN
- EtherType、LLC SAP、SNAP を利用したプロトコル VLAN
- 上記 3 種類の組み合わせ

ポート VLAN

ポート VLAN では、ポート単位で VLAN を構成します。後述するタグ VLAN やプロトコル VLAN も、ポート VLAN がベースになります。各ポートが所属できる純粋なポート VLAN は 1 つだけです。

図 5-1 の例では、ポート 1、2、5 が VLAN *Marketing* に、ポート 3、4、6 が VLAN *Sales* に、ポート 7 と 8 が VLAN *Finance* にそれぞれ所属しています。

図 5-1：ポート VLAN の構成例



この例ではすべての機器が同じ筐体に接続されていますが、異なる VLAN に所属する機器同士が通信を行うためには、IP または IPX ルーティング機能をイネーブルにして VLAN 間のトラフィックをルーティングしてやる必要があります。この場合、各々の VLAN に IP アドレスか IPX ネットワーク番号を割り当て、これを各 VLAN のルータインタフェース（ゲートウェイ）として使用します。

複数の筐体にまたがるポート VLAN

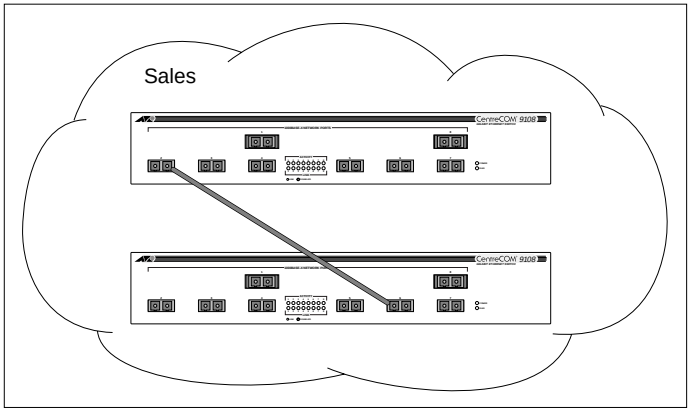
複数の筐体にまたがるポート VLAN を構築するには、次の手順にしたがいます。

1 各筐体上で VLAN を作成します。

2 同じ VLAN に属するポート同士で筐体間を接続します。

図 5-2 **は、**2 **台の筐体にまたがる** VLAN *Sales* **の設定例です。どちらの筐体とも、すべてのポートが** VLAN *Sales* **に所属しています。筐体間は、上の筐体のポート** 2 **と下の筐体のポート** 6 **を使って接続されています。**

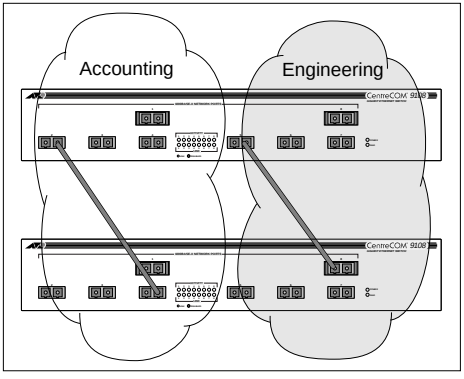
図 5-2：2台の筐体にまたがって構成されたポート VLAN



2 **台の筐体にまたがるポート** VLAN **を複数作成する場合は、**VLAN **ごとに筐体間を接続しなくてはなりません。**

図 5-3 **は、**2 **台の筐体にまたがる** 2 **つの** VLAN**、***Accounting* **と** *Engineering* **の設定例です。両筐体とも、ポート** 1 **～** 4 **は** VLAN *Accounting* **に、ポート** 5 **～** 8 **は**VLAN *Engineering* **に所属しています。**VLAN *Accounting* **は、上の筐体のポート** 2 **と下の筐体のポート** 4 **で、***Engineering* **は、上の筐体のポート** 5 **と下の筐体のポート** 8 **で接続されています。**

図 5-3：2台の筐体にまたがって構成された 2 つのポート VLAN



上記の手順にそって筐体間を数珠つなぎにすれば、3 台以上の筐体にまたがる VLAN を作成することも可能です。各筐体には、VLAN ごとに他の筐体と接続するためのポートが必要です。筐体間を接続するときは、同じ VLAN に所属するポート同士を接続します。

タグ VLAN

タグ付け（Tagging）とは、イーサネットフレームに「タグ」と呼ばれる目印を挿入することをいいます。タグには、VLAN の識別に使う VLANid が含まれています。

IEEE 802.1Q 準拠のタグ付きフレームは、IEEE 802.3/Ethernet で定められた 1518 バイトよりもサイズが大きくなる可能性があります。そのため、他の機器ではパケットエラーが記録される可能性があります。また、経路上に 802.1Q に対応していないブリッジやルータがある場合は、通信不良が発生する可能性もあります。

タグ VLAN の用途

通常、VLAN タグは複数の筐体にまたがる VLAN を作成するときに使われます。筐体間のリンクを「トランク」と呼びますが、VLAN タグを使用すれば、トランクを使って複数の筐体にまたがる VLAN を複数作成することができます。ポート VLAN では、図 5-3 のように VLAN ごとにトランクリンクが必要となりますが、タグ VLAN では、2 台の筐体にまたがる複数の VLAN を 1 本のトランクリンクで実現できます。

また、1 つのポートを複数の VLAN に所属させられることもタグ VLAN の利点です。これは、複数の VLAN に所属する必要がある機器（サーバなど）を接続するときに役立ちます。ただし、この機器には IEEE 802.1Q VLAN タギングをサポートするネットワークインタフェースカード（NIC）が必要です。

あるポートが所属できるポート VLAN は 1 つだけです。このポートを他の VLAN にも所属させるには、VLAN タグの設定と 802.1Q VLAN タギングをサポートする NIC が必要です。

VLAN タグの設定

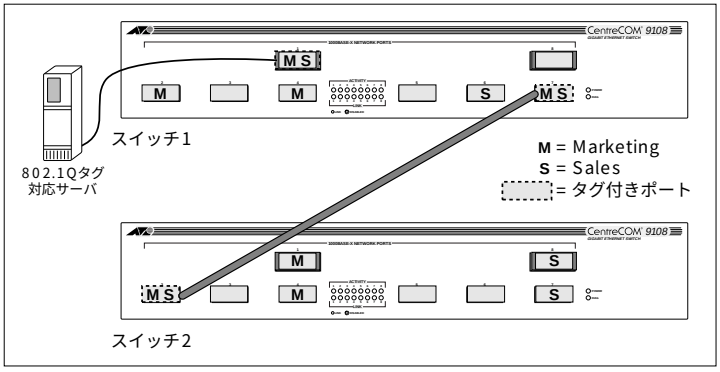
各 VLAN には、802.1Q VLAN タグを 1 つずつ割り当てることができます。802.1Q タグが設定された VLAN にポートを追加する場合、ポートごとに VLAN タグを使用するかどうか選択します。出荷時の状態では、すべてのポートが VLAN *default* に所属しています。VLAN *default* の VLANid は 1 です。

VLAN 内のすべてのポートでタグを使う必要はありません。本製品は、フレームを受け取るたびに、宛先ポートでタグが使用されているかどうかをリアルタイムに判断し、宛先ポートの設定にあわせてタグの追加と削除を行います。

未登録の VLANid を持つタグ付きフレームは破棄されます。

VLAN タグ付きトラフィックと通常のタグなしトラフィックを混在させた例を図 5-4 に示します。

図 5-4：タグ付き / タグなしトラフィックの同時使用例



上記のネットワーク構成をわかりやすくまとめると、図 5-5 のようになります。

図 5-5：タグ付き / タグなしポートの構成図

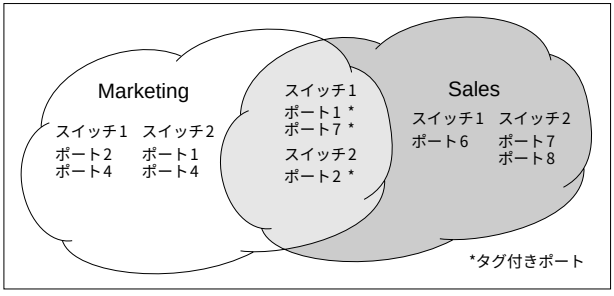


図 5-4、図 5-5 では、

- 両筐体のトランクポートは、VLAN *Marketing* と VLAN *Sales* のトラフィックを通します。
- トランクポートでは VLAN タグを使用します。
- スイッチ 1 のポート 1 に接続されたサーバには、IEEE 802.1Q VLAN タギング対応の NIC が装着されています。
- スイッチ 1 のポート 1 に接続されたサーバは、VLAN *Marketing* と VLAN *Sales* の両方に所属しています。
- それ以外のポートでは VLAN タグを使用していません。

本製品は、データを送信するにあたって、宛先ポートでタグが使われているかどうかを判断します。さきほどの例では、サーバが送受信するフレームにはすべてタグが付いています。また、トランクポートが送受信するフレームもすべてタグ付きです。それ以外のポートで送受信されるフレームにはタグが付いていません。

ポート VLAN とタグ VLAN の同時使用

ポート VLAN とタグ VLAN は同時に使用することができます。ただし、1 つのポートが所属できるポート VLAN は 1 つだけです。言い換えれば、各ポートは 1 つのタグなし VLAN と、複数のタグ付き VLAN に所属できます。

VLANid 0のIEEE 802.1Qタグを持つフレームは、タグなしフレームとして扱われます。

GVRP（GARP VLAN Registration Protocol）

GVRP（GARP VLAN Registration Protocol）は、IEEE 802.1Q ドラフト標準で規定されている VLAN 情報交換のためのプロトコルです。GVRP 対応のネットワーク機器は、他の機器にシグナルを送り、自分が所属している VLAN のトラフィックを要求します。GVRP の主目的は、ネットワーク機器間で VLAN 情報を自動的に交換し、機器ごとに設定を行う手間を省くことにあります。GVRP はネットワークサーバにも実装することができます。こうしたサーバは通常複数の VLAN に所属しており、GVRP を使ってネットワーク上のスイッチに自分が所属している VLAN がどれかを伝達します。

図 5-6 に GVRP を使用したネットワークの例を示します。

図 5-6：GVRPを使用したネットワーク

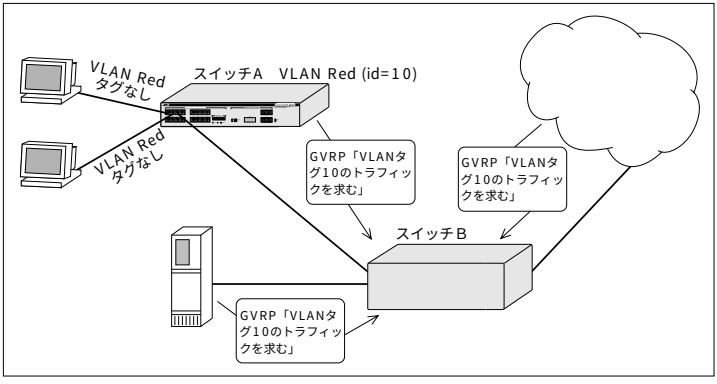


図 5-6 では、スイッチ A は VLAN *Red*（VLANid = 10）に所属しています。スイッチ A のポート 1 とポート 2 は、タグなしに設定されています。

スイッチ A の設定方法は次のとおりです。

```
create vlan red
config vlan red tag 10
config vlan red add ports 1-2 untagged
enable gvrp
```

スイッチ B では、VLAN やタグ付けに関する設定を行う必要はありません。その代わり、スイッチ B に接続されているサーバや他のネットワークは、GVRP を使ってどのトラフィックが必要であるかをスイッチ B に伝えます。スイッチ A は、VLAN *Red* へのアクセスを必要とする機器がポート 3 に接続されていることを知ると、自動的にポート 3 を VLAN *Red* に追加します。

GVRP によって自動生成された VLAN（VLANid = 10）には、次のような名前が付けられます。

```
gvrp vlan xxxx
```

xxxx の部分には、10 進表記の VLANid が入ります。GVRP によって発見されたこれらの VLAN は、NVRAM（不揮発性メモリ）に保存されないため、スイッチを再起動すると消えてしまいます。また、GVRP VLAN では、ポートを追加したり削除したりすることはできません。

GVRP では、明示的に指定されていないかぎり、情報交換対象の VLAN はタグ付きであると仮定しています。通常、ネットワークのエッジ部分ではタグなし VLAN を使い、ネットワークのコア部分では、GVRP を使ってスイッチ間で自動的にタグ VLAN が構成されるようにします。

GVRP VLAN に IP アドレスを割り当てることはできません。

GVRP とスパニングツリードメイン（STPD）

GVRP によって自動生成された VLAN は、すべてデフォルトの STPD（*s0*）に所属します。同一物理ポート上に複数の STPD を設定することができないため、2 つの GVRP クライアントが別々の STPD に所属する VLAN に参加しようとすると、2 つ目のクライアントが拒否されてしまいます。GVRP を使用する可能性のある VLAN はすべて同じ STPD に所属させてください。これを実現する一番簡単な方法は、STPD の設定をデフォルトのままにしておくことです。これにより、すべての VLAN がデフォルト STPD の *s0* 所属となります。

GVRP コマンド

表 5-1 に GVRP 関連コマンドの一覧を示します。

表 5-1：GVRP コマンド

コマンド名	機能
enable gvrp	GVRP をイネーブルにします。デフォルトはディセーブルです。

表 5-1：GVRP コマンド

コマンド名	機能
config gvrp [listen | send | both | none] ports [<portlist> | all]	指定したポートの GVRP 送受信モードを設定します。 • `listen` − GVRP パケットを受信します。 • `send` − GVRP パケットを送信します。 • `both` − GVRP パケットを送受信します。 • `none` − GVRP 情報の交換を行いません。 デフォルトは `both` です。
disable gvrp	GVRP をディセーブルにします。
show gvrp	現在の GVRP 設定とステータスを表示します。

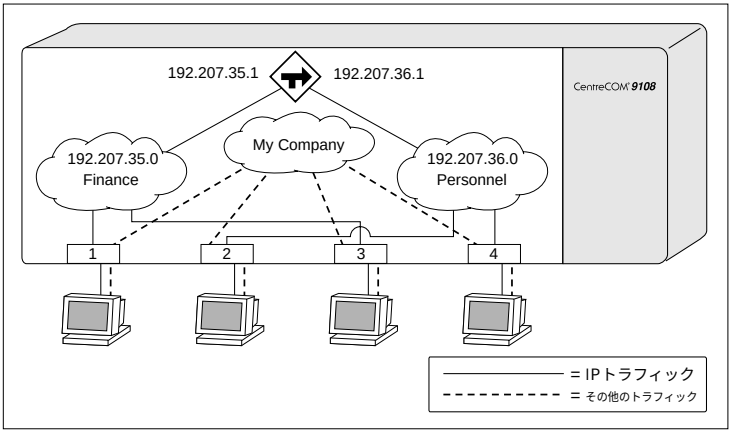
プロトコル VLAN

プロトコル VLAN は、パケットフィルタを使ってプロトコルごとに VLAN を構成する機能です。

プロトコル VLAN は、通常マルチプロトコル環境で使用されます。図 5-7 の例では、各ホストが IP プロトコルと NetBIOS プロトコルを使用しています。

IP トラフィックは、2 つの IP サブネット（192.207.35.0 と 192.207.36.0）に分割され、サブネット間は本製品によって内部的にルーティングされています。2 つのサブネットには、それぞれ *Finance* と *Personnel* という VLAN 名が付けられています。IP 以外のトラフィックはすべて、*MyCompany* という VLAN に所属しています。ここでは、すべてのポートが VLAN *MyCompany* に所属しています。

図 5-7：プロトコル VLAN



プロトコルフィルタの定義

本製品では、上記の定義済みフィルタに加え、独自のプロトコルフィルタを 7 つまで定義できます。プロトコルの判別には、EtherType、LLC、SNAP のいずれかを使います。1 つのプロトコルフィルタには、最大 6 つのプロトコルタイプを含めることができます。プロトコルフィルタの定義方法は次のとおりです。

1 次のコマンドを使ってプロトコルフィルタを作成します。

```
create protocol <protocol_name>
```

例

```
create protocol fred
```

プロトコルフィルタ名は、31 文字以内で指定します。

2 次のコマンドでプロトコルを定義します。

```
config protocol <protocol_name> add <protocol_type> <hex_value>
```

<protocol_type> には次のいずれかを指定します。

- etype ― EtherType

  etype のあとには、EtherType フィールドの値を示す 4 文字の 16 進数を指定します。EtherType の一覧は IEEE によって管理されており、以下の URL で参照することができます。

  http://standards.ieee.org/regauth/ethertype/index.html

- llc ― LLC SAP

  llc のあとには、LLC Destination SAP（DSAP）フィールドと LLC Source SAP（SSAP）フィールドの値をつなげた 4 文字の 16 進数を指定します。LLC SAP の一覧は以下の URL で参照できます。

  http://stdsbbs.ieee.org/pub/general/LLC_list.txt

- snap ― IEEE SNAP ヘッダ内の Ethertype フィールドの値を指定します。

  snap の値は、etype と同じ 4 文字の 16 進数です。

```
config protocol fred add llc feff
config protocol fred add snap 9999
```

プロトコルフィルタは 15 個まで定義できます。また各プロトコルフィルタには、プロトコルタイプを 6 つまで含めることができます。ただし、同時に 7 つを超えるプロトコルをアクティブにしたり、使用することはできません。

SNAP ヘッダによる EtherType のカプセル化については、TR 11802-5:1997 (ISO/IEC) [ANSI/IEEE std. 802.1H, 1997 Edition] をご覧ください。

定義済みのプロトコルフィルタ

本製品にはあらかじめ次のプロトコルフィルタが用意されています。

表 5.2：定義済みプロトコルフィルタ

フィルタ名	フィルタの定義内容
IP	etype 0800 etype 0806
IPX	etype 8137
IPX_8022	llc e0e0
IPX_SNAP	snap 8137
NetBIOS	llc f0f0
DECNet	etype 6003 etype 6004
AppleTalk	snap 809b snap 80f3

プロトコルフィルタの削除

VLAN に割り当てていたプロトコルフィルタを削除すると、その VLAN には none というプロトコルが割り当てられ、まったくフレームが転送されない状態となります。フレームの転送を再開させるには、VLAN に別のプロトコルを割り当ててください。

VLAN タグとプロトコルフィルタの優先順位

VLAN にタグとプロトコルフィルタの両方が設定されている場合、同一ポート上ではプロトコルフィルタよりも VLAN タグが優先されます。

5.3 VLAN 名について

VLAN は 256 個まで作成できます。各 VLAN には 32 文字以内で名前を付けます。VLAN 名に使用できる文字は、基本的に英数字のみです。次に挙げる文字を VLAN 名に使用することはできません。また、VLAN 名の先頭はアルファベットでなくてはなりません。

- スペース
- コンマ
- 引用符

VLAN 名はローカルでのみ意味を持ちます。つまり、あるスイッチで使われている VLAN 名はそのスイッチでのみ有効となり、そのスイッチに他のスイッチを接続したとしても、その VLAN 名は他のスイッチにとって意味を持ちません。

VLAN 名が筐体内でしか意味を持たないとしても、VLAN 名の命名には一貫したポリシーを適用することをおすすめします。

出荷時に定義されているデフォルト VLAN

本製品の出荷時には、つぎのような属性を持つデフォルトの VLAN が定義されています。

- VLAN 名は、*default*。
- すべてのポートが所属。
- すべてのポートがタグなしフレームを使用。内部で使用される VLANid は 1。

5.4 VLAN の設定

ここでは、VLAN 設定用コマンドについて説明します。VLAN 設定の手順は以下のとおりです。

1 VLAN を作成して名前を付けます。

```
create vlan <name>
```

2 必要に応じ、VLAN に IP アドレスまたは IPX ネットワーク番号を設定します。

```
config vlan <name> ipaddress <ipaddress> <mask>
```

```
config vlan <name> xnetid <netid> [enet_ii | enet_8023 | enet_8022 |
enet_snap]
```

VLAN に、IPX ネットワーク番号と IP アドレスの両方を同時に割り当てることはできません。IPX の詳細については、第 12 章「IPX ルーティング」をご覧ください。

VLAN に IP アドレスを割り当てるときは、IP アドレスとネットマスクによって表されるサブネットアドレスが他と重複しないようにしてください。同じ IP サブネットを複数の VLAN に割り当てることはできません。

3 VLAN タグを使用する場合は、VLANid を割り当てます。

```
config vlan <name> tag <value>
```

また、プロトコルフィルタを適用する場合は、次のコマンドを使います。

```
config vlan <name> protocol [<protocol_name> | any]
```

4 ポートを VLAN に割り当てます。

```
config vlan <name> add ports [<portlist> | all] {tagged | untagged}
```

802.1Q タグを使用する場合は、追加するポートごとにタグの有無を指定します。

表 5-3 に VLAN 設定コマンドの一覧を示します。

表 5-3：VLAN 設定コマンド

コマンド名	機能
create vlan <name>	VLAN を作成します。
create protocol <protocol_name>	ユーザ定義のプロトコルを作成します。
enable ignore-stp vlan <name>	指定した VLAN で STP ポート情報を無視するよう設定します。これがイネーブルの場合、VLAN 内の全ポートが STP のフォワーディング状態になります。デフォルトはディセーブルです。
config dot1q ethertype <ethertype>	IEEE 802.1Q パケットのイーサネットプロトコルタイプ（Ethertype）を設定します。このコマンドを使う必要があるのは、他の 802.1Q 対応スイッチが、本製品と異なる Ethertype を使用している場合です。本製品におけるデフォルト値は `8100` です。
config protocol <protocol_name> [add | delete] <protocol_type> <hex_value> {<protocol_type> <hex_value>} ...	プロトコルフィルタの設定を行います。`<protocol_type>` には次のいずれかを指定します。 • `etype` • `llc` • `snap` `<hex_value>` には、`<protocol_type>` で指定した、EtherType、LLC DSAP/SSAP、あるいは SNAP エンコーディングされた EtherType のいずれかを示す、0000 ～ FFFF の 4 桁の 16 進数を指定します。
config vlan <name> ipaddress <ipaddress> {<mask>}	VLAN に IP アドレスとネットマスク（省略可）を割り当てます。
config vlan <name> xnetid <netid> [enet_ii | enet_8023 | enet_8022 | enet_snap]	VLAN に IPX ネットワーク番号を割り当てます。また、同時にフレームタイプも指定します。
config vlan <name> add ports [<portlist> | all] {tagged | untagged}	VLAN にポートを追加します。指定したポートで VLAN タグを使うかどうかも指定できます。デフォルトは `untagged` です。
config vlan <name> delete ports [<portlist> | all]	VLAN からポートを削除します。
config vlan <name> protocol [<protocol_name> | any]	プロトコル VLAN の設定を行います。キーワード `any` を指定した場合、その VLAN はデフォルト VLAN になります。他のプロトコル VLAN に分類できないパケットはすべて、該当するポートのデフォルト VLAN に転送されます。
config vlan <name> qosprofile [<qosname> | none]	VLAN に QoS プロファイルを割り当てます。`none` はデフォルト QoS プロファイル *qp1* を表します。このコマンドを実行すると、FDB 内のダイナミックエントリがいったんフラッシュされます。
config vlan <name> tag <vlanid>	VLANid（1 ～ 4095）を割り当てます。

VLAN 設定例

次の例では、ポート VLAN *accounting* を作成し、IP アドレスを 132.15.121.1 に設定し、ポート 1、2、3、6 を割り当てています。

```
create vlan accounting
config vlan accounting ipaddress 132.15.121.1
config vlan default delete ports 1-3,6
config vlan accounting add ports 1-3,6
```

VLAN 名は重複しないように設定してください。いったん VLAN 名を定義した後は、コマンド中でキーワード vlan を省略できます。

次は、*video* という名前を持つタグ VLAN の作成例です。VLANid として 1000 を割り当て、ポート 4 からポート 8 をこの VLAN に追加しています。

```
create vlan video
config vlan video tag 1000
config vlan video add ports 4-8 tagged
```

次の例では、VLANid = 120 の VLAN *Sales* を作成しています。この VLAN では、タグ付きフレームとタグなしフレームの両方を使用しています。ポート 1 からポート 3 はタグ付き、ポート 4 とポート 7 はタグなしです。明示的に指定しなかった場合はタグなしとなることに注目してください。

```
create vlan sales
config vlan sales tag 120
config vlan sales add ports 1-3 tagged
config vlan sales add ports 4,7
```

次は、プロトコル VLAN *IPSales* にポート 6 からポート 8 を割り当てた例です。

```
create vlan ipsales
config vlan ipsales protocol ip
config vlan ipsales add ports 6-8
```

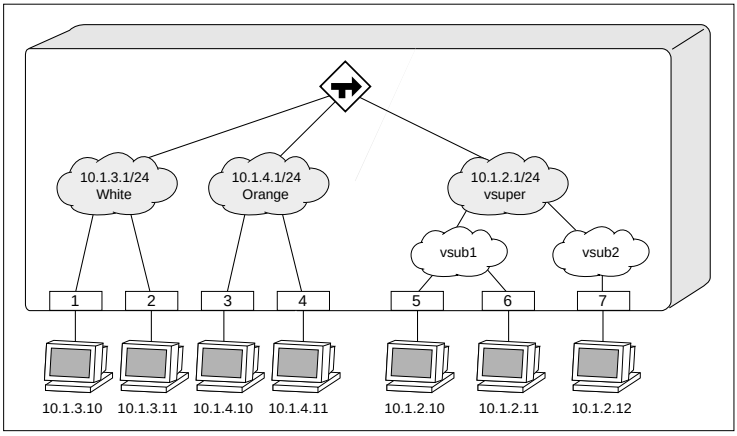
次の例では、プロトコルフィルタ *myprotocol* を定義して、VLAN *myvlan* に適用しています。本例はあくまでも説明のためのサンプルであり、実用的な例ではありませんのでご注意ください。

```
create protocol myprotocol
config protocol myprotocol add etype 0xf0f0
config protocol myprotocol add etype 0xffff
create vlan myvlan
config vlan myvlan protocol myprotocol
```

5.5 VLAN アグリゲーション機能

VLAN アグリゲーションは、IP サブネット（スーパー VLAN）を任意の大きさのブロードキャストドメインに分割し（サブ VLAN）、なおかつサブ VLAN 間で、スーパー VLAN に割り当てた IP アドレスをデフォルトゲートウェイアドレスとして共用し、IP アドレススペースを有効活用するための機能です。図 5-8 に例を示します。

図 5-8：VLAN アグリゲーション



VLAN アグリゲーションでは、次に挙げる 2 種類の VLAN を作成します。

- **スーパー VLAN** － 所属ポートを持たない VLAN。スーパー VLAN には IP アドレスを割り当て、後述するサブ VLAN 共通のデフォルトゲートウェイとして機能させます。ICMP エコー要求（ping などで使用）への応答にのみ使用する 2 つ目の IP アドレスを割り当てることもできます。
- **サブ VLAN** － 実際にポートを割り当てるのは、スーパー VLAN の下位に配置されるサブ VLAN です。サブ VLAN には IP アドレスを割り当てませんが、個々のホストには適宜 IP を割り振り、デフォルトゲートウェイとしてスーパー VLAN の IP アドレスを設定します。サブ VLAN 間の通信はデフォルトで可能になっていますが、禁止することも可能です。

VLAN アグリゲーションの動作

ここでは、VLAN アグリゲーションの動作について説明します。

- ブロードキャストおよび宛先不明（unknown）のトラフィックは各サブ VLAN 内で完結し、他のサブ VLAN には転送されません。すなわち、サブ VLAN ＝ブロードキャストドメインとなります。各サブ VLAN は、デフォルトゲートウェイアドレスだけを共有します。
- 通常、スーパー VLAN にはポートを割り当てません。実際にホストが所属するのは、サブ VLAN です。各ホストには、スーパー VLAN に割り当てたネットワークアドレスの範囲か

ら自由に IP アドレスを割り当てることができます。サブ VLAN 内のホストには、スーパー VLAN と同じネットマスクを割り当てます。また、サブ VLAN 内のホストには、デフォルトゲートウェイアドレスとしてスーパー VLAN のルータインタフェースの IP アドレスを設定します。

- サブ VLAN 間の IP トラフィックは、必ずスーパー VLAN のルータインタフェースを経由します。すなわち、スーパー VLAN にサブ VLAN を追加すると、自動的に Proxy ARP エントリが作成され、Proxy ARP による間接ルーティングが行われます。
- スーパー VLAN で IP マルチキャストルーティングプロトコルがイネーブルに設定されている場合は、サブネット間で IP マルチキャストトラフィックが転送されます。

制限事項

VLAN アグリゲーションには、以下の制限事項がありますのでご注意ください。

- サブ VLAN 内にルータを配置することはできません。サブ VLAN は、末端のネットワークで使用します。
- サブ VLAN 内のホストは DHCP / BOOTP リレー機能を利用できません。
- サブ VLAN を、別のサブ VLAN のスーパー VLAN にすることはできません。また、同様に、スーパー VLAN を他方ではサブ VLAN に設定することもできません。
- サブ VLAN には IP アドレスを割り当てることができません。
- 通常、スーパー VLAN にはポートを割り当てません（ERRP 使用時は例外です。詳しくは、5-16 ページの「VLAN アグリゲーションと ERRP の併用」をご覧ください）。
- サブ VLAN 内のホストを別のサブ VLAN に移動した場合は、ホストかスイッチの ARP テーブルをいったんクリアする必要があります。

サブ VLAN 間通信

デフォルトでは、サブ VLAN をスーパー VLAN に追加すると、自動的に Proxy ARP エントリが作成され、サブ VLAN 間の通信ができるようになります。サブ VLAN 間の通信を禁止するには、次のコマンドを実行して、Proxy ARP エントリの自動追加をディセーブルにします。

```
[enable | disable] subvlan-proxy-arp vlan [<super_vlan_name> | all]
```

VLAN アグリゲーションの設定

VLAN アグリゲーションの設定は、以下の手順で行います。

図 5-8 では、スーパー VLAN *vsuper* の下に、2 つのサブ VLAN *vsub1* と *vsub2* を作成しています。

1 スーパー VLAN を作成し、IP アドレスを割り当てます。

```
create vlan vsuper
config vlan vsuper ipaddress 10.1.2.1/24
```

2 IP ルーティングとルーティングプロトコルをイネーブルにします。

```
enable ipforwarding
enable ospf
config ospf add vlan vsuper
```

3 サブ VLAN を作成し、ポートを割り当てます。

```
create vlan vsub1
config vlan vsub1 add ports 5,6
create vlan vsub2
config vlan vsub2 add ports 7
```

4 スーパー VLAN にサブ VLAN を割り当てます。

```
config vlan <super_vlan_name> [add | delete] subvlan <sub_vlan_name>
```

```
config vlan vsuper add subvlan vsub1
config vlan vsuper add subvlan vsub2
```

5 サブ VLAN 間の通信を禁止したい場合は、次のコマンドを実行します。

```
disable subvlan-proxy-arp vlan [<super_vlan_name> | all]
```

```
disable subvlan-proxy-arp vlan vsuper
```

VLAN アグリゲーションの設定確認には、次のコマンドを使います。

- show vlan ― サブ VLAN とスーパー VLAN の関係を確認できます。
- show iparp ― ARP エントリと関連するスーパー / サブ VLAN の情報が表示されます。

```
C9100:102# show iparp vlan vsuper

Destination     Mac               Age Flags  Vlan
10.1.2.10       00:00:f4:30:4c:b2    3       sub VLAN: vsub1 vsuper (4092)
```

VLAN アグリゲーションと ERRP の併用

VLAN アグリゲーションと ERRP を併用する場合は、次の手順にしたがいます。

1 スーパー VLAN を作成し、IP アドレスを割り当てます。

```
create vlan vsuper
config vlan vsuper ipaddress 10.1.2.1/24
```

2 IP ルーティングとルーティングプロトコルをイネーブルにします。

```
enable ipforwarding
enable ospf
config ospf add vlan vsuper
```

3 サブ VLAN を作成し、ポートを割り当てます。

```
create vlan vsub1
config vlan vsub1 add ports 5,6
creste vlan vsub2
config vlan vsub2 add ports 7
```

4 スーパー VLAN にサブ VLAN を割り当てます。

```
config vlan vsuper add subvlan vsub1
config vlan vsuper add subvlan vsub2
```

次に、スーパー VLAN で ERRP をイネーブルにするために必要な設定を行います。

5 スーパー VLAN に 802.1Q タグを割り当てます。

```
config vlan vsuper tag 1234
```

6 スーパーVLAN に、サブ VLAN と共通のポートをタグ付きとして割り当て、ERRP をイネーブルにします。

```
config vlan vsuper add ports 5-7 tagged
enable esrp vlan vsuper
```

ERRP 設定コマンドのキーワードは、ERRP ではなく **ESRP** です。間違えやすいのでご注意ください。

設定確認には、次のコマンドを使います。

- `show vlan` — サブ VLAN とスーパー VLAN の関係を確認できます。
- `show esrp` — ERRP の設定を確認できます。

表 5-4 に、VLAN アグリゲーションの設定コマンド一覧を示します。

表 5-4：VLAN アグリゲーション設定コマンド

コマンド名	機能
config vlan <super_vlan_name> [add | delete] subvlan <sub_vlan_name>	スーパー VLAN にサブ VLAN を割り当てもしくは削除します。
config vlan <super_vlan_name> [add | delete] secondary-ip <ipaddress>/32	スーパー VLAN に 2 つ目の IP アドレスを割り当てます。このアドレスは、ICMP エコー要求（ping などで使用）への応答にのみ使用されます。
enable subvlan-proxy-arp vlan [<super_vlan_name> | all]	サブ VLAN 間の通信をイネーブルにします。デフォルトはイネーブルです。
disable subvlan-proxy-arp vlan [<super_vlan_name> | all]	サブ VLAN 間の通信をディセーブルにします。

5.6 VLAN 設定の確認

VLAN の設定状況を確認するには、次のコマンドを使います。

```
show vlan {<name>}
```

次に出力例を示します。

```
C9100:61 # show vlan

VLAN "Default" created by user
     Tagging:   802.1Q Tag 1
     IP:        Not configured.
     IPX:       1234 with encapsulation type ether-II
     STPD:      Domain "s0" is not running spanning tree protocol
     Protocol:  Match all unfiltered protocols.
     Qos Profile:       QP1
     Ports:     2.     (Number of active port=2)
                Untag:  1 2

VLAN "orange" created by user
     Tagging:   Untagged (Internal tag 4091)
     IP:        10.3.2.1/255.255.255.0
     IPX:       Not configured
     STPD:      Domain "s0" is running spanning tree protocol
     Protocol:  Match all unfiltered protocols.
     Qos Profile:       QP1
     Ports:     6.     (Number of active port=6)
                Untag:  3 4 5 6 7 8
```

show vlan コマンドを実行すると、VLAN ごとに次のような設定情報が表示されます。

- VLAN 名
- VLANid
- VLAN の作成方法（user または GVRP）
- IP アドレス
- IPX ネットワーク番号とフレームタイプ
- STPD
- プロトコル
- QOS プロファイル
- 所属ポート
- ポートのタグ設定

プロトコル情報を表示するには、次のコマンドを実行します。

```
show protocol {<protocol_name>}
```

show protocol コマンドによって表示される情報は以下のとおりです。

- プロトコル名
- プロトコルタイプを示すヘッダフィールド（etype、llc、snap）
- プロトコルタイプ値

5.7 VLAN の削除

VLAN を削除する、あるいは VLAN 設定をデフォルト値に戻すには、表 5-5 のコマンドを使います。

表 5-5：VLAN の削除 / リセット用コマンド

コマンド名	機能
disable ignore-stp vlan <name>	VLAN が STP ポート情報を使うようにします。
unconfig vlan <name> ipaddress	VLAN に割り当てた IP アドレスをリセットします。
unconfig vlan <name> xnetid	VLAN に割り当てた IPX ネットワーク番号をリセットします。
delete vlan <name>	VLAN を削除します。
delete protocol <protocol_name>	プロトコルを削除します。

6　フォワーディングデータベース（FDB）

この章では、フォワーディングデータベース（FDB）の概要と設定方法について説明します。

6.1 概要

本製品は、受信したフレームの送信元MAC アドレスと受信したポートの関係を、フォワーディングデータベース（FDB）に記憶しています。本製品は、このデータベースの情報を使って、受信したフレームをどのポートに転送すればよいかを判断します。

FDB の内容

FDB には、最大 128K のエントリを格納することができます。各エントリは、送信元機器の MAC アドレス、フレームを受信したポートの識別子、送信元機器が所属する VLAN の識別子から構成されます。受信したフレームの宛先 MAC アドレスが FDB に登録されていない場合、そのフレームは同一 VLAN 内のすべての機器に送信されます。

FDB エントリの種類

FDB エントリには、次のような種類があります。

- **ダイナミック エントリ** － 自己学習機能によって動的に登録されるエントリです。出荷時や初期化直後には、ダイナミックエントリしか存在しません。一定期間（エージングタイム）送信が行われなかったダイナミックエントリは、FDB から削除されます（エージアウト）。これは、ネットワーク構成の変更にあわせて FDB 内のエントリを更新し、FDB が古いデータでいっぱいになるのを防ぐための措置です。ダイナミックエントリは、スイッチを再起動したり電源を切ったりすると消去されます。エージングタイムの設定については、6-3 ページの「FDB エントリの設定」をご覧ください。
- **ノンエージングエントリ** － FDB のエージングタイムをゼロに設定したため、エージアウトされなくなったダイナミックエントリです。ただし、再起動したり電源を切ったりすると消去されます。
- **パーマネントエントリ** － システム管理者によって手動登録されたエントリで、スイッチを再起動しても消去されないエントリです。パーマネントエントリには、単一の MAC アドレスだけでなく、マルチキャストの MAC アドレスも登録できます。コマンドラインインタフェースを使って登録したエントリは、すべてパーマネントエントリになります。パーマネントエントリは、64 個まで登録できます。

一度作成されたパーマネントエントリは、以後作成時のままで変化しません。そのため、次に挙げるようなイベントが発生しても、パーマネントエントリは更新されませんのでご注意ください。

- VLAN が削除された
- VLANid が変更された
- ポートの VLAN タグ設定（タグ付き / タグなし）が変更された
- VLAN からポートが削除された
- ポートがディセーブル状態になった
- ポートがブロッキング状態になった
- ポートの QoS 設定が変更された
- ポートに障害が発生した（リンクがダウンした）

- **ブラックホールエントリ** ― ブラックホールエントリは、特定の宛先 MAC アドレスを持つフレームを転送せずに破棄するためのエントリです。ブラックホールエントリは、セキュリティ対策など、特定のアドレスへの送信を禁止したい場合に便利です。ブラックホールエントリは、ダイナミックエントリと同じように再起動すると消去されますが、エージアウトはされません。

FDB エントリの追加

FDB にエントリが追加されるのは、次のような場合です。

- **MAC アドレス学習機能による自動登録** ― 受信したフレームの送信元 MAC アドレス、ポート、VLAN といった情報から、ダイナミックエントリを自動的に作成・追加します。
- **管理者による手動登録** ― 次節で述べるように、MIB ブラウザや SNMP 対応ネットワークマネージャ、コマンドラインインタフェースを使って、FDB エントリを手動で追加登録できます。

FDB エントリに QoS プロファイルを割り当てる

動的に学習される MAC アドレス（と VLAN）には、QoS プロファイルを割り当てることができます。QoS プロファイルを割り当てられたエントリは、ダイナミックエントリと同様に扱われます。つまり、このエントリは、学習機能によって FDB に登録され、エージアウトの対象となります。あらかじめ QoS を割り当てられたエントリが学習によって登録されると、ただちに QoS プロファイルが適用されます。

6.2 FDB エントリの設定

FDB エントリを設定するには、表 6-1 のコマンドを使います。

表 6-1：FDB 設定コマンド

コマンド名	機能
create fdbentry <mac_address> vlan <name> [blackhole | ports [<portlist> | all] | dynamic] {qosprofile <qosname>}	FDB エントリを作成します。以下のパラメータを指定します。 • mac_address ー MAC アドレス。1 バイトごとにコロンで区切った 16 進数で指定します。 • name ー 所属する VLAN 名を指定します。 • blackhole ー 指定した MAC アドレスをブラックホールエントリにします。 • portlist ー 指定した MAC アドレスを持つ機器が接続されているポートの番号を指定します。 • dynamic ー 指定したエントリをダイナミックエントリにします。これは、QoS プロファイルを割り当てるときに使います。 • qosname ー MAC アドレスに割り当てる QoS プロファイルを指定します。 パーマネントエントリの作成時に複数のポートを指定した場合、そのエントリ宛てのフレームは複数のポートにマルチキャストされます。
config fdb agingtime <value>	FDB のエージングタイムを設定します。有効範囲は 15 ～ 1000000 秒、デフォルトは 300 秒です。0 を指定した場合、ダイナミックエントリはエージアウトされないノンエージングエントリになります。
enable learning ports <portlist>	指定したポートの MAC アドレス学習機能をイネーブルにします。
disable learning ports <portlist>	指定したポートの MAC アドレス学習機能をディセーブルにします。これは、おもにセキュリティ対策のために使用されます。MAC アドレス学習機能がオフの場合、ブロードキャストフレームと、当該ポートのパーマネント MAC アドレスに宛てたフレームだけが転送されます。デフォルトはイネーブルです。

FDB 設定例

次に、FDB にパーマネントエントリを追加する例を示します。

```
create fdbentry 00:E0:2B:12:34:56 vlan marketing ports 4
```

このパーマネントエントリは、次のような属性を持っています。

- MAC アドレスは 00:E0:2B:12:34:56
- VLAN 名は *marketing*
- ポート番号は 4

次の例では、ダイナミックエントリに QoS プロファイル *qp2* を割り当てています。

```
create fdbentry 00:A0:23:12:34:56 vlan net34 dynamic qosprofile qp2
```

このエントリの属性は、以下のとおりです。

- MAC アドレスは 00:A0:23:12:34:56
- VLAN 名は *net34*
- 学習機能によって登録されるダイナミックエントリである
- 学習後、QoS プロファイル *qp2* が適用される

6.3 FDB エントリの確認

FDB エントリを表示するには、次のコマンドを使います。

```
show fdb {<mac_address> | vlan <name> | ports <portlist> | permanent}
```

`show fdb` コマンドのオプションは、以下のとおりです。

- `<mac_address>` ― 指定した MAC アドレスを持つエントリを表示します。
- `<name>` ― 指定した VLAN に属するエントリを表示します。
- `<portlist>` ― 指定したポートに関連するエントリを表示します。
- `permanent` ― すべてのパーマネントエントリを表示します。

次に、FDB 内のすべてのエントリを表示させた例を示します。

```
C9100:140# show fdb

Index    Mac                Vlan           Flags  Port List
-------------------------------------------------------------
0ff0: 0  ff:ff:ff:ff:ff:ff  Default(0001)   sm    CPU,1,19
1823: 0  08:00:4e:2b:f3:00  Default(0001)   sm    CPU
2bfb: 0  00:80:c7:01:cb:bd  Default(0001)   dm    1
373d: 0  01:80:c2:00:00:00    (0000)        sm    CPU

Total: 5 Static: 4 Perm: 0 Dyn: 1 Dropped: 0
FDB Aging time: 300 seconds
```

`show fdb` コマンドが出力する情報は以下のとおりです。

- MAC アドレス
- VLAN 名と VLANid

  VLANid `0000` は、そのエントリがどの VLAN にも属していない特殊なエントリであることを示します。

- **エントリの種類**（Flags **フィールドに表示**）

  s ー **スタティックエントリ（ユーザが登録）**

  d ー **ダイナミックエントリ（スイッチが学習）**

  m ー MAC **アドレスエントリ**

  i ー IP **ルーティング用** MAC **アドレスエントリ**
- **ポート**
- Index **フィールドは、テクニカルサポートのために使用される情報です。**

6.4 FDB の削除

FDB **内のエントリを削除するには、表** 6-2 **のコマンドを使います。**

表 6-2：FDB エントリ削除コマンド

コマンド名	機能
delete fdbentry <mac_address> vlan <name>	パーマネントエントリを削除します。
clear fdb {<mac_address> | vlan <name> | ports <portlist>}	指定した条件にあてはまるダイナミックエントリを削除します。条件を指定しなかった場合は、すべてのダイナミックエントリが削除されます。

7 スパニングツリープロトコル（STP）

スパニングツリープロトコル（STP）は、ネットワーク上に複数の通信経路を設定することで、耐障害性を高める機能です。本章では、STP の概要と本製品の STP 機能について解説します。

7.1 概要

STP は、複数のブリッジを使って通信経路を多重化することにより、ネットワークの耐障害性を高めるメカニズムです。複数の経路を設定した場合、イーサネットでは禁止されているループが形成されるおそれがありますが、STP では次のようにしてループの形成を防いでいます。

- メイン経路の稼働中は、バックアップ経路をブロックする。
- メイン経路の障害発生時には、バックアップ経路を使用する。

STP は、アメリカ電気電子技術者協会（IEEE）の802 委員会が作成した、IEEE 802.1D ブリッジ標準で規定されています。ここでは、802.1D の用語にあわせるため、本製品をブリッジと称します。

7.2 スパニングツリードメイン（STPD）

本製品は、複数の仮想ブリッジとして機能させることができます。各仮想ブリッジは、それぞれ個別にスパニングツリープロトコルを実行します。このスパニングツリープロトコルの実行単位はスパニングツリードメイン（STPD）と呼ばれ、それぞれ独自の STP パラメータ、ルートブリッジ、アクティブ経路を持ちます。STPD には、複数の VLAN を所属させることができます。

- 各 VLAN は、それぞれ個別のブロードキャストドメインを形成する。
- STP は、適切な箇所で経路をブロックしてループの形成を回避する。
- ブロッキング状態のポートでは、データの送受信がまったく行われない。
- 同一 STPD 内では、所属するすべての VLAN が同じスパニングツリーを使用する。

同一ブロードキャストドメイン内に複数の STPD が存在しないように注意してください。これは、異なる STPD に属する VLAN 同士を外部ブリッジで接続したような場合に起こります。

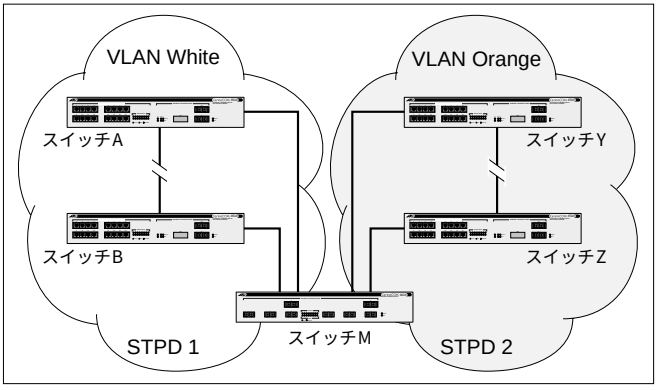
7.3 STP 構成上の注意

STPD の設定を行うときは、必要なトラフィックが正しく転送されるよう、STPD の構成に十分な注意を払ってください。

マルチ STPD

図 7-1 は、VLAN *White* と *Orange* を作成し、それぞれ個別に STPD を形成した例です。各スイッチは、それぞれの STPD 内でループが形成されないよう、適切な箇所でトラフィックをブロックします。この例では、スイッチ A －B 間とスイッチ Y － Z 間の経路がブロックされています。

図 7-1：マルチ STPD 構成



シングル STPD

同一ポート上に複数の VLAN を重ね合わせて設定した場合（VLAN タグ使用時など）は、すべての VLAN を同じ STPD に所属させる必要があります。すなわち、各ポートが所属できる STPD は 1 つだけとなります。

図 7-2 の例では、3 つの筐体すべてに VLAN *White* と *Orange* を設定し、各筐体間を VLAN タグによるトランクポートで接続しています。ここでは、同一ポート上に複数の VLAN を設定しているため、2 つの VLAN を 1 つの STPD に所属させています。

図 7-2 の例では、STPD 内でループが形成されているため、STP の働きによっていずれかのポートがブロッキング状態になり、論理的にループが回避されます。この例では、スイッチ 1 －3 間の経路がブロックされています。

図 7-3 は、図 7-2 のスイッチ 2 から VLAN *Orange* を削除したものです。VLAN *Orange* はスイッチ 2 にポートを持たないため、もしこの構成でスイッチ 1 － 3 の間がブロックされると、VLAN *Orange* に関してはスイッチ 1 － 3 間での通信ができなくなります。一方、VLAN White はすべての筐体にポートを持つため、スイッチ 1 － 2 － 3 の経路で通信可能です。

図 7-2：シングル STPD 構成

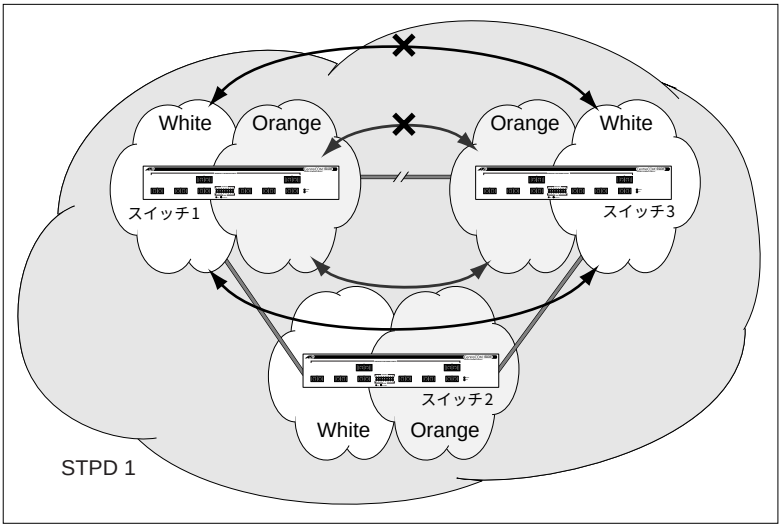
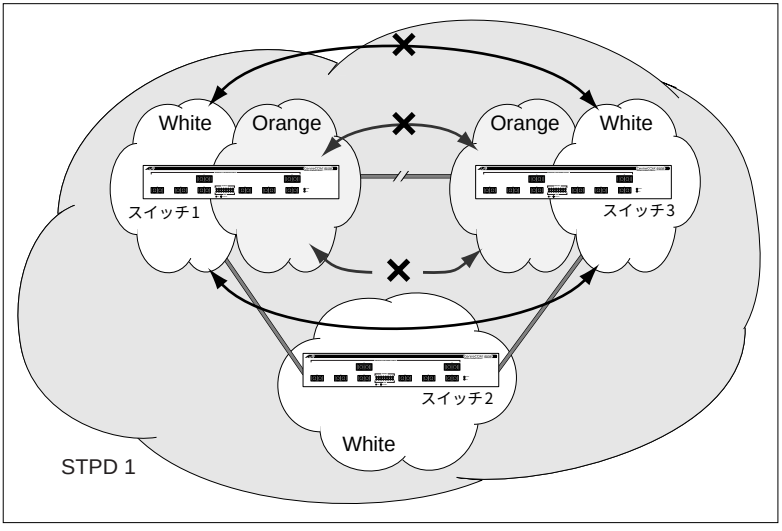


図 7-3：よくない STPD 構成



7.4 STP の設定方法

STP の設定は以下の手順で行います。

1 必要に応じて、STPD を作成します。

```
create stpd <stpd_name>
```

STPD、VLAN、QoS プロファイルには、他と重複しないような名前を付けてください。VLAN名や QoS プロファイル名に使った名前を STPD名として使うことはできません。

2 必要に応じて、STPD に VLAN を追加します。新規作成した VLAN は、デフォルト STPD の *s0* に所属します。

```
config stpd <stpd_name> add vlan <name>
```

3 STPD 内で STP を有効にします。デフォルトはディセーブルです。

```
enable stpd {<stpd_name>}
```

VLAN は必ずどれかの STPD に所属しなくてはなりません。VLAN 内で STP を使いたくないときは、所属する STPD の STP 設定をディセーブルにします。

STPD の作成後は、STP 関連パラメータの調整を行うことも可能です。

STP に関して十分な知識と経験をお持ちでない方は、STP パラメータの設定を変更しないでください。通常は、デフォルトの設定で問題ありません。

以下のパラメータは、STPD ごとに設定できます。

- ハロータイム（Hello time）
- フォワードディレイタイム
- MaxAge
- ブリッジプライオリティ

以下のパラメータは、ポートごとに設定できます。

- パスコスト
- ポートプライオリティ

本製品では、RFC 1493 で規定される標準 Bridge MIB を使用しています。そのため、MIB を通じてアクセスできる STPD はデフォルトの *s0* のみとなります。

出荷時の設定

本製品の出荷時には、*s0* という STPD が定義されています。VLAN *default* は STPD *s0* に所属しています。

STP 関連のパラメータはすべて、IEEE 802.1D の推奨値に設定されています。

GVRP ポートの STP 設定

GVRP によって VLAN に追加されたポートの STP 設定は、所属する VLAN の STP 設定によって決まります。たとえば、VLAN *Red* が STPD *s0* に所属しており、*s0* がイネーブルに設定されているとします。この場合、GVRP によって VLAN *Red* に追加されたすべてのポートで、*s0* がイネーブルになります。GVRP ポートに対しては、通常の STP ディセーブルコマンド（`disable stpd <stpd_name> ports {<portlist>}`）は永続的な効果がありません。

GVRP については、5-6 ページの「GVRP（Generic VLAN Registration Protocol）」をご覧ください。

表 7-1 に STP 設定コマンドの一覧を示します。

表 7-1：STP 設定コマンド

コマンド名	機能
create stpd <stpd_name>	STPD を作成します。作成時のデフォルトパラメータ値は以下のとおりです。 • ブリッジプライオリティ − 32768 • ハロータイム − 2 秒 • フォワードディレイタイム − 15 秒
enable stpd {<stpd_name>}	指定した STPD で STP プロトコルをイネーブルにします。デフォルトはディセーブルです。
enable stpd <stpd_name> ports {<portlist>}	指定したポートで STP プロトコルをイネーブルにします。この場合、ポートが所属する STPD で STP がイネーブルになっていれば、このポートで BPDU が生成されます。デフォルトはイネーブルです。
config stpd <stpd_name> add vlan <name>	STPD に VLAN を追加します。
config stpd <stpd_name> hellotime <value>	ハロータイムを設定します。ルートブリッジになった STPD は、ここで設定された間隔で BPDU（Bridge Protocol Data Unit）を送信します。 有効範囲は 1 〜 10 秒、デフォルトは 2 秒です。
config stpd <stpd_name> forwarddelay <value>	フォワードディレイタイムを設定します。これは、ルートブリッジになった STPD 内のポートが、リスニング、ラーニング状態を経て、フォワーディング状態に移行するまでの時間です。 有効範囲は 4 〜 30 秒、デフォルトは 15 秒です。

表 7-1：STP 設定コマンド

コマンド名	機能
config stpd <stpd_name> maxage <value>	MaxAge を設定します。この時間が過ぎても BPDU を受信できなかった場合、STPD は STP 情報の再構築を行います。 有効範囲は 6 ～ 40 秒、デフォルトは 20 秒です。 MaxAge は、2 ×（ハロータイム＋1）以上、かつ、2 ×（フォワードディレイタイム－1）以下でなくてはなりません。
config stpd <stpd_name> priority <value>	STPD のプライオリティを設定します。この値が小さいほど優先順位が高くなり、STPD がルートブリッジになる可能性が高くなります。 有効範囲は 0 ～ 65535、デフォルトは 32768 です。0 のときにもっともプライオリティが高くなります。
config stpd <stpd_name> ports cost <value> <portlist>	STPD 内のポートのパスコストを設定します。 有効範囲は 1 ～ 65535 です。各ポートには、通信速度に基づいて、以下のデフォルトパスコストが割り当てられます。 • 10Mbps ポート － パスコスト 100 • 100Mbps ポート － パスコスト 19 • 1000Mbps ポート － パスコスト 4
config stpd <stpd_name> ports priority <value> <portlist>	STPD 内のポートのプライオリティを設定します。この値が小さいほど優先順位が高くなり、このポートがルートポートになる可能性が高くなります。 有効範囲は 0 ～ 255、デフォルトは 128 です。0 のときにもっともプライオリティが高くなります。

設定例

次に示すのは、STPD *Backbone_st* の作成例です。この STPD には、VLAN *Manufacturing* が所属しています。ポート 1 ～ 7 と 12 では、STP を無効にしています。

```
create stpd backbone_st
config stpd backbone_st add vlan manufacturing
enable stpd backbone_st
disable stpd backbone_st ports 1-7,12
```

7.5 STP 設定の確認

全ポートの STP 設定を表示するには、次のコマンドを使います。

```
show stpd {<stpd_name>}
```

表示される情報は次のとおりです。

- STPD 名
- ブリッジ ID
- STPD 設定情報

次に出力例を示します。

```
C9100:158# show stpd

Stpd:s0                Stp:DISABLED        Number of Ports:8
Ports: 1,2,3,4,5,6,7,8
Vlans:   Default accounting video sales
BridgeID           80:00:00:e0:2b:00:a4:00
Designated root:   00:00:00:00:00:00:00:00
RootPathCost: 0
MaxAge: 0s         HelloTime: 0s       ForwardDelay: 0s
CfgBrMaxAge: 20s   CfgBrHelloTime: 2s  CfgBrForwardDelay:15s
Topology Change Time: 35s              Hold time: 1s
Topology Change Detected: FALSE        Topology Change:FALSE
Number of Topology Changes: 0
Time Since Last Topology Change: 0s
```

特定のポートの STP 設定を表示するには、次のコマンドを実行します。

```
show stpd <stpd_name> ports [<portlist> | all]
```

表示される情報は次のとおりです。

- STPD ポート設定
- STPD の状態（ルートブリッジの ID など）
- STPD ポートの状態（フォワーディング状態かブロッキング状態か、など）

7.6 STP のディセーブルとリセット

STP を無効にしたり、STP 設定を出荷時の状態に戻したりするには、表 7-2 に示すコマンドを実行します。

STP ディセーブル時には、any 以外のプロトコルフィルタが設定された VLAN では BPDU（Bridge Protocol Data Unit）がフラッディングされません。

表 7-2：STP のディセーブル / リセット用コマンド

コマンド	機能
delete stpd <stpd_name>	STPD を削除します。STPD を削除するには、あらかじめ所属する VLAN をすべて削除しておく必要があります。
disable stpd {<stpd_name>}	指定した STPD で STP プロトコルをディセーブルにします。STPD を指定しなかった場合は、すべての STPD で STP をディセーブルにします。
disable stpd <stpd_name> ports {<portlist>}	指定したポートで STP プロトコルをディセーブルにします。ポートの STP をディセーブルにすると、そのポートはフォワーディング状態になり、そのポートで受信された BPUD はすべて破棄されるようになります。

表 7-2：STP のディセーブル / リセット用コマンド

コマンド	機能
unconfig stpd {<stpd_name>}	指定した STPD の STP パラメータをデフォルト値に戻します。STPD を指定しなかった場合は、すべての STPD の STP パラメータをデフォルトの設定に戻します。

8 QoS（Quality of Service）

この章では、QoS（Quality of Service）の概要と設定方法について説明します。

8.1 概要

QoS は、送出トラフィックに対して任意のサービス品質レベルを設定できる機能です。この機能を利用すれば、異なるトラフィックパターンを持つネットワーク間で、限られた帯域幅を有効に活用することができます。

QoS 最大のメリットは、特定のトラフィックグループに優先的に帯域を割り当てられる点にあります。たとえば、映像データを発信する VLAN には、通常のデータを扱う VLAN よりも優先度の高い QoS プロファイルを割り当てることができます。

8.2 構成要素

QoS の構成要素は以下のとおりです。

- **QoS モード** － Egress モードと Ingress モードがあります（デフォルトは Ingress）。どちらを選択するかによって、利用できる QoS プロファイルの数とトラフィックグループの種類が異なります。
- **QoS プロファイル** － サービス品質レベルを定義します。最小 / 最大帯域幅と優先度（Low、Normal、Medium、High）パラメータで構成されます。
- **トラフィックグループ** － 共通の属性を持つトラフィックを分類したもので、特定 IP アドレスへのトラフィック、特定ポートから送信されるトラフィック、などの分類があります。

QoS 機能を有効にするには、トラフィックグループに対して、任意の QoS プロファイルを割り当てます。トラフィックグループと QoS プロファイルの組み合わせを、QoS ポリシーと呼びます。

8.3 QoS モード

QoS モードには、Ingress モードと Egress モードの 2 種類があります。

- **Ingress モード** － デフォルトの QoS モードです。Egress モードより多くのトラフィックグループを利用できますが、QoS プロファイルはデフォルトの 4 つ（*qp1* ～ *qp4*）しか使えま

せん。デフォルト QoS プロファイルの設定パラメータ（最小 / 最大帯域幅と優先度）は変更可能です。

- **Egress モード** ― 独自の QoS プロファイルを追加作成できますが、利用できるトラフィックグループの種類は Ingress モードよりも少なくなります。QoS プロファイルの設定パラメータも変更可能です。

QoS モードの変更は次のコマンドで行います。ただし、特別な場合を除いて、デフォルトの Ingress モードから Egress モードに変更する必要はありません。詳細については、8-4 ページの「QoS プロファイルとポートキューのマッピング」をご覧ください。

```
config qosmode [ingress | egress]
```

QoS モードの変更は、再起動後から有効になります。QoS モードの設定を確認するには、`show switch` コマンドを使います。

8.4 QoS プロファイル

QoS プロファイルは、以下のパラメータで構成されます。

- **最小帯域幅** ― 最低限確保すべき帯域を全帯域幅のパーセントで指定します。最小値は 0% です。QoS プロファイルの適用時は、他のパラメータにかかわらず、ここで設定した帯域が必ず確保されます。

1 つのポートに対して最小帯域幅の合計が 100% を超えるような設定はできませんのでご注意ください。

- **最大帯域幅** ― トラフィックに割り当てる帯域の上限を、全帯域のパーセントで指定します。たとえ帯域に余裕があっても、ここで指定した以上の帯域が割り当てられることはありません。
- **優先度** ― 最小帯域の確保後に余った帯域を配分する際の優先度を示します。優先度は、以下の 4 つです。
  - Low
  - Normal
  - Medium
  - High

QoS プロファイルは、作成しただけでは意味を持ちません。トラフィックグループに割り当てられて初めてスイッチの動作に影響を与えます。

デフォルト QoS プロファイル（qp1 ～ qp4）

出荷時には、次に挙げる 4 つの QoS プロファイルがあらかじめ定義されています。これらのプロファイルは削除できません。

- *qp1*
- *qp2*
- *qp3*
- *qp4*

デフォルト QoS プロファイルは、Ingress モードと Egress モードの両方で使用できます。Ingress モードでは、デフォルト QoS プロファイルのみ使用できます。Egress モードでは、4 つのデフォルトプロファイルに加え、カスタムプロファイルを 28 個まで追加できます（合計 32 個）。Ingress モードではカスタムプロファイルを追加することはできません。

デフォルト QoS プロファイルのパラメータを表 8-1 にまとめます。

表 8-1：デフォルト QoS プロファイルのパラメータ

プロファイル名	優先度	最小帯域幅	最大帯域幅
qp1	Low	0%	100%
qp2	Normal	0%	100%
qp3	Medium	0%	100%
qp4	High	0%	100%

デフォルトプロファイルのパラメータは、Ingress / Egress の両モードで変更できます。パラメータの変更方法については、8-3 ページの「QoS プロファイルの作成と設定」をご覧ください。

QoS プロファイルの作成と設定

Egress モードでは、カスタム QoS プロファイルを 28 個まで作成できます。QoS プロファイルを作成するには、次のコマンドを使います。

```
create qosprofile <qosname>
```

新規作成された QoS プロファイルには、次のデフォルト値が適用されます。

- **最小帯域幅** ー 0%
- **最大帯域幅** ー 100%
- **優先度** ー low

QoS パラメータの値を変更するには、次のコマンドを実行します。

```
config qosprofile <qosname> minbw <percent> maxbw <percent>
priority <level>
```

QoS プロファイルを削除するには、次のコマンドを実行します。

```
delete qosprofile <qosname>
```

QoS プロファイルを削除すると、そのプロファイルが割り当てられていたトラフィックグループにはデフォルトプロファイルの *qp1* が設定されます。

ブラックホール QoS プロファイル

QoS プロファイル *blackhole* は、特定のトラフィックを転送せずに破棄する特殊なプロファイルです。このプロファイルは、セキュリティ管理やパフォーマンス向上の目的で使用できます。ブラックホール QoS プロファイルは、ICMP トラフィックやルーティングプロトコルパケット（OSPF、RIP、DVMRP など）には適用されません。

QoS プロファイルとポートキューのマッピング

本製品は、ポートごとに 4 つの送信キュー（Q0 ～ Q3）を持っています。Ingress モードでは、デフォルト QoS プロファイルの *qp1* ～ *qp4* がそれぞれ 1 つずつキューにマッピングされます。これに対し、Egress モードでは、QoS プロファイルとキューの関係は、つねに最初のキューにマッピングされる *qp1* を除いて固定されていません。残りの 3 つのキューには、トラフィックグループへの適用順にプロファイルがマッピングされていきます。5 つ以上のプロファイルを使用する場合は、同じ優先度を持つプロファイル同士で 1 つのキューを共有することになります。

さきほども述べたとおり、通常はデフォルトの Ingress モードから Egress モードへの変更は必要ありません。

8.5 トラフィックグループ

QoS プロファイルを作成したら、それをトラフィックグループに割り当てて QoS ポリシーを実施します。トラフィックグループは共通の属性を持つトラフィックを分類したもので、大きく分けて次のような種類があります。

- TCP/IP アドレス（IP QoS）
- 宛先 MAC アドレス（MAC QoS）
- パケットプライオリティ（802.1p ビット、PACE ビット）
- 物理 / 論理構成（物理ポート、VLAN）

どのようなトラフィックグループが利用できるかは、選択した QoS モードによって決まります。パケットが複数のグループ基準に一致する場合は、既定の優先順位にしたがって QoS プロファイルが適用されます。デフォルトでは、すべてのトラフィックグループに QoS プロファイル *qp1* が割り当てられています。

表 8-2 に、Ingress / Egress の各モードで使用できるトラフィックグループと優先順位を示します。

表 8-2：QoS モードとトラフィックグループ

優先順位	QoS タイプ	Ingress モード	Egress モード
高	IP QoS	送信元 IP アドレス	送信元 IP アドレス
↑		送信元レイヤー 4 ポート	送信元レイヤー 4 ポート
		宛先レイヤー 4 ポート	宛先レイヤー 4 ポート
		宛先 IP アドレス	宛先 IP アドレス
	MAC QoS	パーマネントエントリ	パーマネントエントリ
		ダイナミックエントリ	ダイナミックエントリ
		ブラックホールエントリ	ブラックホールエントリ
		ブロードキャスト /unknown	ブロードキャスト /unknown
	パケットプライオリティ	802.1p プライオリティビット	なし
		PACE ビット	なし
↓	物理 / 論理構成	送信元ポート	なし
低		送信元 VLAN	送信元 VLAN

以下、各トラフィックグループの内容とプロファイルの割り当て方法について説明します。

IP QoS トラフィックグループ

IP QoS グループでは、特定 IP アドレス宛てのトラフィックを QoS の適用対象とします。さらに、オプションとしてレイヤー 4 の宛先ポート（TCP / UDP）、送信元 IP アドレス、レイヤー 4 の送信元ポートを指定することもできます。

IP QoS の設定コマンドには、短いフォーマットと長いフォーマットがあります。短いフォーマットでは、宛先 IP アドレスだけが指定できます。一方、長いフォーマットでは、レイヤー 4 ポートなどオプションの IP パラメータも指定できます。

短いフォーマットは次のとおりです。

```
config ipqos [add | delete] <dest_ipaddress> <mask> [qosprofile <qosname> |
blackhole]
```

長いフォーマットは次のとおりです。

```
config ipqos [add | delete] [tcp | udp | other | all]
<dest_ipaddress> <mask> {l4-dstport <tcp_udp_port>}
{<src_ipaddress> <mask>} {l4-srcport <tcp_udp_port>}
[qosprofile <qosname> | blackhole]
```

表 8-3 に、長いフォーマットのオプションを示します。

表 8-3：IP QoS コマンドのオプション

コマンドオプション	説明
[add | delete]	IP トラフィックに QoS プロファイルを割り当て、または削除します。
[tcp | udp | other | all]	レイヤー 4 のプロトコルを指定します。、 • tcp － TCP プロトコル • udp － UDP プロトコル • other － TCP/UDP 以外のプロトコル • all － すべてのプロトコル
<dest_ipaddress> <mask>	QoS プロファイルの適用対象となる IP トラフィックの宛先 IP アドレスを指定します。
{l4-dstport <tcp_udp_port>	QoS プロファイルの適用対象となる IP トラフィックのレイヤー 4 宛先ポート番号を指定します。上記オプションで tcp を指定した場合は TCP ポート番号を、udp を指定した場合は UDP ポート番号を指定します。省略時は、すべてのポート番号が対象となります。
{<src_ipaddress> <mask>}	QoS プロファイルの適用対象となる IP トラフィックの送信元 IP アドレスを指定します。
{l4-srcport <tcp_udp_port>}	QoS プロファイルの適用対象となる IP トラフィックのレイヤー 4 送信元ポート番号を指定します。上記オプションで tcp を指定した場合は TCP ポート番号を、udp を指定した場合は UDP ポート番号を指定します。
[qosprofile <qosname> | blackhole]	上記の各オプションで定義した IP トラフィックに割り当てる QoS プロファイル名を指定します。

`config ipqos` コマンドによる IP QoS 設定時には、次のルールが適用されます。

- 短いフォーマットでは、ユニキャスト IP アドレスのみ指定可能です。
- 宛先 IP アドレスに 0.0.0.0/0 を指定した場合はワイルドカード指定となり、すべての宛先が対象となります。
- サブネット内 QoS（ISQ）ディセーブル時に IP QoS の対象となるのは、ルーティングされたトラフィックのみです。スイッチングされただけのトラフィックは対象外です。
- IP QoS は、ICMP、RIP、OSPF、DVMRP などのトラフィックには適用されません。
- 送信元 IP アドレスに指定できるのは、32 ビットマスクのホストアドレスかワイルドカード（0.0.0.0/0）だけです。ただし、宛先 IP アドレスにマルチキャストアドレスを指定した場合だけは、送信元 IP アドレスの範囲指定が可能です。
- レイヤー 4 プロトコルに other を指定した場合は、レイヤー 4 送信元ポートの値（16 ビット）とレイヤー 4 宛先ポートの値（16 ビット）をつなげた 32 ビット値を、IP ヘッダ直後の 32 ビットと比較してフィルタリングを行います。

- IP QoS プロファイルが実際に適用されるのは、該当するステーションがIP フォワーディングデータベースに登録されたときです。そのため、QoS ポリシーをただちに有効にするには、`clear ipfdb all` コマンドを実行して、IP フォワーディングデータベースの内容をいったんフラッシュする必要があります。

IP QoS の優先順位

IP QoS グループには、他のすべてのトラフィックグループ（MAC QoS、パケットプライオリティ、物理 / 論理構成）に優先して QoS プロファイルが適用されます。IP QoS トラフィック同士での優先順位は次のようになります。

- 短いフォーマットと長いフォーマットでは、長いフォーマットが優先されます。
- 短いフォーマット同士では、ネットマスクが長いものほど優先されます。次に例を示します。

```
config ipqos add 10.1.2.3/32 qp4
config ipqos add 10.1.2.0/24 qp3
```

この例では、まず最初に 32 ビットマスクが指定されたホスト 10.1.2.3 宛てのトラフィックに *qp4* が割り当てられ、次にネットワーク 10.1.2.x 宛てのトラフィック（ただし、10.1.2.3 宛てを除く）に *qp3* が割り当てられます。

- 長いフォーマット同士では、どのオプションパラメータを指定したかによって優先順位が決まります。送信元 IP アドレスの指定があるものがもっとも優先され、次に送信元レイヤー4 ポート、宛先レイヤー 4 ポートの順になります。表 8-4 に、指定したパラメータと優先順位の関係を示します。

表 8-4：IP QoS の優先順位

優先順位	指定したパラメータ			コマンド例（`config ipqos add tcp 10.1.2.0/24` に続く指定）
	送信元 IP	送信元 L4	宛先 L4	
高	○	○	○	`l4-dstport 80 11.12.13.14/32 l4-srcport 80 qosprofile qp3`
	○	○		`11.12.13.14/32 l4-srcport 80 qosprofile qp3`
	○		○	`l4-srcport 80 11.12.13.14/32 qosprofile qp3`
	○			`11.12.13.14/32 qosprofile qp3`
		○	○	`l4-dstport 80 l4-srcport 80 qosprofile qp3`
		○		`l4-srcport 80 qosprofile qp3`
低			○	`l4-dstport 80 qosprofile qp3`

IP QoS の設定例

ネットワーク 10.1.2.x 宛てのすべてのトラフィックに QoS プロファイル *qp2* を割り当てるには、次のようにします。ここでは短いフォーマットを使っています。

```
config ipqos add 10.1.2.0/24 qosprofile qp2
```

前の例に送信元 IP アドレスの指定を追加して、ホスト 10.1.1.1 からネットワーク 10.1.2.x へのトラフィックに *qp2* を割り当てます。宛先 IP アドレス以外のパラメータを指定するには長いフォーマットを使います。

```
config ipqos add all 10.1.2.0/24 10.1.1.1/32 qosprofile qp2
```

ネットワーク 10.1.2.x 宛てのすべての TCP トラフィックに *qp3* を割り当てるには、次のようにします。

```
config ipqos add tcp 10.1.2.0/24 qosprofile qp3
```

ホスト10.1.1.1からネットワーク10.1.2.x宛てのすべてのUDPトラフィックに*qp3*を割り当てます。

```
config ipqos add udp 10.1.2.0/24 10.1.1.1/32 qosprofile qp3
```

128.30.1.1 ～ 128.30.1.63 を宛先とする HTTP トラフィック（TCP ポート番号 80）に QoS プロファイル *qp3* を割り当てるには、次のようにします。

```
config ipqos add tcp 128.30.1.0/26 l4-dstport 80 qp3
```

また、同じ宛先に対する Telnet 要求（TCP ポート番号 23）をブロックするには、次のように QoS プロファイル *blackhole* を使います。

```
config ipqos add tcp 128.30.1.0/26 l4-dstport 23 blackhole
```

サーバ 10.2.3.4 からマルチキャストグループ 227.x.x.x 宛ての UDP トラフィックをブロックするには次のようにします。

```
config ipqos add udp 227.0.0.0/8 10.2.3.4/32 blackhole
```

宛先 IP アドレスにマルチキャストアドレスを指定したときは、送信元 IP アドレスの範囲指定が可能です（宛先がユニキャストアドレスのときは、送信元にはホストアドレスかワイルドカードの 0.0.0.0 / 0 しか指定できません）。次の例では、ネットワーク 10.x.x.x からマルチキャストグループ 227.x.x.x への UDP トラフィックをすべてブロックします。

```
config ipqos add udp 227.0.0.0/8 10.2.3.4/8 blackhole
```

標準 IP マルチキャストアドレス 224.0.0.x（OSPF などで使用）に対する QoS 設定はできません。

IP QoS の設定確認

IP QoS の設定を確認するには、次のコマンドを使います。

```
show ipqos
```

サブネット内 QoS（ISQ）

IP QoS はルーティングされたトラフィックに対してのみ有効ですが、本製品の ISQ 機能をイネーブルにすると、同一サブネット（VLAN）内のスイッチドトラフィックに対しても QoS が有効になります。ISQ は VLAN ごとに設定します。その他の設定方法はディセーブル時と同じです。ISQ 使用時の注意点は次のとおりです。

- ISQ をイネーブルにしたときは、FDB のエージングタイムを ARP エントリのタイムアウトよりも長く設定する必要があります。ISQ をイネーブルにすると、FDB エージングタイムが自動的に 50 分（3000 秒）に設定されます。
- VLAN 内にスタティックな ARP テーブルを使用するクライアントがある場合、ISQ は使用できません。

FDB タイマーの設定を確認するには、次のコマンドを使います。

```
show fdb
```

エージングタイマー値は一番最後に表示されます。

MAC QoS トラフィックグループ

MAC QoS グループでは、特定 MAC アドレス宛てのトラフィックを QoS の対象とします。宛先 MAC アドレスに QoS プロファイルを割り当てるには、以下のコマンドを使用します。

```
create fdbentry <mac_address> vlan <name> [blackhole | ports [<portlist> |
all] | dynamic] qosprofile <qosname>
```

パーマネント FDB エントリ

パーマネント FDB エントリへの QoS プロファイル割り当ては、FDB エントリの作成時に行います。次に例を示します。

```
create fdbentry 00:11:22:33:44:55 vlan default ports 1 qosprofile qp2
```

ダイナミック FDB エントリ

MAC アドレス学習機能によって FDB に登録されるダイナミックエントリにも QoS プロファイルを割り当てられます。次に例を示します。

```
create fdbentry 11:22:33:44:55:66 vlan default dynamic qosprofile qp3
```

QoS プロファイルが実際に適用されるのは、指定した MAC アドレスが FDB に登録されたときです。すでに指定した MAC アドレスが FDB に登録されている場合は、いったん FDB をクリアして MAC アドレスが再登録されるようにします。FDB をクリアするには、次のコマンドを使います。

```
clear fdb
```

ブラックホール FDB エントリ

ブラックホールエントリに指定された MAC アドレスにはパケットが転送されません。

```
create fdbentry 22:33:44:55:66:77 vlan default blackhole
```

ブロードキャスト / 宛先不明パケット

MAC QoS を利用すれば、ブロードキャストおよび宛先不明（unknown）パケットの制御が可能です。ブロードキャストアドレス（ff:ff:ff:ff:ff:ff）に対して、任意の帯域幅と優先度を割り当てます。

```
create fdbentry ff:ff:ff:ff:ff:ff vlan default dynamic qosprofile qp3
```

IP マルチキャストトラフィックがブロードキャストされるのは、IGMP スヌーピングをディセーブルにしたときだけです。

MAC QoS の設定確認

MAC QoS の設定を確認するには、次のコマンドを使います。

- show fdb permanent
- show qosprofile {<qosname>}

パケットプライオリティグループ

パケット自身が持つプライオリティ情報に基づいたトラフィックグループです。Ingress モードでのみ使用可能です。

IEEE 802.1p

IEEE 802.1p 準拠のプライオリティビットを持つパケットには、802.1p ビットの値に応じて 4 つのデフォルト QoS プロファイルのうちのいずれかが割り当てられます。これは自動的に行われるため、ユーザが設定を行う必要はありません。表 8-5 に、802.1p ビットの値と QoS プロファイルの関係を示します。本グループは Ingress モードでのみ有効です。

表 8-5：802.1p ビットの値と QoS プロファイル

802.1p ビット値	QoS プロファイル
0	*qp1*
1	*qp1*
2	*qp2*
3	*qp2*
4	*qp3*

表 8-5：802.1p ビットの値と QoS プロファイル

802.1p ビット値	QoS プロファイル
5	*qp3*
6	*qp4*
7	*qp4*

PACE

3Com の PACE トラフィックには、デフォルトプロファイルの *qp3* が割り当てられます。PACE トラフィックに対する QoS プロファイルの自動割り当てを行うかどうかは、以下のコマンドで変更できます。デフォルトはディセーブルです。本グループはIngressモードでのみ使用可能です。

```
[enable | disable] pace
```

物理 / 論理構成グループ

ネットワークの物理 / 論理構成に基づくトラフィックグループです。

送信元ポート

特定のポートから送信されるトラフィックに QoS プロファイルを割り当てるには、以下のコマンドを使用します。

```
config ports [<portlist> | all] qosprofile [<qosname> | none]
```

ポート 7 から送出されるトラフィックに QoS プロファイル *qp3* を割り当てるには、次のようにします。本グループは Ingress モードでのみ使用可能です。

```
config ports 7 qosprofile qp3
```

VLAN

特定の VLAN で発生したトラフィックに QoS プロファイルを割り当てるには、次のコマンドを使います。

```
config vlan <name> qosprofile [<qosname> | none]
```

VLAN QoS はVLAN 内でスイッチングされるトラフィックとVLAN 外にルーティングされるトラフィックの両方に対して有効です。次の例では、VLAN *servnet* で発生したトラフィックに QoS プロファイル *qp4* を割り当てています。

```
config vlan servnet qosprofile qp4
```

物理 / 論理構成グループの確認

ポートおよび VLAN の QoS 設定を確認するには次のコマンドを使います。

- `show qosprofile {<qosname>}`（ポート / VLAN 共通）

- show ports info（ポート）
- show vlan（VLAN）

8.6 QoS 設定の確認

QoS 設定を確認するには、次のコマンドを使います。

```
show qosprofile {<qosname>}
```

表示される情報は以下のとおりです。

- QoS プロファイル名
- 最小帯域幅
- 最大帯域幅
- 優先度
- この QoS プロファイルが適用されているトラフィックグループの一覧

トラフィックグループを基準に QoS 設定を確認することもできます。以下のコマンドを実行してください。

- show fdb permanent

  宛先 MAC アドレスと QoS プロファイルの関係を表示します。

- show switch

  PACE トラフィックに対するQoSプロファイルの自動割り当て機能がオンになっているかどうかを知ることができます。

- show vlan

  各 VLAN に割り当てられている QoS プロファイルを確認できます。

- show ports info

  ポートに割り当てられた QoS プロファイルを確認できます。

- show ipqos

  IP QoS テーブルを表示します。

8.7 QoS モニタ

QoS モニタは、各ポートのハードウェアキューを監視するためのユーティリティです。各キューにおける送信フレーム数の合計と 1 秒間に送信されたフレーム数を監視できます。

QoS モニタには、リアルタイム表示モードとバックグラウンドのロギングモードがあります。

QoS モニタをリアルタイム表示モードで実行するには、次のコマンドを使います。

```
show ports {<portlist>} qosmonitor
```

監視したいポートを指定すると、各キューの QoS 統計がリアルタイムに表示されます。監視中のポートは、ポート番号の後に表示されるアスタリスク（*）によって示されます。

QoS モニタのサンプリング動作は次のとおりです。

- 1 ポート当たり 20 秒ずつサンプリングする。20 秒経過したら次のポートに移る。
- pps（パケット / 秒）の値は、5 秒間の平均値です。

QoS モニタをバックグラウンドモードで起動するには、次のコマンドを使います。

```
enable qosmonitor <portlist>
```

これにより送信カウンタとオーバーフロー情報がログに記録されるようになります。オーバーフローとは、トラフィックが QoS プロファイルの設定範囲から逸脱したことを示しています。キューオーバーフローのログを精査することにより、適切な QoS 設定を見つけることができます。表 8-6 に、QoS モニタコマンドの一覧を示します。

表 8-6：QoS モニタコマンド

コマンド名	機能
enable qosmonitor <portlist>	QoS モニタをバックグラウンドロギングモードで起動します。トラフィックが QoS プロファイルの設定パラメータから逸脱した場合は、ログにエラーメッセージが記録されます。デフォルトはディセーブルです。
disable qosmonitor <portlist>	QoS モニタによるロギングをディセーブルにします。
show ports {<portlist>} qosmonitor	指定したポートの QoS 統計をリアルタイムに表示します。

8.8 QoS ポリシーの変更

QoS プロファイルをトラフィックグループに適用した後に QoS プロファイルを変更した場合、変更が有効になるまでの時間はトラフィックグループによって異なります。QoS プロファイルの変更時には次のルールが適用されます。

- IP QoS ポリシーの作成時および変更時は、`clear ipfdb` コマンドを実行して IP フォワーディングデータベースをフラッシュする必要があります。IP QoS ポリシーは、IPFDB にエントリが登録された時点で有効になります。
- MAC QoS ポリシーの作成時および変更時は、`clear fdb` コマンドを実行して FDB をフラッシュする必要があります。MAC QoS ポリシーは、FDB に MAC アドレスが登録された時点で有効になります。ただし、パーマネントエントリの場合は、エントリに QoS プロファイルを再度割り当てることで変更が有効になります。また、設定保存後にスイッチを再起動しても変更を有効にできます。
- ポートおよび VLAN QoS の場合は、QoS プロファイルを再割り当てすることで変更が有効になります。また、設定保存後にスイッチを再起動しても変更を有効にできます。

8.9 QoS 設定コマンド

表 8-7 に QoS の設定に使うコマンドの一覧を示します。

表 8-7：QoS 設定コマンド

コマンド名	機能
enable pace	PACE トラフィックに対する QoS プロファイル *qp3* の自動割り当てをイネーブルにします。Ingress モードでのみ使用可能です。
enable isq {vlan <name>}	指定した VLAN でサブネット内 QoS（ISQ）機能を有効にします。FDB エージングタイムが 3000 秒以下に設定されている場合は、自動的に 3000 秒に変更されます。
create qosprofile <qosname>	QoS プロファイルを作成します。新規作成された QoS プロファイルには、以下のデフォルト値が適用されます。 • 最小帯域幅 ― 0% • 最大帯域幅 ― 100% • 優先度 ― low
config qosmode [ingress | egress]	QoS モード（Ingress/Egress）を変更します。
config qosprofile <qosname> minbw <percent> maxbw <percent> priority <level>	QoS プロファイルのパラメータを変更します。以下のオプションが指定できます。 • `minbw` ― 最低限確保すべき帯域を全帯域幅のパーセントで指定します。デフォルトは 0% です。 • `maxbw` ― トラフィックに割り当てる帯域の上限を全帯域幅のパーセントで指定します。デフォルトは 100% です。 • `priority` ― 最小帯域の確保後に余った帯域を配分する際の優先度を指定します。優先度は、low、normal、medium、high のいずれかです。デフォルトは low です。
config ports [<portlist> | all] qosprofile [<qosname> | none]	指定したポートに QoS プロファイルを割り当てます。Ingress モードでのみ有効です。

表 8-7：QoS 設定コマンド

コマンド名	機能
config vlan <name> qosprofile [<qosname> | none]	VLAN に QoS プロファイルを割り当てます。none はデフォルト QoS プロファイル *qp1* を表します。
config ipqos [add | delete] <dest_ipaddress> <mask> [qosprofile <qosname> | blackhole]	指定した IP アドレス宛てのトラフィックに QoS プロファイルを割り当てます（IP QoS。短いフォーマット）。
config ipqos [add | delete] [tcp | udp | other | all] <dest_ipaddress> <mask> {l4-dstport <tcp_udp_port>} {<src_ipaddress> <mask>} {l4-srcport <tcp_udp_port>} [qosprofile <qosname> | blackhole]	指定した IP アドレス宛てのトラフィックに QoS プロファイルを割り当てます（IP QOS。長いフォーマット）。長いフォーマットでは、レイヤー 4 ポートなどのオプションパラメータも指定できます。
delete qosprofile <qosname>	QoS プロファイルを削除します。
disable isq {vlan <name>}	指定した VLAN で ISQ をディセーブルにします。
disable pace	PACE トラフィックに対する QoS プロファイルの自動割り当てをディセーブルにします。Ingress モードでのみ使用可能です。

9 IP ユニキャストルーティング

この章では、基本的な IP ルーティングの設定方法について説明します。ルーティングプロトコルの詳細については第 10 章「ルーティングプロトコル」を、IP マルチキャストルーティングについては第 11 章「IP マルチキャストルーティング」をご覧ください。

9.1 概要

本製品は、完全なレイヤー 3・IP ユニキャストルーティング機能を備えています。本製品は、RIP（Routing Information Protocol）や OSPF（Open Shortest Path First）を使って、ネットワーク上の他のルータと経路情報を交換します。ダイナミックルーティングでは、ルーティングテーブルが動的に作成・維持され、送信先ごとに最適な経路が選択されます。

IP ユニキャストルーティング機能を利用するには、各ホストに IP アドレスを重複しないよう割り当てておく必要があります。また、各ホストには、本製品のルータインタフェース（VLAN）の IP アドレスをデフォルトルートとして設定する必要があります。

RIP と OSPF の詳細については、第 10 章「ルーティングプロトコル」をご覧ください。

ルータインタフェース

本製品では、ルータインタフェース間の IP トラフィックを、ソフトウェアとハードウェアでルーティング処理します。ここで言うルータインタフェースとは、IP アドレスを割り当てられた VLAN のことを表します。

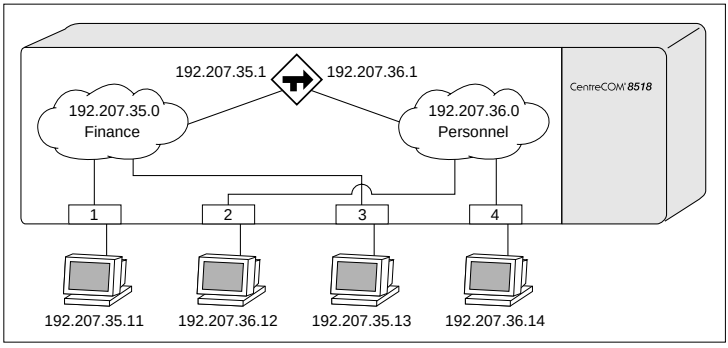
複数の VLAN を作成した場合は、VLAN 間でルーティングを行うかどうかを選択できます。VLAN 内でのスイッチングと VLAN 間の IP ルーティングは、いずれも本製品の内部で実現されます。

VLAN に IP アドレスを割り当てるときは、IP アドレスとネットマスクによって表されるサブネットアドレスが他と重複しないようにしてください。同じサブネットアドレスを複数の VLAN に割り当てることはできません。

図 9-1 は、2 つの VLAN、*Finance* と *Personnel* を示しています。ポート 1 とポート 3 が VLAN *Finance* に、ポート 2 とポート 4 が VLAN *Personnel* に所属しています。VLAN *Finance* の IP アドレス（すなわちルータインタフェースのアドレス）は 192.207.35.1、VLAN *Personnel* のルータインタフェースは 192.207.36.1 に設定されています。両 VLAN のネットワークアドレスは、それぞ

れ 192.207.35.0 と 192.207.36.0 です。同一 VLAN 内のトラフィックは MAC アドレスに基づいてスイッチングされ、VLAN 間のトラフィックは IP アドレスに基づいてルーティングされます。

図 9-1：VLAN 間ルーティング



ルーティングテーブルの構築

IP ルーティングテーブルには、ネットワークとホストへの経路が登録されます。経路情報は、取得方法によって次のように分類できます。

- **ダイナミックルート** ― 他のルータと交換したルーティングプロトコルパケット、あるいは ICMP リダイレクトメッセージを通じて取得された経路情報
- **スタティックルート** ― 管理者によって登録された経路情報
  - **デフォルトルート**
  - **インタフェースアドレス**
  - **その他のスタティックルート**

VLAN を削除した場合、その VLAN（の先）に設定されたデフォルトルートは無効になりますが、デフォルトルートのエントリ自体は残ります。デフォルトルートの削除は手動で行う必要があります。

ダイナミックルート

ダイナミックルートは、RIP や OSPF を通じて学習されたルートです。RIP や OSPF を使用するルータは、ルーティングテーブルの情報を互いに交換しあいます。ダイナミックルーティングを使用する場合、ルーティングテーブルには到達可能な経路だけが保持されます。

ルーティングプロトコルによって定められた一定の時間内に新しい情報が送られてこない場合、その経路情報はルーティングテーブルから削除（エージアウト）されます。

スタティックルート

スタティックルートは、管理者が手動でルーティングテーブルに登録したルートです。スタティックルートは、ルータが広告しないネットワークへの経路を示すために使用されます。スタティックルートは 64 個まで設定できます。

スタティックルートを広告するかどうかは、次のコマンドによって設定可能です。

```
[enable | disable] rip export static
[enable | disable] ospf export static
```

出荷時の設定はイネーブルです。スタティックルートはルーティングテーブルからエージアウトされません。

スタティックルートには有効な IP アドレスを設定しなくてはなりません。VLAN と IP セグメントは 1 対 1 に対応している必要があります。複数の VLAN が同じ IP セグメントに所属するような設定はできませんのでご注意ください。VLAN（IP セグメント）を削除しても、関連するスタティックルートは削除されません。スタティックルートは手動で削除する必要があります。

ブラックホールルート

特定の IP アドレス宛てトラフィックを転送せずに破棄したい場合は、ブラックホールルートを登録します。

```
config iproute [add | delete] blackhole <ipaddress> <mask>
```

複数の経路が存在する場合

目的地への経路が複数存在する場合は、ネットマスクが最も長いエントリが選択されます。ネットマスクが等しい場合は、次の優先順位に基づいて経路が選択されます。

1. ダイレクトルート
2. ICMP リダイレクト（表 9-5 を参照）
3. スタティックルート
4. アクティブでないダイレクトルート

デフォルトルートを複数設定した場合は、メトリックが最小の経路が選択されます。メトリックが等しい場合は、いずれかの経路が選択されます。

IP ルートシェアリング

IP ルートシェアリングは、同一メトリックのルートが複数存在する場合に、トラフィックをこれら複数の経路に分散して送信する機能です。OSPF では、イコールコストマルチパス（ECMP）ルーティングと呼びます。本機能は、スタティックルートと OSPF ルートに対して使用できます。

IP ルートシェアリングの設定方法は、次のとおりです。

1 IP ルートシェアリングをイネーブルにします。

```
enable iproute sharing
```

2 スタティックルート、または OSPF の設定を行います。

IP ルートシェアリングでは、最大 5 つの経路を使用してトラフィックを送信します。

ルートシェアリングは限られた帯域を有効利用するための機能ですが、トラブル発生時のトラフィック監視作業が困難になるため、その点を考慮した上でご使用ください。

Proxy ARP

Proxy ARP（代理 ARP）とは本来、ARP 非対応機器への ARP 要求に対し、ARP 対応機器が代理応答するためのプロトコルでしたが、現在では用法と使用範囲が拡大され、ルータの二重化と IP クライアントの設定を簡素化する目的でも使われています。

Proxy ARP エントリを作成するには、次のコマンドを使います。エントリは 64 個まで作成できます。

```
config iparp add proxy <ipaddress> {<mask>} {<mac_address>} {always}
```

<ipaddress> <mask> には、Proxy ARP の対象となる IP アドレスを指定します。<mask> を省略した場合、指定した IP アドレスはホストアドレスと見なされます。

<mac_address> には、代理応答時に返す MAC アドレスを指定します。省略した場合は、本製品の MAC アドレスが返されます。

always パラメータを指定すると、ARP 要求を出した機器と ARP の対象機器が同じ IP セグメントに属している場合でも本製品が代理応答します。このオプションは、ARP に返答できない機器がある場合にのみ使用します。always パラメータを省略した場合は、要求元と要求先が別の IP セグメントに属している場合にのみ本製品が代理応答し、要求元と要求先が同じ IP セグメントに属している場合は（通常どおり）受信した ARP 要求パケットを IP セグメント内にブロードキャストします。

次に Proxy ARP の使用例を示します。

ARP 非対応機器の代理応答

ネットワーク上に ARP 要求パケットに返答できない機器がある場合は、前述のコマンドを用いて、Proxy ARP テーブルに非対応機器の IP アドレスを登録します。この場合、always パラメータを忘れずに指定してください。

登録後、本製品は以下の条件が満たされた場合に代理応答を行います。

- ルータインタフェース上で有効な ARP 要求を受け取った。
- Proxy ARP テーブル内に ARP 要求対象の IP アドレスがエントリされている。

- **同エントリに** always **パラメータが指定されている（これは、**ARP **の要求元と要求先が同じ** IP **セグメントに属している場合でも本製品が代理応答することを示します）。**

これらの条件が満たされた場合、本製品は Proxy ARP **テーブル内の** MAC **アドレスを要求元のホストに返送します。エントリ作成時に** MAC **アドレスを指定しなかった場合は、本製品の** MAC **アドレスが返されます。**

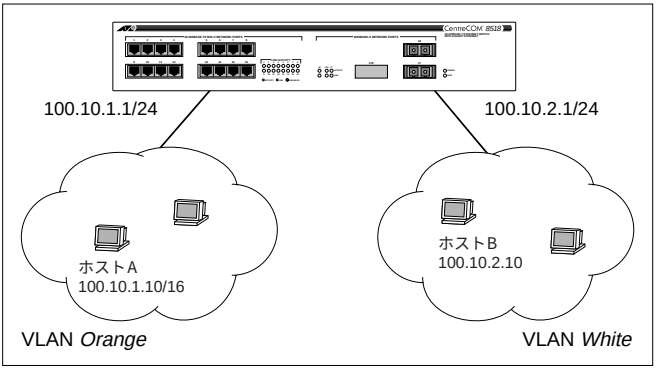
Proxy ARP による間接ルーティング

ネットワーク環境によっては、所属する IP **セグメントのネットマスクとは長さの異なるマスクをホストに設定することがあります。**Proxy ARP **を利用すれば、こうしたホストから別の** IP **セグメントにある機器への** ARP **要求が発生した場合に、本製品に代理応答をさせて間接的なルーティングを行うことができます。**

図 9-2 **の例では、ホスト** A **に** IP **アドレス** 100.10.1.10 **とクラス** B **標準のネットマスク** 255.255.0.0 **が設定されているとします。本製品には** 2 **つの** IP **セグメント（**VLAN *Orange* **と** *White*）**が定義され、ルータインタフェースにはそれぞれ** IP **アドレス** 100.10.1.1/24 **と** 100.10.2.1/24 **が設定されて** VLAN **間ルーティングが有効になっているとします。また、**Proxy ARP **テーブルに、**IP **アドレス** 100.101.0.0**、ネットマスク** 255.255.0.0**、**always **パラメータなしのエントリが登録されています。**

ホスト A **が** VLAN *White* **上のホスト** B**（**100.10.2.10**）と通信する場合、ホスト** A **はホスト** B **が同一** IP **セグメント（**100.10.0.0/16**）上にあるものと認識して、**ARP **要求パケットを送信します。ホスト** B **は別の** VLAN **にあるため、この** ARP **に応答することはできませんが、この例では** Proxy ARP **が設定されているため、本製品がホスト** B **の代理としてこの要求に応答します。このとき本製品は自らの** MAC **アドレスをホスト** A **に返します。これ以降、ホスト** A **からのパケットはすべて、本製品経由で別の** IP **セグメントにあるホスト** B **に転送されます。**

図 9-2：Proxy ARP による間接ルーティング



ルートプライオリティ

本製品のように複数のルーティングプロトコルを使用している環境では、各プロトコルのルーティングテーブルを何らかの方法で融合しなくてはなりません。本製品は、ルート情報のソース（ルーティングプロトコル）ごとに相対的なプライオリティを設定することで、この問題に対処しています。

デフォルトのルートプライオリティは表 9-1 のとおりです。プライオリティの値が小さいほど優先順位が高くなります。

表 9-1：ルートプライオリティ

ルート情報のソース	プライオリティ
ダイレクトルート	10
ブラックホールルート	50
スタティックルート	1100
ICMP	1200
OSPF エリア内ルート	2200
OSPF エリア間ルート	2300
RIP	2400
OSPF 外部ルート 1	3200
OSPF 外部ルート 2	3300
BOOTP	5000

ルートプライオリティを変更するには、次のコマンドを使います。

```
config iproute priority [rip | bootp | icmp | static | ospf-intra | ospf-
inter | ospf-as-external | ospf-extern1 | ospf-extern2] <priority>
```

ルートプライオリティの変更は、ネットワークの構成やルーティングプロトコルの動作などについて充分な理解がある場合を除いて行わないでください。通常、プライオリティを変更する必要はありません。

IP マルチネット

IP マルチネットは、同一物理セグメント上に複数の論理サブネットを作成する機能です。本製品では、ルータインタフェース（VLAN）当たり 1 つしか IP アドレスを設定できません。IP マルチネットを実現するには、同一物理ポートに複数の VLAN を割り当てる必要があります。これにより、同じ物理ポート上に作成された複数のサブネット間で IP ルーティングが可能になります。

IP マルチネットの設定時には、以下のルールが適用されます。

- 各ルータインタフェース（VLAN）には 1 つしか IP アドレスを割り当てられない。

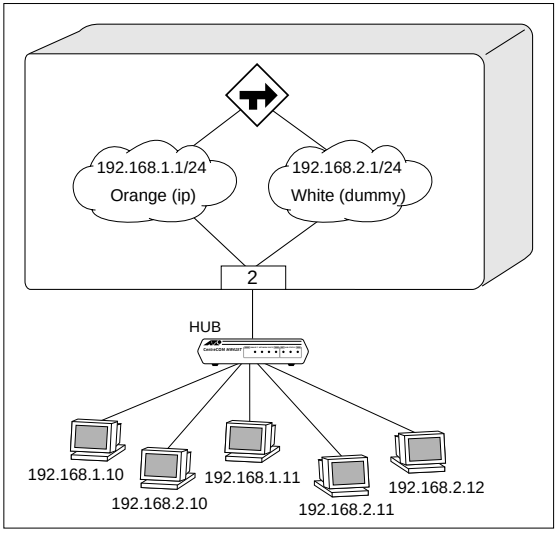
- IP マルチネットを実現するには、複数の VLAN が必要。
- 1 つのポートに設定できる論理サブネットは 4 つまで。
- 複数のポートにまたがる論理サブネットを作成するには、マルチネットを構成する VLAN のポート構成をすべて同じにする必要がある。
- IP マルチネットをイネーブルにすると、FDB のエージングタイムが自動的に 3000 秒（50 分）に変更される。
- DHCP/BOOTP リレー機能は、IP プロトコルを割り当てた VLAN でしか使用できない。

BOOTP は、IP プロトコルを割り当てられた VLAN でしか機能しません。

IP マルチネットの設定

IP マルチネットを使用するには、以下の手順にしたがいます。ここでは、図 9-3 を例に解説します。

図 9-3：IP マルチネットの設定例



1 IP マルチネット機能を使用するポートを選択します。

ここでは、例としてポート 2 を使います。

2 選択したポートを VLAN *default* から削除します。

```
config vlan default delete ports 2
```

3 ダミープロトコルを作成します。

```
create protocol dummy
```

4 マルチネットを構成するサブネット（VLAN）を作成します。

```
create vlan orange
create vlan white
```

5 各 VLAN に IP アドレスを割り当てます。

```
config vlan orange ipaddress 192.168.1.1 255.255.255.0
config vlan white ipaddress 192.168.2.1 255.255.255.0
```

6 いずれかひとつのサブネットに IP プロトコルを割り当てます。

```
config vlan orange protocol ip
```

7 それ以外のサブネットにはダミープロトコルを割り当てます。

```
config vlan white protocol dummy
```

8 サブネットを物理ポート 2 に割り当てます。

```
config vlan orange add ports 2
config vlan white add ports 2
```

9 サブネット間の IP ルーティングをイネーブルにします。

```
enable ipforwarding
```

10 IP マルチネット機能をイネーブルにします。

```
enable multinetting
```

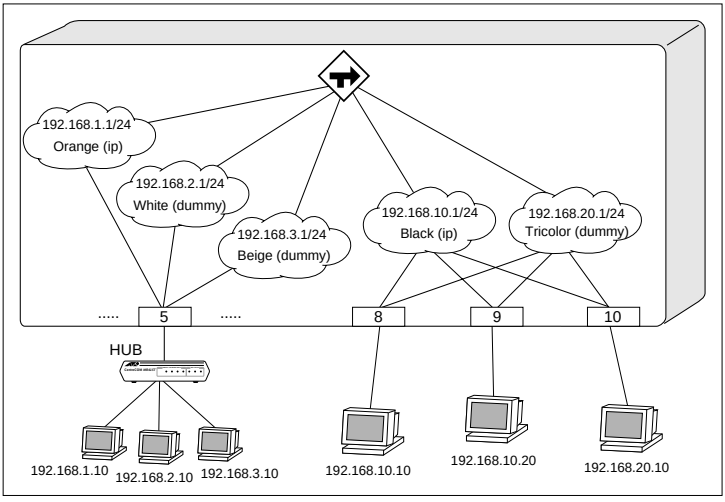
11 ダイナミックルーティングを使用する場合は、RIP や OSPF をイネーブルにします。

```
config rip add vlan all
enable rip
```

IP マルチネットの作成例

図 9-4 **の例では、ポート** 5 **に** 3 **つのサブネット（**192.168.1.0、192.168.2.0、192.168.3.0**）を作成し、さらに、ポート** 8 **〜** 10 **にまたがる論理サブネットを** 2 **つ（**192.168.10.0 **と** 192.168.20.0**）作成します。また、どちらのマルチネットセグメントでも** RIP **を使用しています。**

図 9-4：複数のポートにまたがる IP マルチネットの設定例




```
create protocol dummy
create vlan orange
create vlan white
create vlan beige
config vlan orange ipaddress 192.168.1.1
config vlan white ipaddress 192.168.2.1
config vlan beige ipaddress 192.168.3.1
config vlan orange protocol ip
config vlan white protocol dummy
config vlan beige protocol dummy
config vlan orange add ports 5
config vlan white add ports 5
config vlan beige add ports 5
create vlan black
create vlan tricolor
config vlan black ipaddress 192.168.10.1
config vlan tricolor ipaddress 192.168.20.1
config vlan black protocol ip
config vlan tricolor protocol dummy
config vlan black add ports 8-10
config vlan tricolor add ports 8-10
config rip add vlan all
enable rip
enable ipforwarding
enable multinetting
```

9.2 IP ユニキャストルーティングの設定

ここでは、IP ユニキャストルーティングの設定に使用するコマンドについて解説します。IP ルーティングの設定は、以下の手順で行います。

1 VLAN を複数作成し、各々設定を行います。

VLAN が 1 つしか定義されていなくても、IP ルーティング機能をイネーブルにしたり、ルーティングプロトコル（RIP など）をイネーブルにしたりすることはできますが、ICMP メッセージの作成や応答を適切に行うには、少なくとも 2 つの VLAN を設定しておく必要があります。

VLAN の作成と設定の詳細については、第 5 章「バーチャル LAN（VLAN）」をご覧ください。

2 ルーティング機能を使用する VLAN に IP アドレスを割り当てます。

```
config vlan <name> ipaddress <ipaddress> {<mask>}
```

VLAN には、IP アドレスを他と重複しないように割り当ててください。

3 デフォルトルートを設定します。

```
config iproute add default <gateway> {<metric>}
```

デフォルトルートは、ルーティングテーブル内に目的地への経路が（ダイナミックルート、スタティックルートとも）登録されていなかった場合に使用されるデフォルトの経路です。

4 VLAN の IP ルーティング機能をイネーブルにします。

```
enable ipforwarding {vlan <name>}
```

5 RIP または OSPF を使用するには、次のコマンドを使います。

```
enable rip
enable ospf
```

IP ユニキャストルーティングの設定確認

IP ユニキャストルーティングの設定を確認するには、`show iproute` コマンドを実行します。このコマンドは、ルーティングテーブルに登録されている経路と、各経路がどのようにして取得されたかを表示します。

IP ルーティング設定の確認には、以下のコマンドも使用できます。

- `show iparp`

  ARP テーブルを表示します。

- `show ipfdb`

IP フォワーディングデータベース（IP FDB）を表示します。IP FDB には、パケットの送受信を行ったホストとポート、VLAN の関係が記録されています。

- `show ipconfig`

  指定した VLAN の設定情報を表示します。

9.3 DHCP/BOOTP リレーの設定

本製品は、DHCP（Dynamic Host Configuration Protocol）あるいは BOOTP（Bootstrap Protocol）要求パケットを、別の IP セグメントに転送することができます。DHCP/BOOTP リレー機能の設定は、IP ユニキャストルーティングの設定完了後に行います。この機能は、Windows NT サーバと Windows 95 クライアントの間で DHCP サービスを実行する場合など、さまざまな環境で使用できます。DHCP/BOOTP リレー機能の設定は、以下の手順で行います。

1. VLAN と IP ユニキャストルーティングの設定を行います。
2. 次のコマンドを使って、DHCP/BOOTP リレー機能をイネーブルにします。

   ```
   enable bootprelay
   ```

3. 次のコマンドを使って、DHCP/BOOTP 要求パケットの転送先 IP アドレスを設定します。

   ```
   config bootprelay add <ipaddress>
   ```

BOOTP リレーエントリを削除するには、次のコマンドを実行します。

```
config bootprelay delete [<ipaddress> | all]
```

DHCP/BOOTP リレー機能の設定確認

DHCP/BOOTP リレー機能の設定を確認するには、次のコマンドを使います。

```
show ipconfig
```

このコマンドを実行すると、BOOTP リレー機能の設定状況と登録されている BOOTP リレー先アドレスが表示されます。

9.4 UDP フォワーディング

UDP フォワーディングは、特定 UDP ポート宛てのブロードキャストパケットをあらかじめ指定した IP アドレスまたは VLAN に転送する機能です。DHCP/BOOTP パケットについては、RFC1542 で規定されている BOOTP エージェントとして働き、その他の UDP パケットに対しては、宛先 IP アドレスの書き換え、IP パケットと UDP パケットのチェックサム再計算、TTL 減算を行った上で転送します。

UDP フォワーディングを DHCP/BOOTP パケットの転送に使うときは、前述の DHCP/BOOTP リレー機能をディセーブルに設定してください。また、DHCP サーバの使い分けなどをしない場合は DHCP/BOOTP リレー機能で充分ですので、そちらを使用することをおすすめします。

UDP フォワーディングの設定

UDP **フォワーディングの設定は次の手順で行います。**

1 UDP **フォワーディングプロファイルを作成します。プロファイルは** 10 **個まで作成できます。** VLAN **名などと同様、プロファイル名は他と重複しないようにしてください。**

```
create udp-profile <profile_name>
```

2 UDP **フォワーディングプロファイルに** UDP **パケットタイプ（**UDP **ポート番号）と転送先の** IP **アドレスまたは** VLAN **を設定します。**1 **つのプロファイルには、パケットタイプと転送先を** 8 **組まで設定できます。**

```
config udp-profile <profile_name> [add | delete] <udp_port> [vlan <name>
| ipaddress <dest_ipaddress>]
```

3 VLAN **に**UDP **フォワーディングプロファイルを割り当てます。各**VLAN **にはプロファイルを** 1 **つだけ割り当てることができます。**

```
config vlan <name> udp-profile <profile_name>
```

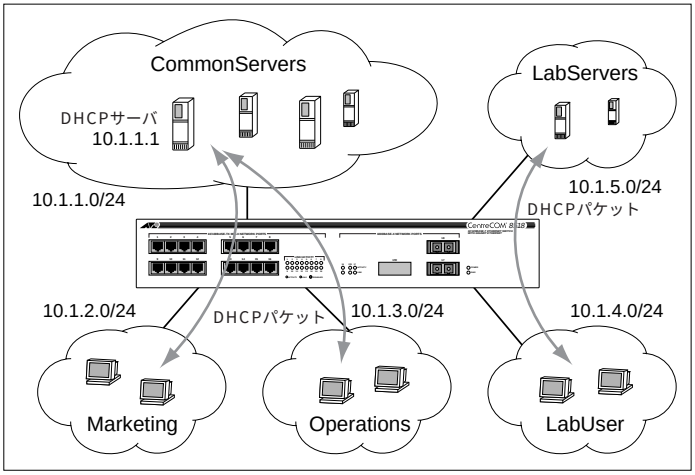
これにより、指定した VLAN **内で発生した** UDP **ブロードキャストパケットのうち、パケットタイプがプロファイルに一致するものが指定した転送先に送られます。転送先が** VLAN **の場合は、転送先** VLAN **のオール** 1 **ブロードキャストアドレスに送信されます。**

設定例

図 9-5 **の例では、次のような設定を行っています。**

- VLAN *Marketing* **と** VLAN *Operations* **の** DHCP **クライアントは、**VLAN *CommonServers* **の** DHCP **サーバ（**10.1.1.1**）を使用**
- VLAN *LabUser* **の** DHCP **クライアントは、**VLAN *LabServers* **上の任意の** DHCP **サーバを使用。**

図 9-5：UDP フォワーディングの設定例



設定コマンド例は次のとおりです。

```
create udp-profile commondhcp
create udp-profile labdhcp
config udp-profile commondhcp add 67 ipaddress 10.1.1.1
config udp-profile labdhcp add 67 vlan labservers
config vlan marketing udp-profile commondhcp
config vlan operations udp-profile commondhcp
config vlan labuser udp-profile labdhcp
```

VLAN *Marketing* と VLAN *Operations* 上のホストが送信した DHCP パケットは、VLAN *Common-Servers* 上の DHCP サーバ（10.1.1.1）に転送されます。また、VLAN *LabUser* 上のホストが送信した DHCP パケットは、VLAN *LabServers* にブロードキャストで転送されます。

表 9-2 に UDP フォワーディングの設定コマンド一覧を示します。

表 9-2：UDP フォワーディング設定コマンド

コマンド名	機能
create udp-profile <profile_name>	UDP フォワーディングプロファイルを作成します。
config udp-profile <profile_name> add <udp_port> [vlan <name> | ipaddress <dest_ipaddress>]	UDP フォワーディングプロファイルに、転送する UDP パケットのタイプ（UDP ポート番号）と、転送先の IP アドレスまたは VLAN を設定します。転送ルールは、8 個まで指定できます。

表 9-2：UDP フォワーディング設定コマンド

コマンド名	機能
config udp-profile <profile_name> delete <udp_port> [vlan <name> | ipaddress <dest_ipaddress>]	UDP フォワーディングプロファイルから、転送対象 UDP パケットタイプ（UDP ポート番号）と転送先を削除します。
config vlan <name> udp-profile <profile_name>	VLAN に UDP フォワーディングプロファイルを割り当てます。これにより、VLAN 内で発生した UDP ブロードキャストパケットのうち、パケットタイプがプロファイルと一致するものが、指定した転送先にフォワードされるようになります。指定した UDP ポートが DHCP/BOOTP ポートの場合は、DHCP/BOOTP リレーエージェントとして機能します。
show udp-profile {<profile_name>}	UDP フォワーディングプロファイルに関する情報（プロファイル名、対象 UDP ポート、転送先、プロファイルの割当先 VLAN）を表示します。
unconfig udp-profile vlan [<name> | all]	指定した VLAN から UDP フォワーディングプロファイルの割り当てを解除します。
delete udp-profile <profile_name>	UDP フォワーディングプロファイルを削除します。

9.5 IP 設定コマンド

表 9-3 に IP 関連の基本的な設定コマンドの一覧を示します。

表 9-3：基本的な IP 設定コマンド

コマンド名	機能
enable bootp vlan [<name> | all]	指定した VLAN の IP アドレスを BOOTP サーバから取得するよう設定します。デフォルトはイネーブルです。
enable bootprelay	DHCP/BOOTP リレー機能をイネーブルにします。
enable ipforwarding {vlan <name>}	指定した VLAN の IP ルーティング機能をイネーブルにします。VLAN 名を指定しなかった場合は、IP アドレスを割り当てられたすべての VLAN 間でルーティングが有効になります。デフォルトはディセーブルです。
enable ipforwarding broadcast {vlan <name>}	指定した VLAN で IP ブロードキャストパケットの転送をイネーブルにします。VLAN 名を指定しなかった場合は、すべての VLAN で IP ブロードキャストの転送が有効になります。この機能を有効にするには、VLAN の IP ルーティング機能をイネーブルにしておく必要があります。デフォルトはイネーブルです。
enable multinetting	IP マルチネット機能をイネーブルにします。
config bootprelay add <ipaddress>	BOOTP パケットのリレー先 IP アドレスを追加します。

表 9-3：基本的な IP 設定コマンド

コマンド名	機能
config bootprelay delete [<ipaddress> | all]	BOOTP パケットのリレー先 IP アドレスエントリを削除します。
config iparp add <ipaddress> <mac_address>	ARP テーブルにパーマネントエントリを追加します。IP アドレスと MAC アドレスをペアで指定してください。
config iparp delete <ipaddress>	ARP テーブルから、指定した IP アドレスを持つエントリを削除します。
disable bootp vlan [<name> | all]	指定した VLAN の IP アドレス設定に BOOTP を使わないよう設定します。
config iparp add proxy <ipaddress> {<mask>} {<mac_address>} {always}	Proxy ARP エントリを作成します。64 個まで作成可能です。<mask>を省略した場合は255.255.255.255を指定したものとみなされます。<mac_address> を省略した場合は、ARP 応答でスイッチの MAC アドレスが返されます。always オプションを指定した場合は、ARP 要求元と ARP 要求先が同じ IP セグメントにある場合でも、本製品が代理応答します。always オプションを指定しなかった場合は、要求元と要求先が異なる IP セグメントにある場合にのみ代理応答し、それ以外の場合は受信した ARP 要求パケットをセグメント内にブロードキャストします。
config iparp delete proxy [<ipaddress> {<mask>} | all]	Proxy ARP エントリを削除します。
config iparp timeout <minutes>	IP ARP エントリのタイムアウトを設定します。デフォルトは 20 分です。0 に設定すると、ARP エントリはエージアウトされなくなります。
disable bootprelay	DHCP/BOOTP リレー機能をディセーブルにします。
disable ipforwarding {vlan <name>}	指定した VLAN の IP ルーティング機能をディセーブルにします。
disable ipforwarding broadcast {vlan <name>}	指定した VLAN で IP ブロードキャストパケットの転送をディセーブルにします。
disable multinetting	IP マルチネット機能をディセーブルにします。
clear iparp {<ipaddress> | vlan <name>}	ARP テーブルから、ダイナミックエントリを削除します。パーマネントエントリは削除されません。
clear ipfdb {<ipaddress> | vlan <name>}	IP フォワーディングデータベースから、ダイナミックエントリを削除します。

表 9-4 に IP ルーティングテーブルの設定に使うコマンドの一覧を示します。

表 9-4：ルーティングテーブル設定用コマンド

コマンド名	機能
enable iproute sharing	宛先への経路が複数存在する場合にトラフィックの分散を行うようにします。負荷分散が行われるのは、最小コストの経路が複数存在するときだけです。デフォルトはディセーブルです。

表 9-4：ルーティングテーブル設定用コマンド

コマンド名	機能
config ipqos [add | delete] <dest_ipaddress> <mask> qosprofile <qosname>	指定した IP アドレス宛てのトラフィックに QoS プロファイルを割り当てます（IP QOS。短いフォーマット）。
config ipqos [add | delete] [tcp | udp | other | all] <dest_ipaddress> <mask> {l4-dstport <tcp_udp_port>} {<src_ipaddress> <mask>} {l4-srcport <tcp_udp_port>} [qosprofile <qosname> | blackhole]	指定した IP アドレス宛てのトラフィックに QoS プロファイルを割り当てます（IP QOS。長いフォーマット）。長いフォーマットでは、レイヤー 4 ポートなどのオプションパラメータも指定できます。
config iproute add <ipaddress> <mask> <gateway> {<metric>}	ルーティングテーブルにスタティックルートを追加します。ホストエントリの場合は、<mask> に 255.255.255.255（32 ビットマスク）を指定します。
config iproute delete <ipaddress> <mask> <gateway>	ルーティングテーブルからスタティックルートを削除します。
config iproute add blackhole <ipaddress> <mask>	ルーティングテーブルに「ブラックホール」ルートを追加します。ブラックホールルートとして設定された IP アドレス宛てのトラフィックはすべて破棄されます。また、このとき ICMP（Internet Control Message Protocol）メッセージは送信されません。
config iproute delete blackhole <ipaddress> <mask>	ルーティングテーブルから「ブラックホール」エントリを削除します。
config iproute add default <gateway> {<metric>}	デフォルトルートを設定します。デフォルトルートは、設定済みの IP インタフェース上になくてはなりません。<metric> が指定されていない場合は、デフォルトとして 1 が使用されます。
config iproute delete default <gateway>	ルーティングテーブルからデフォルトルートを削除します。
config iproute priority [rip | bootp | icmp | static | ospf-intra | ospf-inter | ospf-as-external | ospf-extern-1 | ospf-extern2] <priority>	ルーティングプロトコル間の優先順位を設定します。数が小さいほど優先順位が高くなります。
disable iproute sharing	複数経路を利用したトラフィック分散をディセーブルにします。

表 9-5 に ICMP 設定コマンドの一覧を示します。

表 9-5：ICMP 設定コマンド

コマンド名	機能
enable icmp redirects {vlan <name>}	指定した VLAN で ICMP リダイレクトメッセージの生成をイネーブルにします。デフォルトはイネーブルです。
enable icmp unreachables {vlan <name>}	指定した VLAN で ICMP 宛先到達不能メッセージの生成をイネーブルにします。デフォルトはイネーブルです。

表 9-5：ICMP 設定コマンド

コマンド名	機能
enable icmp useredirects	ICMP リダイレクトメッセージの受信時に、ルーティングテーブルの更新を行うようにします。デフォルトはディセーブルです。
enable irdp {vlan <name>}	指定した VLAN で ICMP ルータ広告メッセージの生成をイネーブルにします。デフォルトはイネーブルです。
config irdp [multicast | broadcast]	ルータ広告メッセージの送信方法を指定します。デフォルトは `multicast` です。
config irdp <mininterval> <maxinterval> <lifetime> <preference>	ICMP ルータ広告メッセージのパラメータを設定します。 • `mininterval` − ルータ広告の最小送信間隔を指定します。デフォルトは 450 秒です。 • `maxinterval` − ルータ広告の最大送信間隔を指定します。デフォルトは 600 秒です。 • `lifetime` − ルータ広告の有効時間を設定します。デフォルトは 1800 秒です。 • `preference` − ルータの優先度を設定します。IRDP クライアントは、優先度がもっとも高いルータをデフォルトルータとして使用します。このルータの使用を奨励したいときは、この値を大きくします。デフォルト値は 0 です。
unconfig icmp	ICMP 関連の設定をデフォルト値に戻します。
unconfig irdp	ICMP ルータ広告メッセージのパラメータをデフォルト値に戻します。
disable icmp redirects {vlan <name>}	指定した VLAN で ICMP リダイレクトメッセージの生成をディセーブルにします。
disable icmp unreachables {vlan <name>}	指定した VLAN で ICMP 宛先到達不能メッセージの生成をディセーブルにします。
disable icmp useredirects	ICMP リダイレクトメッセージを受信しても、ルーティングテーブルを更新しないようにします。
disable irdp {vlan <name>}	指定した VLAN で ICMP ルータ広告メッセージの生成をディセーブルにします。

9.6 ルーティング設定例

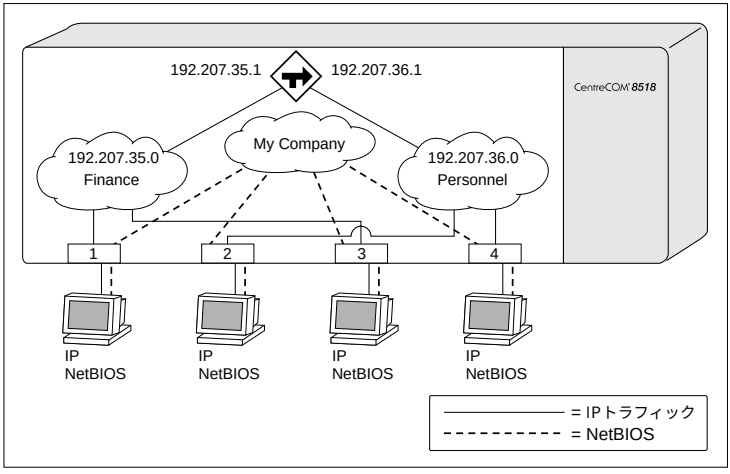
図 9-6 の例では、以下に示す 3 つの VLAN を定義しています。

- *Finance*
  - IP ベースのプロトコル VLAN
  - 所属ポートは 1 と 3
  - IP アドレスは 192.207.35.1
- *Personnel*
  - IP ベースのプロトコル VLAN

  - **所属ポートは** 2 **と** 4
  - IP **アドレスは** 192.207.36.1

- *MyCompany*
  - **ポート** VLAN
  - **すべてのポートが所属**

図 9-6：IP ユニキャストルーティングの設定例



ポート 1 ～ 4 **に接続された各機器は、**IP **と** NetBIOS **の両プロトコルを使用しています。**IP **トラフィックは** 2 **つのプロトコル** VLAN **によってフィルタリングされます。**IP **以外のトラフィックは、すべて** VLAN *MyCompany* **に転送されます。**

この例では、ポート 1 **と** 3 **に接続された機器からの** IP **トラフィックは、**VLAN *Finance* **を通じてルータに到達します。また、ポート** 2 **と** 4 **に接続された機器から送信される** IP **トラフィックは、**VLAN *Personnel* **を通じてルータに到達します。**IP **以外のトラフィック（**NetBIOS**）は、すべて** VLAN *MyCompany* **に所属します。**

図 9-6 **のネットワークは、以下のようにして設定します。**

```
create vlan Finance
create vlan Personnel
create vlan MyCompany

config vlan Finance protocol ip
config vlan Personnel protocol ip

config vlan Finance add ports 1,3
config vlan Personnel add ports 2,4
config vlan MyCompany add ports all

config vlan Finance ipaddress 192.207.35.1
config vlan Personnel ipaddress 192.207.36.1

enable ipforwarding
enable rip
```

9.7 IP ルーティングの設定確認

IP **ルーティング関係の各種設定を確認するには、表** 9-6 **のコマンドを使用します。**

表 9-6：IP ユニキャストルーティングの設定確認用コマンド

コマンド名	機能
show iparp proxy {<ipaddress> <mask>}	Proxy ARP テーブルを表示します。
show ipconfig {vlan <name>}	指定した VLAN の IP 設定内容を表示します。以下の情報が表示されます。 • IP アドレスとサブネットマスク • IP ルーティング情報 • BOOTP 設定 • VLAN 名と VLANid • ICMP 設定（グローバル） • IGMP 設定（グローバル） • IRDP 設定（グローバル）
show ipqos {<dest_ipaddress> <mask>}	IP QoS テーブルを表示します。
show ipstats {vlan <name>}	CPU が処理した IP パケットの統計を表示します。

表 9-6：IP ユニキャストルーティングの設定確認用コマンド

コマンド名	機能
show iparp {<ipaddress> | vlan <name> | permanent}	ARP テーブルを表示します。IP アドレス、VLAN、パーマネントエントリを指定することにより、表示項目のフィルタリングが可能です。表示される情報は、以下のとおりです。 • IP アドレス • MAC アドレス • エージングタイマー値 • VLAN 名、VLANid • フラグ
show ipfdb {<ipaddress> {<mask>} | vlan <name>}	IP フォワーディングデータベースの内容を表示します。テクニカルサポートが使用します。
show iproute {priority | vlan <name> | permanent | <ipaddress> <mask>}	IP ルーティングテーブルを表示します。

9.8 IP ルーティングのディセーブルとリセット

IP ルーティングの設定を出荷時の状態に戻したり、ルーティング機能をディセーブルにするには、表 9-7 のコマンドを使用します。

表 9-7：IP ユニキャストルーティングのディセーブル / リセット用コマンド

コマンド名	機能
clear iparp {<ipaddress> | vlan <name>}	ARP テーブルからダイナミックエントリを削除します。パーマネントエントリは削除されません。
clear ipfdb {<ipaddress> | vlan <name>}	IP フォワーディングデータベースからダイナミックエントリを削除します。
disable bootp vlan [<name> | all]	指定した VLAN の IP アドレス設定に BOOTP を使わないよう設定します。
disable bootprelay	DHCP/BOOTP リレー機能をディセーブルにします。
disable icmp redirects {vlan <name>}	指定した VLAN で ICMP リダイレクトメッセージの生成をディセーブルにします。
disable icmp unreachables {vlan <name>}	指定した VLAN で ICMP 宛先到達不能メッセージの生成をディセーブルにします。
disable icmp useredirects	ICMP リダイレクトメッセージを受信しても、ルーティングテーブルの更新を行わないようにします。
disable ipforwarding {vlan <name>}	指定した VLAN の IP ルーティング機能をディセーブルにします。
disable ipforwarding broadcast {vlan <name>}	指定した VLAN で IP ブロードキャストパケットの転送をディセーブルにします。

表 9-7：IP ユニキャストルーティングのディセーブル / リセット用コマンド

コマンド名	機能
disable irdp {vlan <name>}	指定した VLAN でルータ広告メッセージの生成をディセーブルにします。
unconfig icmp	すべての ICMP 設定をデフォルト値に戻します。
unconfig irdp	すべての IRDP 設定をデフォルト値に戻します。

9.9 参考文献

IP ユニキャストルーティングの詳細については、下記の文献を参考にしてください。

- RFC 1058 ― *Routing Information Protocol*
- RFC 1256 ― *ICMP Router Discovery Messages*
- RFC 1812 ― *Requirements for IP Version 4 Routers*

ルーティングプロトコルの詳細については、第 10 章「ルーティングプロトコル」をご覧ください。

10 ルーティングプロトコル

この章では、本製品がサポートする IP ユニキャストルーティングプロトコルについて解説します。ここでは、読者の皆様が IP ユニキャストルーティングに精通されているものと仮定して話を進めます。ルーティングについてよくご存知ない方は、10-19 ページの「参考文献」を参考にしてください。

10.1 概要

本製品は、IP ユニキャスト用ルーティングプロトコルとして、RIP（Routing Information Protocol）と OSPF（Open Shortest Path First）の 2 つをサポートしています。

RIP は、ベルマン = フォードのディスタンスベクタアルゴリズムに基づく、ディスタンスベクタ型の IGP（Interior Gateway Protocol ＝内部ゲートウェイプロトコル）です。ディスタンスベクタアルゴリズムは、長年にわたる使用実績があり、広く普及しています。

一方 OSPF は、Dijkstra リンクステートアルゴリズムに基づく、リンクステートプロトコルです。OSPF は RIP よりも新しいプロトコルであり、複雑化した今日のネットワーク環境において、RIP を使用した場合に発生するさまざまな問題を解決しています。

RIP と OSPF

RIP と OSPF の差異は、ディスタンスベクタとリンクステートアルゴリズムの本質的相違に起因しています。ディスタンスベクタアルゴリズムでは、隣接するルータから得た要約情報をもとに、各ルータがそれぞれ独自のルーティングテーブルを作成します。リンクステートアルゴリズムでは、自律システム（AS ＝ Autonomous System）内のすべてのルータから集められた情報をもとに、すべてのルータが同じルーティングテーブルを保持します。このテーブルの情報をもとに、各ルータは自分自身をルートとする最短経路ツリーを構築します。リンクステートアルゴリズムでは、他のルータへの更新通知に応答確認が返されるため、すべてのルータが同じトポロジマップを保持していることが保証されます。

RIP の最大の利点は、メカニズムが比較的シンプルなため理解や実装が容易であり、また長年にわたってデファクトスタンダードの地位にあることが挙げられます。

しかし、RIP には以下のような制限があるため、大規模なネットワークでは問題が発生する恐れがあります。

- 経由できるルータの数（ホップ数）が 15 までに制限されている。
- ルーティングテーブル全体が定期的に通知されるため、ネットワークの帯域が大量に消費される。

- 経路情報の収束（安定した状態になること）に時間がかかる。
- 経路選択をホップ数だけで行う。リンクコストや遅延の概念がない。
- エリアの概念がなく、全ルータが平等なフラットなネットワークを想定している。

OSPF が RIP よりも優れているのは、以下の点です。

- ホップ数の制限がない。
- 経路更新情報は、トポロジ変更があったときにだけマルチキャストアドレスに送信される。
- 収束が速い。
- 実際のリンクコストに基づく複数経路へのトラフィック分散が可能。
- ネットワークをエリアに分割した階層型トポロジの概念を導入。

この章では、RIP と OSPF について解説します。

10.2 RIP の概要

RIP は、1969 年に運用が開始された米国の研究ネットワーク ARPANET でも採用された IGP（Interior Gateway Protocol）です。RIP は、比較的規模の小さい均質なネットワークでの使用を前提に設計されました。

RIP ルータは、目的地のネットワークにいたる最適な経路を判断するにあたって、ホップ数が最小となる経路を選択します。ホップ数とは、目的地に到達するまでに経由するルータの数を表します。

ルーティングテーブル

RIP のルーティングテーブルには、既知のネットワークごとにエントリが作られます。各エントリには、以下の情報が含まれています。

- ネットワークの IP アドレス
- ネットワークまでのメトリック（ホップ数）
- 上記のネットワーク宛てのパケットを最初に転送するルータの IP アドレス
- エントリが最後に更新されてからの経過時間

各ルータは、デフォルトでは 30 秒ごとに隣接するルータとアップデートメッセージを交換します。また、経路情報が変化したときにも、隣接ルータに情報を送信します（トリガアップデート）。一定時間（ルートタイムアウト。デフォルトでは 180 秒）隣接するルータからメッセージが送られてこない場合は、そのルータとの間の経路が使用できなくなったと判断します。

スプリットホライズン（Split Horizon）

スプリットホライズンは、隣接ルータから得た経路情報を、情報の出所である隣接ルータに送り返すことによって発生するループを回避するためのアルゴリズムです。スプリットホライズンでは、隣接ルータへのアップデートメッセージに、その隣接ルータから取得した経路情報を含めません。

ポイズンリバース（Poison Reverse）

ポイズンリバースは、スプリットホライズンと同様、経路情報のループを防ぐためのアルゴリズムです。ポイズンリバースでは、隣接ルータから学習した経路情報を出所のルータにも送信しますが、その際にホップ数を 16 すなわち無限大とすることにより、その経路が到達不可能であることを伝えます。

トリガアップデート（Triggered Updates）

ルータがある経路のメトリックを変更したときは、アップデートタイマーの満了を待たずに、ただちにアップデートメッセージを送信します。これをトリガアップデートといいます。これには、収束を早める働きがありますが、RIP 関連のトラフィックが増加するという欠点もあります。

VLAN のルート広告

IP アドレスを持ちながら IP ルーティング機能がディセーブルに設定されている VLAN がある場合、その VLAN のサブネットアドレスは RIP を通じてメトリックが 16、つまり到達不可能であると広告されます。サブネットの広告を完全に停止するには、次のコマンドを実行して VLAN に割り当てた IP アドレスを削除します。

```
unconfig vlan <name> ipaddress
```

RIP1 と RIP2

RIP の新バージョンである RIP2 では、RIP1 に以下のような機能が追加されました。

- 可変長サブネットマスク（VLSM）
- ネクストホップアドレス

ネクストホップアドレスのサポートにより、複数のルーティングプロトコルを使用している環境で最適な経路を選択できるようになりました。

- マルチキャスト

RIP2 パケットはブロードキャスト（不特定多数への送信）ではなくマルチキャスト（特定多数への送信）されるため、ルーティングプロトコルをサポートしていないホストの負荷を軽減することができます。

10.3 OSPF の概要

OSPF は、同じ IP ドメイン（AS ＝自律システムとも呼ばれる）に属するルータ間で経路情報を交換するリンクステートプロトコルです。リンクステートプロトコルでは、各ルータが自律システムのトポロジ情報をデータベースに格納しています。各ルータは、同じデータベースをそれぞれ自分自身の視点から見た形で保持します。

各ルータは、このリンクステートデータベース（LSDB）をもとに、自分自身をルートとする最短経路ツリーを構築します。このツリーは、自律システム内の各目的地までの最適な経路を示すものです。同じコストを持つ経路が複数存在するならば、トラフィックを分散することが可能です。OSPF では、経路のコストを単一のメトリックで表します。

リンクステートデータベース

起動された各ルータは、自分の持つインタフェース上でリンクステート広告（LSA ＝ Link State Advertisement）と呼ばれるパケットを送信します。LSA には、リンクごとに次の情報が含まれています。

- リンクの IP アドレス
- リンクのサブネットマスク
- リンクのメトリック
- リンクの稼働状態（アップ / ダウン）

各ルータは、受信した LSA の情報をリンクステートデータベース（LSDB）に登録します。OSPF では、LSA の配布にフラッディング（Flooding）という方法を用います。経路情報の変更は、ネットワーク内のすべてのルータに送られます。これにより、エリア内のルータはすべて完全に同じ LSDB を持つことになります。表 10-1 に、LSA タイプを示します。

表 10-1：LSA タイプ

タイプ	名称
1	ルータリンク
2	ネットワークリンク
3	要約リンク
4	要約リンク（ASBR）
5	AS 外部リンク
7	AS 外部リンク（NSSA）

エリア

OSPF では、ネットワークをエリアと呼ばれる範囲に分割することができます。あるエリア内のトポロジ情報は、自律システム内の他のエリアからは見えないようになっており、これによって

LSA のトラフィックを大幅に削減し、LSDB の維持に必要なリソースを削減することができます。エリア内の経路は、エリアのトポロジ情報だけに基づいて決定されます。

OSPF では、ルータは次の 3 種類に分類されます。

- **内部ルータ**（IR ＝ Internal Router）

  すべてのインタフェースが同じエリア内にあるルータを内部ルータといいます。

- **エリア境界ルータ**（ABR ＝ Area Border Router）

  複数のエリアにインタフェースを持つルータをエリア境界ルータといいます。ABR は、他の ABR と要約リンク広告を交換する役割を持ちます。

- AS **境界ルータ**（ASBR ＝ Autonomous System Boundary Router）

  OSPF と他の自律システム（他のルーティングプロトコル）の間のゲートウェイとなるルータを AS 境界ルータといいます。

本製品は、内部ルータ、エリア境界ルータ、AS 境界ルータ、いずれの役割も果たすことができます。

エリア 0

複数のエリアを持つ OSPF ネットワークには、エリア番号 0 の「バックボーンエリア」が必要となります。自律システム内のすべてのエリアは、なんらかの形でバックボーンエリアに接続されていなくてはなりません。ネットワークを設計するときは、最初にエリア 0 を作成し、その後他のエリアを追加していくのがよいでしょう。

自律システム内にバックボーンエリアを設けることにより、AS 内の各 ABR はすべての ABR から要約リンク広告を受け取ることができます。ABR は受け取った情報をもとにして、エリア外にあるネットワークの距離関係を把握します。

VLAN で OSPF をイネーブルにすると、その VLAN は自動的にバックボーンエリア（0.0.0.0）の所属となります。VLAN の所属エリアを変更するには、次のコマンドを使います。

```
config ospf vlan <name> area <areaid>
```

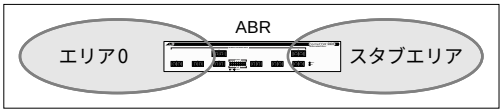
OSPF エリアの作成には、次のコマンドを使います。

```
create ospf area <areaid>
```

スタブエリア

OSPF では、1 つのエリアとしか接しておらず、出口が一つしかないスタブエリアというエリアを作成することができます。スタブエリアから外に出るトラフィックは、すべてデフォルトルートを使ってルーティングされます。スタブエリアには ASBR を置くことができず、AS 外部ルートの情報を持ちません。スタブエリアを使用すれば、OSPF ルータに求められるメモリや処理能力の要件を下げることができます。図 10-1 にスタブエリアの例を示します。

図 10-1：スタブエリア



スタブエリアの設定は、次のコマンドで行います。スタブエリア内のすべてのルータに設定が必要です。

```
config ospf area <areaid> stub [summary | nosummary] stub-default-cost <cost>
```

summary および nosummary は、スタブエリアの ABR に対してのみ有効なオプションで、次のような意味を持ちます。

- summary ― 他エリアの情報を持つ
- nosummary ― 他エリアの情報を持たず、自エリア内のルート情報とデフォルトルートだけを持つ

また、stub-default-cost <cost> もスタブ ABR に対してのみ有効なオプションで、デフォルトルートのコストを指定します。

準スタブエリア（NSSA=Not-So-Stubby-Area）

基本的にスタブエリアと同様ですが、次の 2 つの点が異なります。

- ASBR を置き、AS 外部ルートを持つことができる。
- AS 外部ルートを OSPF 内の他エリアに広告できる。

NSSA の設定コマンドは、スタブエリアとほぼ同じです。

```
config ospf area <areaid> nssa [summary | nosummary] stub-default-cost <cost>
{translate}
```

translate オプションは、NSSA 境界ルータにおいて、タイプ 7 LSA（AS 外部リンク（NSSA））をタイプ 5 LSA（AS 外部リンク）に変換して広告するものです。NSSA 境界ルータに translate オプションが指定されていない場合は、NSSA に接続されている ABR の一台が選出され、代わりにこの変換を行います。この選出メカニズムが正しく機能しなくなるため、NSSA 内部ルータには translate オプションを指定しないでください。

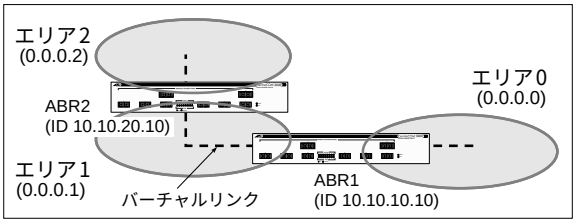
ノーマルエリア

バックボーンエリア、スタブエリア、準スタブエリアのいずれにもあてはまらないエリアをノーマルエリアといいます。ノーマルエリアはバーチャルリンクの通過点として使用できます。また、ノーマルエリア内には外部ルートを広告することができます。

バーチャルリンク

バックボーンエリアに隣接していないエリアでは、バーチャルリンクという仮想的な通信路を設定してバックボーンと通信を行います。バーチャルリンクは、ABR **と** ABR **の間に設定します。図** 10-2 **にバーチャルリンクの例を示します。**

図 10-2：スタブエリアとバックボーンを結ぶバーチャルリンク



バーチャルリンクの設定は次のコマンドで行います。

```
config ospf add virtual-link <routerid> <areaid>
```

バーチャルリンクの設定は、対向する双方の ABR **で行う必要があります。図** 10-2 **の例でいうと、**ABR1 **から** ABR2 **へと、**ABR2 **から** ABR1 **への設定が必要です。**

ABR1

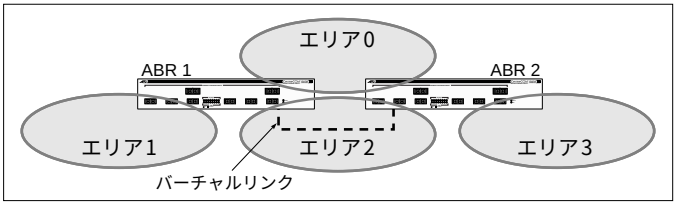
```
config ospf add virtual-link 10.10.20.10 0.0.0.1
```

ABR2

```
config ospf add virtual-link 10.10.10.10 0.0.0.1
```

バーチャルリンクは、バックボーンとのリンクに障害が発生した際にも使用されます。図 10-3 **では、**ABR1 **とバックボーンの間のリンクに障害が発生しても、**ABR1 **は**ABR2 **とのリンクをバーチャルリンクとして使うことにより、バックボーンとの通信を継続できます。**

図 10-3：バーチャルリンクによる冗長構成



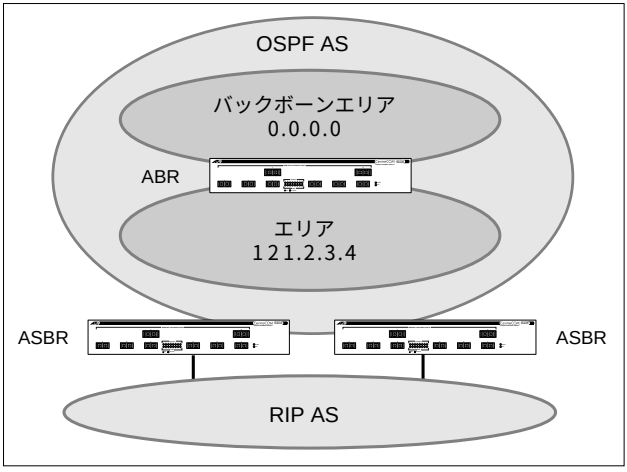
OSPF タイマーと認証設定

OSPF タイマーと認証の設定は、VLAN 単位でもエリア単位でもできますが、エリアに対して設定を行えば、その時点でエリアに属している VLAN すべてに設定が適用されます。ただし、あとで VLAN をエリアに追加した場合は、VLAN に対して明示的に設定を行う必要があります。

10.4 RIP-OSPF 間でのルート交換

本製品は、RIP と OSPF を同時に使用することができます。ルート交換機能を使用すれば、2 つのルーティングプロトコルの間でスタティックルートやダイナミックルートの情報を交換することができます。

図 10-4：RIP ― OSPF ドメイン間でのルート情報交換



筐体内で RIP と OSPF を同時に使用することはできますが、1 つの VLAN に両方を使用することはできません。

ルート交換の設定をする前に、RIP と OSPF それぞれの設定が適切に行われていることを確認してください。個々のルーティングプロトコルが正しく動作していることを確認した上で次の設定に進んでください。

OSPF Export：RIP/ スタティックルートを OSPF ドメイン内に広告する

RIP ルートやスタティックルートを OSPF ドメイン内に広告するには、次のコマンドを実行します。デフォルトはディセーブルです。

```
enable ospf export [static | rip] cost <metric> [ase-type-1 | ase-type-2]
{tag <number>}
```

```
disable ospf export [static | rip]
```

これにより、RIP やスタティックルートの情報が LSA の形で OSPF ドメイン内に広告されます。

OSPF ドメイン内に広告される RIP ルートやスタティックルートには、AS 間のコストメトリック情報が挿入されます。`ase-type-1` オプションは、AS 外部リンク広告のメトリックタイプとしてタイプ 1 を使うことを示します。メトリックタイプ 1 では、OSPF 内部と AS 間の合計コストがメトリック値として広告されます。一方、`ase-type-2` オプションでは、メトリックタイプ 2 を使用し、AS 外部コストのみを広告します。

`{tag <number>}` オプションは、AS 外部リンクの外部ルートタグフィールド値を指定するものですが、このフィールドは RFC でも規定されていないため、通常は 0 を指定しておきます。この値は、802.1Q VLAN タグとは関係がありません。

OSPF Export の設定を確認するには、次のコマンドを使います。

```
show ospf
```

RIP ルートを OSPF 内で広告するときは、RIP アグリゲーション機能をディセーブルにしてください。ファームウェアバージョン 4.1 からは、RIP アグリゲーションのデフォルト設定がディセーブルになりましたが、以前のバージョン（2.1.10 以前）からアップグレードした場合は、アップグレード前の設定が保持されますので、OSPF Export の設定時には show rip コマンドで確認するようにしてください。

RIP Export：OSFP/ スタティックルートを RIP ドメイン内に広告する

OSPF ルートやスタティックルートを RIP ドメイン内に広告するには、次のコマンドを使います。デフォルトはディセーブルです。

```
enable rip export [static | ospf | ospf-intra | ospf-inter | ospf-extern1 |
ospf-extern2] cost <metric> {tag <number>}
```

```
disable rip export [ospf | ospf-intra | ospf-inter | ospf-extern1 | ospf-
extern2]
```

OSPF ルートを RIP ドメイン内に広告するときは、どのタイプの OSPF ルートを広告するかを選択できます。`ospf` オプションを指定した場合は、すべての OSPF ルートが広告されます。

10.5 RIP 設定コマンド

表 10-2 に RIP 設定コマンドの一覧を示します。

表 10-2：RIP 設定コマンド

コマンド名	機能
enable rip	RIP をイネーブルにします。デフォルトの設定はディセーブルです。
enable rip aggregation	RIP2（互換）パケットを送信するよう設定されたインタフェース上で、サブネット情報のアグリゲーション機能（RIP Aggregation）を有効にします。この機能をオンにした場合、複数のサブネットルートが、もっとも近いクラスのネットワークルートに集約して広告されます。本機能の使用時には、以下のルールが適用されます。 • 標準の IP クラス境界をまたぐ複数のサブネットルートは、もっとも近いクラスのネットワークルートに集約されます。 • 標準の各 IP クラスにおけるマスクが適用されるルートは集約されません。 • 本機能がイネーブルのときは、RIP1 と同じ動作になります。 • 本機能がディセーブルのときは、たとえクラス境界をまたぐサブネットマスクが適用されていても、ルート情報の集約は行われません。 デフォルトはディセーブルです。
enable rip export [ospf | ospf-intra | ospf-inter | ospf-extern1 | ospf-extern2 | static] cost <metric> {tag <number>}	OSPF ルートまたはスタティックルートを RIP ドメイン内に広告します。デフォルトはディセーブルです。
enable rip poisonreverse	スプリットホライズンとポイズンリバースアルゴリズムをイネーブルにします。デフォルトはイネーブルです。ポイズンリバースが優先されます。
enable rip splithorizon	スプリットホライズンアルゴリズムをイネーブルにします。デフォルトはイネーブルです。
enable rip triggerupdates	トリガアップデートをイネーブルにします。これは経路情報が変更されると、ただちに隣接ルータに通知する機能です。デフォルトはイネーブルです。
config rip add vlan [<name> | all]	指定した IP インタフェースで RIP をイネーブルにします。IP インタフェース作成時のデフォルト設定はディセーブルです。
config rip delete vlan [<name> | all]	指定した IP インタフェースで RIP をディセーブルにします。ただし、RIP パラメータはデフォルト値に戻りません。
config rip garbagetime <value>	ガーベッジコレクションタイムを 10 秒刻みで設定します。デフォルトは 120 秒です。
config rip routetimeout <value>	ルートタイムアウトを 10 秒刻みで設定します。デフォルトは 180 秒です。

表 10-2：RIP 設定コマンド

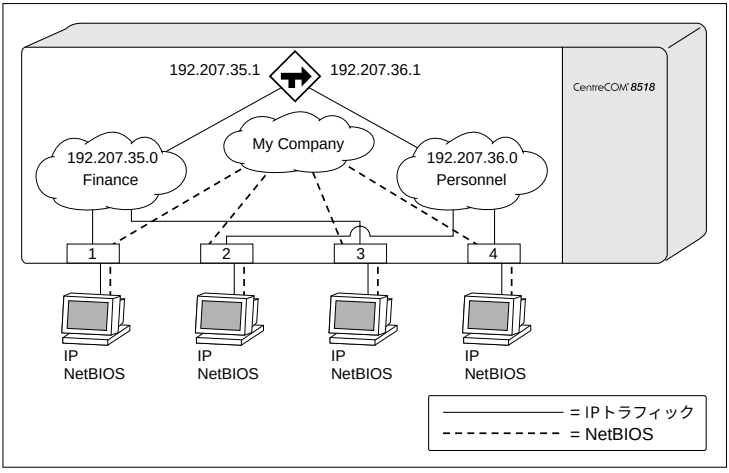
コマンド名	機能
config rip rxmode [none | v1only | v2only | any] {vlan <name> | all}	指定した VLAN の RIP 受信モードを設定します。 • none − RIP パケットを受信しません。 • v1only − RIP1 形式のパケットのみ受信します。 • v2only − RIP2 形式のパケットのみ受信します。 • any − RIP1 と RIP2 形式のパケットを受信します。 VLAN 名を省略した場合、すべての VLAN に設定が適用されます。デフォルトは any です。
config rip txmode [none | v1only | v1compatible | v2only] {vlan <name> | all}	指定した VLAN の RIP 送信モードを設定します。 • none − RIP パケットを送信しません。 • v1only − RIP1 形式のパケットをブロードキャストアドレスにて送出します。 • v1compatible − RIP2 形式のパケットをブロードキャストアドレスにて送出します。 • v2only − RIP2 形式のパケットをマルチキャストアドレスにて送出します。 VLAN 名を省略した場合、すべての VLAN に設定が適用されます。デフォルトは v2only です。
config rip updatetime <value>	RIP アップデートタイマーを 10 秒刻みで設定します。デフォルトは 30 秒です。

RIP 設定例

図 10-5 の例では、3 つの VLAN が設定されています。

- *Finance*
  - IP ベースのプロトコル VLAN
  - 所属ポートは 1 と 3
  - VLAN アドレスは 192.207.35.1
- *Personnel*
  - IP ベースのプロトコル VLAN
  - 所属ポートは 2 と 4
  - VLAN アドレスは 192.207.36.1
- *MyCompany*
  - ポート VLAN
  - すべてのポートが所属

図 10-5：RIP 設定例



この例では、ポート 1 ～ 4 **に** IP **と** NetBIOS **の両トラフィックが混在しています。**IP **トラフィックはプロトコルフィルタ「**ip**」によってフィルタリングされ、残りのトラフィックは** VLAN *MyCompany* **に転送されます。**

この構成例では、ポート 1 **とポート** 3 **に接続された機器から送信された** IP **トラフィックは、**VLAN *Finance* **を通じてルータインタフェースに到達します。ポート** 2 **とポート** 4 **も同様に** VLAN *Personnel* **を通じてルータに到達します。**IP **以外のすべてのトラフィック（**NetBIOS**）は** VLAN *MyCompany* **に所属しています。**

図 10-5 **のネットワークを設定するには、以下のようにします。**

```
create vlan Finance
create vlan Personnel
create vlan MyCompany

config vlan Finance protocol ip
config vlan Personnel protocol ip

config vlan Finance add ports 1,3
config vlan Personnel add ports 2,4
config vlan MyCompany add ports all

config vlan Finance ipaddress 192.207.35.1
config vlan Personnel ipaddress 192.207.36.1

enable ipforwarding
config rip add vlan all
enable rip
```

10.6 RIP 設定内容の確認

表 10-3 に RIP 設定内容を確認するためのコマンドを示します。

表 10-3：RIP 設定確認用コマンド

コマンド名	機能
show rip {vlan <name>}	指定した VLAN の RIP 設定と統計を表示します。
show rip stats {vlan <name>}	RIP 関連の統計情報を表示します。ルータインタフェースごとに、以下の情報が表示されます。 • 送信パケット数 • 受信パケット数 • エラーパケット数 • エラー経路数 • RIP peer 数 • peer 情報

10.7 RIP のディセーブルとリセット

RIP 設定をデフォルト値に戻したり、RIP をディセーブルにするには、表 10-4 のコマンドを使います。

表 10-4：RIP のディセーブル / リセット用コマンド

コマンド名	機能
config rip delete vlan [<name> | all]	指定したインタフェースで RIP をディセーブルにします。RIP パラメータはリセットされません。
disable rip	RIP をディセーブルにします。
disable rip aggregation	RIP2 インタフェースで、サブネット情報のアグリゲーション機能（RIP Aggregation）をディセーブルにします。
disable rip splithorizon	スプリットホライズンをディセーブルにします。
disable rip poisonreverse	ポイズンリバースをディセーブルにします。
disable rip triggerupdates	トリガアップデートをディセーブルにします。
disable rip export static	スタティックルートの広告をディセーブルにします。
diable rip export [ospf | ospf-intra | ospf-inter | ospf-extern1 | ospf-extern2]	RIP ドメイン内への OSPF ルートの広告をディセーブルにします。
unconfig rip {vlan <name>}	RIP パラメータをデフォルト値に戻します。RIP のイネーブル / ディセーブルは変わりません。

10.8 OSPF 設定コマンド

OSPF を使用する場合は、筐体ごとにユニークなルータ ID を設定する必要があります。ルータ ID は自動設定することもできますが（その場合、筐体に設定された IP アドレスのうち最も大きいものがルータ ID になります）、手動で設定することをおすすめします。自動設定にした場合、OSPF のイネーブル / ディセーブルによってルータ ID が変わる可能性があり、規模の大きいネットワークでは変更前の古いルータ ID でリンクステートデータベースが使われ続けるおそれがあるためです。

ルータ ID の設定は、`config ospf routerid <routerid>` コマンドで行います。

表 10-5 に OSPF 設定コマンドの一覧を示します。

表 10-5：OSPF 設定コマンド

コマンド名	機能
create ospf area <areaid>	OSPF エリアを作成します。デフォルトのエリア ID は 0.0.0.0 です。
enable ospf	OSPF をイネーブルにします。
enable ospf export static cost <metric> [ase-type-1 | ase-type-2] {tag <number>}	スタティックルートを他の OSPF ルータに広告します。デフォルトタグ番号は 0 です。デフォルト設定はディセーブルです。
enable ospf export rip cost <metric> [ase-type-1 | ase-type-2] {tag <number>}	RIP ルートを他の OSPF ルータに広告します。デフォルトタグ番号は 0 です。デフォルト設定はディセーブルです。
config ospf [vlan <name> | area <areaid> | virtual-link <routerid> <areaid>] authentication [simple-password <password> | md5 <md5_key_id> <md5_key>| none]	OSPF エリア内のインタフェースの認証パスワード（最大 8 文字）または MD5 キーを設定します。`<md5_key>` には 0 ～ 65536 の数値を指定します。OSPF エリアを指定した場合、認証情報はエリア内のすべてのインタフェースに適用されます。
config ospf vlan <name> area <areaid>	VLAN（ルータインタフェース）と OSPF エリアを関連付けます。ルータインタフェースは、必ず OSPF エリアと関連付けなくてはなりません。デフォルトの `<areaid>` は 0.0.0.0 すなわち バックボーンエリアです。
config ospf [vlan [<name> | all] | area <areaid>] cost <value>	指定したインタフェースのコストメトリックを設定します。デフォルトは 1 です。
config ospf [vlan [<name> | all] | area <areaid>] priority <value>	指名ルータ（DR）の選出アルゴリズムで使用されるルータ優先度を設定します。有効範囲は 0 ～ 255、デフォルトは 1 です。
config ospf add vlan [<name> | all]	指定した VLAN（ルータインタフェース）で OSPF をイネーブルにします。デフォルトはディセーブルです。
config ospf delete vlan [<name> | all]	指定した VLAN で OSPF をディセーブルにします。

表 10-5：OSPF 設定コマンド

コマンド名	機能
config ospf add virtual-link <routerid> <areaid>	他の ABR と接続するバーチャルリンクを追加します。 • routerid − 対向するルータのルータ ID です。 • areaid − 2 点間を結ぶ通過エリアの ID です。通過エリアの ID は、0.0.0.0（バックボーンエリア）以外となります。
config ospf delete virtual-link <routerid> <areaid>	バーチャルリンクを削除します。
config ospf area <areaid> normal	指定した OSFP エリアをノーマルエリアにします。デフォルトは normal です。
config ospf area <areaid> stub [summary | nosummary] stub-default-cost <value>	指定した OSPF エリアをスタブエリアにします。
config ospf area <areaid> nssa [summary | nosummary] stub-default-cost <value> {translate}	指定した OSPF エリアを準スタブエリア（NSSA）にします。
config ospf area <areaid> add range <ipaddress> <mask> [advertise | noadvertise] {type-3 | type-7}	OSPF エリアにアドレスレンジを追加します。ABR がエリア外にルート情報を送信する際、アドレスレンジに含まれるサブネットワークは 1 つのアドレスに集約してから広告します。noadvertise オプションを指定した場合、当該アドレスレンジは広告されません。
config ospf area <areaid> delete range <ipaddress> <mask>	OSPF エリアに設定したアドレスレンジを削除します。
config ospf routerid [automatic | <routerid>]	OSPF のルータ ID を設定します。automatic を指定した場合は、もっとも大きい IP アドレスが使用されます。デフォルトは automatic です。

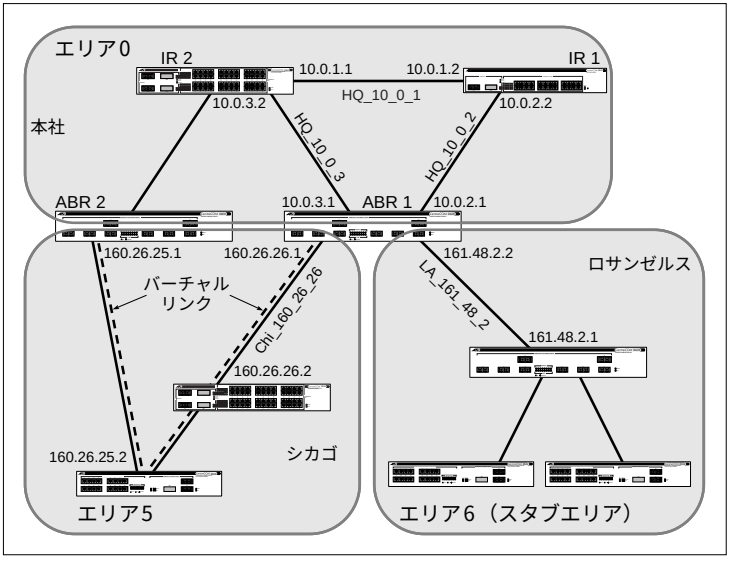
表 10-5：OSPF設定コマンド

コマンド名	機能
config ospf [vlan <name> | area <areaid> | virtual-link <routerid> <areaid>] timer <retransmission_interval> <transmission_delay> <hello_interval> <dead_interval>	指定したインタフェースまたはエリア内の全インタフェースのタイマーを設定します。各タイマーのデフォルト値、最小値、最大値（秒）は以下のとおりです。 • retransmission_interval デフォルト：5 最小：1 最大：3600 • transmission_delay デフォルト：1 最小：0 最大：3600 • hello_interval デフォルト：10 最小：1 最大：65535 • dead_interval デフォルト：40 最小：1 最大：2147483647
config ospf spf-hold-time <second>	SPF（Shortest Path First）の再計算を行う最小間隔を指定します。デフォルトは3 秒です。

10.9 OSPF 設定例

図 10-6 に示すのは、OSPF ルータを用いた自律システムの構成例です。

図 10-6：OSPF構成例



エリア 0 **は、本社に位置するバックボーンエリアで、以下の属性を持ちます。**

- **内部ルータは** 2 **個（**IR1 **と** IR2**）**
- **エリア境界ルータは** 2 **個（**ABR1 **と** ABR2**）**
- **ネットワークアドレスは** 10.0.x.x

エリア 5 **は、シカゴに位置するネットワークで、**ABR1 **と** ABR2 **を介してバックボーンエリアと接続されています。**

- **ネットワークアドレスは** 160.26.x.x
- **内部ルータは** 2 **個**
- ABR1 **から** ABR2 **へのバーチャルリンクが、両方の内部ルータを通過している。**

  エリア境界ルータのどちらかに障害が発生しても、バーチャルリンクを使ってすべてのルータがバックボーンとの通信を継続できます。

エリア 6 **は、ロサンゼルスに位置するスタブエリアで、**ARB1 **を介してバックボーンエリアと接続されています。**

- **ネットワークアドレスは** 161.48.x.x
- **内部ルータは** 3 **個**
- **エリア間ルーティングにデフォルトルートを使用。**

図 10-6 のネットワークを構成するルータのうち、2 つのルータの設定例を次に示します。

ABR1 の設定

エリア境界ルータ ABR1 は、以下のようにして設定します。

```
create vlan HQ_10_0_2
create vlan HQ_10_0_3
create vlan LA_161_48_2
create vlan Chi_160_26_26

config vlan HQ_10_0_2 ipaddress 10.0.2.1 255.255.255.0
config vlan HQ_10_0_3 ipaddress 10.0.3.1 255.255.255.0
config vlan LA_161_48_2 ipaddress 161.48.2.2 255.255.255.0
config vlan Chi_160_26_26 ipaddress 160.26.26.1 255.255.255.0

create ospf area 0.0.0.5
create ospf area 0.0.0.6

enable ipforwarding

config ospf area 0.0.0.6 stub nosummary stub-default-cost 10
config ospf vlan LA_161_48_2 area 0.0.0.6
config ospf vlan Chi_160_26_26 area 0.0.0.5
config ospf add virtual-link 160.26.25.1 0.0.0.5
config ospf add vlan all

enable ospf
```

IR1 の設定

内部ルータ IR1 の設定例を次に示します。

```
config vlan HQ_10_0_1 ipaddress 10.0.1.2 255.255.255.0
config vlan HQ_10_0_2 ipaddress 10.0.2.2 255.255.255.0
config ospf add vlan all
enable ipforwarding
enable ospf
```

10.10 OSPF 設定内容の確認

OSPF の設定内容を確認するには、表 10-6 のコマンドを使います。

表 10-6：OSPF 設定確認用コマンド

コマンド名	機能
show ospf	OSPF 情報全般を表示します。
show ospf area {<areaid>}	指定した OSPF エリアの情報を表示します。

表 10-6：OSPF 設定確認用コマンド

コマンド名	機能
show ospf interfaces {vlan <name> | area <areaid>}	OSPF インタフェースの情報を表示します。オプションを省略した場合は、すべてのインタフェースの情報が表示されます。
show ospf lsdb {detail} area [<areaid> | all] [router | network | summary-net | summary-asb | as-external | external-type7 | all]	リンクステートデータベースの内容を表示します。`detail` オプションを指定すると、エントリごとにすべての LSA 情報が表示されます。
show ospf virtual-link {routerid <routerid> <areaid> | all}	指定したルータのバーチャルリンク情報を表示します。

10.11 OSPF 設定のディセーブルとリセット

OSPF 設定をデフォルト値に戻すには、表 10-7 のコマンドを使用します。

表 10-7：OSPF のディセーブル / リセット用コマンド

コマンド名	機能
unconfig ospf {vlan <name> | <areaid>}	OSPF インタフェースの設定値をデフォルトに戻します。
delete ospf area [<areaid> | all]	OSPF エリアを削除します。関連する OSPF エリアと OSPF インタフェースの情報も削除されます。
disable ospf	OSPF をディセーブルにします。
disable ospf export static	OSPF ドメイン内へのスタティックルートの広告をディセーブルにします。
disable ospf export rip	OSPF ドメイン内への RIP ルートの広告をディセーブルにします。

10.12 参考文献

- RFC 1058 ― *Routing Information Protocol (RIP)*
- RFC 1256 ― *ICMP Router Discovery Messages*
- RFC 1723 ― *RIP Version 2*
- RFC 2178 ― *OSPF Version 2*

11 IP マルチキャストルーティング

この章では、IP マルチキャストルーティングの概要と、本製品における IP マルチキャスト機能の設定方法について説明します。IP マルチキャストの詳細については、章末の参考文献を参照してください。

11.1 概要

IP マルチキャストは、単一のホストから特定多数のホスト（ホストグループ）に IP パケットを送信する一対多の通信機能です。ホストグループには、ローカルネットワーク内の機器だけでなく、外部ネットワークの機器を含めることもできます。

IP マルチキャストルーティングには、以下のものが必要です。

- IP マルチキャストパケットをフォワードできるルータ
- ルータ間でマルチキャストルーティング情報を交換するためのプロトコル（例：DVMRP、PIM-DM）
- IP ホストがマルチキャストグループへの所属情報をルータに伝えるためのプロトコル（例：IGMP）

IP マルチキャストルーティングを使用するには、あらかじめ IP ユニキャストルーティングの設定を行っておく必要があります。

DVMRP（Distance Vector Multicast Routing Protocol）

DVMRP は、ルータ間で IP マルチキャストルーティング情報を交換するためのディスタンスベクタ型ルーティングプロトコルです。DVMRP では、RIP と同じように、隣接するルータ間で定期的にルーティングテーブルの交換が行われます。

DVMRP には、IP マルチキャストによる帯域の消費量を減らすため、マルチキャストツリーから不要な経路を削除する Prune（枝刈り）メカニズムと、ツリーに新しい経路を追加する Graft（接ぎ木）メカニズムが備わっています。

PIM-DM（Protocol Independent Multicast - Dense Mode）

PIM-DM は、DVMRP と同様に Reverse Path Multicasting（RPM）を利用するマルチキャストルーティングプロトコルです。マルチキャストツリーを最適な状態に保つ Prune と Graft のメカニズムも備えています。

DVMRP と大きく異なるのは、DVMRP が RPM 用に独自のルーティングテーブルを持つのに対し、PIM-DM ではユニキャストルーティング用のルーティングテーブルを使用する点です。これにより、PIM-DM ではメモリの消費量を抑えています。

DVMRP と PIM-DM を同時に使用することはできません。

IGMP（Internet Group Management Protocol）

IGMP は、IP ホストが IP マルチキャストグループへの所属情報をルータに伝えるためのプロトコルです。IGMP 対応のルータは、マルチキャストグループに対して定期的に問い合わせを行い、グループに属するホストがまだ存在しているかどうかを調べます。グループが活動中の場合は、グループ内のホストの 1 つが問い合わせに応答して、グループに所属するホストが存在していることをルータに伝えます。

IGMP スヌーピング

IGMP スヌーピングは、レイヤー 2 機器（スイッチなど）向けのマルチキャストフィルタリング技術です。IGMP スヌーピングでは、マルチキャストトラフィックを必要とするホストが接続されたポートにだけマルチキャストパケットを転送するため、ネットワークの帯域を有効に利用できるようになります。ただし、ローカルマルチキャストドメイン（224.0.0.x）のマルチキャストトラフィックはフィルタリングしません。

IGMP はデフォルトでイネーブルになっています。マルチキャストルーティングを使用するときは、必ず IGMP スヌーピングをイネーブルにしてください。IGMP スヌーピングをディセーブルにしてしまうと、すべての IGMP および IP マルチキャストパケットが VLAN 内にフラッディングされてしまいます。IGMP スヌーピングでは、ネットワーク上に少なくとも 1 台は IGMP クエリーメッセージを定期的に送信するノードがあると仮定しています。IGMP クエリーを受信できない場合は、すべてのポートについて IP マルチキャストパケットの転送を完全にストップします。

IGMP スヌーピングでは、オプションとして、DVMRP（224.0.0.4）あるいは PIM（224.0.0.13）マルチキャストグループに参加しているデバイスのみをマルチキャストルータと見なし、これらにのみマルチキャストトラフィックを転送する設定も可能です。

11.2 IP マルチキャストルーティングの設定

IP マルチキャストルーティングの設定は、以下の手順で行います。

1　IP ユニキャストルーティングの設定を行います。

IP ユニキャストルーティングの設定方法については、第 9 章「IP ユニキャストルーティング」と第 10 章「ルーティングプロトコル」をご覧ください。

2 IP マルチキャストルーティングを実行したい IP インタフェース（VLAN）に対して、以下のコマンドを実行します。

```
enable ipmcforwarding {vlan <name>}
```

3 IP インタフェース（VLAN）単位で DVMRP または PIM-DM をイネーブルにします。

```
config dvmrp add vlan [<name> | all]
config pim-dm add vlan [<name> | all]
```

4 ルータの DVMRP または PIM-DM 設定をイネーブルにします。

```
enable dvmrp
enable pim-dm
```

表 11-1 に IP マルチキャストルーティング設定コマンドの一覧を示します。

表 11-1：IP マルチキャストルーティング設定コマンド

コマンド名	機能
enable dvmrp	スイッチ全体で DVMRP をイネーブルにします。デフォルトはディセーブルです。
enable dvmrp txmode vlan [<name> | all]	指定した IP インタフェース（VLAN）で DVMRP パケットの送信をイネーブルにします。
disable dvmrp txmode vlan [<name> | all]	指定した IP インタフェース（VLAN）で DVMRP パケットの送信をディセーブルにします。
enable dvmrp rxmode vlan [<name> | all]	指定した IP インタフェース（VLAN）で DVMRP パケットの受信をイネーブルにします。
disable dvmrp rxmode vlan [<name> | all]	指定した IP インタフェース（VLAN）で DVMRP パケットの受信をディセーブルにします。
enable ipmcforwarding {vlan <name>}	指定した IP インタフェース（VLAN）上で IP マルチキャストルーティングをイネーブルにします。VLAN 名を指定しなかった場合は、IP アドレスを割り当てられたすべての VLAN でマルチキャストルーティングが有効になります。新規追加された IP インタフェースのデフォルト設定はディセーブルです。
config dvmrp add vlan [<name> | all]	指定した IP インタフェースで DVMRP をイネーブルにします。新規に追加された IP インタフェースのデフォルト設定はイネーブルです。
config dvmrp delete [vlan <name> | all]	指定した IP インタフェースで DVMRP をディセーブルにします。

表 11-1：IP マルチキャストルーティング設定コマンド

コマンド名	機能
config dvmrp vlan <name> timer <probe_interval> <neighbor_timeout_interval>	指定した IP インタフェースの DVMRP タイマーを設定します。 • probe_interval － DVMRP プローブメッセージの送信間隔を指定します。有効範囲は 1 ～ 2147483647 秒（68 年）、デフォルトは 10 秒です。 • neighbor_timeout_interval － 隣接する DVMRP ルータのタイムアウトを設定します。ここで設定した時間が過ぎても隣接する DVMRP ルータからの反応がない場合は、そのルータとの間の経路が不通になったものと判断します。有効範囲は 1 ～ 2147483647 秒（68 年）、デフォルトは 35 秒です。
config dvmrp timer <route_report_interval> <route_replacement_time>	グローバルに適用される DVMRP タイマーを設定します。 • route_report_interval － ルートリポートパケットの送信間隔を指定します。有効範囲は 1 ～ 2147483647 秒（68 年）、デフォルトは 60 秒です。 • route_replacement_time － ある経路が削除された後、新しいルートを学習するまでの待機時間（ホールドダウンタイム）を指定します。有効な値は 1 ～ 2147483647 秒（68 年）、デフォルトは 140 秒です。
enable pim-dm	PIM-DM をイネーブルにします。デフォルトはディセーブルです。
config pim-dm add vlan [<name> | all]	指定した IP インタフェースで PIM-DM をイネーブルにします。
config pim-dm delete vlan [<name> | all]	指定した IP インタフェースで PIM-DM をディセーブルにします。
config pim-dm timer <hello_interval>	PIM-DM Hello パケットの送信間隔を設定します。1 ～ 65519 秒の間で指定します。デフォルトは 30 秒です。

表 11-2 に IGMP 設定コマンドの一覧を示します。

表 11-2：IGMP 設定コマンド

コマンド名	機能
enable igmp {vlan <name>}	指定した IP インタフェース（VLAN）で IGMP をイネーブルにします。デフォルトはイネーブルです。
enable igmp snooping {forward-mcrouter-only}	IGMP スヌーピングをイネーブルにします。forward-mcrouter-only オプションを指定した場合は、マルチキャストルータにのみマルチキャストトラフィックを転送します。指定がない場合は、すべての IP ルータにマルチキャストトラフィックを転送します。

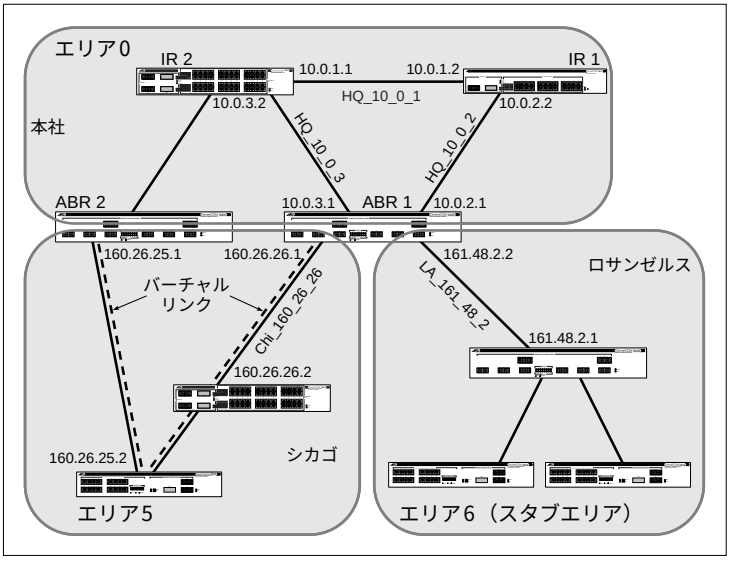
表 11-2：IGMP 設定コマンド

コマンド名	機能
config igmp <query_interval> <query_response_interval> <last_member_query_interval>	IGMP タイマーを設定します。以下のタイマーは RFC2236 に基づいています。 • query_interval ー General Querie の送信間隔を 1 ～ 2147483647 秒（68 年）で指定します。デフォルトは 125 秒です。 • query_response_interval ー General Query パケットに挿入される Max Response Time を設定します。有効範囲は 1 ～ 25 秒、デフォルトは 10 秒です。 • last_member_query_interval ー Leave Group メッセージへの応答として、Group-Specific Query パケットに挿入される Max Response Time を設定します。有効範囲は 1 ～ 25 秒、デフォルトは 1 秒です。
config igmp snooping timer <router_timeout> <host_timeout>	IGMP スヌーピングタイマーを設定します。以下のタイマーは、通常 query_interval の約 2.5 倍に設定します。 • router_timeout ー 発見されたルータの有効時間を設定します。有効範囲は 10 ～ 2147483647 秒（68 年）、デフォルトは 260 秒です。 • host_timeout ー IGMP グループリポートメッセージ送信後のホストの有効時間を設定します。有効範囲は 10 ～ 2147483647 秒（68 年）、デフォルトは 260 秒です。

11.3 IP マルチキャストルーティングの設定例

図 11-1 は、第 10 章でも登場した本製品による OSPF 構成例です。OSPF の詳しい設定方法については、10-14 ページの「OSPF 設定コマンド」をご覧ください。この例では、エリア 0 の内部ルータ IR1 を IP マルチキャストルーティング用に設定します。

図 11-1：IP マルチキャストルーティングの設定例



IR1 の設定

内部ルータ IR1 **の設定は、次のようにして行います。**

```
config vlan HQ_10_0_1 ipaddress 10.0.1.2 255.255.255.0
config vlan HQ_10_0_2 ipaddress 10.0.2.2 255.255.255.0
config ospf add vlan all
enable ipforwarding
enable ospf
enable ipmcforwarding
config dvmrp add vlan all
enable dvmrp
```

11.4 IP マルチキャストルーティング設定の確認

IP **マルチキャストルーティングの設定内容を確認するには、表** 11-3 **に示すコマンドを使います。**

表 11-3：IP マルチキャストルーティングの設定確認用コマンド

コマンド名	機能
show dvmrp {vlan <name> | route {detail}}	DVMRP の設定および統計、あるいはユニキャストルーティングテーブルを表示します。オプションを指定しなかった場合は、すべての情報が表示されます。

表 11-3：IP マルチキャストルーティングの設定確認用コマンド

コマンド名	機能
show igmp snooping {vlan <name>}	IGMP スヌーピングの登録情報と IGMP タイマーおよびステータスの要約情報を表示します。
show ipmc cache {detail} {<group> {<src_ipaddress> <mask>} | all}	IP マルチキャストフォワーディングキャッシュの内容を表示します。以下の情報が表示されます。 • マルチキャストグループアドレス • 送信元IP アドレスとネットマスクおよび VLAN • ルーティングプロトコル • ルーティングの状態
show pim-dm {vlan <name>}	PIM-DM の設定と統計情報を表示します。VLAN 名を指定しなかった場合は、すべての PIM-DM インタフェースに関する情報が表示されます。

11.5 IP マルチキャスト設定のディセーブルとリセット

IP マルチキャストルーティングの設定を出荷時の状態に戻したり、IP マルチキャストルーティング機能を無効にしたいときは、表 11-4 に示すコマンドを使います。

表 11-4：IP マルチキャストルーティング設定のディセーブル / リセット用コマンド

コマンド名	機能
disable dvmrp	DVMRP をディセーブルにします。
disable ipmcforwarding {vlan <name>}	IP マルチキャストルーティング機能をディセーブルにします。
disable igmp {vlan <name>}	指定したIP インタフェース（VLAN）で IGMP をディセーブルにします。
disable igmp snooping	IGMP スヌーピングをディセーブルにします。IP マルチキャストルーティング使用時は、ディセーブルにしないでください。IGMP スヌーピングがディセーブルのときは、IGMP および IP マルチキャストトラフィックが、VLAN 内にフラッディングされます。
disable pim-dm	PIM-DM をディセーブルにします。
unconfig dvmrp {vlan <name>}	DVMRP タイマーをデフォルト値に戻します。
unconfig igmp	IGMP 設定をデフォルト値に戻し、IGMP グループテーブルを初期化します。
unconfig pim-dm {vlan <name>}	PIM-DM パラメータをデフォルト値に戻します。
clear igmp snooping {vlan <name>}	IGMP スヌーピングのエントリを削除します。

表 11-4：IP マルチキャストルーティング設定のディセーブル / リセット用コマンド

コマンド名	機能
clear ipmc cache {<group> {<src_ipaddress> <mask>} | all}	IP マルチキャストキャッシュテーブルを初期化します。オプションを指定しなかった場合は、すべてのエントリが消去されます。

11.6 参考文献

- RFC 1112 ー *Host Extension for IP Multicasting*
- RFC 2236 ー *Internet Group Management Protocol, Version 2*
- DVMRP Version 3 ー *draft-ietf-idmr-dvmrp-v3-08*
- PIM-DM Version2 ー *draft-ietf-pim-v2-dm-01*
- IETF DVMRP Working Group ー *http://www.ietf.org/html.charters/idmr-charter.html*
- IEFT PIM-DM Working Group ー *http://www.ietf.org/html.charters/pim-charter.html*

12 IPX ルーティング

この章では、IPX の概要と IPX ルーティングの設定方法について説明します。

12.1 概要

IPX（Internet Packet eXchange）は、Novell 社のネットワークオペレーティングシステム「NetWare」で使用されるネットワークプロトコルです。OSI の参照モデルでは第 3 層のネットワーク層にあたり、IP と同様のインターネットワーキング機能を提供します。

本製品は、IPX パケットのルーティング機能を備えています。スタティックルーティングに加え、IPX/RIP によるダイナミックルーティングも可能です。また、ネットワーク上で使用可能なリソースを広告する IPX/SAP にも対応しています。

IPX のルーティングは、ハードウェア（ASIC）ではなくソフトウェアによって実現されます。そのため、IP ルーティングと同じワイヤスピードのルーティングは不可能ですのでご注意ください。なお、同一 VLAN 内における IPX パケットのスイッチング（ブリッジング）はワイヤスピードで行われます。

IPX アドレス

IPX ネットワークアドレスは次の各要素で構成されます。IPX アドレスは、通常 16 進数で表記します。

- **ネットワーク番号(32 ビット)** − IPX インターネットワーク内で個々の IPX ネットワークを識別するための番号です（0x00 00 00 00 はローカルネットワークを表す）。インターネットワーク内で重複がないよう管理者が設定します。なお、NetWare サーバは、それ自身が仮想的なネットワーク番号（内部ネットワーク番号。通常は NetWare 製品のシリアル番号）を持ちます。
- **ノード番号（48 ビット）** − IPX ネットワーク上で個々のノードを識別するための番号です。通常はノードのハードウェアアドレス（イーサネットでは MAC アドレス）がノード番号になります。0xff ff ff ff ff ff はブロードキャストを表します。サーバのノード番号は通常 1（0x00 00 00 00 00 01）です。
- **ソケット番号（16 ビット）** − IPX ノード内で動作中のプロセスを識別するための番号です。0x4000 ～ 0x8000 は Novell 社によって予約されています。表 12-1 にソケット番号の例を示します。

表 12-1：IPX ソケット番号の例

ソケット	ソケット番号
ファイルサーバ（NCP）	0x0451
IPX/SAP	0x0452
IPX/RIP	0x0453
NetBIOS	0x0455
リモートコンソール	0x8104
名前付きパイプ	0x9100

フレームタイプ

IPX はさまざまなデータリンクプロトコル上で動作します。イーサネット上では、NetWare のバージョンによって 4 種類の異なるフレームタイプが使用されています。IPX VLAN を作成するときは、IPX アドレスに加え、どのフレームタイプを使用するかも指定します（表 12-2）。

表 12-2：IPX フレームタイプ

本製品での名称	説明
enet_ii	Ethernet Version 2 フレーム
enet_8023	IEEE 802.3 フレーム（LLC ヘッダなし）。NetWare 2 および NetWare 3.11 で使用。
enet_8022	IEEE 802.3 フレーム＋IEEE 802.2 LLC（Logical Link Control）ヘッダ。NetWare Version 3.12 および 4.x で使用。
enet_snap	IEEE 802.3 フレーム＋IEEE 802.2 LLC ＋ SNAP（Subnetwork Access Protocol）ヘッダ。

同一 VLAN 内では、すべての IPX ノードが同じフレームタイプを使用する必要があります。フレームタイプの異なるノード間で通信を行うには、フレームタイプごとに IPX VLAN を作成してルーティングを行います。

12.2 IPX VLAN の作成

IPX VLAN を作成するには、VLAN に IPX ネットワーク番号（NetID）とフレームタイプを割り当てます。すると、その VLAN は仮想的な IPX ルータインタフェースとなります。ネットワーク番号の異なる VLAN を複数作成すると、その時点で IPX ルーティングが自動的にイネーブルとなり、IPX VLAN 間の通信が可能になります。

VLAN に、IPX ネットワーク番号と IP アドレスの両方を同時に割り当てることはできません。また、1 つの VLAN で使用できるフレームタイプは 1 種類のみです。

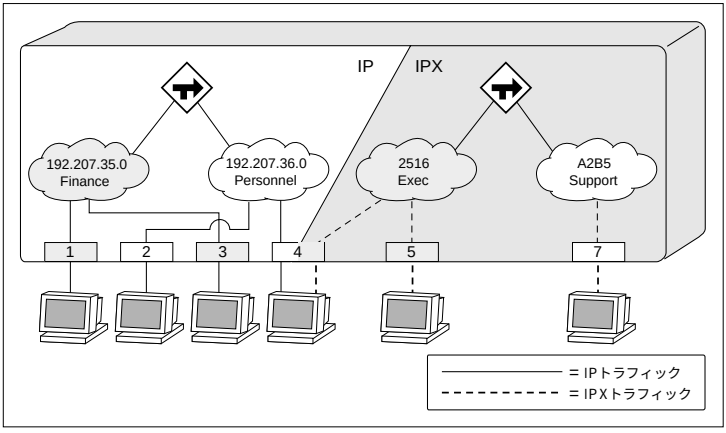
IPX VLAN を作成するには、次のコマンドを使います。

```
config vlan <name> xnetid <netid> [enet_ii | enet_8023 | enet_8022 |
enet_snap]
```

図 12-1 に IPX ルーティングの設定例を示します。この例では、2 つの IP VLAN（*Finance* と *Personnel*）に加えて、*Exec*（ネットワーク番号 2516）と *Support*（同 A2B5）という 2 つの IPX VLAN が作成されています。本製品のルーティング機能により、IP VLAN 間、および IPX VLAN 間ではそれぞれ通信が可能になっています。IP VLAN（*Finance* と *Personnel*）と IPX VLAN の間で通信することはできません。

VLAN 間の IPX トラフィックはネットワーク番号を元にルーティングされ、VLAN 内のトラフィックは MAC アドレスを元にワイヤスピードでスイッチングされます。

図 12-1：IPX VLAN



プロトコルVLAN の詳細については、第 5 章「バーチャル LAN(VLAN)」をご覧ください。

12.3 IPX/RIP ルーティング

ルーティングテーブル

IPX ルーティングは、ルーティングテーブル内の経路情報に基づいて行われます。ルーティングテーブル内のエントリは、情報のソースによって次のように大別できます。

スタティックルート

スタティックルートは、管理者が手動でルーティングテーブルに登録したルートエントリです。IPX のスタティックルートは 64 個まで登録できます。スタティックルートはエージアウトされません。また、IPX/RIP によって他のネットワークに広告されます。

ダイナミックルート

ダイナミックルートは、ルーティングプロトコルパケットの交換を通じて学習されたルートエントリです。IPX/RIP をサポートするルータは、ルーティングテーブルの情報を互いに交換しあいます。ダイナミックルーティングを使用する場合、ルーティングテーブルには到達可能な経路だけが保持されます。

一定の時間内に新しい情報が送られてこない場合、その経路情報はルーティングテーブルから削除（エージアウト）されます。

IPX/RIP

IPX/RIP（Routing Information Protocol）は、名前だけでなく概念的にも IP/RIP とよく似たディスタンスベクタ型のダイナミックルーティングプロトコルです。IPX/RIP に対応したルータやサーバは、ネットワーク番号、ホップ数、到達時間（チック =1/18 秒。LAN ではルータ－ルータ間が 1 チック）といった情報を定期的に交換し、最適な経路情報を保持します。また、クライアントからの要求に応じてルート情報を送信します。本製品では、IPX/RIP の機能のうち、次のものをサポートしています。

- スプリットホライズン
- ポイズンリバース
- トリガアップデート

ルーティングプロトコルの諸概念については、第 10 章を参考にしてください。

IPX/RIP は、VLAN に IPX ネットワーク番号を割り当てると自動的にイネーブルになります。IPX/RIP によるルート広告を行いたくない場合は、次のコマンドを使って IPX/RIP をディセーブルにします。

```
config ipxrip delete vlan [<name> | all]
```

スタティックルートを登録するには、次のコマンドを使います。

```
config ipxroute add [<dest_netid> | default] <nexthop_netid> <nexthop_nodeid>
<hops> <tics>
```

IPX/SAP

IPX ルータや NetWare サーバは、ネットワーク上のリソース（ファイルサーバやプリントサーバ）に関する情報を IPX サービステーブルに保持しています。この情報は、NetWare クライア

ントにサーバの名前やアドレスを教えるために使用されます。IPX/SAP（Service Advertisement Protocol）は、IPX ルータや NetWare サーバが互いにサービス情報を交換するためのプロトコルです。インターネットワーク上のルータおよびサーバは、定期的に SAP 広告パケットを他のルータに送信しあい、サービステーブルを構築します。SAP 広告パケットには次の情報が含まれます。

- サービスタイプ
- サービス名
- サーバのネットワーク番号
- サーバのノード番号

表 12-3：SAP サービスタイプの例

サービス	サービスタイプ
ファイルサーバ	0x0004
プリントサーバ	0x0007
アーカイブサーバ	0x0009

IPX サービステーブルに手動でエントリを追加するには、次のコマンドを使います。

```
config ipxservice add <service_type> <service_name> <netid> <nodeid> <socket>
<hops>
```

GNS（Get Nearest Server）

GNS（Get Nearest Server）リクエストは、IPX ノードが必要なサービスを探すときに送信するメッセージです。これに対し、サービス情報を持つサーバやルータは、サーバの名前やアドレスなどをクライアントに返答します。

本製品では、VLAN に IPX ネットワーク番号を割り当てた時点で、クライアントの GNS リクエストに応答する機能が自動的にイネーブルになります。

GNS リプライ機能をディセーブルにするには、次のコマンドを使用します。

```
disable ipxsap gns-reply {vlan <name>}
```

12.4 IPX の設定

ここでは、IPX、IPX/RIP、IPX/SAP の設定コマンドについて説明します。IPX ルーティングの設定手順は次のとおりです。

1 VLAN を 2 つ以上作成します。

同一ポート上に IPX VLAN と他の VLAN を重ね合わせる場合は、プロトコルフィルタか 802.1Q タグを使用します。

VLAN の設定方法については、第 5 章「バーチャル LAN（VLAN）」をご覧ください。

2 VLAN **に** IPX **ネットワーク番号を割り当て、フレームタイプを指定します。**

```
config vlan <name> xnetid <netid> [enet_ii | enet_8023 | enet_8022 |
enet_snap]
```

ネットワーク番号は VLAN **ごとに一意になるように設定します。また、フレームタイプが** VLAN **内で使用されているものと合致しているかどうか確認してください。同一** VLAN **内では、すべてのノードが同じフレームタイプを使用する必要があります。**

IPX VLAN **の設定が終わると、自動的に** IPX **ルーティングが有効になります。**IPX/RIP**、**IPX/SAP**、**GNS **リプライの各サービスも自動的に開始されます。**

設定確認コマンド

IPX **ルーティングの設定を確認するには、次のコマンドを使います。**

- `show vlan` **－** IPX **ネットワーク番号とフレームタイプを確認できます。**
- `show ipxconfig` **－** IPX/RIP**、**IPX/SAP**、**IPX **ルートシェアリング、**IPX **サービスシェアリングのイネーブル / ディセーブルなど、グローバルな** IPX **設定パラメータと** VLAN **ごとの** IPX **設定を確認できます。**
- `show ipxroute` **－** IPX **ルーティングテーブルを確認できます。**
- `show ipxsap` **－** IPX/SAP **のイネーブル / ディセーブル、**GNS **リプライ機能のイネーブル / ディセーブルなどを確認できます。**IPX/SAP Neighbor **の情報や** SAP **パケット統計、タイマー設定なども表示されます。**
- `show ipxrip` **－** IPX/RIP **のイネーブル / ディセーブル、**IPX/RIP Neighbor**、**RIP **パケット統計、タイマー設定などを確認できます。**
- `show ipxservice` **－** IPX **サービステーブルを確認できます。**

IPX フレームタイプに対応した定義済みプロトコルフィルタ

同一ポート上に IPX VLAN **と他の** VLAN **を共存させるには、**802.1Q **タグかプロトコルフィルタを** VLAN **に割り当てる必要があります。**

本製品にはIPX **の各フレームタイプに対応したプロトコルフィルタがあらかじめ**3 **種類定義されています。**IPX VLAN **の作成時には、これらの定義済みプロトコルフィルタを使うと便利です。**

ただし、IEEE 802.3（`enet_8023`）**形式のフレームをフィルタリングするプロトコル** VLAN **は仕様により作成できませんのでご注意ください。**802.3 **フレームを使用する** VLAN **が必要な場合**

は、ポートを共用する他の VLAN にプロトコルフィルタを割り当て、802.3 フレーム VLAN にはデフォルトのプロトコルフィルタ（any）を使用してください。

表 12-4：定義済みの IPX プロトコルフィルタと対応するフレームタイプ

フィルタ名	フィルタの定義内容	対応する IPX フレームタイプ
IPX	etype 8137	enet_ii
IPX_8022	llc e0e0	enet_8022
IPX_snap	snap 8137	enet_snap

12.5 IPX 設定コマンド

表 12-5 に IPX 設定コマンドの一覧を示します。

表 12-5：IPX 設定コマンド

コマンド名	機能
enable type20 forwarding {vlan <name>}	IPX Type 20 パケット（NetBIOS over IPX）の転送をイネーブルにします。デフォルトはディセーブルです。
config ipxmaxhops <number>	IPX パケット転送時の最大ホップ数を設定します。デフォルト値は 16 です。このパラメータは、NLSP（NetWare Link Services Protocol）を使用するとき以外変更しないでください。
config vlan <name> xnetid <netid> [enet_ii | enet_8023 | enet_8022 | enet_snap]	VLAN に IPX ネットワーク番号を割り当てます。また、VLAN 内で使用する IPX フレームタイプを指定します。
config ipxroute add [<dest_netid> | default] <nexthop_netid> <nexthop_nodeid> <hops> <tics>	IPX ルーティングテーブルにスタティックルートを追加します。以下のパラメータを指定します。 • <dest_netid> − 目的地のネットワーク番号。default はデフォルトルートを意味します。 • <nexthop_netid> − ネクストホップルータのネットワーク番号 • <nexthop_nodeid> − ネクストホップルータのノード番号（MAC アドレス） • <hops> − 目的地までのホップ数 • <tics> − 目的地までの到達時間（1 チック =1/18 秒）。LAN の場合はルータ−ルータ間が 1 と決められています。
config ipxroute delete [<dest_netid> | default] <nexthop_netid> <nexthop_nodeid>	IPX ルーティングテーブルからスタティックルートを削除します。

表 12-5：IPX 設定コマンド

コマンド名	機能
config ipxservice add <service_type> <service_name> <netid> <nodeid> <socket> <hops>	IPX サービステーブルにスタティックエントリを追加します。以下のパラメータを指定します。 • <service_type> ― SAP サービスタイプ • <service_name> ― サービス名 • <netid> ― サーバの IPX ネットワーク番号 • <nodeid> ― サーバのノード番号（MAC アドレス） • <socket> ― サーバのソケット番号 • <hops> ― サーバまでのホップ数（SAP ルーティングに使用）
config ipxservice delete <service_type> <service_name> <netid> <nodeid> <socket>	IPX サービステーブルからスタティックエントリを削除します。
xping {continuous} {size <n>} <netid> <nodeid>	IPX エコーパケットを使って IPX ノードへの到達性を調べます。デフォルトでは 4 個のパケットを送信しますが、continuous オプションを指定した場合は断続的にパケットを送信します。パケットサイズは 1 ～ 1484 バイトの範囲で指定します。デフォルトのパケットサイズは 256 バイトです。

表 12-6 に IPX ルーティングテーブル設定コマンドの一覧を示します。

表 12-6：IPX ルーティングテーブル設定コマンド

コマンド名	機能
enable ipxrip	IPX/RIP をイネーブルにします。デフォルトはイネーブルです。
config ipxrip add vlan [<name> | all]	指定した VLAN で IPX/RIP をイネーブルにします。IPX/VLAN 作成時のデフォルトはイネーブルです。
config ipxrip delete vlan [<name> | all]	指定した VLAN で IPX/RIP をディセーブルにします。
config ipxrip vlan [<name> | all] max-packet-size <number>	IPX/RIP の最大パケットサイズ（MTU）を設定します。デフォルトは 432 バイトです。
config ipxrip vlan [<name> | all] update-interval <time> {hold-multiplier <number>}	IPX/RIP パケットの送信間隔と経路情報のエージングタイムを設定します。デフォルトの送信間隔は 60 秒です。エージングタイムは、update-interval × hold-multiplier で求められます。hold-multiplier のデフォルト値は 3 です。
config ipxrip vlan [<name> | all] delay <msec>	個々の IPX/RIP パケットの送出間隔（パケット間ギャップ）を設定します。デフォルトは 55 ミリ秒です。

表 12-7 に IPX / SAP 設定コマンドの一覧を示します。

表 12-7：IPX/SAP 設定コマンド

コマンド名	機能
enable ipxsap	IPX/SAP をイネーブルにします。

表 12-7：IPX/SAP 設定コマンド

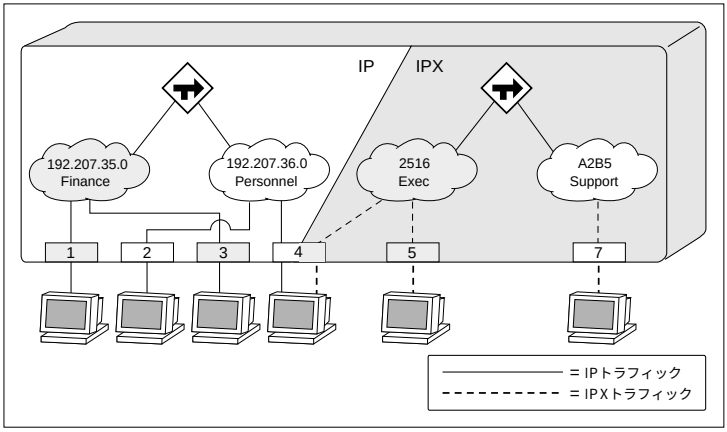
コマンド名	機能
enable ipxsap gns-reply {vlan <name>}	指定した VLAN で GNS リプライ機能をイネーブルにします。デフォルトはイネーブルです。
config ipxsap vlan [<name> | all] gns-delay <msec>	GNS リクエストに応答するまでの時間を設定します。デフォルトでは 0 ミリ秒、すなわち可能な限り直ちに応答します。
config ipxsap add vlan [<name> | all]	指定した VLAN で IPX/SAP をイネーブルにします。IPX VLAN 作成時のデフォルトはイネーブルです。
config ipxsap delete vlan [<name> | all]	指定した VLAN で IPX/SAP をディセーブルにします。
config ipxsap vlan [<name> | all] max-packet-size <number>	IPX/SAP の最大パケットサイズ（MTU）を設定します。デフォルトは 432 バイトです。
config ipxsap vlan [<name> | all] update-interval <time> {hold-multiplier <number>}	IPX/SAP パケットの送信間隔と経路情報のエージングタイムを設定します。デフォルトの送信間隔は 60 秒です。エージングタイムは、`update-interval` × `hold-multiplier` で求められます。`hold-multiplier` のデフォルト値は 3 です。なお、トリガアップデートが常に有効になっているため、情報に変更があった場合は次の送信時期を待たずに直ちにアップデートパケットが送信されます。
config ipxsap vlan [<name> | all] delay <msec>	個々の IPX/SAP パケットの送出間隔（パケット間ギャップ）を設定します。デフォルトは 55 ミリ秒です。

12.6 IPX ルーティングの設定例

図 12-2 **の例では、次に示す** 2 **つの** IPX VLAN **が定義されています。**

- *Exec*
  - IPX（IPX_8022）**ベースのプロトコル** VLAN
  - **所属ポートは** 4 **と** 5
  - IPX **ネットワーク番号は** 2516
  - **フレームタイプは** IEEE 802.2
- *Support*
  - **所属ポートは** 7
  - IPX **ネットワーク番号は** A2B5
  - **フレームタイプは** IEEE 802.2

図 12-2：IPX ルーティング設定例



各ノードは IP **と** IPX **の両プロトコルを使用しています。**IP **トラフィックは** IP **プロトコル** VLAN **の** *Finance* **と** *Personnel* **によってフィルタリングされ、**IPX **トラフィックは** IPX VLAN **によってフィルタリングされます。**

この例では、ポート 1 **と** 3 **に接続された機器からの** IP **トラフィックは、**VLAN *Finance* **を通じて** IP **ルータに到達します。また、ポート** 2 **と** 4 **に接続された機器から送信される** IP **トラフィックは、**VLAN *Personnel* **を通じて** IP **ルータに到達します。**

これと同様に、ポート 4 **と** 5 **からの** IPX **トラフィックは、**VLAN *Exec* **を通じて** IPX **ルータに到達します。また、ポート**7 **からの** IPX **トラフィックは、**VLAN *Support* **経由で** IPX **ルータに到達します。***Exec* **と** *Support* **はともに** IEEE 802.2 **フレームタイプを使用しています。**

IP VLAN と IPX VLAN の間で通信を行うことはできません。

図 12-2 **のネットワーク（**IPX VLAN **のみ）は、以下のようにして設定します。**

```
create vlan Exec
create vlan Support

config vlan Exec protocol ipx_8022

config vlan Exec add ports 4,5
config vlan Support add ports 7

config vlan Exec xnetid 2516 enet_8022
config vlan Support xnetid A2B5 enet_8022
```

12.7 IPX ルーティングの設定確認

IPX ルーティング関係の各種設定を確認するには、表 12-8 のコマンドを使用します。

表 12-8：IPX ルーティングの設定確認用コマンド

コマンド名	機能
show ipxconfig {vlan <name>}	指定した VLAN の IPX 設定を表示します。
show ipxroute {vlan <name> | xnetid <netid> | origin [static | rip | local]}	IPX ルーティングテーブルを表示します。
show ipxstats {vlan <name>}	IPX パケットの統計情報を表示します。
show ipxservice {vlan <name> | name <service_name> | type <service_type> | origin [static | ipxsap] }	IPX サービステーブルを表示します。
show ipxrip {vlan <name>}	指定した VLAN の IPX/RIP 設定と統計情報を表示します。
show ipxsap {vlan <name>}	指定した VLAN の IPX/SAP 設定と統計情報を表示します。

12.8 IPX ルーティングのディセーブルとリセット

IPX ルーティングの設定を出荷時の状態に戻したり、IPX ルーティング機能をディセーブルにするには、表 12-9 のコマンドを使用します。

表 12-9：IPX ルーティングのディセーブル/ リセット用コマンド

コマンド名	機能
disable type20 forwarding {vlan <name>}	IPX Type 20 パケットの転送をディセーブルにします。
disable ipxrip	IPX/RIP をディセーブルにします。
disable ipxsap	IPX/SAP をディセーブルにします。
disable ipxsap gns-reply {vlan <name>}	指定した VLAN で GNS リプライ機能をディセーブルにします。
unconfig vlan <name> xnetid	VLAN に割り当てた IPX ネットワーク番号を削除します。
unconfig ipxrip {vlan <name>}	指定した VLAN の IPX/RIP パラメータをデフォルト値に戻します。インポート/ エクスポートフィルタは削除され、最大パケットサイズ、RIP パケットの送信間隔、パケット間ギャップがリセットされます。

表 12-9：IPX ルーティングのディセーブル / リセット用コマンド

コマンド名	機能
unconfig ipxsap {vlan <name>}	指定した VLAN の IPX/SAP パラメータをデフォルト値に戻します。インポート / エクスポートフィルタは削除され、最大パケットサイズ、SAP パケットの送信間隔、パケット間ギャップがリセットされます。

13 ERRP

この章では、ルータの多重化を実現する ERRP（Enterprise Router Redundancy Protocol）の概要と設定方法について説明します。

13.1 概要

ERRP（Enterprise Router Redundancy Protocol）は、同一ネットワーク上で複数の C9100 / 8500 を連携させ、ルーティングサービスに冗長性を持たせるためのプロトコルです。

ERRP を実行している複数のルータは、IP アドレス（または IPX ネットワーク番号）と MAC アドレス（ERRP 用に予約された単一の MAC アドレス）を共有し、クライアントホストに対して 1 つのルータであるかのように見せかけます。通常は、1 台がマスタールータとして実際にルーティングとスイッチングを行い、それ以外のルータはスレーブルータとなって待機します。

ERRP ルータは定期的に ERRP Hello パケットを交換してマスタールータが稼働しているかどうかを調べており、マスタールータに障害が発生すると、スレーブルータが直ちに役割を引き継ぎます。切り替わりに要する時間は環境にもよりますが、通常 2 ～数 10 秒と非常に短時間です。

クライアントホスト側からはもともと 1 つのルータとしてしか認識されていないため、物理的にルータの入れ替わりがあったとしても、ホスト側には認識できません。ERRP ルータは IP アドレス（または IPX ネットワーク番号）を共有しているため、クライアントのデフォルトゲートウェイ設定を変更する必要はなく、また、ERRP ルータは MAC アドレスも共有しているため、クライアント側で ARP キャッシュを更新する必要もありません。

さらに、ERRP はレイヤー 2 レベルでの冗長性も提供します。こちらも 4 ～ 9 秒と STP よりはるかに高速な切り替えを実現しています。

このようにして、ERRP は IP および IPX ネットワークにおいて、冗長性のある信頼性の高いネットワークを構築します。

ERRP と STP を併用することはできません。

マスタールータとスレーブルータ

ERRP ルータは定期的に Hello パケットを送信して下記の情報を交換します。この情報を元に、VLAN 内で実際にルーティングおよびスイッチングを行うマスタールータを選出します。

1 **対象 VLAN におけるアクティブリンク数** － 対象 VLAN におけるアクティブな物理リンクの数が最も多いルータがマスタールータになります。リンク数が等しい場合は、次の条件を比較します。

2 **トラック対象 VLAN におけるアクティブリンク数** － 後述する VLAN トラッキング機能を有効にしている場合、監視対象の VLAN（Tracked VLAN）におけるアクティブリンクの数が最も多い VLAN がマスターに選出されます。監視対象 VLAN のアクティブリンク数が 0 になると、次に述べる ERRP プライオリティが自動的に 255（つねにスレーブ）になります。

3 **プライオリティ** － ERRP ルータには 0～255 の範囲で優先度を設定できます。数値が大きいほど優先度が高くなりますが、255 は特殊な値で常にスレーブになることを示します。デフォルトは 0 です。優先度も等しい場合は、最後の条件に進みます。

4 **MAC アドレス** － ERRP ルータの内部 MAC アドレス（ERRP ルータ間で共有する仮想的な MAC アドレスではないことに注意）を比較し、値の大きいほうがマスターになります。MAC アドレスが重複することはありえないので、ここで必ずマスターが決定します。

このようにして決定されたマスターおよびスレーブルータは次のような動作をします。

- **マスタールータ** － 対象 VLAN から他の VLAN へのトラフィックをルーティングし、また、対象 VLAN 内のトラフィックをスイッチングします。また、待機中のスレーブルータと ERRP Hello パケットを交換します。
- **スレーブルータ** － 対象 VLAN に対してはパケットの転送を行いません。RIP や OSPF を使用している場合、スタンバイ状態のルータインタフェースはダウンしているものと見なされます。またレイヤー 2 レベルでは、VLAN 内でのパケット転送を行いません。これによりループの形成を防ぎます。ただし、同一 VLAN 内の ERRP ルータとは Hello パケットを交換します。

VLAN トラッキング

VLAN トラッキングとは、ERRP ルータ切り替わりの条件として、ERRP を使用している VLAN とは別の VLAN を指定する機能です。たとえば、バックボーンに通じるアップリンク VLAN を監視対象（Tracked VLAN）に設定しておけば、マスタールータとアップリンク VLAN のリンクが切れると、マスタールータと ERRP の対象 VLAN のリンクが正常でも、スレーブへの切り替えが起こります。このとき、マスタールータのプライオリティは 255（常にスレーブ）となります。

新しいマスタールータの選出

Hello パケットで交換されるパラメータ（プライオリティやリンク数）に変更があるか、マスタールータとスレーブルータの通信が途絶えると、新しいマスタールータが選出されます。

パラメータ変化時は、通常 1 タイマーサイクル（ERRP Hello パケットの送信間隔。デフォルトでは 2 秒）以内に新しいマスタールータが選出されます。マスター / スレーブ間の通信断絶時は、通常 3 タイマーサイクル（デフォルトでは 6 秒）以内に選出が行われます。

障害復旧時間

障害発生時の復旧時間は、次の要素によって決まります。

- ERRP Hello パケットの送信間隔

- **使用するルーティングプロトコル。**RIP **よりも** OSPF **のほうが短時間で切り替わる**

ERRP Hello **パケットの送信間隔は** 1 **〜** 255 **秒の範囲で設定します。デフォルトでは** 2 **秒に設定されています。この場合の復旧時間は、障害の性格にもよりますが、通常** 5 **〜** 8 **秒です。**

ダイナミックルーティングを使用している場合は、該当するルーティングプロトコル（RIP V1/V2**、**OSPF**）の復旧時間が** ERRP **の復旧時間に加算されます。**

ERRP Awareness

ERRP **ルータの下位にレイヤー** 2 **の** C9100/8500 **スイッチを配置すると、さらに高速な冗長性を実現することができます。**ERRP **ディセーブルに設定された下位の** C9100/8500 **は、自分を通過する** ERRP Hello **パケットを常時監視しており、マスタールータに障害が発生すると自らのフォワーディングデータベース（**FDB**）をフラッシュしてスタンバイルータのエントリがすぐに登録されるようにします。これを** ERRP Aware **な状態といいます。**

ERRP **に対応していないスイッチを** ERRP **ルータの下位に接続した場合は、未対応スイッチの** FDB **エージングタイムの設定などにもよりますが、切り替わりに要する時間が長くなります。**

ERRP Aware **なスイッチと** ERRP **ルータを接続するポートには、**802.1Q VLAN **タグを設定しておく必要があります。**VLAN **が** 1 **つしかない場合はタグを使用しなくてもかまいませんが、その場合は同ポートに対して明示的にプロトコルフィルタを割り当てないようにしてください。プロトコル** VLAN **に属するタグなしポートを使って** ERRP Aware **なスイッチを** ERRP **ルータと接続すると、**ERRP **が正しく機能しません。なお、**ERRP **に対応していないスイッチ等を接続する場合は、タグを使用しなくても問題ありません。**

VLAN 設定の詳細については、第 5 章「バーチャル LAN（VLAN）」をご覧ください。

13.2 ERRP 設定の基本

ERRP **設定時の基本的事項をまとめます。**

- ERRP **は** VLAN **ごとに設定**
- ERRP **ルータは** 1VLAN **あたり** 4 **台まで**
- 1 **筐体あたり最大** 24 **個の** VLAN **で個別に** ERRP **を実行可能**
- **各** VLAN **で実際にルーティング / スイッチングを行うのはマスタールータだけ**
- **同一** VLAN **上の** ERRP **ルータには同じ** IP/IPX **アドレスを設定する**
- **同一** VLAN **上の** ERRP **ルータは同じ** MAC **アドレス（**ERRP **専用）を共有する**
- **同じ筐体をある** VLAN **ではマスターに、ある** VLAN **ではスレーブにすることができる**

OSPF と ERRP を併用するときは、各 ERRP ルータの OSPF ルータ ID が重複しないように手動で設定する必要があります。OSPF の設定については、第 10 章「ルーティングプロトコル」をご覧ください。

- ERRP ルータは、各 VLAN 内で ERRP Hello パケットを交換する
- ERRP Hello パケットの交換経路を複数作成するとよい
- ERRP を有効にするには、それぞれの筐体に同じ IP アドレスまたは IPX ネットワーク番号を割り当てる必要がある。VLAN 名は無視されるので異なっていてもよい
- それぞれの筐体で該当する VLAN の ERRP をイネーブルにする

VLAN *default* は ERRP をイネーブルにすることができません。

- ERRP VLAN に所属するポートで EDP（Enterprise Discovery Protocol）をイネーブルにする

  EDP の設定を確認するには次のコマンドを使います。デフォルトはイネーブルです。

  ```
  show edp
  ```

  EDP のイネーブル / ディセーブルを切り替えるには、次のコマンドを使います。

  ```
  [enable | disable] edp ports [<portlist> | all]
  ```

ERRP と IP マルチネット

ERRP と IP マルチネットを併用するときは、マスター選出に関わる各種パラメータ（リンクの数、プライオリティ、Hello タイマーなど）をすべての VLAN で同じにする必要があります。

有効なポートの組み合わせ

ERRP 使用時は、10/100M ポートの組み合わせに関して次のような制限があります。

ERRP VLAN に 10/100M ポートが含まれている場合、隣接する 8 つの物理ポートをすべて同じ VLAN に所属させる必要があります。

次に ERRP VLAN で有効な 10/100M ポートの組み合わせを示します。

図 13-1：C8518 における ERRP ポートの組み合わせ

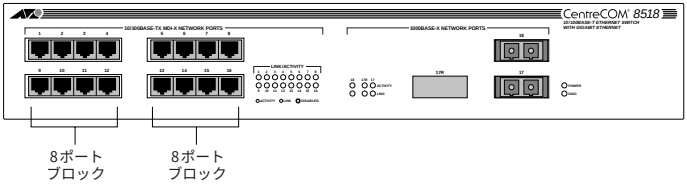


図 13-2：C8525 における ERRP ポートの組み合わせ

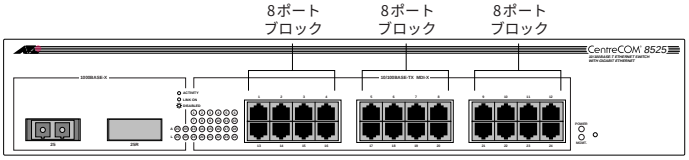
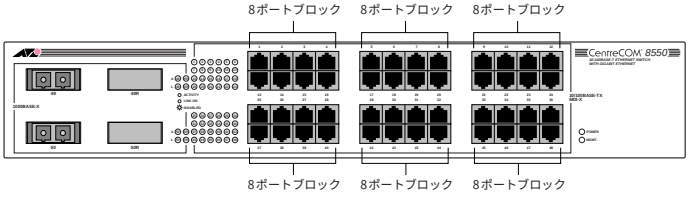


図 13-3：C8550 における ERRP ポートの組み合わせ



13.3 ERRP の設定

ERRP の設定は次の手順で行います。

1 通常どおり VLAN を作成します。

```
create vlan <name>
```

2 VLANにIP またはIPXアドレスを割り当てます。すべてのERRPルータに同じアドレスを割り当てます。

```
config vlan <name> ipaddress <ipaddress> {<mask>}
```
（IP の場合）

または

```
config vlan <name> xnetid <netid> [enet_ii | enet_8023 | enet_8022 |
enet_snap]
```
（IPX の場合）

3 VLAN にポートを割り当てます。

```
config vlan <name> add ports <portlist>
```

4 特定の VLAN へのリンク数を切り替わり条件としたい場合は、次のコマンドを使って監視対象の VLAN（Tracked VLAN）を指定します。

```
config vlan <name> [add | delete] track-vlan <tracked_vlan_name>
```

5 IP の場合、ユニキャストルーティングを有効にします（IPX の場合は、IPX アドレス割り当て時に自動的に有効になります）。

```
enable ipforwarding
```

6 ERRP をイネーブルにします。

```
enable esrp vlan <name>
```

ERRP 設定コマンドのキーワードは、ERRP ではなく ESRP です。間違えやすいのでご注意ください。

表 13-1 に ERRP 設定コマンドの一覧を示します。

表 13-1：ERRP 設定コマンド

コマンド名	機能
enable esrp vlan <name>	指定した VLAN で ERRP をイネーブルにします。
disable esrp {vlan <name> | all}	指定した VLAN で ERRP をディセーブルにします。
enable edp ports [<portlist> | all]	指定したポートで EDP をイネーブルにします。
disable edp ports [<portlist> | all]	指定したポートで EDP をディセーブルにします。
config vlan <name> esrp priority <value>	ERRP ルータのプライオリティを設定します。0 ～ 255 の範囲で指定します。デフォルトは 0 で値が大きいほど優先度が高くなります。ただし、255 を指定した場合は常にスレーブとなります。
config vlan <name> esrp timer <hello_timer>	ERRP Hello パケットの送信間隔を設定します。1 ～ 255 秒の範囲で指定します。デフォルトは 2 秒。特定の VLAN に対して冗長性を提供する ERRP ルータはすべて同じタイマー設定にする必要があります。
config vlan <name> add track-vlan <tracked_vlan_name>	マスター切り替わり条件の 1 つとして監視する VLAN（Tracked VLAN）を指定します。これにより、Tracked VLAN へのリンク数が切り替わり条件に加えられます。
config vlan <name> delete track-vlan <tracked_vlan_name>	Tracked VLAN の設定を取り消します。
show esrp {vlan <name>}	ERRP の設定情報を表示します。

設定例

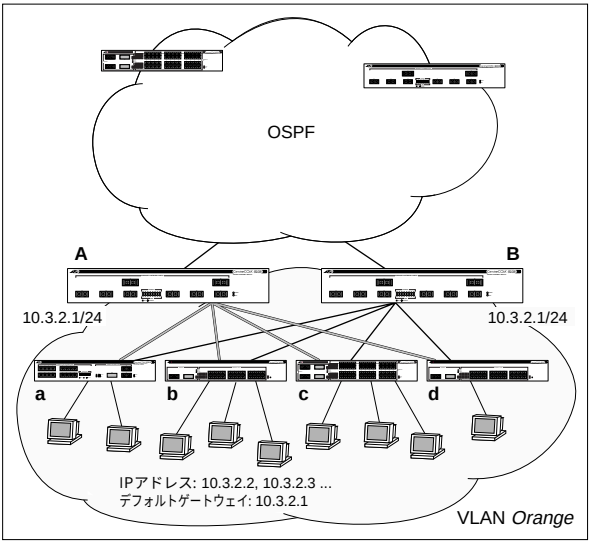
ここでは、ERRP の設定例を 3 つ紹介します。

1 つの VLAN に対するルータの多重化

図 13-4 の例では、VLAN *Orange* 内のトラフィックを 4 台の C8500（a ～ d）でスイッチングしています。さらに、それぞれの C8500 は VLAN 外部へのゲートウェイとなる 2 台の C9108（A と B）にデュアルホームで接続しています。2 台の C9108 は、4 台の C8500 に対して、スイッチングとルーティングのサービスを提供します。

C8500 は 2 台の C9108 に対して、それぞれ 1 つずつアクティブなポートを用いて接続しています。C9108 では、VLAN *Orange* 側のルータインタフェースに同じ IP アドレスが割り当てられ、ERRP がイネーブルに設定されています。また、2 台の C9108 は外部のネットワークとも接続されており、ここでは OSPF を用いてルーティング情報を発信 / 収集しています。

図 13-4：1つの VLAN に対するルータの多重化



2台の C9108 は互いに ERRP パケットを交換してどちらがマスターになるかを決定します。マスターになった C9108 は、VLAN *Orange* に対してスイッチングとルーティングのサービスを提供します。一方、スタンバイ状態（スレーブ）の C9108 は、VLAN *Orange* 側のインタフェースではまったくパケットの転送を行わず、これによりブリッジループを回避します。

この例では、2 台の C9108 を結ぶ経路が 4 本あります。このように設定することにより、ERRP ルータ間での Hello パケットの交換にも冗長性を持たせることができます。

ERRP Aware な C8500 スイッチは、C9108 の間で交換される ERRP Hello パケットを常に監視しており、マスタールータの障害発生を検知するとただちに自らの FDB をフラッシュして、新しいマスタールータのエントリがすぐに登録されるようにして障害復旧時間を短縮します。

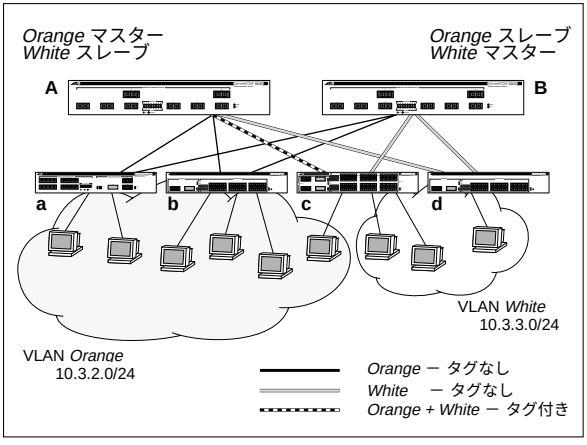
次に挙げる設定コマンド例は、2 台の C9108（A と B）に共通して用いられます。この例では、バックボーンで OSPF を使用しており、他の VLAN はすでに適切に設定されているものと仮定しています。

```
create vlan orange
config vlan orange ipaddress 10.3.2.1/24
config vlan orange add ports 1-4
enable ipforwarding
enable esrp vlan orange
config ospf add vlan orange
enable ospf
```

複数の VLAN に対するルータの多重化

図 13-5 は、2 つの VLAN *Orange* と *White* に対してルータの多重化を行う設定例です。

図 13-5：複数の VLAN に対するルータの多重化



この例は図 13-4 の例を元にしています。設定のポイントは次のとおりです。

- 下位の C8500 に VLAN *White* を追加
- VLAN *Orange* は 2 台の C9108 に対してそれぞれ 3 本ずつリンクを持つ
- VLAN *White* は 2 台の C9108 に対してそれぞれ 2 本ずつリンクを持つ
- 3 台目の C8550（c）と 1 台目の C9108（A）は、802.1Q タグを使用して VLAN *Orange* と VLAN *White* のトラフィックを同一ポート上に混在させている

- 2 台目の C9108（B）は、3 台目の C8550（c）に対して、VLAN *Orange* 用と VLAN *White* 用のポートを別々に持っている。

この例では、プライオリティの設定により、VLAN *Orange* は通常 1 台目の C9108（A）を使用し、VLAN *White* では 2 台目の C9108（B）を使用するようにしています。そのため、この例では 2 台の C9108 で設定内容が異なります。

1 台目の C9108（A）は次のようにして設定します。

```
create vlan orange
config vlan orange ipaddress 10.3.2.1/24
config vlan orange tag 10
config vlan orange add ports 1-2
config vlan orange add ports 3 tagged

create vlan white
config vlan white ipaddress 10.3.3.1/24
config vlan white tag 20
config vlan white add ports 4
config vlan white add ports 3 tagged

enable ipforwarding
enable esrp vlan orange
enable esrp vlan white
config vlan orange esrp priority 5
```

2 台目の C9108（B）は次のようにして設定します。

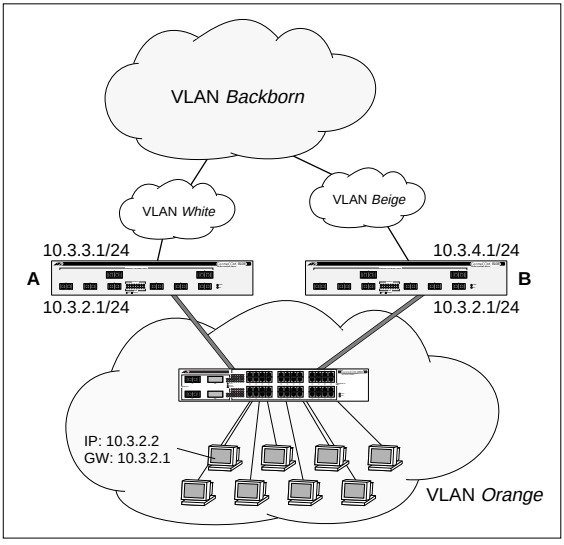
```
create vlan orange
config vlan orange ipaddress 10.3.2.1/24
config vlan orange add ports 1-3

create vlan white
config vlan white ipaddress 10.3.3.1/24
cnofig vlan white add ports 4-5

enable ipforwarding
enable esrp vlan orange
enable esrp vlan white
config vlan white esrp priority 5
```

VLAN トラッキング

図 13-6 **の例では、**2 **台の** C9108**（**A **と** B**）が** VLAN *Orange* **にリダンダントなルーティングサービスを提供しています。**C9108 **の配下にはレイヤー** 2 **スイッチの** C8550 **が配置され、**VLAN *Orange* **所属のクライアントホスト間でスイッチングを行っています。さらに、**VLAN *Backborn* **との通信が途切れないよう、**A **では** VLAN *White* **を、**B **では** VLAN *Beige* **を監視対象** VLAN **(**Tracked VLAN**）に指定し、それぞれ監視対象** VLAN **へのアクティブリンク数をルータ切り替えの条件としています。**

たとえば、A **がマスタールータになった場合、**ERRP **を実行している** VLAN *Orange* **内の通信が正常でも、監視対象** VLAN *White* **とのリンクが切れると、**A **の** ERRP **プライオリティが** 255**（常にスレーブ）となり、**B **がマスターになります。これにより、**VLAN *Beige* **経由で** VLAN *Backborn* **との通信が継続できます。**

図 13-6：VLAN トラッキングの設定例



スイッチ A **の設定は次のとおりです。**

```
create vlan orange
config vlan orange ipaddress 10.3.2.1/24
config vlan orange add ports 3

create vlan white
config vlan white ipaddress 10.3.3.1/24
config vlan white add ports 1

enable ipforwarding
enable esrp vlan orange

config ospf add vlan orange
config ospf add vlan white
enable ospf

config vlan orange add track-vlan white
```

スイッチ B **の設定は次のとおりです。**

```
create vlan orange
config vlan orange ipaddress 10.3.2.1/24
config vlan orange add ports 3

create vlan beige
config vlan beige ipaddress 10.3.4.1/24
config vlan beige add ports 1

enable ipforwarding
enable esrp vlan orange

config ospf add vlan orange
config ospf add vlan beige
enable ospf

config vlan orange add track-vlan beige
```

14 アクセスポリシー

この章では、アクセスポリシーの設定方法について説明します。

14.1 概要

アクセスポリシーとは、おもにセキュリティ上の観点から、ルーティング情報の広告および学習を制御するための機能です。セキュリティ管理というとトラフィックをフィルタリングする（本製品のブラックホール QoS プロファイルなど）ことがすぐに思い付きますが、アクセスポリシーでは保護したいサブネットへの経路を広告しないことでセキュリティを確保します。

アクセスポリシーは、アクセスプロファイル（IP アドレス、許可 / 拒否）をルーティングプロトコル（RIP、OSPF など）に適用することで作成します。アクセスポリシーには、大きくわけて次のような機能があります。

- **インポートフィルタ** ― 特定ルート情報の学習を許可 / 拒否します。
- **エクスポートフィルタ** ― 特定ルート情報の広告を許可 / 拒否します。
- **ゲートウェイフィルタ** ― 特定ルータからの情報を許可 / 拒否します。

14.2 アクセスポリシーの設定

アクセスの設定は、次の手順で行います。

1 アクセスプロファイルを作成する

2 アクセスプロファイルに IP アドレスを関連付ける

3 アクセスプロファイルのアクセスモード（許可 / 拒否）を指定する

4 アクセスプロファイルをルーティングプロトコルに適用する。

以下の各項では、それぞれの手順について詳しく説明します。

アクセスプロファイルの作成

アクセスプロファイルは、アクセス制御の対象となる IP アドレスとアクセスモード（その IP アドレスを許可するか、拒否するか）から構成されます。アクセスプロファイルの作成は次の手順で行います。

1 **アクセスプロファイルを作成します。**VLAN**、プロトコルフィルタ、**STPD **などと同じように、プロファイルには他と重複しないような名前を付けてください。**

```
create access-profile <access_profile> ipaddress
```

例

```
create access-profile nointernet ipaddress
```

2 **アクセスプロファイルに制御対象の** IP **アドレスを関連付けます。**

```
config access-profile <access_profile> [add | delete] ipaddress <ipad-
dress> <mask>
```

例

```
config access-profile nointernet add ipaddress 192.168.1.32 255.255.255.255
```

3 **アクセスモードを指定します。**

```
config access-profile <access_profile> mode [permit | deny]
```

- permit **ー指定した** IP **アドレスのみアクセスを許可します。**
- deny **ー指定した** IP **アドレスのアクセスを拒否します。**

permit モードに設定した場合、当該プロファイルに関連付けた IP アドレス以外はすべて拒否する設定になります。逆に、deny モードでは、指定した IP アドレス以外はすべて許可します。

アクセスプロファイルの適用

アクセスプロファイルを作成したら、これを任意のルーティングプロトコルに適用します。これによりアクセスポリシーが有効となり、指定したアクセス制御が行われます。

アクセスプロファイルの適用には、以下のルールがあります。

- **同じアクセスプロファイルを複数のプロトコル（および機能）に割り当てることができる。**
- 1 **つのプロトコルに割り当てられるプロファイルは** 1 **つだけ。**

アクセスプロファイルの適用方法はルーティングプロトコルごとに異なるため、以下個別に説明していきます。

RIP への適用

RIP **を使用している** VLAN **には、次に示す** 3 **種類のアクセスポリシーを適用できます。**

- **インポートフィルタ**

  アクセスプロファイルで指定した IP **アドレスに一致するルート情報を学習するか否かを設定します。後述するゲートウェイフィルタと組み合わせれば、信頼できる特定のルータから得た特定のルート情報だけを使用するような設定が可能です。**

```
config rip vlan [<name> | all] import-filter [<access_profile> | none]
```

- **エクスポートフィルタ**

  アクセスプロファイルで指定した IP **アドレスに一致するルート情報を広告するか否かを設定します。**

```
config rip vlan [<name> | all] export-filter [<access_profile> | none]
```

- **ゲートウェイフィルタ**

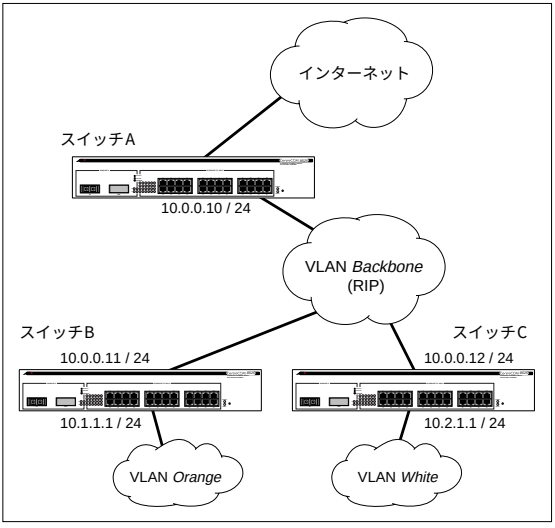
  アクセスプロファイルで指定した IP **アドレスを持つルータからの情報を信頼できるものとして受け入れるか否かを設定します。**

```
config rip vlan [<name> | all] trusted-gateway [<access_profile> | none]
```

設定例

図 14-1 **の例では、スイッチ** B **と** C **に** deny **モードのゲートウェイフィルタを適用することで、内部からインターネットへのアクセスを禁止しています。アクセスプロファイルで制御の対象となっているのは、内部ネットワークとインターネットを接続しているスイッチ** A **です。**

図 14-1：RIP アクセスポリシーの適用例



スイッチ B **と** C **の設定は次のとおりです。**

```
create access-profile nointernet ipaddress
config access-profile nointernet add ipaddress 10.0.0.10/32
config access-profile nointernet mode deny
config rip vlan backbone trusted-gateway nointernet
```

さらに、VLAN *Orange* から VLAN *White* へのアクセスを禁止するには、スイッチ B に次のアクセスポリシーを設定します。

```
create access-profile nowhite ipaddress
config access-profile nowhite add ipaddress 10.2.1.0/24
config access-profile nowhite mode deny
config rip vlan backbone import-filter nowhite
```

これにより、スイッチ B は VLAN *White* へのルート情報を持たなくなります。

OSPF への適用

OSPF を使用している VLAN には、次に示す 3 種類のアクセスポリシーを適用できます。OSPF はリンクステート型のルーティングプロトコルであるため、ディスタンスベクタ型の RIP とはアクセスポリシーの性格も異なります。OSPF には、すでにリンク認証機構や IP アドレスレンジなどアクセス制御のメカニズムがあるため、OSPF アクセスポリシーはこれらをさらに補強するものと考えられます。

- **エリア間（Interarea）フィルタ**

  アクセスプロファイルで指定した IP アドレスに一致するエリア間ルート情報をエリア内に広告するか否かを設定します。OSPF エリアに対して設定します。複数の OSPF エリアを設定している（ABR が存在する）場合に有効です。

  ```
  config ospf area <areaid> interarea-filter [<access_profile> | none]
  ```

- **外部ルート（External）フィルタ**

  アクセスプロファイルで指定した IP アドレスに一致する外部ルート情報をエリア内に広告するか否かを設定します。OSPF エリアに対して設定します。複数の OSPF エリアを設定している（ABR が存在する）場合に有効です。

  ```
  config ospf area <areaid> external-filter [<access-profile> | none]
  ```

フィルタ適用前にすでにエリア内に広告されていた外部ルートは、LSA がタイムアウトするまでルーティングテーブルに残ります。

- **ASBR フィルタ**

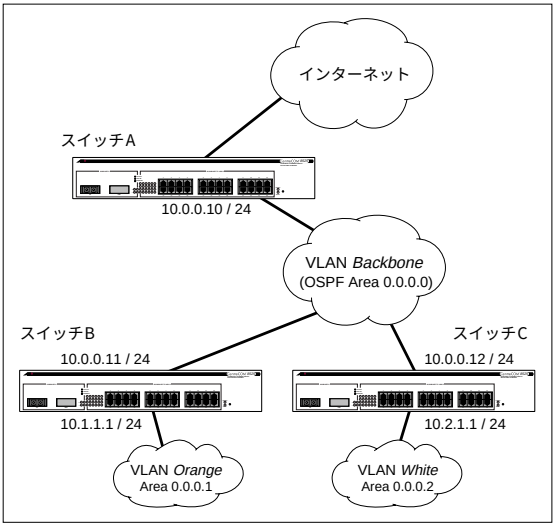
  アクセスプロファイルで指定した IP アドレスに一致する外部ルート情報を、OSPF ドメイン内に広告するか否かを設定します。筐体単位で設定します。OSPF Export（RIP ルートを OSPF ドメイン内に広告する機能）が設定されている場合に有効です。

  ```
  config ospf asbr-filter [<access_profile> | none]
  ```

設定例

図 14-2 の例では、内部の OSPF ネットワークとインターネットを接続している AS 外部ルータ、スイッチ A に deny モードの ASBR フィルタを適用することで、インターネット上の特定アドレスへのアクセスを制限しています。

図 14-2：OSPF アクセスポリシーの設定例



ASBR **であるスイッチ** A **の設定は次のとおりです。**

```
create access-profile nointernet ipaddress
config access-profile nointernet add ipaddress 123.45.67.0/24
config access-profile nointernet mode deny
config ospf asbr-filter nointernet
```

DVMRP への適用

マルチキャストルーティングプロトコルの DVMRP **には、**RIP **とほぼ同様のアクセスポリシーを適用できます。**

- **インポートフィルタ**

  アクセスプロファイルで指定した IP **アドレスに一致する** DVMRP **ルート情報を学習するか否かを設定します。**

  ```
  config dvmrp vlan [<name> | all] import-filter [<access_profile> | none]
  ```

- **エクスポートフィルタ**

  アクセスプロファイルで指定した IP **アドレスに一致する** DVMRP **ルート情報を広告するか否かを設定します。**

  ```
  config dvmrp vlan [<name> | all] export-filter [<access_profile> | none]
  ```

- **ゲートウェイフィルタ**

アクセスプロファイルで指定した IP アドレスを持つ DVMRP ルータからの情報を信頼できるものとして受け入れるか否かを設定します。

```
config dvmrp vlan [<name> | all] trusted-gateway [<access_profile> |
none]
```

設定例

ここでは、図 14-1 のネットワークで DVMRP を使用しているものと仮定します。この例では、スイッチ B に deny モードのゲートウェイフィルタを適用することで、VLAN *Orange* のユーザがインターネット上のマルチキャストトラフィックにアクセスできないようにしています。アクセスプロファイルで制御の対象となっているのは、内部ネットワークとインターネットを接続しているマルチキャストルータ、スイッチ A です。

スイッチ B の設定は次のとおりです。

```
create access-profile nointernet ipaddress
config access-profile nointernet add ipaddress 10.0.0.10/32
config access-profile nointernet mode deny
config dvmrp vlan backbone trusted-gateway nointernet
```

さらに、VLAN *Orange* のユーザが VLAN *White* をソースとするマルチキャストトラフィックにアクセスできないようにするには、スイッチ B に次のアクセスポリシーを設定します。

```
create access-profile nowhite ipaddress
config access-profile nowhite add ipaddress 10.2.1.0/24
config access-profile mode deny
config dvmrp vlan backbone import-filter nowhite
```

PIM-DM への適用

マルチキャストルーティングプロトコルの PIM-DM には、次のアクセスポリシーを適用できます。PIM-DM は、マルチキャスト専用のルーティングテーブルを持たずに通常のユニキャストルーティングテーブルを利用するため、ルート情報の制御はおもにユニキャストルーティングプロトコルで行います。

- **ゲートウェイフィルタ**

  アクセスプロファイルで指定した IP アドレスを持つ PIM-DM ルータからの情報を信頼できるものとして受け入れるか否かを設定します。

  ```
  config pim-dm vlan [<name> | all] trusted-gateway [<access_profile> |
  none]
  ```

設定例

ここでも、図 14-1 のネットワークが PIM-DM を使用できるように設定されているものと仮定します。この例では、スイッチ B に deny モードのゲートウェイフィルタを適用することで、VLAN *Orange* のユーザがインターネット上のマルチキャストトラフィックにアクセスできないようにしています。アクセスプロファイルで制御の対象となっているのは、内部ネットワークとインターネットを接続しているスイッチ A です。

スイッチ B の設定は次のとおりです。

```
create access-profile nointernet ipaddress
config access-profile nointernet add ipaddress 10.0.0.10/32
config access-profile nointernet mode deny
config pim-dm vlan backbone trusted-gateway nointernet
```

アクセスプロファイルの変更

アクセスプロファイルは、プロトコルへの適用後であっても修正が可能です。ただし、変更が行き届くまでにはある程度の時間が必要となります。RIP、DVMRP、PIM-DM の場合は、エージングタイムの設定によって必要な時間が決まります。OSPF の場合は、スイッチを再起動するか、OSPF をいったんディセーブルにしてから再度イネーブルにする必要があります。

アクセスポリシーの削除

アクセスポリシーを削除するには、プロトコルからアクセスプロファイルの適用を解除します。アクセスプロファイルの削除は、アクセスポリシーの適用に使ったコマンドで none キーワードを指定することによって行います。

14.3 アクセスポリシー設定コマンド

表 14-1 に、アクセスポリシー設定コマンドの一覧を示します。

表 14-1：アクセスポリシー設定コマンド

コマンド名	機能
create access-profile <access_profile> ipaddress	アクセスプロファイルを作成します。作成したプロファイルには複数の IP アドレスを関連付けて許可 / 拒否モードを設定し、ルーティングプロトコルに適用できます。
config access-profile <access_profile> mode [permit | deny]	アクセスプロファイルのアクセスモードを設定します。 • permit － 指定した IP アドレスのみアクセスを許可します。 • deny － 指定した IP アドレスのアクセスを拒否します。 デフォルトは permit です。
config access-profile <access_profile> add ipaddress <ipaddress> <mask>	アクセスプロファイルに IP アドレスを追加します。
config access-profile <access_profile> delete ipaddress <ipaddress> <mask>	アクセスプロファイルから IP アドレスを削除します。
config rip vlan [<name> | all] trusted-gateway [<access_profile> | none]	RIP VLAN にゲートウェイフィルタを適用し、特定のルータからの情報を受け入れるか否かを設定します。

表 14-1：アクセスポリシー設定コマンド

コマンド名	機能
config rip vlan [<name> | all] import-filter [<access_profile> | none]	RIP VLAN にインポートフィルタを適用し、特定のルート情報を受け入れるか拒否するかを設定します。
config rip vlan [<name> | all] export-filter [<access_profile> | none]	RIP VLAN にエクスポートフィルタを適用し、特定のルート情報を広告するか否かを設定します。
config ospf area <areaid> interarea-filter [<access_profile> | none]	OSPF エリアにエリア間ルートフィルタを適用し、特定のエリア間ルート情報をエリア内に広告するか否かを設定します。
config ospf area <areaid> external-filter [<access_profile> | none]	OSPF エリアに外部ルートフィルタを適用し、特定の外部ルート情報をエリア内に広告するか否かを設定します。
config ospf asbr-filter [<access_profile> | none]	ASBR フィルタを適用し、特定の外部ルート情報を OSPF ドメイン内に広告するか否かを設定します。
config dvmrp vlan [<name> | all] trusted-gateway [<access_profile> | none]	DVMRP VLAN にゲートウェイフィルタを適用し、特定のルータからの情報を受け入れるか否かを設定します。
config dvmrp vlan [<name> | all] import-filter [<access_profile> | none]	DVMRP VLAN にインポートフィルタを適用し、特定のルート情報を受け入れるか拒否するかを設定します。
config dvmrp vlan [<name> | all] export-filter [<access_profile> | none]	DVMRP VLAN にエクスポートフィルタを適用し、特定のルート情報を広告するか否かを設定します。
config pim-dm vlan [<name> | all] trusted-gateway [<access_profile> | none]	PIM-DM VLAN にゲートウェイフィルタを適用し、特定のルータからの情報を受け入れるか否かを設定します。
delete access-profile <access_profile>	アクセスプロファイルを削除します。
show access-profile {<access_profile>}	アクセスプロファイルの情報を表示します。

15 ステータス表示と統計機能

この章では、ステータス表示コマンド、ポート統計機能、ログ情報、RMON 機能の使用方法について説明します。

15.1 ステータス表示コマンド

本製品には、スイッチの動作状態や設定を表示するさまざまな'show' コマンドが用意されています。これらのコマンドが出力する情報は、障害発生時の原因究明にも役立ちます。

表 15-1 に、show コマンドの一覧を示します。

表 15-1：ステータス表示コマンド

コマンド名	機能
show access-profile {<access_profile>}	アクセスプロファイルの情報を表示します。
show accounts	ユーザデータベース内の情報を表示します。アカウント名、アクセスレベル、ログイン成功回数と失敗回数、アクティブセッション数を表示します。このコマンドを実行するには、管理者の権限が必要です。
show banner	ユーザ定義のバナーを表示します。
show configuration	現在の設定を表示します。端末側の機能を使えば、表示された設定をファイルに保存することもできます。
show diagnostics	ソフトウェアの自己診断結果を表示します。
show dns-client	DNS クライアント機能の設定情報を表示します。
show dvmrp {vlan <name> | route {detail} }	DVMRP の設定および統計、あるいはユニキャストルーティングテーブルを表示します。オプションを指定しなかった場合は、すべての情報が表示されます。
show esrp {vlan <name>}	ERRP の設定情報を表示します。
show fdb {<mac_address> | vlan <name> | ports <portlist> | permanent}	スイッチフォワーディングデータベース（FDB）の内容を表示します。MAC アドレス、VLAN 名と VLANid、ポート、エントリの種類などが表示されます。オプションを指定することにより、条件に合致する情報だけを表示させることができます。VLAN 名を指定した場合は、その VLAN の全エントリが表示されます。特定のエントリだけを表示させるには、MAC アドレスを指定します。
show gvrp	GVRP の設定とステータスを表示します。

表 15-1：ステータス表示コマンド

コマンド名	機能
show igmp snooping {vlan <name>}	IGMP スヌーピングの登録情報と、IGMP タイマーおよびステータスの要約情報を表示します。
show iparp {<ipaddress> | vlan <name> | permanent}	ARP テーブルを表示します。IP アドレス、VLAN、パーマネントエントリ単位で表示項目のフィルタリングが可能です。
show iparp proxy {<ipaddress> <mask>}	Proxy ARP テーブルを表示します。
show ipconfig {vlan <name>}	指定した VLAN の IP 設定内容を表示します。以下の情報が表示されます。 • IP アドレスとサブネットマスク • IP ルーティング情報 • BOOTP 設定 • VLAN 名と VLANid • ICMP 設定（グローバル） • IGMP 設定（グローバル） • IRDP 設定（グローバル）
show ipfdb {<ipaddress> {<mask>} | vlan <name>}	IP フォワーディングデータベースを表示します。
show ipmc cache {detail} {<group> {<src_ipaddress> <mask>} | all}	IP マルチキャストルーティングテーブルを表示します。以下の情報が表示されます。 • マルチキャストグループアドレス • 送信元 IP アドレスとネットマスクおよび VLAN • ルーティングプロトコル • ルーティングの状態
show ipqos {<dest_ipaddress> <mask> | all}	IP QoS テーブルを表示します。
show iproute {priority | vlan <name> | permanent | <ipaddress> <mask>}	IP ルーティングテーブルを表示します。
show ipstats {vlan <name>}	CPU が処理したパケットの統計を表示します。以下の情報が表示されます。 • 受信パケット数、送信パケット数 • ICMP/IGMP 統計 • IRDP 統計 • VLAN ごとの送受信パケット数
show ipxconfig {vlan <name>}	指定した VLAN の IPX 設定を表示します。
show ipxroute {vlan <name> | xnetid <netid> | origin [static | rip | local]}	IPX ルーティングテーブルを表示します。
show ipxstats {vlan <name>}	IPX パケットの統計情報を表示します。

表 15-1：ステータス表示コマンド

コマンド名	機能
show ipxservice {vlan <name> | name <service_name> | type <service_type> | origin [static | ipxsap] }	IPX サービステーブルを表示します。
show ipxrip {vlan <name>}	指定した VLAN の IPX/RIP 設定と統計情報を表示します。
show ipxsap {vlan <name>}	定した VLAN の IPX/SAP 設定と統計情報を表示します。
show log {<priority>}	現時点におけるログのスナップショットを表示します。以下のフィルタリングオプションを指定できます。 • `priority` — ここで指定したレベル以上のメッセージだけを表示します。`priority` には、critical、emergency、error、alert、warning、notice、info、debug のいずれかを指定します。デフォルトは info です。
show log configuration	ログ設定を表示します。syslog ホストの IP アドレス、ローカルログに記録するメッセージのレベル、syslog ホストに送信されるメッセージのレベルなどが表示されます。
show management	ネットワーク管理の設定と統計を表示します。Telnet と SNMP のイネーブル/ ディセーブル、SNMP コミュニティ名、登録済み SNMP 管理ステーションとトラップレシーバの一覧、ログイン統計、RMON 設定などが表示されます。
show memory	現在のシステムメモリ情報を表示します。
show mirroring	ポートミラーリング機能の設定を表示します。
show ospf	グローバルな OSPF 情報を表示します。
show ospf area {<areaid>}	指定したエリアの OSPF 情報を表示します。
show ospf interfaces {vlan <name> | area <areaid>}	指定した VLAN またはエリアの OSPF 情報を表示します。オプションを省略した場合は、すべての VLAN の情報が表示されます。
show ospf lsdb {detail} area [<areaid> | all] [router | network | summary-net | summary-asb | as-external | external-type7 | all]	リンクステートデータベースの内容を表示します。detail オプションを指定すると、エントリごとにすべての LSA 情報が表示されます。
show ospf virtual-link {routerid <routerid> <areaid> | all}	指定したルータのバーチャルリンク情報を表示します。
show pim-dm {vlan <name>}	PIM-DM の設定および統計情報を表示します。
show ports {<portlist>} collisions	コリジョン統計をリアルタイムに表示します。

表 15-1：ステータス表示コマンド

コマンド名	機能
show ports {<portlist>} configuration	以下に示すポートの設定内容を表示します。 • ポートの状態 • リンクの状態 • オートネゴシエーションの状態 • 通信速度 • 通信モード • フロー制御 • ロードシェアリング情報 • リンクメディア情報
show ports {<portlist>} info	ポートに関する詳細な情報を表示します。以下の情報が表示されます。 • ポートの状態 • リンクの状態 • オートネゴシエーションの状態 • 通信速度 • 通信モード • STP 情報 • リダンダントポートの状態 • ロードシェアリング情報 • VLAN 情報 • QoS 情報
show ports {<portlist>} packet	パケットの分布情報をリアルタイムに表示します。
show ports {<portlist>} qosmonitor	QoS に関する統計情報をリアルタイムに表示します。
show ports {<portlist>} rxerrors	受信エラー統計をリアルタイムに表示します。
show ports {<portlist>} stats	ポート統計をリアルタイムに表示します。
show ports {<portlist>} txerrors	送信エラー統計をリアルタイムに表示します。
show ports {<portlist>} utilization	ポートの使用状況をリアルタイムに表示します。「Space」キーを使って、パケット、バイト、帯域使用状況の表示を切り替えます。
show protocol {<protocol_name>}	プロトコル情報を表示します。表示されるのは、プロトコル名、プロトコルフィールド、そのプロトコルを使用している VLAN です。
show qosprofile {<qosname>}	QoS プロファイル情報を表示します。表示される情報は、QoS プロファイル名、最小帯域幅、最大帯域幅、優先度です。QoS プロファイルが割り当てられたトラフィックグループも表示されます。
show radius	RADIUS クライアントの設定を表示します。
show rip {vlan <name>}	指定した VLAN の RIP 設定と統計を表示します。

表 15-1：ステータス表示コマンド

コマンド名	機能
show rip stats {vlan <name>}	RIP 関連の統計情報を表示します。ルータインタフェースごとに以下の情報が表示されます。 • 送信パケット数 • 受信パケット数 • エラーパケット数 • エラー経路数 • RIP の peer 情報
show session	現在開かれている Telnet セッションとコンソールセッションを表示します。ユーザ名、Telnet クライアントの IP アドレス、コンソールセッションのアクティブ / 非アクティブ、ログイン時間が表示されます。各セッションは、番号で識別されます。
show sntp-client	SNTP クライアント機能の設定と統計情報を表示します。
show stpd {<stpd_name>}	指定した STPD の STP 情報を表示します。
show stpd <stpd_name> ports [<portlist> | all]	指定したポートの STP 設定を表示します。
show switch	以下に示す本製品のシステム情報を表示します。 • sysName、sysLocation、sysContact 各変数 • MAC アドレス • 現在時刻とシステムの稼働時間 • 動作環境（温度、ファンの状態、電源の状態） • NVRAM 内のファームウェアに関する情報（primary/secondary、日付、時刻、サイズ、バージョン） • NVRAM 内の設定情報（primary/secondary、日付、時刻、サイズ、バージョン） • 再起動スケジュール情報 • 802.1p 情報
show udp-profile {<profile_name>}	UDP フォワーディングプロファイルに関する情報を表示します。以下の情報が表示されます。 • プロファイル名 • 対象 UDP ポート • 転送先 • プロファイルの割り当て先
show version	ハードウェアとファームウェアのバージョン、およびスイッチのシリアル番号を表示します。
show vlan {<name>}	VLAN 情報を表示します。VLAN 名を指定しなかった場合は、VLAN 名の一覧と、各 VLAN に所属するポートなどの情報が表示されます。VLAN 名を指定した場合は、その VLAN に所属するポート情報（IP アドレスやタグ情報）が表示されます。

15.2 ポート統計機能

本製品には、ポートの統計情報を表示する機能が備わっています。この機能では、約2秒ごとにポートごとの最新統計値が表示されます。統計値の有効桁数は9桁です。

ポート統計を表示するには、次のコマンドを使用します。

```
show ports {<portlist>} stats
```

表示される情報は、以下のとおりです。

- Link Status ― ポートのリンク状態を示します。
  - READY ― リンク可能
  - ACTIVE ― リンク確立
- Transmit Packet Count (Tx Pkt Count) ― 正常に送信されたパケットの数
- Transmit Byte Count (Tx Byte Count) ― 正常に送信されたバイト数
- Receive Packet Count (Rx Pkt Count) ― 受信した正常なパケットの数
- Receive Byte Count (Rx Byte Count) ― 受信バイト数（エラーフレームや失われたフレームを含みます）。バイト数には、FCS（Frame Check Sequence）が含まれますが、プリアンブルは含まれません。
- Received Broadcast (Rx Bcast) ― 受信したブロードキャストフレームの数
- Received Multicast (Rx Mcast) ― 受信したマルチキャストフレームの数

15.3 ポートエラー統計

本製品では、ポートごとのエラー統計を追跡することができます。

送信エラーの統計を表示するには、次のコマンドを使います。

```
show ports {<portlist>} txerrors
```

表示されるエラー情報は、以下のとおりです。

- Link Status ― ポートのリンク状態を示します。
  - READY ― リンク可能
  - ACTIVE ― リンク確立
- Transmit Collisions (Tx Coll) ― 該当するポートで検出されたコリジョンの合計数（ポートに接続された機器がコリジョンの発生源とは限りません）
- Transmit Late Collisions (Tx Late Coll) ― ポートの送信ウィンドウがタイムアウトした後に発生したコリジョンの合計数

- **Transmit Deferred Frames (Tx Deferred) ― 最初の送信要求が他のトラフィックによって延期された後に送信されたフレームの合計数**
- **Transmit Errored Frames (Tx Error) ― ネットワークエラー（**late collision **や** excessive collision **など）により、送信が完了できなかったフレームの数**
- **Transmit Parity Errored Frames (Tx Parity) ― 送信時にパリティエラーが発生したフレームの数**

受信エラーの統計を表示するには、次のコマンドを使います。

```
show ports {<portlist>} rxerrors
```

表示される情報は、以下のとおりです。

- **Receive Bad CRC Frames (Rx CRC) ―** CRC **エラーフレーム数。フレーム長は正しいが、**FCS **の値が正しくなかったもの。**
- **Receive Oversize Frames (Rx Over) ― フレーム長が** 1522 **バイトを上回っているフレームの数。フレームデータ自体は正常。**
- **Receive Undersize Frames (Rx Under) ―** 64 **バイト未満のフレームの数。**
- **Receive Fragment Frames (Rx Frag) ― フレーム長**64**バイト未満の**CRC**エラーフレームの数。**
- **Receive Jabber Frames (Rx Jabber) ― フレーム長が** 1522 **バイトを上回っている** CRC **エラーフレームの数。**
- **Receive Alignment Errors (Rx Align) ― フレーム長がオクテットの整数倍にならず、**CRC **エラーが発生したフレームの数**
- **Receive Frames Lost (Rx Lost) ― バッファオーバーフローにより失われたフレームの数**

15.4 show ports コマンドの表示切り替えキー

表 15-2 **に** show ports **コマンドの表示画面切り替えに使うキーの一覧を示します。**

表 15-2：show ports コマンドの表示切り替えキー

キー	機能
「U」	前ページに戻る
「D」	次ページに進む
「Esc」「Return」	コマンドの終了
「0」	全カウンタのクリア

表 15-2：show ports コマンドの表示切り替えキー

キー	機能
「Space」	表示単位を切り替える。 • パケット / 秒 • バイト / 秒 • 帯域幅（%） show ports utilization コマンドでのみ使用可

15.5 ログ機能

ログには、スイッチに関するすべての設定情報と障害情報が記録されます。ログの各エントリは、以下の情報から構成されます。

- タイムスタンプ ― イベントの発生日時が記録されます。時刻は HH:MM:SS の形式です。ユーザイベントの場合は、ユーザ名も記録されます。
- レベル ― イベントの重要度です。ログレベルは次のとおりです（重要度の高い順）。
  - Critical
  - Emergency
  - Error
  - Alert
  - Warning
  - Notice
  - Info
  - Debug
- サブシステム ― 本製品のどの機能に関係するイベントであるかを示します。表 15-3 にサブシステムの一覧を示します。

表 15-3：サブシステム一覧

サブシステム	説明
Syst	システム全般（メモリ、電源、セキュリティ違反、ファン故障、オーバーヒート状態、設定モードなど）の情報を示します。
STP	STP 関連の情報（STP 状態の変化など）を示します。
Brdg	ブリッジ機能関連の情報（FDB テーブルの空き容量不足、キューのオーバーフローなど）を示します。
SNMP	SNMP 関連の情報（コミュニティ名違反など）を示します。
Telnet	Telnet ログインの情報や、Telnet による設定変更などの情報を示します。

表 15-3：サブシステム一覧

サブシステム	説明
Port	ポート情報（ポート統計やエラー統計など）を示します。

- メッセージ ― イベントに関する情報をテキストで記録します。

ローカルログ

ローカルログには 1000 件のメッセージを記録できます。現時点におけるログのスナップショットを表示するには、次のコマンドを使います。

```
show log {<priority>}
```

priority には、ログレベルを指定します。表示されるのは、ここで指定したレベル以上のエントリだけです。critical、emergency、error、alert、warning、notice、info、debug のいずれかを指定してください。デフォルトは、info です。

ログのリアルタイム表示

ログのスナップショットだけでなく、リアルタイムにログを表示させることもできます。リアルタイムのログ表示をオンにするには、次のコマンドを実行します。

```
enable log display
```

表示内容の設定は、次のコマンドで行います。

```
config log display {<priority>}
```

priority のデフォルトは info です。

コンソールセッションでリアルタイムログ表示をイネーブルにした場合は、明示的にディセーブルにしない限り、コンソールセッションの終了後も設定が保持されます。

Telnet でリアルタイムログ表示をイネーブルにした場合は、セッションを終了する（タイムアウトなど）と同時にログ表示機能もディセーブルになります。次回の Telnet ログイン時には、もういちど enable log display コマンドを実行しなくてはなりません。

リモートログ

本製品では、ローカルログに加え、UNIX の syslog デーモンを利用したリモートロギングもサポートしています。リモートログを有効にするには、以下の手順にしたがいます。

1 本製品のログメッセージを受信・記録する syslog ホスト側の設定を行います。

2 本製品側で、次のコマンドを実行します。

```
enable syslog
```

3 次のコマンドで、リモートログの設定を行います。

```
config syslog <ipaddress> <facility> {<priority>}
```

指定するパラメータは以下のとおりです。

- `ipaddress` ー syslog **ホストの** IP **アドレス**
- `facility` ー syslog **の** local facility level。local0 ～ local7 **を使用できます。**
- `priority` ー **ここで指定したレベル以上のエントリだけを** syslog **ホストに送信します。** critical、emergency、error、alert、warning、notice、info、debug **のいずれかを指定します。デフォルトでは、**critical **レベルのメッセージだけが** syslog **ホストに送信されます。**

syslog 機能の詳細については、ご使用の UNIX 環境のマニュアル等を参考にしてください。

設定変更ログ機能

この機能を有効にすると、CLI**（コンソールまたは** Telnet**）から設定の変更が行われた場合に、変更時刻、変更内容、ユーザ名、**Telnet **クライアントの** IP **アドレスなどがログに記録されます。設定変更ログを有効にするには、次のコマンドを使います。**

```
[enable | disable] cli-config-logging
```

ログ関連コマンド

表 15-4 **にログ関連コマンドの一覧を示します。**

表 15-4：ログ関連コマンド

コマンド名	機能
config log display {<priority>}	**リアルタイムログ表示機能の設定を行います。以下のオプションを指定できます。** • `priority` ー **ここで指定したレベル以上のメッセージだけを表示します。**critical、emergency、error、alert、warning、notice、info、debug **のいずれかを指定します。デフォルトは** info **です。**
config syslog <ipaddress> <facility> {<priority>}	**syslog を利用したリモートロギングに必要な設定を行います。** • `ipaddress` ー **syslog ホストの IP アドレス** • `facility` ー **syslog の** local facility level • `priority` ー **ここで指定したレベル以上のメッセージだけを syslog ホストに送信します。**critical、emergency、error、alert、warning、notice、info、debug **のいずれかを指定します。デフォルトでは、**critical **レベルのメッセージのみが syslog ホストに送信されます。**
enable log display	**リアルタイムログ表示をイネーブルにします。**
enable syslog	**syslog ホストへのリモートロギングをイネーブルにします。**
disable log display	**リアルタイムログ表示をディセーブルにします。**
disable syslog	**syslog ホストへのリモートロギングをディセーブルにします。**

表 15-4：ログ関連コマンド

コマンド名	機能
enable cli-config-logging	設定変更ログをイネーブルにします。
disable cli-config-logging	設定変更ログをディセーブルにします。
show log {<priority>}	現時点におけるログのスナップショットを表示します。 • `priority` − ここで指定したレベル以上のメッセージだけを表示します。critical、emergency、error、alert、warning、notice、info、debug のいずれかを指定します。デフォルトは info です。
show log configuration	syslog ホストの IP アドレス、ローカルログに記録されるメッセージのレベル、syslog ホストに送信されるメッセージのレベルなど、ログ機能の設定内容を表示します。
clear counters	すべての統計およびポートカウンタをリセットします。
clear log {static}	ログをクリアします。`static` オプションを指定した場合は、critical レベルのメッセージも削除されます。

15.6 RMON

本製品は、運用効率の改善とネットワークの負荷軽減に役立つ RMON（Remote Monitoring）機能を備えています。

以下の節では、RMON の概要と本製品がサポートする RMON 機能について説明します。

RMON 機能を使用するには、RMON 管理アプリケーションが必要です。また、本製品の RMON 機能をイネーブルにしてください。

RMON の概要

RMON とは、LAN のリモート監視を目的とする Remote Monitoring Management Information Base（RMON MIB）の略称です。RMON MIB は、RFC 1271 と RFC 1757 で規定されています。

RMON による LAN 管理には、通常次のものが必要です。

- **RMON プローブ** − LAN セグメント（または VLAN）の統計情報を収集する、リモートコントロール可能なインテリジェントデバイスあるいはエージェント（ソフトウェア）。RMON プローブは、管理ステーションから要求があった場合、あるいは、統計データがあらかじめ設定されたしきい値を超えた場合に、情報を送信します。
- **管理ステーション** − RMON プローブと交信して、情報を収集するワークステーション。必ずしもプローブと同じネットワーク上になくてもよく、ネットワークを通じて、あるいは、コンソールポートなどを通じてプローブを管理します。

サポートされる RMON グループ

IETF では、9 つの RMON グループを定義しています。本製品では、以下の 4 グループをサポートします。

- Statistics
- History
- Alarms
- Events

この節では、これらのグループについて説明します。

Statistics

Statistics グループは、パケット数、バイト数、ブロードキャストパケット数、マルチキャストパケット数、エラーパケット数など、LAN セグメント（あるいは VLAN）上のトラフィックやエラーに関する統計情報を提供します。

Statistics グループの情報は、重要なネットワークエリアでトラフィックパターンやエラーパターンの変化を察知するために使用されます。

History

History グループは、統計データのサンプリング間隔や保持するサンプルの数などを定義します。Statistics グループが提供するカウンタを一定の間隔でサンプリングすることにより、ネットワークパフォーマンスの時系列データを得ることができます。

History グループは、LAN セグメント（VLAN）上のトラフィックパターン分析に最適で、正常な状態におけるパラメータを求める上で基礎となる情報を提供します。

Alarms

Alarms グループは、任意の RMON 変数にしきい値とサンプリング間隔を設定し、変数の値がしきい値を横切った場合にアラームを発生させます。しきい値には、rising threshold（上限値）と falling threshold（下限値）があり、それぞれ設定値を上回ったときと下回ったときにアラームを発生します。また、しきい値は絶対値と相対値の両方による設定が可能です。さらに、しきい値は手動設定のほか自動調整も可能です。

Alarms グループでしきい値を適切に設定しておけば、パフォーマンス上の問題が発生した際に、Events グループを通じて自動的な対応を行うことができます。

Events

Events グループでは、RMON アラームの発生を受けて、イベントログにエントリを作成したり、管理ステーションに SNMP トラップを送信したりします。アラーム発生時のアクションは、(1) 無視する、(2) ログに記録する、(3) SNMP トラップを送信する、(4) ログに記録してトラップを送信する、のいずれかから選択できます。SNMP トラップは、Trap Receiver テーブルに登録

されたトラップレシーバに送られます。RMON トラップは、RFC 1757 で risingAlarm と fallingAlarm の 2 種類が定義されています。

Events グループの有効活用は、時間の節約につながります。リアルタイムのグラフ表示を眺め続けなくても、Events グループを利用すれば重要なイベントの発生時に通知を受けることができるからです。SNMP トラップを利用して他のアクションを発生させることにより、イベント発生時に自動的な対策をとることができます。

RMON 機能のイネーブル / ディセーブル

RMON 機能のイネーブル / ディセーブルを切り替えるには、次のコマンドを使います。デフォルトはディセーブルです。ただし、ディセーブル時も RMON の問い合わせには応答し、アラームとイベントを生成します。

```
[enable | disable] rmon
```

RMON 機能の設定を確認するには、次のコマンドを使います。

```
show management
```

イベントアクション

表 15-5 に、アラーム発生時に実行するアクションの一覧を示します。どのアクションを実行するかは、個別に設定可能です。

表 15-5：イベントアクション

名前	アラーム発生時のアクション
No action	何もしない
Notify only	すべてのトラップレシーバにトラップを送信
Notify and log	トラップを送信し、RMON ログにエントリを追加

SNMP トラップによるイベント通知を利用するには、トラップレシーバの設定が必要です。詳しくは、3-16 ページの「SNMP による管理」をご覧ください。

16 ファームウェアのアップグレードと設定の保存

この章では、ファームウェアのアップグレード手順と設定の保存方法について解説します。

16.1 ファームウェアのアップグレード

ファームウェアをアップグレードするには、TFTP サーバからネットワーク経由でダウンロードする方法と、コンソールポートに接続した PC から XMODEM プロトコルでダウンロードする方法があります。

ファームウェアのアップグレードは、以下の手順で行います。

1 ファームウェアファイルを TFTP サーバ、またはコンソールポートに接続された PC にコピーします。

2 次のコマンドを実行して、ファームウェアを本製品にダウンロードします。

```
download image [xmodem | [<ipaddress> | <hostname>] <filename>] {primary
| secondary}
```

コンソールポート経由でダウンロードするには、`xmodem` オプションを指定します。TFTP サーバからダウンロードするときは、`[<ipaddress> | <hostname>]` にサーバの IP アドレスかホスト名（DNS クライアント設定時）を、`<filename>` にファームウェアのファイル名を指定します。

本製品は、ファームウェアの保存領域を 2 つ（*primary* エリアと *secondary* エリア）持っています。ファームウェアをダウンロードするときは、`primary`、`secondary` の両オプションでどちらの領域に保存するかを選択できます。保存領域を指定しなかった場合は、使用中のファームウェアが上書きされますのでご注意ください。

3 次のコマンドを実行して、再起動後に使用するファームウェアを指定します。

```
use image [primary | secondary]
```

デフォルトでは、*primary* 領域のファームウェアを使って起動します。

再起動

本製品を再起動するには、次のコマンドを使います。

```
reboot {time <date> <time> | cancel}
```

<date> と <time> には、再起動を行う日付と時刻を以下の形式で指定します。

```
mm/dd/yyyy hh:mm:ss
```

日付と時刻を指定しなかった場合は、コマンド入力後ただちに再起動が行われます。この場合、予約済みの再起動スケジュールはキャンセルされます。また、再起動スケジュールだけを取り消したい場合は、cancel オプションを使います。

16.2 設定の保存

起動後に施した設定は一時保存用のランタイムメモリに保存されるため、本製品を再起動すると消えてしまいます。再起動後も同じ設定を使用したい場合は、以下の手順で設定内容を不揮発性メモリ（NVRAM）に保存してください。

本製品は、2 つの設定保存領域（*primary* エリアと *secondary* エリア）を持っています。そのため、設定を保存するときはどちらの領域に設定を保存するかを選択できます。領域を指定しなかった場合は、現在使用中の設定が上書きされますのでご注意ください。

普段と異なる設定をテストをするような場合、テスト対象の設定を通常使用する設定と別の領域に保存しておけば、たとえ設定に失敗した場合でも再起動後に元の設定に戻すことができます。

設定を保存するには、次のコマンドを使います。

```
save {configuration} {primary | secondary}
```

次の再起動時に使用する設定を変更するには、次のコマンドを使います。

```
use configuration [primary | secondary]
```

設定保存中に再起動を行った場合は、工場出荷時の設定で起動します。保存中でなかったほうの設定には影響ありません。

工場出荷時の設定に戻す

設定を工場出荷時の状態に戻すには、次のコマンドを使います。

```
unconfig switch
```

このコマンドを実行すると、ユーザアカウントとパスワードを除くすべての設定が出荷時の状態に戻ります。

ユーザアカウント情報を含むすべての設定パラメータをリセットするには、次のように all オプションを指定します。

```
unconfig switch all
```

主な設定項目の出荷時設定については、付録 D「出荷時の設定」をご覧ください。

16.3 TFTP による設定のアップロードとダウンロード

現在の設定内容は、CLI コマンドの書式で記述されたテキストファイルとして、ネットワーク上の TFTP サーバにアップロードすることができます。この機能は次のような点で便利です。

- テキストエディタで設定ファイルを編集できる。
- アップロードした設定ファイルを別のスイッチにダウンロードして使用できる。
- 障害発生時に設定ファイルをテクニカルサポートに送ることができる。
- 設定ファイルを毎日自動的にアップロードし、TFTP サーバ上にバックアップコピーを作成できる。

設定ファイルをアップロードするには、次のコマンドを使います。

```
upload configuration [[<ipaddress> | <hostname>] <filename> {<time>} | can-
cel]
```

[<ipaddress> | <hostname>]にはTFTPサーバのIP アドレスかホスト名を、<filename>にはアップロード後のファイル名を指定します。<time> オプションを省略した場合は、ただちにアップロードが実行されます。<time> を指定すると、毎日指定された時刻に設定が自動的にアップロードされます。自動アップロードをオフにするには、cancel オプションを使用します。

設定ファイルをダウンロードするには、次のコマンドを使います。

```
download configuration [<ipaddress> | <hostname>] <filename>
```

[<ipaddress> | <hostname>]にはTFTPサーバのIP アドレスかホスト名を、<filename>にはダウンロードする設定ファイルの名前を指定します。

ダウンロードした設定ファイルの内容は、再起動後から有効になります。ただし、ダウンロードした設定は一時的なもので、電源を切ると消えてしまうため、再起動後は必要に応じてsave コマンドを実行し、*primary* または *secondary* エリアに保存してください。

16.4 BootROM のアップグレード

BootROM をアップグレードするには、次のコマンドを使います。

```
download bootrom [<ipaddress> | <hostname>] <filename>
```

TFTP サーバの IP アドレス（またはホスト名）と、BootROM のファイル名を指定してください。

16.5 ファームウェア / 設定関連コマンド

表 16-1 に、ファームウェアと設定に関連するコマンドの一覧を示します。

表 16-1：ファームウェア / 設定関連コマンド

コマンド名	機能
show configuration	現在の設定内容を一連の CLI コマンドとして表示します。
download bootrom [<ipaddress> | <hostname>] <filename>	指定した TFTP サーバから BootROM イメージをダウンロードし、フラッシュメモリ上の BootROM をアップデートします。
download configuration [<ipaddress> | <hostname>] <filename>	指定した TFTP サーバから、テキスト形式の設定ファイルをダウンロードします。
download image [xmodem | [<ipaddress> | <hostname>] <filename>] {primary | secondary}	XMODEM または TFTP を使ってファームウェアをダウンロードします。保存領域を指定しなかった場合は、現在使用中のファームウェアが上書きされます。
reboot {time <date> <time> | cancel}	指定した日時にスイッチを再起動します。日時を指定しなかった場合は、コマンド入力後ただちに再起動が行われます。この場合、すでに予約されていた再起動スケジュールはキャンセルされます。再起動スケジュールを取り消すには、`cancel` オプションを指定します。
save {configuration} {primary | secondary}	現在の設定内容を不揮発性メモリ（NVRAM）に保存します。設定保存領域を primary エリアと secondary エリアから選択できます。保存領域を指定しなかった場合は、現在使用中の設定が上書きされます。
upload configuration [[<ipaddress> | <hostname>] <filename> {<time>} | cancel]	指定した TFTP サーバに現在の設定内容をアップロードします。`<time>` オプションを省略した場合は、ただちにアップロードが実行されます。`<time>` を指定すると、毎日指定した時刻に設定が自動的にアップロードされます。自動アップロードをオフにするには、`cancel` オプションを指定します。
use configuration [primary | secondary]	次の再起動時に使用する設定を指定します。
use image [primary | secondary]	次の再起動時に使用するファームウェアを指定します。

A　トラブルシューティング

この章では、予想される問題とその解決方法について説明します。ここに記載されていない問題が発生した場合は、ユーザーサポートにご連絡ください。

A.1 LED

POWER LED が点灯しない

電源ケーブルがスイッチ本体と電源コンセントにしっかりと接続されているかどうか確認してください。

電源投入時に DIAG（MGMT）LED が橙色に点灯する。

電源投入時テスト（POST）の実行中にエラーが発生しました。販売店にご相談ください。

ネットワークケーブルを接続しても LINK LED が点灯しない

以下の項目をチェックしてください。

- ケーブルがしっかりと接続されていますか。
- ケーブルに断線等はありませんか。
- ケーブルの種類（カテゴリ 3/5、SMF/MMF）や結線（ストレート / クロス）は正しいですか。
- リンクの両端の機器に電源が投入されていますか。
- ギガビットリンクの両端でオートネゴシエーション設定が同じになっていますか。

  ギガビットリンクの両側でオートネゴシエーションの設定が異なっている場合、オートネゴシエーションがオフになっている側の LINK LED が点灯し、オンになっている側の LINK LED は点灯しないのが普通です。デフォルトでは、ギガビットポートはオートネゴシエーションがオンに設定されています。対向機器がオートネゴシエーションをサポートしていない場合は、本製品側ギガビットポートのオートネゴシエーションをオフに設定してください。オートネゴシエーションの設定は、次のコマンドで確認できます。

  ```
  show ports configuration
  ```

A.2 管理インタフェース

ログインプロンプトが表示されない。

端末あるいは端末エミュレータが正しく設定されているか確認してください。

コンソールポート経由でアクセスした場合は、ログインプロンプトが表示されるまで、数回「Return」キーを押さなくてはならない場合があります。

端末（エミュレータ）の設定を確認します。通信速度は 9600 ボー、データビットは 8、ストップビットは 1、パリティはなし、フロー制御は XON / OFF になっていますか。

SNMP 対応ネットワークマネージャからスイッチにアクセスできない

本製品の IP アドレス、サブネットマスク、デフォルトルートが正しく設定されているかどうか確認してください。IP 設定の変更後は再起動が必要です。ご注意ください。

ネットワークマネージャに、本製品の IP アドレスが正しく登録されていますか。詳細については、ネットワークマネージャのマニュアルをご覧ください。

本製品とマネージャに同じコミュニティ名が設定されていますか。

本製品の SNMP アクセス機能がディセーブルに設定されていないか確認してください。

Telnet によるアクセスができない

本製品の IP アドレス、サブネットマスク、デフォルトルートが正しく設定されているかどうかを確認してください。IP 設定の変更後は再起動が必要ですのでご注意ください。

Telnet クライアントに入力した本製品の IP アドレスが間違っていませんか。

スイッチの Telnet アクセス機能がディセーブルに設定されていないか確認してください。

すでに限度いっぱい Telnet セッションが開かれているときにログインしようとすると、そのことを示すエラーメッセージが表示されます。

SNMP 対応ネットワークマネージャでトラップを受信できない

SNMP 対応ネットワークマネージャの IP アドレスとコミュニティ名が正しく設定されているかどうかを確認します。本製品にトラップレシーバの IP アドレスが正しく設定されているかどうかも確認してください。

SNMP/Telnet アクセスができなくなった

本製品の Telnet / SNMP アクセス機能がイネーブルに設定されていますか？

SNMP マネージャまたは Telnet ワークステーションが接続されているポートがディセーブルに設定されていないか確認してください。ポートがイネーブルに設定されている場合は、ケーブルがポートにしっかりと接続されているか確認してください。

上記のポートが所属している VLAN は、正しく設定されていますか？

他のポートから本製品にアクセスしてみてください。これでうまくいけば、先ほどのポートに問題があることがわかります。ケーブルの配線等を再確認してください。

原因は、ネットワークの問題によるものかもしれません。コンソールポート経由のアクセスはできますか。

スイッチとマネージャのコミュニティ名が同じかどうか確認してください。

スイッチの SNMP アクセス機能がディセーブルに設定されていませんか。

ログインパスワードを忘れてしまった

一般ユーザのパスワードを忘れてしまった場合は、管理者レベルの別のユーザでログインし、パスワードを忘れてしまったユーザをいったん削除してから、新しいユーザとパスワードを設定します。

管理者レベルでログインして、スイッチを初期化する方法もあります。この場合、すべての設定情報（パスワードを含む）が出荷時の状態に戻ります。

管理者権限を持つユーザのパスワードが誰にもわからなくなってしまった場合は、販売店にご相談ください。

A.3 ポート

大量の Receive Bad CRC Frames（Rx CRC）が記録される

10/100M ポートでは、オートネゴシエーション設定が本製品オン、対向機器オフの場合、通信速度（10/100M）のみ自動検出され、通信モードは常にハーフデュプレックスとなります。フルデュプレックスで通信を行うには、対向機器のオートネゴシエーションをオンにするか、本製品・対向機器ともに通信モードをフルデュプレックス固定に設定してください。

本製品と対向機器の通信モード設定が異なる場合は、`show ports {<portlist>} rxerrors` コマンドで大量の受信 CRC エラーフレーム（Rx CRC）が表示されますが、これは本製品の問題ではありません。

パフォーマンスをフルに発揮するため、リンク両端で通信モードが同じになるよう設定してください。

A.4 VLAN

VLAN にポートを追加できない

VLAN にポートを追加しようとした際に、次のようなエラーメッセージが表示されることがあります。

```
C9100:79 # config vlan orange add ports 1,2
ERROR: There is a protocol conflict with adding port 1 untagged to
       vlan "orange".  Either add this port as tagged or assign another
       protocol to this vlan
ERROR: There is a protocol conflict with adding port 2 untagged to
       vlan "orange".  Either add this port as tagged or assign another
       protocol to this vlan
```

これは、指定したポートが、すでにタグなし VLAN に所属していることを示しています。タグなし VLAN は、ポートあたり 1 つしか設定できません。次のコマンドを使って、VLAN の構成を確認してください。

```
show vlan {<name>}
```

このエラーが発生したときは、さきほど指定したポートを、設定済みのタグなし VLAN から削除します。たとえば、ポート 1 と 2 がすでに VLAN *default* に所属している場合は、次のコマンドを実行します。

```
C9100:80 # config vlan default delete ports 1,2
```

これで、次のコマンドがエラーなく実行できるようになります。

```
C9100:81 # config vlan orange add ports 1,2
```

VLAN 名

VLAN 名に使用できる文字は、英数字とアンダースコア（_）およびハイフン（-）です。スペースやコンマを使うことはできません。また VLAN 名の先頭は必ず英字（アルファベット）でなくてはなりません。VLAN 名は 32 文字以内で設定します。

802.1Q タグ VLAN の問題

VLAN 名が意味を持つのは、コマンドラインインタフェースからローカルにアクセスするときだけです。802.1Q タグを使って複数のスイッチにまたがる VLAN を構成するときは、VLANid が食い違わないように注意してください。

本製品を他社の機器と接続する場合は、たとえ VLANid が同じでも、802.1Q パケットを示す EtherType フィールドの値が異なっている可能性があります。この値は、本製品では 8100 に設定されています。もし他社の機器が別の値を使っていて変更できない場合は、次のコマンドを使って本製品の 802.1Q パケットの EtherType を変更することができます。

```
config dot1q ethertype <ethertype>
```

このパラメータは、VLAN タグ付きフレームの識別に使われるもので、本製品が送信するタグ付きフレームにもこの値が挿入されます。

VLAN と IP アドレス、デフォルトルートについて

本製品では、VLAN ごとに IP アドレスを設定できます。ただし、Telnet や SNMP、Ping による管理を行う必要がないなら、VLAN に IP アドレスを設定しなくてもかまいません。また、本製品は複数のデフォルトルートを持つことができます。スイッチは、メトリックが最小のデフォルトルートを最初に使用します。

VLAN 削除後のパーマネント FDB エントリ

VLAN を削除しても、その VLAN に所属していたパーマネント FDB エントリは削除されません。このエントリをあえて削除しなくても問題はありませんが、削除したいときは手動で削除する必要があります。

デフォルトルートとスタティックルート

デフォルトルートとスタティックルートは、VLAN およびその IP アドレスが削除されてもそのまま残ります。使われなくなったルートは、手動で削除する必要があります。

A.5 STP

スイッチに直接接続した端末機器が正常に起動しない

スイッチの STP 初期化プロセス完了前に、端末機器が起動しようとしたことが考えられます。この場合は、VLAN の STP 設定をディセーブルにするか、端末機器が接続されているポートと通信相手が接続されているポートの STP 設定をオフにしてから、端末機器を再起動します。

端末機器の FDB エントリが頻繁にエージアウトされる

冗長経路を使用しないスイッチでは、STP をディセーブルにしてトポロジ変化を減らしてください。

端末機器のエントリをスタティックまたはパーマネントに設定します。

B　Web インタフェース

この章では、Web インタフェースの使用方法について説明します。Web インタフェースでは、コマンドラインインタフェース（CLI）で実行できる設定 / 監視コマンドのうち、よく使われるものだけが使用できます。Web インタフェースで実行できない設定を行うには、CLI を使ってください。

B.1 Web アクセスのイネーブル / ディセーブル

出荷時には、Web アクセス機能はイネーブルになっています。Web アクセスをディセーブルにするには、次のコマンドを使います。

```
disable web
```

Web アクセスを再開するには、次のコマンドを実行します。

```
enable web
```

Web アクセスの設定変更は再起動後から有効になります。

再起動の方法については、16-1 ページの「再起動」をご覧ください。

Web インタフェースを使用するには、少なくとも 1 つの VLAN を作成し、IP アドレスを割り当てておく必要があります。

VLAN に IP アドレスを割り当てる方法については、3-10 ページの「IP パラメータの設定」をご覧ください。

B.2 ブラウザの設定

通常、Web インタフェースはブラウザのデフォルト設定で問題なく使用できます。さらに操作性を向上させたいときは、以下のガイドラインを参考にブラウザの設定を調整してください。

- 新しいソフトウェアイメージをダウンロードしたら、いったんブラウザのディスクキャッシュとメモリキャッシュをクリアして、新しいメニュー画面が表示されることを確認してください。すべての GIF ファイルが更新されるよう、キャッシュのクリアは Web インタフェースのログイン画面で実行してください。

- **ブラウザのキャッシュ設定で、ページにアクセスするたびに文書の確認が行われるようにしてください。**

  Netscape Navigator 3.0x **では、「オプション」→「ネットワークの設定」→「キャッシュ」タブ→「文書の確認」で「毎回」を選択してください。**

  Microsoft Internet Explorer 3.0 **では、「表示」→「オプション」→「詳細設定」タブ→「インターネット一時ファイル」の「設定」ボタン→「保存しているページの新しいバージョンの確認」で「ページを表示するごとに確認する」を選択してください。**

- **画像の自動読み込みをオンにしてください。**
- **フレーム内になるべく多くの情報が表示できるよう、高解像度のモニタを使ってください。画面解像度は、**1024 x 768 **ピクセルに設定することをお勧めします。**800 x 600 **ピクセルでもいいでしょう。**
- **表示される情報量をさらに増やすには、ブラウザのツールバー表示をオフにします。**
- Web **インタフェースから電子メールを送りたいときは、ブラウザの電子メール情報を設定してください。**
- **おすすめフォント設定は以下のとおりです。**
  - **プロポーショナルフォント** ― Times **系フォント**
  - **固定ピッチフォント** ― Courier **系フォント**

B.3 Web インタフェースにアクセスする

Web **インタフェースにアクセスするには、以下の** URL **をブラウザに入力してください。**<ipaddress> **には、**VLAN **に割り当てた本製品の** IP **アドレスを指定します。**

```
http://<ipaddress>
```

ホームページにアクセスすると、ログイン画面が表示されます。ユーザ名とパスワードを入力して、「OK**」ボタンをクリックしてください。**

管理者レベルでログインした場合は、Web **インタフェースのすべてのページにアクセスできます。一般ユーザは、統計情報とサポート情報にのみアクセスできます。**

ユーザ名、ユーザレベル、およびパスワードの設定方法については、3-7 **ページの「ユーザアカウント」をご覧ください。**

複数のユーザが同時に Web **インタフェースにアクセスした場合、次のようなエラーメッセージが表示されることがあります。**

```
Web:server busy
```

その場合は、いったんログアウトしてから、再度ログインしてください。

B.4 Web インタフェースの画面

ログインに成功すると、Web インタフェースのホームページが表示されます。

Web インタフェースの画面は、次の 3 つの部分から構成されています。

- タスクフレーム
- コンテンツフレーム
- スタンドアローンボタン

タスクフレーム

タスクフレームは 2 つの部分から構成されています。タスクフレームの上部には、次に示す 4 つのタスクタブが表示されます。

- Configuration
- Statistics
- Support
- Logout

タスクタブの下にはさまざまなオプションが表示されます。表示されるオプションは、選択したタスクタブによって異なります。オプションを選択すると、コンテンツフレームに表示されている情報が変化します。ただし、新しいタスクタブを選択しても、オプションを選択するまではコンテンツフレームの情報が更新されないので注意してください。

コンテンツフレーム

コンテンツフレームは、さまざまな情報が表示される Web インタフェースのメインスクリーンです。たとえば、「Configuration」タスクタブからオプションを選択すると、コンテンツフレームに設定パラメータの入力フィールドが表示されます。また、「Statistics」タブを選択した場合は、コンテンツフレームに統計情報が表示されます。

複数選択の方法

ブラウザの画面には、ドロップダウンリストボックスや、チェックボックス、複数選択可能なリストボックスなど、さまざまな GUI コンポーネントが表示されます。複数選択可能なリストボックスには、右側にスクロールバーが表示されます。表 B-1 に複数選択の方法をまとめます。

表 B-1：複数選択リストボックスの操作

選択方法	操作
1 つだけ選択	マウスで項目をクリックする。
すべての項目を選択	最初の項目をクリックし、最後の項目までドラッグする。

表 B-1：複数選択リストボックスの操作

選択方法	操作
連続した項目を選択	最初の項目をクリックし、任意の項目までドラッグする。
任意の項目を複数選択	「Ctrl」キーを押したまま、選択したい項目をクリックしていく。

ステータスメッセージ

コンテンツフレームの上部にはステータスメッセージが表示されます。ステータスメッセージには、以下の 4 種類があります。

- Information ー 設定変更の前に知っておくと便利な情報、あるいは設定変更の結果が表示されます。
- Warning ー 設定に関する警告が表示されます。
- Error ー 設定が正しく行われなかったために発生したエラーが表示されます。
- Success ー 「Submit」ボタンを押すと表示されます。文面は、「Request was submitted successfully.」です。

スタンドアローンボタン

コンテンツフレームの一番下に、スタンドアローンボタンが表示されることがあります。スタンドアローンボタンは、設定オプションとは関係のない操作を実行するために使います。代表的な例に、「Reboot Switch」ボタンがあります。

B.5 設定の保存

Web インタフェースを使ってスイッチの設定内容を不揮発性メモリ（NVRAM）に保存するには、2 つの方法があります。

- 「Configuration」タスクタブの「Switch」オプションから、「Save Configuration」を選択します。

  設定保存領域を指定するドロップダウンリストボックスから、「primary」と「secondary」のどちらかを選び、「Submit」ボタンをクリックします。

  設定保存領域の詳細については、16-1 ページの「再起動」をご覧ください。

- 「Logout」タブをクリックします。

  設定変更後に保存を行わないままログアウトしようとすると、Web インタフェースは設定を保存するかどうか確認してきます。

「Yes」を選択すると、以前選択した保存領域に設定が保存されます。保存領域を変更したいときは、「Configuration」タブの「Switch」オプションを使用する必要があります。

B.6 VLAN 選択後の「Get」を忘れずに

VLAN 設定時には、適切な VLAN を選択したら必ず「Get」ボタンをクリックしてください。VLAN を選択しただけで「Get」を実行しなかった場合は、以前表示されていた VLAN に対して設定が適用されます。

ある VLAN の設定を行った後にその VLAN を削除すると、VLAN 名ウィンドウには VLAN *default* が表示されますが、ページの下部にある VLAN 情報は更新されません。「Get」ボタンをクリックして、最新の情報を表示させてください。

B.7 Web インタフェースの画面を保存する

ユーザーサポートなどの目的で、Web インタフェースの画面を保存して電子メールで送信したいときは、以下の手順にしたがってください。

1. 保存したい画面のコンテンツフレームをクリックします。
2. Netscape Navigator では、「ファイル」メニューから「フレームに名前を付けて保存」を選択し、ファイル名を入力します。
3. Microsoft Internet Explorer の場合は、「ファイル」メニューから「名前を付けて保存」を選択し、ファイル名を入力します。
4. 保存したファイルをメールに添付して送信します。

C CentreCOM RPS1000 接続時の補足事項

本製品にリダンダントパワーサプライ CentreCOM RPS1000 を接続している場合、以下の方法によって RPS1000 の電源とファンの状態などを知ることができます。

1 CentreCOM 9100/8500 のコマンドラインインタフェース（CLI）上で `show switch` コマンドを実行します。電源供給状況と RPS1000 の温度およびファンの状態が表示されます。

2 本製品の SNMP トラップ送信機能をイネーブルにし、トラップレシーバの IP アドレスを設定します。RPS1000 は、本体内温度の上昇時またはファン回転数の低下時に RPS ケーブルを通じて本製品に信号を送ります。本製品は、RPS1000 から信号を受け取ると次ページの表に記載されている SNMP トラップを送出して異常を知らせます。また、電源供給状態が変化したときにも、SNMP トラップが送信されます。

3 LED を確認します。温度上昇時やファン障害発生時には、RPS1000 の該当する LED が黄色に点灯します。また、電源供給状態が変化したときにも LED の点灯状態が変化します。

表 C-1：RPS1000 のステータス通知機能一覧

状態	SNMP トラップ	C9100/8500 LED	RPS1000 LED	show switch の出力*
RPS 接続正常時	なし	POWER 点灯（緑）	RPS1、2 点灯（緑） FAN FAIL 消灯 OVER TEMP 消灯	Primary OK, RPS OK, RPS fan/temp OK
RPS ファン回転低下	rpsAlarm	変化なし	FAN FAIL 点灯（黄）	Primary OK, RPS OK, RPS fan/overtemp alarm
RPS ファン回転復旧	rpsNoAlarm	変化なし	正常時に戻る	正常時に戻る
RPS 内部温度上昇	rpsAlarm	変化なし	OVER TEMP 点灯（黄）	Primary OK, RPS OK, RPS fan/overtemp alarm
RPS 内部温度正常化	rpsNoAlarm	変化なし	正常時に戻る	正常時に戻る
C9100/8500 電源障害 **	powerSupplyFail	POWER 点滅（橙）	変化なし	Primary failed, RPS OK, RPS fan/temp OK
C9100/8500 電源復旧	powerSupplyGood	正常時に戻る	変化なし	正常時に戻る
RPS ケーブル障害 ***	powerSupplyFail	変化なし	RPS1/2 点滅（緑）	Primary OK, RPS not present
RPS ケーブル復旧	powerSupplyGood	変化なし	正常時に戻る	正常時に戻る
RPS AC 電源障害 ****	powerSupplyFail	変化なし	RPS1/2 消灯	Primary OK, RPS failed, RPS fan/temp OK
RPS AC 電源復旧	powerSupplyGood	変化なし	正常時に戻る	正常時に戻る

＊　show switch コマンドの Power Supply 状態表示

＊＊　C9100/8500 の内蔵電源ユニットの故障、AC 電源ケーブルの断線、接触不良、あるいは AC 供給源の停電など

＊＊＊　C9100/8500 と RPS1000 を接続する専用 RPS（DC）ケーブルの断線など

＊＊＊＊　RPS1000 の内蔵電源ユニットの故障、AC 電源ケーブルの断線、接触不良、あるいは AC 供給源の停電など

D　出荷時の設定

表 D-1 に本製品の出荷時設定を示します。

表 D-1：本製品の出荷時設定

設定項目	出荷時設定
ポート	全ポートイネーブル
ユーザアカウント	*admin*、*user*（ともにパスワード未設定）
コンソールポート	9600 ボー、データビット 8、ストップビット 1、パリティなし、フロー制御 XON/XOFF
Telnet アクセス	イネーブル
Web アクセス	イネーブル
SNMP アクセス	イネーブル
SNMP read コミュニティ名	*public*
SNMP write コミュニティ名	*private*
RMON	ディセーブル
BOOTP	VLAN *default* でイネーブル
QoS	全トラフィック *qp1*
802.1p プライオリティ	イネーブル
802.3x フロー制御	イネーブル（ギガビットポートのみ）
VLAN	全ポート VLAN *default*（VLANid=1）に所属。VLAN *default* は、STPD *s0* に所属
802.1Q VLAN タギング	VLAN *default* 所属のパケットはすべてタグなし
GVRP	ディセーブル
FDB エージングタイム	300 秒（5 分）
スパニングツリープロトコル	ディセーブル。ポートの設定はイネーブル
IP ユニキャストルーティング	ディセーブル
RIP	ディセーブル
RIP Aggregation	ディセーブル
OSPF	ディセーブル。VLAN *default* はバックボーンエリア（0.0.0.0）に所属
IP マルチキャストルーティング	ディセーブル
DVMRP	ディセーブル

表 D-1：本製品の出荷時設定

設定項目	出荷時設定
PIM-DM	ディセーブル
IGMP スヌーピング	イネーブル
IPX ルーティング	ディセーブル
SNTP クライアント	ディセーブル
DNS クライアント	ディセーブル
ポートミラーリング	ディセーブル
ルータディスカバリー（IRDP）	ディセーブル

E　製品仕様

電源部仕様	
定格入力電圧	AC 100-120 / 200-240V（自動切替）
入力電圧範囲	AC 90-120 / 180-255V（自動切替）
定格周波数	50 / 60Hz
最大消費電力	118W
最大入力電流	3.0A（入力電圧 AC 100V 時）
発熱量	102kcal/h
環境条件	
動作時温度	0 ～ 40 ℃
保管時温度	-20 ～ 60 ℃
動作時湿度	80% 以下（ただし、結露なきこと）
保管時湿度	95% 以下（ただし、結露なきこと）
寸法 :	約 440（W）× 432（D）× 89（H）mm
重量	約 8.2kg（C9108）、約 8.3kg（C8518）、 約 8.1kg（C8525）、約 8.5kg（C8550）
適合規格	
安全	• UL1950 • CSA 22.2 No.950（cUL） • TUV EN60950
EMI	• VCCI Class B（C9108/8518） • VCCI Class A（C8525/8550） • FCC part 15 Class A • EN55022 Class B
EMS	• EN50082 -1 • EN61000-4-2 • EN61000-4-3 • EN61000-4-4

ネットワーク標準	• SNMP (RFC 1157) • MIB-II (RFC 1213) • Bridge MIB (RFC 1493) • Interfaces MIB (RFC 1573) • Ethernet-like MIB (RFC 1650) • Ethernet-like MIB + gigabit (draft-ietf-hubmib-etherif-mib-v2-00) • RMON MIB (RFC 1757) • RMON II Probe Configuration (RFC 2021) • 802.3 MAU MIB (RFC 2239) • 802.3 MAU MIB + gigabit (draft-ietf-hubmib-mau-mib-v2-01) • IP Forwarding MIB (RFC 1354) • Entity MIB (RFC 2037) • RIP2 MIB (RFC 1724) • Telnet (RFC 854) • HTTP 1.0 • UDP (RFC 768) • IP (RFC 791) • ICMP (RFC 792) • TCP (RFC 793) • ARP (RFC 826) • TFTP (RFC 1350) • BOOTP (RFC 1542) Ethernet-like MIB + gigabit および 802.3 MAU MIB + gigabit については、http://www.ietf.org/html.charters/hub-mib-charter.html をご参照ください。

C9108 / 8518

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報処理装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

C8525 / 8550

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

F　ユーザーサポート

本製品のユーザーサポートに関しては、ご購入先の販売店までお問い合わせください。

索引

X

あ

い

え

お

か

き

く

け

こ

さ

し

ろ

コマンド名索引

D

E

H

L

N

P

Q

R

S

T

U

X