CentreCOM 9100/8500 シリーズ
ユーザーガイド

アライドテレシス株式会社

http://www.allied-telesis.co.jp/

Published: June 1999
PN J613-M6673-00 Rev.A

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ついては、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。

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

1999 年 6 月　Rev.A　初版

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 °C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

2　設置と初期設定

3　管理機能へのアクセス

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 ステータス表示と統計機能

13 Web インタフェース

図目次

表目次

はじめに

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、保証書とともに大切に保管くださいますようお願い申し上げます。

対象読者

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、読者の皆様が以下の事柄に関する基本的な知識を持っているものと仮定しています。

- 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
- SNMP（Simple Network Management Protocol）

製品に同梱されているリリースノートと本書の記載内容が異なる場合は、リリースノートの情報が優先されます。

表記規則

本書の表記規則を、表 0-1 と表 0-2 にまとめます。

表 0-1: アイコン

アイコン	名前	意味
	ヒント	重要な情報や指示を示します。
	注意	人体やシステムに危害や損害がおよぶ恐れがあることを示します。
	警告	人体に重大な危害がおよぶ恐れがあることを示します。

表 0-2: 書体

書体	意味
`Screen displays`	画面に表示される文字は、タイプライタ体で表します。
`User Entry`	ユーザが入力する文字は、太字のタイプライタ体で表します。
「Esc」	キーは、「Return」や「Esc」のようにかぎかっこで囲んで表します。 2 つ以上のキーを同時に押す場合は、「Ctrl」+「Alt」+「Del」のように表記します。

コマンド構文の説明に使う記号については、3-4 ページの「記号について」をご覧ください。

製品名の表記

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。

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インテリジェントスイッチです。

この章では、以下の事柄について説明します。

- 製品ラインナップ
- 特徴
- 外観図
- LED 表示
- 出荷時の設定

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ギガビットインターフェースコネクタ（GBIC）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 モデルでは、IP ルーティングなどのレイヤー 3 機能が使用できませんが、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、1-3 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。

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り、すべてのポートでワイヤスピードのパケット送受信が可能
- オプションでリダンダントパワーサプライ（RPS1000）を装着可能
- 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が可能（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
- IEEE 802.1Q VLAN タギングにも対応した VLAN（バーチャル LAN）機能
- スパニングツリープロトコル（IEEE 802.1D）に対応。複数の STPD を設定可能
- ポリシーベースの QoS（Quality of Service）機能により、ポートや VLAN ごとにサービス品質レベルの設定が可能
- 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 *
- RIP バージョン 1 および 2 *
- OSPF（Open Shortest Path First）*
- 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 IP マルチキャストトラフィックの制御
- DVMRP（Distance Vector Multicast Routing Protocol）による、ダイナミックなマルチキャストルーティング *
- 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
- GVRP による VLAN 自動登録機能

* の付いた機能は、レイヤー 2 モデルでは使用できません。

ポート構成

本製品が備えているポートは次のいずれかです。

- 固定式 1000BASE-SX ポート（SC コネクタ）
- モジュール式 1000BASE-SX/LX ポート（モジュラーポートに GBIC モジュールを装着）
- 10BASE-T/100BASE-TX 自動認識ポート（RJ-45 コネクタ）

各モデルのポート構成を表 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
CentreCOM 9108SX	6	2（GBIC-SX）		
CentreCOM 9108LX	6	2（GBIC-LX）		
CentreCOM 8518SX		2（GBIC-SX）	1（GBIC 未装着）	16
CentreCOM 8518LX		2（GBIC-LX）	1（GBIC 未装着）	16
CentreCOM 8525SX		1（GBIC-SX）	1（GBIC 未装着）	24
CentreCOM 8525LX		1（GBIC-LX）	1（GBIC 未装着）	24
CentreCOM 8550SX		2（GBIC-SX）	2（GBIC 未装着）	48
CentreCOM 8550LX		2（GBIC-LX）	2（GBIC 未装着）	48

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。

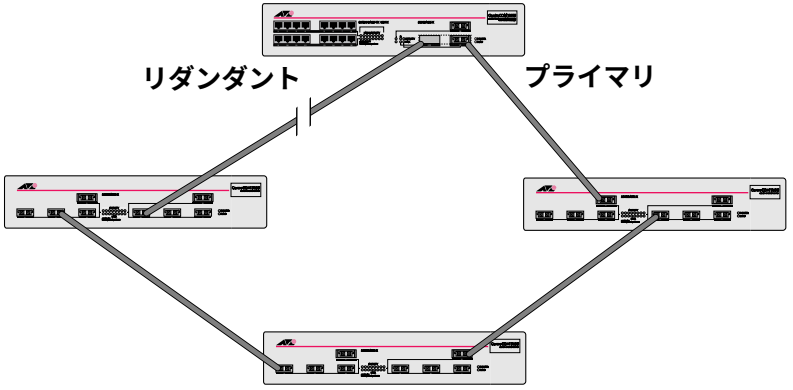

図 1-1: デュアルホーム構成

この構成では、プライマリポートに障害が発生するかリンクがダウンした場合に、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。この機能（スマートリダンダンシー機能）は、使用できないようにすることも可能です。

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。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。

ロードシェアリング機能の詳細については、4-5 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 機能を使用すれば、物理的なネットワーク構成にとらわれずにブロードキャストドメインを設定することができます。VLAN は 256 個まで作成可能です。同一 VLAN 内では、あたかも同じネットワークの一員であるかのように通信を行うことができます。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 間で通信を行うには、ルーティングサービスを提供するルータなどのデバイスが必要となります。
- **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。

VLAN の詳細については、第 5 章をご覧ください。

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。

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 章をご覧ください。

QoS（Quality of Service）

本製品では、ポリシーベースの QoS 機能により、トラフィックグループごとに最小 / 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できます。デフォルトでは、すべてのトラフィックに QoS ポリシープロファイル *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 DVMRP（Distance Vector Multicast Routing Protocol）によるダイナミックルーティング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 章をご覧ください。

C9108 前面図

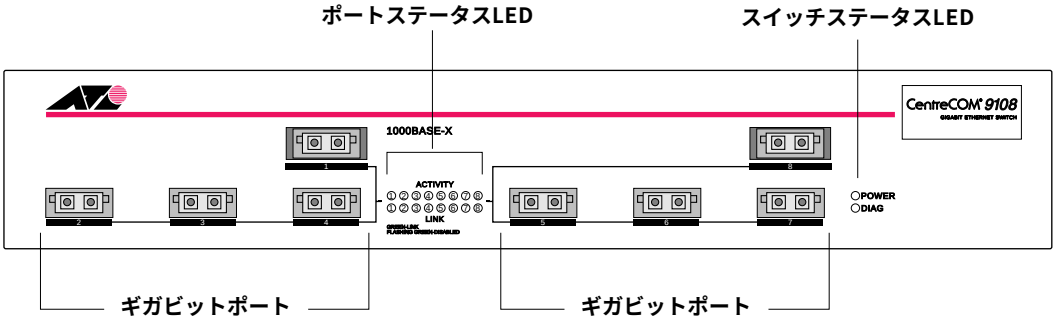

図 1-2: C9108 前面図

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 コネクタです。

C8518 前面図

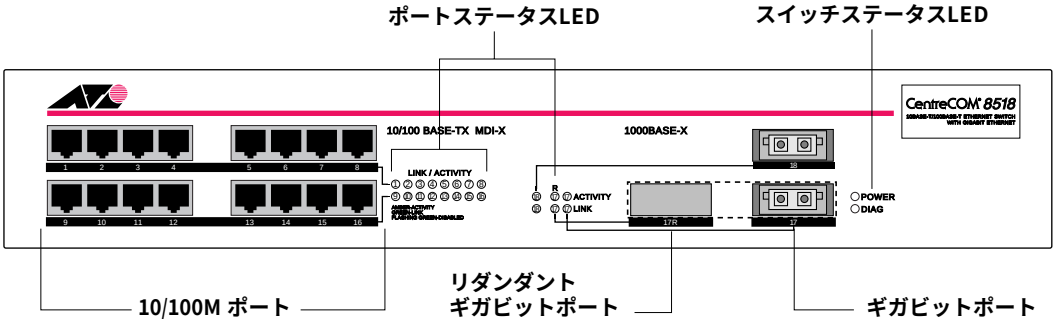

図 1-3: C8518 前面図

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。

LED の詳細については、1-9 ページの「LED 表示」をご覧ください。

C8525 前面図

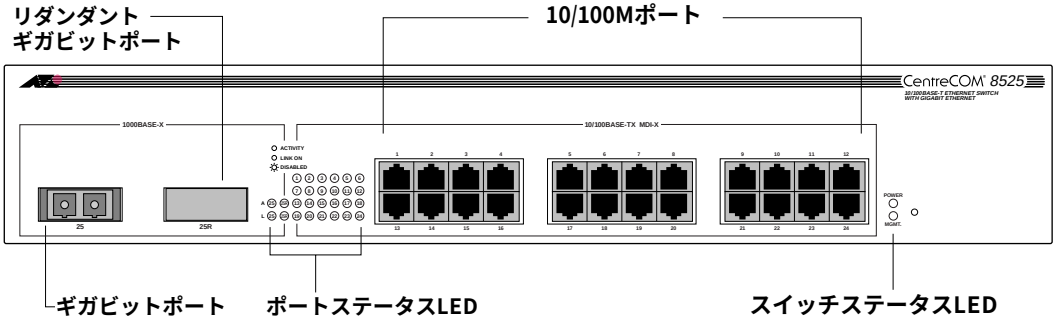

図 1-4: C8525 前面図

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。

C8550 前面図

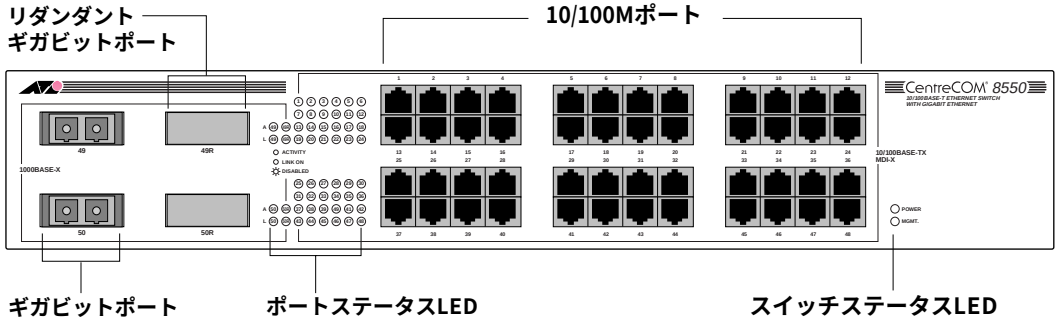

図 1-5: C8550 前面図

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。

対応するケーブルと伝送距離については、2-2 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。

LED 表示

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、またはソフト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 1-6 に本製品の背面図を示します。

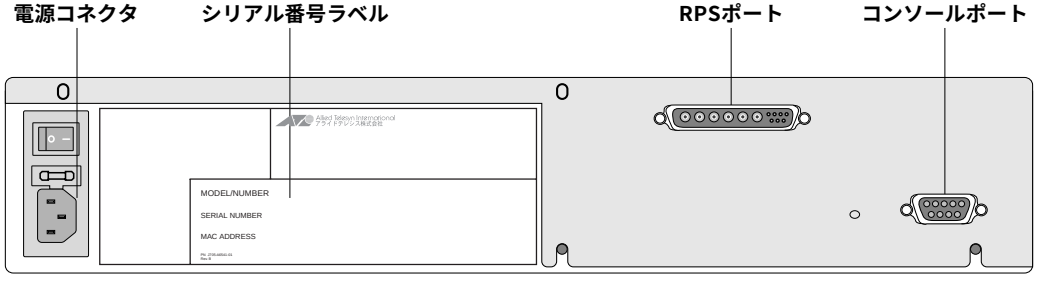

図 1-6: 本製品の背面図

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端末を接続します。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。

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 B をご覧ください。

出荷時の設定

表 1-4 に本製品の出荷時設定を示します。

表 1-4: 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
Web 管理	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 history セッション	イネーブル
RMON alarms	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
VLAN	全ポート VLAN *default* 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
スパニングツリープロトコル	スイッチ全体ではディセーブル。STPD 内のポートはイネーブル
IP ユニキャストルーティング	ディセーブル
FDB エージングタイム	300 秒（5 分）
RIP	スイッチ全体ではディセーブル。IP アドレスを持つ各 VLAN ではイネーブル
OSPF	スイッチ全体ではディセーブル。IP アドレスを持つ各 VLAN ではイネーブル。全 VLAN がバックボーンエリアに所属
IP マルチキャストルーティング	ディセーブル
DVMRP	スイッチ全体ではディセーブル。IP アドレスを持つ各 VLAN ではイネーブル
IGMP スヌーピング	ディセーブル
GVRP	ディセーブル
ルータディスカバリー（IRDP）	ディセーブル

2 設置と初期設定

この章では、本製品の設置方法について説明します。

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。

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、1-3 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）
- 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

設置場所

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。本製品は水平な場所に設置することも、EIA 規格の標準 19 インチラックに収納することもできます。また、ワイヤリングクローゼットやマシンルームに設置することもできます。ラックに取り付けるときは、付属のマウンティングブラケットを使用します。

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
- 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

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最長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	カテゴリ 5 UTP ケーブル（100Mbps）		100
10BASE-T	カテゴリ 3 UTP ケーブル（10Mbps）		100

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。

設置方法

設置方法には、ラックに取り付ける方法と水平な場所に設置する方法があります。

ラックへの取り付け

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。

ラックへの取り付け方法は以下のとおりです。

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。

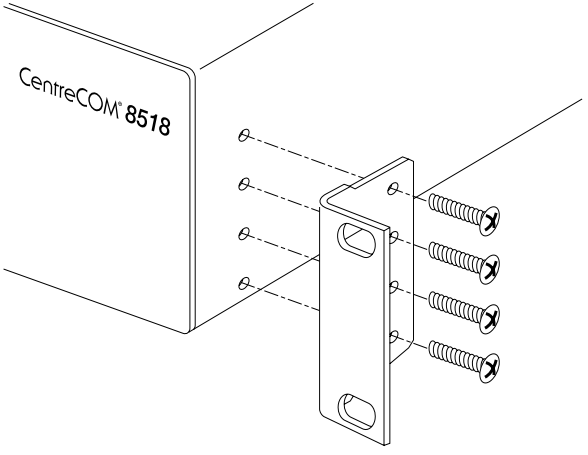

図 2-1: マウンティングブラケットの取り付け

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。

7 本製品をリダンダントパワーサプライに接続します（オプション）。

8 ケーブル類を接続します。

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。

コンソール端末の接続

コンソールポートには、本製品の管理に使用する VT100 互換のコンソール端末（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。

- **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する必要があります。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 2-2 のピン配置を参考にしてください。.

表 2-2: 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。

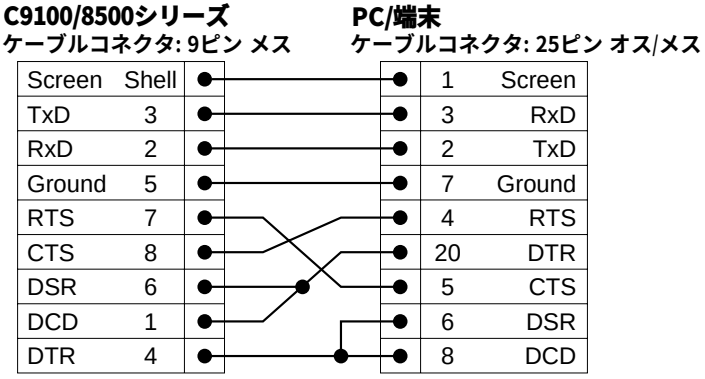

図 2-2: 9 ピン－ 25 ピン クロスケーブルの結線

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。

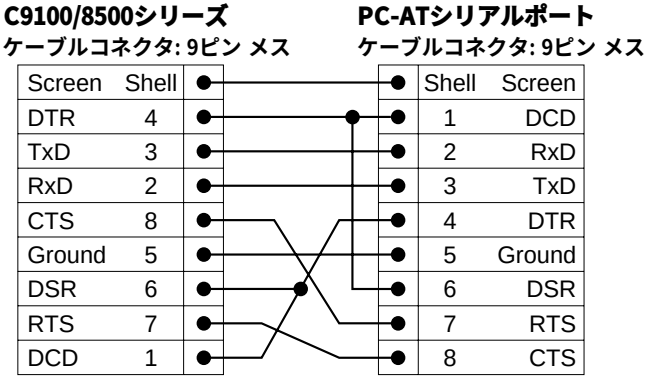

図 2-3: 9 ピン－ 9 ピン クロスケーブルの結線

電源投入

本体に AC 電源ケーブルを接続し、次に電源ケーブルをコンセントに接続します。電源を投入するには、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 は点灯、DIAG LED は速い（毎秒 2 回）点滅状態になります。DIAG LED の速い点滅は、POST が正常に終了するまで続きます。

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 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、1-9 ページの「LED 表示」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、3-8 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、14-2 ページの「設定の保存」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
```

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 管理機能へのアクセス

この章では、本製品の管理に必要な以下の事柄について説明します。

- コマンドの入力方法
- コマンドライン編集機能
- コマンド履歴
- ユーザアカウント
- 管理機能へのアクセス方法
- SNMP の設定
- 接続の確認

電源オフ後も設定が消えないようにするには、設定変更後に save コマンドを実行する必要があります。save コマンドの詳細については、14-2 ページの「設定の保存」をご覧ください。

コマンドの入力方法

ここでは、コマンド入力の手順について説明します。コマンドラインインタフェース（CLI）の詳しい使用方法については、この章の後半で説明します。

コマンドの入力方法は次のとおりです。

1 コマンドを入力する前に、必要なユーザ権限があ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 2a 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、14-2 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すれば、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
< >	**変数または値を示します。たとえば、次の例では、** `config vlan <name> ipaddress <ipaddress>` **<name>の部分には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。**
[ ]	**カッコに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> | all}` **この例では、VLAN 名 <name> とキーワード all のどちらも指定されなかった場合は、すべての VLAN が表示されます。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。
「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。

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
```

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> {<password>}	ユーザアカウントを作成します。
create vlan <name>	VLAN を作成します。
config account <username> {<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。
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 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。
clear session <number>	Telnet セッションを終了させます。
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。

表 3-3: 一般的な管理コマンド

コマンド名	機能
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。
disable telnet	Telnet アクセスをディセーブルにします。
disable web	Web アクセスをディセーブルにします。
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。
show banner	ユーザ定義のバナーを表示します。

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 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。

admin **アカウントを削除することはできません。**

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「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。

```
#show accounts

User Name      Access  LoginOK  Failed  Session
-------------  ------  -------  ------  --------
       admin    R/W      0         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>
```

本製品の管理

本製品を管理するには、次のような方法があります。

- コンソールポートに接続した端末（または端末エミュレータがインストールされた 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（CLI）にアクセスする。
- TCP/IP ネットワーク上で、Telnet を使って CLI にアクセスする。
- TCP/IP ネットワーク上で、Web ブラウザを使って Web インタフェースにアクセスする。
- TCP/IP ネットワーク上で、SNMP 対応のネットワークマネージャを使用する。

同時に開くことのできるユーザセッションは 7 つまでです（例：コンソールセッション × 1、Web セッション × 1、Telnet セッション × 5）。

コンソール端末からのアクセス

本製品にはコマンドラインベースの管理インタフェースが組み込まれており、本体背面の RS-232 ポート（9 ピンオス D タイプ）に接続した端末からアクセスすることができます。

コンソールポートのピン配置については、2-5 ページをご覧ください。

コンソールポートに端末を接続すると、端末画面上にシステムプロンプトが表示され、ログイン可能な状態になります。

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。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、「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、システム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> {<port_number>}
```

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。

IP パラメータの設定

Telnet や 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。

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く必要があります。

- 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。

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、9-10 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 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。

- 管理者レベルでログインします。
- VLAN に IP アドレスとサブネットマスクを割り当てます。

  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。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。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の識別名が表示されます。

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
```

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. 次のコマンドを使って、現在開かれているセッションを確認します。

   show session

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。

```
show session:

  0  Wed Sep 17 20:48:38 1997   admin  console serial
* 4  Wed Sep 17 21:52:16 1997   admin  telnet 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。

IP 設定コマンド

表 3-5 に IP 設定コマンドの一覧を示します。

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> | all}	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> | all}	指定した VLAN の設定情報を表示します。
show ipstats {vlan <name> | all}	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> | all | permanent | proxy {<ipaddress> <mask> | all} }	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。

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 や Microsoft Internet Explorer 3.0 など、HTML フレームに対応した Web ブラウザを使ってスイッチの管理が可能です。

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、3-12 ページの「IP パラメータの設定」をご覧ください。

Web 管理機能のデフォルトホームページには、以下の URL でアクセスできます。

```
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。

Web インタフェースの使用方法については、第 13 章をご覧ください。

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、14-2 ページの「再起動」をご覧ください。

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。ただしその場合は、管理ステーションに適切な MIB（Management Information Base）がインストールされている必要があります。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、表 3-3 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
拡張 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 カウンタはサポートしていません。

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 6 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 6 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。
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。

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 コマンドは、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>
```

表 3-10 に ping コマンドのパラメータを示します。

表 3-10: 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連続して送信します。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。

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 コマンドは、指定したホストまでの経路を表示します。traceroute コマンドの構文は次のとおりです。

```
traceroute <ipaddress>
```

<ipaddress> には、リモートホストの IP アドレスを指定します。

4 ポートの設定

本製品のポートは、次のような設定が可能です。

- ポートのイネーブル / ディセーブル
- 通信速度（10/100M ポートのみ）
- 通信モード（フルデュプレックス / ハーフデュプレックス）
- ロードシェアリンググループの設定
- ポートごとの QoS 設定

QoS 機能の詳細については、第 8 章をご覧ください。

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。

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。これらは手動で設定することもできます。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
```

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。ギガビットポートでは、つねに 1Gbps フルデュプレックスで通信が行われるため、`config ports` コマンドの `duplex` パラメータは意味をなしませんが、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
```

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。10/100M 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> | 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。

表 4-1: ポート設定コマンド

コマンド名	機能
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

表 4-1: ポート設定コマンド

コマンド名	機能
show ports {<portlist>} packet	パケットの分布統計を表示します。
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。QoS 機能の詳細については、第 8 章をご覧ください。
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、12-7 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、12-7 ページの「ポートエラー統計」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、12-7 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。

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。

この機能は、本製品でのみ使用できるものですが、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機能の使用中に 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機能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。

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。
- **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。
- **VLANと物理ポートの組み合わせ** ― 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。
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、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。

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 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。

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、コマンドラインインタフェースを用いて、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**

  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**

  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。VLAN *Marketing* 内の機器と VLAN *Sales* 内の機器が通信するには、ルータを経由しなくてはなりません。

- **機器の取り替えや移動が容易に**

  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。

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
- 上記の 3 つを組み合わせたコンビネーション VLAN

ポート VLAN

ポート VLAN では、ポートグループに対して VLAN 名を割り当てます。各ポートが所属できるポート 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。

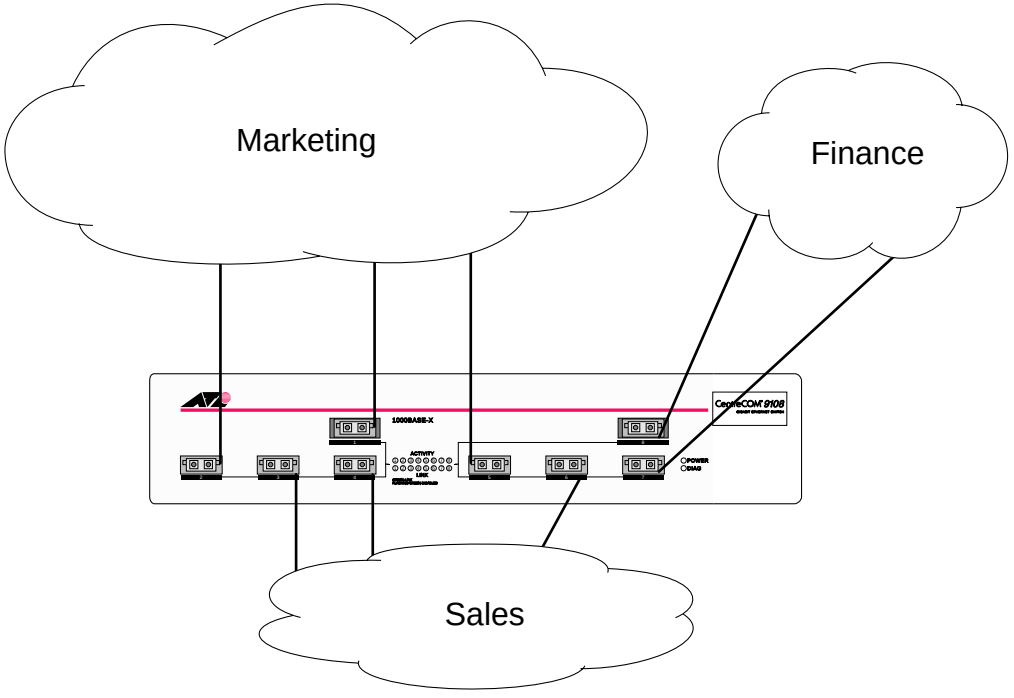

図 5-1: ポート VLAN の構成例

ここではすべての機器が同じスイッチ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には、本製品の IP ルーティング機能を利用しなくてはなりません。この場合、各 VLAN には、ルータインタフェースとなる固有の IP アドレスを割り当てておく必要があります。

複数のスイッチにまたがるポート VLAN

複数のスイッチにまたがるポート VLAN を構築するには、次の手順にしたがいます。

- 各スイッチ上で VLAN を作成します。
- 同じ VLAN に属するポート同士でスイッチ間を接続します。

図 5-2 は、2 台のスイッチにまたがる VLAN *Sales* の設定例です。どちらのスイッチとも、すべてのポートが VLAN *Sales* に所属しています。2 台のスイッチは、上のスイッチのポート 2 と下のスイッチのポート 6 を使って接続されています。

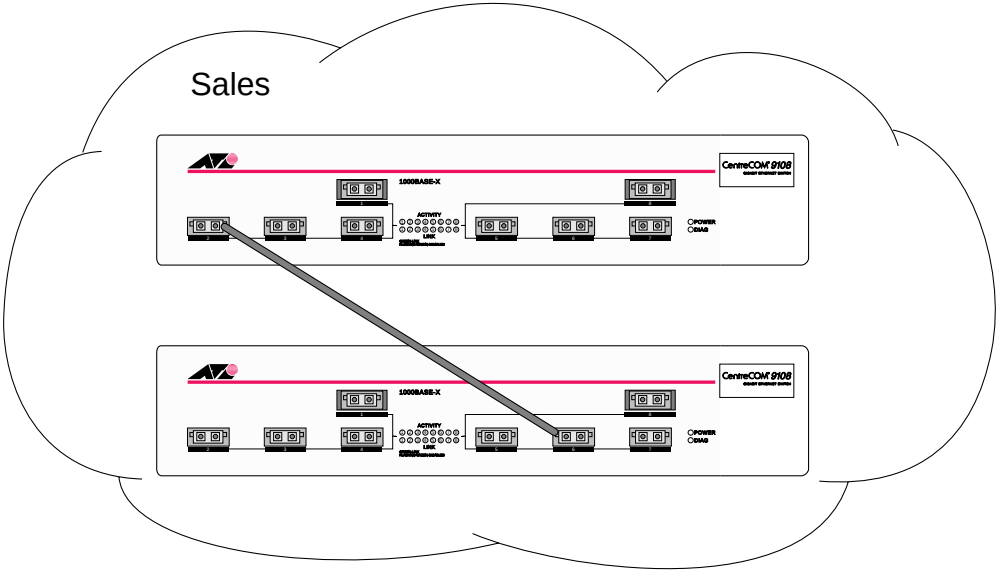

図 5-2: 2 台のスイッチにまたがって構成されたポート VLAN

2 台のスイッチにまたがるポート VLAN を複数作成する場合は、VLAN ごとにスイッチ間を接続しなくてはなりません。

図 5-3 は、2 台のスイッチにまたがる 2 つの VLAN、*Accounting* と *Engineering* の設定例です。両スイッチとも、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、上のスイッチのポート 2 と下のスイッチのポート 4 で、*Engineering* は、上のスイッチのポート 5 と下のスイッチのポート 8 で接続されています。

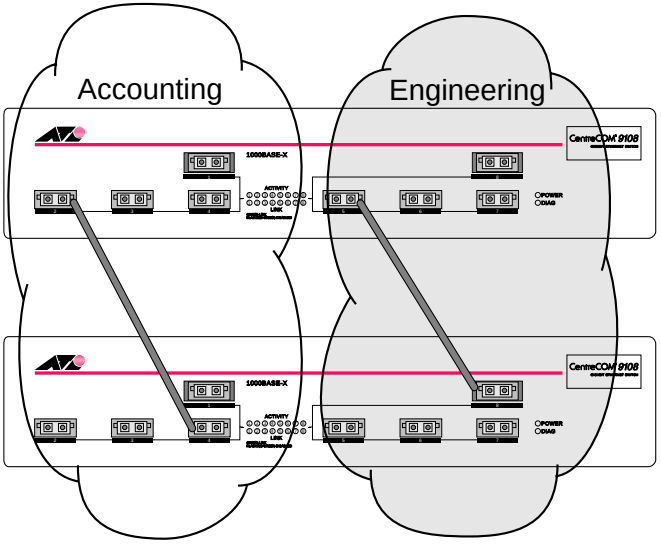

図 5-3: 2 台のスイッチにまたがって構成された 2 つのポート VLAN

上記の手順にそってスイッチを数珠つなぎにすれば、3 台以上のスイッチにまたがる VLAN を作成することも可能です。各スイッチには、VLAN ごとに他のスイッチと接続するためのポートが必要です。スイッチ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 タグは複数のスイッチにまたがる VLAN を作成するときに使われます。スイッチ間のリンクを「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スイッチにまたがる 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 台のスイッチにまたがる複数の 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。

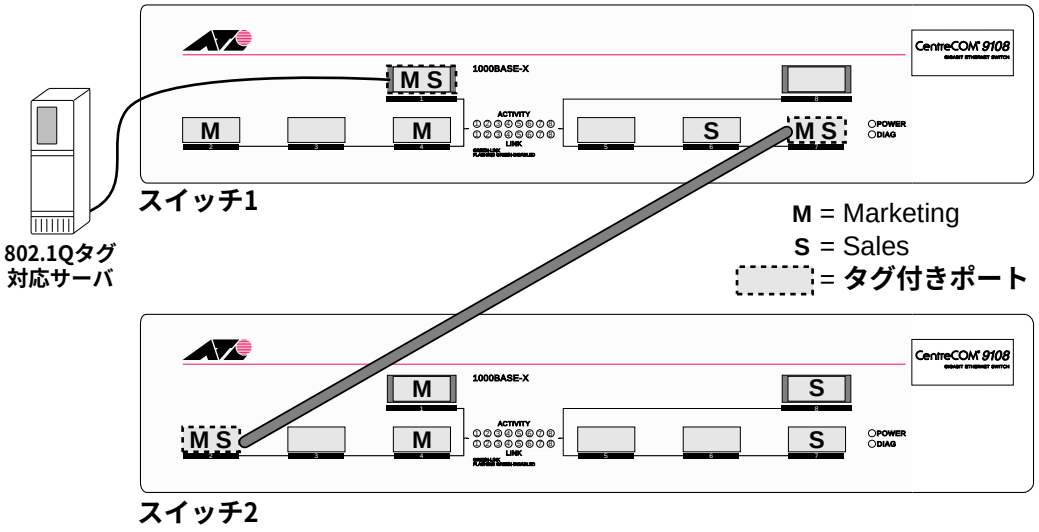

図 5-4: タグ付き / タグなしトラフィックの同時使用例

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。

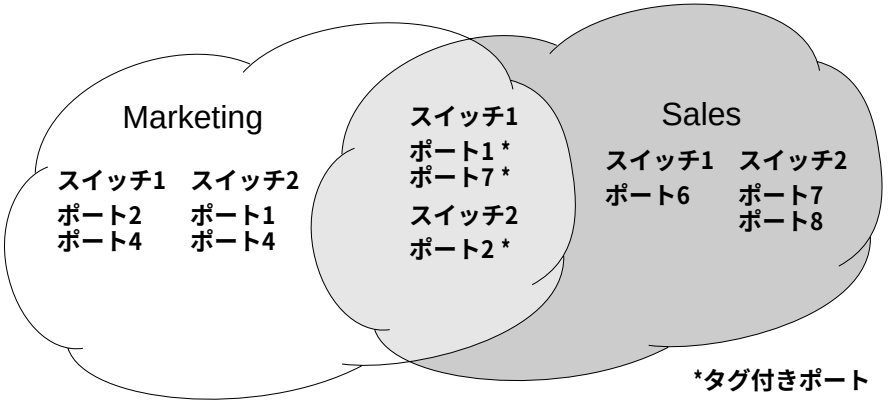

図 5-5: タグ付き / タグなしポートの構成図

図 5-4、図 5-5 では、

- 2つのスイッチ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。

i **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（Generic VLAN Registration Protocol）

GVRP（Generic 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。

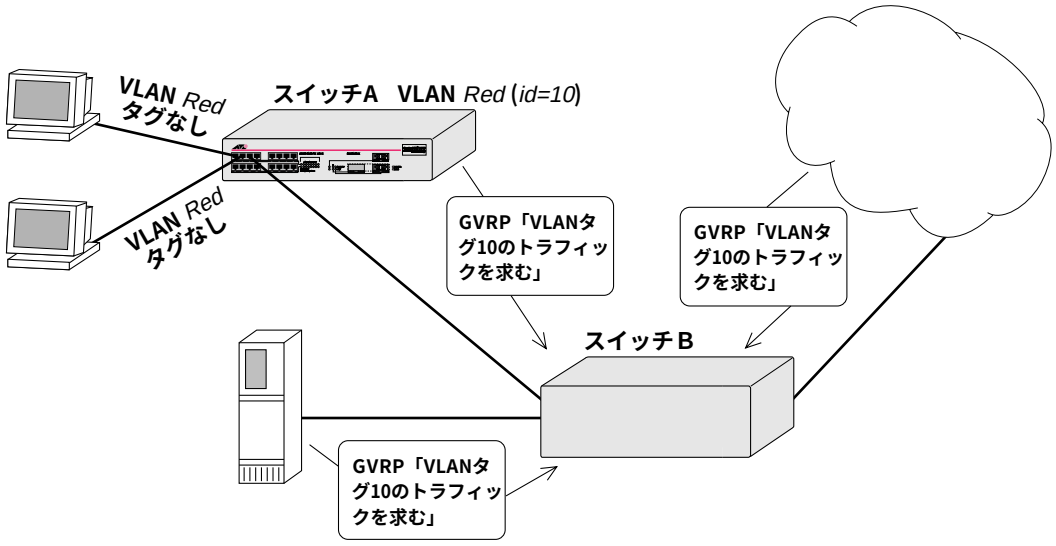

図 5-6: GVRP を使用したネットワーク

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 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。**
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。

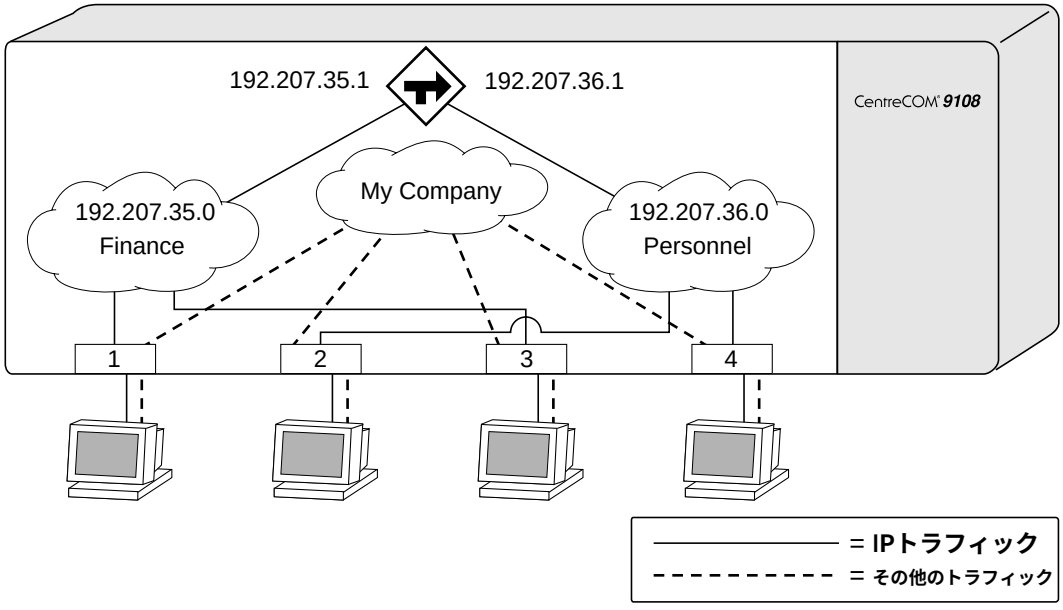

図 5-7: プロトコル VLAN

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。

- IP
- IPX
- NetBIOS
- DECNet
- IPX_8022
- IPX_SNAP
- AppleTalk

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。

- 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。

- 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 7 つまで定義できます。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。

プロトコルフィルタの削除

VLAN から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す。これ以降もその VLAN の設定を行うことはできますが、別のプロトコルを割り当てるまで、その VLAN にはまったくフレームが転送されなくなります。

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。

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。

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。

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。

2 必要に応じ、VLAN に IP アドレスとネットマスクを設定します。

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 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 内にタグ付きフレームを使うポートがある場合は、VLANid を割り当てます。

4 ポートを VLAN に割り当てます。

追加するポートごとに、IEEE 802.1Q タグを使うかどうかを指定します。

表 5-2 に VLAN 設定コマンドの一覧を示します。

表 5-2: 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。

表 5-2: VLAN 設定コマンド

コマンド名	機能
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 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 Ethernet タイプのいずれかを示す、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> 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 accounting ipaddress 132.15.121.1
config default delete ports 1-3,6
config accounting add ports 1-3,6
```

VLAN 名は他と重複しないように設定することが決められているので、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 video tag 1000
config 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 sales tag 120
config sales add ports 1-3 tagged
config 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 ipsales protocol ip
config 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 myvlan protocol myprotocol
```

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> | all}
```

次に出力例を示します。

```
show vlan all

VLAN "net142" created by user
      Tagging:    Untagged (Internal tag 4095)
      IP:          Not configured.     IGMP Snooping is enabled
      STPD:       Domain "s0" is not running spanning tree protocol
      Protocol:  appletalk = SNAP:809b SNAP:80f3
      Qos Profile:         QP1
      Ports:      4.      (Number of active port=4)
                   Untag:    1   2   3 10

VLAN "net123" created by user
      Tagging:    802.1Q Tag 1054
      IP:          123.45.67.1/255.0.0.0 IGMP Snooping is enabled
      STPD:       Domain "s0" is not running spanning tree protocol
      Protocol:  Match all unfiltered protocols.
      Qos Profile:         QP1
      Ports:      18.      (Number of active port=6)
                   Untag:    1   2   3   4   5   8   9 10
                   Tagged:   6   7 11 12 13 14 15 16 17 18
```

`show vlan` コマンドを実行すると、VLAN ごとに以下の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）
- IGMP スヌーピングの動作状況
- IP アドレス
- STPD
- プロトコル
- QOS プロファイル
- VLAN に所属するポート

- ポートごとのタグ付き / タグなし設定
- ポートがどのようにして VLAN に追加されたか（user または GVRP）

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> | all}
```

`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 Type（etype、llc、snap）
- プロトコル Value

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 5-3 のコマンドを使います。

表 5-3: 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。
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 スイッチフォワーディングデータベース（FDB）

この章では、スイッチフォワーディングデータベース（FDB）の内容と働き、設定方法について説明します。

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、スイッチ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。

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` − **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` − **所属する VLAN 名を指定します。** ■ `blackhole` − **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` − **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` − **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` − **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。**

表 6-1: FDB 設定コマンド

コマンド名	機能
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 00E02B123456
- 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 00A023123456
- 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

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 {all | <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。

- `all` ― FDB 内のすべてのエントリを表示します。
- `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。

```
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 ― スタティックエントリ（ユーザが登録）
  d ― ダイナミックエントリ（スイッチが学習）
  m ― MAC アドレスエントリ
  i ― 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。

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 {all | <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。キーワード** `all` **を指定した場合は、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。

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。

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恐れがありますが、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。

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。

各ポートは、1 つの STPD にしか所属できません。ポートが複数の VLAN に所属している場合、すべての VLAN が同じ STPD に所属していなければなりません。

VLAN と STP の設定時に気を付けるべきポイントを次に示します。

- 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、経路を適切に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。
- 同一の 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。

1 台のスイッチ内では、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。

STPD を削除すると、その STPD に所属する VLAN も削除されます。STPD を削除するときは、あらかじめ STPD から VLAN を外しておいてください。

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。

STP 構成上の注意

STPD に VLAN を割り当てるときは、VLAN トラフィックが正しく転送されるよう、STP の構成に十分な注意を払ってください。

図 7-1 に、VLAN タグを使ってトランク間を接続したネットワーク構成例を示します。ここでは、次に挙げる 5 つの VLAN が定義されています。

- *Sales* ― スイッチ A、B、M
- *Personnel* ― スイッチ A、B、M
- *Manufacturing* ― スイッチ Y、Z、M
- *Engineering* ― スイッチ Y、Z、M

- *Marketing* — すべてのスイッチ（A、B、Y、Z、M）

また、ここでは 2 つの STPD が定義されています。

- STPD1 には、VLAN *Sales* と *Personnel* が所属
- STPD2 には、VLAN *Manufacturing* と *Engineering* が所属

VLAN *Marketing* は、デフォルト STPD に所属しています。

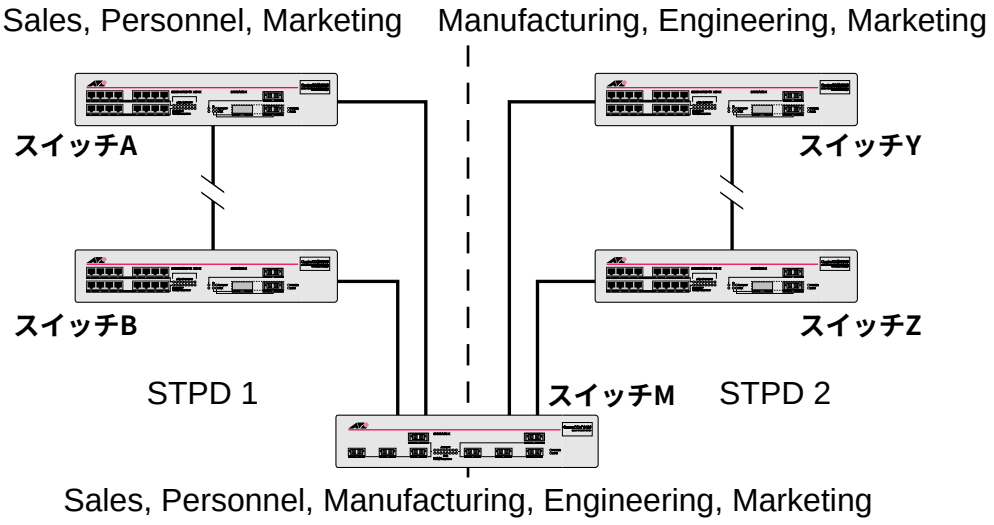

図 7-1: 複数のスパニングツリードメイン

この構成で各スイッチを起動すると、STP の働きにより、トポロジ内にループが構成されないよう各 STPD が設定されます。STP がネットワーク内でループが構成されないようにする方法はさまざまです。

図 7-1 では、スイッチ A — B 間とスイッチ Y — Z の間の経路がブロックされます。STP が安定した状態になると、すべての VLAN が通信可能になり、ブリッジループもすべて回避されます。

STPD1 と STPD2 のどちらにも所属していない VLAN *Marketing* は、5 つのスイッチすべてを使って通信します。すでに、スイッチ A — B 間とスイッチ Y — Z の間の経路はブロックされているので、ネットワーク内でループが形成されることはありません。

単一の STPD 内では、VLAN 構成時に十分な注意が必要です。図 7-2 は、よくないネットワーク構成の例です。この例では、STP の働きによって VLAN 間の転送ができなくなっています。

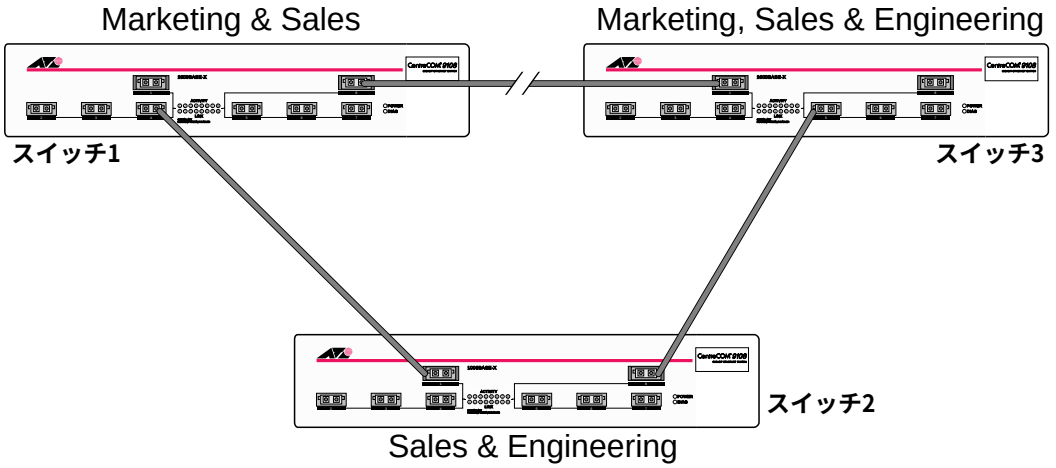

図 7-2: VLAN タグを使った STP 構成

図 7-2 のネットワークは次のような構成になっています。

- スイッチ 1 には、VLAN *Marketing* と *Sales* が定義されている。
- スイッチ 2 には、VLAN *Engineering* と *Sales* が定義されている。
- スイッチ 3 には、VLAN *Marketing*、*Engineering*、*Sales* が定義されている。
- VLAN タグを使ったトランク間接続により、STP では許されない三角形のループが形成されている。
- 各スイッチ上のすべての VLAN が同じ STPD に所属している。

この構成では、STP の働きにより、スイッチ 1 とスイッチ 3 のトランクポートがディセーブルとなり、スイッチ 1 ― 3 間のトラフィックが ブロックされる可能性があります。

スイッチ 2 には、VLAN *Marketing* に所属するポートがないため、スイッチ 1 とスイッチ 3 上にある VLAN *Marketing* のトランクポートがブロックされると、VLAN *Marketing* のトラフィックは、スイッチ（1 と 3）から出ることができなくなります。

STP の設定方法

STP を設定するには、以下の手順にしたがいます。

- 次のコマンドを使って、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なくてはなりません。すなわち、VLAN 名に使った名前を STPD 名や QoS プロファイル名として使うことはできません。

- 次のコマンドを実行して、STPD に VLAN を追加します。

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

- STPD 内で STP を有効にします。

  ```
  enable stpd [<stpd_name> | all]
  ```

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 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（ポートからブリッジへのルートコスト）
- 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。

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> | all]	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> | all]	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。
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。

表 7-1: STP 設定コマンド

コマンド名	機能
config stpd <stpd_name> ports cost <value> [<portlist> | all]	**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> | all]	**STPD内のポートのプライオリティを設定します。この値が大き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低くなります。**

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
```

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> | all}
```

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。

```
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）

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。

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> | all]	指定した STPD で STP プロトコルをディセーブルにします。キーワード all を指定した場合は、すべての STPD で STP をディセーブルにします。
disable stpd <stpd_name> ports [<portlist> | all]	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。
unconfig stpd [<stpd_name> | all]	指定した STPD の STP パラメータをデフォルト値に戻します。キーワード all を指定した場合は、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。

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。

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）パラメータから構成されます。
- **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。

QoS モード

QoS モードには、Ingress モード（デフォルト）と Egress モードの 2 種類があります。Ingress モードでは、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は、最小 / 最大帯域幅のみ変更できます。

Egress モードでは、独自の QoS プロファイルを追加できますが、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。Egress モードでは、定義した QoS プロファイルの最小 / 最大帯域幅に加え、優先度パラメータも変更可能です。

デフォルト QoS プロファイル

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。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。

QoS プロファイルは、以下のパラメータによって定義されます。

- **最小帯域幅** — 最小限必要な帯域を全帯域幅のパーセントで示します。最小値は 0% です。
- **最大帯域幅** — 使用が許可される最大帯域幅を、全帯域のパーセントで示します。
- **優先度** — トラフィックがサービスを受け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最小 / 最大帯域幅は、Ingress/Egress の両モードで変更できます。優先度設定は、Egress モードでのみ変更可能です。

トラフィックグループ

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トラフィックグループが適用されます。出荷時は、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。

以下に挙げるトラフィックグループは、優先順位の高いものから順番に並んでいます。

Ingress モード

Ingress モードでは、以下のトラフィックグループが利用できます。

- **宛先 IP アドレス** — 特定の宛先 IP アドレス、あるいは、サブネットマスクを使って表される一定範囲の宛先 IP アドレスに、QoS プロファイルを割り当てることができます。オプションとして、宛先の TCP/UDP ポート番号、送信元の IP アドレス、送信元の TCP/UDP ポート番号を指定することもできます（ポリシーベースのレイヤー 4 QoS 機能。8-7 ページ）。QoS パラメータは、ルーティングテーブルの作成にともない動的に適用されます。宛先 IP 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います。

```
config ipqos [add | delete] {all | TCP | UDP | other}
[<destination_ipaddress> <mask>] {dst-ipport <ipport>}
{<source_ipaddress>} {src-ipport <ipport>} [qosprofile <qosname> |
blackhole]
```

- **宛先 MAC アドレス** ― パーマネント FDB エントリの作成時に、QoS プロファイルを割り当てることができます。また、学習機能によって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。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>}
  ```

  次に例を示します。

  ```
  create fdbentry 00:11:22:33:44:55 vlan default ports 1 qosprofile qp1
  ```

- **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 8-2 に、802.1p ビットの値と QoS プロファイルの関係を示します。

表 8-2: 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
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。

  ```
  {enable | disable} pace
  ```

- **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]
  ```

- **VLAN** ― VLAN 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]
  ```

Egress モード

Egress モードでは、以下のトラフィックグループを利用できます。

- **宛先 IP アドレス** ― 前節 「Ingress モード」の「宛先 IP アドレス」と同じです。
- **宛先 MAC アドレス** ―前節 「Ingress モード」の「宛先 MAC アドレス」と同じです。
- **VLAN** ― 前節「Ingress モード」の「VLAN」と同じです。

トラフィックグループの優先順位

トラフィックが複数の基準に当てはまる場合は、次の優先順位が適用されます。

Ingress モード

- 宛先 IP アドレス
- 宛先 MAC アドレス
- IEEE 802.1p プライオリティビット
- PACE
- 送信元ポート
- VLAN

Egress モード

- 宛先 IP アドレス
- 宛先 MAC アドレス
- VLAN

優先度について

ポート上で送信要求の競合が発生した場合、QoS プロファイルの優先度にしたがって送信が行われます。競合するトラフィックグループが同じ優先度を持っていた場合は、ラウンドロビンアルゴリズムによって解決されます。

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 ― 0%
- 最大帯域幅 ― 100%
- 優先度 ― low

QoS パラメータの値を変更するには、Egress モードで次のコマンドを実行します。

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

Ingress モードでも、同じコマンドを使ってデフォルト QoS プロファイルの最小 / 最大帯域幅を変更できます。ただし、Ingress モードでは優先度を指定しても無視されます。

QoS プロファイルの割り当て

使用するトラフィックグループを決め、QoS プロファイルを作成したら、以下のコマンドを使ってプロファイルを割り当てます。

VLAN 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]
```

送信元ポートに 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（egress モードでは使用不可）。

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

MACアドレスエントリに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。

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

IP アドレスに 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 ipqos [add | delete] {all | TCP | UDP | other}
[<destination_ipaddress> <mask>] {dst-ipport <ipport>}
{<source_ipaddress>} {src-ipport <ipport>} [qosprofile <qosname> |
blackhole]
```

ポリシーベースのレイヤー 4 QoS 機能

特定の TCP/UDP ポートを使用するアプリケーショントラフィックに QoS プロファイルを割り当てることができます。この「レイヤー 4 フロー」は、宛先 / 送信元 IP アドレスと組み合わせて使用することができます。レイヤー 4 QoS を使用しても、本製品のワイヤスピードパフォーマンスに影響を与えることはありません。この機能は、宛先 IP アドレスに QoS プロファイルを割り当てる IP QoS 機能を拡張したものです。IP QoS 設定は、ルーティングの対象となる通常の VLAN 間トラフィックに適用されます。

IP QoS の設定は、以下の手順にしたがって行います。

1. 第 4 層のプロトコルを、TCP、UDP、all、other から選択して指定します。other* は、TCP/UDP 以外のプロトコルを意味します。

   * 「other」には、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）は含まれません。

2. 宛先の IP アドレスとネットマスクを指定します。オプションとして、宛先の TCP/UDP ポート番号も指定できます。TCP/UDP ポート番号を省略した場合は、すべての TCP/UDP ポートがグループ化の対象になります。
3. オプションとして、送信元の IP アドレスと TCP/UDP ポート番号を指定します。
4. 他のトラフィックグループと同じように、QoS プロファイルか `blackhole` オプションを指定します。QoS の設定は、`show ipqos` コマンドで確認できます。
5. 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 コマンドの構文をわかりやすくまとめると次のようになります。

config ipqos [add | delete] { 第 4 層プロトコル } [宛先ネットワーク] { 宛先 TCP/UDP ポート番号 } { 送信元 IP アドレス } { 送信元 TCP/UDP ポート番号 } [QoS プロファイル]

実際の構文は以下の例のとおりです。宛先ネットワークのマスクを `255.255.0.0` のようなドット区切り 10 進表記ではなく、マスクのビット長（例：`16`）で指定することに注意してください。IP アドレスとマスク長の間はスラッシュ（`/`）で区切ります。

たとえば、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 dst-ipport 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、次のようにします。

```
config ipqos add tcp 128.30.1.0/26 dst-ipport 23 blackhole
```

IP QoS プロファイル "blackhole"

IP QoS トラフィックグループ（宛先ネットワーク、TCP/UDP ポート番号、送信元 IP アドレスなど）に対して、特殊な QoS プロファイル "*blackhole*" を割り当てることができます。*blackhole* プロファイルを割り当てられたトラフィックは転送されずに破棄されます。このプロファイルを使えば、ネットワークやホスト、アプリケーション単位でトラフィックのフィルタリングが可能です。IP QoS の適用対象はルーティングの対象となる通常の VLAN 間トラフィックであり、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。

ポートキューモニタ（PQM）

本製品は、ポートごとに 4 つのキューを持っています。Ingress モードでは、4 つのデフォルト QoS プロファイルに、それぞれ 1 つずつキューが割り当てられます（*qp1* ＝第 1 キュー、*qp2* ＝第 2 キュー、といった具合）。Egress モードにおける QoS プロファイルとキューの関係は、環境によって異なります。

ポートキューモニタ（PQM）は、各ポートのキューを監視するためのユーティリティです。PQM を使えば、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。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。

表 8-3 に PQM コマンドの一覧を示します。

表 8-3: PQM コマンド

コマンド名	機能
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。**

QoS の設定

表 8-4 に QoS の設定に使うコマンドの一覧を示します。

表 8-4: 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。
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` − 最小限保証される帯域幅をパーセントで指定します。デフォルト値は 0 です。 ■ `maxbw` − 使用可能な最大帯域幅をパーセントで指定します。デフォルト値は 100 です。 ■ `priority` − サービスを受け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。デフォルト値は low です。Egress モードでのみ有効です。
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。
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。
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。
config ipqos [add | delete] {all | TCP | UDP | other} [<destination_ipaddress> <mask>] {dst-ipport <ipport>} {<source_ipaddress>} {src-ipport <ipport>} [qosprofile <qosname> | blackhole]	IP アドレスに QoS プロファイルを割り当てます。

Ingress モードにおける QoS 設定例

次の例では、デフォルト QoS プロファイル *qp4* の帯域幅設定を変更し、VLAN *Sales* に割り当てています。Ingress モードでデフォルト QoS プロファイルを変更するときは、指定する必要があるにもかかわらず priority パラメータは無視されます。

```
config qosprofile qp4 minbw 15% maxbw 100% priority high
config vlan sales qosprofile qp4
```

Egress モードにおける QoS 設定例

次に示すのはEgressモードにおけるQoS設定例です。ここでは、次の設定を行っています。

- スイッチの QoS モードを変更します。
- QoS プロファイル *mktgqos* を作成し、パラメータを以下のように設定します。
  - 最小帯域幅 = 0%
  - 最大帯域幅 = 10%
  - 優先度 = low
- QoS プロファイル *mktgqos* を、一定範囲の IP アドレスに適用します。

上記の設定は、以下の手順にそって実行します。

1. QoS モードを Egress モードに変更します。

   config qosmode egress
2. スイッチを再起動します。
3. QoS プロファイル *mktgqos* を作成し、パラメータを変更します。

   create qosprofile mktgqos

   config qosprofile mktgqos minbw 0% maxbw 10% priority low
4. 作成した QoS プロファイルを、一連の IP アドレスに関連付けます。

   config ipqos add 128.1.0.0/16 qosprofile mktgqos

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> | all}
```

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 ipqos`

  IP QoS テーブルを表示します。

QoS プロファイルの削除

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>
```

このコマンドは、Egress モードでのみ使用できます。

9 IP ユニキャストルーティング

この章では、IP ルーティングの設定方法について説明します。ここでは、読者の皆様がすでに IP ルーティングに精通しておられるものと仮定して話を進めます。IP ルーティングについてよくご存知ない方は、以下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 章をご覧ください。

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も選択できます。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。

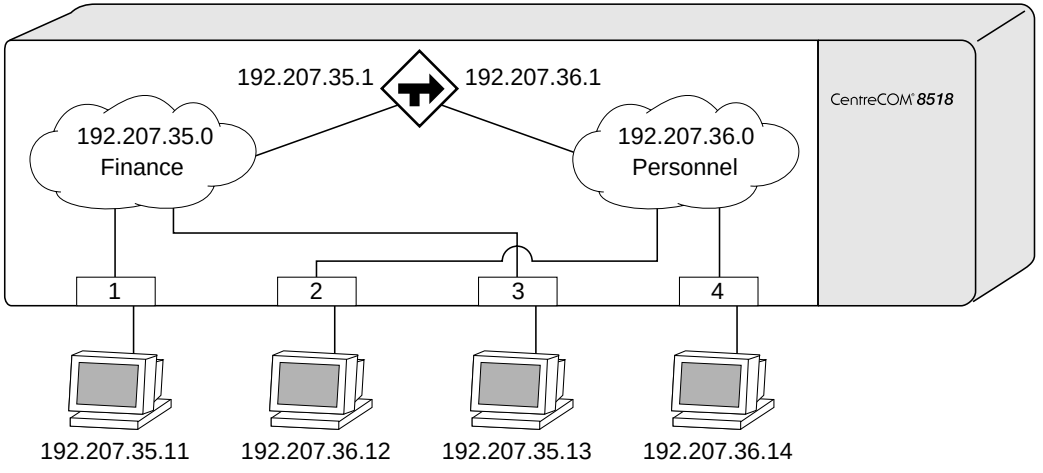

図 9-1: VLAN 間ルーティング

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 exportstatic
[enable | disable] ospf exportstatic type <value>
```

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。

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、ネットマスクの最も長い経路が選択されます。ネットマスクも等しい場合は、以下の基準にしたがって経路選択が行われます。上位のものほど優先されます。

- 直接接続されたネットワークインタフェース
- ICMP リダイレクト（表 9-3 を参照）
- スタティックルート
- アクティブではないが直接接続されたネットワークインタフェース

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。

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定義することができます。

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。

IP セグメント間での Proxy ARP

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ることができます。

たとえば、ホスト A に、クラス B の IP アドレス 100.101.102.103 とサブネットマスク 255.255.0.0 が設定されているとします。本製品のルータインタフェースには、IP アドレス 100.101.102.1、ネットマスク 255.255.255.0 が設定されており、Proxy ARP テーブルには、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 IP アドレス 100.101.45.67 のホスト B 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（100.101.0.0/16）上にあるものと認識して、ARP 要求パケットを送信します。この場合、本製品がホスト B の代理としてこの要求に応答しますが、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 に送られます。

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。
- RIP を使用できる VLAN は 1 つだけ。この VLAN は IP プロトコルを使用しなくてはならない。

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。

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 default delete ports 2
```

3 ダミープロトコルを作成します。

```
create protocol mnet
```

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 net21
create vlan net22
```

5 各 VLAN に IP アドレスを割り当てます。

```
config net21 ipaddress 123.45.21.1 255.255.255.0
config net22 ipaddress 192.24.22.1 255.255.255.0
```

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 net21 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 net22 protocol mnet
```

8 サブネットを物理ポート 2 に割り当てます。

```
config net21 add ports 2
config net22 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 RIP を使用するときは、ダミー VLAN の RIP をディセーブルにします。

```
config rip delete net22
```

IP マルチネットの作成例

以下に、IP マルチネット機能を使って、物理ポート 5 の下に 3 つの論理サブネット（192.67.34.0、192.67.35.0、192.67.37.0）を作成した例を示します。

```
config default delete ports 5
create protocol mnet
create vlan net34
create vlan net35
create vlan net37
config net34 ipaddress 192.67.34.1
config net35 ipaddress 192.67.35.1
config net37 ipaddress 192.67.37.1
config net34 protocol ip
config net35 protocol mnet
config net37 protocol mnet
config net34 add ports 5
config net35 add ports 5
config net37 add ports 5
enable ipforwarding
enable multinetting
```

次の例では、マルチネット機能を使って、物理ポート 5 の下に 3 つの論理サブネット（192.67.34.0、192.67.35.0、192.67.37.0）を作成し、さらに物理ポート 8 ～ 10 の下に 2 つの論理サブネット（192.67.36.0 と 192.99.45.0）を作成しています。両方のマルチネットセグメントとも RIP がイネーブルになっています。

```
config default delete ports 5
create protocol mnet
create vlan net34
create vlan net35
create vlan net37
config net34 ipaddress 192.67.34.1
config net35 ipaddress 192.67.35.1
config net37 ipaddress 192.67.37.1
config net34 protocol ip
config net35 protocol mnet
config net37 protocol mnet
config net34 add ports 5
config net35 add ports 5
config net37 add ports 5
config default delete ports 8-10
create vlan net36
create vlan net45
config net36 ipaddress 192.67.36.1
config net45 ipaddress 192.99.45.1
config net36 protocol ip
config net45 protocol mnet
config net36 add ports 8-10
config net45 add ports 8-10
config rip delete vlan all
config rip add net34
config rip add net36
enable rip
enable ipforwarding
enable multinetting
```

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。

- 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 章をご覧ください。

- 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。

- 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。

- 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> | all}
  ```

- 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
  ```

1 台のスイッチ上で、RIP と OSPF を同時に使用することはできません。

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。

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。

表 9-1 に IP 関連の基本的な設定コマンドの一覧を示します。

表 9-1: 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> | all}	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。オプションを省略した場合は、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> | all}	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。オプションを省略した場合は、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。
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。

表 9-1: 基本的な IP 設定コマンド

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。
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。
disable bootprelay	DHCP/BOOTP リレー機能をディセーブルにします。
disable ipforwarding {vlan <name> | all}	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> | all}	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> | all}	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> | all}	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 9-2 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 9-2: 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。
config ipqos add <destination_address> <mask> qosprofile <qosname>	宛先 IP アドレスに QoS プロファイルを割り当てます。
config ipqos delete <destination_address> <mask> qosprofile <qosname>	宛先 IP アドレスから QoS プロファイルを削除します。
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。
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 9-3 に ICMP 設定コマンドの一覧を示します。

表 9-3: ICMP 設定コマンド

コマンド名	機能
enable icmp redirects {vlan <name> | all}	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> | all}	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。
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> | all]}	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> | all}	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> | all]}	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。

表 9-3: ICMP 設定コマンド

コマンド名	機能
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> | all]}	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。

ルーティング設定例

図 9-2 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

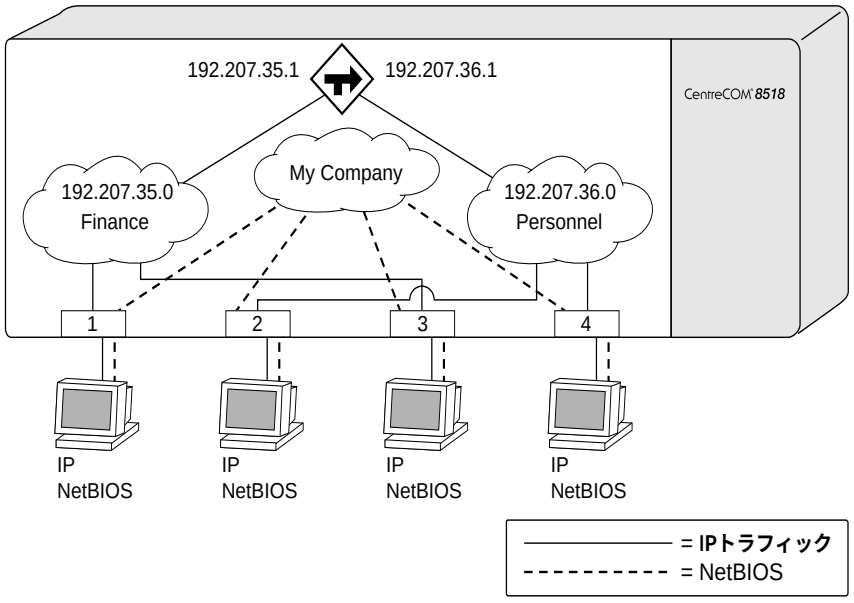

図 9-2: IP ユニキャストルーティングの設定例

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 9-2 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 Finance protocol ip
config Personnel protocol ip

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

```
config Finance ipaddress 192.207.35.1
config Personnel ipaddress 192.207.36.1
enable ipforwarding
enable rip
```

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 9-4 のコマンドを使用します。

表 9-4: 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> | all}	Proxy ARP テーブルを表示します。
show ipconfig {vlan <name> | all}	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 {<destination_address> <mask> | all}	IP QoS テーブルを表示します。
show ipstats {vlan <name> | all}	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> | all | 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> | all}	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。

表 9-4: 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 iproute {vlan [<name> | all] | permanent | <ipaddress> <mask>}	IP ルーティングテーブルを表示します。

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 9-5 のコマンドを使用します。

表 9-5: 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> | all}	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> | all}	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> | all}	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> | all]}	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> | all}	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> | all}	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 irdp {vlan [<name> | all]}	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。

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、以下の文献を参考にしてください。

RFC 1058 — *Routing Information Protocol (RIP)*
RFC 1256 — *ICMP Router Discovery Messages*
RFC 1723 — *RIP Version 2*
RFC 2178 — *OSPF Version 2*

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。

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、マルチプロトコル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。

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。

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、内部ルータおよびエリア境界ルータとして使用可能です。

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。

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。

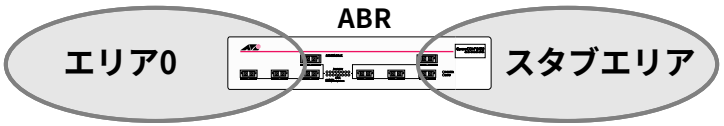

図 10-1: スタブエリア

バーチャルリンク

バックボーンエリアと直接接続されていないエリアでは、バーチャルリンクが使用されます。バーチャルリンクは、バックボーンの ABR と離れた場所にあるエリアの ABR の間を、共通のエリアを使って結ぶものです。図 10-2 にバーチャルリンクの例を示します。

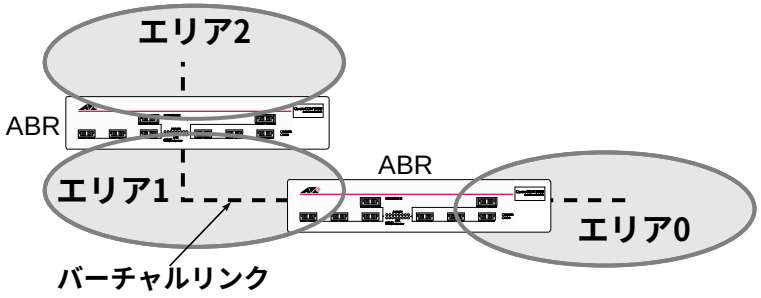

図 10-2: スタブエリアとバックボーンを結ぶバーチャルリンク

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。

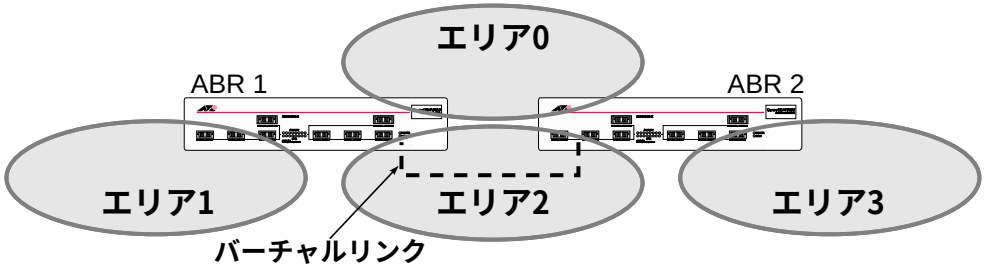

図 10-3: バーチャルリンクによる冗長構成

RIP 設定コマンド

表 10-1 に RIP 設定コマンドの一覧を示します。

表 10-1: 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。 デフォルトはイネーブルです。
enable rip exportstatic	RIP によるスタティックルートの広告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 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。

表 10-1: RIP 設定コマンド

コマンド名	機能
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。
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 10-4 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

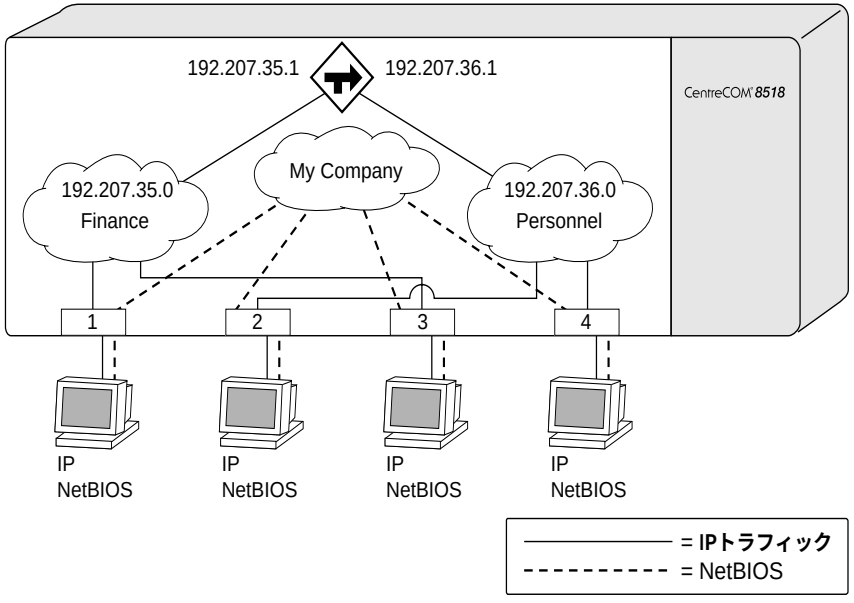

図 10-4: RIP 設定例

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 トラフィックはポート VLAN 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 10-4 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 Finance protocol ip
config Personnel protocol ip

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

config Finance ipaddress 192.207.35.1
config Personnel ipaddress 192.207.36.1

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

RIP 設定内容の確認

表 10-2 に RIP 設定内容を確認するためのコマンドを示します。

表 10-2: RIP 設定確認用コマンド

コマンド名	機能
show rip {vlan <name> | all}	**指定した VLAN の RIP 設定と統計を表示します。**
show rip stats {vlan <name> | all}	**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**

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 10-3 のコマンドを使います。

表 10-3: 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 exportstatic	ルートの広告をディセーブルにします。
unconfig rip {vlan <name> | all}	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。

OSPF 設定コマンド

表 10-4 に OSPF 設定コマンドの一覧を示します。

表 10-4: 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 exportstatic type [1 | 2]	ルートを他のOSPFルータに広告します。デフォルト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 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。
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 − 対向するルータインタフェースの ID 番号です。 ■ 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 以外となります。

表 10-4: OSPF 設定コマンド

コマンド名	機能
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。デフォルトは normal です。
config ospf area <areaid> add range <ipaddress> <mask> [advertise | noadvert]	指定した範囲の IP アドレスを OSPF エリアに追加します。advertise オプションを指定した場合、指定したアドレスは、ABR によって単一の要約リンク広告としてエクスポートされます。
config ospf area <areaid> delete range <ipaddress> <mask>	指定範囲の IP アドレスを OSPF エリアから削除します。
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。
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**

OSPF 設定例

図 10-5 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。

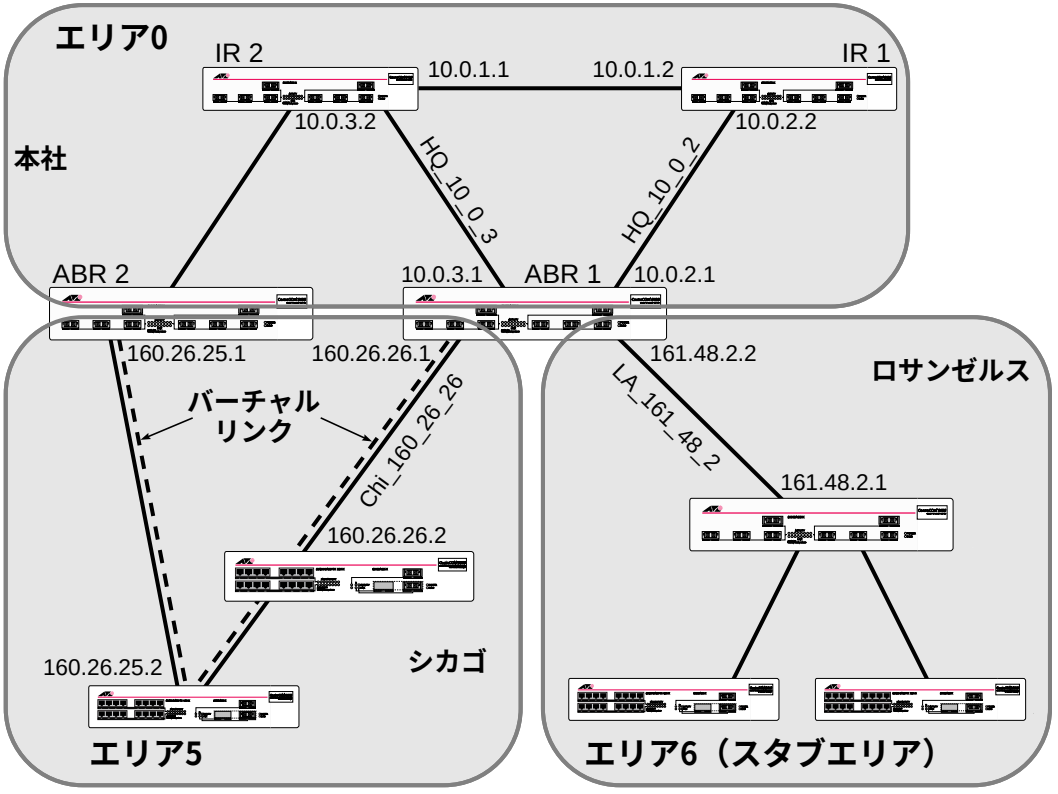

図 10-5: OSPF 構成例

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
- VLAN は 2 個（*HQ_10_0_2* と *HQ_10_0_3*）

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
- VLAN は 1 個（*Chi_160_26_26*）
- 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ルータ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
- VLAN は 1 個（*LA_161_48_2*）
- 内部ルータは 3 個
- エリア間ルーティングにはデフォルトルートを使う。

図 10-5 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の節で示します。

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_2

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_2 ipaddress 160.26.2.1 255.255.255.0

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_2 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
```

OSPF 設定内容の確認

OSPF の設定内容を確認するには、表 10-5 のコマンドを使います。

表 10-5: 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> | all}	指定した OSPF エリアの情報を表示します。
show ospf interfaces {vlan <name> | area <areaid> | all}	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 | all]	リンクステートデータベースの内容を表示します。エリア ID、ルータ ID、リンクステート ID のいずれかによる表示項目のフィルタリングが可能です。デフォルトは `all`（detail なし）です。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。

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 10-6 のコマンドを使用します。

表 10-6: OSPF のディセーブル / リセット用コマンド

コマンド名	機能
config ospf delete vlan [<name> | all]	指定した VLAN（ルータインタフェース）で OSPF をディセーブルにします。
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 exportstatic	ルートの広告をディセーブルにします。

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、RFC 1112、RFC 1075、RFC 2236 等の文献を参照してください。

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 ＝ Distance Vector Multicast Routing Protocol、ディスタンスベクタマルチキャストルーティングプロトコル）
- 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手段（例：IGMP ＝ Internet Group Management Protocol、インターネットグループ管理プロトコル）

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の prune と graft を行うメカニズムが備わっています。

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、そのグループがまだ活動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 スヌーピングを使用すれば、マルチキャストパケットの無駄な伝達を防ぎ、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。

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。

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 章と第 10 章をご覧ください。

- 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> | all}
  ```

- IP インタフェース（VLAN）単位で DVMRP をイネーブルにします。

  ```
  config dvmrp add vlan [<name> | all]
  ```

- ルータの DVMRP 設定をイネーブルにします。

  ```
  enable dvmrp
  ```

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 ipmcforwarding {vlan <name> | all}	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。キーワード `all` を指定した場合は、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。
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。

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> | all}	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。
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 − 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 − 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 − 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 − 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 − 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。

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。

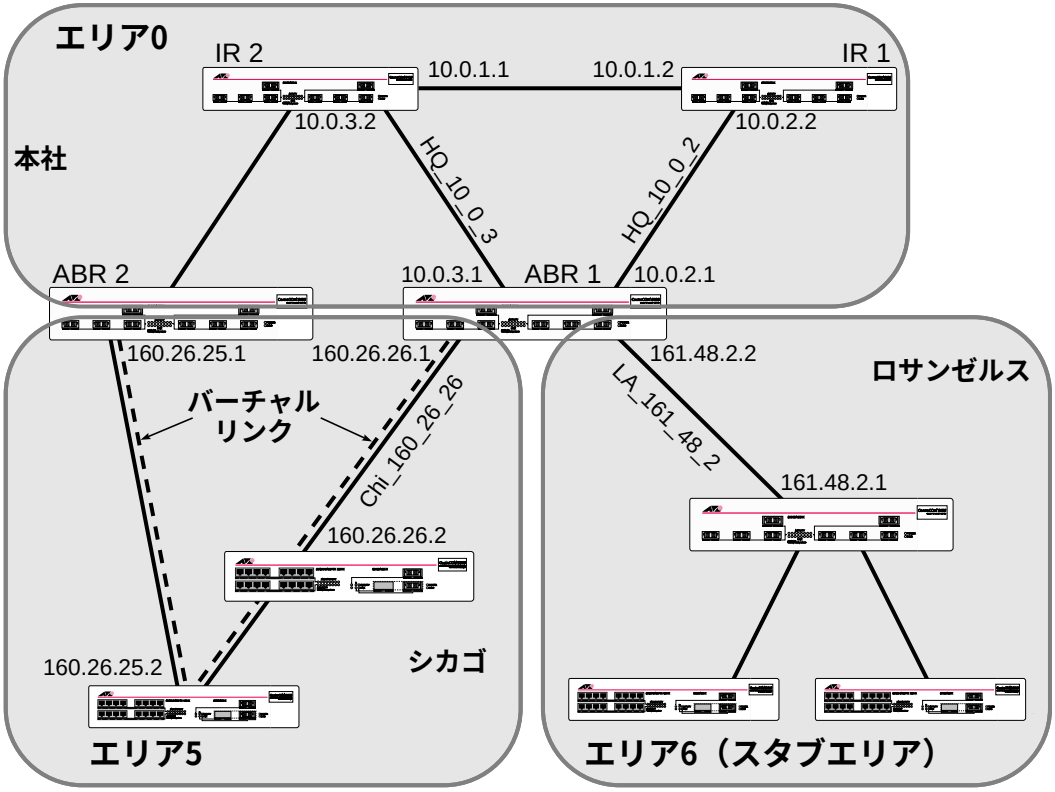

図 11-1: IP マルチキャストルーティングの設定例

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
```

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} | all}	**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、`all` を指定したものとみなされます。**
show igmp snooping {vlan <name> | all}	**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**

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> | all}	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> | all}	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。
unconfig dvmrp {vlan <name> | all}	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。
clear igmp snooping {vlan <name> | all}	IGMP スヌーピングのエントリを削除します。
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。

12 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。

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 12-1 に、show コマンドの一覧を示します。

表 12-1: ステータス表示コマンド

コマンド名	機能
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 dvmrp {vlan <name> | route {detail} | all}	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、all を指定したものとみなされます。

表 12-1: ステータス表示コマンド

コマンド名	機能
show fdb {all | <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。
show igmp snooping {vlan <name> | all}	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> | all | 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> | all}	Proxy ARP テーブルを表示します。
show ipconfig {vlan <name> | all}	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> | all}	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 {<destination_address> <mask> | all}	IP QoS テーブルを表示します。

表 12-1: ステータス表示コマンド

コマンド名	機能
show iproute {vlan [<name> | all] | permanent | <ipaddress> <mask>}	IP ルーティングテーブルを表示します。
show ipstats {vlan <name> | all}	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 log {<priority>} {<subsystem>}	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、warning、info のいずれかを指定します。省略時はすべてのメッセージが表示されます。 ■ `subsystem` − ここで指定したサブシステムに関連するメッセージだけを表示します。subsystem には、任意のサブシステム（system、snmp、bridging、ports など）を指定します。省略時はすべてのメッセージが表示されます。
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> | all}	指定したエリアの OSPF 情報を表示します。
show ospf interfaces {vlan <name> | area <areaid> | all}	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。

表 12-1: ステータス表示コマンド

コマンド名	機能
show ospf lsdb {detail} area [<areaid> | all] [router | network | summary_net | summary_asb | as_external | all]	リンクステートデータベースの内容を表示します。エリア ID、ルータ ID、リンクステート ID のいずれかによるフィルタリングが可能です。デフォルトは `all`（detail なし）です。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 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。

表 12-1: ステータス表示コマンド

コマンド名	機能
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> | all}	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> | all}	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 rip {vlan <name> | all}	指定した VLAN の RIP 設定と統計を表示します。
show rip stats {vlan <name> | all}	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 stpd {<stpd_name> | all}	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。

表 12-1: ステータス表示コマンド

コマンド名	機能
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 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> | all}	VLAN 情報を表示します。キーワード `all` を指定するかオプションを省略した場合は、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。

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

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

show ports コマンドの表示切り替えキー

表 12-2 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 12-2: 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
「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

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** ― イベントの重要度に応じて表 12-3 に示す 3 つのレベルのいずれかが記録されます。

表 12-3: イベントレベル

レベル	説明
CRIT (Critical)	正常運用に必要な機能が停止しています。再起動の必要があるかもしれません。
WARN (Warning)	機能障害につながる可能性のある（それほど深刻ではない）エラーを示します。
INFO (Informational)	エラーや障害ではない通常のイベントを示します。

- **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 12-4 にサブシステムの一覧を示します。

表 12-4: 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。
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>} {<subsystem>}
```

オプションは次のとおりです。

- `priority` ― 指定したレベル以上のエントリだけを表示します。critical、warning、info のいずれかを指定できます。デフォルトは、info です。
- `subsystem` ― 指定したサブシステムに関するエントリだけを表示します。syst、snmp、bridging、telnet、ports など、任意のサブシステムを指定してください。デフォルトではすべてのサブシステムに関するエントリが表示されます。

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>} {<subsystem>}
```

`priority` を指定しなかった場合は、critical レベルのメッセージのみが表示されます。`subsystem` を指定しなかった場合は、すべてのサブシステムに関するメッセージが表示されます。

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。

- 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。
- 本製品側で、次のコマンドを実行します。

  ```
  enable syslog
  ```

- 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>} {<subsystem>}
  ```

指定するパラメータは以下のとおりです。

- `ipaddress` ― syslog ホストの IP アドレス
- `facility` ― syslog の local facility level。`local0` ～ `local7` を使用できます。
- `priority` ― 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、warning、info のいずれかを指定できます。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。
- `subsystem` ― ここで指定したサブシステムに関するエントリだけを syslog ホストに送信します。syst、snmp、bridging、telnet、ports など、任意のサブシステムを指定してください。デフォルトでは、すべてのサブシステムに関するエントリが 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。

ログ関連コマンド

表 12-5 にログ関連コマンドの一覧を示します。

表 12-5: ログ関連コマンド

コマンド名	機能
config log display {<priority>} {<subsystem>}	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` − 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、warning、info のいずれかを指定します。デフォルトは info です。 ■ `subsystem` − ここで指定したサブシステムに関連するメッセージだけを表示します。syst、snmp、bridging、ports など、任意のサブシステムを指定してください。デフォルトでは、すべてのサブシステムに関するメッセージが表示されます。
config syslog <ipaddress> <facility> {<priority>} {<subsystem>}	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` − syslog ホストの IP アドレス ■ `facility` − syslog の local facility level ■ `priority` − 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、warning、info 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。 ■ `subsystem` − ここで指定したサブシステムに関連するメッセージだけをsyslogホストに送信します。syst、snmp、bridging、ports など、任意のサブシステムを指定してください。デフォルトでは、すべてのサブシステムに関するメッセージが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 12-5: ログ関連コマンド

コマンド名	機能
show log {<priority>} {<subsystem>}	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、warning、info のいずれかを指定します。デフォルトは info です。 ■ `subsystem` − ここで指定したサブシステムに関連するメッセージだけを表示します。syst、snmp、bridging、ports など、任意のサブシステムを指定してください。デフォルトでは、すべてのサブシステムに関するメッセージが表示されます。
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。

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。

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 とスイッチ

RMON では、LAN セグメントごとにプローブが必要となりますが、通常、専用の RMON プローブはたいへん高価です。そこで当社は、スイッチに低価格の RMON プローブを組み込む戦略をとりました。これにより、通常のネットワーク管理コストの範囲内で RMON を広く利用できるようになります。本製品では、全ポート回線速度で RMON 統計を正確に維持します。

統計はポートごとに行うことが可能です。プローブはすべてのトラフィックを監視する必要があるため、専用プローブの場合はセキュリティ機能のないポートに接続しなくてはなりませんが、本製品の内蔵プローブではすべてのポートでセキュリティ機能を使用できます。

イベントアクション

表 12-6 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 12-6: 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、3-18 ページの「SNMP による管理」をご覧ください。

13 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。

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、14-2 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、3-12 ページの「IP パラメータの設定」をご覧ください。

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

Web インタフェースにアクセスする

Web インタフェースのデフォルトホームページ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。

```
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、3-8 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。

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 13-1 に複数選択の方法をまとめます。

表 13-1: 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。
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 ― 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 ― 設定に関する警告が表示されます。
- Error ― 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 ―「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。

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、14-2 ページの「設定の保存」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。

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。

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。

14 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。

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> <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>` にサーバの IP アドレスを、`<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。

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
```

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> <filename> {<time>} | cancel]
```

`<ipaddress>` には TFTP サーバの IP アドレスを、`<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> <filename>
```

`<ipaddress>` には TFTP サーバの IP アドレスを、`<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。

ファームウェア / 設定関連コマンド

表 14-1 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 14-1: 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 configuration <ipaddress> <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> <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> <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。

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 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。
- 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。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
```

コマンドラインインタフェース

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ないか確認してください。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。

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。

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。

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。

```
C9100:7 # config vlan marketing add ports 1,2
ERROR: Protocol conflict on port 5
```

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> | all}
```

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。

```
C9100:23 # 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。

```
C9100:26 # config vlan marketing add ports 1,2
```

VLAN 名

VLAN 名には次のような制限があります。VLAN 名に使用できる文字は基本的に英数字のみです。スペースやコンマを使うことはできません。また VLAN 名の先頭はアルファベットで始まら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 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。

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 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 シリーズ（以下、本製品）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 B-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

C 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） VCC! 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**	**端末エミュレーション**
	SNMP (RFC 1157)	**Telnet (RFC 854)**
	MIB-II (RFC 1213)	**HTTP 1.0**
	Bridge MIB (RFC 1493)	**その他のプロトコル**
	Interfaces MIB (RFC 1573)	**UDP (RFC 768)**
	RMON MIB (RFC 1757)	**IP (RFC 791)**
	802.3 MAU MIB (RFC 2239)	**ICMP (RFC 792)**
	IP Forwarding MIB (RFC 1354)	**TCP (RFC 793)**
	Entity MIB (RFC 2037)	**ARP (RFC 826)**
	RIP2 MIB (RFC 1724)	**TFTP (RFC 1350)**
		BOOTP (RFC 1542)

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

D 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

G

I

L

M

O

P

Q

れ

ろ

コマンド索引

D

E

H

L

P

R

S

T

U