Junos®ファブリックおよびスイッチングテクノロジーシリーズ

Day One：EXシリーズ イーサネットスイッチの設定

著者：ヨン・キム、デビッド・グエン

JUNIPER NETWORKS

出版：Juniper Networks Books
著者：デビッド・グエン
編集長：パトリック・エイムズ
編集および校正：ナンシー・ケルベル
Junos プログラムマネージャ：キャシー・ガデッキ

ISBN：978-1-936779-14-7（印刷）
印刷：Vervante Corporation（米国）
ISBN：978-1-936779-15-4（電子書籍）

改訂：第 3 版、2011 年 1 月
4 5 6 7 8 9 10　　#7100127

著者の紹介
デビッド・グエンは、ファブリックおよびスイッチングテクノロジーの技術マーケティングエンジニアです。ジュニパーネットワークスへの入社前に、Spirent Communications 社でシステムエンジニアとして、また Cisco Systems 社で顧客サポートエンジニアとしての経験があります。

著者の謝辞
本書の制作にご協力いただいた多くの方々に感謝を申し上げます。第一に、Day One シリーズに貢献する機会を与えてくれたキャシー・ガデッキ氏およびパトリック・エイムズ氏にお礼を申し上げます。また、クリス・スペイン氏およびジョゼフ・リー氏には、意見および指導を賜りました。最後に、クリスティ・カルデロン氏およびレニー・ボンサル氏に感謝いたします。彼らの助けがなければ、本書が実現することはなかったでしょう。

本書は、さまざまな形式で www.juniper.net/dayone から入手できます。

皆様のご意見、ご要望、ご批判を電子メールで dayone@juniper.net までお送りください。

Twitter で Day One シリーズをフォローする：@Day1Junos

本書を読む前に知っておくべきこと

本書を読む前に、Junos オペレーティングシステムの基礎を理解しておいてください。具体的には、設定を変更したり、コマンドライン階層内を移動したりできる必要があります。*『Junos 基本シリーズ』*（www.junper.net/dayone）のその他の Day One ブックレット、*ジュニパーネットワークス技術ライブラリ*（www.juniper.net/books）で紹介されている優れた書籍、Junos およびその動作に関する参考資料（www.juniper.net）を参照することにより、必要な予備知識を身に付けることができます。

この他、本書を読み進めるうえで以下の知識が重要になります。

- ✓ TCP/IP について理解していること。
- ✓ ブリッジング、スパニングツリープロトコルなど基本的なスイッチング概念について理解していること。
- ✓ Junos オペレーティングシステムが稼働するデバイスにおけるインタフェース命名に精通していること。
- ✓ 必須ではありませんが、EX シリーズ デバイスを実際に使用しながら読み進めると、以降のページで説明するさまざまなシナリオの設定を練習できるため、ネットワークへの EX シリーズ デバイスの実装時間を短縮することができます。

本書の学習目標

- ✓ Junos コマンドラインインタフェース（CLI）を使用した EX シリーズの管理
- ✓ さまざまな接続方法を使用した主なバーチャルシャーシ構成の設定と、バーチャルシャーシ構成の設計に関する重要な考慮事項の理解
- ✓ LAG（リンクアグリゲーショングループ）の設定
- ✓ レイヤー 2 スイッチングおよびレイヤー 3 ルーティングの設定
- ✓ リモートアクセスを可能にするための基本的な IP 接続および要素の設定
- ✓ 基本的なスタティックルーティングの設定
- ✓ 音声 VLAN、L2 セキュリティ（DHCP スヌーピング、Dynamic ARP Inspection など）、その他のレイヤー 2 固有の機能など、さまざまなイーサネットスイッチングオプションの設定
- ✓ イーサネット OAM、MVRP、マルチキャスト、EZQOS-Voice、ポートミラーリングなど、EX シリーズの主な機能の設定

EX シリーズ イーサネットスイッチ

EX シリーズ イーサネットスイッチという名称は、読み上げるには長い名前です。また、Junos デバイスは、ネットワーキングの用途に応じて設計された多様なプラットフォームで提供されており、EX シリーズ イーサネットスイッチには、小規模なものもあれば大規模なものもあります。

本書では、簡潔に示すために、これらを総称して EX と呼びます。

注　EX シリーズ イーサネットスイッチの一部の機能は、プラットフォームによって設定が異なります。本書では、この違いを指摘するよう努めています。

第1章

EXシリーズの概要

ジュニパーネットワークス EX シリーズ イーサネットスイッチは、キャンパス、支社、およびデータセンター環境向けの、パフォーマンスと拡張性に優れたソリューションです。EX シリーズにより、キャリアクラスの信頼性、セキュリティリスクの管理、ネットワークの仮想化、アプリケーションの制御、そして運用コストの軽減を実現する、経済性に優れた Junos® スイッチングソリューションを導入できます。

他のイーサネットスイッチの管理または運用経験がある方なら、ジュニパーネットワークス EX シリーズ イーサネットスイッチを違和感なく扱えるはずです。一方、イーサネットスイッチのセットアップが初めての方には、本書でこのプロセスを案内します。

EX シリーズは、以下のスイッチ製品シリーズで構成されています。

- エントリーレベルの EX2200 および EX2200-C シリーズ イーサネットスイッチ
- 固定構成の EX3200、EX3300、および EX4200 シリーズ イーサネットスイッチ
- EX4500 および EX4550 10GbE トップオブラック（TOR）/アグリゲーションイーサネットスイッチ
- モジュラー型 EX6200 および EX8200 スイッチ
- プログラム可能なシャーシ型 EX9200 スイッチ

EX2200、EX2200-C、EX3300、EX4200、EX4500、EX4550、および EX8200 スイッチはジュニパーネットワークスのバーチャルシャーシテクノロジーを搭載しています（詳細は第 2 章を参照）。本書では、EX4200 スイッチを中心に設定手順を説明します。

さらに詳しくは 各 EX シリーズの詳細については、この製品の参考資料（http://www.juniper.net/us/en/products-services/switching/ex-series/）を参照してください。

EX4200 イーサネットスイッチの探求

イーサネットスイッチを設定するために、最初のステップとして、デバイスの物理レイアウトを理解しましょう。EX4200 スイッチの背面パネル（図 1.1 を参照）には多数のポートがあります。

- コンソールポート：スイッチの設定は、RJ-45 コネクターを使用する背面パネルの RS-232 シリアルインタフェースから行えます。コンピュータをスイッチコンソールポートに直接接続し、ターミナルエミュレーションプログラムを使用して設定できます。この方法で設定する場合、ターミナルエミュレーションプログラム

のパラメータをボーレート 9600、データビット 8、パリティなし、ストップビット 1、フロー制御なし、に設定する必要があります。

- 管理ポート：背面パネルのコンソールポートの左側にある専用イーサネット RJ-45 ポートは、アウトバンド（OOB）スイッチ管理に使用できます。このポートでは、10/100/1000BASE-T 接続をサポートする自動認識 RJ-45 コネクターが使用されています。このポートの横にある 2 個の LED は、リンクの動作とポートのステータスを示します。スイッチ管理および運用管理を行うには、管理ポートに IP アドレスとサブネットマスクを設定する必要があります。
- USB ポート：フラッシュドライブなどのストレージデバイスは、背面パネルの USB ポートで EX4200 スイッチに直接接続できます。USB フラッシュドライブは、設定ファイルや Junos ソフトウェアリリースを保存およびアップロードするために使用できます。
- バーチャルシャーシポート（VCP）：背面パネルの 2 つのバーチャルシャーシポートにより、専用の 128Gbps 高速バーチャルバックプレーンを介して EX4200 スイッチを相互接続することができます。ワイヤリングクローゼット、トップオブラックデータセンターのアプリケーションなど至近距離に導入されたスイッチは、バーチャルシャーシケーブルで簡単に接続できます（第 2 章を参照）。

注 VCP では、EX4200 イーサネットスイッチを相互接続するために、特定のバーチャルシャーシケーブル（付属）を使用します。詳細については、*『Connecting a Virtual Chassis Cable to an EX4200 Switch Guide』*（www.juniper.net/techpubs）を参照してください。

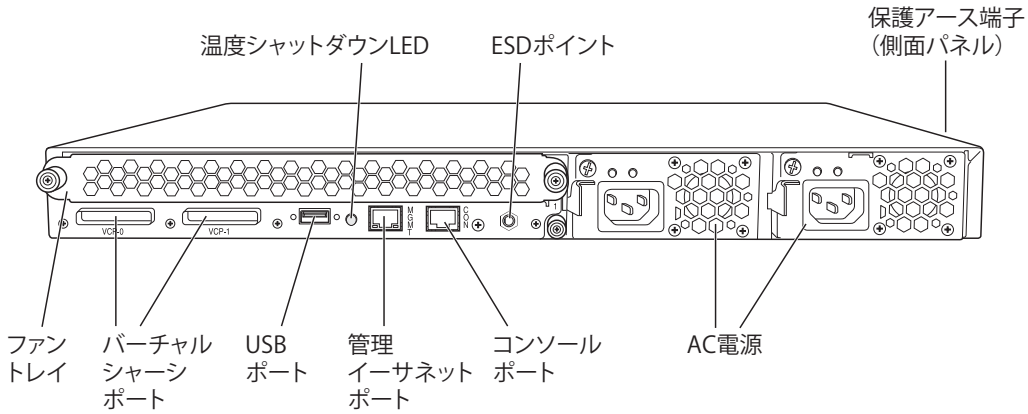


図 1.1 **EX4200 イーサネットスイッチの背面パネル**

EX4200 スイッチのフロントパネル（図1.2 を参照）には、LCD パネル、オプションのアップリンクモジュールベイ、最大 48 基のホストネットワークポートがあります。

- LCD パネル：バックライト式 LCD パネルには、起動プロセスの主なステージ、スイッチのホスト名、バーチャルシャーシ構成におけるスイッチのロール、スイッチの現在のステータスなど、スイッチに関するさまざまな情報が表示されます。また、スイッチの初期セットアップや再起動などの基本操作を実行するためのメニューも表示されます。
- LCD ボタンとステータス LED：LCD パネルの横にある LED およびボタンでは、スイッチのステータスを素早く判断したり、基本操作を実行したりできます。上側の *[Menu]* ボタンを押すと、さまざまな LCD パネルメニューが循環表示されます。下側の *[Enter]* ボタンでは、選択した内容を確定できます。LCD パネルの保守モードで使用するときも、[Enter] ボタンは確定機能として動作します。

さらに詳しくは

LCD パネルおよびボタンでは、スイッチを工場出荷時のデフォルト設定に戻したり、管理のためにコンピュータを使用せずにスイッチを再起動するなど、その他の目的にも役立ちます。 www.juniper.net/techpubs/ の「EX Switches」セクションから入手可能な『LCD Panel in EX3200/EX4200 Switches』を参照してください。

- LCD ボタンの横にあるステータス LED は、さまざまな色で点灯することによりスイッチのステータスを通知します。
- アップリンクモジュール：EX4200 スイッチの右下にあるスロットには、オプションのフィールド交換可能なユニット（FRU）である光インタフェースアップリンクモジュールを取り付けることができます。オプションのフロントパネルのアップリンクモジュールでは、SFP 光トランシーバ搭載のギガビットイーサネット（GbE）ポート 4 基、XFP 光トランシーバ搭載の 10GbE ポート 2 基、あるいはユーザーが設定可能な SFP+ 光トランシーバ搭載の 10GbE ポート 2 基または GbE ポート 4 基のオプションがサポートされ、ワイヤリングクローゼットと上流アグリゲーションスイッチ間に高速バックボーンまたはリンクアグリゲーション接続を確立することができます。
- ネットワークポート：EX4200 スイッチには、フロントパネルに 24 基または 48 基の 10/100/1000BASE-T イーサネットポートがあり、通常はここにホストを接続します。EX4200 シリーズスイッチには、100BASE-FX/1000BASE-X SFP 光ポート 24 基搭載モデルもあります。

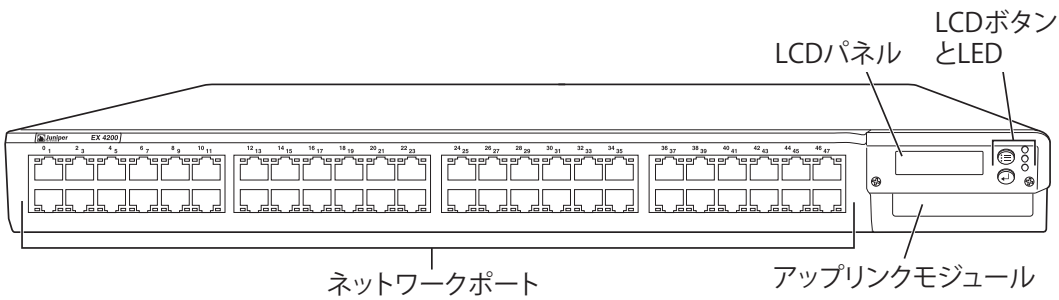


図 1.2 EX4200-48T イーサネットスイッチのフロントパネル

EX シリーズ イーサネットスイッチの管理

EX シリーズは、Junos コマンドラインインタフェース（CLI）、またはジュニパーネットワークスのウェブデバイスマネージャ（J-Web）などのウェブベースのインタフェースで管理できます。CLI には、インバンドおよびアウトバンドの 2 つの方法でアクセスできます。一方の方法が必ずしも他方より優れているわけではなく、どちらを使用するかは個人の好みです。どちらの方法を使用する場合も、最初のステップではスイッチに接続してログインします（本書では、スイッチに電源が投入され、起動プロセスが完了しているものと想定）。

さらに詳しくは CLI 設定およびコマンドの詳細については、『*Day One: Exploring the Junos CLI*』で、ネットワークデバイスにログインするためのステップごとの手順を参照してください（www.juniper.net/dayone）。

インバンドマネージメント

フロントパネルのネットワークポートを使用して、スイッチをインバンドで管理および設定することができます。この方法の選択理由が便宜的なものか企業ポリシーに準拠するためかに関わらず、インバンドマネージメントには、フロントパネルでの最小限の設定が必要になります。

この方法では、別のネットワークサブネットを作成したり使用したりする必要はありません。ネットワークポートに割り当てられ、設定された IP アドレスを使用し、管理用コンピュータを接続するだけで済みます。インバンドマネージメントは、スイッチが正しく起動され、初期化され、設定されている場合のみ使用できます。

アウトバンドマネージメント

スイッチのアウトバンドマネージメントには、背面パネルのコンソールポートまたは管理イーサネットポートを使用して、スイッチをアウトバンドで管理することができます。コンソールポートを使用する場合、必要な作業は、コンピュータにターミナルエミュレーションソフトウェアをインストールし、コンソールアクセス用に正しく設定することのみです。

管理ポートを使用する場合は、インバンドマネージメントと同様に、有効な IP アドレスとサブネットマスクを必要とする最小限の設定を行わなければなりません。また、スイッチへのアクセスは、フロントパネルのインバンドネットワークポートではなく、アウトバンドポートを介して行います。アウトバンドマネージメントをどちらのポートで行う場合も、管理ポートに対して最小限の設定を行い、スイッチを正しく起動して初期化する必要があります。

ヒント デフォルトでは、EX シリーズのルートのユーザーログイン資格情報として、ユーザー名が使用され、パスワードはありません。デバイスの Junos パスワードの変更方法については、*『Day One：Junos の基本設定』*を参照してください（www.juniper.net/dayone）。

J-Web による管理

ジュニパーネットワークスのウェブデバイスマネージャ（J-Web）は、スイッチを管理するためのグラフィカルユーザーインタフェース（GUI）です。J-Web では、図 1.3 および図 1.4 に示すように、一般的なウェブブラウザーと同様にインタフェースのナビゲーション、ページのスクロール、要素の展開と折りたたみを行えます。

J-Web インタフェースから、現在の設定を確認するための CLI ビューワー、設定を表示および変更できる CLI エディター、使用可能なすべての CLI ステートメントをナビゲートできるポイントアンドクリック CLI エディターなど、Junos CLI から入手可能なすべてのタスクを実行できる GUI ツールを利用できます。

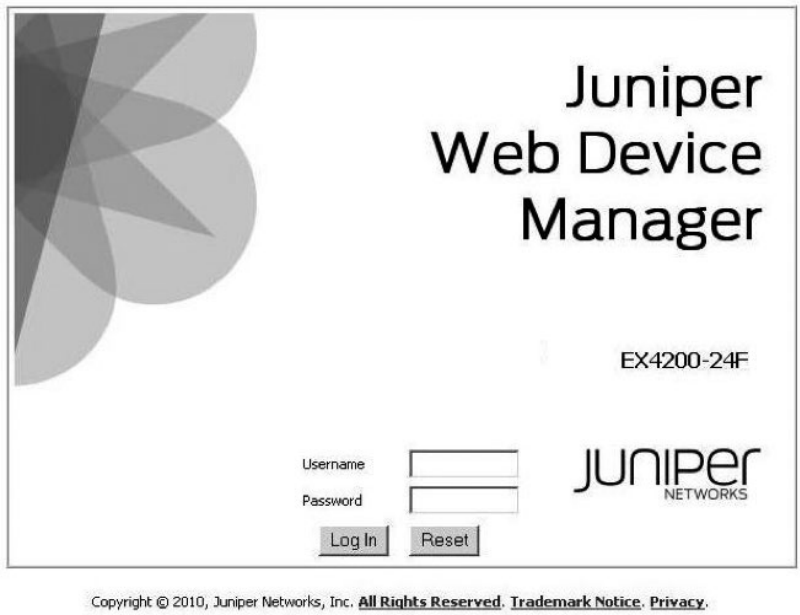


図 1.3　J-Web の初期ログイン画面

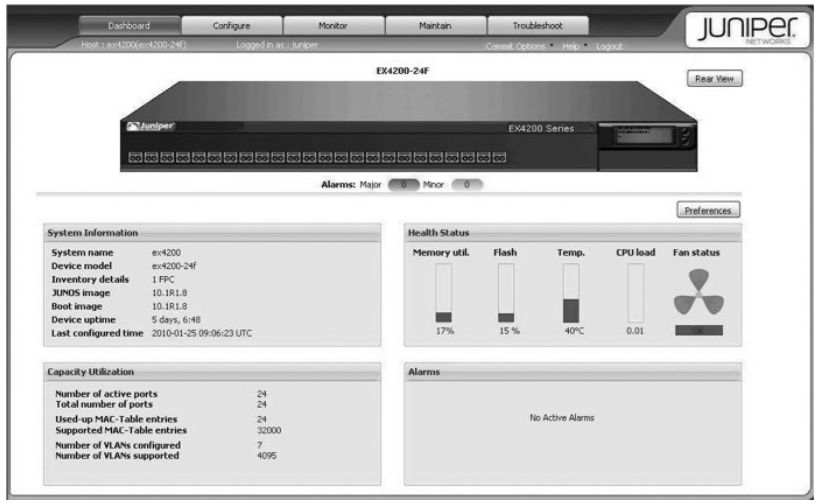


図 1.4　EX4200-24F スイッチのメイン J-Web 画面

さらに詳しくは Junos ウェブデバイスマネージャの詳細については、*『Connecting and Configuring an EX Series Switch J-Web Guide』*（www.juniper.net/techpubs/）を参照してください。

まとめ

この章では、EX スイッチのさまざまな管理方法について説明しました。先ほど述べたように、管理方法に良し悪しはなく、どの方法を使用するかは各自の好みで決めることができます。Junos では、EX シリーズイーサネットスイッチを複数の方法で初期設定し、導入できます。

ここで説明した内容は本書全般で使用することになりますが、この情報は、実際のネットワークに EX スイッチを配置し、設定する際にも役立ちます。

これで、スイッチがどのような外観をしているかが分かりました。次に、複数の EX スイッチをバーチャルシャーシとしてセットアップし、相互接続して 1 つの広帯域デバイスとして機能させる方法について説明します。

第2章

バーチャルシャーシの物理接続

ジュニパーネットワークス EX4200 シリーズ イーサネットスイッチには、バーチャルシャーシテクノロジーが搭載されています。このテクノロジーにより、最大 10 台の EX4200 スイッチを相互接続し、単一の広帯域デバイスとして運用することができます。スイッチ（バーチャルシャーシメンバー）は、各スイッチの背面パネルにある専用のバーチャルシャーシポート、オプションのアップリンクモジュールポート、または EX4200-24F スイッチにバーチャルシャーシポートとして設定されたフロントパネルの光 SFP ネットワークポートを介して相互接続できます。

バーチャルシャーシ構成で導入された EX4200 イーサネットスイッチは、1 つの論理デバイスとして管理および監視されます。このアプローチにより、ネットワークの運用が大幅に簡素化されます。また、導入場所が異なる物理デバイスであっても論理的にグループ化できるため、リソースを効率的に活用することができます。

この章では、バーチャルシャーシ構成をさまざまな接続方法で構築する方法を説明し、バーチャルシャーシ構成の設計に関する考慮事項を示します。

バーチャルシャーシ構成

EX4200 スイッチは、バーチャルシャーシ構成の一部としてさまざまな方法で導入できます。例えば、単一ラック内での構成、複数のラックにまたがる構成、単一のワイヤリングクローゼット内での構成、複数のフロアまたは建物に設置された複数のワイヤリングクローゼットにまたがる構成が可能です。

物理的なバーチャルシャーシ構成には 2 つのタイプがあります。1 つは「VCP（Virtual Chassis Port）構成」と呼ばれるもので、図 2.1 に示すように、専用のバーチャルシャーシポートケーブルで各スイッチの背面パネルのバーチャルシャーシポートへ接続することにより、隣接するスイッチが相互接続されます。

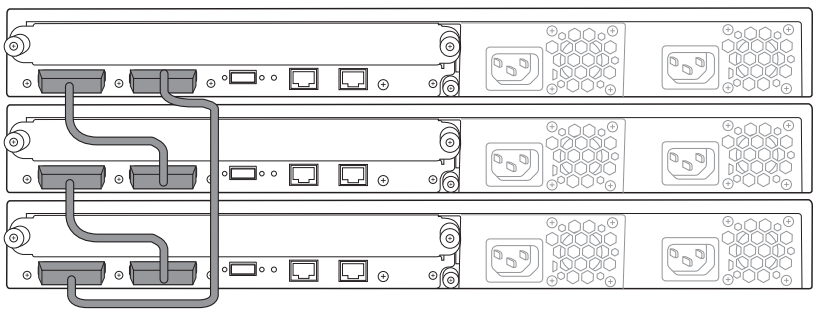


図 2.1　VCP 構成

バーチャルシャーシ構成は、オプションのアップリンクポートを使用するか、EX4200-24F スイッチのフロントパネルの光 SFP ネットワークポートをバーチャルシャーシポートとして設定して、直接接続されるメンバースイッチ間の距離を延長することによって拡張することも可能です。このように、GbE または 10GbE アップリンクポート、あるいはフロントパネルの光 SFP ネットワークポートを介して相互接続されたバーチャルシャーシ構成を「VCEP（Virtual Chassis Extension Port）構成」と呼びます。これを図 2.2 に示します。

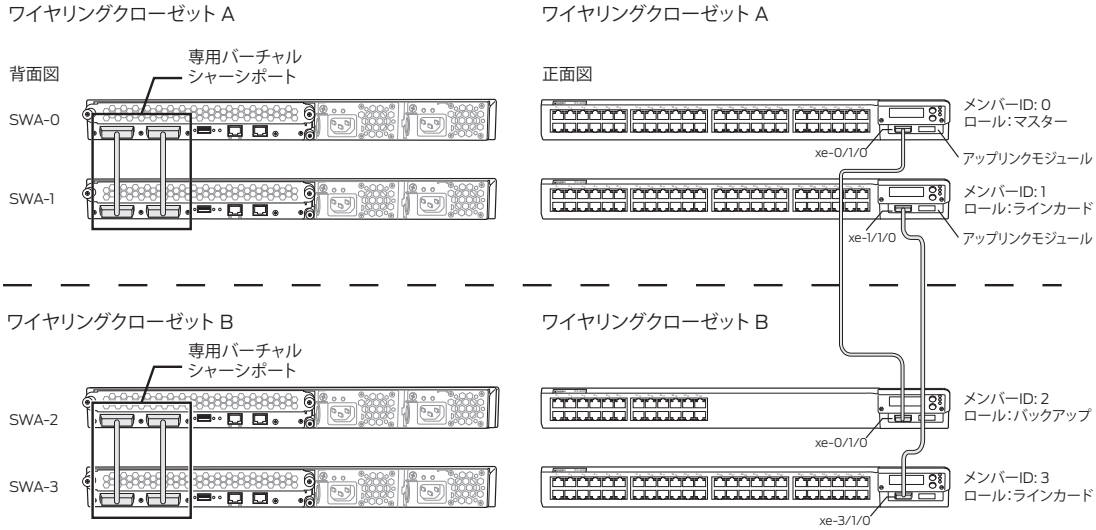


図 2.2 **VCEP 構成**

バーチャルシャーシ構成のメンバースイッチを相互接続するための基本的な配線オプションには、デイジーチェーンリング、ブレイデッドリング、および VCEP 構成があります。

ベストプラクティス　バーチャルシャーシテクノロジーでは、ケーブルをリング状に接続する必要はありません。ただし、障害許容力を実装するために、リング構成によって冗長性を担保することを強くお奨めします。

デイジーチェーンリング構成

デイジーチェーンリング構成では、バーチャルシャーシ構成の各メンバーを隣接するメンバーに接続し、バーチャルシャーシ構成の両端に位置するメンバーを長いバーチャルシャーシケーブルで相互接続する

ことによって、リングトポロジーを完成させます。図 2.3 に示すように、デイジーチェーンリング構成は、デバイスを相互接続する単純かつ直感的な方法です。

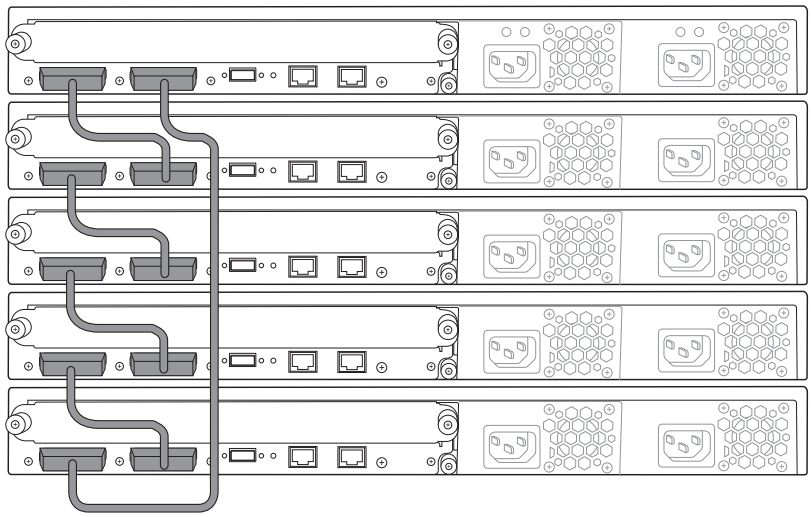


図 2.3　デイジーチェーンリング構成によるリングトポロジーの EX4200 バーチャルシャーシ構成

ブレイデッドリング構成

ブレイデッドリング配線方法では、図 2.4 に示すように、バーチャルシャーシポートケーブルによるバーチャルシャーシ構成がサポートされます。ブレイデッドリング配線では、バーチャルシャーシ構成のメンバーを互い違いに接続し、両端にある 2 つのメンバーを相互に直接接続することによって、リングトポロジーを完成させます。

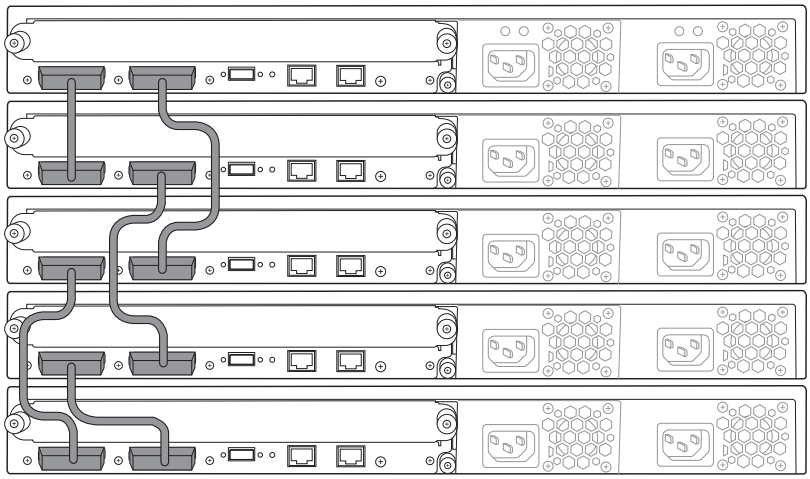


図 2.4 ブレイデッドリング構成の EX4200 のバーチャルシャーシ

VCEP 構成

バーチャルシャーシメンバーが地理的に広範囲に分散している VCEP 構成では、バーチャルシャーシメンバーをオプションの GbE または 10GbE アップリンクモジュール、あるいは EX4200-24F のフロントパネルにある光 SFP ネットワークポートを介して相互接続できます。バーチャルシャーシポートとして機能するようにポートを設定することにより、相互接続されたスイッチは同じバーチャルシャーシ構成のメンバーとして認識されます。また、複数のアップリンクを使用して VCEP 構成を相互接続し、帯域幅とパス冗長性を高めることもできます。

注 Junos 9.6 以降、複数の拡張バーチャルシャーシ接続を 1 つの論理グループにまとめ、バーチャルシャーシの帯域幅を高めることができるようになりました。

オプションの GbE または 10GbE アップリンクポートを拡張バーチャルシャーシポートとして設定するには、以下の CLI コマンドを使用します。

```
user@switch> request virtual-chassis vc-port set pic-slot <pic-slot> port <port>
member <member-id>
```

多様な環境に柔軟に対応できるようにするために、専用バーチャルシャーシ接続と拡張バーチャルシャーシ接続を組み合わせてバーチャルシャーシ構成を構築することも可能です。

バーチャルシャーシのポート番号

各 EX4200 スイッチの背面パネルには、VCP 0 および VCP 1 として指定された 2 つの専用バーチャルシャーシポートがあります。これらの専用ポートのインタフェースは、ポートに専用バーチャルシャーシポートケーブルを配線した時点で、デフォルトで動作します。バーチャルシャーシポートはポート番号に依存しません。例えば、VCP 0 を別のバーチャルシャーシスイッチメンバーの VCP 0 または VCP 1 のどちらにも相互接続できます。

バーチャルシャーシメンバーの各スイッチネットワークポートには、x/y/z という番号が割り当てられます。ここで、各記号の意味は以下のとおりです。

- x は、スイッチのメンバー ID です。
- y は、ポートインタフェースコントローラ（PIC）ID です。ネットワークポートは常に PIC 0 にあり、アップリンクモジュールポートは常に PIC 1 にあります。
- z は、アップリンクポートまたはネットワークポートの PIC におけるポート番号です。

例えば、0/1/3 というポート番号は、バーチャルシャーシ構成に属する最初のメンバースイッチ（0）のアップリンクモジュール（PIC ID 1）にある 4 番目のポート（ポート番号は 0 から始まるため）を示します。

```
user@switch> show interfaces ge-0/1/3
Physical interface: ge-0/1/3, Enabled, Physical link is Up
...
```

さらに詳しくは CLI 設定およびコマンドの詳細については、*『Day One:Exploring the Junos CLI』* で、ネットワークデバイスにログインするためのステップごとの手順を参照してください（www.juniper.net/dayone）。

バーチャルシャーシメンバーのロール

バーチャルシャーシ構成の各メンバーには、特定のロールが割り当てられ、そのロールによって実行する機能が決定されます。

バーチャルシャーシ構成では、1 つのメンバーにマスターすなわちルーティングエンジン（RE）ロールが割り当てられ、このメンバーは、バーチャルシャーシ構成に含まれる他のメンバーを管理する役割を担います。もう一つのメンバーにはバックアップロール（BK）が割り当てられ、

マスタースイッチが障害になった場合にマスターロールを引き継ぎます。その他すべてのメンバーには*ラインカード*ロール（LC）が割り当てられます。メンバーのロールは、システムで実行されるマスターシップ選出アルゴリズムによって決定されます。

さらに詳しくは バーチャルシャーシのマスターシップ選出アルゴリズムの詳細については、*『Understanding Virtual Chassis Components Guide』* を参照してください（www.juniper.net/techpubs/）。

マスターロール（RE）

バーチャルシャーシ構成のマスタースイッチは、以下の機能を実行します。

- バーチャルシャーシ構成のアクティブなルーティングエンジンとして動作します。
- バーチャルシャーシ構成のすべてのメンバースイッチを管理します。
- バーチャルシャーシ構成に対して Junos を実行します。
- シャーシ管理プロセスおよびネットワーク制御プロトコルを実行します。
- ルーティング情報を送受信します。
- すべてのメンバースイッチの代表となります（マスタースイッチに割り当てられたホスト名およびその他プロパティがバーチャルシャーシ構成のすべてのメンバーに適用される）。
- バーチャルシャーシ構成全体のアクティブなマスターコピーを保持します。

バックアップロール（BK）

バーチャルシャーシ構成でバックアップとして機能するメンバースイッチは、以下の機能を実行します。

- バーチャルシャーシ構成のバックアップルーティングエンジンとして動作します。
- マスタースイッチに障害がある場合にマスターロールを引き継げるように、マスタースイッチとの同期を保ちます。
- バーチャルシャーシ構成に対してバックアップロールで Junos を実行します。

- マスタースイッチのプロトコル状態、フォワーディングテーブル、およびその他の設定を同期し、マスタースイッチが使用不可になった場合に、中断なく、または最小限の中断で、ネットワーク接続性を維持できるように備えます。

ラインカードロール（LC）

ラインカードメンバースイッチは、以下の機能を実行します。

- バーチャルシャーシ構成に対してラインカードロールで Junos を実行します。
- マスタースイッチを通して設定されたすべてのインタフェースで、ケーブルが接続されていないなどスイッチのエラー状態を検出し、この情報をマスタースイッチに伝達します。
- マスタースイッチから送信された転送情報のアップデートを受信し、これらのアップデートを、トラフィックを転送するローカルの PFE（パケットフォワーディングエンジン）にプログラムします。
- バーチャルシャーシ構成のラインカードメンバーは、このロールで動作している間は、完全なネットワーク制御プロトコルを実行しません。ただし、マスターまたはバックアップスイッチが障害になった場合には、いずれかのラインカードスイッチがバックアップロールを引き継ぎます。

メンバースイッチとメンバー ID

各 EX4200 スイッチには、動的な導入シナリオでバーチャルシャーシ構成のメンバーになる資格があります。EX4200 スイッチは、電源が投入されると、メンバー ID を受け取ります。スタンドアロンスイッチとしてスイッチに電源が投入された場合は、そのメンバー ID は常に 0 になります。スイッチがバーチャルシャーシ構成の他のメンバースイッチと相互接続されると、そのスイッチがバーチャルシャーシ構成に追加された順序などさまざまな要因に基づいて、マスターによりメンバー ID（0 ～ 9）が割り当てられます。スイッチを追加して電源を投入するたびに、そのスイッチは次に使用可能な（未使用の）メンバー ID を受け取り、そのメンバー ID がフロントパネルの LCD に表示されます。

バーチャルシャーシ構成の既存のメンバースイッチが物理的に切断されるかバーチャルシャーシ構成から削除された場合、そのスイッチのメンバー ID は、自動的には、マスターによる標準的な連続番号割り当てに使用できるようになりません。例えば、バーチャルシャーシ構成からメンバー 1 が削除され、バーチャルシャーシ構成がメンバー 0、メンバー 2、およびメンバー 3 で構成されているとします。この状態

で別のメンバースイッチを追加して電源を投入すると、マスターによりこのスイッチにメンバー 4 が割り当てられます。

ただし、以下のコマンドを使用することにより、新しいメンバースイッチのメンバー ID を明示的に ID1 に変更することができます。

```
user@switch> request virtual-chassis renumber member-id 4 new-member-id 1
```

バーチャルシャーシの実装

バーチャルシャーシテクノロジーを実装する方法には、動的および事前プロビジョニングの 2 つがあります。

動的な方法では、単純なプラグアンドプレイでバーチャルシャーシ構成を構築できます。この方法に手動での設定は必要ありませんが、ユーザーがマスターおよびバックアップスイッチを選択することはできません。また、バーチャルシャーシ構成に誤ったスイッチを追加するなど、特定のユーザーエラーを防ぐことができません。

一方、事前プロビジョニングによる方法では、バーチャルシャーシ構成を導入する前に、あらかじめプランニングと手動での設定が必要になります。特定のバーチャルシャーシに属するすべてのメンバースイッチとそのロールを手動で設定する必要があるため、ユーザーエラーを最小限に抑え、メンバースイッチに障害が発生した場合でも、予め想定した確実な挙動を想定することができます。

ベストプラクティス　動的な方法は、スイッチに初めて電源を投入したときのデフォルト設定です。ただし、ユーザーエラーの可能性を最小限に抑え、動作の一貫性を最大限に高めるために、事前プロビジョニングによる方法を使用することをお奨めします。

動的な導入

動的な導入方法では、ユーザーがあらかじめ設定を行わなくても、バーチャルシャーシ構成を構築したり、既存のバーチャルシャーシ構成に新しいメンバーを追加したりできます。

動的な導入では、スイッチのマスターシップ優先度を 1 ～ 255 に設定することにより、バーチャルシャーシ構成でメンバースイッチが担うロール（マスター、バックアップ、またはラインカード）を指定できます。マスターシップ優先度値は、バーチャルシャーシ構成のマスターを選択するときに最も優先される要因です。EX4200 スイッチは、電源が投入されると、デフォルトのマスターシップ優先度値 128 を受け取ります。必須ではありませんが、マスタースイッチおよびバックアップスイッチのマスターシップ優先度を全メンバーの中で最高の値に設定することにより、これらのスイッチを指定することをお奨めします。

注 バーチャルシャーシのマスターシップ優先度値の範囲は0～255です。

また、マスターシップ優先度を割り当てるときは、マスタースイッチおよびバックアップスイッチに対して可能な限り高いマスターシップ優先度値（255）を設定することをお奨めします。この設定により、新しいメンバーがバーチャルシャーシ構成に追加されたときに、これらのメンバーが引き続きマスタースイッチおよびバックアップスイッチとして動作できます。また、マスタースイッチが使用不可になったときにも、マスターからバックアップへとスムーズに引き継ぐことができます。さらに、元のマスタースイッチがオンラインに戻ったときに、バックアップスイッチから制御を取り戻すことがありません。このような状況は*フラッピング*または*プリエンプション*と呼ばれ、システムの動作効率を低下させる原因になります。

工場出荷時の設定

スイッチが新品の状態でない場合、バーチャルシャーシ構成に追加する前に、*すべて*のバーチャルシャーシスイッチメンバーに工場出荷時の設定をロードすることをお奨めします。この手順により、新しいメンバーの追加時に、マスターが新たに再選出されたり現在の設定が消去されるなど、予測外の動作を防ぐことができます。

工場出荷時の設定は、以下のいずかの方法でロードできます。

1. 以下の設定モードの CLI コマンドを使用します。

```
user@switch# load factory-default
user@switch# set system root-authentication plain-password
```

次に、プロンプトに従ってルートパスワードを設定し、変更を適用します。

```
user@switch# commit
```

2. スイッチの LCD メニューを使用します。
   - [Maintenance Menu] が表示されるまで、LCD パネルの横にある [Menu] ボタンを押します。
   - [Enter] ボタンを押して、[Maintenance Menu] を選択します。
   - [Load Factory] メニューが表示されるまで [Menu] ボタンを押します。
   - [Enter] を押して選択します。
   - 指示が出されたら、再度 [Enter] を押して確定します。

事前プロビジョニングによる導入

設定を事前にプロビジョニングすることにより、スイッチをそのシリアル番号に関連付けて、メンバースイッチに割り当てられるメンバー IDとロールを確定的に制御できます。事前プロビジョニング設定ファイルでは、各 EX4200 スイッチのシリアル番号を、指定したメンバーID およびロールにリンクします。メンバーがバーチャルシャーシ構成の一部として認識されるためには、シリアル番号を設定ファイルに指定する必要があります。

この設定では、2 つのメンバーをルーティングエンジンのロールに設定して、マススイッチおよびバックアップスイッチとしての選出資格を与える必要があります。事前プロビジョニング設定にこれらの 2つのメンバーが登録されている場合、一方はバーチャルシャーシ構成のマススイッチとして、もう一方はバックアップスイッチとして機能します。事前プロビジョニング設定では、これらの 2 つのメンバースイッチはルーティングエンジンのロールのみを担うことができ、手動でマスターまたはバックアップとして設定することはできません。

マススイッチまたはバックアップスイッチとしての選出資格のないその他のメンバーは、事前プロビジョニング設定で*ラインカード*として設定できます。

事前プロビジョニング設定では、メンバースイッチに明示的にロールを割り当てないようにすることもできます。、マススイッチまたはバックアップスイッチに障害がある場合、これらのスイッチにバックアップとしての選出資格が与えられます。また、マススイッチおよびバックアップスイッチの両方に障害がある場合は、マススイッチになることができます。

明示的にラインカードのロールを設定したメンバースイッチには、マススイッチまたはバックアップスイッチとして機能する資格はなくなります。

指定されたロールに基づいて、以下のマスターシップ優先度値が Junos により割り当てられます。

- マススイッチおよびバックアップスイッチ（ルーティングエンジンロールのメンバー）には、マスターシップ優先度 129 が割り当てられます。
- ラインカードスイッチには、マスターシップ優先度 0 が割り当てられ、マスター選出への参加資格がなくなります。
- ロールが明示的に割り当てられていないスイッチには、マスターシップ優先度 128（デフォルト）が設定され、マスター選出への参加資格が与えられます。

バーチャルシャーシ構成への IP アドレスの割り当て

バーチャルシャーシ構成は、1 つの論理ネットワーク要素として管理されます。そのため、割り当てられる管理 IP アドレスは 1 つのみで、この IP アドレスは VME（バーチャル管理イーサネット）インタフェースに対して設定されます。VME インタフェースは、バーチャルシャーシ構成に属するすべてのメンバースイッチの管理イーサネットインタフェースを接続するバーチャルシャーシ内部管理 VLAN に関連付けられる論理 IP インタフェースです。IP アドレスを割り当てるには、以下の CLI 設定を使用します。

```
user@switch> configure
[edit]
user@switch# set interfaces vme unit 0 family inet address <ip-address>/<subnet-mask>
```

ベストプラクティス　障害許容力を高めるために、個々の管理イーサネット（me0）ではなく VME に IP アドレスを設定することをお奨めします。

バーチャルシャーシメンバーの同期

マスタースイッチの設定が変更されるたびに、バーチャルシャーシ構成のその他すべてのスイッチに変更を伝播することをお奨めします。これを行うには、以下の設定モードの CLI コマンドを使用します。

```
user@switch> configure
[edit]
user@switch# commit synchronize
```

CLI コマンドによる動作の監視

バーチャルシャーシ構成は、CLI コマンドで監視することができます。バーチャルシャーシの全メンバーまたは特定メンバーの情報を表示することができます。

バーチャルシャーシの全メンバーに関するメンバー詳細を表示するには、以下のように `show virtual-chassis status` コマンドを入力します。

```
user@switch> show virtual-chassis status
Virtual Chassis ID:1234.5678.90ab
                                          Mastership            Neighbor List
Member ID  Status   Serial No    Model    priority    Role      ID  Interface
0 (FPC 0)  Prsnt    ABC012345678 ex4200-24p      250  Master*    1  vcp-0
                                                                1  vcp-1
1 (FPC 1)  Prsnt    ABC012345679 ex4200-24p      200  Backup     0  vcp-0
                                                                0  vcp-1
Member ID for next new member:2 (FPC 2)
```

さらに詳しくは　バーチャルシャーシテクノロジーの実装の詳細については、『*Virtual Chassis Technology Best Practices Guide*』を参照してください（www.juniper.net/techpubs/）。

ネットワークでの役割

これまでバーチャルシャーシテクノロジーについて詳しく説明してきましたが、実際にバーチャルシャーシ構成をどこに導入すればよいか疑問に思う方もいるでしょう。この疑問に答える前に、まずネットワークの役割の基礎について説明しておかなければなりません。

エンタープライズ LAN アーキテクチャは、アクセスレイヤーでワイヤリングクローゼットスイッチに接続されたエンドユーザーのコンピュータやデバイスから、大規模なエンタープライズ LAN の中央に位置するコアレイヤーまで、最大 3 つのレイヤーにまたがることがあります。この階層型トポロジーでは、ネットワークを物理的な構成要素に分割することにより、動作を簡素化し、可用性を高めることができます。階層型インフラを構成する各レイヤーは、以下のように特定の役割を担います。

- アクセスレイヤー：LAN 内のエンドユーザーにアクセスコントロール境界およびネットワーク接続性を提供します。
- アグリゲーションレイヤー：複数のアクセスレイヤースイッチからの接続およびトラフィックフローを集約し、コアレイヤースイッチにトラフィックを引き渡します。
- コアレイヤー：アグリゲーションレイヤースイッチと、WAN またはインターネットに接続しているルーター間の接続性を提供し、ネットワークコラボレーションを実現にします。

本書では主に、3 層構造の LAN 設計について扱いますが、非常に小規模なキャンパスや支社で一般的な、アグリゲーションレイヤーとコアレイヤーが統合された 2 層構造の設計を実装することもできます。

さらに詳しくは　エンタープライズネットワークの設計の詳細については、『*Campus LAN Design Guide*』（www.juniper.net/techpubs/）を参照してください。

アクセスレイヤー

アクセスレイヤーは、PC、ネットワークプリンター、IP 電話、PoE（Power over Ethernet）カメラなどのデバイスを LAN（ローカルエリアネットワーク）に接続することにより、ネットワークユーザーにネットワーク接続性を提供します。通常、アクセスレイヤーのスイッチは、各建物内または施設内の各フロアに設置されたワイヤリングクローゼットに導入されます。

一般的な LAN では、LAN 上のデバイスを物理的に移動する代わりに、VLAN（バーチャルローカルエリアネットワーク）を使用し、ソフトウェア設定を通して、アクセスレイヤーに存在する一連のユーザー、デバイス、またはデータを複数の論理ネットワークに論理的にグループ化します。VLAN では、拡張性、セキュリティ、ネットワーク管理などの問題に対処できます。これについては第 4 章で説明します。

バーチャルシャーシテクノロジー搭載の EX4200 イーサネットスイッチは、10/100/1000BASE-T ポート 24 基または 48 基、あるいは 100BASE-FX/1000BASE-X ポート 24 基を備えたアクセスレイヤーソリューションとして利用できます。EX4200 イーサネット スイッチが独自に備える優位性の 1 つとして、pay-as-you-grow design（成長に応じて拡張可能な設計）が挙げられます。すなわち、1 台の EX4200 スイッチから始め、その後、段階的に最大 9 台のスイッチをバーチャルシャーシ構成に追加することが可能です。

各 EX4200 イーサネットスイッチでは、オプションのアップリンクがサポートされます。アップリンクを使用することで、アクセスレイヤーからアグリゲーションレイヤーへとスイッチを相互接続できます。また、EX3200 または EX2200 は、ハードウェア冗長性が不要で、ポート数が 48 基以下の単一ボックスソリューションとして、これらのタイプの環境に理想的なスイッチです。

アグリゲーションレイヤー

アグリゲーションレイヤーは*分散レイヤー*とも呼ばれ、複数のアクセスレイヤースイッチからの接続とトラフィックフローを集約し、コアレイヤーへの高密度な接続性を提供します。アグリゲーションレイヤーに位置するスイッチの主な機能は、拡張性、高密度、高可用性を実現することです。

バーチャルシャーシ構成の EX4200 スイッチ、EX4500、またはモジュラー型 EX8200 シリーズ イーサネットスイッチは、アグリゲーションレイヤーで必要とされるパフォーマンスとサービスを提供することができます。EX4500 には、10GbE または 1GbE ポート 40 基とモジュラー型アップリンクスロット 2 基が搭載されています。EX8200 シリー

ズ イーサネットスイッチには、最大 64 基（8 スロットシャーシ）または 128 基（16 スロットシャーシ）の 10GbE ポートが搭載されています。EX4200-24F スイッチは、100BASE-FX/1000BASE-X ポート 24 基と、オプションの 10GbE ポート 2 基のアップリンクモジュールをバーチャルシャーシ構成で搭載し、低～中密度の GbE アグリゲーションレイヤーに適したソリューションです。

さらに詳しくは モジュラー型 EX4500 および EX8200 シリーズ イーサネットスイッチの詳細については、www.juniper.net/techpubs/ から入手可能な製品情報を参照してください。

コアレイヤー

コアレイヤーはバックボーンとも呼ばれ、複数のアグリゲーションレイヤー間、または集約型ネットワークのアクセスレイヤーとの間で高速パケットスイッチングを行うための構造です。ゲートウェイとして機能し、信頼性および効率性を実現する基盤となります。

一般に、コアレイヤーでは、大容量のスループットを処理し、優れたパフォーマンスを実現するために、10GbE インタフェースが使用されます。また、高可用性も重要な要素です。通常、システムおよびネットワーク冗長性を提供するために、コアレイヤーは複数のコアレイヤースイッチで構成されます。

モジュラー型 EX8200 シリーズ イーサネットスイッチは、コアレイヤーソリューションとして使用できます。これは、このスイッチが冗長ルーティングエンジンとスイッチファブリックに加え、冗長電源およびファンを備えているからです。また、デバイスまたはリンクの障害に備えて、コアレイヤーの各デバイスへの冗長リンクが提供されます。

リンク冗長性を実現するには、ネットワークデバイス間で複数の冗長リンクを確立することが第一ステップです。または、リンクアグリゲーショングループを使用し、あたかもネットワークデバイス間の 1 本の大容量リンクであるかのように複数のリンクをグループ化することもできます。

LAG（リンクアグリゲーショングループ）

LAG（リンクアグリゲーショングループ）は、複数の物理リンクを論理的に 1 本の束にグループ化したものです。図 2.9 に示すように、LAG では、1 本に集約されたイーサネットリンクの束に含まれるメンバーリンク間でトラフィックが分散されるため、リンク帯域幅が効果的に向上します。また、LAG が複数のメンバーリンクで構成されていることから、可用性が高まるという優位性ももたらされます。いずれかのメン

バーリンクで障害が発生しても、LAG では残りのリンクで引き続きトラフィックを送信できます。

通常、LAG は、EX シリーズ イーサネットスイッチのアップリンクに設定され、アップリンクポートは上流の他のネットワークデバイスに接続されるため、下流のホストに LAG のメリットがもたらされます。

LAG には、レイヤー 2 ポートまたはレイヤー 3 ポートを使用できます（ポートレイヤーモードについては第 3 章で説明）。LAG は、静的または動的な方法で設定でき、動的な方法で設定する場合は、LACP（Link Aggregation Control Protocol）を使用できます。

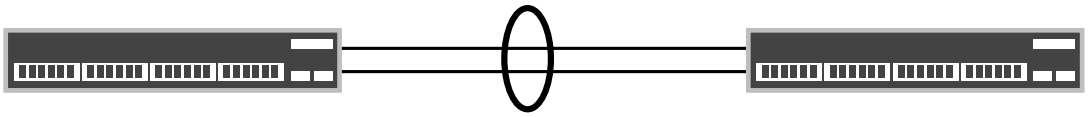


図 2.5 LAG で接続された 2 台の EX シリーズ イーサネットスイッチ

リンクアグリゲーショングループに関するガイドライン

EX シリーズ イーサネットスイッチに LAG を設定するときは、以下のガイドラインを覚えておいてください。

- LAG は、集約されたイーサネットインタフェースとして設定します。
- すべてのリンク速度および二重化の設定は同じにする必要があります。
- LAG 内の物理リンクの最大数は、EX2200、EX2200-C、EX3200、EX3300、EX4200、EX4500、EX4550、および EX6200 スイッチでは 8 本、EX8200 スイッチでは 12 本です。
- EX2200、EX2200-C、EX3200、および EX3300 では、最大 32 個の LAG がサポートされます。
- EX4200、EX4500、EX4550、および EX6200 では、最大 64 個（Junos 12.3 からは 111 個）の LAG がサポートされます。
- EX8200 イーサネットスイッチでは、最大 255 個の LAG がサポートされます。
- LAG は、リンクの両側に設定する必要があります。

注 LAG 内のポートは隣接している必要はありません。バーチャルシャーシ構成の場合、複数のスイッチメンバーに渡って LAG を設定することが可能です。

LACP（Link Aggregation Control Protocol）

LACP は、複数の物理ポートを束ねた 1 本のリンクを定義し、IEEE 802.3ad 仕様で規定されています。LACP では、誤った設定に対する基本的なエラーチェックが行われるため、LAG の両側に LAG を適切に設定することができます。設定が誤っていると、LAG はアクティブになりません。

プロトコル定義の一部として、*アクター*（送信リンクと*パートナー*（受信リンク）間で LACP が交換されます。LACP モードは、アクティブまたはパッシブのいずれかにできます。

警告！ 両側がどちらもパッシブモードの場合、LACP パケットが交換されず、LAG が有効になりません。デフォルトでは、LACP はパッシブモードです。LACP パケットの送信を開始して LAG を有効にするには、LAG の少なくとも一方の側で LACP をアクティブモードで有効にする必要があります。

LACP を使用して動的 LAG を設定するには

1. スイッチ（またはバーチャルシャーシ構成）の LAG の数を定義します。

```
user@switch# set chassis aggregated-devices ethernet device-count 1
```

2. 既存のインタフェース設定を削除します（以下の例では、ge-0/0/10 および ge-0/0/11 を使用）。

```
user@switch# delete interfaces ge-0/0/10
user@switch# delete interfaces ge-0/0/11
```

3. LAG に含めるインタフェースを設定します。

```
user@switch# set interfaces ge-0/0/10 ether-options 802.3ad ae0
user@switch# set interfaces ge-0/0/11 ether-options 802.3ad ae0
```

4. LACP を設定します（アクティブモードを使用）。

```
user@switch# set interfaces ae0 aggregated-ether-options lacp active periodic fast
```

5. LAG インタフェースを、すべての VLAN に転送するレイヤー 2 トランクポートとして設定します。アクセスおよびトランクなどのポートモードについては、第 4 章で説明します。

```
user@switch# set interfaces ae0 unit 0 family ethernet-switching port-mode trunk vlan
members all
```

注 デフォルトでは、アクターおよびパートナーは LACP パケットを毎秒送信します（fast モード）。この間隔は、fast（毎秒）または slow（30秒ごと）に設定できます。

LAG の全メンバーに関する LAG 詳細を表示するには

1. show lacp interfaces ae0 コマンドを入力します。

```
user@switch> show lacp interfaces ae0
Aggregated interface: ae0
    LACP state:        Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/10       Actor    No    No   Yes  Yes  Yes   Yes    Fast    Active
      ge-0/0/10       Partner  No    No   Yes  Yes  Yes   Yes    Fast    Active
      ge-0/0/11       Actor    No    No   Yes  Yes  Yes   Yes    Fast    Active
      ge-0/0/11       Partner  No    No   Yes  Yes  Yes   Yes    Fast    Active
    LACP protocol:    Receive State  Transmit State          Mux State
      ge-0/0/10       Current     Fast periodic           Collecting distributing
      ge-0/0/11       Current     Fast periodic           Collecting distributing
```

さらに詳しくは リンクアグリゲーショングループの詳細については、『*Understanding Aggregated Ethernet Interface and LACP*』を参照してください（www.juniper.net/techpubs/）。

第3章

ネットワークトポロジー（論理トポロジー）

第 2 章では、物理トポロジー（OSI モデルのレイヤー 1）と、ネットワーク内のどの位置に EX シリーズを導入できるかについて説明しました。すなわち、EX8200 または EX9200 はコア / アグリゲーションレイヤ ー に、EX8200、EX4500、EX4550、EX6200、EX3300 または EX4200 はアグリゲーション / アクセスレイヤーのバーチャルシャーシに、EX2200、EX3200、EX3300 または EX4200 はスタンドアロンで、あるいはアクセスレイヤーにバーチャルシャーシ構成で導入できます。

それでは、OSI モデルのさらに上位レイヤーであるデータリンクレイヤー（レイヤー 2）およびネットワークレイヤー（レイヤー 3）に進み、EX スイッチがネットワークトポロジー全体のどこに適しているかについて説明しましょう。一般に、データリンクレイヤー、すなわちレイヤー 2（L2）は、同一ネットワーク内のエンティティ間のデータ転送を担います。図 3.1 に示すように、L2 ドメインは、単一のネットワーキングデバイスに限定することも、複数のネットワーキングデバイス（複数のワイヤリングクローゼットにまたがる）に拡張することもできます。一方、ネットワークレイヤー、すなわちレイヤー 3（L3）は、ネットワーク間のデータ転送を担い、異なるネットワークにあるデバイス間の通信を促進します。

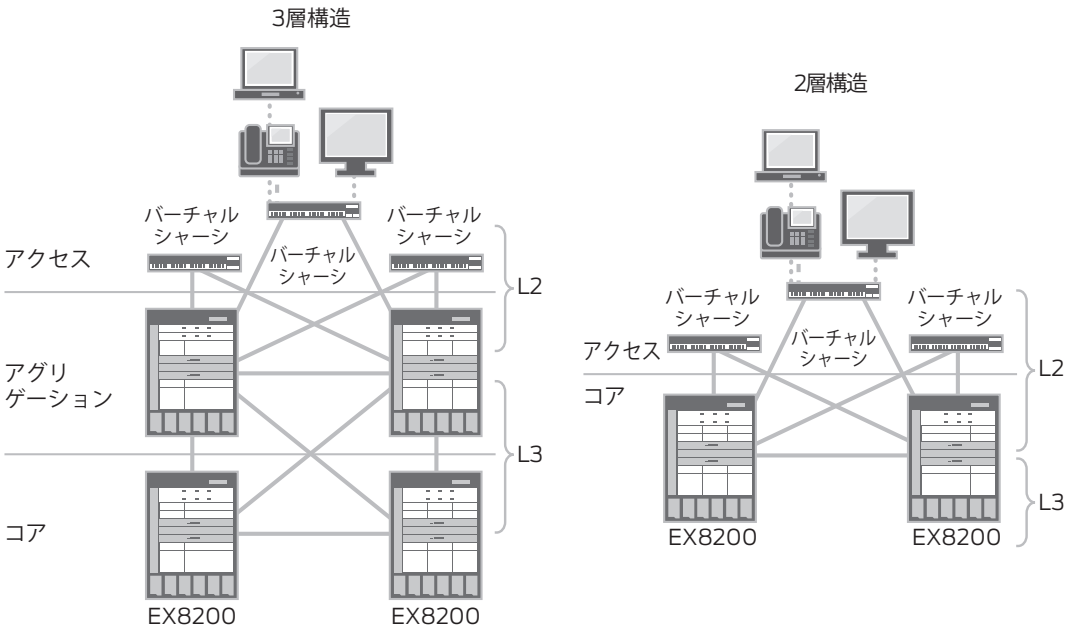


図 3.1　2 層または 3 層構造のネットワークにおけるルーティングドメインとスイッチングドメイン

レイヤー 3（ルーティング）

L3 境界がアグリゲーションからアクセスへと移動している環境もありますが、多くのエンタープライズキャンパス環境では、ルーティングはアグリゲーションレイヤーから始まります。アクセスレイヤーでのルーティングのメリットとして、スパニングツリーを排除し、マルチパスのアクティブ - アクティブリンクを使用できることが挙げられます。

さらに詳しくは アクセスレイヤーへのルーティングの詳細については、『*Campus LAN Reference Architecture*』および『*Deploying Fixed-Configuration and Chassis-Based EX Series Ethernet Switches in Campus LANs*』を参照してください www.juniper.net/。

IP アドレスは、ホストを定義し、ホストにネットワーク内での「位置」を与えます。ネットワークを通過するすべてのデータは、IP ホスト（送信元）から始まり、別のホスト（宛先）で終了します。EX シリーズの IP 設定は、T、M、MX、SRX、および J シリーズデバイスを含む他の Junos ベースのプラットフォームと同じコマンド構文に従います。

レイヤー 3 インタフェース（IPv4 または IPv6）

EX シリーズでは、シングルスタック（IPv4 または IPv6 のみ）、デュアル IP スタック（IPv4 および IPv6）、またはシングルスタック設定とデュアルスタック設定の任意の組み合わせがサポートされます。IPv4 ルーティングおよびスイッチングと、IPv6 スイッチングは、基本ライセンスに含まれています。ただし、IPv6 ルーティングには、アドバンスト機能ライセンス（AFL）が必要です（Junos 12.3 からは EX4200 以上のモデルであれば IPv6 Routing も Base License でサポートされる形に変更されました）。

以下は、IPv4 アドレス設定のコマンド例です。

```
user@switch# set interfaces ge-0/0/0 unit 0 family inet address x.x.x.x/yy
```

以下は、IPv6 アドレス設定のコマンド例です。

```
user@switch# set interface ge-0/0/0 unit 0 family inet6 address xxxx::xxxx/yy
```

IP アドレスは、物理ポート、または RVI（*Routed VLAN Interface*）とも呼ばれる仮想 VLAN インタフェースで設定できます。

RVI（Routed VLAN Interface）

RVI は、特定の VLAN にルーティング機能を提供する論理 L3 インタフェースです。RVI の設定は、2 ステップのプロセスです。最初のステップでは、RVI に IP アドレスを設定します（VLAN インタフェースであることを除き、物理ポートに IP アドレスを設定する場合と同様）。

```
user@switch# set interfaces vlan unit 1 family inet address x.x.x.x/yy
```

注　追加の RVI に IP アドレスを設定する場合は、ユニット番号を増加させます。ユニット番号には任意の数値を使用でき、連続している必要はありません。ただし、RVI ユニット番号と VLAN ID を一致させることをお奨めします。

2 番目のステップでは、以下のコマンドを使用して RVI を VLAN にバインドします。

```
user@switch# set vlans vlan-name l3-interface vlan.1
```

以下の例では、2 つの VLAN に対して 2 つの RVI を作成しています。

```
user@switch# set interfaces vlan unit 1 family inet address 10.0.1.1/24
user@switch# set interfaces vlan unit 2 family inet address 10.0.2.1/24

user@switch# set vlans vlan-1 l3-interface vlan.1
user@switch# set vlans vlan-2 l3-interface vlan.2
```

注　IPv6 アドレスを設定するには、「family inet6」を使用します。

ルーティングプロトコル（OSPF）

次のステップでは、ルーティングプロトコルを有効にします。他の Junos ベースのプラットフォームと同様に、ルーティングプロトコルの設定は、Junos のプロトコルのスタンザで行います。EX シリーズ スイッチでは、RIP、OSPF、IS-IS、および BGP がサポートされます。RIP および OSPF は基本ライセンスに含まれますが、IS-IS および BGP にはアドバンスト機能ライセンス（AFL）が必要です。

注　本書では、OSPF の基本設定を中心に扱います。OSPF プロトコル自体についての詳細な説明は行いません。OSPF の高度な設定、またはその他のルーティングプロトコルの設定については、*『Technical Documentation Software Guide for EX Series Switches』* を参照してください www.juniper.net.techpubs/。

OSPF は、2 層構造のリンクステート型ルーティングプロトコルです。各ルーターでは、OSPF リンクステートアドバタイズメント（LSA）に基づいてルーティングデータベースが構築されます。以下のコマンドにより、EX シリーズで OSPF が有効になります。

```
user@switch# set protocols ospf area 0.0.0.0 interface vlan.1
```

以下の show ospf neighbor コマンドでは、ローカルインタフェース、OSPF が有効になっている IP アドレス、各隣接機器の状態、隣接機器の情報など、隣接機器間の役立つ OSPF サマリーが得られます。

```
user@switch> show ospf neighbor
Address         Interface              State     ID               Pri    Dead
172.16.31.2     ge-0/0/23.0            Full      10.0.0.2         128      32
172.16.3.2       vlan.1                Full      10.0.0.3           1      16
```

OSPF が有効になっている他のルーターから学習した OSPF ルートを表示するには、show ospf route コマンドを使用します。また、すべてのルーティングテーブルを表示するには、show route コマンドを使用します。

```
user@switch> show ospf route
Topology default Route Table:

Prefix               Path  Route      NH       Metric NextHop       Nexthop
                     Type  Type       Type             Interface     Address/LSP
1.0.0.1              Intra Area/AS BR IP            2 ge-0/0/0.0    192.168.150.2
1.0.0.2              Intra Area/AS BR IP            2 ge-0/0/0.0    192.168.150.2
172.16.3.2           Intra Router     IP            1 vlan.1        172.16.3.2
192.0.0.1            Intra Router     IP            1 ge-0/0/0.0    192.168.150.2
10.0.0.1/32          Intra Network    IP            0 lo0.0
172.16.3.0/24        Intra Network    IP            1 vlan.1
172.16.31.0/24       Intra Network    IP            1 ge-0/0/23.0
172.16.81.0/24       Intra Network    IP            3 ge-0/0/0.0    192.168.150.2
172.16.82.0/24       Intra Network    IP            3 ge-0/0/0.0    192.168.150.2
192.168.150.0/24     Intra Network    IP            1 ge-0/0/0.0
```

レイヤー 2（スイッチング）

通常、L2（スイッチング）ドメインはアクセスレイヤーにあり、複数のスイッチにまたがることもあります。L2 ループおよび L2 ドメインの特性により、トラフィックがそのドメイン全体にブロードキャストされ、これによって送信元から送信されたトラフィックが送信元にエンドレスに戻される可能性があります。このような L2 ループに対処するために、スパニングツリーなどのプロトコルが必要になります。ループを回避しないと、ブロードキャストストームによってネットワークが機能しなくなる可能性が高まります。

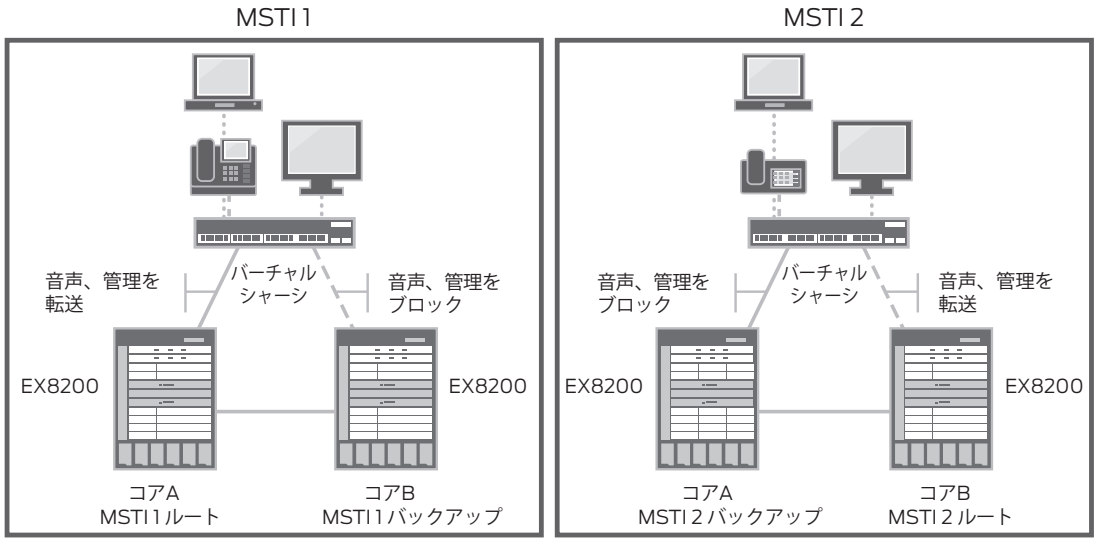


図 3.2 ループフリーの L2 トポロジーを維持しながらアクティブ - アクティブアップリンクを提供する MSTP の例

スパニングツリーは、冗長したレイヤー 2 パスをブロックすることによってネットワークをループフリーにするレイヤー 2 プロトコルです。スイッチ間では、ブリッジ ID とパスコストが保持された BPDU（Bridge Protocol Data Unit）がやり取りされます。ブリッジ ID は、ブリッジ優先度と MAC アドレスで構成され、この情報を基にスイッチでルートブリッジが選出されます。ルートブリッジ（最小のブリッジ ID）が選出されると、ルート以外ではルートブリッジへの最短パスが作成され、冗長パスがすべてブロックされます。

EX シリーズでは、以下の 4 つのスパニングツリープロトコルがサポートされます。

- 802.1D（STP）：単一インスタンスのスパニングツリープロトコルをサポートします（1 つのスパニングツリー（レイヤー 2）転送トポロジーをサポート）。
- 802.1w（RSTP（Rapid Spanning Tree Protocol））：STP と同じですが、ブリッジの通信 / やり取りを改善することにより、収束時間を短縮します。STP との後方互換性があります。
- 802.1s（MSTP（Multiple Spanning Tree Protocol））：MSTP は、RSTP（高速収束をサポート）の機能を拡張したもので、スパニングツリーでより多くのレイヤー 2 トポロジーインスタンスをサポートします。すなわち、各インスタンスが異なる

スパニングツリー転送トポロジーを保持します。MSTP では、最大 64 インスタンスがサポートされるため、スパニングツリーにおいて、ループフリーのトポロジーを維持しながら、すべてのリンクでトラフィックを転送することができます。STP/RSTP との後方互換性があります。

- VSTP（VLAN Spanning-Tree Protocol）：VSTP は VLAN ごとのスパニングツリープロトコルで、各 VLAN が独自のスパニングツリーインスタンスを保持します。VSTP では、RSTP/MSTP で定義されている高速収束がサポートされます。EX シリーズでは、最大 253 個の VLAN スパニングツリーインスタンスがサポートされます。

すべてのスパニングツリープロトコルは、Junos のプロトコルのスタンザで設定します。本書では、RSTP、MSTP、および VSTP の基本設定について説明します。

さらに詳しくは その他のスパニングツリープロトコルの詳細については、*『Spanning Tree in L2/L3 Environment Implementation Guide』* を参照してください。この参考資料では、各プロトコルについて詳しく解説し、設定例を掲載しています。この他、*『Technical Documentation Software Guide for EX Series Switches』* も役立ちます。どちらの参考資料も www.juniper.net から入手できます。

RSTP（Rapid Spanning Tree Protocol）

RSTP は、EX シリーズでデフォルトで有効になります。そのため、EX シリーズをネットワークに接続すれば、RSTP によってループフリーのネットワークが構築されます。

ただし、ネットワークのどこにスイッチを配置するかに基づいて、ブリッジ優先度を設定することをお奨めします。ブリッジ優先度によって、スイッチがルートブリッジになる可能性が左右されます。ブリッジ優先度が低いほど、スイッチがルートブリッジになる可能性は高くなります。各ブリッジでは、ルートブリッジまでの最低コストパスに基づいてリンクが転送状態またはブロック状態になるため、ルートブリッジは、レイヤー 2 転送トポロジーに影響を与えます。

スイッチのデフォルトのブリッジ優先度は 32678 です。この優先度を変更するコマンドは以下のとおりです。

```
user@switch# set protocols rstp bridge-priority bridge-priority-value
```

スパニングツリーのブリッジ優先度値は 0 ～ 65535 です。

MSTP（Multiple Spanning Tree Protocol）

MSTP は RSTP の機能を拡張したもので、RSTP で定義されている高速収束がサポートされることに加え、サポートされるスパニングツリーインスタンスの数が 1 個（STP/RSTP）から 64 個に増加します。これにより、VLAN において 1 対の冗長アップリンク（アクティブ - アクティブアップリンク）間での負荷分散が可能になり、STP/RSTP（アクティブ - スタンバイアップリンク）に比べてリンクをより有効に活用できるようになります。

注 MSTP は、他のスパニングツリープロトコルと同時に有効にすることはできません。そのため、実行中の他のスパニングツリープロトコルをすべて「削除」または「無効化」する必要があります。

これらの機能を利用するには、MSTP が有効になっているすべてのスイッチを同じリージョンに含める必要があります。リージョンとは、設定名、リビジョンレベル、MSTI（MSTI の数および VLAN マッピング）などの MSTP パラメータがすべて同じ MSTP スイッチのグループです。これらのパラメータが異なるスイッチは別のリージョンに含められ、スイッチ間で複数のスパニングツリーインスタンスをサポートする機能を失います。

```
user@switch# set protocols mstp configuration-name configuration-name
user@switch# set protocols mstp revision-level revision-level-number
```

注 CST（Common spanning-tree）のブリッジ優先度とスパニングツリータイマーは、メイン MSTP コンテキストで設定します。

MSTI（MST Instances）

MSTI とは、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングしたものです。同じ MSTI にマッピングされた一連の VLAN では、同じスパニングツリー転送トポロジーが共有されます。これは、MSTI ルートブリッジへの最短パスが MSTI ごとに作成されるためです。MSTI のブリッジ ID は、そのインスタンス内でのみ意味を持ちます。

以下は、インスタンスへの VLAN のマッピングです。

```
user@switch# set protocols mstp msti msti-number vlan vlan-ids
```

MSTI 番号には、1 ～ 64 の任意の番号を使用できます。VLAN ID は、名前、vlan-id、または範囲（1-100、[1 3 5 7-10]）として設定できます。

MSTI のブリッジ優先度（0 ～ 65535）を設定するには、以下のコマンドを使用します。

```
user@switch# set protocols mstp msti msti-number bridge-priority bridge-priority-value
```

VSTP（VLAN Spanning-Tree Protocol）

VSTP では、複数のスパニングツリーインスタンスが提供されますが、スパニングツリーインスタンスは VLAN ごとに 1 つずつ存在します。この点が、多数の VLAN を 1 つのインスタンスにマッピングできる MSTP と異なります。ただし、機能に関しては RSTP/MSTP との類似点があります。すなわち、同じポート状態とロールに従い、RSTP/MSTP で一般的な高速収束も利用されます。

各 VLAN には、それぞれ固有のブリッジ優先度とスパニングツリーパラメータを設定できます。VLAN で VSTP を有効にするには、以下のコマンドを使用します。

```
user@switch # set protocols vstp vlan vlan-id
```

特定の VLAN にブリッジ優先度を設定するには、以下のコマンドを使用します。

```
user@switch# set protocols vstp vlan vlan-id bridge-priority bridge-priority-value
```

注 Junos 10.2 以降では、RSTP を VSTP と同時に設定することができます。これにより、Cisco PVST+/R-PVST+ との相互運用性を確保できます。

以下の show コマンドは、すべてのスパニングツリープロトコルで使用できます。`show spanning-tree bridge` コマンドを使用すると、プロトコル、ブリッジ ID、タイマーなどスパニングツリーに関する基本情報を取得できます。

```
user@switch> show spanning-tree bridge
STP bridge parameters
Context ID                        :0
Enabled protocol                  :RSTP
  Root ID                         :4096.00:19:e2:50:86:60
  Hello time                      :2 seconds
  Maximum age                     :20 seconds
  Forward delay                   :15 seconds
  Message age                     :0
  Number of topology changes      :10
  Time since last topology change :7642 seconds
  Local parameters
    Bridge ID                     :4096.00:19:e2:50:86:60
    Extended system ID            :0
    Internal instance ID          :0
```

この他、便利なコマンドとして show spanning-tree interface があります。このコマンドでは、インタフェースのスパニングツリーポート状態とポートロールが表示されます。

```
user@switch> show spanning-tree interface

Spanning tree interface parameters for instance 0

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ae0.0          128:1        128:1     4096.0019e2508660     10000  FWD    DESG
ge-0/0/0.0     128:513      128:513   4096.0019e2508660     20000  FWD    DESG
ge-0/0/3.0     128:516      128:516  32768.0019e2508660     20000  BLK    DIS
ge-0/0/4.0     128:517      128:517  32768.0019e2508660     20000  BLK    DIS
ge-0/0/5.0     128:518      128:518  32768.0019e2508660     20000  BLK    DIS
```

以下のコマンドは、MSTP に固有です。設定名、リビジョンレベル、MSTI-VLAN のマッピングなどの MSTP 設定のサマリーが提供されます。このコマンドは、スイッチが目的の MSTP リージョンに含まれているかどうかを確認する際に役立ちます。

```
user@switch> show spanning-tree mstp configuration
MSTP information
Context identifier     :0
Region name            :MST-Region-1
Revision               :2
Configuration digest   :0x57c9f50482c9c9ae3c404a5d3212715d


MSTI     Member VLANs
   0 0,401-4094
   1 1-100
   2 101-200
   3 201-300
   4 301-400
```

冗長トランクグループ (RTG)

冗長トランクグループ（RTG）は、EX シリーズのもう 1 つの機能で、アクセスレイヤースイッチでスパニングツリーを実行しなくても、ループフリーのレイヤー 2 トポロジーを構築できます。RTG では、一方のリンクをアクティブにし、もう一方のリンクをスタンバイにすることにより、このようなトポロジーが実現されます。RTG が有効になっているリンクは、RTG が有効なポートで受信した BPDU を送信 / 転送せずに破棄します。図 3.3 に示すように、物理リンクがダウンすると、スイッチオーバーが実行されます。RTG は、アクセススイッチでのみ設定してください。

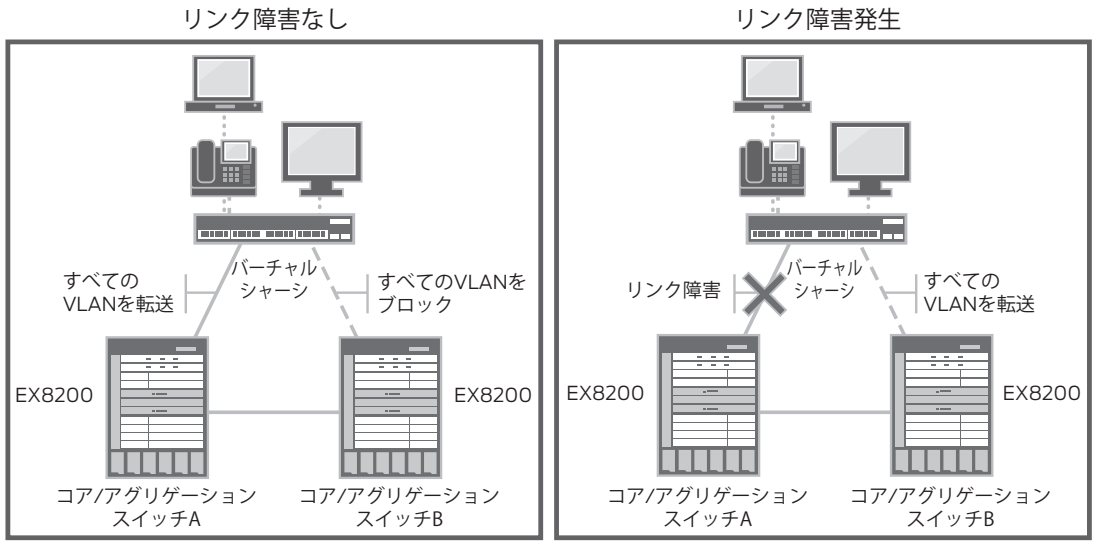


図 3.3 プライマリリンクでの障害発生前後の RTG

EX シリーズでは、最大 16 個の RTG グループがサポートされます。1 つの RTG グループに設定できるリンクは最大 2 本です。このうち 1 本がアクティブになりトラフィックを転送し、残りの 1 本はスタンバイモードになります。コマンドの入力順序に関係なく、RTG グループ内で最高の番号を持つインタフェースがアクティブリンクになります。

注 RTG と STP は相互に排他的です。RTG が設定されたインタフェースでは、スパニングツリーを無効にする必要があります。

スパニングツリーをグローバルに無効にするには、以下のコマンドを使用します。

```
user@switch# delete protocols [stp|rstp|mstp|vstp]
```

または、インタフェース単位でスパニングツリーを無効にすることもできます。

```
user@switch# set protocols [stp|rstp|mstp|vstp] interface interface-name disable
```

ヒント ジュニパーネットワークスは、レイヤー 2 ループにつながる可能性のあるユーザーエラーを防ぐために、2 番目の方法を使用して、RTG が有効になっていない他のポートではスパニングツリーを有効なままにすることをお奨めします。

RTG は、Junos の ethernet-switching-options スタンザで設定します。

```
user@switch# set ethernet-switching-options redundant-trunk-group RTG-1 interface ge-
0/1/0.0
user@switch# set ethernet-switching-options redundant-trunk-group RTG-1 interface ge-
0/1/1.0
```

RTG リンク状態を表示するには、show redundant-trunk-group コマンドを使用します。以下の例では、番号 1.0 のインタフェースが有効になっています。

```
user@switch> show redundant-trunk-group
Group       Interface   State       Time of last flap                    Flap
name                                                                     count

RTG-1       ge-0/1/1.0  Up/Act      Never                                   0
            ge-0/1/0.0  Up          Never                                   0
```

注 ジュニパーネットワークスは、レイヤー 2 ループにつながる可能性のある設定エラーまたは物理的エラーを防ぐために、コア / アグリゲーションスイッチでスパニングツリーを有効なままにすることをお奨めします。

「primary」キーワード

「primary」キーワードには 2 つの機能があります。1 つは、「primary」として設定されているリンクをアクティブにし、転送状態にすることです。もう 1 つは、その他のリンクがアクティブにならないように阻止することです。RTG でスタンバイリンクにフェイルオーバーしたかどうかに関わらず、リンクは有効になると、常にアクティブになり、転送状態になります。

```
user@switch# set ethernet-switching-options redundant-trunk-group group RTG-1
interface ge-0/1/1.0 primary
```

以下の例では、インタフェース ge-0/1/0.0 がアクティブになっています。その横にある「Pri」は、そのポートに「primary」が設定されたことを示します。

```
user@switch# run show redundant-trunk-group
Group       Interface   State       Time of last flap     Flap
name                                                      count

RTG-1       ge-0/1/0.0  Up/Pri/Act   Never                 0
            ge-0/1/1.0  Up           Never                 0
```

第4章

イーサネットスイッチング

イーサネットスイッチングデーモン（ESWD）は、EX シリーズのすべてのレイヤー 2（L2）機能の管理と制御を担う、Junos の新たなデーモンです。その対象には、MAC アドレステーブル、VLAN、および L2 プロトコル（スパニングツリー、LLDP など）が含まれます。ESWD の導入により、以下の機能が Junos CLI に追加されました。

- 新たなファミリ ethernet-switching が追加されました。ethernet-switching ファミリにより、論理ユニットがレイヤー 2 ポートに移行されます。これについては、「ポートモード」セクションで詳しく説明します。
- 以下の 2 つの設定スタンザが新たに Junos に導入されました。

  VLAN：VLAN データベース、メンバーシップ、および機能を管理します。

  Ethernet-switching-options：音声 VLAN、アクセスセキュリティ（DHCP スヌーピング、Dynamic ARP Inspection など）など L2 固有の機能を設定します。アクセスセキュリティ機能については、第 5 章で説明します。

バーチャル LAN（VLAN）

LAN（ローカルエリアネットワーク）は、ハブに接続しているデバイスのように、同じ L2 ブロードキャストドメインに属するデバイスの集合です。バーチャル LAN（VLAN）は、この概念を、スイッチなどの同じ L2 デバイス上に存在する複数の論理 LAN に拡張したもので、図 4.1 に示すように、基本的には、同じ L2 ブロードキャストドメインを共有するスイッチポートのグループです。

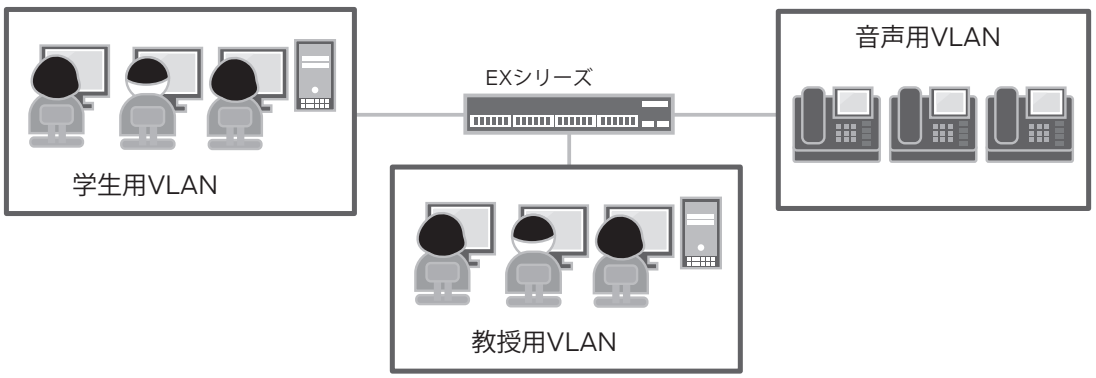


図 4.1 **複数の論理 VLAN に分割された EX シリーズ**

EX シリーズでは、最大 4,094 個の VLAN がサポートされ、VLAN には任意の vlan-id を使用できます。デフォルトでは、すべてのポートは「デフォルト」VALN の一部になり、null の vlan-id が割り当てられます（以下を参照）。

```
user@switch> show vlans
Name          Tag     Interfaces
default
                       ge-0/0/0.0*, ge-0/0/3.0, ge-0/0/4.0, ge-0/0/5.0,
                       ge-0/0/6.0, ge-0/0/7.0, ge-0/0/8.0, ge-0/0/9.0,
                       ge-0/0/10.0, ge-0/0/11.0, ge-0/0/12.0, ge-0/0/13.0,
                       ge-0/0/14.0, ge-0/0/15.0, ge-0/0/16.0, ge-0/0/17.0,
                       ge-0/0/18.0, ge-0/0/19.0, ge-0/0/20.0, ge-0/0/21.0,
                       ge-0/0/22.0, ge-0/0/23.0
```

注 上記の出力は、EX シリーズのモデルによって異なる場合があります。アスタリスク（*）は、そのポートがアクティブ（リンクが有効）であることを示します。

VLAN の追加または削除は、VLAN スタンザで行います。最小限の VLAN 設定では、以下のように VLAN 名を定義します。

```
user@switch# set vlans faculty
```

VLAN を削除する場合は、set コマンドを delete に置き換えます。

同じコマンドラインで、802.1Q vlan-id（1 ～ 4094 の数値）を割り当てることができます。vlan-id は、スイッチがトランクリンクによって接続され、そのスイッチに渡って拡張されている場合のみ必要になります。以下に例を示します。

```
user@switch# set vlans faculty vlan-id 10
```

VLAN レンジ

VLAN レンジを指定することにより、以下のように 1 つのコマンドで VLAN の範囲を定義することができます。

```
user@switch# set vlans vlan-name vlan-range low-high
```

vlan-range では、番号が連続していない vlan-id はサポートされません。また、vlan-range で設定された属性は、その vlan-range にあるすべての VLAN に継承されます。

例えば、以下の設定例では、VLAN 名が Bldg_A で、VLAN レンジが 20 ～ 30 の VLAN について、MAC テーブルのエイジングタイムが 300 秒（デフォルト）から 60 秒に変更されています。この変更は、vlan-range が 20 ～ 30 の VLAN に適用されます。

```
user@switch# show vlans
Bldg_A {
    vlan-range 20-30;
    mac-table-aging-time 60;
}
```

以下に示すように、vlan-id が vlan-name に付加され、各 VLAN に固有の VLAN 名が付けられます。

```
user@switch> show vlans
Name            Tag     Interfaces
__Bldg_A_20__   20
                        None
__Bldg_A_21__   21
                        None
__Bldg_A_22__   22
                        None
__Bldg_A_23__   23
<output truncated>
```

VLAN メンバーシップ

VLAN へのポートの配置は、VLAN 設定またはポート設定のいずれかの方法で行えます。これらの方法に優劣はなく、得られる結果は同じです。

メンバーシップ：VLAN 設定

VLAN で VLAN メンバーシップを設定するには、以下のコマンドを使用します。

```
user@switch# set vlans faculty interface ge-0/0/0.0
```

メンバーシップ：ポート設定

interface で VLAN メンバーシップを設定するには、以下のコマンドを使用します。

```
user@switch# set interfaces ge-0/0/0.0 family ethernet-switching vlan members faculty
```

または：

```
user@switch# set interfaces ge-0/0/0.0 family ethernet-switching vlan members 10
```

ベストプラクティス　CLI での管理を簡単に行えるようにするために、ジュニパーネットワークスは、VLAN 設定の方法でメンバーシップを設定することをお奨めします。アクセスポートの場合は、VLAN スタンザですべての VLAN メンバーシップを設定します。トランクポートの場合は、interface（ポート設定の方法）ですべての VLAN メンバーシップを設定します。この章で後に説明する「インタフェースレンジ」セクションも参照してください。

VLAN リストは、ポート設定の方法でサポートされます。以下の設定を使用できます。これはトランクポートに非常に役立ちます。

```
user@switch# set interfaces ge-0/1/0.0 family ethernet-switching vlan members [1 5
7-100]
```

show vlan 以外に便利なコマンドとして show ethernet-swtching interfaces <interface-name> があります。このコマンドにより、VLAN メンバーシップ、802.1Q タグ、および転送状態の詳細が表示されます。

```
user@switch> show ethernet-switching interfaces ge-0/1/0
Interface    State  VLAN members        Tag   Tagging  Blocking

ge-0/1/0.0   up     default             1     untagged unblocked
                    faculty             10    tagged   unblocked
                    student             30    tagged   unblocked
                    voice               5     tagged   unblocked
```

ポートロール（ポートモード）

通常、スイッチに設定されるポートモードはエンドポイントによって決まります。例えば、エンドポイントがホスト（PC）のときは、多くの場合、ポートはアクセスポートとして設定されます。電話と PC がある場合は、ほとんどがアクセスポートと音声 VLAN になります。一般的なポートロールには、ホスト、サーバー、ネットワークデバイス（ルーター、スイッチ、または無線 AP）、およびサービスデバイス（ファイアウォール、IDP など）があります。また、スイッチのポートタイプは、アクセス、トランク、またはルーテッドの 3 つです。表 4.1 に、デバイスとポートタイプの対応表を示します。

表 4.1　一般に エンドポイントに設定されるスイッチポート

ポートタイプ / デバイス	アクセス	トランク	ルーテッド
ホスト	○		
ホスト +IP テレフォニー（IPT）	○	○	
サーバー	○	○	
ネットワークデバイス	○	○	○
サービスデバイス	○	○	

アクセスインタフェースは、特定 VLAN のメンバーである L2 ポートで、通常はホストまたはサーバーに接続されます。設定するには、以下のコマンドを使用します。

```
user@switch# set interfaces ge-0/0/0.0 family ethernet-switching port-mode access
```

トランクインタフェースは、L2 ポートで、複数の VLAN のメンバーです。一般的な接続は、サーバー、ルーター、サービスデバイス、または 1 本のリンクで複数の VLAN に渡る必要のあるデバイスです。設定するには、以下のコマンドを使用します。

```
user@switch# set interfaces ge-0/1/0.0 family ethernet-switching port-mode trunk
```

ルーテッドインタフェースは、IP アドレスを持つインタフェースで、通常は 2 つのルーテッドノード間に設定されます。以下のようなコマンドを使用します。

```
user@switch# set interfaces ge-0/1/1.0 family inet address 10.1.3.1/30
```

また、デスクトップ +IPT は、音声 VLAN が有効になっているアクセスポートです。IPT とデスクトップは、デイジーチェーン接続で同じスイッチポートに接続されます（図 4.2 を参照）。物理的には、音声トラフィックとデータトラフィックは同じポートに接続されますが、論理的には、別々の VLAN にあります。データトラフィックは、タグなしとして送受信されるのに対し、音声トラフィックにはタグが付けられます。設定については、「音声 VLAN」セクションを参照してください。

図 4.2 音声 VLAN、IP テレフォニー、および PC が同じスイッチポートを共有している、アクセスポートとして設定されたスイッチポート

LLDP（Link-Layer Discovery Protocol）

IEEE 802.1AB 標準で定義されている LLDP（Link-Layer Discovery Protocol）により、ネットワークデバイスはそれ自体の身元と機能を LAN 上でアドバタイズすることができます。特に、EX シリーズは、アドバタイズされるこの情報によって、LAN で効率的に相互運用可能なさまざまなデバイスを識別することができます。

標準では、LLDP 対応デバイスは*エージェント*と呼ばれ、LLDPDU（*Link Layer Discovery Protocol データユニット*）と呼ばれる情報を TLV（タイプ、長さ、値）メッセージの形式で隣接機器に送信します。これらのメッセージには、シャーシおよびポート識別子、システム名および機能など、デバイス固有の情報を含めることができます。LLDPDU は各エージェントから送信され、受信エージェントに保存されます。有効な状態を保つためには、この情報を定期的に更新する必要があります。

EX4200 イーサネットスイッチでは、デフォルトで LLDP が有効になりますが、再度有効化する必要がある場合や、その他のモデルでは、以下の CLI 設定を使用します。

```
user@switch# set protocols lldp interface all
```

さらにきめ細かい制御が必要な場合は、`all` キーワードの代わりにインタフェースを指定して、インタフェース単位で LLDP を有効にすることもできます。

```
user@switch# set protocols lldp interface ge-0/0/0
```

さらに詳しくは　LLDP TLV、開始タイマー、アドバタイズ間隔の設定など LLDP 設定の詳細については、www.juniper.net/techpubs/ を参照してください。

LLDP-MED

LLDP-MED（LLDP-Media Endpoint Discovery）は、LLDP（IEEE 802.1AB）標準を拡張したもので、VoIP エンドポイントデバイスと他のネットワーキングエンドデバイス間の相互運用性をサポートします。通常、LLDP-MED は、スイッチなどのネットワーク機器に接続された VoIP 電話を検出するために使用されます。

LLDP-MED には、LLDP エージェントから送信される TLV 情報に加え、ネットワークポリシーの検出および PoE（Power over Ethernet）給電機能の管理などの追加情報が含まれます。

ネットワークポリシー TLV では、インタフェースに設定されている VLAN 情報（「音声 VLAN」セクションを参照）の他、802.1Q タギングなどの関連するレイヤー 2 およびレイヤー 3 属性、DSCP などの QoS 情報がアドバタイズされます。スイッチはこの TLV 情報を IP 電話にアドバタイズすることにより、音声トラフィックが適切な優先度で処理されるようにします。

また、PoE 管理 TLV により、スイッチは必要な電力レベルと PoE 優先度をアドバタイズできます。例えば、スイッチは、PoE インタフェースに接続された IP 電話で必要な電力と使用可能なリソースを比較できます。スイッチが IP 電話で必要とされるリソースを提供できない場合、電力に関して妥協点に達するまで IP 電話とネゴシエーションを行うこともできます。

また、位置情報では、エンドポイントに設定されている物理的位置がアドバタイズされます。これは、物理的位置または緊急位置識別番号（ELIN）によって決定できます。

さらに詳しくは LLDP-MED TLV の詳細については、EX スイッチに関する参考資料を参照してください（www.juniper.net/techpubs/）。

EX4200 イーサネットスイッチでは、デフォルトで LLDP-MED が有効になりますが、再度有効にする必要がある場合や他のスイッチモデルでは、以下の設定を使用します。

```
user@switch# set protocols lldp-med interface all
```

LLDP と同様に、さらにきめ細かい制御が必要な場合は、`all` キーワードの代わりにインタフェースを指定して、インタフェース単位で LLDP-MED を有効にすることもできます。

```
user@switch# set protocols lldp-med interface ge-0/0/0
```

さらに詳しくは 位置情報や fast start の設定など、本書の範囲外の LLDP-MED 設定に関する詳細については、www.juniper.net/techpubs/ を参照してください。

LLDP と LLDP-MED のやり取り

デフォルトでは、LLDP および LLDP-MED が両方設定されているインタフェースは、LLDP で定義されている TLV のみをアドバタイズします。インタフェースは、LLDP-MED TLV を受信することによって LLDP-MED 対応デバイスを検出すると、そのインタフェースから LLDP-MED TLV を送信するように切り替わります。

EX4200 イーサネットスイッチの LLDP ステータスを確認するには、show lldp コマンドを使用します。

```
user@switch> show lldp

LLDP                     :Enabled
Advertisement interval :30 seconds
Transmit delay         :2 seconds
Hold timer             :4 seconds
Notification interval  :0 Second(s)
Config Trap Interval   :0 seconds
Connection Hold timer  :300 seconds

LLDP MED                 :Enabled
MED fast start count   :3 Packets

Interface      Parent Interface    LLDP        LLDP-MED
all            -                   Enabled     Enabled
```

さらに詳しくは LLDP/LLDP-MED の show CLI コマンドの出力に関する詳細については、www.juniper.net/techpubs/ を参照してください。

最も役立つ LLDP 情報の 1 つに、EX4200 イーサネットスイッチのデータベースに格納されている隣接機器のリストがあります。この情報を確認するには、show lldp neighbors コマンドを使用します。

```
root> show lldp neighbors
Local Interface    Parent Interface    Chassis Id          Port info     System Name
ge-0/0/0.0         -                   00:11:22:33:44:00   ge-0/0/10.0   L2-Switch
ge-0/0/1.0         -                   00:55:66:77:88:00   ge-0/0/5.0    L2-Switch
ge-0/0/2.0         -                   00:99:aa:bb:cc:00   ge-0/0/12.0   L2-Switch
```

既存の LLDP 隣接機器リストをクリアする必要がある場合は、以下のコマンドでクリアできます。

```
user@switch> clear lldp neighbors
```

データベース全体をクリアすることが望ましくない場合は、個々のインタフェースを指定できます。

```
user@switch> clear lldp neighbors interface ge-0/0/0
```

また、隣接機器にアドバタイズされている情報も役立ちます。これを確認するには、以下に示すように show lldp local-information コマンドを使用します。

```
user@switch> show lldp local-information
LLDP Local Information details
```

```
Chassis ID   :00:11:22:33:44:50
System descr :Juniper Networks, Inc. ex4200-24t , version 10.1R1.8
              Build date:2010-xx-xx 01:31:39 UTC

System Capabilities
    Supported       :Bridge Router
    Enabled         :Bridge Router

Management Information
    Port Name       : me0.0
    Port Address    :192.168.1.1
    Address Type    :IPv4
    Port ID         :34
    Port ID Subtype : local(7)
    Port Subtype    : ifIndex(1)

Interface name    Parent Interface  Interface ID    Interface description    Status
Tunneling
me0.0             -             34            me0.0                    Up       Disabled
ge-0/0/0.0        -             502           ge-0/0/0.0               Up       Disabled
ge-0/0/1.0        -             504           ge-0/0/1.0               Up       Disabled
ge-0/0/2.0        -             526           ge-0/0/2.0               Up       Disabled
```

EX4200 イーサネットスイッチについて収集された統計情報は、statistics キーワードを使用することにより表示できます。

```
user@switch> show lldp statistics
Interface    Parent Interface  Received  Unknown TLVs  With Errors
ge-0/0/0.0   -                 158502    0             0
ge-0/0/1.0   -                 158510    0             0
ge-0/0/2.0   -                 158517    0             0

Discarded TLVs  Transmitted  Untransmitted
0               158502       1
0               158510       1
0               158517       1
```

最後に、EX4200 スイッチについて収集された LLDP 統計情報をクリアするには、clear キーワードを使用します。

```
user@switch> clear lldp statistics
```

ヒント 必要に応じて、個々のインタフェースを指定することもできます（clear lldp neighbors interface ge-0/0/0 CLI コマンドと同様）。

音声 VLAN

音声 VLAN では、802.1Q タグ付きパケットをアクセスポートに送信できます。これは、コンピュータや VoIP 電話など複数のデバイスが 1 つのポートに接続されている場合に非常に役立ちます。EX4200 イーサネットスイッチは、LLDP-MED（Link Layer Discovery Protocol Media Endpoint Discovery）を通して、音声 VLAN-ID および QoS 情報を VoIP 電話にアドバタイズできるため、デバイスの導入が容易になります。EX4200 イーサネットスイッチでは、デフォルトで LLDP および LLDP-MED が有効になることを覚えておいてください。そのため、LLDP-MED をサポートしている VoIP 電話では、EX4200 イーサネットスイッチから提供される LLDP-MED 情報が使用され、適切な VLAN-ID および QoS マーキングによって音声パケットにタグ付けされます。

音声 VLAN 機能を設定するには、まずユーザー VLAN の一部としてアクセスポートを設定する必要があります（設定の構文については、この章の「VLAN メンバーシップ」セクションを参照）。次に、以下のコマンドを使用して音声 VLAN 機能を有効にします。これにより、アクセスポートでタグ付けパケットとタグなしパケットの両方を受け入れられるようになります（voip-vlan は vlan-name）。

```
user@switch# set ethernet-switching-options voip interface ge-0/0/0.0 vlan voip-vlan
```

オプションのコマンドを使用すると、LLDP-MED が有効な場合に、設定されている転送クラスに関連付けられた QoS コードポイントを LLDP-MED でアドバタイズできます。

```
user@switch# set ethernet-switching-options voip interface <interface_name>
forwarding-class <forwarding_class_name>
```

注　適切な QoS コードポイントをアドバタイズするには、動作集約（BA）をインタフェースにバインドする必要があります。第 5 章の「EZCOS-Voice」セクションを参照してください。

さらに詳しくは　EX シリーズ イーサネットスイッチにおける IP テレフォニーの詳細については、*『Deploying IP Telephony with Juniper Networks EX Series Ethernet Switches』*アプリケーションノートを参照してください（http://www.juniper.net/products-services/switching/ex-series）。

ポート状態の確認または特定

ポート状態の確認または特定には、以下の show コマンドが役立ちます。`show interface interface_name` コマンドは、ポートタイプの確認に役立ちます。

```
user@switch> show interfaces ge-0/0/0.0
  Logical interface ge-0/0/0.0 (Index 65) (SNMP ifIndex 119)
    Flags:Device-Down SNMP-Traps Encapsulation:ENET2
    Input packets :0
    Output packets:710
    Protocol eth-switch     <-- L2 port
      Flags:Is-Primary     <-- no flags, therefore access-port

user@switch> show interfaces ge-0/0/0.0
  Logical interface ge-0/0/0.0 (Index 65) (SNMP ifIndex 119)
    Flags:Device-Down SNMP-Traps 0x0 Encapsulation:ENET2
    Input packets :0
    Output packets:710
    Protocol eth-switch     <-- L2 port
      Flags:Trunk-Mode     <-- trunk port

user@switch> show interfaces ge-0/0/0.0
  Logical interface ge-0/0/0.0 (Index 65) (SNMP ifIndex 119)
    Flags:Device-Down SNMP-Traps 0x0 Encapsulation:ENET2
    Input packets :0
    Output packets:711
    Protocol inet            <-- L3 port
      Flags:None
      Addresses, Flags:Dest-route-down Is-Preferred Is-Primary
        Destination:192.168.32/24, Local:192.168.32.1,
        Broadcast:192.168.32.255
```

この他、役立つコマンドとして show ethernet-switching interface <interface_name> detail があります。この L2 show コマンドでは、L2 ポート状態、VLAN メンバーシップ、ポート転送状態、および学習された MAC アドレス数に関する情報が得られます。

```
user@switch> show ethernet-switching interfaces ge-0/0/22 detail
Interface: ge-0/0/23.0, Index:68, State: up, Port mode:Access
VLAN membership:
    student, 802.1Q Tag:30, untagged, msti-id:0, unblocked
    voip-vlan, 802.1Q Tag:5, tagged, msti-id:0, unblocked
Number of MACs learned on IFL:2

user@switch> show ethernet-switching interfaces ge-0/1/0 detail
Interface: ge-0/1/0.0, Index:69, State: up, Port mode:Trunk
VLAN membership:
    faculty, 802.1Q Tag:10, tagged, msti-id:0, unblocked
    student, 802.1Q Tag:30, tagged, msti-id:0, unblocked
    voip-vlan, 802.1Q Tag:5, tagged, msti-id:0, unblocked
Number of MACs learned on IFL:1000
```

インタフェースレンジ

インタフェースレンジ関数を使用すると、特定範囲のインタフェースグループ全体に共通の設定を適用することができるため、EX シリーズの設定が簡素化され、設定ファイルの行数を減らすことができます。インタフェースレンジは、バーチャルシャーシ構成に EX4200 を導入する場合、またはすべてのインタフェースがデフォルト設定で明示的に定義されていない状況で EX8200 スイッチを導入する場合に、非常に役立ちます。インタフェースレンジは、interface スタンザで設定します。

```
user@switch# set interfaces interface-range interface-range-name [member|member-range]
```

メンバー / ラインカード内またはその全体のインタフェースレンジを追加するには、member-range を使用します。このステートメントでは、正規表現がサポートされないことに注意してください。以下に例を示します。

```
member-range ge-0/0/0 to ge-2/0/47;

member-range ge-3/0/0 to 3/0/23;
```

個々のインタフェース、または限定的な正規表現を使用して複数のインタフェースを追加するには、アスタリスク（*）を使用するか、角括弧を使用して [start-end] の形式で範囲を指定します。

```
member ge-0/0/0;

member ge-0/*/*;

member ge-0/0/[0-23];
```

注　複数のメンバー範囲、メンバー、またはその両方の組み合わせを同じ interface-range グループで設定できます。

それでは、インタフェースレンジの例を見ていきましょう。この例では、アクセススイッチのポートの半分を教授、残り半分を学生に割り当てます。インタフェース単位で VLAN メンバーシップを設定する代わりに、インタフェースレンジコマンドを使用して、特定の設定オプションセットを教授グループに、別のセットを学生グループにまとめて割り当てることができます。

```
user@switch# set interfaces interface-range faculty-ports member ge-0/0/[0-23]
user@switch# set interfacss interface-range faculty-ports unit 0 family ethernet-
switching vlan members faculty

user@switch# set interfaces interface-range student-ports member ge-0/0/[24=47]
user@switch# set interfaces interface-range student-ports unit 0 family ethernet-
switching vlan members student
```

または、VLAN スタンザで VLAN メンバーシップを割り当てることもできます。これを行うには、まず 2 つのインタフェースグループ（1 つは教授用、もう 1 つは学生用）をアクセスグループとして作成し、VLAN スタンザで interface-range グループ名を参照します。

```
user@switch# set interfaces interface-range faculty-ports member ge-0/0/[0-23]
user@switch# set interfaces interface-range faculty-ports unit 0 family ethernet-
switching

user@switch# set interfaces interface-range student-ports member ge-0/0/[24-47]
user@switch# set interfaces interface-range student-ports unit 0 family ethernet-
switching

user@switch# set vlans faculty interface faculty-ports
user@switch# set vlans student interface student-ports
```

各 interface-range グループ名はインタフェースエンティティになり、ethernet-switching-options での機能として、またはスパニングツリー、OSPF、802.1X などのプロトコルでの機能としてなど、Junos CLI の他の部分で参照できるようになります。interface-range グループを参照することにより、そのグループ内のすべてのポートに対して一様に機能が適用されます。または、機能を interface-range グループの単一ポートまたはサブネットに適用することもできます。

```
user@switch# set interfaces interface-range faculty-ports member ge-0/0/[0-23]

user@switch# set protocols rstp interface ge-0/0/0 edge
```

第5章

EXの機能

それでは、キャンパスおよび支社環境の両方で一般的に使用されている EX シリーズの機能をいくつか紹介しましょう。

- イーサネット OAM（802.3ah）：単方向リンクを防ぎます。
- MVRP（802.1ak）：スイッチネットワーク全体の VLAN 管理に役立ちます。
- マルチキャスト：ユーザーのサブセットまたはグループに対する配信オプション。
- EZQOS-Voice：CoS 設定からあいまいな推測を排除します。
- アクセスポートセキュリティ：中間者または DoS 攻撃からの LAN の保護に役立ちます。
- PoE（Power over Ethernet）給電機能：接続されているデバイスに電力を供給します。
- ポートミラーリング：ネットワークポリシーを適用したり、トラブルシューティング時に異常または過剰な帯域幅などの問題を特定できます。

もちろん、EX イーサネットスイッチプラットフォームには、これ以外にも実際のネットワークで利用できる機能が多数あります。レイノルドおよびマーシュキー著『*Junos Enterprise Switching*』（O'Reilly Media 出版、2009 年）、および Junos オペレーティングシステムの新たな各リリースの機能概要（http://www.juniper.net/us/en/community/junos/releases/ で入手可能）を参照してみてください。

OAM リンク障害管理（802.3ah）

IEEE 802.3ah は、運用、管理、および保守（OAM）のための標準ベースの機能で、イーサネットの信頼性向上と管理および保守の能率化に役立ちます。802.3ah 標準は、リンクレイヤーのポイントツーポイントプロトコルであるため、ローカルリンクを超えることはありません。802.3ah 標準では、リモート障害検出、リモートループバック、リンクモニタリング、および検出機能が提供されますが、本書では、2 台のデバイス間のリンクが有効であるにも関わらず、ハードウェアまたはソフトウェアエラーにより一方のデバイスがトラフィックを受信しなくなったときに生じる単方向リンクを検出するために、これをいかに使用できるかに焦点を当てます。

そのためには、両方のデバイスのインタフェースで 802.3ah 標準がサポートされ、有効になっている必要があります。2 つのエンドポイントは、検出（OAMPDU（OAM Protocol Data Unit））を通して隣接関係を確立し、相互の機能を学習します。また、一方のエンドポイントが隣接関係を失った場合には、インタフェースを強制的にダウンできます。

802.3ah は、Junos の oam スタンザで設定します。最初のステップでは、隣接関係が失われたときにリンクをダウンする、隣接関係喪失に対する OAM アクションプロファイルを設定します。

```
user@switch# set protocols oam ethernet link-fault-management action-profile action-profile-name event link-adjacency-loss
user@switch# set protocols oam ethernet link-fault-management action-profile action-profile-name action link-down
```

次に、インタフェースで 802.3ah を有効にします。

```
user@switch# set protocols oam ethernet link-fault-management interface ge-0/1/0.0 link-discovery active
```

最後のステップでは、このアクションプロファイルをインタフェースにバインドします。

```
user@switch# set interface ge-0/1/0.0 apply-action-profile action-profile-name
```

802.3ah を確認するには、`show oam ethernet link-fault-management` コマンドを使用します。このコマンドの出力には、隣接機器の機能と、呼び出されたアクションプロファイルに関する情報が示されます。出力に表示された Peer Address が MAC アドレスで、Discovery State が *Send Any* であれば、OAM のリンク障害管理は正しく設定されています。

```
root@ex4200-VC1-re0> show oam ethernet link-fault-management
  Interface: ge-0/0/23.0
    Status:Running, Discovery state:Send Any
    Peer address:00:1f:12:38:0f:97
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    Remote entity information:
      Remote MUX action: forwarding, Remote parser action: forwarding
      Discovery mode: active, Unidirectional mode: unsupported
      Remote loopback mode: unsupported, Link events: supported
      Variable requests: unsupported
Application profile statistics:
  Profile Name                  Invoked     Executed
  down-link                           0            0
```

MVRP（802.1ak）

MVRP は、GVRP（Generic VLAN Registration Protocol）の後継となる標準ベースのプロトコルです。レイヤー 2 ネットワークに渡って VLAN を動的に管理するために使用され、スイッチネットワークの管理オーバーヘッドを軽減し、トランクポート上の VLAN トラフィックをプルーニングすることによって帯域幅の効率を高めます。MVRP により、スイッチは join および leave メッセージングを通して、同じレイヤー 2 ドメインにある他のスイッチに VLAN 情報を登録したり取り

消したりできます。図 5.1 に示すように、join および leave メッセージはトランクポートを通して送信され、アクティブなスパニングツリートポロジーに従います。

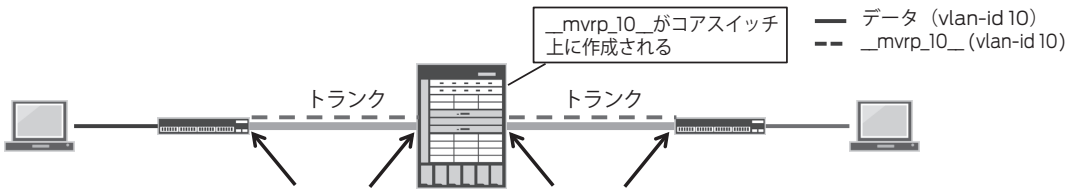


図 5.1 L2 ネットワークに伝播される VLAN 情報

EX スイッチでは、デフォルトで MVRP が無効になるため、以下のようにトランクポートに設定する必要があります。

```
user@switch# set protocols mvrp interface <interface-name>
```

VLAN および VLAN メンバーシップは、ネットワークのエッジスイッチ（*両方*のエッジスイッチ）に設定します。MVRP により、エッジデバイス間での伝播と L2 パスの確立が行われます。

注 MVRP で学習する VLAN の一部にするポートを手動で設定するには、対応する VLAN-id をスイッチに手動で設定する必要があります。

MVRP で学習する VLAN の命名構造は、「__mvrp_vlan-id__」です。MVRP で学習する VLAN メンバーシップを表示するには、MVRP コマンド `show mvrp dynamic-vlan-memberships` を使用します（標準の `show vlan` でも、MVRP で学習する VLAN を表示可能）。

```
user@switch> show mvrp dynamic-vlan-memberships
VLAN Name        Interfaces
--------------   ----------
__mvrp_10__      ge-0/0/0.0
                 ge-0/0/1.0
```

`statistics` キーワードを使用すると、join や leave などの MVRP 統計情報を表示できます。

```
user@switch> show mvrp statistics interface ge-0/1/0
MVRP statistics
Interface name                  :ge-0/1/0.0
  MRPDU received                :162
  Invalid PDU received          :0
```

```
  New received                  :0
  Join Empty received           :380
  Join In received              :106

<output truncated>
```

マルチキャストとマルチキャストルーティング

マルチキャストは、単一の送信元からユーザーの特定サブセットまたは多数の宛先メンバーにパケットを配信するためのテクノロジーです。

マルチキャストルーティングは、EX シリーズ スイッチの基本ライセンスでサポートされます。EX シリーズでは、以下の 3 種類の PIM モードがサポートされます（PIM は、IP ネットワーク用マルチキャストルーティングプロトコルのファミリ）。

- PIM-DM（デンスモード、フラッディング、およびプルーニング）：マルチキャストの参加要求は、まずすべての PIM-DM 対応ルーターにフラッディングされます。下流にメンバーがない場合、ルーターは送信元に向かうトラフィックをプルーニングします。
- PIM-SM（スパースモード、明示的参加）：宛先 / 受信メンバーは、RP（rendezvous point）ルーターに明示的な「参加」要求を送信する必要があります。
- PIM-SSM（送信元固有）：1 対多モデル。受信ホストは、IGMPv3（Internet Group Management Protocol バージョン 3）または MLDv2（Multicast Listener Discovery バージョン 2）によって参加する必要があります。

注 本書では、PIM-SM およびスタティック RP（rendezvous point）の設定構文のみを示します。

すべてのマルチキャストルーティングの設定は、Junos の PIM スタンザで行います。

共有ツリーでは、RP がマルチキャスト配信ツリーのルートになります。最初に、マルチキャストの送信元と、ラストホップルーターからの PIM 参加要求が RP に集まります。RP は、すべてのマルチキャストルーターからアクセスできなければなりません。RP として指定されたルーターに以下のコマンドを設定する必要があります。

```
user@switch# set protocols pim rp local address <ip_address>
```

ヒント ループバック 0 を RP インタフェースにすることをお奨めします。

その他すべてのルーターに対して、以下を設定します。

```
user@switch# set protocols pim rp static address <ip_address>
```

マルチキャストトラフィックをルーティングする、RP インタフェースを含むすべてのルーテッドインタフェースで PIM-SM を有効にする必要があります。

```
user@switch# set protocols pim interface <interface_name> mode sparse
```

RP を確認するには、show pim rps を使用します。このコマンドの出力では、RP のアドレス、RP の学習方法、アクティブなマルチキャストグループの数、RP が転送可能なマルチキャストグループが示されます。

```
user@swtich> show pim rps
Instance:PIM.master
Address family INET
RP address                Type        Holdtime Timeout Groups Group prefixes
10.1.1.1                  static             0    None      1 224.0.0.0/4
```

PIM 隣接機器を確認するには、以下の show pim neighbors コマンドを使用します。

```
user@switch> show pim neighbors
Instance:PIM.master
B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority

Interface            IP V Mode        Option      Uptime Neighbor addr
ge-1/0/23.0           4 2             HPLG      02:18:42 10.1.2.2
```

show multicast route コマンドでは、特定マルチキャストグループのマルチキャストルートと、マルチキャスト送信元、上流および下流のマルチキャストパスが表示されます。

```
user@switch> show multicast route
Family:INET

Group:224.0.1.39
    Source:1.1.1.2/32
    Upstream interface: ge-0/1/0.0
    Downstream interface list:
        local ge-1/0/23.0
```

マルチキャストスイッチング

デフォルトでは、スイッチは、マルチキャストパケットをブロードキャストパケットと同様に扱います。すなわち、送信元ポートを除く、VLAN 内のすべてのポートにパケットがフラッディングされます。IGMP スヌーピングでは、ルーターとホスト間で送信される IGMP を監視することによりテーブルが作成され、VLAN ごとに L3 マルチキャストグループとスイッチポートを関連付けることにより、マルチキャストトラフィックが調整されます。これにより、マルチキャストパケットの転送先ポートがスイッチで認識されます。IGMP スヌーピングはデフォルトで有効になります。

IGMP をサポートしていないホストについては、以下のコマンドを使用してグループを手動で設定できます。

```
user@switch# set protocols igmp-snooping vlan <vlan_name> interface <interface_name>
static group <multicast_ip_group_address>
```

スイッチにより作成された IGMP スヌーピングテーブルを表示するには、show igmp-snooping membership コマンドを使用します。このコマンドの出力には、すべてのマルチキャストグループが VLAN 別に示されます。

```
user@switch> show igmp-snooping membership
VLAN: v2
    225.1.1.1      *               199 secs
        Interfaces: xe-0/0/1.0, xe-0/0/2.0, xe-0/0/3.0
```

EZQOS-Voice

EX シリーズでは、CoS（Class of Service）がサポートされます。この機能により、ビジネスアプリケーションの要件を満たしながら、特定のトラフィックがネットワークの遅延およびジッター要件を超えないようにすることができます。EX シリーズでは、ポートあたり 8 個の CoS キューがサポートされ、各キューは、最善の状態でビジネスニーズが満たされるように独自に形成することができます。アプリケーションで必要なサービスレベルが満たされるようにするために、エンドツーエンドで CoS を有効にすることをお奨めします。

図 5.2 に示すように、EX シリーズにおける CoS の基本的な構成要素は、分類、ポリシング、キューイング、スケジューリング、およびリマーキングです。CoS の設定には、十分な知識と QoS の設定が必要なため、大変な作業になる可能性があります。トラフィックをどのように分類すればよいか、帯域幅をどの程度割り当てればよいか、またキュー間にバッファをどの程度割り当てればよいかといった疑問は、どれも QoS を導入する際に直面する疑問です。

さらに詳しくは 2010 年第 4 四半期に John Wiley & Sons 社から出版が予定されている、ジュニパーネットワークスのエンジニアであるミゲル・バレイロスおよびピーター・ルンドクヴィストによる『*QoS-Enabled Networks*』は、QoS について解説された優れた著書です。 www.juniper.net/books で探してみてください。

図 5.2 EX シリーズの一般的な QoS ステージ

EZQOS-Voice により、複雑さが排除され、固定ベースおよびモジュラーベースの両方のスイッチにおけるベストエフォート、ビデオ、音声、およびネットワーク制御タイプのトラフィックの CoS 設定を効率化できます。また、トラフィック分類、トラフィックキューイング、およびトラフィックスケジューリングのための基本設定が提供されます。

注 EZQOS-Voice では、すべての QOS ステージが実装されるわけではありませんが、必要に応じて利用できます。EX シリーズの CoS の詳細については、EX シリーズの技術資料を参照してください（www.juniper.net/techpub/）。

トラフィックの分類

トラフィックの分類は最初の QoS プロセスで、スイッチが最初にトラフィックを受信した時点で行われます。スイッチは、トラフィックフローを分割することにより、その優先度設定に基づいてトラフィックを処理することができます。トラフィックの差別化は、以下のポート分類方法を使用して行うことができます。

- 動作集約（BA）：802.1P、DSCP、または IP Precedence に基づいてトラフィックを分類します。
- マルチフィールド分類子（MF）：L2、L3、および / または L4 情報に基づいてトラフィックを分類します。
- ポートベース：この方法ではトラフィックは差別化されませんが、すべての着信トラフィックが指定の転送クラスに関連付けられます。

EZQOS-VOICE では BA が使用され、DSCP 値に基づいてトラフィックが分類されます。その一部を表 5.1 に示します。パケットは、DSCP に基づいて特定のサービスクラスのサービスレベル、転送クラスに関連付けられます。転送クラスは、特定の送信キューにマッピングされます。

表 5.1 EZQOS-VOICE テンプレートのデフォルト設定

転送クラス	キュー	DSCP	スケジューラ
ベストエフォート	0	0-23、25、26-33、35-45、46-47、49-55、57-63	SDWRR
ビデオ	4	34	SDWRR
音声	5	46	絶対優先
ネットワーク制御	7	24、26、48、56	絶対優先

トラフィックのキューイング

トラフィックのキューイングで重要になる要因として、キューの数、キューの深さ、およびキューの管理があります。EX シリーズでは、ポートあたり最大 8 個のキューがサポートされ、そのうち 4 個が EZQOS-VOICE で使用されます。各キューは、特定のトラフィッククラス（転送クラス）を担当します。EZQOS-VOICE にはキュー 0、4、5、7 が使用され、それぞれベストエフォート、ビデオ、音声、およびネットワーク制御に関連付けられます。各キューには、トラフィックタイプとプラットフォームに応じて異なるバッファサイズが設定されます。

トラフィックのスケジューリング

キューに設定できるキュースケジューラには、絶対優先（strict-high）と SDWRR（low）の 2 つのタイプがあります。キューが strict-high に設定されている場合、このキューに入ったパケットは必ず優先処理されます。SDWRR に設定されているキューでは、重みに基づいて帯域幅が全体に配分されるように維持しながら、ラウンドロビン方式（優先度の高いキューから低いキューへ）でパケットが処理されます。

ベストエフォートとビデオに対する帯域幅の配分は、EX4200 スイッチでは 30/70、EX8200 では 20/50 です。音声およびネットワーク制御は絶対優先として扱われるため、キューに入った音声またはネットワーク制御パケットは即座に処理されます。

EZQOS-VOICE テンプレートは、/etc/config ディレクトリに *ezqos-voice.conf* ファイルとして保存されます。EZQOS-VOICE テンプレートをロードして設定にマージするには、`load merge` コマンドを使用します。

```
user@switch# load merge /etc/config/ezqos-voip.conf
```

注 EZQOS-VOICE は編集可能なテンプレートです。管理者は、ビジネスまたはネットワークの要件がより的確に満たされるように、このテンプレートを編集したり、このテンプレートを基に新しいテンプレートを作成したりできます。

このテンプレートは、Junos の group スタンザで *ezqos-voip* としてロードします。テンプレートは設定の一部ですが、EZQOS-VOICE 設定はアクティブになりません。

次のステップでは、Junos の CoS スタンザでグループ（ezqos-voip）を適用して EZQOS-VOICE 設定をアクティブにします。

```
user@switch# set class-of-service apply-groups ezqos-voip
```

最後に、分類子とスケジューラをインタフェースにバインドします。

```
user@switch# set class-of-service interfaces ge-0/0/0 unit 0 classifier dscp ezqos-
dscp-classifier
user@switch# set class-of-service interfaces ge-0/0/0 scheduler-map ezqos-voip-sched-
maps
```

ヒント アスタリスクを使用することにより、同様のインタフェース（ge や xe）に対する設定を簡素化し、繰り返しを減らすことができます。アスタリスクにより、同じタイプのすべてのインタフェースに同じ分類子やスケジューラが適用されるため、`set class-of-service interfaces ge-* unit 0 classifier dscp ezqos-dscp-classifier` とします。

Junos の CoS に関する show コマンドのほとんどは、show class-of-service スタンザにあります。`show interface <interface-name> extensive | find, <Cos Information>` または `show class-of-service interface <interface-name>` は、役立つサマリーコマンドです。

```
user@switch> show class-of-service interface ge-0/0/0
Physical interface: ge-0/0/0, Index:129
Queues supported:8, Queues in use:5
  Scheduler map: ezqos-voip-sched-maps, Index:37585

  Logical interface: ge-0/0/0.0, Index:2684275700
    Object            Name                    Type             Index
    Classifier        ezqos-dscp-classifier   dscp             57624
```

上記の show コマンドの出力例には、設定されている送信キューの数、設定されているスケジューラ、および設定されている分類子とそのタイプが示されています。

特定の分類子またはスケジューラマップの設定を表示するには、以下のコマンドを使用します。

```
user@switch> show class-of-service classifier name classifier-name
user@switch> show class-of-service scheduler-map scheduler-map-name
```

この他、適切なトラフィックキューイングの確認やパケットドロップの確認に役立つコマンドとして、`show interface interface-name [detail|extensive]| find <Queue counters>` コマンドや `show interface queue <interface-name>` コマンドがあります。

```
user@switch> show interfaces queue ge-0/0/0
Physical interface: ge-0/0/0, Enabled, Physical link is Down
  Interface index:129, SNMP ifIndex:501
Forwarding classes:16 supported, 5 in use
Egress queues:8 supported, 5 in use
Queue:0, Forwarding classes: ezqos-best-effort
  Queued:
```

```
    Packets              :Not Available
    Bytes                :Not Available
    Packets              :              41570904
    Bytes                :            5320940436
    Tail-dropped packets :                     0

<output truncated>
```

アクセスポートセキュリティ

イーサネット LAN 上の他のネットワークデバイスと同様に、イーサネットスイッチがアドレスのなりすましや中間者攻撃など悪意のある攻撃の標的になることも少なくありません（図 5.3 を参照）。そのため、EX シリーズイーサネットスイッチには、ネットワークアクセスを妨害し、生産性に悪影響を及ぼす可能性のあるこのような攻撃からアクセスポートを保護する多数のアクセスセキュリティ機能が備わっています。攻撃には多様なカテゴリーがありますが、EX シリーズ イーサネットスイッチでは、最小限の設定で適切なアクセスセキュリティ保護機能を選択的に設定することができます。

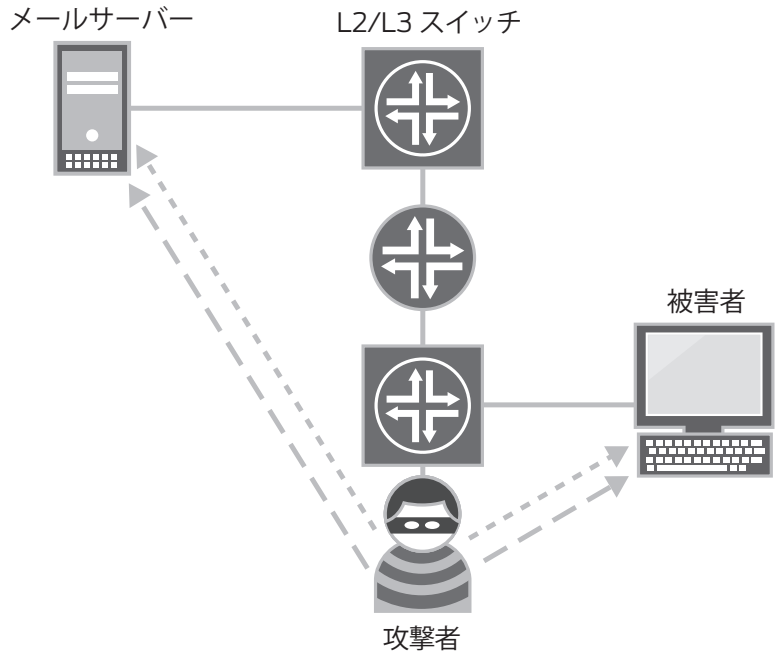
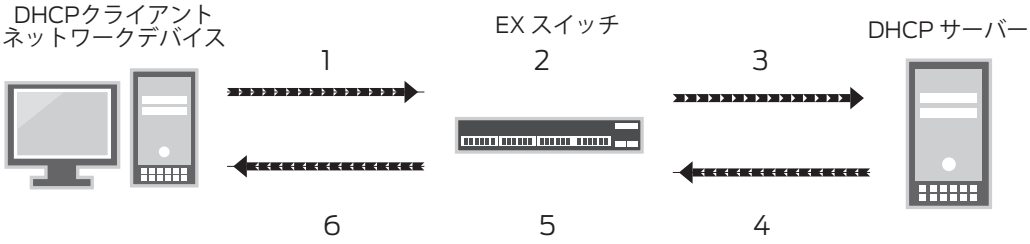


図 5.3 ゲートウェイになりすますハッカー（中間者攻撃）

DHCP スヌーピング

DHCP（Dynamic Host Configuration Protocol）は、IP アドレスを動的に（DHCP）クライアントに割り当て、アドレスを再利用できるようにアドレスを一時的にデバイスにリースします。DHCP によって取得した IP アドレスを必要とするエンドデバイスは、LAN を通して DHCP サーバーと通信する必要があります。

DHCP スヌーピングでは、スイッチが DHCP パケットを認識できるようにすることにより、不正な DHCP サーバーを阻止します。スイッチは、DHCP サーバーポートとして定義されていない（信頼されていないポート）に着信する DHCP サーバータイプのメッセージをアクティブにフィルタリングし、ブロックします。一方、スイッチは、DHCP スヌーピングエントリーで構成される DHCP スヌーピングバインディングデータベースを構築して維持し、ここにクライアントの MAC アドレス、DHCP プロセスによって取得した IP アドレス、ポート情報、VLAN 情報、DHCP リースに関するその他の情報を保存します。DHCP クライアントが IP アドレスを開放するか、DHCP のリースが期限切れになると、それに関連する DHCP スヌーピングバインディングエントリがデータベースから削除されます。



1. デバイスが、IPアドレスを要求する場合はDHCPDISCOVER、IPアドレスを受信またはリースする場合はDHCPREQUESTを送信します。
2. スイッチがパケットをスヌープします。IP-MACプレースホルダバインディングがデータベースに追加されます。
3. スイッチがDHCPDISCOVERまたはDHCPREQUESTを転送します。
4. サーバーが、アドレスを提示する場合はDHCPOFFER、アドレスをアサインする場合はDHCPACK、アドレス要求を拒否する場合はDHCPNAKを送信します。
5. スイッチがパケットをスヌープします。プレースホルダが存在する場合は、DHCPACK受信時にIP-MACバインディングと交換されます。
6. スイッチがDHCPOFFER、DHCPACK、またはDHCPNAKを転送します。

図 5.4 DHCP スヌーピングプロセス

ヒント DHCP スヌーピングは、DAI（Dynamic ARP Inspection）や IP ソースガードなどの他のアクセスポートセキュリティ機能の基盤となります。

EX シリーズで DHCP スヌーピングを有効にするときは、以下のガイドラインに留意してください。

1. クライアントが通常接続すると予測されるすべてのアクセスポートは信頼されていません。また、ネットワークインフラが面しているトランクポートはデフォルトで信頼されます。
2. 信頼されていないポートでは、*discoveries/requests* などの DHCP クライアントタイプメッセージのみが許可され、その他すべての DHCP パケットは破棄されます。スイッチは、これらのポートに関する DHCP スヌーピングデータベースも構築し、ここに、クライアントとサーバー間でやり取りされた DHCP の MAC アドレス、ポートの位置、VLAN、および IP バインディングが保存されます。
3. ネットワークデバイスを特定の VLAN から別の VLAN に移動した場合、通常、そのデバイスは新しい IP アドレスを取得する必要があります。これにより、DHCP スヌーピングバインディングデータベースの、VLAN ID を含むそのデバイスのエントリが更新されます。

不正な DHCP サーバーが LAN セグメント上の正当な DHCP サーバーになりすまし、DHCP クライアントにリースオファーを提供して、そのクライアントのネットワークアクセスを妨害するような状況で、DHCP スヌーピングは最も効果を発揮します。不正なサーバーは、DHCP リースオファーパケット内でそれ自体をネットワークのデフォルトゲートウェイとして割り当てる可能性もあり、これによって攻撃者は、ネットワークトラフィックを「のぞき見」して中間者攻撃を仕掛け、正当なデバイスやリソースのためのネットワークトラフィックを誤った方向に向けることができます。

DHCP スヌーピング機能は、VLAN ごとに有効にすることができます。EX シリーズ イーサネットスイッチで DHCP スヌーピング機能を有効にするには、以下の設定を使用します。

```
user@switch# set ethernet-switching-options secure-access-port vlan vlan_name
examine-dhcp
```

トランクポートではなくアクセスポートでスイッチに接続されているローカル DHCP サーバーがある場合、ポートの特性を「untrusted」から「trusted」に変更する必要があります。

また、DHCP サーバーインタフェースのセキュリティを物理的に確保することも重要です。ポートを信頼されたポートとして設定する前に、サイトで DHCP サーバーへのアクセスを監視し、制御することをお奨めします。

```
user@switch# set ethernet-switching-options secure-access-port interface interface_
name dhcp-trusted
```

スタティック IP アドレスを持ち、DHCP を使用しないデバイスについて、DHCP スヌーピングデータベースにスタティックエントリーを設定するには、以下のコマンドを使用します。

```
user@switch# set ethernet-switching-options secure-access-port interface <interface_
name> static-ip <ip_address mac mac_address vlan vlan_name>
```

注 デフォルトでは、スイッチを再起動すると IP-MAC のバインディングが失われるため、DHCP クライアント（ネットワークデバイスまたはホスト）はバインドを取得しなおす必要があります。ただし、dhcp-snooping-file ステートメントを設定してデータベースファイルをローカルまたはリモートに保存することにより、バインディングを存続させることができます。

以下のコマンドにより、DHCP スヌーピングバインディングデータベースが表示されます。

```
user@switch> show dhcp snooping binding

DHCP Snooping Information:
MAC address         IP address    Lease (seconds)  Type     VLAN             Interface

00:01:23:45:67:89  192.168.1.10  -                 static   corp-access    ge-0/0/10.0
00:01:23:45:67:90  192.168.2.11  653               dynamic  corp-access    ge-0/0/11.0
00:01:23:45:67:91  192.168.2.12  720               dynamic  corp-access    ge-0/0/12.0
```

DAI（Dynamic ARP Inspection）

ネットワーク（イーサネットネットワークなど）上で IP パケットを送信するには、IP アドレス（レイヤー 3）をイーサネット MAC アドレス（レイヤー 2）にマッピングする必要があります。ARP（Address Resolution Protocol）は、イーサネット LAN 上の MAC アドレスを IP アドレスにマッピングするために使用されます。

ネットワークデバイスは、このマッピングを ARP キャッシュで維持し、他のネットワークデバイスにパケットを転送するときにこのキャッシュを照会します。ARP キャッシュに宛先デバイスの既存エントリーが保持されていない場合、デバイスは、宛先デバイスのアドレスを求める ARP 要求をブロードキャストし、その応答をキャッシュに保存します。

DAI（Dynamic ARP Inspection）では、ネットワーク上の ARP パケットの妥当性が確認されます。スイッチは、アクセスポートから送信された ARP パケットを傍受し、DHCP スヌーピングによって作成された IP-MAC データベース（DHCP スヌーピングバインディングデータベース）に照会します。すなわち、この機能では、DHCP スヌーピン

グで定義されている信頼されていないポートから ARP パケットを受信したときにフィルタリングに関する決定を行うために、DHCP スヌーピングが使用されます。不一致が見つかった場合、その ARP パケットは破棄されるため、ARP なりすまし / 汚染などの中間者攻撃を防ぐことができます。

警告！ DAI は DHCP スヌーピング、特に DHCP スヌーピングバインディングデータベースに完全に依存することを覚えておいてください。バインディングデータベースに対応する DHCP スヌーピングエントリーがない場合、信頼されていないポートで受信された ARP パケットはすべて破棄されます。

注 DAI および IP ソースガードにおける信頼されていないポートおよび信頼されたポートの概念は、DHCP スヌーピング機能のものと同じです。

ARP なりすまし攻撃では、攻撃者は、ARP パケットを生成してネットワークに送信し、通常はこれによって中間者攻撃を仕掛けます。攻撃者は、LAN 上にある別のデバイス（標的）の MAC アドレスになりすました ARP パケットを送信することにより、それ自体の MAC アドレスを、スイッチに接続されたネットワークデバイスの IP アドレスに関連付けます。一般的な ARP なりすましでは、Gratuitous ARP が使用されます。これは、エンドホストなどのネットワークデバイスがそれ自体の IP アドレスを解決するための ARP 要求を送信するときに使用される ARP パケットです。標準的な LAN では、この Gratuitous ARP メッセージに、同じ MAC アドレスを持つデバイスが 2 台存在することが示されます。Gratuitous ARP メッセージは、エンドホストのネットワークインタフェースカードが変更されたときや、デバイスが再起動したときにも送信され、LAN 上の他のネットワークデバイスはこの情報を基にそれぞれの ARP キャッシュを更新します。

ただし、ARP なりすまし攻撃では、攻撃者は、それ自体をターゲットデバイスとしてアナウンスすることにより、悪意をもってデバイスの ARP キャッシュを汚染します。その IP アドレスに送信されるトラフィックは、代わりに攻撃者に送信されるため、正当なデバイスが妨害されます。正当なデバイス宛てのトラフィックを受信した攻撃者は、パケットをのぞき見したり中間者攻撃を仕掛けるなど、さまざまなタイプの悪質な行為を行うことができます（中間者攻撃では、攻撃者は、2 つのホスト間のメッセージを傍受して読み、場合によっては改ざんし、通信が妨害されていることを元のホストに気付かれることはない）。

DAI 機能も VLAN ごとに有効にすることができます。EX シリーズ イーサネットスイッチで DAI 機能を有効にするには、以下の設定を使用します。

```
user@switch# set ethernet-switching-options secure-access-port vlan vlan_name arp-
inspection
```

DAI 統計情報を表示するには、以下の show コマンドを使用します。

```
user@switch> show arp inspection statistics

ARP inspection statistics:
Interface        Packets received  ARP inspection pass   ARP inspection failed
---------------  ----------------  --------------------  ---------------------
ge-0/0/10.0                    9                       9                      0
ge-0/0/11.0                   30                      30                      0
ge-0/0/12.0                   25                      24                      1
```

IP ソースガード

IP ソースガードは、イーサネット LAN での IP なりすまし攻撃に効果的です。通常、IP なりすましは、攻撃者が、LAN 管理者により実際の攻撃元が特定されないようにするために使用します。IP ソースガード機能は DAI（Dynamic ARP Inspection）に似ていますが、信頼されていないポートでデバイスから送信される ARP パケットではなく IP パケットに適用されます。

ヒント 一般的な形態の IP なりすましとして DoS 攻撃があります。この攻撃の攻撃者は、実際の攻撃元を隠しながら、正常に機能できない状態にデバイスを陥れるために、標的に大量の TCP SYN パケットを送りつけます。

IP ソースガード機能は、信頼されていないポートでデバイスから送信された IP パケットを調べてフィルタリングの決定を行うために DHCP スヌーピングバインディングデータベースを必要とするため、EX シリーズの DHCP スヌーピング機能を使用します。IP ソースガードは、IP 送信元アドレスとそれを受信したポートを照合し、パケットが DHCP スヌーピングバインディングデータベースと一致しない場合は、そのパケットを破棄します。IP ソースガード機能は、VLAN ごとに設定します。

```
user@switch# set ethernet-switching-options secure-access-port <vlan_name> ip-source-guard
```

show ip-source-guard コマンドでは、IP ソースガード情報が表示されます。

```
user@switch> show ip-source-guard

IP source guard information:
Interface    Tag  IP Address   MAC Address        VLAN

ge-0/0/11.0  0    192.168.2.11  00:01:23:45:67:90  corp-access
ge-0/0/12.0  0    192.168.2.12  00:01:23:45:67:91  corp-access
```

さらに詳しくは アクセスポートセキュリティの CLI 設定の詳細については、『*Port Security on EX Series Switches Guide*』を参照してください（www.juniper.net/techpubs/）。

PoE（Power over Ethernet）給電機能

PoE（Power over Ethernet）給電機能は、銅線イーサネット LAN ケーブルで電力を供給する機能です。PoE は、IEEE 802.3af として標準的に定義されており、電力供給機器（PSE）からの出力において、安定化された 15.4 ワットの電力を供給することを規定しています。図 5.5 に示すように、この電力は、VoIP 電話、無線アクセスポイント、IP ベースのビデオカメラなど、接続された給電デバイス（PD）で使用されます。

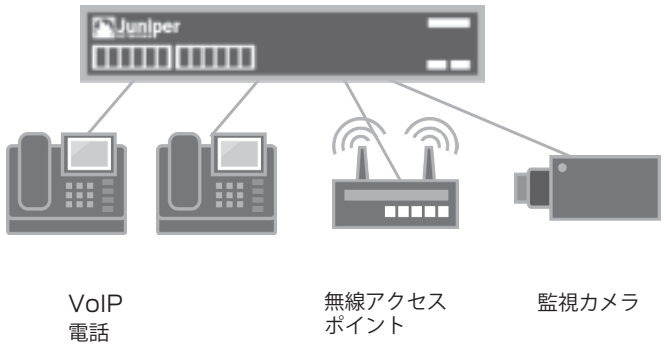


図 5.5 EX4200 スイッチに接続された給電デバイス（PD）

データ送信に使用されるものと同じイーサネット LAN ケーブルで電力を供給できるため、PD を電源に接続する必要がありません。また、デバイス導入の簡素化、導入コストの軽減、柔軟性の向上、リモート管理などのメリットももたらされます。

EX2200、EX3200、EX3300、EX4200、EX6200、および EX8200 スイッチでは、すべて PoE がサポートされ、この場合、スイッチは PSE として機能します。EX4200 スイッチでは、すべてのモデルで完全または部分的な PoE が提供されます（ファイバーベースの EX4200-24F モデルを除く）。完全な PoE モデルでは、24 または 48 ポートのすべてで電力が供給され、部分的な PoE モデルでは、最初の 8 ポートのみで電力が供給されます。

注 PoE をサポートする固定構成タイプの EX シリーズでは、デフォルトで PoE が有効になります。PD を給電ポートに接続するだけで、PoE が有効になります。

PoE を設定するには、以下の CLI コマンドを使用します。

```
user@switch# set poe interface all
```

EX シリーズスイッチでは、PoE 管理に以下の 2 つのモードを使用できます。

- スタティックモード：名称が示しているとおり、このモードでは、スイッチの使用可能な電力消費のうちの指定電力量が個々のインタフェースに割り当てられます。
- クラスモード：ポートに接続された PD のクラスに基づいて電力がインタフェースに割り当てられます。割り当てられる電力量は、PD のクラスの最大になります。各 PoE クラスと対応する電力割り当て範囲については、表 5.2 を参照してください。

表 5.2 PoE クラスと電力割り当て

PoE クラス	PSE の出力ポートにおける最大電力
0	15.4 ワット予約済み
1	4 ワット
2	7 ワット
3	15.4 ワット

警告！ デフォルトの PoE 管理モードはスタティックモードです。EX2200 では、モードをスタティックからクラスに変更することをお奨めします。詳細については、www.juniper.net/techpubs/ を参照してください。

注 表 5.2 に PSE の出力電力量を示しましたが、実際に PD が受け取る電力では線路損失を考慮する必要があります。例えば、クラス 3 の PoE の場合、電力損失を考慮して、表に示された 15.4 ワットから 16% を減算します。これにより、PD で保証される電力は 12.95 ワットになります。IEEE 802.3af 準拠の PD は、最大 12.95 ワットを必要とします。

PoE 電力管理モードを変更するには、`set poe management class` コマンドを使用します。

```
user@switch# set poe management class
```

EX シリーズの PoE ステータスを確認するには、show poe interface コマンドを使用します。

```
user@switch> show poe interface
Interface Admin status Oper status Max power Priority Power consumption Class
 ge-0/0/0 Enabled      ON          15.4W     Low      12.95W     0
 ge-0/0/1 Enabled      ON          15.4W     Low      12.95W     0
 ge-0/0/2 Enabled      ON          15.4W     Low      12.95W     0
 ge-0/0/3 Enabled      ON          15.4W     Low      12.95W     0
 ge-0/0/4 Enabled      ON          15.4W     Low      12.95W     0
 ge-0/0/5 Enabled      ON          15.4W     Low      12.95W     0
 ge-0/0/6 Enabled      ON          15.4W     Low      12.95W     0
 ge-0/0/7 Enabled      ON          15.4W     Low      12.95W     0

user@switch> show poe interface ge-0/0/0
PoE interface status:
PoE interface                :ge-0/0/0
Administrative status        :Enabled
Operational status           :ON
Power limit on the interface :15.4W
Priority                     :Low
Power consumed               :12.95W
Class of power device        :0

user@switch> show poe controller
Controller  Maximum   Power              Guard band  Management
index       power     consumption
   0        305 W       0W                 0W        Static
```

EX シリーズスイッチでは、PoE 電力消費とインタフェースを通した配電をトラッキングするために、他の方法も使用できます。

- EX シリーズは、電力スパイクに対応するために限定量の電力（最大 19 ワット）を予約できます。これは、guard-band を使用して設定できます。

  ```
  user@switch# set poe guard-band 15
  ```

- 接続された PD に対する PoE 電力消費が不足している場合、インタフェースに PoE 優先度（*high* または *low*）を設定し、優先度 high として指定されたインタフェースで電力が保証されるようにすることができます。電力消費が限定されている場合、優先度 high のインタフェースが優先され、優先度 low のインタフェースには電力が供給されません。

注 ビジネスに不可欠な PoE PD を優先度 high のインタフェースに配置することをお奨めします。これにより、スイッチの電力消費が低下した場合も、これらのデバイスに継続的に電力が供給されます。

インタフェースの PoE 優先度を変更するには、以下の CLI コマンドを使用します。

```
user@switch# set poe interface ge-0/0/0 priority high
```

また、インタフェースごとの PoE 電力消費は、以下のテレメトリを使用して監視できます。

```
user@switch# set poe interface all telemetries
```

注 PoE の追加サポートの設定に関する詳細については、www.juniper.net/techpubs/ を参照してください。

ポートミラーリング

通常、EX4200 などのイーサネットスイッチは、宛先 MAC アドレスが分かっているときは、すべてのパケットをフラッディングするわけではありません。ただし、当初の宛先インタフェースとは異なるインタフェースでのトラフィック分析のために、パケットのコピーを受信する必要がある場合もあります。ポートミラーリングを使用することにより、レイヤー 2 の EX シリーズ イーサネットスイッチのトラフィックを分析することができます。ポートミラーリングは、ネットワークを適切に使用するためのビジネスおよびネットワークポリシーを適用する目的で、またトラブルシューティング時にノードまたはアプリケーションによる異常または過剰な帯域幅の使用などの問題を特定するために使用できます。

ポートミラーリングでは、送信元から宛先に送信されるパケットがコピーされます。この送信元と宛先の対は、ポートミラーリングの*セッション*と見なされます。ミラーリングされたパケットは、プロトコルアナライザーアプリケーションを使用して分析できます。プロトコルアナライザーは、宛先ポートに直接ローカル接続されたホスト（図 5.5 を参照）、またはリモートのモニタリングステーションで実行できます。このモニタリングステーションは、宛先として設定された VLAN を持つ異なるイーサネットスイッチ上にあってもかまいません（図 5.6 を参照）。

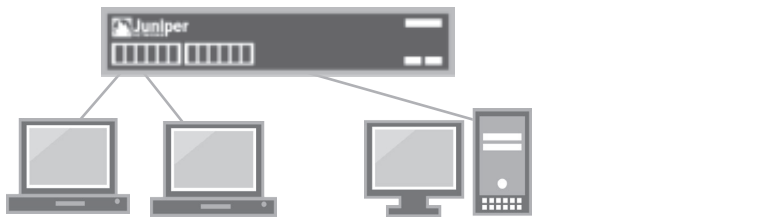


図 5.6 ローカルポートモニタリング

図 5.7 リモートポートモニタリング

警告！ ポートモニタリングは、EX シリーズ イーサネットスイッチのハードウェアレベルに実装されます。そのため、EX シリーズ イーサネットスイッチのモデルによって、ハードウェア機能が異なります。例えば、システムあたりサポートされるセッション数は、EX4200 では 1 セッションですが、EX8200 では 7 セッションです。詳細なガイドラインについては、『*Understanding Port Mirroring on EX Series Switches*』を参照してください（www.juniper.net）。

パケットをミラーリングする方法は多数あります。

- ポートに入ってくる（受信）および / またはポートから出ていく（送信）パケット
- 複数のポートをミラーリングセッションの送信元にすること可能
- VLAN に入ってくる（受信）および / または出ていく（送信）パケット

警告！ ポートミラーリングを設定するときは、いくつかの制限を考慮する必要があります。ポートミラーリングセッションの送信元ポートを宛先ポートにすることはできません。また、宛先ポートは、STP（Spanning Tree Protocol）などのレイヤー 2 プロトコルには参加しません。これらの制限の詳細については、www.juniper.net/techpubs/ を参照してください。

ポートミラーリングの送信元を設定するには

1. ミラーリングの送信元にするインタフェースに受信パケットを設定します。

```
user@switch# set ethernet-switching-options analyzer LOCAL-MIRROR input ingress
interface ge-0/0/0.0
```

2. ミラーリングの送信元にするインタフェースに送信パケットを設定します。

```
user@switch# set ethernet-switching-options analyzer LOCAL-MIRROR input egress
interface ge-0/0/1.0
```

3. ミラーリングの送信元にするVLANに受信パケットを設定します。

```
user@switch# set ethernet-switching-options analyzer LOCAL-MIRROR input ingress vlan
Employee_VLAN
```

ポートミラーリングの宛先を設定するには

1. ポートを宛先として設定します。

```
user@switch# set ethernet-switching-options analyzer LOCAL-MIRROR output interface
ge-0/0/10.0
```

ミラーリングされたパケットを、プロトコルアナライザーアプリケーションが実行されているリモートのモニタリングステーションに転送するには

1. 宛先として設定可能な VLAN を設定します。

```
user@switch# set ethernet-switching-options analyzer REMOTE-MIRROR output vlan
Mirror_VLAN
```

ポートミラーリングセッションの設定は、show analyzer コマンドで確認できます。

```
user@switch> show analyzer
  Analyzer name                 :LOCAL-MIRROR
  Output interface              :ge-0/0/10.0
  Mirror ratio                  :1
  Loss priority                 :Low
  Ingress monitored interfaces :ge-0/0/0.0
  Egress monitored interfaces  :ge-0/0/1.0
```

EX シリーズ イーサネットスイッチでは、ミラーリングの統計サンプリングがサポートされます。これにより、1:x など、設定された割合でパケットをミラーリングできます。デフォルトでは、この割合は 1 です。すなわち、すべてのパケットがミラーリングされます（1:1 の割合）。この割合は、最大 2047 まで増加させることができます。この場合、指定送信元で 2047 パケットごとに 1 パケットがミラーリングされます。ミラーリングする割合をデフォルト値（1）から変更するには、以下のコマンドを使用します。

```
user@switch# set ethernet-switching-options analyzer MIRRORING ratio 1000
```

デフォルトでは、ミラーリングされたパケットにはロス優先順位 low が割り当てられます。すなわち、ミラーリングされたパケットの優先度は通常のトラフィックより低くなり、輻輳状態になった場合には、より低い優先度のパケットが破棄されます。この設定は、必要に応じて high に設定できます。

ロス優先順位を high に設定するには、以下のコマンドを使用します。

```
user@switch# set ethernet-switching-options analyzer MIRRORING loss-priority high
```

また、すべてのパケットではなく、特に選択されたパケットがミラーリングの送信元を通過しなければならないことがよくあります。EX シリーズ イーサネットスイッチでは、ポリシーベースのポートミラーリングが可能です。すなわち、特定のパケットを選択してアナライザーにミラーリングするようにファイアウォールフィルターを設定することができます。ファイアウォールフィルターを使用したポリシーベースのミラーリングの詳細については、www.juniper.net/techpubs/ を参照してください。

次のステップと参照 URL

www.juniper.net/dayone

本書の印刷版を読んでいる場合、このブックレットの PDF 版をダウンロードしたり、現在入手可能な他の Day One ブックレットを見つけるには、以下のサイトにアクセスしてください。

www.juniper.net/junos

Junos の導入およびトレーニングに関して必要なすべての情報は以下のサイトで入手できます。

http://forums.juniper.net/jnet

ジュニパーネットワークスがスポンサーとなっている J-Net コミュニケーションフォーラムは、ジュニパーネットワークスの製品、テクノロジー、およびソリューションに関する情報、ベストプラクティス、および疑問点を共有するための場です。是非、この無料フォーラムに参加登録してください。

www.juniper.net/techpubs

このサイトでは、ジュニパーネットワークスが開発したすべての製品資料を無料で利用できます。各製品シリーズのページから、Junos オペレーティングシステムに関する必要な情報を見つけてください。

www.juniper.net/books

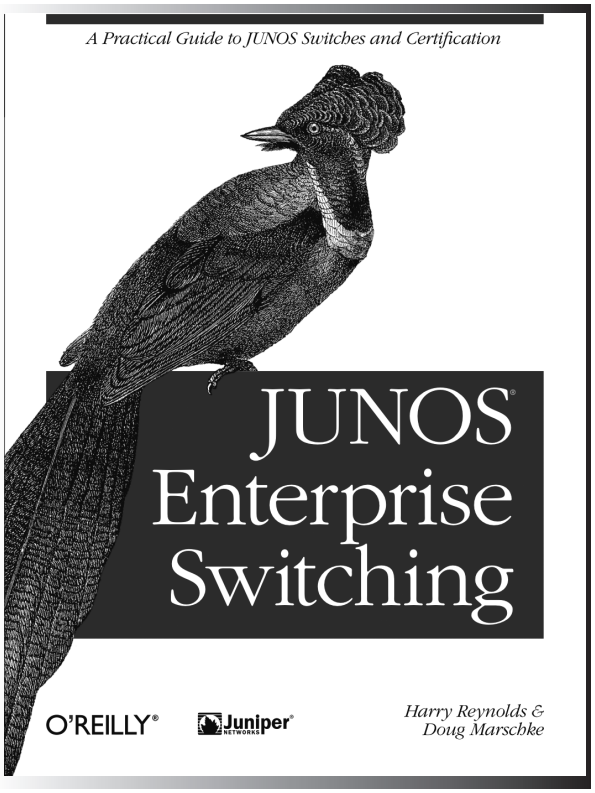
ジュニパーネットワークスは複数の出版社と協力し、ネットワーク管理者にとって不可欠なトピックを扱った技術書を制作、出版しています。新たな SRX 固有の『Junos Security』を含む書籍がどんどん出版されていますので、是非ご覧ください。

www.juniper.net/training/fasttrack

トレーニングコースをオンライン、オンサイト、または世界中にあるパートナートレーニングセンターで受講できます。ジュニパーネットワークス技術認定資格プログラム（JNTCP）では、ジュニパーネットワークス製品の設定およびトラブルシューティング能力を示すことにより、認定資格を取得することができます。エンタープライズルーティング、スイッチング、またはセキュリティの認定資格を短期間で取得したい方は、オンラインコース、受講者ガイド、およびラボガイドをご利用ください。

EX シリーズ イーサネットの決定版

*『Junos Enterprise Switching』*は、ジュニパーネットワークスの新たなイーサネットスイッチング EX 製品プラットフォームについて詳細に解説した唯一の技術書です。EX プラットフォームの優れたハードウェアおよび ASIC 設計は、まさに驚くべきものであり、その真の威力は Junos にあります。Junos は、実環境で実証された堅牢な実績ある主力製品であり、地球上の大規模なサービスプロバイダネットワークで活用されています。著者であるハリー・レイノルド氏とダグ・マーシュキー氏はその理解者であり、*『Junos Enterprise Switching』* を読むことで、読者も理解することができます。この書籍は、イーサネットスイッチング EX プラットフォームの優れた実践ガイドとして現場で利用でき、各章の最後に掲載されている演習問題は、JNTCP エンタープライズコースの認定資格試験の学習ガイドとして役立ちます。すでに認定資格を取得している方もそうでない方も、以下の内容を学習できます。



- エンタープライズスイッチングとバーチャル LAN（VLAN）
- スパニングツリープロトコルとその必要性
- ルートテーブルやプリファレンスなど、VLAN 相互のルーティング
- ルーティングポリシーとファイアウォールフィルタ
- DHCP スヌーピングなどのスイッチングセキュリティ
- VLAN 音声などのテレフォニーの統合

技術書を扱っている書店で入手できます。この書籍、およびジュニパーネットワークス技術ライブラリのその他書籍の詳細については、www.juniper.net/books を参照してください。