Cisco IE 3000 スイッチ ソフトウェア コンフィギュレーション ガイド

Cisco IE 3000 Switch Software Configuration Guide

Cisco IOS Release 12.2(55)SE
2010 年 8 月

Text Part Number: OL-13018-05-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

はじめに

対象読者

このマニュアルは、IE 3000 スイッチ（以降、*スイッチ*と表記）を管理するネットワーキング専門家を対象としています。また、Cisco IOS ソフトウェアの使用経験があることと、イーサネットと LAN の概念および用語を理解していることも前提としています。

目的

Catalyst 3560 スイッチは IP ベース イメージまたは IP サービス イメージのどちらか一方でサポートされます。IP ベース イメージは、Access Control List（ACL; アクセス コントロール リスト）、Quality of Service（QoS）、スタティック ルーティング、Routing Information などのレイヤ 2+ 機能を備えています。ルーティング情報 IP サービス イメージは、さらに高度なエンタープライズ クラスの機能を備えています。これには、レイヤ 2+ 機能およびフル レイヤ 3 ルーティング（IP ユニキャスト ルーティング、IP マルチキャスト ルーティング、およびフォールバック ブリッジング）が含まれています。また、それを レイヤ 2+ スタティック ルーティングや RIP と区別するために、この IP サービス イメージでは、Enhanced IGRP（EIGRP）や Open Shortest Path First（OSPF）といったプロトコルを搭載しています。

IE 3000 スイッチは、レイヤ 2 LAN Base イメージまたはレイヤ 3 IP サービス イメージでサポートされています。レイヤ 3 ルーティング機能をサポートするには、スイッチで IP サービス イメージを実行している必要があります。

このマニュアルには、スイッチの Cisco IOS ソフトウェア機能を設定するために必要な情報が記載されています。

このマニュアルでは、スイッチで使用するために作成または変更されたコマンドの使用方法について説明します。これらのコマンドの詳細については説明しません。これらのコマンドの詳細については、このリリースの『*IE 3000 Switch Command Reference*』を参照してください。標準 Cisco IOS Release 12.2 コマンドについては、Cisco.com のホームページにアクセスして（[Documentation] > [Cisco IOS Software]）、Cisco IOS のマニュアル セットを参照してください。

このマニュアルでは、スイッチの管理に使用できる組み込みデバイス マネージャや Cisco Network Assistant（以降、*Network Assistant* と表記）の GUI（グラフィカル ユーザ インターフェイス）の詳細については説明しません。ただし、このマニュアルで説明する概念は、GUI ユーザにも当てはまります。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。Network Assistant の詳細については、Cisco.com の『*Getting Started with Cisco Network Assistant*』を参照してください。

このマニュアルでは、表示されるシステム メッセージやスイッチの設置手順については説明しません。詳細については、このリリースの『*IE 3000 Switch System Message Guide*』および『*IE 3000 Switch Hardware Installation Guide*』を参照してください。

資料の更新については、このリリースに対応するリリース ノートを参照してください。

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

- コマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。
- 角カッコ（[ ]）の中の要素は、省略可能です。
- 必ずどれか 1 つを選択しなければならない要素は、波カッコ（{ }）で囲み、縦棒（|）で区切って示しています。
- 任意で選択する要素の中で、必ずどれか 1 つを選択しなければならない要素は、角カッコと波カッコで囲み、縦棒で区切って（[{ | }]）示しています。

対話形式の例では、次の表記法を使用しています。

- 端末セッションおよびシステムの表示は、`screen` フォントで示しています。
- ユーザが入力する情報は、**太字の `screen`** フォントで示しています。
- パスワードやタブのように、出力されない文字は、かぎカッコ（< >）で囲んで示しています。

注、注意、およびワンポイント アドバイスには、次の表記法および記号を使用しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

以下に挙げる、スイッチに関する詳細情報が記載されているマニュアルは、次の Cisco.com サイトから入手できます。
http://www.cisco.com/en/US/products/ps9703/tsd_products_support_series_home.html

（注） スイッチの取り付け、設定、アップグレードを行う前に、次のマニュアルを参照してください。

- 初期設定情報については、入門ガイドの「Using Express Setup」またはハードウェア インストレーション ガイドの付録「Configuring the Switch with the CLI-Based Setup Program」を参照してください。
- デバイス マネージャの要件については、リリース ノート（発注できませんが、Cisco.com で入手可能）の「System Requirements」を参照してください。
- Network Assistant の要件については、『*Getting Started with Cisco Network Assistant*』（発注できませんが、Cisco.com で入手可能）を参照してください。

- クラスタの要件については、『*Release Notes for Cisco Network Assistant*』（発注できませんが、Cisco.com で入手可能）を参照してください。
- アップグレード情報については、リリース ノートの「Downloading Software」を参照してください。

スイッチに関するその他の情報については、以下の資料を参照してください。

- 『*Release Notes for the Cisco IE 3000 Switch*』
- 『*Cisco IE 3000 Switch Command Reference*』
- 『*Cisco IE 3000 Switch System Message Guide*』
- デバイス マネージャのオンライン ヘルプ（スイッチで利用可能）
- 『*Cisco IE 3000 Switch Hardware Installation Guide*』
- 『*Cisco IE 3000 Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch*』
- 『*Getting Started with Cisco Network Assistant*』
- 『*Release Notes for Cisco Network Assistant*』
- Network Admission Control（NAC）機能の詳細については、『*Network Admission Control Software Configuration Guide* 』を参照してください。
- Cisco Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）、SFP+、および Gigabit Interface Converter（GBIC; ギガビット インターフェイス コンバータ）モジュールに関する情報は、Cisco.com の次のページから入手できます。
  http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

  SFP 互換性マトリクス ドキュメントは、Cisco.com の次のページから入手できます。
  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

概要

この章では、IE 3000 スイッチ ソフトウェアについて説明します。この章の内容は次のとおりです。

このマニュアルでは、特に IP Version 6（IPv6）に言及していない限り、IP という用語は IP Version 4（IPv4）を指します。

機能

このスイッチには、次のいずれかのソフトウェア イメージがすでにインストールされています。

- LAN ベースのイメージは、Access Control List（ACL; アクセス制御リスト）や Quality of Service（QoS; サービス品質）などの基本的なレイヤ 2 インテリジェント機能をサポートします。
- IP サービス イメージには、すべてのレイヤ 2+ 機能と、すべてのレイヤ 3 ルーティング（IP ユニキャスト ルーティング、IP マルチキャスト ルーティング、フォールバック ブリッジング）が含まれています。

この章で説明する機能の中には、暗号化（暗号化をサポートする）バージョンのソフトウェアでしか使用できないものがあります。この機能を使用するため、および Cisco.com から暗号化バージョンのソフトウェアをダウンロードするためには、許可を得る必要があります。詳細については、このリリースに対応するリリース ノートを参照してください。

Ease-of-Deployment 機能および Ease-of-Use 機能

- Express Setup により、最初にブラウザベースのプログラムから、スイッチの基本 IP 情報、連絡先情報、スイッチおよび Telnet のパスワード、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）情報をすばやく設定できます。Express Setup の詳細については、クイック スタート ガイドを参照してください。
- ユーザ定義および Cisco のデフォルトの SmartPort マクロにより、カスタム スイッチ コンフィギュレーションを作成して、ネットワーク経由での配置を簡素化できます。
- 着脱式のコンパクト フラッシュ カードに、Cisco IOS ソフトウェア イメージと、スイッチのコンフィギュレーション ファイルが格納されています。ソフトウェア機能を再設定せずに、スイッチの交換やアップグレードを実行できます。更新版のブート ローダーに含まれるセカンダリ ブート ローダー イメージがサポートするコンパクト フラッシュ ファイル システム ドライバにより、コンパクト フラッシュ メモリ カードにアクセスできます。スイッチのブート ローダーにはプライマリ ブート ローダーとセカンダリ ブート ローダーが含まれ、どちらもブート フラッシュに格納されています。
- 組み込みデバイス マネージャの GUI により、Web ブラウザから単一スイッチの設定とモニタを実行できます。デバイス マネージャの起動の詳細については、クイック スタート ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Cisco Network Assistant（以後、*Network Assistant と表記*）により、次のことを実行できます。
  - コミュニティを管理できます。コミュニティはクラスタのような装置グループですが、ルーターとアクセス ポイントを含めることができ、セキュリティを強化できます。
  - イントラネット内の任意の場所からスイッチとスイッチ クラスタの管理を簡素化および最小化できます。
  - 特定の作業を実行する CLI（コマンドライン インターフェイス）コマンドを覚えなくても、単一のグラフィカル インターフェイスから複数の設定作業を実行できます。
  - 対話式のガイド モードで、VLAN、ACL、Quality of Service（QoS）などの複雑な機能をガイドに従って設定できます。
  - コンフィギュレーション ウィザードのプロンプトに従って、必要最小限の情報を指定するだけで、トラフィックの QoS プライオリティ、データ アプリケーションのプライオリティ レベル、セキュリティなどの複雑な機能を設定できます。
  - スイッチにイメージをダウンロードできます。
  - VLAN 設定と QoS 設定、目録レポートと統計レポート、リンク レベルとスイッチ レベルのモニタおよびトラブルシューティング、複数のスイッチ ソフトウェアのアップグレードなど、複数のポートや複数のスイッチに対して同時にアクションを適用できます。
  - 相互接続された装置のトポロジを表示して、既存のスイッチ クラスタとクラスタに参加できる適格なスイッチを識別し、スイッチ間のリンク情報を識別できます。
  - フロントパネル イメージで表示される LED から、1 つまたは複数のスイッチのリアルタイム ステータスをモニタできます。イメージに表示されるシステム LED、Redundant Power System（RPS; 冗長電源システム）LED、およびポート LED の色は、物理的な LED の色と類似しています。

（注） Network Assistant は cisco.com/go/cna からダウンロードする必要があります。

- スイッチ クラスタリング テクノロジーにより、次のことが可能になります。
  - 複数のクラスタ対応スイッチの設定、モニタ、認証、ソフトウェア アップグレードをまとめて実行できます。地理的な距離や相互接続メディア（イーサネット、ファスト イーサネット、Fast EtherChannel、Small Form-Factor Pluggable（SFP）モジュール、ギガビット イーサネット、Gigabit EtherChannel 接続など）は問いません。クラスタ対応スイッチのリストについては、リリース ノートを参照してください。
  - 候補スイッチを自動検出し、単一 IP アドレスを通して管理できるスイッチ（最大 16 台）のクラスタを作成できます。
  - コマンド スイッチに直接接続していないクラスタ候補を拡張検出できます。

パフォーマンス機能

- Cisco EnergyWise により、Power over Ethernet（PoE）デバイスおよび非シスコ デバイスを含むエンド ポイントのエネルギー使用量を管理します。詳細については、『*Cisco EnergyWise Configuration Guide*』を参照してください。
- すべてのスイッチ ポートの速度自動検知、およびデュプレックス モードの自動ネゴシエーションにより、帯域幅の利用を最適化します。
- 10/100 インターフェイス、10/100/1000 Mb/s インターフェイス、および 10/100/1000 BASE-TX SFP モジュール インターフェイス上の Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能により、インターフェイスが自動的に必要なケーブル接続タイプ（ストレートまたはクロス）を検出し、接続を適切に設定できるようにします。
- ルーテッド フレームでは最大 1546 バイト、ハードウェアでブリッジングされるフレームでは最大 9000 バイト、ソフトウェアによってブリッジングされるフレームでは最大 2000 バイトをサポートします。
- 全ポート上で IEEE 802.3x フロー制御を行います（スイッチはポーズ フレームを送信しません）。
- EtherChannel により、耐障害性を高め、スイッチ、ルータ、およびサーバ間に最大 8 Gbps（ギガビット EtherChannel）または 800 Mbps（ファスト EtherChannel）全二重の帯域幅が確保されます。
- Port Aggregation Protocol（PAgP; ポート集約プロトコル）および Link Aggregation Control Protocol（LACP）により、EtherChannel リンクが自動的に作成されます。
- レイヤ 2 およびレイヤ 3 のパケットをギガビットのラインレートで転送します。
- マルチキャスト Virtual Routing and Forwarding（VRF; 仮想ルーティング / 転送）Lite により、ネットワークの仮想化およびマルチキャスト仮想私設網に使用する複数のプライベート ルーティング ドメインを設定できます（IP サービス イメージを実行しているスイッチ上）。
- ポート単位でのストーム制御により、ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームを防止できます。
- レイヤ 2 の不明なユニキャスト、マルチキャスト、およびブリッジド ブロードキャスト トラフィック転送に対するポート ブロッキングを行います。
- Cisco Group Management Protocol（CGMP）サーバのサポートと、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング（IGMP バージョン 1、2、3 に対応）については、次のようになります。
  - （CGMP 装置の場合）CGMP が特定のエンド ステーションへのマルチキャスト トラフィックを制限し、ネットワーク全般のトラフィックを軽減します。
  - （IGMP 装置の場合）IGMP スヌーピングにより、マルチメディア トラフィックおよびマルチキャスト トラフィックを転送します。

- IGMP レポート抑制により、1 つのマルチキャスト ルータ クエリーにつき 1 つの IGMP レポートだけをマルチキャスト デバイスへ送信します(IGMPv1 または IGMPv2 クエリーだけをサポート)。
- IGMP スヌーピング クエリアのサポートにより、IGMP の一般的なクエリー メッセージを定期的に生成するようスイッチを設定できます。
- IGMP ヘルパーにより、スイッチでホスト要求を転送して、特定の IP 宛先アドレスにマルチキャスト ストリームを加入させることができます。
- Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）により、マルチキャスト VLAN でマルチキャスト ストリームを連続送信すると同時に、帯域幅やセキュリティ上の理由により、それらのストリームを加入者 VLAN から分離します。
- IGMP フィルタリングにより、スイッチ ポート上のホストが所属できるマルチキャスト グループセットを管理します。
- IGMP スロットリングにより、IGMP 転送テーブルのエントリ数が最大になったときのアクションを設定できます。
- IGMP Leave タイマーにより、ネットワークに対する脱退の待ち時間を設定できます。
- Switch Database Management（SDM）テンプレートにより、ユーザ側で選択する機能へのサポートを最大化するようにシステム リソースを割り当てられます。
- Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）により、ローカルの広域アプリケーション エンジンへのトラフィックのリダイレクト、コンテンツ要求のローカル対応、ネットワーク内の Web トラフィック パターンのローカライズを実行できます（IP サービス イメージが必要)。
- Cisco IOS ソフトウェアの一部である Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）により、アクティブなトラフィック モニタリングを使用してネットワーク パフォーマンスを測定できます。
- 設定可能なスモール フレーム到達スレッシュホールドにより、スモール フレーム（64 バイト以下）が指定したレート（スレッシュホールド）でインターフェイスに到達した場合のストーム制御を防ぎます。
- Flex Link マルチキャスト高速コンバージェンスにより、Flex Link 障害の発生後にマルチキャストトラフィックのコンバージェンスにかかる時間を短縮できます。
- RADIUS サーバのロード バランシングにより、アクセス要求と認証要求をサーバ グループ内で均等に配分できるようにします。
- 出力ネットワーク ポート上で、CPU 生成トラフィックと、キューの CPU 生成トラフィックの QoS マーキングをサポートします。

管理オプション

- 組み込みデバイス マネージャ：このデバイス マネージャは、ソフトウェア イメージに統合された GUI です。これを使用して、単一スイッチの設定とモニタを行います。デバイス マネージャの起動の詳細については、クイック スタート ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Network Assistant : Network Assistant は、Cisco.com からダウンロードできるネットワーク管理アプリケーションです。これを使用して、単一のスイッチ、スイッチのクラスタ、または装置のコミュニティを管理します。Network Assistant の詳細については、Cisco.com から入手可能な『*Getting Started with Cisco Network Assistant*』を参照してください。

- CLI : Cisco IOS ソフトウェアは、デスクトップ スイッチング機能とマルチレイヤ スイッチング機能をサポートしています。CLI にアクセスするには、管理ステーションを直接スイッチ コンソール ポートに接続するか、PC をイーサネット管理ポートに直接接続するか、またはリモート管理ステーションあるいは PC から Telnet を使用します。CLI の詳細については、第 2 章「CLI（コマンドライン インターフェイス）の使用」を参照してください。
- SNMP : CiscoWorks2000 LAN Management Suite（LMS）や HP OpenView などの SNMP 管理アプリケーションです。HP OpenView や SunNet Manager などのプラットフォームが稼動している SNMP 対応の管理ステーションから管理できます。スイッチは、Management Information Base（MIB; 管理情報ベース）拡張機能の包括的なセットと 4 つの Remote Monitoring（RMON; リモート モニタリング）グループをサポートしています。SNMP の詳しい使用方法については、第 36 章「SNMP の設定」を参照してください。
- Cisco IOS Configuration Engine（旧称 Cisco IOS CNS エージェント）：コンフィギュレーション サービスにより、ネットワーク装置およびサービスの配置と管理が自動化されます。スイッチ固有の設定変更を生成し、それらをスイッチに送信し、設定変更を実行し、結果をログに記録することで、初期設定と設定更新を自動化できます。

  CNS の詳細については、第 5 章「Cisco IOS Configuration Engine の設定」を参照してください。
- CIP : Common Industrial Protocol（CIP）はピアツーピアのアプリケーション プロトコルであり、スイッチと工業用装置（I/O コントローラ、センサー、リレーなど）間でアプリケーション レベルの接続を実現します。CIP ベースの管理ツール（RSLogix など）を使用してスイッチを管理できます。スイッチでサポートされる CIP コマンドの詳細については、コマンド リファレンスを参照してください。
- Common Industrial Protocol（CIP）の機能拡張により、CIP で DHCP パラメータを設定できるようになりました。

管理機能

- CNS 組み込みエージェントにより、スイッチの管理、設定の保管、および配信を自動化できます。
- DHCP により、スイッチ情報（IP アドレス、デフォルト ゲートウェイ、ホスト名、Domain Name System（DNS; ドメイン ネーム システム）、TFTP サーバ名など）の設定を自動化できます。
- DHCP リレーにより、IP アドレス要求を含む User Datagram Protocol（UDP）ブロードキャストを DHCP クライアントから転送します。
- DHCP サーバにより、IP アドレスなどの DHCP オプションを IP ホストに自動的に割り当てます。
- DHCP ベースの自動設定とイメージ更新により、指定の設定と新しいイメージを多数のスイッチにダウンロードできます。
- DHCP サーバのポート ベースのアドレス割り当てにより、IP アドレスをスイッチ ポートに事前に割り当てることができます。
- ユニキャスト要求を DNS サーバに転送することにより、スイッチの IP アドレスとそれに対応するホスト名でスイッチを識別できます。また、ユニキャスト要求を TFTP サーバに転送することにより、TFTP サーバからソフトウェア アップグレードを管理できます。
- Address Resolution Protocol（ARP; アドレス解決プロトコル）により、スイッチの IP アドレスとそれに対応する MAC アドレスでスイッチを識別できます。
- ユニキャスト MAC アドレス フィルタリングにより、特定の送信元または宛先 MAC アドレスを持つパケットを廃棄できます。
- MAC アドレス スケーリングを設定することにより、VLAN 上で MAC アドレス学習をディセーブルにして、MAC アドレス テーブルのサイズを制限できます。

- Cisco Discovery Protocol（CDP; シスコ検出プロトコル）バージョン 1 および 2 により、ネットワーク上にあるスイッチと他のシスコ デバイス間のネットワーク トポロジを検出およびマッピングできます。
- Link Layer Discovery Protocol（LLDP）および LLDP Media Endpoint Discovery（LLDP-MED）により、サードパーティ製の IP 電話とのインターオペラビリティを実現します。
- LLDP メディア拡張（LLDP-MED）のロケーション TLV により、スイッチからエンドポイント装置までのロケーション情報が提供されます。
- CDP および LLDP 拡張のサポートにより、サーバからの動的ロケーション ベースのコンテンツ配布用にビデオ エンド ポイントとロケーション情報を交換できます。
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）により、すべてのスイッチで一貫したタイム スタンプが外部ソースから提供されます。
- IEEE 1588 標準で定められた Precision Time Protocol（PTP; 高精度時間プロトコル）により、ネットワーク内の装置のリアルタイム クロックをナノ秒精度で同期できます。
- Cisco IOS File System（IFS）により、スイッチが使用するすべてのファイル システムに単一のインターフェイスが提供されます。
- SSM PIM プロトコルのサポートにより、ビデオなどのマルチキャスト アプリケーションを最適化できます。
- マルチキャスト アプリケーション用の Source Specific Multicast（SSM）マッピングにより、ソースとグループをマッピングしてリスナーがマルチキャスト ソースにダイナミックに接続できるようにし、アプリケーションへの依存を軽減します。
- Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 のサポートにより、IPv6 トランスポートの利用、IPv6 ピアとの通信、および IPv6 ルートのアドバタイズを実行できます。
- HSRP、ARP、SNMP、IP SLA、TFTP、FTP、syslog、traceroute、ping の各 IP サービスのサポートにより、これらを VRF 認識にして、複数のルーティング インスタンスで動作できるようにします。
- コンフィギュレーション ロギングにより、スイッチ設定の変更をログに記録および表示できます。
- 固有の装置 ID により、**show inventory** ユーザ EXEC コマンド出力を通じて製品の ID 情報が提供されます。
- Netscape Navigator または Microsoft Internet Explorer のブラウザ セッション上で、デバイス マネージャを通じて帯域内管理アクセスできます。
- ネットワーク上で CLI ベースのセッションを複数実行するために、同時に最大 16 の Telnet 接続に対して帯域内管理アクセスできます。
- ネットワーク上で CLI ベースのセッションを複数実行するために、同時に最大 5 つの暗号化 Secure Shell（SSH; セキュア シェル）接続に対して帯域内管理アクセスできます。
- SNMP バージョン 1、2c、3 の get 要求と set 要求を通じて帯域内管理アクセスできます。
- スイッチ コンソール ポートを通じて、直接接続された端末またはシリアル接続やモデムを介したリモート端末に帯域外管理アクセスできます。
- Secure Copy Protocol（SCP）機能により、セキュアかつ認証済みの方法でスイッチ設定またはスイッチ イメージ ファイルをコピーできます（暗号化バージョンのソフトウェアが必要）。
- コンフィギュレーションの交換とロールバックにより、スイッチ上で実行中の設定を、任意の保存済み Cisco IOS コンフィギュレーション ファイルと交換することができます。
- Cisco IOS サポートの HTTP クライアントは IPv4 と IPv6 の両方の HTTP サーバに要求を送信でき、Cisco IOS の HTTP サーバは IPv4 と IPv6 の両方の HTTP クライアントからの HTTP 要求を処理できます。

- IPv6 ホストが、IPv6 を実行している装置へ SNMP クエリーを送信したり、その装置から SNMP 通知を受信したりできるように、IPv6 トランスポート上で Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を設定できます。
- IPv6 ステートレス自動設定により、リンク、サブネット、サイトのアドレッシング変更を管理できます（ホストおよびモバイル IP アドレスの管理など）。
- VLAN 上で MAC アドレス学習をディセーブル化できます。
- DHCP サーバのポート ベースのアドレス割り当てにより、IP アドレスをスイッチ ポートに事前に割り当てることができます。
- 有線ロケーション サービスにより、接続されているデバイスのロケーション情報およびアタッチメント追跡情報を Cisco Mobility Services Engine（MSE）に送信します。
- CPU 使用率スレッシュホールド トラップにより、CPU の使用率をモニタします。
- LLDP-MED ネットワークポリシー プロファイルの Time, Length, Value（TLV; 時間、長さ、値）により、VLAN、Class of Service（CoS; サービス クラス）、Differentiated Services Code Point（DSCP）、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成できます。
- DHCPDISCOVER パケットの Option 12 フィールドにホスト名を含めることができます。これにより、DHCP プロトコルを使用して同一の設定ファイルが送信されます。
- DHCP スヌーピング拡張により、オプション 82 DHCP フィールドで circuit-id サブオプションに固定文字列ベースの形式の選択がサポートされます。
- PROFINET IO（分散型オートメーション アプリケーション用のモジュラー通信フレームワーク）をサポートします。スイッチから IO コントローラへの PROFINET 管理接続が可能です。

アベイラビリティ機能および冗長性機能

- HSRP により、コマンド スイッチおよびレイヤ 3 ルータの冗長構成が可能です（IP サービス イメージが必要）
- 拡張オブジェクト追跡により、HSRP から追跡メカニズムが分離され、HSRP 以外のプロセスで使用できる個別のスタンドアロン追跡プロセスが作成されます（IP サービス イメージが必要）。
- UniDirectional Link Detection（UDLD; 単方向リンク検出）およびアグレッシブ UDLD により、間違った光ファイバ配線やポート障害によって発生する光ファイバ インターフェイス上の単方向リンクを検出し、ディセーブルにすることができます。
- IEEE 802.1D Spanning Tree Protocol（STP; スパニング ツリー プロトコル）により、冗長構成のバックボーン接続とループフリー ネットワークを実現します。STP には次の機能があります。
  - 最大 128 のスパニング ツリー インスタンスがサポートされます。
  - Per-VLAN Spanning-Tree Plus（PVST+）により、VLAN 間のロード バランシングを実行できます。
  - Rapid PVST+ により、VLAN 間のロード バランシングを実行し、スパニング ツリー インスタンスの高速コンバージェンスを実現します。
  - UplinkFast および BackboneFast により、スパニング ツリー トポロジの変更後に高速コンバージェンスを実現し、ギガビット アップリンクを含む冗長アップリンク間のロード バランシングを実行できます。
- IEEE 802.1s Multiple Spanning Tree Protocol（MSTP）により、VLAN をスパニング ツリー インスタンスにグループ化し、データ トラフィックとロード バランシング用に複数の転送パスを提供できます。また、IEEE 802.1w Rapid Spanning Tree Protocol（RSTP）ベースの Rapid Per-VLAN Spanning Tree Plus（Rapid PVST+）により、ルートおよび指定ポートを直ちにフォワーディング ステートに変更して、スパニング ツリーの高速コンバージェンスを実現します。

- PVST+、Rapid-PVST+、および MSTP モードで使用可能なオプションのスパニング ツリー機能は次のとおりです。
  - PortFast により、ポートがブロッキング ステートからフォワーディング ステートに直ちに変更できるようにして、転送遅延を解消できます。
  - BPDU ガードにより、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信する PortFast 対応ポートをシャットダウンできます。
  - BPDU フィルタリングにより、PortFast 対応ポートが BPDU を送受信できないようにします。
  - ルート ガードにより、ネットワーク コアの外部にあるスイッチがスパニング ツリー ルートとして使用されないようにします。
  - ループ ガードにより、単一方向リンクの原因となる障害によって代替ポートまたはルート ポートが指定ポートとして使用されないようにします。
- 等価コスト ルーティングにより、リンク レベルおよびスイッチレベルの冗長性を実現します（IP サービス イメージが必要）。
- Flex Link レイヤ 2 インターフェイスは、互いをバックアップすることにより、STP の代替として基本的なリンクの冗長構成を実現します。
- リンクステート トラッキングにより、接続されたホストとサーバからのアップストリーム トラフィックを伝送するポートのステートをミラーリングし、サーバ トラフィックを別のシスコ製イーサネット スイッチ上の動作リンクにフェールオーバーできるようにします。
- 短い Resilient Ethernet Protocol（REP）hello：REP Link Status Layer（LSL; リンク ステータス レイヤ）のエージング タイマーの範囲を 3000 ～ 10000 ms（500 ms 間隔）から 120 ～ 10000 ms（40 ms 間隔）に変更します。

VLAN 機能

- 最大 1005 の VLAN のサポートにより、適切なネットワーク リソース、トラフィック パターン、および帯域幅と関連付けて、VLAN にユーザを割り当てることができます。
- IEEE 802.1Q 標準で許可される、1 ～ 4094 の範囲の VLAN ID をサポートします。
- VLAN Query Protocol（VQP）により、ダイナミック VLAN メンバーシップに対応します。
- 全ポート上での IEEE 802.1Q トランキング カプセル化により、ネットワークの移動/追加/変更、ブロードキャスト トラフィックとマルチキャスト トラフィックの管理/制御、高セキュリティのユーザおよびネットワーク リソース用の VLAN グループの確立によるネットワーク セキュリティを実現します。
- Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）により、2 つの装置間のリンク上でトランキングをネゴシエートし、使用するトランキング カプセル化のタイプ（IEEE 802.1Q）をネゴシエートします。
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）および VTP プルーニングにより、トラフィックを受信するステーション宛てのリンクにフラッディング トラフィックを制限することでネットワーク トラフィックを低減できます。
- 音声 VLAN により、Cisco IP Phone からの音声トラフィック用のサブネットを作成できます。

- VLAN 1 の削除により、任意の各 VLAN トランク リンク上で VLAN 1 をディセーブルにできるようにして、スパニング ツリー ループまたはストームのリスクを低減します。この機能がイネーブルの場合は、トランク上でユーザ トラフィックの送受信が行われません。スイッチの CPU は制御プロトコル フレームの送受信を継続します。
- プライベート VLAN により、VLAN のスケーラビリティ問題に対処し、制御性の高い IP アドレス割り当てを実現し、スイッチ上の他のポートからレイヤ 2 ポートを分離することができます（IP サービス イメージが必要）。
- PVLAN ホスト上のポート セキュリティにより、ポート上で学習する MAC アドレスの数を制限したり、ポート上で学習できる MAC アドレスを定義することができます。
- VLAN Flex Link ロード バランシングにより、スパニング ツリー プロトコル（STP）を必要とせずにレイヤ 2 の冗長構成を実現できます。プライマリ リンクおよびバックアップ リンクとして設定した 2 つのインターフェイス間で、VLAN ベースでトラフィックのロード バランシングを実行できます。
- 制限 VLAN（*認証失敗 VLAN* とも呼ばれる）での 802.1X 認証をサポートします。
- VTP バージョン 3 のサポートにより、任意の VTP モードでの拡張範囲 VLAN（VLAN 1006 ～ 4094）、機能強化された認証（非表示またはシークレット パスワード）、VTP 以外のデータベースの伝播、VTP プライマリおよびセカンダリ サーバ、ポートごとの VTP のオン / オフ切り替えオプションなどを設定できます。

セキュリティ機能

- IP サービス レベル契約（IP SLA）のサポートにより、アクティブなトラフィック モニタリングを使用してネットワーク パフォーマンスを測定できます（IP サービス イメージが必要）。
- IP SLA EOT により、スタンバイ ルータのフェールオーバー引き継ぎを行うために、遅延、ジッタ、パケット損失などのアクションによってトリガーされる IP SLA 追跡動作からの出力を使用できます（IP サービス イメージが必要）。
- Web 認証により、Web ブラウザを使用して、IEEE 802.1x 機能をサポートしていないサプリカント（クライアント）を認証できます。
- ローカルの Web 認証バナーにより、カスタム バナーやイメージ ファイルを Web 認証のログイン画面に表示できます。
- MAC Authentication Bypass（MAB; MAC 認証バイパス）のエージング タイマーにより、MAB を使用して認証済みの非アクティブ ホストを検出できます。
- 管理インターフェイス（デバイス マネージャ、Network Assistant、CLI）へパスワード保護付きアクセス（読み取り専用アクセス、読み取り / 書き込みアクセス）により、不正な設定変更を防ぎます。
- 複数レベルのセキュリティにより、セキュリティ レベル、通知、および対応するアクションを選択できます。
- スタティック MAC アドレッシングにより、セキュリティを実現します。
- 保護ポート オプションにより、同じスイッチ上の指定ポートへのトラフィック転送を制限できます。
- ポート セキュリティ オプションにより、ポートへのアクセスが許可されるステーションの MAC アドレスを制限および識別できます。
- VLAN 認識ポートのセキュリティ オプションにより、違反の発生時にポート全体をシャットダウンするのではなく、ポート上の VLAN をシャットダウンすることができます。
- ポート セキュリティ エージングにより、ポート上のセキュア アドレスにエージング タイムを設定できます。

- BPDU ガードにより、無効な設定が発生した場合に PortFast 設定ポートをシャットダウンできます。
- 標準および拡張 IP アクセス制御リスト（ACL）により、ルーテッド インターフェイス（ルータ ACL）と VLAN 上の双方向、およびレイヤ 2 インターフェイス上の受信方向（ポート ACL）に関するセキュリティ ポリシーを定義できます。
- 拡張 MAC アクセス制御リストにより、レイヤ 2 インターフェイス上の受信方向でセキュリティ ポリシーを定義できます。
- VLAN ACL（VLAN マップ）により、MAC、IP、および TCP/UDP ヘッダー内の情報に基づいてトラフィックをフィルタリングすることで、VLAN 内のセキュリティを実現できます（IP サービス イメージが必要）。
- 送信元および宛先 MAC ベースの ACL により、非 IP トラフィックをフィルタリングできます。
- IPv6 ACL をインターフェイスに適用して、IPv6 トラフィックをフィルタリングできます（IP サービス イメージが必要）。
- DHCP スヌーピングにより、信頼できないホストと DHCP サーバ間で、信頼できない DHCP メッセージをフィルタリングできます。
- IP ソース ガードにより、DHCP スヌーピング データベースと IP 送信元バインディングに基づいてトラフィックをフィルタリングすることで、非ルーテッド インターフェイス上のトラフィックを制限できます。
- ダイナミック ARP インスペクションにより、無効な ARP 要求と ARP 応答を同じ VLAN 内の他のポートにリレーしないことで、スイッチに対する悪意ある攻撃を防止できます。
- IEEE 802.1Q トンネリングにより、サービス プロバイダー ネットワークを介したリモート サイトのユーザがいるカスタマーが、VLAN を他のカスタマーから分離することができます。また、レイヤ 2 プロトコル トンネリングにより、カスタマーのネットワークで全ユーザに関する完全な STP、CDP、および VTP 情報を取得することができます（IP サービス イメージが必要）。
- レイヤ 2 ポイントツーポイント トンネリングにより、EtherChannels を自動的に作成できます（IP サービス イメージが必要）。
- レイヤ 2 プロトコル トンネリング バイパス機能により、サードパーティ ベンダーとの相互運用性を実現します。
- IEEE 802.1x ポートベースの認証により、無認可の装置（クライアント）によるネットワークへのアクセスを防止します。次の機能がサポートされます。
  - Multidomain Authentication（MDA; マルチドメイン認証）により、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が、同じ IEEE 802.1x 対応スイッチ ポート上で独立して認証を行うことができます。
  - MDA 対応のダイナミック音声 VLAN により、MDA 対応ポート上でダイナミック音声 VLAN を実現できます。
  - VLAN 割り当てにより、802.1x で認証されたユーザを指定の VLAN に制限できます。
  - マルチ認証モード用に設定されたポートでの VLAN 割り当てをサポートします。RADIUS サーバが VLAN をポートで最初のホストに割り当てて認証を行い、後続のホストは同じ VLAN を使用します。音声 VLAN 割り当ては、1 台の IP Phone に対してサポートされます。
  - ポート セキュリティにより、802.1x ポートへのアクセスを制御できます。
  - 音声 VLAN により、ポートが認可ステートか無認可ステートかを問わず、Cisco IP Phone から音声 VLAN へのアクセスを許可できます。
  - IP Phone 検出機能拡張により、Cisco IP Phone の検出と認識を行うことができます。
  - ゲスト VLAN により、802.1x に準拠していないユーザに限定的なサービスを提供できます。

  - 制限 VLAN により、802.1x には準拠しているが、標準の 802.1x プロセスで認証するためのクレデンシャルを持たないユーザに、限定的なサービスを提供できます。
  - 802.1x アカウンティングにより、ネットワークの使用状況を追跡できます。
  - 802.1x と Wake-on-LAN（WoL）により、特定のイーサネット フレームの受信に基づいて、休止中の PC を起動できます。
  - 802.1x 準備状態チェックにより、スイッチ上で IEEE 802.1x を設定する前に、接続されたエンド ホストの準備状態を判別できます。
  - 音声認識 802.1x セキュリティにより、セキュリティ違反が発生した VLAN 上だけでトラフィック違反アクションを適用できます。
  - MAC 認証バイパスにより、クライアント MAC アドレスに基づいてクライアントを認可できます。
  - 802.1X スイッチ サプリカントを使用した Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）、CISP を使用したホスト認可、および自動イネーブル化により、ワイヤリング クローゼットの外部にあるスイッチを別のスイッチのサプリカントとして認証できます。
  - IEEE 802.1x とオープン アクセスにより、認証前にホストからネットワークにアクセスできます。
  - ダウンロード可能 ACL とリダイレクト URL を使用した IEEE 802.1x 認証により、Cisco Secure ACS サーバから認証済みスイッチにユーザごとの ACL をダウンロードできます。
  - 柔軟な認証シーケンス設定により、新しいホストの認証時にポートが試行する認証方式の順序を設定できます。
  - 複数ユーザの認証により、802.1x 対応ポート上で複数のホストが認証を実行できます。

- Network Admission Control（NAC）の機能は次のとおりです。
  - NAC レイヤ 2 802.1x 検証により、装置にネットワーク アクセス権を与える前に、エンドポイント システムまたはクライアントのアンチウイルス状態または*ポスチャ*を検証します。

    NAC レイヤ 2 802.1x 検証の設定については、「NAC レイヤ 2 802.1X 検証の設定」（P.12-59）を参照してください。
  - NAC レイヤ 2 IP 検証により、装置にネットワーク アクセス権を与える前に、エンドポイント システムまたはクライアントのポスチャを検証します。

    NAC レイヤ 2 IP 検証の設定については、『*Network Admission Control Software Configuration Guide*』を参照してください。
  - IEEE 802.1x アクセス不能認証バイパス。

    この機能の設定については、「アクセス不能認証バイパス機能の設定」（P.12-54）を参照してください。
  - ホストの NAC レイヤ 2 IP 検証に関する Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）ダウン ポリシー（ポスチャ検証の発生時に AAA サーバが使用できない場合）。

    この機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- 自社開発機能の TACACS+ により、TACACS サーバを通じてネットワーク セキュリティを管理できます。
- RADIUS により、AAA サービスを通じてリモート ユーザの ID の確認、アクセス権の付与、アクションの追跡を実行できます。
- Kerberos セキュリティ システムにより、信頼できるサードパーティを使用して、ネットワーク リソースの要求を認証できます（暗号化バージョンのソフトウェアが必要）。

- Secure Socket Layer（SSL; セキュア ソケット レイヤ）バージョン 3.0 により、HTTP 1.1 サーバ認証、暗号化、メッセージ完全性および HTTP クライアント認証がサポートされ、セキュアな HTTP 通信が実現されます（暗号化バージョンのソフトウェアが必要）。
- 音声認識 IEEE 802.1x および MAC 認証バイパス（MAB）のセキュリティ違反機能により、セキュリティ違反の発生時にポート上でデータ VLAN だけをシャットダウンできます。
- スタティック ホスト上での IP ソース ガードをサポートします。
- RADIUS Change of Authorization（CoA）により、特定のセッションの認証後にそのセッションの属性を変更できます。AAA でユーザまたはユーザ グループに関するポリシーが変更された場合、管理者は Cisco Secure ACS などの AAA サーバから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーに適用することができます。
- IEEE 802.1X ユーザ分散により、（ユーザ グループ用に）複数の VLAN を使用した配置が可能になり、異なる VLAN 間でユーザのロード バランシングを行うことで、ネットワークのスケーラビリティを向上できます。認可されたユーザは、RADIUS サーバによって割り当てられた、グループ内で最もユーザ数の少ない VLAN に割り当てられます。
- 複数のホストの認証を使用したクリティカル VLAN のサポートにより、ポートが multi-auth に設定されていて、AAA サーバが到達不能になった場合、クリティカル リソースへのアクセスを引き続き許可するために、そのポートがクリティカル VLAN に配置されます。
- カスタマイズ可能な Web 認証の機能拡張により、ローカルの Web 認証用にユーザ定義の *ログイン*、*成功*、*失敗*、*期限切れ*の各 Web ページを作成できます。
- ネットワーク エッジ アクセス トポロジ（NEAT）のサポートにより、ポートのホスト モードを変更し、オーセンティケータのスイッチ ポート上で標準のポート設定を適用することができます。
- VLAN ID ベースの MAC 認証により、VLAN と MAC アドレスの組み合わせ情報をユーザ認証に使用して、無認可の VLAN からのネットワーク アクセスを防止することができます。
- MAC 移行により、ホスト（IP 電話の背後で接続されているホストを含む）が同じスイッチ内のポートを制約なしで移行して、モビリティを実現できます。MAC 移行を使用すると、スイッチは別のポート上で同じ MAC アドレスを検出しても、まったく新しい MAC アドレスと同様に扱います。
- 簡易ネットワーク管理プロトコル バージョン 3（SNMPv3）で 3DES および AES をサポートします。このリリースでは、168 ビットの Triple Data Encryption Standard（3DES）と、128 ビット、192 ビット、256 ビットの Advanced Encryption Standard（AES; 高度暗号化規格）暗号化アルゴリズムが SNMPv3 に追加されています。

QoS 機能および CoS 機能

- Automatic QoS（auto-QoS）により、トラフィックを分類し、出力キューを設定することで、既存の QoS 機能を容易に配置できます。
- Automatic Quality Of Service（QoS）Voice over IP（VoIP）の機能拡張により、ポートベースで DSCP を信頼し、出力トラフィックのプライオリティ キューイングを実行することができます。
- 分類
  - ポートごとの IP Type-of-Service/Differentiated Services Code Point（IP ToS/DSCP）および IEEE 802.1p CoS マーキング プライオリティにより、基幹業務アプリケーションのパフォーマンスを保護できます。
  - フローベースのパケット分類（MAC、IP、および TCP/UDP ヘッダー内の情報に基づく分類）に基づく IP ToS/DSCP および IEEE 802.1p CoS マーキングにより、ネットワーク エッジでハイパフォーマンスの Quality of Service を実現して、各種ネットワーク トラフィックに合わせたサービス レベルの差別化を可能にし、ネットワーク内の基幹業務トラフィックを優先することができます。

  - QoS ドメイン内で、別の QoS ドメインと隣接するポートを使用して、信頼できるポート ステート（CoS、DSCP、および IP precedence）を実現します。
  - 信頼境界により、Cisco IP Phone の存在を検出し、受信した CoS 値を信頼して、ポート セキュリティを実現することができます。
- ポリシング
  - スイッチ ポート上のトラフィック ポリシング ポリシーにより、特定のトラフィック フローに割り振るべきポート帯域幅の量を管理できます。
  - 階層ポリシー マップに複数のクラス マップを設定する場合、各クラス マップを専用のポート レベル（第 2 レベル）のポリシー マップと関連付けることができます。第 2 レベルの各ポリシー マップには、異なるポリサーを使用できます。
  - 集約ポリシングにより、集約内のトラフィック フローをポリシングして、特定のアプリケーションやトラフィック フローを計測済みの事前定義レートに制限することができます。
- 不適合
  - 帯域幅利用限度を超えているパケットに対して、不適合マークダウンを行います。
- 入力キューイングおよびスケジューリング
  - ユーザ トラフィックに対して、2 つの入力キューを設定できます（一方のキューをプライオリティ キューに設定できます）。
  - 輻輳回避メカニズムとしての Weighted Tail Drop（WTD）により、キューの長さを管理して、さまざまなトラフィック分類の廃棄優先度を設定できます。
  - スケジューリング サービスとして Shaped Round Robin（SRR; シェイプド ラウンド ロビン）を使用することにより、パケットが内部リングに送信される際のレートを指定できます（入力キューでサポートされるモードは共有だけです）。
- 出力キューおよびスケジューリング
  - ポートあたり 4 つの出力キューを使用できます。
  - 輻輳回避メカニズムとして WTD を使用することにより、キューの長さを管理して、さまざまなトラフィック分類の廃棄優先度を設定できます。
  - スケジューリング サービスとして SRR を使用することにより、出力インターフェイスにパケットが送り出される際のレートを指定できます（出力キューではシェーピングまたは共有がサポートされます）。シェーピングされた出力キューには割り当て分のポート帯域幅が保証されますが、その帯域幅しか使用できません。シェーピングされた出力キューには設定済みの割り当て帯域幅も保証されますが、他のキューが空になり、それらのキューの割り当て帯域幅が使用されていない場合は、保証分以上の帯域幅を使用することができます。
- auto-QoS 拡張によって、ビデオ装置（Cisco Telepresence System や Cisco Surveillance Camera など）からのトラフィック フローの自動設定分類が追加されます。

レイヤ 3 機能

（注） ここに記載する機能は、IP サービス イメージだけで使用できます。

- HSRP バージョン 1（HSRPv1）および HSRP バージョン 2（HSRPv2）により、レイヤ 3 ルータの冗長構成を実現できます。

- IP ルーティング プロトコルにより、ロード バランシングを実行し、拡張可能なルーテッド バックボーンを構築することができます。
  - RIP バージョン 1 および 2。
  - 完全な OSPF（IP サービス フィーチャ セットが必要）

    Cisco IOS Release 12.2(55)SE 以降、IP ベース フィーチャ セットによって、レイヤ 3 ルーティング機能をアクセスまたはワイヤリング クローゼットに拡張できるようにするルーテッド アクセス対応の OSPF がサポートされています。
  - Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 により、IPv6 トランスポートの利用、IPv6 ピアとの通信、および IPv6 ルートのアドバタイズを実行できます。
  - HSRP for IPv6。
  - Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）バージョン 4。
- VLAN 間の IP ルーティング（VLAN 間ルーティング）により、2 つ以上の VLAN 間で完全なレイヤ 3 ルーティングが実現され、各 VLAN で専用の自律データリンク ドメインを維持できるようになります。
- Policy-Based Routing（PBR; ポリシーベース ルーティング）により、トラフィック フローに対して定義済みのポリシーを設定できます。
- カスタマー エッジ装置内の Multiple VPN Routing/Forwarding（multi-VRF）インスタンスにより、サービス プロバイダーが複数の Virtual Private Networks（VPN; 仮想私設網）をサポートし、VPN 間で IP アドレスが重複できるようにします。
- フォールバック ブリッジングにより、2 つ以上の VLAN 間で非 IP トラフィックを転送できます。
- スタティック IP ルーティングにより、ネットワーク パス情報のルーティング テーブルを手動で作成できます。
- 等価コスト ルーティングにより、ロード バランシングを実行して冗長構成を実現することができます。
- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）および ICMP Router Discovery Protocol（IRDP）により、ルータ アドバタイズ メッセージとルータ請求メッセージを使用して、直接接続されたサブネット上のルータのアドレスを検出できます。
- Protocol-Independent Multicast（PIM）により、ネットワーク内でマルチキャスト ルーティングを実現し、ネットワーク内の装置が要求されたマルチキャスト フィードを受信でき、マルチキャストに参加していないスイッチがプルーニングされるようにします。PIM Sparse Mode（PIM-SM; PIM sparse（疎）モード）、PIM Dense Mode（PIM-DM; PIM dense（密）モード）、および PIM sparse-dense モードのサポートが含まれます。
- Multicast Source Discovery Protocol（MSDP）により、複数の PIM-SM ドメインを接続できます。
- Distance Vector Multicast Routing Protocol（DVMRP）トンネリングにより、非マルチキャスト ネットワークを経由した 2 つのマルチキャスト対応ネットワーク間のインターオペラビリティが実現されます。
- DHCP リレーにより、IP アドレス要求を含む UDP ブロードキャストを DHCP クライアントから転送できます。
- DHCP for IPv6 リレー、クライアント、サーバのアドレス割り当てとプレフィクスの委任を実行できます。
- IPv6 ユニキャスト ルーティング機能により、設定したインターフェイスを通じて IPv6 トラフィックを転送できます。
- IPv6 Default Router Preference（DRP; デフォルト ルータ プリファレンス）により、ホストが適切なルータを選択する機能を強化できます。

- Nonstop Forwarding（NSF; ノンストップ フォワーディング）認識により、プライマリ Route Processor（RP; ルート プロセッサ）に障害が発生したためにバックアップ RP が引き継ぐ場合や、中断のないソフトウェア アップグレードのためにプライマリ RP が手動でリロードされる場合に、レイヤ 3 スイッチが NSF 対応のネイバー ルータからパケット転送を継続できるようにします。
- SVI ラインステート アップ/ダウン計算から、VLAN 内のポートを除外できます。
- Intermediate System-to-Intermediate System（IS-IS）ルーティングにより、Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）ネットワーク対応のダイナミック ルーティング プロトコルがサポートされます。

モニタリング機能

- EOT および IP SLA EOT スタティック ルートにより、事前設定されたスタティック ルートや DHCP ルートがダウンした場合にそれを判別できます。
- デバイスおよびシステム管理用の Embedded Event Manager（EEM; 組み込みイベント マネージャ）により、主要なシステム イベントをモニタし、ポリシーを使用して処理できます。
- MAC アドレス通知トラップおよび RADIUS アカウンティングにより、スイッチが学習または削除した MAC アドレスを保管することで、ネットワーク上のユーザを追跡できます。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN; リモート SPAN）により、任意のポートまたは VLAN 上でトラフィックをモニタできます。
- SPAN および RSPAN の Intrusion Detection System（IDS; 侵入検知システム）サポートにより、ネットワーク セキュリティ違反のモニタ、撃退、レポートを実行できます。
- 組み込み RMON エージェントの 4 つのグループ（履歴、統計、アラーム、イベント）により、ネットワークのモニタとトラフィック分析を実行できます。
- Syslog 機能により、認証または認可エラー、リソースの問題、タイムアウト イベントに関するシステム メッセージをログに記録できます。
- レイヤ 2 traceroute により、パケットが送信元装置から宛先装置に送られる際の物理パスを識別できます。
- Time Domain Reflector（TDR）により、銅線のイーサネット 10/100 および 10/100/1000 ポート上のケーブル接続の問題を診断し、解決することができます。
- SFP モジュール診断管理インターフェイスにより、SFP モジュールの物理ステータスまたは動作ステータスをモニタできます。
- 温度、電源状態、イーサネット ポートのステータスに関するアラームの処理機能が備わっています。
- 外部のリレー システムに使用できるアラーム リレー接点が備わっています。
- On-Board Failure Logging（OBFL）により、スイッチとそれに接続されている電源装置の情報を収集します（Catalyst 2960-S のみ）。
- HSRP 対応のオブジェクト追跡が機能強化されています。
- Digital Optical Monitoring（DOM）により、X2 SFP（着脱可能小型フォーム ファクタ）モジュールのステータスをチェックできます。

スイッチの初期設定後のデフォルト設定

このスイッチはプラグアンドプレイ動作に対応しているため、スイッチに基本 IP 情報を割り当て、ネットワーク内の他の装置に接続するだけで済みます。特定のネットワーク要件がある場合は、インターフェイス固有の設定およびシステム規模の設定を変更できます。

（注）　ブラウザベースの Express Setup プログラムを使用した IP アドレスの割り当てについては、クイック スタート ガイドを参照してください。CLI ベースのセットアップ プログラムを使用した IP アドレスの割り当てについては、ハードウェア インストレーション ガイドを参照してください。

スイッチの設定を行わない場合、スイッチは次のデフォルト設定で動作します。

- スイッチのデフォルトの IP アドレス、サブネット マスク、およびデフォルト ゲートウェイは 0.0.0.0 です。詳細については、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」および第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- デフォルトのドメイン名は設定されていません。詳細については、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」を参照してください。
- DHCP クライアントはイネーブル、DHCP サーバはイネーブル（DHCP サーバとして動作する装置が設定済みでイネーブルの場合だけ）、DHCP リレー エージェントはイネーブル（DHCP リレー エージェントとして動作する装置が設定済みでイネーブルの場合だけ）です。詳細については、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」および第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- スイッチ クラスタはディセーブルです。スイッチ クラスタの詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com で入手可能な『*Getting Started with Cisco Network Assistant*』を参照してください。
- パスワードは定義されていません。詳細については、第 7 章「スイッチの管理」を参照してください。
- システム名とプロンプトは *Switch* です。詳細については、第 7 章「スイッチの管理」を参照してください。
- NTP はイネーブルです。詳細については、第 7 章「スイッチの管理」を参照してください。
- DNS はイネーブルです。詳細については、第 7 章「スイッチの管理」を参照してください。
- TACACS+ はディセーブルです。詳細については、第 11 章「スイッチベース認証の設定」を参照してください。
- RADIUS はディセーブルです。詳細については、第 11 章「スイッチベース認証の設定」を参照してください。
- 標準 HTTP サーバと Secure Socket Layer（SSL）HTTPS サーバはどちらもイネーブルです。詳細については、第 11 章「スイッチベース認証の設定」を参照してください。
- IEEE 802.1x はディセーブルです。詳細については、第 12 章「IEEE 802.1X ポートベースの認証の設定」を参照してください。
- ポート パラメータ
  - 動作モードはレイヤ 2（switchport）です。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。
  - インターフェイス速度とデュプレックス モードは自動ネゴシエーションです。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。
  - Auto MDIX は、イネーブルです。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。

  - フロー制御はオフです。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。
- VLAN
  - デフォルトの VLAN は VLAN 1 です。詳細については、第 16 章「VLAN の設定」を参照してください。
  - VLAN トランキング設定は dynamic auto（DTP）です。詳細については、第 16 章「VLAN の設定」を参照してください。
  - トランク カプセル化はネゴシエーションです。詳細については、第 16 章「VLAN の設定」を参照してください。
  - VTP モードはサーバです。詳細については、第 17 章「VTP の設定」を参照してください。
  - VTP バージョンはバージョン 1 です。詳細については、第 17 章「VTP の設定」を参照してください。
  - プライベート VLAN は設定されていません。詳細については、第 19 章「プライベート VLAN の設定」を参照してください。
  - 音声 VLAN はディセーブルです。詳細については、第 18 章「音声 VLAN の設定」を参照してください。
- IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングはディセーブルです。詳細については、第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。
- STP、PVST+ は VLAN 1 上でイネーブルです。詳細については、第 21 章「STP の設定」を参照してください。
- MSTP はディセーブルです。詳細については、第 22 章「MSTP の設定」を参照してください。
- オプションのスパニング ツリー機能はディセーブルです。詳細については、第 23 章「オプションのスパニング ツリー機能の設定」を参照してください。
- Flex Link は設定されていません。詳細については、第 25 章「Flex Link および MAC アドレス テーブル移行更新機能の設定」を参照してください。
- DHCP スヌーピングは、ディセーブルです。DHCP スヌーピング情報オプションはイネーブルです。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- IP ソース ガードはディセーブルです。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- DHCP サーバ ポートベースのアドレス割り当てはディセーブルです。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- ダイナミック ARP インスペクションはすべての VLAN 上でディセーブルです。詳細については、第 27 章「ダイナミック ARP 検査の設定」を参照してください。
- IGMP スヌーピングはイネーブルです。IGMP のフィルタは適用されていません。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スロットリング設定は拒否です。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スヌーピング クエリア機能はディセーブルです。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- MVR はディセーブルです。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。

- ポート ベースのトラフィック
  - ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。
  - 保護ポートは定義されていません。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。
  - ユニキャストおよびマルチキャスト トラフィック フラッディングはブロックされません。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。
  - セキュア ポートは設定されていません。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。
- CDP はイネーブルです。詳細については、第 32 章「CDP の設定」を参照してください。
- UDLD はディセーブルです。詳細については、第 33 章「UDLD の設定」を参照してください。
- SPAN および RSPAN はディセーブルです。詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。
- RMON はディセーブルです。詳細については、第 34 章「RMON の設定」を参照してください。
- Syslog メッセージはイネーブルで、コンソール上に表示されます。詳細については、第 35 章「システム メッセージ ロギングの設定」を参照してください。
- SNMP はイネーブルです（バージョン 1）。詳細については、第 36 章「SNMP の設定」を参照してください。
- ACL は設定されていません。詳細については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- QoS はディセーブルです。詳細については、第 39 章「QoS の設定」を参照してください。
- EtherChannels は設定されていません。詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
- IP ユニキャスト ルーティングはディセーブルです。詳細については、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。
- IPv6 ユニキャスト ルーティングはディセーブルです。詳細については、第 42 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。
- HSRP グループは設定されていません。詳細については、第 45 章「HSRP の設定」を参照してください。
- IP マルチキャスト ルーティングはすべてのインターフェイス上でディセーブルです。詳細については、第 49 章「IP マルチキャスト ルーティングの設定」を参照してください。
- MSDP はディセーブルです。詳細については、第 50 章「MSDP の設定」を参照してください。
- フォールバック ブリッジングは設定されていません。詳細については、第 51 章「フォールバック ブリッジングの設定」を参照してください。

ネットワークの設定例

ここでは、ネットワーク設定の概念について説明し、スイッチを使用した専用ネットワーク セグメントの作成例と Fast Ethernet および Gigabit Ethernet 接続を通じたセグメントの相互接続例を示します。

スイッチを使用するための設計概念

ネットワーク ユーザ間でネットワーク帯域幅を取り合う状態になると、データの送受信に時間がかかるようになります。ネットワークの設定時には、ネットワーク ユーザに必要な帯域幅と、ユーザが利用するネットワーク アプリケーションの相対的なプライオリティを考慮します。

表 1-1 で、ネットワーク パフォーマンスの低下を引き起こす原因と、ネットワーク設定によってネットワーク ユーザが利用できる帯域幅を増やす方法について説明します。

表 1-1　ネットワーク パフォーマンスの向上

ネットワーク デマンド	推奨される設計方法
単一ネットワーク セグメント上のユーザ数過多、およびインターネットにアクセスするユーザ数の増加	• 小規模なネットワーク セグメントを作成して、帯域幅を共有するユーザ数を減らします。また、VLAN および IP サブネットを使用して、アクセス頻度の高いユーザと同じ論理ネットワーク内にネットワーク リソースを配置します。 • スイッチと接続先ワークステーションとの間で全二重動作を使用します。
• 新しい PC、ワークステーション、およびサーバの性能向上 • ネットワーク アプリケーション（大きな添付ファイル付き E メールなど）および帯域幅を大量に使用するアプリケーション（マルチメディアなど）からの帯域幅要求の増大	• グローバル リソース（ネットワーク ユーザが同等にアクセスできる必要のあるサーバやルータなど）を高速スイッチ ポートに直接接続して、ユーザが専用の高速セグメントを使用できるようにします。 • スイッチと接続先サーバおよびルータとの間で EtherChannel 機能を使用します。

ネットワークの設計時の考慮事項は、帯域幅だけではありません。ネットワーク トラフィックのプロファイルが発展してきたら、音声とデータの統合、マルチメディアの統合、アプリケーションの優先付け、セキュリティなどのアプリケーションをサポートできるネットワーク サービスの提供を検討してください。表 1-2 で、ネットワーク デマンドと各デマンドに対応する方法について説明します。

表 1-2　ネットワーク サービスの提供

ネットワーク デマンド	推奨される設計方法
マルチメディア アプリケーションにおける帯域幅の効率的な利用および基幹業務アプリケーションに対する帯域幅の保証	• IGMP スヌーピングを使用して、マルチメディアおよびマルチキャスト トラフィックを効率的に転送します。 • その他の QoS メカニズム（パケット分類、マーキング、スケジューリング、輻輳回避など）を使用して適切なプライオリティ レベルでトラフィックを分類し、それによって最大限の柔軟性と、基幹業務アプリケーション、ユニキャスト アプリケーション、マルチキャストおよびマルチメディア アプリケーションのサポートを実現します。 • MVR を使用して、マルチキャスト VLAN でマルチキャスト ストリームを連続送信すると同時に、帯域幅やセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。
基幹業務アプリケーションを *常時オン* にするための、ネットワークの冗長構成と可用性に対する高いデマンド	• Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用して、クラスタ コマンド スイッチおよびルータを冗長構成にします。 • VLAN トランクおよび BackboneFast を使用して、アップリンク ポート上でトラフィックのロード バランシングを実行し、VLAN トラフィックの伝送時にポート コストが相対的に低いアップリンク ポートが選択されるようにします。

表 1-2　ネットワーク サービスの提供 （続き）

ネットワーク デマンド	推奨される設計方法
IP テレフォニーに対する高いデマンド	• QoS を使用して、輻輳中に IP テレフォニーなどのアプリケーションを優先付け、ネットワーク内の遅延とジッタの両方を制御できるようにします。 • 1 ポートあたり 2 つ以上のキューをサポートするスイッチを使用して、音声およびデータ トラフィックを IEEE 802.1p/Q に基づいてハイプライオリティかロープライオリティのいずれかとして優先付けます。このスイッチでは、ポートあたり少なくとも 4 つのキューをサポートしています。 • 音声 VLAN ID（VVID）を使用して、音声トラフィック用に個別の VLAN を提供します。
既存のインフラストラクチャを使用して、自宅やオフィスからインターネットまたはイントラネットに高速でデータおよび音声を転送するデマンドの増大	Catalyst Long-Reach Ethernet（LRE; 長距離イーサネット）スイッチを使用して、既存のインフラストラクチャ（既存の電話回線など）上で最大 15 Mb の IP 接続を提供します。 **（注）** LRE は、Catalyst 2900 LRE XL および Catalyst 2950 LRE スイッチで使用されているテクノロジーです。LRE の詳細については、これらのスイッチに固有のマニュアル セットを参照してください。

Ethernet-to-the-Factory アーキテクチャ

ここでは、Ethernet-to-the-Factory（EttF）アーキテクチャについて概説します。EttF は、オートメーション システムや制御システム内の装置やアプリケーションにネットワーク サービスとセキュリティ サービスを提供します。そして、それらをより大規模な企業ネットワークに統合します。

EttF アーキテクチャはさまざまなタイプの製造環境に応用できますが、産業タイプ、製造タイプ、および生産施設の規模に合わせて調整する必要があります。また、小規模ネットワーク（装置が 50 台未満）から中規模ネットワーク（装置が 200 台未満）および大規模ネットワーク（装置が最大 1000 台およびそれ以上）まで、さまざまな規模での配置が可能です。

EttF アーキテクチャにはゾーンと呼ばれる概念構造が含まれています。ゾーンとは、最上位となる企業レベルのスイッチおよびプロセスから、より詳細なプロセスを制御する最小の装置、あるいは工場のフロアにある装置に至るまでのさまざまな機能を区分するものです。図 1-1 を参照してください。

EttF アーキテクチャの詳細については、次の URL を参照してください。

http://wwwin.cisco.com/enterprise/solutions/manufacturing/solutions/ettf.shtml

企業ゾーン

*企業ゾーン*は、一元管理されている IT システムと機能で構成されます。企業リソース管理サービス、企業間（B2B）サービス、企業/顧客間（B2C）サービスなどの企業ネットワーク サービスへの有線およびワイヤレス アクセスが可能です。サイト ビジネス プランニングやロジスティクスなどの基本的なビジネス管理作業はここで実行され、標準の IT サービスに依存します。ゲスト アクセス システムは多くの場合ここに置かれますが、企業レベルでは実現しにくい柔軟性を得るために、より下位レベルのフレームワークに置かれることも珍しくありません。

非武装ゾーン

非武装ゾーン（DMZ）は、企業ゾーンと製造ゾーンの間でデータやサービスを共有するためのバッファを提供します。DMZ では、可用性の維持、セキュリティ上の脆弱性への対処、および適合認定の義務の遵守を行います。DMZ は、たとえば IT 部門と生産部門を分けるなど、組織的な管理区分を提供します。組織ごとに異なるポリシーの適用や組み込みが可能です。たとえば、製造部門では、IT 部門と異なるセキュリティ ポリシーを製造ゾーンに適用できます。

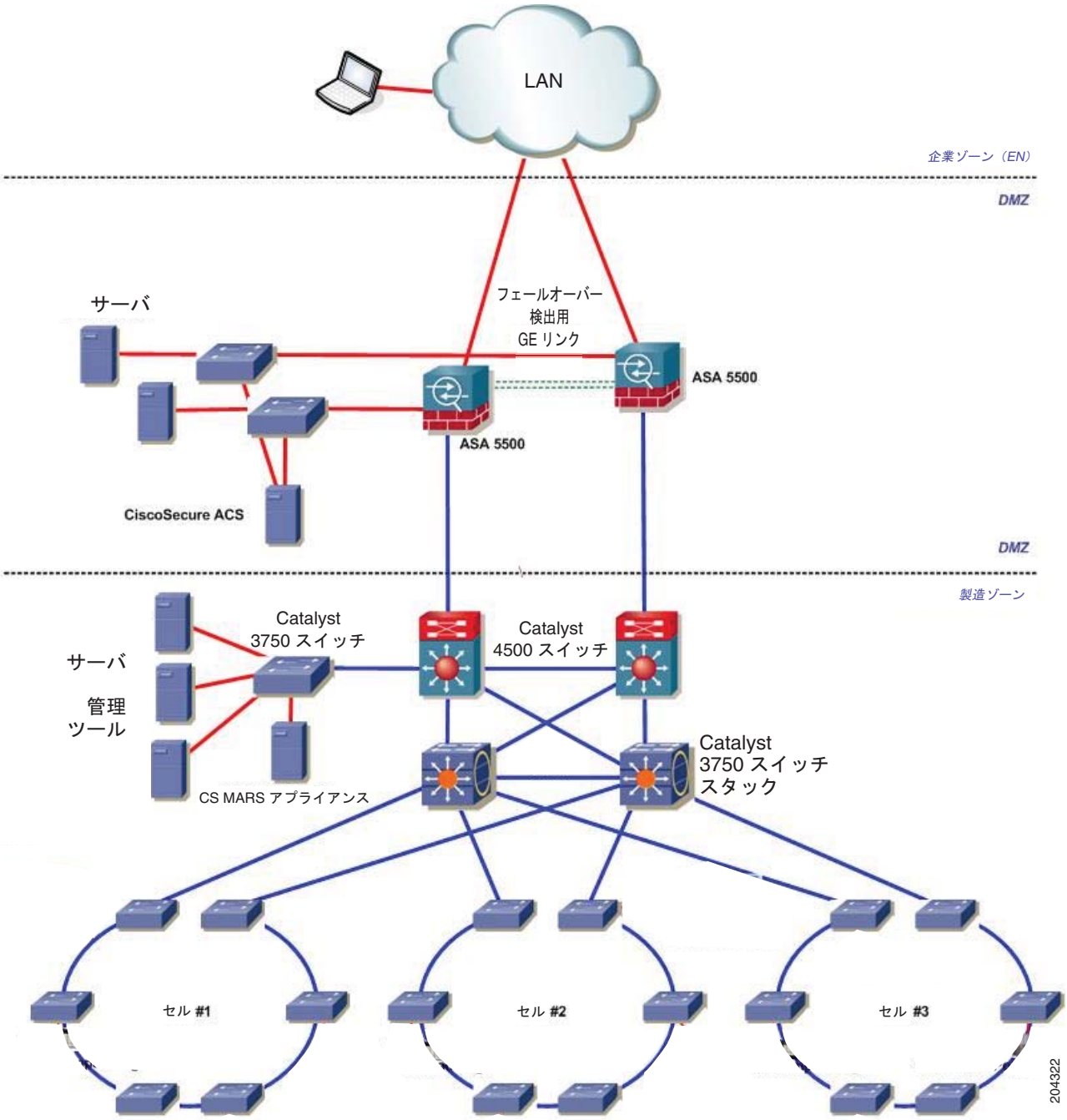
製造ゾーン

*製造ゾーン*は、セル ネットワークとサイトレベルのアクティビティで構成されます。工場のオペレーションをモニタするシステム、装置、コントローラはすべてこのゾーンに置かれます。生産施設内の 1 つの機能エリアを表すのが、セル ゾーンです。

セル ゾーンは、オートメーション プロセスの機能面をリアルタイムで制御する装置やコントローラなどで構成されます。これらはすべて互いにリアルタイム通信を行います。このゾーンは、工場や企業における他のレベルのオペレーションから明確に分離し、保護する必要があります。

図 1-1 に、EttF アーキテクチャを示します。

図 1-1　Ethernet-to-the-Factory アーキテクチャ



トポロジのオプション

トポロジの設計ではまず、装置をネットワークに接続する方法を検討します。セル ネットワークでは、生産フロアの物理的な制約に応じた物理トポロジも必要です。ここでは、トポロジの設計に関する注意事項を示し、トランク廃棄トポロジ、リング トポロジ、および冗長構成のスター トポロジについて説明します。

- 物理レイアウト：トポロジの設計は、生産環境のレイアウトに左右されます。たとえば、長いコンベアベルト システムにはトランク廃棄トポロジやリング トポロジが適していますが、冗長構成のスター トポロジは適していません。
- リアルタイム通信：遅延やジッタの主な発生原因は、トラフィックの量や、パケットが宛先に到達するまでに必要とするホップの数です。レイヤ 2 ネットワーク内のトラフィックの量はさまざまな要因に左右されますが、装置の数が重要となります。リアルタイム通信については、次の注意事項に従ってください。
  - レイヤ 2 ホップごとに生じる遅延の量を考慮してください。たとえば、100 Mb のインターフェイスを使用した場合は、1 ギガビットのインターフェイスを使用した場合に比べて遅延が大きくなります。
  - どのスイッチでも常に、帯域幅がインターフェイス キャパシティの 50% を継続的に超えることがないようにしてください。
  - CPU の使用率は、50 ～ 70% を継続的に超えることがないようにしてください。このレベルを超えると、スイッチが制御パケットを正しく処理できない可能性や、異常な動作をする可能性があります。

接続に関する主な考慮事項は次のとおりです。

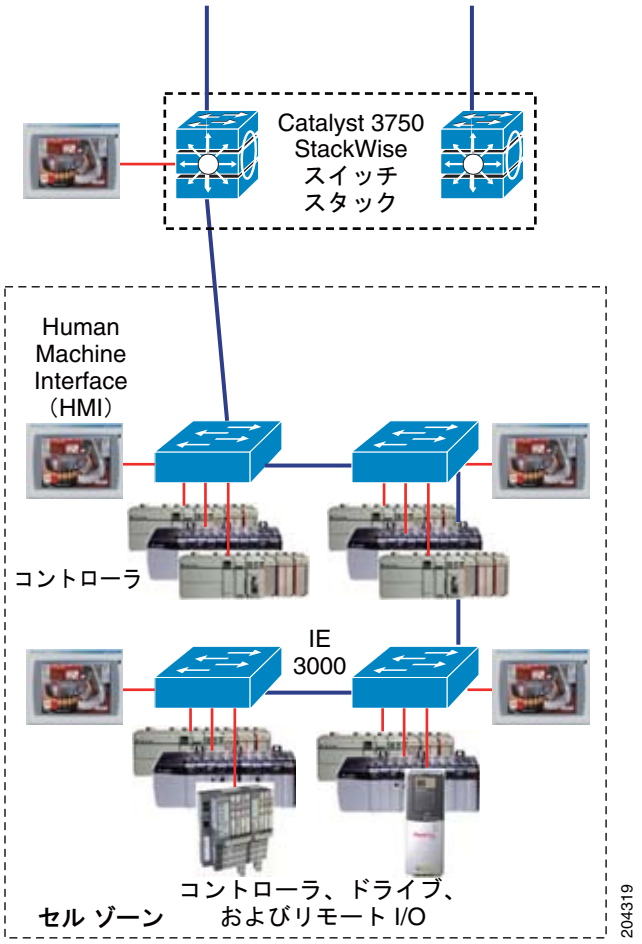
- 装置は、単一のネットワーク接続または IP 対応の I/O ブロックやリンク装置（イーサネットがサポートされていない場合）を通じてスイッチに接続されます。大半の装置にはフェールオーバー機能がないか、あっても機能が制限されているため、冗長構成のネットワーク接続を効果的に利用できません。
- 冗長構成の接続は、基幹インフラストラクチャに該当するプロセス関連の産業など、特定の産業やアプリケーションで利用されます。

セル ネットワーク：トランク廃棄トポロジ

*トランク廃棄*トポロジ（*カスケード*トポロジとも呼ばれる）では、スイッチが互いに接続され、スイッチ チェーンが形成されます。図 1-2 を参照してください。

- レイヤ 3 スイッチと最初のレイヤ 2 スイッチ間の接続はオーバーサブスクリプションの影響を受けやすく、これが発生するとネットワーク パフォーマンスが低下する可能性があります。
- 接続損失に対する冗長構成はありません。

図 1-2　セル ネットワーク：トランク廃棄トポロジ

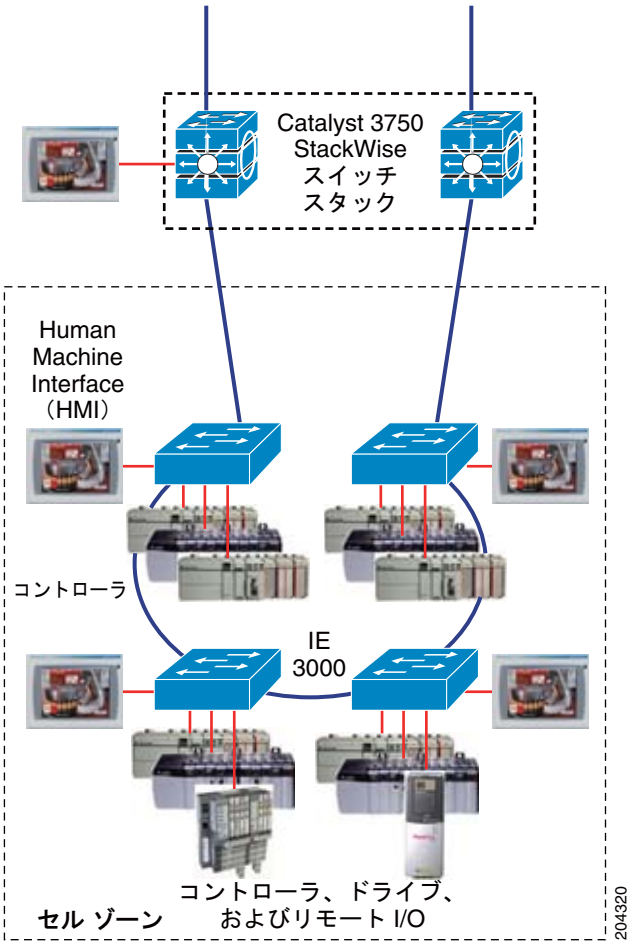


セル ネットワーク：リング トポロジ

リング トポロジはトランク廃棄トポロジと似ていますが、チェーンの最後のスイッチがレイヤ 3 スイッチに接続され、ネットワーク リングが形成される点が異なります。リング内で接続損失が発生しても、各スイッチは他のスイッチとの接続を維持します。図 1-3 を参照してください。

- ネットワークは、単一の接続損失からだけ回復できます。
- 追加プロトコルの実装と Rapid Spanning Tree Protocol（RSTP）を必要とするため、このトポロジの実装は比較的難しくなります。
- トランク廃棄よりも優れていますが、リングの最上部（レイヤ 3 スイッチとの接続）がボトルネックになる可能性があります。この部分はオーバーサブスクリプションの影響を受けやすく、これが発生するとネットワーク パフォーマンスが低下する可能性があります。

図 1-3　セル ネットワーク：リング トポロジ

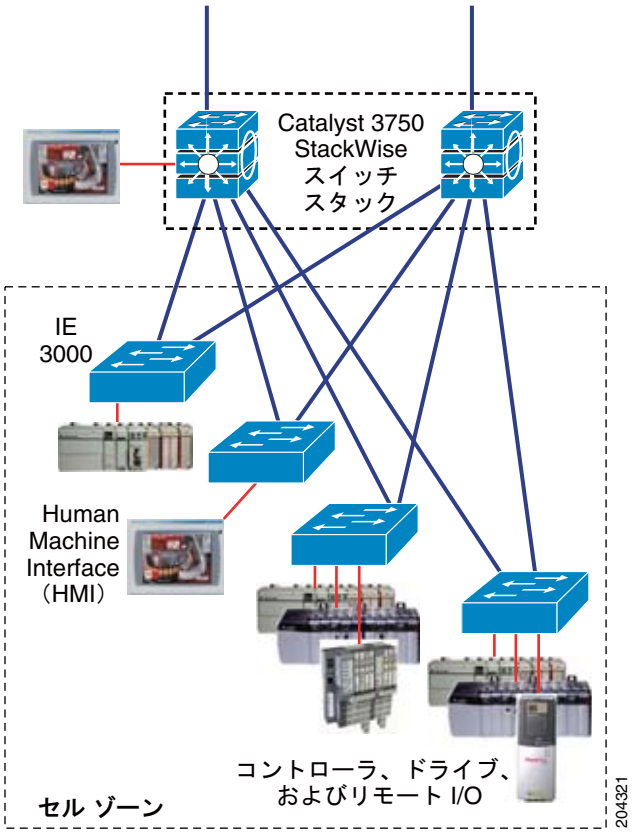


セル ネットワーク：冗長構成のスター トポロジ

冗長構成のスター トポロジでは、各レイヤ 2 アクセス スイッチがレイヤ 3 ディストリビューション スイッチにデュアル接続します。装置はレイヤ 2 スイッチに接続されます。図 1-4 を参照してください。

- どのレイヤ 2 スイッチでも、他のレイヤ 2 スイッチまでのホップ数は常に 2 つだけです。
- レイヤ 2 ネットワークでは、各スイッチがレイヤ 3 装置にデュアル接続します。
- 複数の接続損失が発生した場合でも、レイヤ 2 ネットワークは維持されます。

図 1-4　セル ネットワーク：冗長構成のスター トポロジ



次の作業

スイッチを設定する前に、次の項でスタートアップ情報を確認してください。

- 第 2 章「CLI（コマンドライン インターフェイス）の使用」
- 第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」

CHAPTER 2

CLI（コマンドライン インターフェイス）の使用

この章では、Cisco IOS CLI（コマンドライン インターフェイス）について説明します。また、CLI を使用して IE 3000 スイッチを設定する方法についても説明します。

コマンド モードの概要

Cisco IOS ユーザ インターフェイスには、多数のモードがあります。使用できるコマンドは、現在のモードによって異なります。システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。

スイッチ上でセッションを開始すると、ユーザ モード（別名ユーザ EXEC モード）から始まります。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえば、ユーザ EXEC コマンドの大部分は、現在のコンフィギュレーション ステータスを表示する **show** コマンドや、カウンタまたはインターフェイスを消去する **clear** コマンドなどのように、1 回限りのコマンドです。ユーザ EXEC コマンドは、スイッチの再起動時に保存されません。

すべてのコマンドを使用できるようにするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードの入力が必要です。このモードでは、任意の特権 EXEC モードを入力したり、グローバル コンフィギュレーション モードを開始したりすることができます。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用すると、実行コンフィギュレーションを変更できます。設定を保存すると、これらのコマンドが保存され、スイッチの再起動時に使用されます。各種のコンフィギュレーション モードにアクセスするには、最初にグ

ローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードを開始できます。

表 2-1 に、主なコマンド モード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。表の例では、ホスト名として *Switch* を使用しています。

表 2-1　コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチでセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	このモードでは、次の作業を行います。 • 端末の設定の変更。 • 基本テストの実行。 • システム情報の表示。
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	このモードでは、入力したコマンドを確認します。このモードへのアクセスを保護するには、パスワードを使用します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Switch(config)#`	特権 EXEC モードに戻る場合は、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードでは、スイッチ全体に適用されるパラメータを設定します。
VLAN 設定	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻る場合は、Ctrl+Z を押すか、**end** を入力します。	このモードでは、VLAN パラメータを設定します。VTP モードがトランスペアレントのときは、拡張範囲 VLAN（VLAN ID が 1005 より上）を作成して、スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存できます。

表 2-1　コマンド モードの概要 （続き）

モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、インターフェイスを指定して **interface** コマンドを入力します。	`Switch(config-if)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** を入力します。 特権 EXEC モードに戻る場合は、Ctrl+Z を押すか、**end** を入力します。	このモードでは、イーサネット ポートのパラメータを設定します。 インターフェイスの定義については、「インターフェイス コンフィギュレーション モードの使用」（P.14-8）を参照してください。 同じパラメータで複数のインターフェイスを設定するには、「インターフェイスの範囲設定」（P.14-10）を参照してください。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**line vty** または **line console** コマンドを入力します。	`Switch(config-line)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** を入力します。 特権 EXEC モードに戻る場合は、Ctrl+Z を押すか、**end** を入力します。	このモードでは、端末回線のパラメータを設定します。

コマンド モードの詳細については、このリリースのコマンド リファレンスを参照してください。

ヘルプ システムの概要

システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。表 2-2 を参照してください。

表 2-2　ヘルプの概要

コマンド	目的
help	任意のコマンド モードで、ヘルプ システムの簡単な説明を表示します。

コマンドの先頭部分?	特定の文字列で始まるコマンドの一覧を表示します。
	次に例を示します。
	`Switch# di?`
	`dir disable disconnect`

コマンドの先頭部分<Tab>	部分的なコマンド名を完全なコマンド名にします。
	次に例を示します。
	`Switch# sh conf<tab>`
	`Switch# show configuration`

表 2-2　ヘルプの概要 （続き）

コマンド	目的
?	特定のコマンド モードで使用できるコマンドの一覧を表示します。 次に例を示します。 `Switch> ?`
*コマンド***?**	コマンドに関連付けらているキーワードの一覧を表示します。 次に例を示します。 `Switch> show ?`

*コマンド キーワード***?**	キーワードに関連付けらている引数の一覧を表示します。
	次に例を示します。
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`

コマンドの省略の概要

コマンドを入力する場合は、スイッチがコマンドを一意として認識できるだけの文字を入力し、残りは省略できます。

次に、**show configuration** 特権 EXEC コマンドを省略形式で入力する例を示します。

```
Switch# show conf
```

コマンドの no 形式および default 形式の概要

ほぼすべてのコンフィギュレーション コマンドに **no** 形式があります。通常、**no** 形式は、機能をディセーブルにしたり、コマンドのアクションを取り消したりする場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを実行すると、インターフェイスのシャットダウンが取り消されます。ディセーブルにした機能を再びイネーブルにしたり、デフォルトでディセーブルに設定されている機能をイネーブルにするには、キーワード **no** を指定せずにコマンドを使用します。

コンフィギュレーション コマンドには **default** 形式もあります。コマンドの **default** 形式は、コマンドの設定をデフォルトに戻します。大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じです。ただし、一部のコマンドは、デフォルトでイネーブルに設定されていて、変数が特定のデフォルト値に設定されています。このような場合に **default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI エラー メッセージの概要

表 2-3 に、CLI を使用してスイッチを設定するときに表示される可能性があるエラー メッセージの一部を示します。

表 2-3　一般的な CLI エラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	スイッチがコマンドを認識できるだけの文字が入力されていません。	コマンドを再度入力し、疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに入力できるキーワードが表示されます。
`% Incomplete command.`	このコマンドに必須のキーワードまたは値が一部入力されていません。	コマンドを再度入力し、疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに入力できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。間違っている箇所がキャレット（^）記号で示されます。	疑問符（?）を入力すると、そのコマンド モードで使用できるすべてのコマンドが表示されます。 コマンドとともに入力できるキーワードが表示されます。

コンフィギュレーション ロギングの使用

スイッチの設定変更をログに記録して表示することができます。設定変更ロギングおよび通知機能を使用すると、セッション単位およびユーザ単位で変更を追跡できます。ロガーは、適用された各コンフィギュレーション コマンド、コマンドを入力したユーザ、コマンドが入力された時間、およびコマンドのパーサー リターン コードを追跡します。この機能には、設定が変更された場合に登録済みのアプリケーションに非同期通知を送信する機能を備えています。Syslog に通知を送信するかどうかを選択できます。

詳細については、次の URL にある『*Configuration Change Notification and Logging*』のフィーチャ モジュールを参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1e81.html

（注）　CLI または HTTP の変更だけがログに記録されます。

コマンド履歴の使用

ソフトウェアでは、入力したコマンドの履歴（記録）を使用できます。コマンド履歴機能は、アクセスリストなど長くて複雑なコマンドやエントリを呼び出す場合に特に便利です。次の各項で説明するように、この機能はニーズに合わせてカスタマイズできます。

- 「コマンド履歴バッファ サイズの変更」（P.2-6）（任意）
- 「コマンドの呼び出し」（P.2-6）（任意）
- 「コマンド履歴機能のディセーブル化」（P.2-6）（任意）

コマンド履歴バッファ サイズの変更

デフォルトでは、スイッチの履歴バッファに 10 行のコマンドラインが記録されます。現在の端末セッションまたは特定のラインのすべてのセッションで、この数を変更することができます。これらの手順は任意です。

現在の端末セッションでスイッチに記録されるコマンドラインの数を変更するには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# terminal history [size number-of-lines]
```

指定できる範囲は 0 ～ 256 です。

特定のラインのすべてのセッションでスイッチに記録されるコマンドラインの数を設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
Switch(config-line)# history [size number-of-lines]
```

指定できる範囲は 0 ～ 256 です。

コマンドの呼び出し

履歴バッファからコマンドを呼び出すには、表 2-4 に示すいずれかの処理を実行します。これらの処理は任意です。

表 2-4　コマンドの呼び出し

アクション[1]	結果
Ctrl+P または上矢印キーを押す。	直前に入力されたコマンドから、履歴バッファに保管されているコマンドを呼び出します。キー シーケンスを繰り返すと、さらに古いコマンドが順に呼び出されます。
Ctrl+N または下矢印キーを押す。	Ctrl+P または上矢印キーを使用してコマンドを呼び出したあと、履歴バッファ内のより新しいコマンドに戻ります。キー シーケンスを繰り返すと、さらに新しいコマンドが順に呼び出されます。
show history	特権 EXEC モードで、直前に入力したコマンドをいくつか表示します。表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定で制御します。

1. 矢印キーは、VT100 などの ANSI 互換端末に限り有効です。

コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルに設定されます。現在の端末セッションまたはコマンドラインで、この機能をディセーブルにすることができます。これらの手順は任意です。

現在の端末セッションでコマンド履歴をディセーブルにするには、**terminal no history** イネーブル EXEC コマンドを入力します。

ラインのコマンド履歴をディセーブルにするには、**no history** ライン コンフィギュレーション コマンドを入力します。

編集機能の使用

ここでは、コマンドラインの操作に役立つ編集機能について説明します。この章で説明する内容は、次のとおりです。

- 「編集機能のイネーブル化およびディセーブル化」（P.2-7）（任意）
- 「キーストロークによるコマンドの編集」（P.2-7）（任意）
- 「折り返しコマンドラインの編集」（P.2-9）（任意）

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的にイネーブルに設定されますが、ディセーブルにしたり、再度イネーブルにしたり、特定のラインを拡張編集モードに設定したりできます。これらの手順は任意です。

拡張編集モードをグローバルにディセーブルにするには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
Switch (config-line)# no editing
```

現在の端末セッションで拡張編集モードを再度イネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# terminal editing
```

特定のラインを拡張編集モードに再設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
Switch(config-line)# editing
```

キーストロークによるコマンドの編集

表 2-5 に、コマンドラインを編集するために必要なキーストロークを示します。これらのキーストロークは任意です。

表 2-5　キーストロークによるコマンドの編集

機能	キーストローク[1]	目的
コマンドライン上を移動して変更または修正を行う。	Ctrl+B または左矢印キーを押す。	カーソルを 1 文字分だけ後退させます。
	Ctrl+F または右矢印キーを押す。	カーソルを 1 文字分だけ進めます。
	Ctrl+A を押す。	コマンドラインの先頭にカーソルを移動します。
	Ctrl+E を押す。	コマンドラインの末尾にカーソルを移動します。
	Esc+B を押す。	カーソルを単語 1 つ分だけ後退させます。
	Esc+F を押す。	カーソルを単語 1 つ分だけ進めます。
	Ctrl+T を押す。	カーソルの左側の文字をカーソルの位置にある文字と置き換えます。

表 2-5　キーストロークによるコマンドの編集 （続き）

機能	キーストローク[1]	目的
バッファからコマンドを呼び出してコマンドラインに貼り付ける。（スイッチには、直前に削除された 10 個の項目を格納するバッファがあります）	Ctrl+Y を押す。	バッファ内の最も新しいエントリを呼び出します。
	Esc+Y を押す。	バッファの次のエントリを呼び出します。 バッファには、直前に削除または切り取られた 10 個の項目しか格納されていません。Esc+Y を 11 回以上押すと、バッファの最初のエントリに戻ります。
エントリを誤って入力した場合、または取りやめたい場合に削除する。	Delete キーまたは Backspace キーを押す。	カーソルの左側の文字を消去します。
	Ctrl+D を押す。	カーソルの位置にある文字を削除します。
	Ctrl+K を押す。	カーソルの位置からコマンドラインの末尾までの文字をすべて削除します。
	Ctrl+U または Ctrl+X を押す。	カーソルの位置からコマンドラインの先頭までの文字をすべて削除します。
	Ctrl+W を押す。	カーソルの左側の単語を削除します。
	Esc+D を押す。	カーソルの位置から単語の末尾までを削除します。
単語を大文字または小文字にするか、文字列を大文字にします。	Esc+C を押す。	カーソルの位置にある単語を大文字にします。
	Esc+L を押す。	カーソルの位置にある単語を小文字にします。
	Esc+U を押す。	カーソルの位置から単語の末尾までの文字列を大文字にします。
特定のキーストロークを実行可能コマンド（おそらくはショートカット）として指定する。	Ctrl+V または Esc+Q を押す。	
端末の画面に表示しきれない長さの行または画面を下にスクロールする。 **（注）** 端末画面に表示しきれない数の行が出力される（**show** コマンドの出力など）場合は、More プロンプトが表示されます。More プロンプトが表示されている場合は、いつでも Return キーおよび Space バーのキーストロークを使用できます。	Return キーを押す。	1 行下にスクロールします。
	Space バーを押す。	1 画面下にスクロールします。
スイッチからのメッセージが急に画面に表示された場合に、現在のコマンドラインを再表示する。	Ctrl+L または Ctrl+R を押す。	現在のコマンドラインを再表示します。

1. 矢印キーは、VT100 などの ANSI 互換端末に限り有効です。

折り返しコマンドラインの編集

コマンドが画面に 1 行で表示しきれない場合は、折り返し機能を使用できます。カーソルが右マージンに達すると、コマンドラインは 10 スペース分左にシフトします。その行の最初の 10 文字は見えませんが、左にスクロールして、コマンドの先頭で構文を確認できます。これらのキーストローク操作は任意です。

コマンド エントリの先頭まで左にスクロールするには、Ctrl+B または左矢印キーを繰り返し押します。Ctrl+A を押して行の先頭にすぐ移動することもできます。

矢印キーは、VT100 などの ANSI 互換端末に限り有効です。

次の例では、**access-list** グローバル コンフィギュレーション コマンドのエントリが 1 行を超えています。カーソルが行の末尾に達すると、行が 10 スペース分左にシフトして再表示されます。ドル記号（$）は行が左にシフトしたことを示します。カーソルが行の末尾に達するたびに、行が再度 10 スペース分左にシフトされます。

```
Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Switch(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Switch(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Switch(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

入力が完了したら、Ctrl+A を押して構文全体を確認してから、Return キーを押してコマンドを実行してください。行の末尾には、行が右にシフトしたことを示すドル記号（$）が表示されます。

```
Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

ソフトウェアでは、端末画面の幅が 80 カラムであると想定しています。端末の幅がそれ以外である場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。

以前の複雑なコマンド エントリを呼び出して変更するには、コマンド履歴機能で行の折り返しを使用します。以前のコマンド エントリの呼び出しについては、「キーストロークによるコマンドの編集」（P.2-7）を参照してください。

show および more コマンドの出力の検索とフィルタリング

show および **more** コマンドの出力を検索してフィルタリングできます。この機能は、大量の出力をソートしたり、表示する必要がない出力を除外する場合に便利です。これらのコマンドの使用は任意です。

この機能を使用するには、**show** コマンドまたは **more** コマンドを入力し、そのあとに*パイプ*文字（|）そして、**begin**、**include**、**exclude** のいずれかのキーワード、および検索またはフィルタリングする文字列を入力します。

command | {**begin** | **include** | **exclude**} *regular-expression*

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

次に、*protocol* を含む行だけが表示されるように指定する例を示します。

```
Switch# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/1 is up, line protocol is down
GigabitEthernet1/2 is up, line protocol is up
```

CLI のアクセス

CLI には、コンソール接続または Telnet を介してアクセスできます。また、ブラウザを使用してアクセスすることもできます。

コンソール接続または Telnet 経由での CLI アクセス

CLI にアクセスするには、スイッチに付属している『クイック スタート ガイド』の説明に従って、スイッチのコンソール ポートに端末または PC を接続し、スイッチの電源をオンにする必要があります。次に、起動プロセスと IP 情報の割り当てに使用できるオプションについて理解するため、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」を参照してください。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションを介して CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。詳細については、「端末回線への Telnet パスワードの設定」（P.11-6）を参照してください。

次のいずれかの方法で、スイッチとの接続を確立できます。

- 管理ステーションまたはダイヤルアップ モデムにスイッチのコンソール ポートを接続します。コンソール ポートへの接続については、スイッチの『クイック スタート ガイド』またはハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化 Secure Shell（SSH; セキュアシェル）パッケージを使用します。スイッチは、Telnet または SSH クライアントにネットワーク接続されていて、イネーブル シークレット パスワードが設定されている必要があります。

  スイッチに Telnet アクセスを設定する方法については、「端末回線への Telnet パスワードの設定」（P.11-6）を参照してください。スイッチは最大 16 個の Telnet セッションを同時にサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

  スイッチに SSH を設定する方法については、「セキュア シェル用のスイッチの設定」（P.11-44）を参照してください。スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソール ポート、Telnet セッション、または SSH セッションを介して接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。

CHAPTER 3

Cisco IE 3000 スイッチ アラームの設定

ここでは、Cisco IE 3000 スイッチのさまざまなアラームを設定する方法を説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのスイッチのコマンド リファレンスを参照してください。

IE 3000 スイッチ アラームの概要

IE 3000 スイッチ ソフトウェアは、スイッチの状態を、ポート単位またはスイッチ単位でモニタします。スイッチまたはポートの現在の状態と設定されているパラメータとが一致しない場合、スイッチ ソフトウェアはアラームを発生させるかシステム メッセージを表示します。デフォルトでは、スイッチ ソフトウェアは、システム メッセージ ロギング ファシリティ（*syslog* ファシリティ）にシステム メッセージを送信します。また、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップを SNMP サーバに送信するようにスイッチを設定することもできます。独立した 2 つのアラーム リレー（メジャーまたはマイナー）を使用すると、外部のアラーム装置をトリガーするようにスイッチを設定することもできます。アラームの設定方法の詳細については、「IE 3000 スイッチ アラームの設定」（P.3-4）を参照してください。

ここでは、次の内容について説明します。

グローバル ステータス モニタリング アラーム

IE 3000 スイッチでは、グローバル アラームまたはファシリティ アラームと呼ばれる、温度と電源装置の状態に関連するアラームを処理できます。表 3-1 に、グローバル アラームの一覧、その説明、および機能を示します。

表 3-1　IE 3000 グローバル ステータス モニタリング アラーム

アラーム	説明
電源装置アラーム	スイッチは、デュアル DC 電源装置レベルをモニタします。システムがデュアル電源モードで動作するように設定されていると、片方の電源装置が故障するか欠けた場合にアラームが発生します。両方の電源装置が揃うか稼動状態になると、アラームは自動的にクリアされます。電源装置アラームをハードウェア リレーに接続するように設定できます。詳細については、「電源装置アラームの設定」（P.3-5）を参照してください。
温度アラーム	スイッチは、スイッチ内部の環境条件をモニタする温度センサーを 2 つ備えています。 • プライマリ アラームは、低温時（–20 ℃）および高温時（95 ℃）で、発生し自動的にイネーブルになります。これをディセーブルにはできません。デフォルトでは、プライマリ温度アラームはメジャー リレーに関連付けられています。 • セカンダリ アラームは、設定されている高温と低音の温度スレッシュホールドよりシステムの温度が高くなった場合もしくは低くなった場合に発生します。デフォルトでは、セカンダリ アラームはディセーブルになっています。 詳細については、「スイッチの温度アラームの設定」（P.3-6）を参照してください。

FCS エラー ヒステリシス スレッシュホールド

イーサネット標準コールの最大ビット エラー レートは 10^{-8} です。IE 3000 スイッチのビット エラー レートは、10^{-6} ～ 10^{-11} の範囲内です。ビット エラー レートをスイッチに入力するには、正の指数を使用します。ビット エラー レートを 10^{-9} に設定する場合、指数の値として 9 を入力します。デフォルトの FCS ビット エラー レートは 10^{-8} です。

実際のビット エラー レートが設定値付近を変動する場合に、FCS エラー ヒステリシス スレッシュホールドを設定することによってアラームの切り替えを防ぐことができます。ヒステリシス スレッシュホールドは、アラーム設定スレッシュホールドに対するアラーム クリア スレッシュホールドの値を比率（%）で定義します。

たとえば、FCS ビット エラー レートのアラーム値が 10^{-8} に設定されている場合、この値がアラーム設定スレッシュホールドです。アラーム クリア スレッシュホールドを $5*10^{-10}$ に設定するには、ヒステリシス、つまり値 *h* を次のように設定します。

h = アラーム クリア スレッシュホールド / アラーム設定スレッシュホールド

$h = 5*10^{-10} / 10^{-8} = 5*10^{-2} = 0.05 = 5\%$

FCS ヒステリシス スレッシュホールドは、スイッチのすべてのポートに適用されます。指定できる範囲は 1 ～ 10% です。デフォルト値は 10% です。詳細については、「FCS Bit Error Rate アラームの設定」（P.3-8）を参照してください。

ポート ステータス モニタリング アラーム

IE 3000 スイッチでは、イーサネット ポートのステータスをモニタし、表 3-2 に示すアラームに基づくアラーム メッセージを生成することもできます。ユーザの時間と手間を省くため、このスイッチはアラーム プロファイルを使用したアラーム設定の変更をサポートしています。プロファイルを複数作成し、各イーサネット ポートに 1 つずつ割り当てることができます。

アラーム プロファイルを使用すると、ポートのアラーム条件をイネーブルまたはディセーブルにしたり、1 つまたは両方のアラーム リレーにアラーム条件を関連付けたりできます。また、アラーム プロファイルを使用してアラーム条件を設定すると、アラーム トラップを SNMP サーバに送信することや、システム メッセージを Syslog サーバに送信することもできます。出荷時の設定（デフォルト）では、すべてのインターフェイスにアラーム プロファイル *defaultPort* が適用されています。

（注）　1 つのリレーに対し複数のアラームを関連付けることも、両方のリレーに対し 1 つのアラームを関連付けることもできます。

表 3-2 に、ポート ステータス モニタリング アラームの一覧、その説明、および機能を示します。各障害には、Cisco IOS システム エラー メッセージ重大度に基づく重大度が割り当てられています。

表 3-2　IE 3000 ポート ステータス モニタリング アラーム

アラーム	説明
Link Fault アラーム	ポートの物理層に問題があり、データ伝送の信頼性が低い場合、スイッチは Link Fault アラームを生成します。一般的なリンク障害は信号またはクロック消失です。リンク障害がクリアされると、Link Fault アラームも自動的にクリアされます。このアラームの重大度は、レベル 3、*エラー状態*です。
Port not Forwarding アラーム	ポートでパケット転送が行われていない場合、スイッチは Port not Forwarding アラームを生成します。ポートでパケット転送が開始されると、このアラームは自動的にクリアされます。このアラームの重大度は、レベル 4、*警告*です。
Port not Operating アラーム	起動時のセルフテスト中にポート障害が発生すると、スイッチは Port not Operating アラームを生成します。発生した Port not Operating アラームは、スイッチの再起動時にポートが動作可能である場合にだけ、クリアされます。このアラームの重大度は、レベル 3、*エラー状態*です。
FCS Bit Error Rate アラーム	設定されている FCS ビット エラー レートに実際のレートが近づくと、スイッチは FCS Bit Error Rate アラームを生成します。各ポートの FCS ビット エラー レートは、インターフェイス コンフィギュレーション CLI を使用して設定できます。詳細については、「FCS Bit Error Rate アラームの設定」（P.3-8）を参照してください。このアラームの重大度は、レベル 3、*エラー状態*です。

アラーム発生のオプション

スイッチでは、次のアラーム発生方法がサポートされています。

- リレー設定

  スイッチは、2 つの独立したアラーム リレーを備えています。アラーム リレーは、グローバル ステータスおよびポート ステータスの状態によって発生させることができます。リレーを設定すると、外部のアラーム装置（ベル、ライト、その他の信号装置など）に障害信号を送信できます。任意のアラーム条件を、アラーム リレーのいずれかまたは両方に関連付けることができます。各障害には、Cisco IOS システム エラー メッセージ重大度に基づく重大度が割り当てられています。

  リレーを設定する方法については、「IE 3000 スイッチ アラームの設定」（P.3-4）を参照してください。

- SNMP トラップ

  SNMP は、マネージャとエージェントの間の通信のメッセージのフォーマットを提供する、アプリケーション層のプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および management information base（MIB; 管理情報ベース）で構成されます。

  snmp-server enable traps コマンドを変更すると、アラーム トラップを SNMP サーバに送信できるようになります。アラーム プロファイルを使用して、SNMP アラーム トラップを送信するための環境またはポート ステータス アラーム条件を設定できます。詳細については、「SNMP トラップのイネーブル化」（P.3-11）を参照してください。

- Syslog メッセージ

  アラーム プロファイルを使用すると、システム メッセージを Syslog サーバに送信できます。詳細については、「IE 3000 スイッチ アラームの設定」（P.3-4）を参照してください。

IE 3000 スイッチ アラームの設定

IE 3000 スイッチ アラームのデフォルト設定

表 3-3　IE 3000 スイッチ アラームのデフォルト設定

	アラーム	デフォルト設定
グローバル	電源装置アラーム	スイッチのシングル電源モードの場合にイネーブルになります。アラームはありません。 デュアル電源装置モードの場合、デフォルトのアラーム通知として、システム メッセージがコンソールに表示されます。
	プライマリ温度アラーム	スイッチ温度が最高 95 ºC から最低 –20ºC の範囲のときにイネーブルになります。 スイッチのプライマリ温度アラームは、メジャー リレーに関連付けられています。
	セカンダリ温度アラーム	ディセーブル。
Port	Link Fault アラーム	すべてのインターフェイスでディセーブル。
	Port not Forwarding アラーム	すべてのインターフェイスでディセーブル。
	Port not Operating アラーム	すべてのインターフェイスでイネーブル。
	FCS Bit Error Rate アラーム	すべてのインターフェイスでディセーブル。

電源装置アラームの設定

ここでは、スイッチの電源装置アラームを設定する方法を説明します。次の設定情報について説明します。

電源モードの設定

IE 3000 スイッチには DC 電源入力が 2 つあります。デフォルトでは、システムはシングル電源モードで稼動します。**power-supply dual** グローバル コンフィギュレーション コマンドを使用すると、デュアル モードで稼動するように設定できます。デュアル電源モードでは、プライマリ電源装置が故障すると、2 番めの電源装置からスイッチに電源が供給されます。

デュアル電源モードでスイッチが稼動するように設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**power-supply dual**	デュアル モードで稼動するようにシステムを設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show alarm settings**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

シングル電源モードで稼動するようにスイッチの設定を戻すことによって、このアラームをディセーブルにするには、**no power-supply dual** コマンドを使用します。

電源装置アラーム オプションの設定

電源装置アラームをリレーに関連付けるには、**alarm facility power-supply** グローバル コンフィギュレーション コマンドを使用します。電源装置アラームに関連付けたすべてのアラームとトラップを、Syslog サーバおよび SNMP サーバに送信するように設定することもできます。

電源装置アラームをリレーに関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm facility power-supply relay** {**major** | **minor**}	電源装置アラームをメジャー リレーまたはマイナー リレーに関連付けます。
ステップ 3	**alarm facility power-supply notifies**	電源装置アラーム トラップを SNMP サーバに送信します。
ステップ 4	**alarm facility power-supply syslog**	電源装置アラーム トラップを Syslog サーバに送信します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show alarm settings**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

リレー、Syslog サーバ、または SNMP サーバへのアラーム送信をディセーブルにするには、**no alarm facility power-supply relay**、**no alarm facility power-supply notifies**、**no alarm facility power-supply syslog** の各グローバル コンフィギュレーション コマンドを使用します。

（注）　**notifies** コマンドを使用してアラーム トラップを SNMP サーバに送信するには、まず **snmp-server enable traps alarms** グローバル コンフィギュレーション コマンドを使用して SNMP サーバをセットアップする必要があります。「SNMP トラップのイネーブル化」（P.3-11）を参照してください。

次に、電源装置モニタリング アラームをマイナー リレーに設定する例を示します。

```
Switch(config) # alarm facility power-supply relay minor
```

スイッチの温度アラームの設定

プライマリ温度アラームおよびセカンダリ温度アラームの温度スレッシュホールドは変更できます。また、プライマリ温度アラームおよびセカンダリ温度アラームの、メジャー リレーまたはマイナー リレーへの関連付けも変更できます。

ここでは、スイッチの温度アラームを設定する方法を説明します。次の設定情報について説明します。

- 「スイッチのプライマリ温度スレッシュホールドの設定」（P.3-6）
- 「スイッチのセカンダリ温度スレッシュホールドの設定」（P.3-7）
- 「温度アラームのリレーへの関連付け」（P.3-7）

スイッチのプライマリ温度スレッシュホールドの設定

alarm facility temperature primary グローバル コンフィギュレーション コマンドを使用すると、プライマリ温度モニタリング アラームの低温スレッシュホールドおよび高温スレッシュホールドを設定できます。

高温スレッシュホールドを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm facility temperature primary high** *threshold*	プライマリ高温スレッシュホールド値を設定します。スレッシュホールドは、–150 ℃～ 300 ℃の範囲に設定します。
ステップ 3	**alarm facility temperature primary low** *threshold*	プライマリ低温スレッシュホールド値を設定します。スレッシュホールドは、–200 ℃～ 250 ℃の範囲に設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show alarm settings**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

温度モニタリング アラーム設定を削除してデフォルト設定に戻すには、**no alarm facility temperature primary high** *threshold* グローバル コンフィギュレーション コマンドを使用します。

次に、プライマリ温度モニタリング アラーム設定を削除してデフォルト設定に戻す例を示します。

```
Switch(config) # no alarm facility temperature primary high 45
```

スイッチのセカンダリ温度スレッシュホールドの設定

alarm facility temperature secondary グローバル コンフィギュレーション コマンドを使用すると、セカンダリ温度モニタリング アラームの低温スレッシュホールドおよび高温スレッシュホールドを設定できます。

低温スレッシュホールドを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm facility temperature secondary high** *threshold*	セカンダリ高温スレッシュホールド値を設定します。スレッシュホールドは、–150 ℃～ 300 ℃の範囲に設定します。
ステップ 3	**alarm facility temperature secondary low** *threshold*	セカンダリ低温スレッシュホールド値を設定します。スレッシュホールドは、–200 ℃～ 250 ℃の範囲に設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show alarm settings**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

セカンダリ温度スレッシュホールド アラームをディセーブルにするには、**no alarm facility temperature secondary** *threshold* グローバル コンフィギュレーション コマンドを使用します。

次に、セカンダリ温度スレッシュホールド アラームをディセーブルにする例を示します。

```
Switch(config) # no alarm facility temperature secondary 45
```

温度アラームのリレーへの関連付け

デフォルトでは、プライマリ温度アラームはメジャー リレーに関連付けられています。**alarm facility temperature** グローバル コンフィギュレーション コマンドを使用すると、マイナー リレー、SNMP トラップ、Syslog メッセージにプライマリ温度アラームを関連付けたり、メジャー リレー、マイナー リレー、SNMP トラップ、Syslog メッセージにセカンダリ温度アラームを関連付けたりできます。

セカンダリ温度アラームをリレーに関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm facility temperature** {**primary** | **secondary**} **relay** {**major** | **minor**}	プライマリ温度アラームまたはセカンダリ温度アラームをリレーに関連付けます。
ステップ 3	**alarm facility temperature** {**primary** | **secondary**} **notifies**	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを SNMP サーバに送信します。
ステップ 4	**alarm facility temperature** {**primary** | **secondary**} **syslog**	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを Syslog サーバに送信します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show alarm settings**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　**notifies** コマンドを使用してアラーム トラップを SNMP サーバに送信するには、まず **snmp-server enable traps alarms** グローバル コンフィギュレーション コマンドを使用して SNMP サーバをセットアップする必要があります。「SNMP トラップのイネーブル化」（P.3-11）を参照してください。

セカンダリ温度アラームをディセーブルにするには、**no alarm facility temperature secondary** グローバル コンフィギュレーション コマンドを使用します。

次に、高温スレッシュホールド値を 45ºC にして、セカンダリ温度アラームをマイナー リレーに設定する例を示します。このアラームに関連付けられたすべてのアラームとトラップは、Syslog サーバと SNMP サーバに送信されます。

```
Switch(config) # alarm facility temperature secondary high 45
Switch(config) # alarm facility temperature secondary relay minor
Switch(config) # alarm facility temperature secondary syslog
Switch(config) # alarm facility temperature secondary notifies
```

次に、1 番めの（プライマリ）温度アラームをメジャー リレーに設定する例を示します。このアラームに関連付けられたすべてのアラームとトラップは、Syslog サーバに送信されます。

```
Switch(config) # alarm facility temperature primary syslog
Switch(config) # alarm facility temperature primary relay major
```

FCS Bit Error Rate アラームの設定

ここでは、スイッチの FCS Bit Error Rate アラームを設定する方法について説明します。

- 「FCS エラー スレッシュホールドの設定」（P.3-8）
- 「FCS エラー ヒステリシス スレッシュホールドの設定」（P.3-9）

FCS エラー スレッシュホールドの設定

設定されているレートに実際のレートが近づくと、スイッチは FCS Bit Error Rate アラームを生成します。FCS エラー スレッシュホールドを設定するには、**fcs-threshold** インターフェイス コンフィギュレーション コマンドを使用します。

ポートのビット エラー レート値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを入力して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**fcs-threshold** *value*	FCS エラー レートを設定します。 *value* に 6 ～ 11 の範囲の値を指定することにより、最大ビット エラー レート 10^{-6} ～ 10^{-11} を設定できます。 デフォルトの FCS ビット エラー レートは 10^{-8} です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show fcs-threshold**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの FCS スレッシュホールド値に戻すには、**no fcs-threshold** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの FCS ビット エラー レートを 10^{-10} に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if) # fcs-threshold 10
```

FCS エラー ヒステリシス スレッシュホールドの設定

実際のビット エラー レートが設定値付近を変動する場合に、ヒステリシスを設定することによってアラームの切り替えを防ぐことができます。FCS エラー ヒステリシス スレッシュホールドを設定するには、**alarm facility fcs-hysteresis** グローバル コンフィギュレーション コマンドを使用します。

（注）　FCS ヒステリシス スレッシュホールドは、IE 3000 スイッチのすべてのポートに適用されます。

スイッチの FCS エラー ヒステリシス スレッシュホールドを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm facility fcs-hysteresis** *percentage*	スイッチのヒステリシスをパーセント値で設定します。 *percentage* に指定できる範囲は 1 ～ 10 です。デフォルト値は 10% です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

FCS エラー ヒステリシス スレッシュホールドをデフォルト値に設定するには、**no alarm facility fcs-hysteresis** コマンドを使用します。

（注）　**show running config** コマンドを使用すると、デフォルト値以外の FCS エラー ヒステリシスが表示されます。

次に、FCS エラー ヒステリシスを 5% に設定する例を示します。

```
Switch(config)# alarm facility fcs-hysteresis 5
```

アラーム プロファイルの設定

ここでは、スイッチのアラーム プロファイルを設定する方法を説明します。次の設定情報について説明します。

- 「アラーム プロファイルの作成または変更」（P.3-10）
- 「特定のポートへのアラーム プロファイルの割り当て」（P.3-11）

アラーム プロファイルの作成または変更

alarm profile グローバル コンフィギュレーション コマンドを使用すると、アラーム プロファイルを作成したり、既存のプロファイルを変更したりできます。新しいアラーム プロファイルを作成した時点では、いずれのアラームもイネーブルになっていません。

（注）　*defaultPort* プロファイルでイネーブルになるアラームは、Port not Operating アラームだけです。

アラーム プロファイルを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm profile** ***name***	新しいプロファイルを作成するか、既存のプロファイルを指定して、アラーム プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**alarm** *alarm-id*	特定アラームのアラーム パラメータを追加または変更します（表 3-4 を参照）。指定できる値は 1 ～ 4 です。スペースで区切ることにより、複数のアラーム ID を入力できます。
ステップ 4	**notifies** *alarm-id*	（任意）SNMP トラップを SNMP サーバに送信するようにアラームを設定します。
ステップ 5	**relay-major** *alarm-id* **relay-minor** *alarm-id*	（任意）アラーム トラップをメジャー リレーに送信するようにアラームを設定します。 （任意）アラーム トラップをマイナー リレーに送信するようにアラームを設定します。
ステップ 6	**syslog** *alarm-id*	（任意）アラーム トラップを Syslog サーバに送信するようにアラームを設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show alarm profile** ***name***	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アラーム プロファイルを削除するには、**no alarm profile** ***name*** グローバル コンフィギュレーション コマンドを使用します。

次に、fastEthernetPort 用のアラーム プロファイル *fastE* を、リンクダウン（*alarmList* ID 3）アラームと 30% の FCS エラー レート（*alarmList* ID 4）アラームをイネーブルにした状態で作成または変更する例を示します。リンクダウン アラームはマイナー リレーに、FCS エラー レート アラームはメジャー リレーに接続されます。また、これらのアラームは、SNMP サーバに通知を、Syslog サーバにシステム メッセージを送信します。

```
Switch(config)# alarm profile fastE
Switch(config-alarm- prof)# alarm 3 4
Switch(config-alarm- prof)# relay major 4
Switch(config-alarm- prof)# relay minor 3
Switch(config-alarm- prof)# notifies 3 4
Switch(config-alarm- prof)# syslog 3 4
```

（注）　**notifies** コマンドを使用してアラーム トラップを SNMP サーバに送信するには、まず **snmp-server enable traps alarms** グローバル コンフィギュレーション コマンドを使用して SNMP サーバをセットアップする必要があります。「SNMP トラップのイネーブル化」（P.3-11）を参照してください。

表 3-4 に、*alarmList* ID と、対応するアラーム定義の一覧を示します。こららのアラームの詳細については、「ポート ステータス モニタリング アラーム」（P.3-3）を参照してください。

表 3-4　AlarmList ID 番号とアラームの説明

AlarmList ID	アラームの説明
1	リンク障害
2	ポートで転送が行われていない
3	ポートが動作していない
4	FCS エラー レートがスレッシュホールドを超えている

特定のポートへのアラーム プロファイルの割り当て

インターフェイス コンフィギュレーション モードで **alarm-profile** コマンドを使用すると、アラーム プロファイルを特定のポートに割り当てることができます。

アラーム プロファイルをポートに割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *port interface*	設定するスイッチ ポートの番号を入力して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**alarm-profile** ***name***	指定したプロファイルをインターフェイスに割り当てます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show alarm profile**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

特定のポートからアラーム プロファイルを削除するには、**no alarm-profile** ***name*** インターフェイス コンフィギュレーション コマンドを使用します。

次に、*fastE* というアラーム プロファイルをポートに割り当てる例を示します。

```
Switch(config)# interface fastethernet 1/2
Switch(config-if)# alarm profile fastE
```

次に、*fastE* というアラーム プロファイルをポートから削除する例を示します。

```
Switch(config)# interface fastethernet 1/2
Switch(config-if)# no alarm profile fastE
```

SNMP トラップのイネーブル化

alarm トラップを送信するようにスイッチをイネーブル化するには、**snmp-server enable traps alarms** グローバル コンフィギュレーション コマンドを使用します。

（注）　アラーム プロファイルを使用して、SNMP アラーム トラップ通知を SNMP サーバに送信するようにスイッチを設定するには、まず **snmp-server enable traps alarms** グローバル コンフィギュレーション コマンドを使用して SNMP をイネーブル化する必要があります。

アラーム トラップを送信するようにスイッチをイネーブル化するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server enable traps alarms**	SNMP トラップを送信するようにスイッチをイネーブル化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show alarm settings**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IE 3000 スイッチのアラーム ステータスの表示

グローバルおよびポートのアラーム ステータスを表示するには、表 3-5 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 3-5　グローバルおよびポートのアラーム ステータスを表示するコマンド

コマンド	目的
show alarm description port	アラームの番号とその説明文を表示します。
show alarm profile [*name*]	システム内のすべてのアラーム プロファイル、または指定したプロファイルを表示します。
show alarm settings	スイッチに設定されているすべてのグローバル アラームを表示します。
show env {**all** | **power** | **temperature**}	スイッチの環境ファシリティのステータスを表示します。
show facility-alarm status [**critical** | **info** | **major** | **minor**]	スイッチに生成されたアラームを表示します。

CHAPTER 4

スイッチの IP アドレスとデフォルト ゲートウェイの割り当て

この章では、自動および手動の各方法を使用して IE 3000 スイッチのスイッチ初期設定（IP アドレスおよびデフォルト ゲートウェイ情報の割り当てなど）を作成する方法について説明します。また、スイッチ スタートアップ コンフィギュレーションの変更方法についても説明します。この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスと、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』を参照してください。

この章で説明する内容は、次のとおりです。

（注） IP アドレスおよび Dynamic Host Configuration Protocol（DHCP）の設定に関するこの章の情報は、IP Version 4（IPv4）に固有の情報です。スイッチ上で IP Version 6（IPv6）フォワーディングをイネーブルにする場合は、第 42 章「IPv6 ユニキャスト ルーティングの設定」で、IPv6 アドレスのフォーマットおよび設定に固有の情報を参照してください。IPv6 をイネーブルにするには、スイッチが IP サービス イメージを実行している必要があります。

起動プロセスの概要

スイッチを起動するには、『*クイック スタート ガイド*』またはハードウェア インストレーション ガイドの手順に従って、スイッチを設置して電源を投入し、スイッチの初期設定（IP アドレス、サブネット マスク、デフォルト ゲートウェイ、シークレット パスワード、Telnet パスワードなど）を行う必要があります。

通常の起動プロセスには、ブート ローダ ソフトウェアの動作が含まれます。ブート ローダは、次の処理を実行します。

- 低レベルの CPU 初期化を実行します。CPU レジスタを初期化することにより、物理メモリがマッピングされる場所、物理メモリの量および速度などを制御します。
- CPU サブシステムの Power-on Self-Test（POST; 電源投入時セルフテスト）を実行します。CPU Dynamic Random Access Memory（DRAM; ダイナミック ランダム アクセス メモリ）と、フラッシュ ファイル システムを構成するフラッシュ装置の部分をテストします。
- システム ボード上のコンパクト フラッシュ ファイル システムを初期化します。
- デフォルトのオペレーティング システム ソフトウェア イメージをメモリにロードし、スイッチを起動します。

ブート ローダによってフラッシュ ファイル システムにアクセスしてから、オペレーティング システムをロードします。ブート ローダは通常、オペレーティング システムのロード、圧縮解除、および起動の目的でだけ使用します。オペレーティング システムが CPU を制御できるようになると、次にシステムがリセットされるかシステムの電源が投入されるまで、ブート ローダはアクティブになりません。

スイッチには、Cisco IOS ソフトウェアのイメージおよびコンフィギュレーション ファイルを格納するリムーバブル コンパクト フラッシュ カードがあります。スイッチを再設定しなくても、スイッチを交換およびアップグレードできます。コンパクト フラッシュ カードを取り外しても、電源のオフ/オンまたはユーザの操作のために Cisco IOS ソフトウェアのリロードが必要にならない限り、スイッチ動作は中断されません。ただし、コンパクト フラッシュ カードを取り外すと、フラッシュ ファイル システムにアクセスできなくなり、アクセスを試みるとエラー メッセージが生成されます。スイッチには、インストール済みのコンパクト フラッシュ メモリ カードが付属しています。また、スイッチは、あらゆるサイズのコンパクト フラッシュ カードに対応しています。

コンパクト フラッシュ ファイルの設定を表示するには、**show flash:** 特権 EXEC コマンドを使用します。このコマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf009.html#wp1018357

スイッチのコンパクト フラッシュ メモリ カードの取り外しまたは交換方法については、『*Cisco IE 3000 Hardware Installation Guide*』を参照してください。

オペレーティング システムに重大な問題が発生し、オペレーティング システムを使用できない場合、ブート ローダはトラップドアからシステムにアクセスします。トラップドア メカニズムにより、システムへの十分なアクセスが提供され、必要に応じて、フラッシュ ファイル システムをフォーマットし、Xmodem プロトコルを使用してオペレーティング システム ソフトウェア イメージを再インストールし、失われたパスワードを回復して、最終的にオペレーティング システムを再起動できます。詳細については、「ソフトウェア障害からの回復」（P.52-2）および「パスワードを忘れた場合の回復」（P.52-3）を参照してください。

（注） パスワード回復はディセーブルにできます。詳細については、「パスワード回復のディセーブル化」（P.11-5）を参照してください。

スイッチ情報を割り当てるには、PC または端末をコンソール ポートに接続し、PC またはターミナル エミュレーション ソフトウェアのボー レートおよびキャラクタ フォーマットをスイッチ コンソール ポートの設定と一致させておく必要があります。

- ボー レートのデフォルトは 9600 です。
- データ ビットのデフォルトは 8 です。

（注） データ ビット オプションが 8 に設定されている場合、パリティ オプションは「なし」に設定します。

- ストップ ビットのデフォルトは 1 です。
- パリティ設定のデフォルトは「なし」です。

スイッチ情報の割り当て

IP 情報の割り当ては、スイッチのセットアップ プログラムを使用するか、DHCP サーバを使用するか、手動で実行できます。

特定の IP 情報の設定が必要な場合は、スイッチのセットアップ プログラムを使用します。このプログラムを使用すると、ホスト名とイネーブル シークレット パスワードを設定することもできます。また、任意で、Telnet パスワードを割り当てたり（リモート管理中のセキュリティを確保する場合）、スイッチをクラスタのコマンド スイッチまたはメンバー スイッチ、あるいはスタンドアロン スイッチとして設定したりすることもできます。セットアップ プログラムの詳細については、ハードウェア インストレーション ガイドを参照してください。

DHCP サーバの設定後は、DHCP サーバを使用して IP 情報の一元管理および自動割り当てを行います。

（注）　DHCP を使用する場合、スイッチがダイナミックに割り当てられた IP アドレスを受信してコンフィギュレーション ファイルを読み込むまでは、セットアップ プログラムの質問に応答しないでください。

スイッチの設定手順に精通した上級ユーザの場合は、手動でスイッチを設定してください。それ以外のユーザは、前述のセットアップ プログラムを使用してください。

- 「デフォルトのスイッチ情報」（P.4-3）
- 「DHCP ベースの自動設定の概要」（P.4-4）
- 「手動での IP 情報の割り当て」（P.4-15）

デフォルトのスイッチ情報

表 4-1 に、デフォルトのスイッチ情報を示します。

表 4-1　デフォルトのスイッチ情報

機能	デフォルト設定
IP アドレスおよびサブネット マスク	IP アドレスまたはサブネット マスクは定義されていません。
デフォルト ゲートウェイ	デフォルト ゲートウェイは定義されていません。
イネーブル シークレット パスワード	パスワードは定義されていません。
ホスト名	出荷時に割り当てられたデフォルトのホスト名は、*Switch* です。
Telnet パスワード	パスワードは定義されていません。
クラスタ コマンド スイッチ機能	ディセーブル。
クラスタ名	クラスタ名は定義されません。

DHCP ベースの自動設定の概要

DHCP は、インターネット ホストおよびインターネットワーキング装置に設定情報を提供します。このプロトコルは、2 つのコンポーネントで構成されています。1 つは DHCP サーバから装置に設定パラメータを提供するコンポーネントで、もう 1 つは装置にネットワーク アドレスを割り当てるメカニズムです。DHCP はクライアント サーバ モデルに基づいています。このモデルでは、指定された DHCP サーバが、ダイナミックに設定された装置に対して、ネットワーク アドレスを割り当てて設定パラメータを提供します。スイッチは、DHCP クライアントと DHCP サーバの両方として動作できます。

DHCP ベースの自動設定では、スイッチ（DHCP クライアント）は起動時に、IP アドレス情報およびコンフィギュレーション ファイルを使用して自動的に設定されます。

DHCP ベースの自動設定を使用する場合、スイッチ上で DHCP クライアント側の設定を行う必要はありません。ただし、DHCP サーバには、IP アドレスに関連する各種リース オプションを設定する必要があります。DHCP を使用してネットワーク上のコンフィギュレーション ファイルをリレーする場合は、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバおよび Domain Name System（DNS; ドメイン ネーム システム）サーバの設定が必要なこともあります。

スイッチの DHCP サーバは、スイッチと同じ LAN 上に配置することも、スイッチとは別の LAN 上に配置することもできます。DHCP サーバが別の LAN 上で実行されている場合は、スイッチと DHCP サーバの間に DHCP リレー装置を設定する必要があります。リレー装置は、直接接続されている 2 つの LAN の間でブロードキャスト トラフィックを転送します。ルータは、ブロードキャスト パケットを転送しませんが、受信したパケットの宛先 IP アドレスに基づいてパケットを転送します。

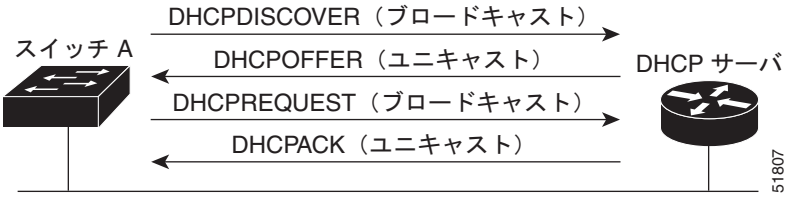
DHCP ベースの自動設定は、スイッチの Bootstrap Protocol（BOOTP）クライアント機能に代わるものです。

DHCP クライアントの要求プロセス

スイッチの起動時にスイッチにコンフィギュレーション ファイルが存在しない場合、DHCP クライアントが呼び出され、DHCP クライアントが DHCP サーバに設定情報を要求します。コンフィギュレーション ファイルが存在し、その設定に特定のルーテッド インターフェイスの **ip address dhcp** インターフェイス コンフィギュレーション コマンドが含まれる場合、DHCP クライアントが呼び出され、DHCP クライアントがインターフェイスに IP アドレス情報を要求します。

図 4-1 に、DHCP クライアントと DHCP サーバ間で交換される一連のメッセージを示します。

図 4-1　　DHCP クライアントと サーバ間のメッセージ交換



クライアントであるスイッチ A は、DHCP サーバを見つけるために DHCPDISCOVER メッセージをブロードキャストします。DHCP サーバは、DHCPOFFER ユニキャスト メッセージによって、設定パラメータ（IP アドレス、サブネット マスク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレス用のリースなど）をクライアントに提供します。

DHCPREQUEST ブロードキャスト メッセージで、クライアントは、提供された設定情報に対する正式な要求を DHCP サーバに返します。この正式な要求はブロードキャストされるため、クライアントから DHCPDISCOVER ブロードキャスト メッセージを受信した他のすべての DHCP サーバは、クライアントに提供した IP アドレスを再利用できます。

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに返すことで、IP アドレスがクライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバインドされ、クライアントはサーバから受信した設定情報を使用します。スイッチが受信する情報量は、DHCP サーバの設定方法によって異なります。詳細については、「TFTP サーバの設定」（P.4-7）を参照してください。

DHCPOFFER ユニキャスト メッセージによってクライアントに送信された設定パラメータが無効である（設定エラーが存在する）場合、クライアントは DHCPDECLINE ブロードキャスト メッセージを DHCP サーバに返します。

DHCP サーバはクライアントに、提供した設定パラメータが割り当てられてない、パラメータのネゴシエーション中にエラーが発生した、または DHCPOFFER メッセージに対するクライアントの応答が遅れている（DHCP サーバがパラメータを別のクライアントに割り当てた）という意味の DHCPNAK 拒否ブロードキャスト メッセージを送信します。

DHCP クライアントは、複数の DHCP サーバまたは BOOTP サーバから提供された情報を受信し、そのうちの任意の 1 つを受け入れることができますが、通常は最初に受け取った情報を受け入れます。DHCP サーバから提供された IP アドレスが必ずしもスイッチに割り当てられるわけではありません。ただし、サーバは通常、クライアントが正式にアドレスを要求するまでアドレスを予約します。スイッチが BOOTP サーバからの応答を受け入れて、そのスイッチ自体を設定する場合、スイッチはスイッチ コンフィギュレーション ファイルを取得するために、TFTP 要求をユニキャストではなくブロードキャストします。

DHCP hostname オプションを使用すると、スイッチのグループは、一元管理している DHCP サーバからホスト名および標準設定を取得できます。クライアント（スイッチ）は DCHPDISCOVER メッセージに、ホスト名およびその他の設定パラメータを DHCP サーバに要求するために使用するオプション 12 フィールドを含めます。すべてのクライアントのコンフィギュレーション ファイルは、DHCP から取得したホスト名を除いてすべて同じになります。

クライアントのホスト名がデフォルトの場合（**hostname** *name* グローバル コンフィギュレーション コマンドが設定されていないか、ホスト名を削除するための **no hostname** グローバル コンフィギュレーション コマンドが入力されていない場合）、**ip address dhcp** インターフェイス コンフィギュレーション コマンドを入力したときに DHCP hostname オプションがパケット内に含まれません。この場合、クライアントがインターフェイスの IP アドレスの取得中に DHCP 経由で DCHP hostname オプションを受け取った場合、クライアントは DCHP hostname オプションを受け入れ、システムにホスト名が設定されたことを示すフラグを設定します。

DHCP ベースの自動設定およびイメージ更新の概要

DHCP イメージ アップグレード機能を使用すると、新しいイメージと新しいコンフィギュレーション ファイルの両方をネットワーク内の 1 つまたは複数のスイッチにダウンロードするように DHCP サーバを設定できます。これにより、ネットワークに新しく追加された各スイッチが同じイメージおよび設定を受信することが保証されます。

DHCP イメージのアップグレードには、DHCP 自動設定と DHCP 自動イメージ更新の 2 種類があります。

DHCP 自動設定

DHCP 自動設定では、DHCP サーバからネットワーク内の 1 つまたは複数のスイッチにコンフィギュレーション ファイルをダウンロードします。ダウンロードされたコンフィギュレーション ファイルが、そのスイッチの実行コンフィギュレーションになります。スイッチをリロードするまで、フラッシュ メモリに保存されているブートアップ設定は上書きされません。

DHCP 自動イメージ更新

DHCP 自動設定とともに DHCP 自動イメージ更新を使用すると、設定と新しいイメージの両方をネットワーク内の 1 つまたは複数のスイッチにダウンロードできます。新しい設定と新しいイメージをダウンロード中のスイッチは、ブランクになる（または、出荷時のデフォルト設定がロードされるだけの）場合があります。

すでに設定を含むスイッチに新しい設定をダウンロードすると、ダウンロードされた設定はスイッチに格納されているコンフィギュレーション ファイルに追加されます（既存の設定は、ダウンロードされた設定によって上書きされません）。

（注）　スイッチの DHCP 自動イメージ更新をイネーブルにするには、イメージとコンフィギュレーション ファイルが配置されている TFTP サーバのオプション 67（コンフィギュレーション ファイル名）、オプション 66（DHCP サーバ ホスト名）、オプション 150（TFTP サーバ アドレス）、およびオプション 125（ファイルの説明）を正しく設定する必要があります。

スイッチを DHCP サーバとして設定する手順については、「DHCP ベースの自動設定の設定」（P.4-6）と、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」にある「Configuring DHCP」を参照してください。

スイッチをネットワーク内に設置したあと、自動イメージ更新機能を起動します。ダウンロードされたコンフィギュレーション ファイルは、スイッチの実行コンフィギュレーションに保存されます。また、新しいイメージは、スイッチにダウンロードされてインストールされます。スイッチを再起動すると、その設定がスイッチの保存済みコンフィギュレーションに格納されます。

制限事項および制約事項

次に、制限事項について説明します。

- ネットワーク内で割り当てられた IP アドレスを使用せずにアップ状態になっているレイヤ 3 インターフェイスが 1 つも存在しない場合、保存済みの設定プロセスを使用した DHCP ベースの自動設定は停止します。
- タイムアウトを設定しない限り、保存済みの設定機能を使用した DHCP ベースの自動設定は IP アドレスのダウンロードを無期限に試行します。
- コンフィギュレーション ファイルがダウンロードできない、またはコンフィギュレーション ファイルが破損している場合、自動インストール プロセスは停止します。

（注）　TFTP からダウンロードされたコンフィギュレーション ファイルは、実行コンフィギュレーションの既存の設定に結合されますが、**write memory** または **copy running-configuration startup configuration** 特権 EXEC コマンドを入力しない限り、Nonvolatile Random-Access Memory（NVRAM; 不揮発性 RAM）に保存されません。ダウンロードされた設定がスタートアップ コンフィギュレーションに保存されると、それ以降はシステムが再起動しても機能はトリガーされません。

DHCP ベースの自動設定の設定

- 「DHCP サーバ設定時の注意事項」（P.4-7）
- 「TFTP サーバの設定」（P.4-7）
- 「DNS の設定」（P.4-8）

DHCP サーバ設定時の注意事項

装置を DHCP サーバとして設定する場合は、次の注意事項に従ってください。

DHCP サーバには、スイッチのハードウェア アドレスによって各スイッチにバインドされている予約済みリースを設定する必要があります。

スイッチが IP アドレス情報を受信するようにするには、DHCP サーバに次のリース オプションを設定する必要があります。

- クライアントの IP アドレス（必須）
- クライアントのサブネット マスク（必須）
- ルータの IP アドレス（スイッチで使用するデフォルト ゲートウェイ アドレス）（必須）
- DNS サーバの IP アドレス（任意）

スイッチが TFTP サーバからコンフィギュレーション ファイルを受信するようにするには、DHCP サーバに次のリース オプションを設定する必要があります。

- TFTP サーバ名（必須）
- ブート ファイル名（クライアントに必要なコンフィギュレーション ファイルの名前）（推奨）
- ホスト名（任意）

DHCP サーバの設定によっては、スイッチは IP アドレス情報またはコンフィギュレーション ファイル、あるいはその両方を受信できます。

前述のリース オプションを設定しなかった場合、DHCP サーバは、設定されたパラメータだけを使用してクライアントの要求に応答します。IP アドレスおよびサブネット マスクが応答に含まれていないと、スイッチは設定されません。ルータの IP アドレスまたは TFTP サーバ名が見つからなかった場合、スイッチは TFTP 要求を、ユニキャストではなく、ブロードキャスト送信することがあります。その他のリース オプションは、使用できなくても自動設定には影響しません。

スイッチは、DHCP サーバとして動作できます。デフォルトでは、Cisco IOS DHCP サーバおよびリレー エージェントの機能はスイッチ上でイネーブルになっていますが、設定されていません。つまり、これらの機能は動作可能な状態ではありません。DHCP サーバがシスコ デバイスである場合、DHCP の設定方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] で『*Cisco IOS IP Configuration Guide*』の「IP Addressing and Services」にある「Configuring DHCP」を参照してください。

TFTP サーバの設定

DHCP サーバの設定に基づいて、スイッチは TFTP サーバから 1 つまたは複数のコンフィギュレーション ファイルをダウンロードしようとします。TFTP サーバへの IP 接続に必要なすべてのオプションを指定して、スイッチに応答するように DHCP サーバを設定しており、さらに、TFTP サーバ名、アドレス、およびコンフィギュレーション ファイル名を DHCP サーバに指定している場合、スイッチは指定された TFTP サーバから指定されたコンフィギュレーション ファイルをダウンロードしようとします。

コンフィギュレーション ファイル名および TFTP サーバを指定しなかった場合、またはコンフィギュレーション ファイルをダウンロードできなかった場合、スイッチは、ファイル名と TFTP サーバ アドレスをさまざまに組み合わせてコンフィギュレーション ファイルをダウンロードしようとします。

ファイルには、指定されたコンフィギュレーション ファイル名（ある場合）と、network-config、cisconet.cfg、*hostname*.config、または *hostname*.cfg の各ファイルが含まれています（*hostname* はスイッチの現在のホスト名です）。使用される TFTP サーバ アドレスには、指定された TFTP サーバ アドレス（ある場合）、およびブロードキャスト アドレス（255.255.255.255）が含まれています。

スイッチがコンフィギュレーション ファイルを正常にダウンロードするには、TFTP サーバのベース ディレクトリに 1 つまたは複数のコンフィギュレーション ファイルが含まれている必要があります。含めることができるファイルは、次のとおりです。

- DHCP 応答で指定されているコンフィギュレーション ファイル（実際のスイッチ コンフィギュレーション ファイル）
- network-confg または cisconet.cfg ファイル（デフォルトのコンフィギュレーション ファイル）
- router-confg または ciscortr.cfg ファイル（これらのファイルには、すべてのスイッチに共通のコマンドが含まれています。通常、DHCP および TFTP サーバが適切に設定されている場合、これらのファイルにはアクセスしません）

DHCP サーバリース データベースに TFTP サーバ名を指定する場合は、DNS サーバのデータベースに TFTP サーバ名から IP アドレスへのマッピングを設定する必要もあります。

使用する TFTP サーバがスイッチとは別の LAN 上にある場合、またはスイッチがブロードキャスト アドレスを使用して TFTP サーバにアクセスする場合（前述のすべての必須情報が DHCP サーバの応答に含まれていない場合）は、TFTP サーバに TFTP パケットを転送するようにリレーを設定する必要があります。詳細については、「リレー装置の設定」（P.4-8）を参照してください。問題を解決するには、必要なすべての情報を DHCP サーバに設定することを推奨します。

DNS の設定

DHCP サーバは、DNS サーバを使用して TFTP サーバ名を IP アドレスに解決します。DNS サーバ上で、TFTP サーバ名から IP アドレスへのマッピングを設定する必要があります。TFTP サーバには、スイッチのコンフィギュレーション ファイルが含まれています。

DNS サーバの IP アドレスを、DHCP 応答が IP アドレスを取得する DHCP サーバのリース データベースに設定できます。リース データベースには、DNS サーバの IP アドレスを 2 つまで入力できます。

DNS サーバは、スイッチと同じ LAN 上に配置することも、スイッチとは別の LAN 上に配置することもできます。DNS サーバが別の LAN 上に存在する場合、スイッチはルータを介して DNS サーバにアクセスできる必要があります。

リレー装置の設定

スイッチが、異なる LAN 上のホストからの応答を必要とするブロードキャスト パケットを送信する場合は、リレー装置（*リレー エージェント*とも呼ぶ）を設定する必要があります。スイッチが送信する可能性のあるブロードキャスト パケットの例として、DHCP パケット、DNS パケット、場合によっては TFTP パケットが挙げられます。このリレー装置は、インターフェイス上で受信されたブロードキャスト パケットを宛先ホストに転送するように設定する必要があります。

リレー装置が Cisco ルータである場合、IP ルーティングをイネーブルにし（**ip routing** グローバル コンフィギュレーション コマンド）、**ip helper-address** インターフェイス コンフィギュレーション コマンドを使用してヘルパー アドレスを設定します。

図 4-2 では、ルータ インターフェイスを次のように設定しています。

インターフェイス 10.0.0.2 の設定：

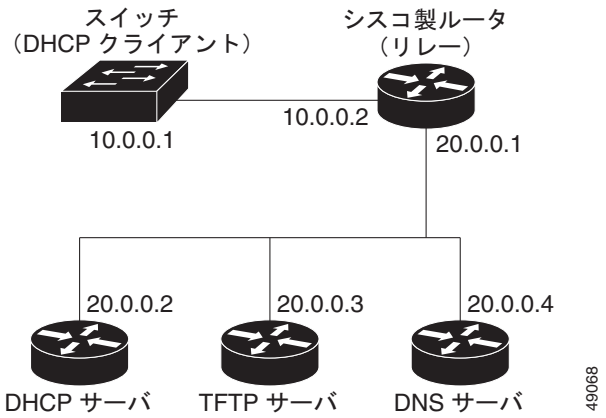
```
router(config-if)# ip helper-address 20.0.0.2
router(config-if)# ip helper-address 20.0.0.3
router(config-if)# ip helper-address 20.0.0.4
```

インターフェイス 20.0.0.1 の設定：

```
router(config-if)# ip helper-address 10.0.0.1
```

（注）　スイッチがリレー装置として動作するようにするには、インターフェイスをルーテッド ポートとして設定します。詳細については、「ルーテッド ポート」（P.14-4）および「レイヤ 3 インターフェイスの設定」（P.14-21）を参照してください。

図 4-2　　自動設定でのリレー装置の使用



コンフィギュレーション ファイルの取得

DHCP の予約済みリースで IP アドレスおよびコンフィギュレーション ファイル名のアベイラビリティに応じて、スイッチは次の方法で設定情報を取得します。

- スイッチの IP アドレスおよびコンフィギュレーション ファイル名が予約され、DHCP 応答に含まれている場合（1 ファイル読み込み方式）。

  スイッチは、IP アドレス、サブネット マスク、TFTP サーバ アドレス、およびコンフィギュレーション ファイル名を DHCP サーバから受信します。スイッチは、TFTP サーバにユニキャスト メッセージを送信し、名前付きコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、起動プロセスを完了します。

- スイッチの IP アドレスおよびコンフィギュレーション ファイル名が予約されているが、DHCP 応答に TFTP サーバ アドレスが含まれていない場合（1 ファイル読み込み方式）。

  スイッチは、IP アドレス、サブネット マスク、およびコンフィギュレーション ファイル名を DHCP サーバから受信します。スイッチは、TFTP サーバにブロードキャスト メッセージを送信し、名前付きコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、起動プロセスを完了します。

- スイッチの IP アドレスだけが予約されて DHCP 応答に含まれていて、コンフィギュレーション ファイル名は含まれていない場合（2 ファイル読み込み方式）。

  スイッチは、IP アドレス、サブネット マスク、および TFTP サーバ アドレスを DHCP サーバから受信します。スイッチは、TFTP サーバにユニキャスト メッセージを送信し、network-confg または cisconet.cfg のデフォルト コンフィギュレーション ファイルを取得します（network-confg ファイルが読み込めない場合、スイッチは cisconet.cfg ファイルを読み込みます）。

デフォルトのコンフィギュレーション ファイルには、スイッチのホスト名から IP アドレスへのマッピングが含まれています。スイッチは、ファイルの情報をホスト テーブルに書き込み、ホスト名を取得します。ファイルでホスト名が見つからない場合、スイッチは DHCP 応答内のホスト名を使用します。ホスト名が DHCP 応答で指定されていない場合、スイッチはデフォルトの *Switch* をホスト名として使用します。

デフォルトのコンフィギュレーション ファイルまたは DHCP 応答からホスト名を取得したあと、スイッチはホスト名と同じ名前のコンフィギュレーション ファイル（network-confg または cisconet.cfg のどちらが先に読み込まれたかによって、ファイル名は *hostname*-confg または *hostname*.cfg になります）を TFTP サーバから読み込みます。cisconet.cfg ファイルが読み込まれた場合は、ホストのファイル名は 8 文字に切り捨てられます。

network-confg、cisconet.cfg、またはホスト名と同じ名前のファイルを読み込むことができない場合、スイッチは router-confg ファイルを読み込みます。router-confg ファイルを読み込むことができない場合、スイッチは ciscortr.cfg ファイルを読み込みます。

（注） DHCP 応答から TFTP サーバを取得できなかった場合、ユニキャスト送信によるコンフィギュレーション ファイルの読み込みにすべて失敗した場合、または TFTP サーバ名を IP アドレスに解決できない場合には、スイッチは TFTP サーバ要求をブロードキャストします。

設定例

図 4-3 に、DHCP ベースの自動設定を使用して IP 情報を取得するネットワークの例を示します。

図 4-3　DHCP ベースの自動設定ネットワークの例

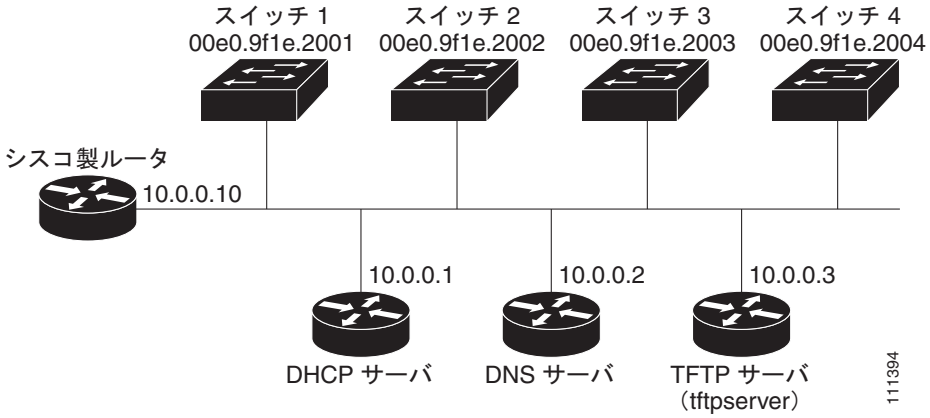


表 4-2 に、DHCP サーバ上の予約済みリースの設定を示します。

表 4-2　DHCP サーバの設定

	スイッチ A	スイッチ B	スイッチ C	スイッチ D
バインディング キー（ハードウェア アドレス）	00e0.9f1e.2001	00e0.9f1e.2002	00e0.9f1e.2003	00e0.9f1e.2004
IP アドレス	10.0.0.21	10.0.0.22	10.0.0.23	10.0.0.24
サブネット マスク	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
ルータ アドレス	10.0.0.10	10.0.0.10	10.0.0.10	10.0.0.10

表 4-2　DHCP サーバの設定 （続き）

	スイッチ A	スイッチ B	スイッチ C	スイッチ D
DNS サーバ アドレス	10.0.0.2	10.0.0.2	10.0.0.2	10.0.0.2
TFTP サーバ名	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*
ブート ファイル名（コンフィギュレーション ファイル）（任意）	switcha-confg	switchb-confg	switchc-confg	switchd-confg
ホスト名（任意）	switcha	switchb	switchc	switchd

DNS サーバの設定

DNS サーバは、TFTP サーバ名 *tftpserver* を IP アドレス 10.0.0.3 にマッピングします。

TFTP サーバの設定（UNIX の場合）

TFTP サーバのベース ディレクトリは、/tftpserver/work/ に設定されています。このディレクトリには、2 ファイル読み込み方式で使用される network-confg ファイルがあります。このファイルには、IP アドレスに基づいてスイッチに割り当てられるホスト名が含まれています。ベース ディレクトリには、次に示すように、各スイッチのコンフィギュレーション ファイル（*switcha-confg*、*switchb-confg* など）も含まれています。

```
prompt> cd /tftpserver/work/
prompt> ls
network-confg
switcha-confg
switchb-confg
switchc-confg
switchd-confg
prompt> cat network-confg
ip host switcha 10.0.0.21
ip host switchb 10.0.0.22
ip host switchc 10.0.0.23
ip host switchd 10.0.0.24
```

DHCP クライアントの設定

スイッチ A ～ D には、コンフィギュレーション ファイルは存在しません。

設定の説明

図 4-3 の場合、スイッチ A は、コンフィギュレーション ファイルを次のようにして読み込みます。

- DHCP サーバから IP アドレス 10.0.0.21 を取得します。
- DHCP サーバの応答にコンフィギュレーション ファイル名が含まれていない場合、スイッチ A は TFTP サーバのベース ディレクトリから network-confg ファイルを読み込みます。
- ホスト テーブルに network-confg ファイルの内容を追加します。
- IP アドレス 10.0.0.21 をホスト名（switcha）にインデックス付けすることで、ホスト テーブルを読み込みます。
- ホスト名に対応するコンフィギュレーション ファイルを読み込みます。たとえば、TFTP サーバから *switch1-confg* ファイルを読み込みます。

スイッチ B ～ D も同様に、それぞれのコンフィギュレーション ファイルおよび IP アドレスを取得します。

DHCP 自動設定およびイメージ更新機能の設定

DHCP を使用して新しいイメージと新しい設定をスイッチにダウンロードするには、少なくとも 2 つのスイッチを設定する必要があります。1 つのスイッチは、DHCP および TFTP サーバとして動作します。クライアント スイッチは、新しいコンフィギュレーション ファイルだけ、または新しいコンフィギュレーション ファイルと新しいイメージ ファイルの両方をダウンロードするように設定されます。

DHCP 自動設定の設定（コンフィギュレーション ファイルのみ）

DHCP 自動設定を設定し、新しいコンフィギュレーション ファイルをダウンロードする新しいスイッチに TFTP および DHCP の設定値を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp** *poolname*	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**bootfile** *filename*	ブート イメージとして使用するコンフィギュレーション ファイルの名前を指定します。
ステップ 4	**network** *network-number mask prefix-length*	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。 **（注）** プレフィクス長は、アドレス プレフィクスを構成するビット数を指定します。プレフィクスは、クライアントのネットワーク マスクを指定する代替の方法です。プレフィクス長の先頭には、スラッシュ（/）を付加する必要があります。
ステップ 5	**default-router** *address*	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。
ステップ 6	**option 150** *address*	TFTP サーバの IP アドレスを指定します。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**tftp-server flash**:*filename.text*	TFTP サーバ上のコンフィギュレーション ファイルを指定します。
ステップ 9	**interface** *interface-id*	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ 10	**no switchport**	インターフェイスをレイヤ 3 モードにします。
ステップ 11	**ip address** *address mask*	インターフェイスの IP アドレスとマスクを指定します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、スイッチがコンフィギュレーション ファイルをダウンロードするように、スイッチを DHCP サーバとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

DHCP 自動イメージ更新の設定（コンフィギュレーション ファイルとイメージ）

DHCP 自動設定を設定し、新しいイメージと新しいコンフィギュレーション ファイルをダウンロードする新しいスイッチに TFTP および DHCP の設定値を指定するには、特権 EXEC モードで次の手順を実行します。

（注）　次の表の手順を実行する前に、スイッチにアップロードするテキスト ファイル（autoinstall_dhcp など）を作成する必要があります。テキスト ファイルには、ダウンロードするイメージの名前を指定します。このイメージは、bin ファイルではなく、tar ファイルである必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *name*	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**bootfile** *filename*	ブート イメージとして使用するファイルの名前を指定します。
ステップ 4	**network** *network-number mask prefix-length*	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。 （注）　プレフィクス長は、アドレス プレフィクスを構成するビット数を指定します。プレフィクスは、クライアントのネットワーク マスクを指定する代替の方法です。プレフィクス長の先頭には、スラッシュ（/）を付加する必要があります。
ステップ 5	**default-router** *address*	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。
ステップ 6	**option 150** *address*	TFTP サーバの IP アドレスを指定します。
ステップ 7	**option 125** *hex*	イメージ ファイルへのパスが記述されているテキスト ファイルへのパスを指定します。
ステップ 8	**copy tftp flash** *filename.txt*	テキスト ファイルをスイッチにアップロードします。
ステップ 9	**copy tftp flash** *imagename.tar*	新しいイメージの tar ファイルをスイッチにアップロードします。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**tftp-server flash**:*config.text*	TFTP サーバ上の Cisco IOS コンフィギュレーション ファイルを指定します。
ステップ 12	**tftp-server flash**:*imagename.tar*	TFTP サーバ上のイメージ名を指定します。
ステップ 13	**tftp-server flash**:*filename.txt*	ダウンロードするイメージ ファイルの名前を含むテキスト ファイルを指定します。
ステップ 14	**interface** *interface-id*	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ 15	**no switchport**	インターフェイスをレイヤ 3 モードにします。
ステップ 16	**ip address** *address mask*	インターフェイスの IP アドレスとマスクを指定します。
ステップ 17	**end**	特権 EXEC モードに戻ります。
ステップ 18	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、スイッチがコンフィギュレーション ファイルをダウンロードするように、スイッチを DHCP サーバとして設定する例を示します。

```
Switch# config terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:c-ipservices-mz.122-44.3.SE.tar
Switch(config)# tftp-server flash:ies-lanbase-tar.122-44.EX.tar
Switch(config)# tftp-server flash:boot-config.text
Switch(config)# tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

クライアントの設定

DHCP サーバからコンフィギュレーション ファイルと新しいイメージをダウンロードするようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot host dhcp**	保存済みコンフィギュレーションを使用した自動設定をイネーブルにします。
ステップ 3	**boot host retry timeout** *timeout-value*	（任意）システムがコンフィギュレーション ファイルのダウンロードを試行する時間を設定します。 **（注）** タイムアウトを設定しない場合、システムは DHCP サーバからの IP アドレスの取得を無期限に試行します。
ステップ 4	**banner config-save ^C** *warning-message* **^C**	（任意）コンフィギュレーション ファイルを NVRAM に保存しようとしたときに表示される警告メッセージを作成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show boot**	設定を確認します。

次に、VLAN 99 のレイヤ 3 Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を使用して、保存済みコンフィギュレーションを使用した DHCP ベースの自動設定をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(conf)# boot host dhcp
Switch(conf)# boot host retry timeout 300
Switch(conf)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause
You to No longer Automatically Download Configuration Files at Reboot^C
Switch(config)# vlan 99
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:         no
Manual Boot:          no
HELPER path-list:
NVRAM/Config file
      buffer size:    32768
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
Switch#
```

（注）　実行することは、レイヤ 3 インターフェイスを設定してイネーブルにすることだけです。IP アドレス、または保存済みコンフィギュレーションを使用した DHCP ベースの自動設定は割り当てないでください。

手動での IP 情報の割り当て

複数のスイッチ仮想インターフェイス（SVI）に手動で IP 情報を割り当てるには、特権 EXEC モードで次の手順を実行します。

（注）　スイッチが IP サービス イメージを実行している場合、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してポートをレイヤ 3 モードに設定しておくと、ポートにも手動で IP 情報を割り当てることができます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id*	インターフェイス コンフィギュレーション モードを開始し、IP 情報を割り当てる VLAN を入力します。指定できる VLAN 範囲は 1 ～ 4094 です。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスおよびサブネット マスクを入力します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 5	**ip default-gateway** *ip-address*	デフォルト ゲートウェイが設定されているスイッチに直接接続されているネクストホップ ルータ インターフェイスの IP アドレスを入力します。デフォルト ゲートウェイは、解決されていない宛先 IP アドレスを含む IP パケットをスイッチから受信します。 デフォルト ゲートウェイが設定されると、スイッチは、ホストが通信する必要のあるリモート ネットワークに接続できます。 **（注）** IP でルーティングするようにスイッチを設定した場合は、デフォルト ゲートウェイを設定する必要はありません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces vlan** *vlan-id*	設定された IP アドレスを確認します。
ステップ 8	**show ip redirects**	設定されたデフォルト ゲートウェイを確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチの IP アドレスを削除するには、**no ip address** インターフェイス コンフィギュレーション コマンドを使用します。Telnet セッションでアドレスを削除すると、スイッチへの接続が切断されます。デフォルト ゲートウェイ アドレスを削除するには、**no ip default-gateway** グローバル コンフィギュレーション コマンドを使用します。

スイッチのシステム名の設定、特権 EXEC コマンドへのアクセス保護、時刻サービスとカレンダー サービスの設定については、第 7 章「スイッチの管理」を参照してください。

実行コンフィギュレーションの確認と保存

入力した設定値または変更内容を確認するには、次の特権 EXEC コマンドを入力します。

```
Switch# show running-config
Building configuration...

Current configuration: 1363 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch A
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
.
<output truncated>
.
interface gigabitethernet1/1
no switchport
ip address 172.20.137.50 255.255.255.0
!
interface gigabitethernet1/2
mvr type source

<output truncated>

...!
```

```
interface VLAN1
 ip address 172.20.137.50 255.255.255.0
 no ip directed-broadcast
!
ip default-gateway 172.20.137.1 !
!
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12
!
end
```

スタートアップ コンフィギュレーションに対して行った設定や変更をフラッシュ メモリに保存するには、次の特権 EXEC コマンドを入力します。

```
Switch# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

このコマンドは、入力した設定値を保存します。このコマンドを実行しないと、次回システムをリロードするときに設定が消失します。フラッシュ メモリの NVRAM セクションに保存されている情報を表示するには、**show startup-config** または **more startup-config** 特権 EXEC コマンドを使用します。

コンフィギュレーション ファイルのコピーの代替保管場所については、付録 B「Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作」を参照してください。

NVRAM バッファ サイズの設定

デフォルトの NVRAM バッファ サイズは 512 KB です。場合によっては、コンフィギュレーション ファイルが大きすぎ、NVRAM に保存できないことがあります。一般的に、これは、スイッチ スタックのスイッチが多いときに発生します。大きなコンフィギュレーション ファイルをサポートするために、NVRAM バッファのサイズを設定できます。新しい NVRAM バッファ サイズは、現在および新規のメンバー スイッチすべてで同期されます。

（注） NVRAM バッファ サイズを設定したあと、スイッチまたはスイッチ スタックをリロードします。

スイッチがスタックに追加され、NVRAM サイズが異なる場合、新しいスイッチはスタックと同期し、自動的にリロードされます。

NVRAM バッファ サイズを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot buffersize** *size*	NVRAM バッファ サイズを KB 単位で設定します。*size* に指定できる範囲は 4096 ～ 1048576 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show boot**	設定を確認します。

次の例では、NVRAM バッファ サイズを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# boot buffersize 524288
Switch(config)# end
Switch# show boot
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   :
NVRAM/Config file
      buffer size:   524288
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
Switch#
```

スタートアップ コンフィギュレーションの変更

- 「デフォルトのブート コンフィギュレーション」（P.4-18）
- 「コンフィギュレーション ファイルの自動ダウンロード」（P.4-19）
- 「手動での起動」（P.4-19）
- 「特定のソフトウェア イメージの起動」（P.4-20）
- 「環境変数の制御」（P.4-21）

スイッチ コンフィギュレーション ファイルの詳細については、付録 B「Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作」も参照してください。

デフォルトのブート コンフィギュレーション

表 4-3　デフォルトのブート コンフィギュレーション

機能	デフォルト設定
オペレーティング システム ソフトウェア イメージ	スイッチは、BOOT 環境変数内の情報を使用して、自動的にシステムの起動を試みます。この変数が設定されていない場合、スイッチは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初の実行可能イメージをロードして実行しようとします。 Cisco IOS イメージは、イメージ ファイル（拡張子 .bin を除く）と同じ名前のディレクトリに保存されています。 ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。
コンフィギュレーション ファイル	設定済みのスイッチは、フラッシュ メモリのシステム ボードに保存されている *config.text* ファイルを使用します。 新しいスイッチには、コンフィギュレーション ファイルがありません。

コンフィギュレーション ファイルの自動ダウンロード

DHCP ベースの自動設定機能を使用すると、スイッチにコンフィギュレーション ファイルを自動的にダウンロードできます。詳細については、「DHCP ベースの自動設定の概要」（P.4-4）を参照してください。

システム設定を読み書きするファイル名の指定

デフォルトでは、Cisco IOS ソフトウェアは、*config.text* ファイルを使用して、システム設定の不揮発性コピーを読み書きします。ただし、別のファイル名を指定することもでき、このファイルは次の起動サイクル時にロードされます。

別のコンフィギュレーション ファイル名を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot config-file flash:***/file-url*	次の起動サイクル時にロードするコンフィギュレーション ファイルを指定します。 *file-url* には、パス（ディレクトリ）とコンフィギュレーション ファイル名を指定します。 ファイル名およびディレクトリ名では、大文字と小文字が区別されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show boot**	設定を確認します。 **boot config-file** グローバル コンフィギュレーション コマンドは、CONFIG_FILE 環境変数の設定を変更します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no boot config-file** グローバル コンフィギュレーション コマンドを使用します。

手動での起動

デフォルトでは、スイッチは自動的に起動しますが、手動で起動するように設定することができます。

次の起動サイクル時に手動で起動するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot manual**	次の起動サイクル時に手動で起動するようにスイッチをイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show boot**	設定を確認します。 **boot manual** グローバル コマンドは、MANUAL_BOOT 環境変数の設定を変更します。 次回システムを再起動すると、スイッチはブート ローダ モードで起動します。このことは *switch:* プロンプトで確認できます。システムを起動するには、**boot** *filesystem***:**/*file-url* ブート ローダ コマンドを使用します。 • システム ボード フラッシュ装置の場合、*filesystem***:** に **flash:** を使用します。 • *file-url* には、パス（ディレクトリ）と、ブート可能イメージの名前を指定します。 ファイル名およびディレクトリ名では、大文字と小文字が区別されます。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

手動での起動をディセーブルにするには、**no boot manual** グローバル コンフィギュレーション コマンドを使用します。

特定のソフトウェア イメージの起動

デフォルトでは、スイッチは、BOOT 環境変数内の情報を使用して自動的にシステムの起動を試みます。この変数が設定されていない場合、スイッチは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初の実行可能イメージをロードして実行しようとします。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。ただし、起動する特定のイメージを指定できます。

次の起動サイクル時に特定のイメージを起動するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot system** *filesystem***:**/*file-url*	次の起動サイクル時にフラッシュ メモリ内の特定のイメージを起動するようにスイッチを設定します。 • システム ボード フラッシュ装置の場合、*filesystem***:** に **flash:** を使用します。 • *file-url* には、パス（ディレクトリ）と、ブート可能イメージの名前を指定します。 ファイル名およびディレクトリ名では、大文字と小文字が区別されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show boot**	設定を確認します。 **boot system** グローバル コマンドは、BOOT 環境変数の設定を変更します。 次の起動サイクル時、スイッチは、BOOT 環境変数内の情報を使用して自動的にシステムを起動しようとします。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no boot system** グローバル コンフィギュレーション コマンドを使用します。

環境変数の制御

正常に動作しているスイッチでは、9600 b/s に設定されたスイッチ コンソール接続でだけブート ローダ モードが開始されます。スイッチの電源コードを取り外し、電源コードの再接続中に **Mode** ボタンを押します。ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、**Mode** ボタンを放します。すると、ブート ローダの *switch:* プロンプトが表示されます。

スイッチのブート ローダ ソフトウェアは不揮発性の環境変数をサポートするので、この環境変数を使用して、ブート ローダまたはシステムで稼動する他のソフトウェアの動作を制御できます。ブート ローダの環境変数は、UNIX または DOS システムで設定できる環境変数と類似しています。

値が設定された環境変数は、フラッシュ ファイル システム外のフラッシュ メモリに保存されています。

これらのファイルの各行には、環境変数名と等号、その後ろに変数の値が格納されています。このファイルに表示されていない変数には値がありません。表示されていればヌル ストリングであっても値があります。ヌル ストリング（たとえば " "）に設定されている変数は、値が設定された変数です。多くの環境変数は事前に定義されており、デフォルト値が設定されています。

環境変数には、次の 2 種類のデータが保存されます。

- Cisco IOS コンフィギュレーション ファイルを読み込まないコードを制御するデータ。たとえば、ブート ローダの機能を拡張したり、その機能にパッチを適用したりするブート ローダ ヘルパー ファイルの名前は、環境変数として保存できます。
- Cisco IOS コンフィギュレーション ファイルを読み込むコードを制御するデータ。たとえば、Cisco IOS コンフィギュレーション ファイル名は環境変数として保存できます。

環境変数の設定を変更するには、ブート ローダにアクセスするか、Cisco IOS コマンドを使用します。通常の環境では、環境変数の設定を変更する必要はありません。

（注） ブート ローダ コマンドと環境変数の構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

表 4-4 で、最も一般的な環境変数の機能について説明します。

表 4-4　環境変数

変数	ブート ローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BOOT	**set BOOT** *filesystem***:**/*file-url ...* 自動起動時にロードおよび実行しようとする実行可能ファイルのセミコロン区切りリスト。BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 環境変数が設定されていても指定されたイメージをロードできない場合は、システムはフラッシュ ファイル システムで最初に見つかったブート可能ファイルを起動しようとします。	**boot system** *filesystem:/file-url ...* 次の起動サイクル時にロードする Cisco IOS イメージを指定します。このコマンドは、BOOT 環境変数の設定を変更します。
MANUAL_BOOT	**set MANUAL_BOOT yes** スイッチが自動で起動するか、または手動で起動するかを決定します。 有効値は 1、yes、0、および no です。no または 0 に設定されている場合、ブート ローダはシステムを自動的に起動しようとします。他の値に設定されている場合は、ブート ローダ モードから手動でスイッチを起動する必要があります。	**boot manual** 次の起動サイクル時の手動スイッチ起動をイネーブルにし、MANUAL_BOOT 環境変数の設定を変更します。 次回システムを再起動すると、スイッチはブート ローダ モードで起動します。システムを起動するには、**boot flash:***filesystem***:**/*file-url* ブート ローダ コマンドを使用してブート可能イメージの名前を指定します。
CONFIG_FILE	**set CONFIG_FILE flash:**/*file-url* Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を変更します。	**boot config-file flash:**/*file-url* Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。このコマンドは、CONFIG_FILE 環境変数を変更します。

ソフトウェア イメージのリロードのスケジューリング

スイッチへのソフトウェア イメージのリロードをあとで（深夜、週末などスイッチをあまり使用しないときに）実行するようにスケジューリングできます。または、（ネットワーク内のすべてのスイッチでソフトウェアをアップグレードする場合などに）ネットワーク全体でリロードを同時に行うことができます。

（注）　リロードは、約 24 日以内に実行されるようにスケジューリングする必要があります。

リロードのスケジューリング設定

ソフトウェア イメージのリロードをあとで実行するようにスイッチを設定するには、特権 EXEC モードで次のいずれかのコマンドを使用します。

- **reload in** [*hh*:]*mm* [*text*]

  このコマンドは、指定した時間内（時間および分で指定）に実行するようにソフトウェアのリロードをスケジューリングします。リロードは、約 24 日以内に実行される必要があります。リロードの理由を最大 255 文字の文字列で指定できます。

- **reload at** *hh*:*mm* [*month day* | *day month*] [*text*]

  このコマンドは、指定した時刻（24 時間表記）に実行するようにソフトウェアのリロードをスケジューリングします。月日を指定すると、リロードは指定された日時で実行するようにスケジューリングされます。月日を指定しない場合、リロードは、現在の日付の指定された時刻（指定された時刻が現在の時刻よりもあとの場合）または翌日（指定された時刻が現在の時刻よりも前の場合）に実行されます。00:00 を指定すると、リロードのスケジューリングは午前 0 時に設定されます。

（注）　**at** キーワードを使用するのは、Network Time Protocol（NTP; ネットワーク タイム プロトコル）、ハードウェアのカレンダー、または手動によってスイッチのシステム クロックが設定されている場合だけです。時刻は、スイッチに設定されているタイム ゾーンに基づきます。複数のスイッチでリロードが同時に実行されるようスケジューリングするには、各スイッチの時刻が NTP と同期している必要があります。

reload コマンドは、システムを停止します。手動で起動するように設定されていない場合、システムは自動的に再起動します。**reload** コマンドは、スイッチの設定情報をスタートアップ コンフィギュレーション（**copy running-config startup-config**）に保存したあとで使用してください。

手動で起動するようにスイッチが設定されている場合は、仮想端末からリロードしないでください。これは、スイッチがブート ローダ モードになり、その結果、リモート ユーザが制御を失うことを防止するためです。

コンフィギュレーション ファイルを変更すると、リロードの前に設定を保存するよう求めるプロンプトが表示されます。保存操作時に、すでに存在しないスタートアップ コンフィギュレーション ファイルが CONFIG_FILE 環境変数によって指定された場合、保存を続行するかどうかを確認するメッセージが表示されます。この状況で保存を続行すると、リロード時にセットアップ モードが開始されます。

次に、現在の日付の午後 7 時 30 分にソフトウェアをスイッチにリロードする例を示します。

```
Switch# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 1996 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

次に、将来の日時を指定して、ソフトウェアをスイッチにリロードする例を示します。

```
Switch# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 1996 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

スケジューリング済みのリロードをキャンセルするには、**reload cancel** 特権 EXEC コマンドを使用します。

リロードのスケジューリング情報の表示

スケジューリング済みのリロードに関する情報を表示したり、スイッチにリロードがスケジューリングされているかどうかを調べたりするには、**show reload** 特権 EXEC コマンドを使用します。

このコマンドは、リロードの予定実行時刻、リロードの理由（リロードのスケジューリング設定時に指定した場合）など、リロードに関する情報を表示します。

CHAPTER 5

Cisco IOS Configuration Engine の設定

この章では、IE 3000 スイッチでこの機能を設定する方法について説明します。

（注） Cisco Configuration Engine の設定の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

この章で使用しているコマンドの構文および使用方法の詳細については、次の URL にある『*Cisco IOS Network Management Command Reference, Release 12.4*』を参照してください。
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

Cisco Configuration Engine ソフトウェアの概要

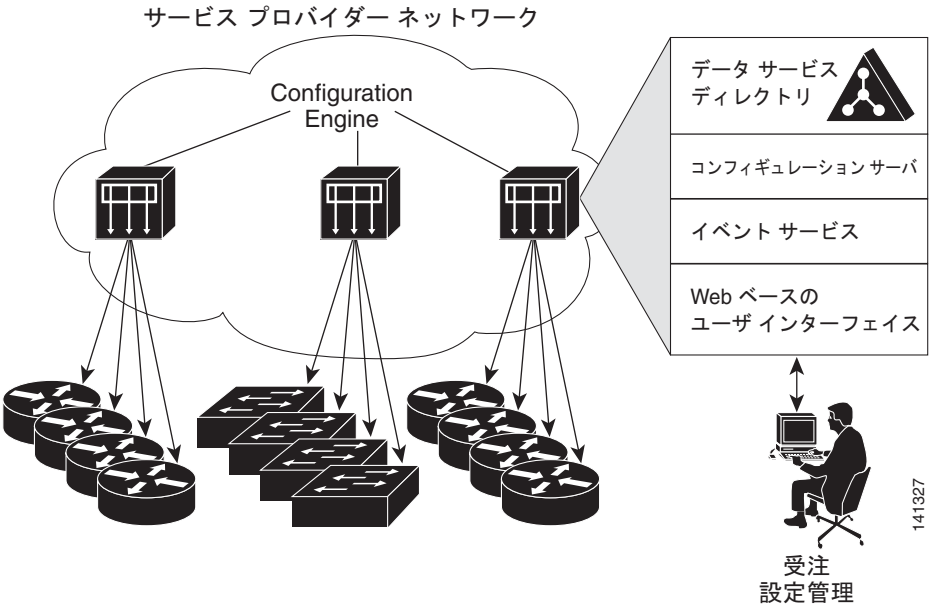
Cisco Configuration Engine は、ネットワーク装置とサービスの配置および管理を自動化するコンフィギュレーション サービスとして機能するネットワーク管理ソフトウェアです（図 5-1 を参照）。各 Configuration Engine は、シスコ デバイス（スイッチおよびルータ）のグループと、それらの装置が提供するサービスを管理し、それぞれの設定を保管し、必要に応じて配信します。Configuration Engine では、装置に固有の設定変更を生成して装置に送信し、設定変更を実行して、結果をログに記録することで、初期設定と設定更新を自動化します。

Configuration Engine は、スタンドアロン モードおよびサーバ モードをサポートし、次の CNS コンポーネントを含みます。

- コンフィギュレーション サービス（Web サーバ、ファイル マネージャ、および名前空間マッピング サーバ）
- イベント サービス（イベント ゲートウェイ）
- データ サービス ディレクトリ（データ モデルおよびスキーマ）

スタンドアロン モードでは、Configuration Engine は組み込みのディレクトリ サービスをサポートします。このモードでは、外部ディレクトリまたはその他のデータ ストアは必要ありません。サーバ モードでは、Configuration Engine はユーザ定義の外部ディレクトリの使用をサポートします。

図 5-1　Configuration Engine アーキテクチャの概要



- 「コンフィギュレーション サービス」（P.5-2）
- 「イベント サービス」（P.5-3）
- 「CNS ID および装置のホスト名に関する重要事項」（P.5-3）

コンフィギュレーション サービス

コンフィギュレーション サービスは、Cisco Configuration Engine のコア コンポーネントです。コンフィギュレーション サービスは、スイッチの Cisco IOS CNS エージェントと連携して機能するコンフィギュレーション サーバで構成されています。コンフィギュレーション サービスは、論理グループによる初期設定および大量の再設定のために、スイッチに装置およびサービスの設定を配信します。スイッチは、ネットワーク上で初めて起動するときに、コンフィギュレーション サービスから初期設定を受信します。

コンフィギュレーション サービスは CNS イベント サービスを使用して設定の変更イベントを送受信し、成功および失敗の通知を送信します。

コンフィギュレーション サーバは、コンフィギュレーション テンプレートや組み込み（スタンドアロン モード）またはリモート（サーバ モード）のディレクトリに保存されている装置固有の設定情報を使用する Web サーバです。

コンフィギュレーション テンプレートは、CLI コマンドの形式でスタティックな設定情報を含むテキスト ファイルです。テンプレートでは、変数は Lightweight Directory Access Protocol（LDAP）URL を使用して指定されます。LDAP URL は、ディレクトリに保存されている装置固有の設定情報を参照します。

Cisco IOS エージェントは、受信したコンフィギュレーション ファイルで構文チェックを実行し、イベントをパブリッシュして構文チェックの成功または失敗を示します。コンフィギュレーション エージェントは設定をすぐに適用するか、コンフィギュレーション サーバから同期イベントを受信するまで適用を遅延できます。

イベント サービス

Cisco Configuration Engine では、設定イベントの受信と生成にイベント サービスを使用します。イベント エージェントはスイッチ上にあり、スイッチと Configuration Engine 上のイベント ゲートウェイ間の通信を簡素化します。

イベント サービスは、拡張性の高いパブリッシュおよびサブスクライブ通信方式です。イベント サービスは、サブジェクト ベースのアドレッシングを使用して、メッセージを宛先に送信します。サブジェクト ベースのアドレッシング規則では、メッセージおよびそれらの宛先について単純で同一の名前空間を定義します。

NameSpace Mapper

Configuration Engine には NameSpace Mapper（NSM）が含まれています。NSM は、アプリケーション、装置またはグループ ID、およびイベントに基づいて装置の論理グループを管理するための検索サービスを提供します。

Cisco IOS 装置は、Cisco IOS ソフトウェアで設定された名前（cisco.cns.config.load など）と一致するイベント サブジェクト名だけを認識します。名前空間マッピング サービスを使用すると、目的の命名規則を使用してイベントを指定できます。データ ストアをサブジェクト名で設定している場合、NSM はイベント サブジェクト名ストリングを Cisco IOS で認識される名前に変更します。

サブスクライバの場合は、一意の装置 ID とイベントを指定すると、名前空間マッピング サービスから、サブスクライブする一連のイベントが返されます。同様に、パブリッシャの場合は、一意のグループ ID、装置 ID、およびイベントを指定すると、マッピング サービスから、パブリッシュする一連のイベントが返されます。

CNS ID および装置のホスト名に関する重要事項

Configuration Engine では、設定された各スイッチに一意の ID が関連付けられていると見なされます。一意の ID は複数のシノニムで使用できます。各シノニムは特定の名前空間においては一意です。イベント サービスは、メッセージのサブジェクト ベースのアドレッシングに、名前空間コンテンツを使用します。

Configuration Engine では、2 つの名前空間が交差します。1 つはイベント バスで使用され、もう 1 つはコンフィギュレーション サーバで使用されます。コンフィギュレーション サーバの名前空間の範囲内では、*ConfigID* が装置の一意の ID を表します。イベント バスの名前空間の範囲内では、*DeviceID* が装置の CNS 固有の ID を表します。

Configuration Engine ではイベント バスとコンフィギュレーション サーバの両方を使用して装置に設定を提供するため、設定されるスイッチごとに ConfigID と Device ID の両方を定義する必要があります。

コンフィギュレーション サーバの単一のインスタンスの範囲内では、設定された 2 つのスイッチは、ConfigID に対して同じ値を共有できません。イベント バスの単一のインスタンスの範囲内では、設定された 2 つのスイッチは、DeviceID に対して同じ値を共有できません。

ConfigID

設定済みスイッチごとに一意の ConfigID があります。ConfigID は、対応するスイッチ CLI 属性のセットに対する Configuration Engine ディレクトリのキーとして使用されます。スイッチで定義されている ConfigID は、Configuration Engine の対応するスイッチ定義の ConfigID と一致する必要があります。

ConfigID は起動時に固定され、装置が再起動するまでは、スイッチのホスト名が再設定された場合でも変更できません。

DeviceID

イベント バスに関与する設定済みスイッチごとに一意の DeviceID があります。DeviceID はスイッチの送信元アドレスと同じであるため、スイッチをバス上の特定の宛先として指定できます。**cns config partial** グローバル コンフィギュレーション コマンドで設定されたすべてのスイッチが、イベント バスにアクセスする必要があります。したがって、スイッチから発信される DeviceID は、Configuration Engine の対応するスイッチ定義の DeviceID と一致する必要があります。

DeviceID の発信元は、スイッチの Cisco IOS ホスト名で定義されます。ただし、DeviceID 変数とその使用は、スイッチに隣接するイベント ゲートウェイ内部に限られます。

イベント バス上の論理 Cisco IOS 終端地点はイベント ゲートウェイに組み込まれ、その後スイッチの代わりにプロキシとして機能します。イベント ゲートウェイは、スイッチとそれに対応するイベント バスの DeviceID を表します。

スイッチは、イベント ゲートウェイへの接続に成功した直後に、イベント ゲートウェイに対してそのホスト名を宣言します。この接続が確立されるたびに、イベント ゲートウェイは、DeviceID 値を Cisco IOS ホスト名に組み合わせます。イベント ゲートウェイは、スイッチに接続している間、この DeviceID 値をキャッシュに格納します。

ホスト名と DeviceID

DeviceID は、イベント ゲートウェイへの接続時に固定され、スイッチのホスト名が再設定されても変更されません。

スイッチ上でスイッチのホスト名を変更するときに、DeviceID を更新するには、スイッチとイベント ゲートウェイ間の接続を切断するのが唯一の方法になります。**no cns event** グローバル コンフィギュレーション コマンドのあとに **cns event** グローバル コンフィギュレーション コマンドを入力します。

接続が再確立されると、スイッチは変更したホスト名をイベント ゲートウェイに送信します。イベント ゲートウェイは DeviceID を新しい値に再定義します。

注意　Configuration Engine ユーザ インターフェイスを使用している場合は、最初に DeviceID フィールドを、スイッチで **cns config initial** グローバル コンフィギュレーション コマンドを使用する*前*ではなく*あと*に取得したホスト名の値に設定する必要があります。このように設定しない場合、以降の **cns config partial** グローバル コンフィギュレーション コマンドは正しく機能しません。

ホスト名、DeviceID、および ConfigID の使用

スタンドアロン モードでは、スイッチにホスト名の値が設定されると、コンフィギュレーション サーバはイベントをホスト名に送信する場合、そのホスト名を DeviceID として使用します。ホスト名が設定されていない場合、イベントは装置の cn=<*value*> で送信されます。

サーバ モードでは、ホスト名は使用されません。このモードでは、バス上のイベントの送信には常に一意の DeviceID 属性が使用されます。この属性が設定されていない場合、スイッチは更新できません。

これらの属性および関連の属性（タグ値のペア）は、Configuration Engine で **Setup** を実行するときに設定されます。

（注）　Configuration Engine のセットアップ プログラムの実行については、次の URL から Configuration Engine のセットアップおよび設定ガイドを参照してください。
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/prod_installation_guides_list.html

Cisco IOS エージェントの概要

CNS イベント エージェント機能を使用すると、スイッチはイベント バスでイベントをパブリッシュおよびサブスクライブし、Cisco IOS エージェントと連携して動作できます。Cisco IOS エージェント機能は、次の機能を提供してスイッチをサポートします。

- 「初期設定」（P.5-5）
- 「差分（部分）設定」（P.5-6）
- 「同期設定」（P.5-6）

初期設定

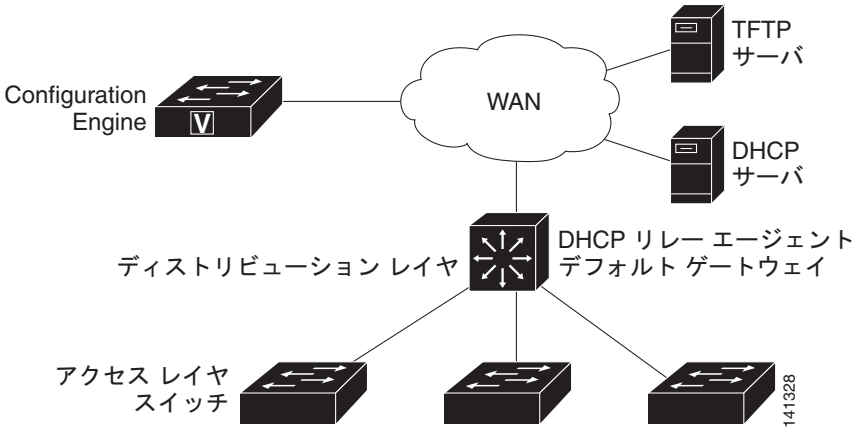
スイッチは、最初の起動時に、ネットワーク上で DHCP 要求をブロードキャストして IP アドレスを取得しようとします。サブネット上に DHCP サーバがない場合、ディストリビューション スイッチが DHCP リレー エージェントとして機能し、要求を DHCP サーバに転送します。要求を受信すると、DHCP サーバは IP アドレスを新しいスイッチに割り当てて、DHCP リレー エージェントへのユニキャスト応答に TFTP サーバの IP アドレス、ブートストラップ コンフィギュレーション ファイルへのパス、およびデフォルト ゲートウェイ IP アドレスを含めます。DHCP リレー エージェントは応答をスイッチに転送します。

スイッチは、インターフェイス VLAN 1（デフォルト）に割り当てられた IP アドレスを自動的に設定し、TFTP サーバからブートストラップ コンフィギュレーション ファイルをダウンロードします。ブートストラップ コンフィギュレーション ファイルのダウンロードに成功すると、スイッチはファイルをその実行コンフィギュレーションにロードします。

Cisco IOS エージェントは、適切な ConfigID および EventID を使用して Configuration Engine との通信を開始します。Configuration Engine は、Config ID をテンプレートにマッピングし、完全なコンフィギュレーション ファイルをスイッチにダウンロードします。

図 5-2 に、DHCP ベースの自動設定を使用して初期のブートストラップ コンフィギュレーション ファイルを取得するためのネットワーク設定の例を示します。

図 5-2　　初期設定の概要



差分（部分）設定

ネットワークの実行後に、Cisco IOS エージェントを使用して新しいサービスを追加できます。差分（部分）設定はスイッチに送信できます。実際の設定は、イベント ゲートウェイを使用してイベント ペイロードとして送信するか（プッシュ操作）、スイッチにプル操作を開始するための信号イベントとして送信できます。

スイッチでは、設定を適用する前に設定の構文をチェックできます。構文が正しい場合、スイッチは差分設定を適用し、コンフィギュレーション サーバに成功を伝えるイベントをパブリッシュします。スイッチで差分設定が適用されない場合は、エラー ステータスを示すイベントがパブリッシュされます。スイッチでは、差分設定を適用した場合、NVRAM にその設定を書き込むか、書き込むように通知されるまで待機できます。

同期設定

スイッチは、設定を受信すると、書き込み信号イベントの受信時に設定の適用を遅らせることができます。書き込み信号イベントは、スイッチに対して更新された設定をその NVRAM に保存しないように指示します。スイッチは更新された設定を、その実行コンフィギュレーションとして使用します。これにより、スイッチの設定は他のネットワーク アクティビティと同期されてから NVRAM に保存され、次の再起動時に使用できます。

Cisco IOS エージェントの設定

スイッチ Cisco IOS ソフトウェアに組み込まれた Cisco IOS エージェントを使用すると、スイッチに接続されて、「自動 CNS 設定のイネーブル化」（P.5-6）で説明しているように自動的に設定されます。設定を変更する場合やカスタムの設定をインストールする場合は、次の項を参照してください。

- 「CNS イベント エージェントのイネーブル化」（P.5-7）
- 「Cisco IOS CNS エージェントのイネーブル化」（P.5-9）

自動 CNS 設定のイネーブル化

スイッチの自動 CNS 設定をイネーブルにするには、最初に表 5-1 の前提条件を満たす必要があります。これらの条件を満たしたら、スイッチの電源を入れます。**setup** プロンプトでは何も実行しないでください。スイッチは、「初期設定」（P.5-5）で説明している初期設定を開始します。スイッチに完全なコンフィギュレーション ファイルをロードする場合は、他に何もする必要はありません。

表 5-1　自動設定をイネーブル化するための前提条件

装置	必要な設定
アクセス スイッチ	出荷時のデフォルト（コンフィギュレーション ファイルなし）。
ディストリビューション スイッチ	• IP ヘルパー アドレス。 • DHCP リレー エージェントのイネーブル化。 • IP ルーティング（デフォルト ゲートウェイとして使用されている場合）。

表 5-1　自動設定をイネーブル化するための前提条件 （続き）

装置	必要な設定
DHCP サーバ	• IP アドレスの割り当て。 • TFTP サーバの IP アドレス。 • TFTP サーバ上のブートストラップ コンフィギュレーション ファイルへのパス。 • デフォルト ゲートウェイ IP アドレス。
TFTP サーバ	• スイッチと Configuration Engine との通信をイネーブルにするための CNS コンフィギュレーション コマンドを含むブートストラップ コンフィギュレーション ファイル。 • ConfigID と EventID を生成するためのスイッチの MAC アドレスまたはシリアル番号（デフォルトのホスト名の代わり）のいずれかを使用するように設定されたスイッチ。 • コンフィギュレーション ファイルをスイッチにプッシュするように設定されている CNS イベント エージェント。
CNS Configuration Engine	装置のタイプごとに 1 つまたは複数のテンプレート。装置の ConfigID はテンプレートにマッピングされています。

（注）　Configuration Engine でのセットアップ プログラムの実行とテンプレートの作成の詳細については、次の URL にある『*Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux*』を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/1.5/installation_linux/guide/setup_1.html

CNS イベント エージェントのイネーブル化

（注）　CNS コンフィギュレーション エージェントを有効にする前に、スイッチで CNS イベント エージェントをイネーブルにする必要があります。

スイッチで CNS イベント エージェントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cns event** {*hostname* | *ip-address*} [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**reconnect** *time*] [**source** *ip-address*]	イベント エージェントをイネーブルにし、ゲートウェイ パラメータを入力します。 • {*hostname* | *ip-address*} に、イベント ゲートウェイのホスト名または IP アドレスのいずれかを入力します。 • （任意）*port number* に、イベント ゲートウェイのポート番号を入力します。デフォルトのポート番号は 11011 です。 • （任意）バックアップ ゲートウェイであることを示すには、**backup** を入力します（省略すると、プライマリ ゲートウェイになります）。 • （任意）**failover-time** *seconds* に、バックアップ ゲートウェイへのルートが確立されたあと、スイッチでプライマリ ゲートウェイ ルートを待機する期間を入力します。 • （任意）**keepalive** *seconds* に、スイッチでキープアライブ メッセージを送信する間隔を入力します。*retry-count* に、スイッチから送信する非応答キープアライブ メッセージの数を入力します。この数を過ぎると、接続が終了します。それぞれのデフォルト値は 0 です。 • （任意）**reconnect** *time* に、イベント ゲートウェイに再接続するまでスイッチが待機する最大時間を入力します。 • （任意）**source** *ip-address* に、この装置の送信元 IP アドレスを入力します。 **（注）** **encrypt** および **clock-timeout** *time* キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show cns event connections**	イベント エージェントに関する情報を確認します。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

CNS イベント エージェントをディセーブルにするには、**no cns event** {*ip-address* | *hostname*} グローバル コンフィギュレーション コマンドを使用します。

次に、CNS イベント エージェントをイネーブルにし、IP アドレス ゲートウェイを 10.180.1.27 に設定して、キープアライブの間隔を 120 秒に設定し、再試行回数を 10 に設定する例を示します。

```
Switch(config)# cns event 10.180.1.27 keepalive 120 10
```

Cisco IOS CNS エージェントのイネーブル化

CNS イベント エージェントをイネーブルにしたあと、スイッチで Cisco IOS CNS エージェントを起動します。Cisco IOS エージェントをイネーブルにするには、次のコマンドを使用します。

- **cns config initial** グローバル コンフィギュレーション コマンドを使用して、Cisco IOS エージェントをイネーブルにし、スイッチで初期設定を開始します。
- **cns config partial** グローバル コンフィギュレーション コマンドを使用して、Cisco IOS エージェントをイネーブルにし、スイッチで部分設定を開始します。Configuration Engine を使用して、差分設定をスイッチにリモートで送信できます。

初期設定のイネーブル化

CNS コンフィギュレーション エージェントをイネーブルにしてスイッチで初期設定を開始するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cns template connect** *name*	CNS テンプレート接続コンフィギュレーション モードを開始し、CNS 接続テンプレートの名前を指定します。
ステップ 3	**cli** *config-text*	CNS 接続テンプレートのコマンドラインを入力します。テンプレートのコマンドラインごとにこのステップを繰り返します。
ステップ 4		別の CNS 接続テンプレートを設定するには、ステップ 2 ～ 3 を繰り返します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**cns connect** *name* [**retries** *number*] [**retry-interval** *seconds*] [**sleep** *seconds*] [**timeout** *seconds*]	CNS 接続コンフィギュレーション モードを開始し、CNS 接続プロファイルの名前を指定して、プロファイル パラメータを定義します。スイッチでは CNS 接続プロファイルを使用して Configuration Engine に接続します。 • CNS 接続プロファイルの名前を入力します。 •（任意）**retries** *number* に、接続の再試行回数を入力します。指定できる範囲は 1 ～ 30 です。デフォルト値は 3 です。 •（任意）**retry-interval** *seconds* に、Configuration Engine へ連続して接続を試行する間隔を入力します。指定できる範囲は 1 ～ 40 秒です。デフォルト値は 10 秒です。 •（任意）**sleep** *seconds* に、最初の接続試行が行われるまでの時間を入力します。指定できる範囲は 0 ～ 250 秒です。デフォルト値は 0 です。 •（任意）**timeout** *seconds* に、接続試行が終了するまで時間を入力します。指定できる範囲は *10* ～ 2000 秒です。デフォルト値は 120 です。

	コマンド	目的
ステップ 7	**discover** {**controller** *controller-type* | **dlci** [**subinterface** *subinterface-number*] | **interface** [*interface-type*] | **line** *line-type*}	CNS 接続プロファイルのインターフェイス パラメータを指定します。 • **controller** *controller-type* に、コントローラ タイプを入力します。 • **dlci** に、アクティブな Data-Link Connection Identifier（DLCI; データリンク接続識別子）を入力します。 （任意）**subinterface** *subinterface-number* に、アクティブな DLCI を検索するために使用されるポイントツーポイント サブインターフェイス番号を指定します。 • **interface** [*interface-type*] に、インターフェイス タイプを入力します。 • **line** *line-type* に、回線タイプを入力します。
ステップ 8	**template** *name* [... *name*]	スイッチ設定に適用する CNS 接続プロファイル内の CNS 接続テンプレートのリストを指定します。複数のテンプレートを指定できます。
ステップ 9		追加のインターフェイス パラメータおよび CNS 接続プロファイルの CNS 接続テンプレートを指定する場合は、ステップ 7 ～ 8 を繰り返します。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**hostname** *name*	スイッチのホスト名を入力します。
ステップ 12	**ip route** *network-number*	（任意）IP アドレスが *network-number* の Configuration Engine へのスタティック ルートを確立します。

	コマンド	目的
ステップ 13	**cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] または **cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**]	（任意）Configuration Engine で使用される一意の EventID または ConfigID を設定します。 • *interface num* に、インターフェイス タイプ（ethernet、group-async、loopback、virtual-template など）を入力します。この設定では、一意の ID を定義するための IP または MAC アドレスの取得元インターフェイスを指定します。 • {**dns-reverse** | **ipaddress** | **mac-address**} には、ホスト名を取得してそれを一意の ID として割り当てる場合は **dns-reverse** を入力します。IP アドレスを使用する場合は **ipaddress** を、MAC アドレスを一意の ID として使用する場合は **mac-address** を入力します。 • （任意）スイッチの識別に使用する event-id 値となる ID を設定するには、**event** を入力します。 • （任意）スイッチの識別に使用する image-id 値となる ID を設定するには、**image** を入力します。 （注）　**event** および **image** の両方のキーワードを省略すると、image-id 値がスイッチの識別に使用されます。 • {**hardware-serial** | **hostname**| **string** *string* | **udi**} には、スイッチのシリアル番号を一意の ID として設定する場合は **hardware-serial** を入力し、スイッチのホスト名を一意の ID として選択する場合は **hostname**（デフォルト）を入力します。テキスト ストリングを一意の ID として使用する場合は **string** *string* に任意のテキスト ストリングを入力し、Unique Device Identifier（UDI）を一意の ID として設定する場合は **udi** を入力します。

	コマンド	目的
ステップ 14	**cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**]	Cisco IOS エージェントをイネーブルにし、初期設定を開始します。 • {*hostname* | *ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port-number* に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • （任意）設定の完了時に設定の成功、失敗、または警告のメッセージを示すには、**event** をイネーブルにします。 • （任意）**cns config initial** グローバル コンフィギュレーション コマンドを入力した結果プルされた設定の NVRAM への自動書き込みを無効にするには、**no-persist** をイネーブルにします。**no-persist** キーワードが入力されていない場合に **cns config initial** コマンドを使用すると、結果の設定が自動的に NVRAM に書き込まれます。 • （任意）**page** *page* には、初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。 • （任意）送信元 IP アドレスに使用する場合は、**source** *ip-address* を入力します。 • （任意）このパラメータの入力時に構文をチェックする場合は、**syntax-check** をイネーブルにします。 **（注）** **encrypt**、**status** *url*、および **inventory** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 15	**end**	特権 EXEC モードに戻ります。
ステップ 16	**show cns config connections**	コンフィギュレーション エージェントに関する情報を確認します。
ステップ 17	**show running-config**	設定を確認します。

CNS Cisco IOS エージェントをディセーブルにするには、**no cns config initial** {*ip-address* | *hostname*} グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチの設定が不明の場合にリモート スイッチで初期設定を設定する例（CNS ゼロタッチ機能）を示します。

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist
```

次に、スイッチの IP アドレスが認識されるときに、リモート スイッチで初期設定を設定する例を示します。Configuration Engine の IP アドレスは 172.28.129.22 です。

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1
RemoteSwitch(config)# cns id ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 172.28.129.22 no-persist
```

部分設定のイネーブル化

Cisco IOS エージェントをイネーブルにしてスイッチで部分設定を開始するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source** *ip-address*]	コンフィギュレーション エージェントをイネーブルにし、部分設定を開始します。 • {*ip-address* | *hostname*} に、コンフィギュレーション サーバの IP アドレスまたはホスト名を入力します。 • （任意）*port-number* に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • （任意）送信元 IP アドレスを使用する場合は、**source** *ip-address* を入力します。 **（注）** **encrypt** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show cns config stats** または **show cns config outstanding**	コンフィギュレーション エージェントに関する情報を確認します。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

CNS Cisco IOS エージェントをディセーブルにするには、**no cns config partial** {*ip-address* | *hostname*} グローバル コンフィギュレーション コマンドを使用します。部分設定をキャンセルするには、**cns config cancel** 特権 EXEC コマンドを使用します。

CNS 設定の表示

表 5-2　特権 EXEC show コマンド

コマンド	目的
show cns config connections	CNS Cisco IOS エージェント接続のステータスを表示します。
show cns config outstanding	開始されているが、まだ完了していない差分（部分）CNS 設定に関する情報を表示します。
show cns config stats	Cisco IOS エージェントに関する統計情報を表示します。
show cns event connections	CNS イベント エージェント接続のステータスを表示します。
show cns event stats	CNS イベント エージェントに関する統計情報を表示します。
show cns event subject	アプリケーションでサブスクライブされているイベント エージェント サブジェクトのリストを表示します。

CHAPTER 6

スイッチのクラスタ化

この章では、IE 3000 スイッチ クラスタの作成と管理に関する概念と手順について説明します。スイッチ クラスタの作成と管理には、Cisco Network Assistant（以後、Network Assistant と表記）、CLI（コマンドライン インターフェイス）、または SNMP を使用できます。詳細な手順については、オンライン ヘルプを参照してください。CLI クラスタ コマンドについては、スイッチのコマンド リファレンスを参照してください。

（注） Network Assistant ではスイッチ クラスタがサポートされていますが、スイッチをクラスタ化するよりも、グループ化してコミュニティにすることを推奨します。Network Assistant にはクラスタ変換ウィザードが用意されており、クラスタをコミュニティに変換できます。スイッチ クラスタの管理とコミュニティへの変換に関する基本的な情報など、Network Assistant の詳細については、Cisco.com の『*Getting Started with Cisco Network Assistant*』を参照してください。

この章では、IE 3000 スイッチ クラスタを中心に説明します。他のクラスタ対応 Catalyst スイッチが混在したクラスタにおける注意事項や制限事項も含まれますが、これらのスイッチについてのクラスタ機能の詳細は含まれません。特定の Catalyst プラットフォームに関するクラスタの詳細については、そのスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

この章で説明する内容は、次のとおりです。

（注） **ip http access-class** グローバル コンフィギュレーション コマンドを使用して特定のホストやネットワークへのアクセスを制限することは推奨しません。アクセスを制御するには、クラスタ コマンド スイッチを使用するか、IP アドレスが設定されているインターフェイスに Access Control List（ACL; アクセス制御リスト）を適用してください。ACL の詳細については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。

スイッチ クラスタの概要

*スイッチ クラスタ*は、クラスタ対応 Catalyst スイッチのセットです。スイッチは最大 16 台接続され、単一エンティティとして管理されます。クラスタ内のスイッチでスイッチ クラスタリング テクノロジーを使用することによって、単一の IP アドレスを介して、異なる Catalyst デスクトップ スイッチ プラットフォームのグループを設定およびトラブルシューティングできます。

スイッチ クラスタでは、1 台のスイッチを*クラスタ コマンド スイッチ*として指定する必要があります。さらに最大 15 台のスイッチを*クラスタ メンバー スイッチ*として指定できます。1 つのクラスタに含めることができるスイッチは、合計 16 台までです。クラスタ コマンド スイッチは、クラスタ メンバー スイッチの設定、管理、およびモニタに使用する単一アクセス ポイントです。クラスタ メンバーが属することができるクラスタは、一度に 1 つだけです。

スイッチのクラスタ化には、次のような利点があります。

- 相互接続メディアや物理的な場所に左右されずにスイッチを管理できます。スイッチは、同じ場所に設置することも、レイヤ 2 またはレイヤ 3（クラスタ内のレイヤ 2 スイッチどうしの間に Catalyst 3550、Catalyst 3560、または Catalyst 3750 スイッチをレイヤ 3 ルータとして使用している場合）ネットワークに分散して設置することもできます。

  クラスタ メンバーは、「クラスタ候補とクラスタ メンバーの自動検出」（P.6-5）で説明する接続上の注意事項に従って、クラスタ コマンド スイッチに接続します。ここでは、Catalyst 1900、Catalyst 2820、Catalyst 2900 XL、Catalyst 2950、Catalyst 3500 XL の各スイッチに関する管理 VLAN の考慮事項について説明します。スイッチ クラスタ環境におけるこれらのスイッチの詳細については、それぞれのスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

- クラスタ コマンド スイッチの障害発生時に、コマンド スイッチの冗長性が得られます。1 つまたは複数のスイッチを*スタンバイ クラスタ コマンド スイッチ*として指定すると、クラスタ メンバーとの接続を維持できます。*クラスタ スタンバイ グループ*は、スタンバイ クラスタ コマンド スイッチのグループです。

- さまざまなスイッチを、1 つの IP アドレスで管理できます。特に IP アドレス数が限られている場合、IP アドレスの節約に役立ちます。スイッチ クラスタとのすべての通信に、クラスタ コマンド スイッチの IP アドレスが使用されます。

表 6-1 に、スイッチ クラスタリングに対応するスイッチの一覧を示します。必要なソフトウェア バージョンのほか、クラスタ コマンド スイッチとして使用できるのかクラスタ メンバー スイッチとしてだけ使用できるのかも示します。

表 6-1　スイッチ ソフトウェアとクラスタ機能

スイッチ	Cisco IOS リリース	クラスタ機能
IE 3000 スイッチ	12.2(40)EX 以降	メンバーまたはコマンド スイッチ
Catalyst 3750-X または Catalyst 3560-X	12.2(53)SE2 以降	メンバーまたはコマンド スイッチ
Catalyst 3750-E または Catalyst 3560-E	12.2(35)SE2 以降	メンバーまたはコマンド スイッチ
Catalyst 3750	12.1(11)AX 以降	メンバーまたはコマンド スイッチ
Catalyst 3560	12.1(19)EA1b 以降	メンバーまたはコマンド スイッチ
Catalyst 3550	12.1(4)EA1 以降	メンバーまたはコマンド スイッチ
Catalyst 2975	12.2(46)EX 以降	メンバーまたはコマンド スイッチ
Catalyst 2970	12.1(11)AX 以降	メンバーまたはコマンド スイッチ
Catalyst 2960-S	12.2(53)SE 以降	メンバーまたはコマンド スイッチ

表 6-1　スイッチ ソフトウェアとクラスタ機能 （続き）

スイッチ	Cisco IOS リリース	クラスタ機能
Catalyst 2960	12.2(25)FX 以降	メンバーまたはコマンド スイッチ
Catalyst 2955	12.1(12c)EA1 以降	メンバーまたはコマンド スイッチ
Catalyst 2950	12.0(5.2)WC(1) 以降	メンバーまたはコマンド スイッチ
Catalyst 2950LRE	12.1(11)JY 以降	メンバーまたはコマンド スイッチ
Catalyst 2940	12.1(13)AY 以降	メンバーまたはコマンド スイッチ
Catalyst 3500XL	12.0(5.1)XU 以降	メンバーまたはコマンド スイッチ
Catalyst 2900 XL（8MB スイッチ）	12.0(5.1)XU 以降	メンバーまたはコマンド スイッチ
Catalyst 2900 XL（4MB スイッチ）	11.2(8.5)SA6（推奨）	メンバー スイッチのみ
Catalyst 1900 および Catalyst 2820	9.00（-A または -EN）以降	メンバー スイッチのみ

クラスタ コマンド スイッチの特性

クラスタ コマンド スイッチは次の要件を満たす必要があります。

- Cisco IOS Release 12.2(40)EX 以降が実行されていること。
- IP アドレスが割り当てられていること。
- Cisco Discovery Protocol（CDP; シスコ検出プロトコル）バージョン 2 がイネーブル（デフォルト）になっていること。
- 他のクラスタのコマンド スイッチまたはクラスタ メンバー スイッチでないこと。
- 管理 VLAN 経由でスタンバイ クラスタ コマンド スイッチに、共通の VLAN 経由でクラスタ メンバー スイッチに、それぞれ接続されていること。

スタンバイ クラスタ コマンド スイッチの特性

スタンバイ クラスタ コマンド スイッチは次の要件を満たす必要があります。

- Cisco IOS 12.2(40)EX 以降が実行されていること。
- IP アドレスが割り当てられていること。
- CDP バージョン 2 がイネーブルになっていること。
- コマンド スイッチおよび他のスタンバイ コマンド スイッチに管理 VLAN 経由で接続されていること。
- 他のすべてのクラスタ メンバー スイッチ（クラスタ コマンド スイッチおよびスタンバイ コマンド スイッチを除く）に共通の VLAN 経由で接続されていること。
- クラスタ メンバー スイッチとの接続が維持されるように、クラスタに冗長接続されていること。
- 他のクラスタのコマンド スイッチまたはメンバー スイッチでないこと。

IE 3000 候補スイッチおよびクラスタ メンバー スイッチの特性

IE 3000 *候補スイッチ*とは、クラスタにまだ追加されていないクラスタ対応スイッチのことです。クラスタ メンバー スイッチは、スイッチ クラスタに実際に追加されているスイッチです。必須ではありませんが、候補スイッチまたはクラスタ メンバー スイッチに、固有の IP アドレスとパスワードを割り当てることもできます（考慮事項については、「IP アドレス」（P.6-13）および「パスワード」（P.6-14）を参照してください）。

候補スイッチをクラスタに追加するには、そのスイッチが次の要件を満たす必要があります。

- クラスタ対応ソフトウェアが実行されていること。
- CDP バージョン 2 がイネーブルになっていること。
- 他のクラスタのコマンド スイッチまたはクラスタ メンバー スイッチでないこと。
- クラスタ スタンバイ グループが存在する場合は、1 つ以上の共通の VLAN 経由ですべてのスタンバイ クラスタ コマンド スイッチに接続されていること。各スタンバイ クラスタ コマンド スイッチへの VLAN は異なっていてもかまいません。
- 1 つ以上の共通の VLAN 経由でクラスタ コマンド スイッチに接続されていること。

（注） Catalyst 1900、Catalyst 2820、Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL 候補スイッチとクラスタ メンバー スイッチは、管理 VLAN 経由でクラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチに接続されている必要があります。スイッチ クラスタ環境におけるこれらのスイッチの詳細については、それぞれのスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 クラスタ コマンド スイッチには、この要件は適用されません。候補スイッチおよびクラスタ メンバー スイッチは、任意の共通の VLAN 経由でクラスタ コマンド スイッチに接続できます。

スイッチ クラスタのプランニング

クラスタを使用して複数のスイッチを管理する場合は、競合と互換性の問題について予測しておくことが重要です。ここでは、クラスタの作成前に理解しておくべき注意事項、要件、および危険について説明します。

- 「クラスタ候補とクラスタ メンバーの自動検出」（P.6-5）
- 「HSRP とスタンバイ クラスタ コマンド スイッチ」（P.6-10）
- 「IP アドレス」（P.6-13）
- 「ホスト名」（P.6-13）
- 「パスワード」（P.6-14）
- 「SNMP コミュニティ ストリング」（P.6-14）
- 「TACACS+ と RADIUS」（P.6-14）
- 「LRE プロファイル」（P.6-15）

スイッチ クラスタリングに対応する Catalyst スイッチの一覧、クラスタ コマンド スイッチとして使用できるスイッチとクラスタ メンバー スイッチとしてだけ使用できるスイッチ、ソフトウェア バージョン、ブラウザ、および Java プラグイン設定の要件については、リリース ノートを参照してください。

クラスタ候補とクラスタ メンバーの自動検出

クラスタ コマンド スイッチはシスコ検出プロトコル（CDP）を使用して、スター型またはカスケード型のトポロジを持つ複数の VLAN から、クラスタ メンバー スイッチ、候補スイッチ、ネイバー スイッチ クラスタ、およびエッジ装置を検出します。

（注）　クラスタ コマンド スイッチ、クラスタ メンバー、およびクラスタ コマンド スイッチに検出させるクラスタ対応スイッチでは、CDP をディセーブルにしないでください。CDP の詳細については、第 32 章「CDP の設定」を参照してください。

次に示す接続上の注意事項に従うことにより、スイッチ クラスタ、クラスタ候補、接続されたスイッチ クラスタ、およびネイバー エッジ装置が、確実に自動検出されます。

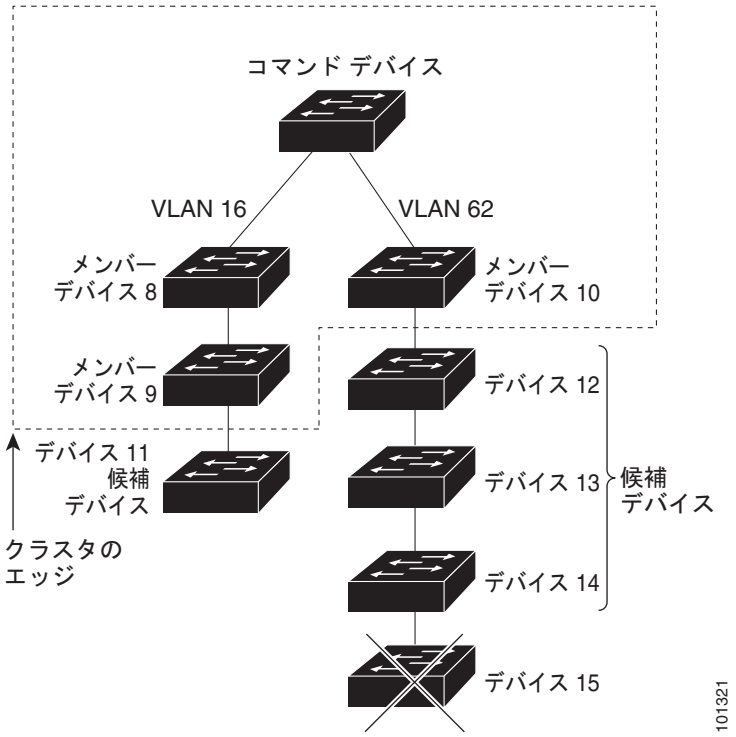
- 「CDP ホップ経由の検出」（P.6-5）
- 「CDP 非対応装置およびクラスタ非対応装置経由の検出」（P.6-6）
- 「異なる VLAN 経由の検出」（P.6-7）
- 「異なる管理 VLAN 経由の検出」（P.6-7）
- 「ルーテッド ポート経由の検出」（P.6-8）
- 「新しく設置されたスイッチの検出」（P.6-9）

CDP ホップ経由の検出

クラスタ コマンド スイッチは、CDP を使用することによって、クラスタのエッジから最大 7 CDP ホップ先にあるスイッチを検出できます（デフォルトは 3 ホップ先まで）。クラスタのエッジとは、最後のクラスタ メンバー スイッチがクラスタおよび候補スイッチに接続している部分を指します。たとえば、図 6-1 のクラスタ メンバー スイッチ 9 と 10 はクラスタのエッジに位置しています。

図 6-1 では、クラスタ コマンド スイッチのポートに VLAN 16 と 62 が割り当てられています。CDP ホップ カウントは 3 です。クラスタ コマンド スイッチは、クラスタのエッジから 3 ホップ以内にある 11、12、13、および 14 のスイッチを検出します。スイッチ 15 は、クラスタのエッジから 4 ホップ先にあるため、検出されません。

図 6-1　CDP ホップ経由の検出

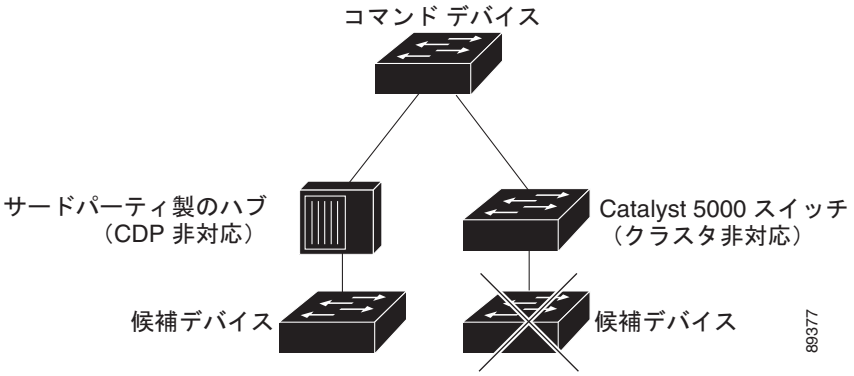


CDP 非対応装置およびクラスタ非対応装置経由の検出

クラスタ コマンド スイッチを *CDP 非対応のサードパーティ製ハブ*（他社製のハブなど）に接続している場合、そのサードパーティ製ハブに接続されたクラスタ対応装置は検出することができます。ただし、クラスタ コマンド スイッチを*クラスタ非対応のシスコ デバイス*に接続している場合は、クラスタ非対応のシスコ デバイスの先に接続されたクラスタ対応装置を検出できません。

図 6-2 に、サードパーティ製ハブに接続されているスイッチをクラスタ コマンド スイッチが検出する様子を示します。ただし、クラスタ コマンド スイッチは、Catalyst 5000 スイッチに接続されているスイッチは検出しません。

図 6-2　CDP 非対応装置およびクラスタ非対応装置経由の検出

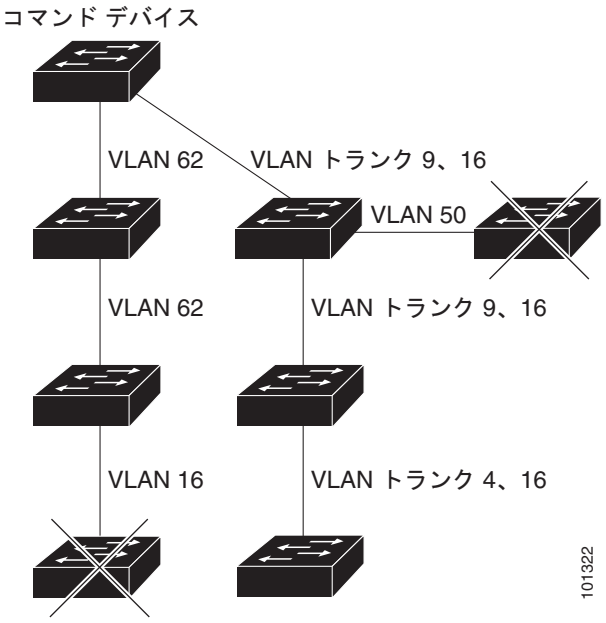


異なる VLAN 経由の検出

クラスタ コマンド スイッチが Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 スイッチの場合、異なる VLAN 内のクラスタ メンバー スイッチをクラスタに含めることができます。それらのクラスタ メンバー スイッチは、1 つ以上の共通の VLAN 経由でクラスタ コマンド スイッチに接続されている必要があります。図 6-3 のクラスタ コマンド スイッチは、ポートに VLAN 9、16、および 62 が割り当てられているため、これらの VLAN 内のスイッチを検出します。VLAN 50 内のスイッチは検出しません。最初の列の VLAN 16 内のスイッチも、クラスタ コマンド スイッチと VLAN 接続されていないため、検出しません。

Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL クラスタ メンバー スイッチは、管理 VLAN 経由でクラスタ コマンド スイッチに接続されている必要があります。管理 VLAN 経由の検出については、「異なる管理 VLAN 経由の検出」（P.6-7）を参照してください。VLAN の詳細については、第 16 章「VLAN の設定」を参照してください。

図 6-3　　異なる VLAN 経由の検出



異なる管理 VLAN 経由の検出

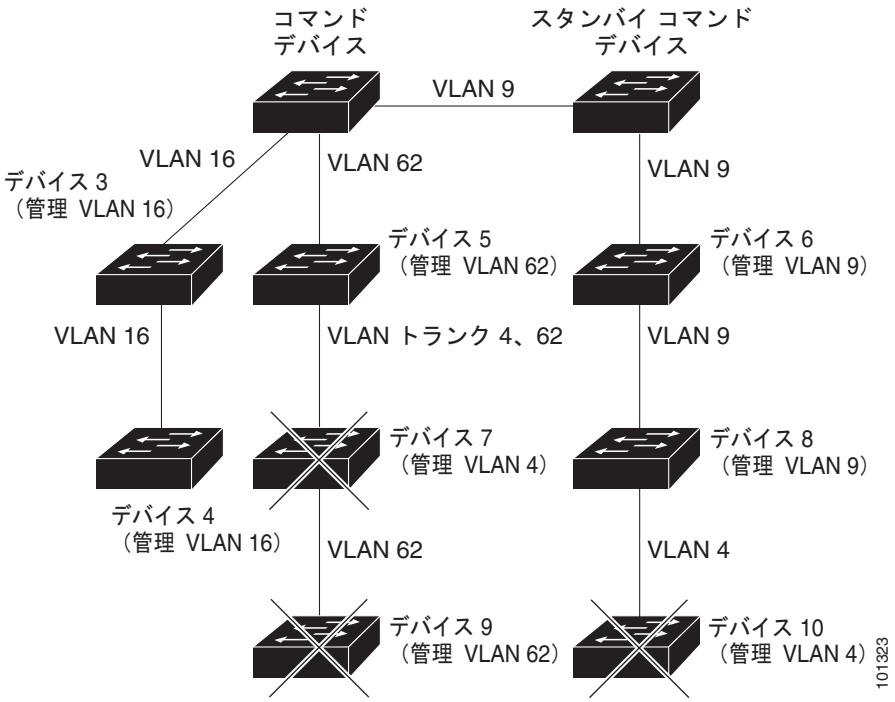
Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 クラスタ コマンド スイッチは、異なる VLAN 内や異なる管理 VLAN 内のクラスタ メンバー スイッチを検出および管理できます。それらのクラスタ メンバー スイッチは、1 つ以上の共通の VLAN 経由でクラスタ コマンド スイッチに接続されている必要があります。管理 VLAN 経由でクラスタ コマンド スイッチに接続されている必要はありません。デフォルトの管理 VLAN は VLAN 1 です。

（注） Catalyst 3750 スイッチ、Catalyst 2975 スイッチ、またはスイッチ スタックがスイッチ クラスタに含まれている場合は、そのスイッチまたはスイッチ スタックをクラスタ コマンド スイッチにする必要があります。

図 6-4 のクラスタ コマンド スイッチおよびスタンバイ コマンド スイッチ（Catalyst 2960、Catalyst 2970、Catalyst 2975、Catalyst 3550、Catalyst 3560、または Catalyst 3750 クラスタ コマンド スイッチの場合）は、VLAN 9、16、および 62 にポートを割り当てています。クラスタ コマンド スイッチの管理 VLAN は VLAN 9 です。各クラスタ コマンド スイッチは、次の例外を除き、異なる管理 VLAN 内のスイッチを検出します。

- スイッチ 7 および 10（管理 VLAN 4 内のスイッチ）。共通の VLAN（つまり VLAN 62 および 9）経由でクラスタ コマンド スイッチに接続されていないため。
- スイッチ 9。非候補装置（スイッチ 7）を経由すると自動検出が機能しないため。

図 6-4　レイヤ 3 クラスタ コマンド スイッチによる異なる管理 VLAN 経由の検出

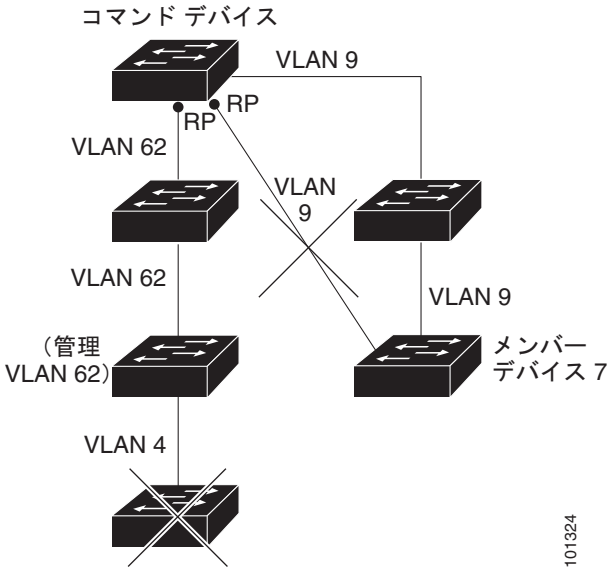


ルーテッド ポート経由の検出

クラスタ コマンド スイッチに Routed Port（RP; ルーテッド ポート）が設定されている場合は、ルーテッド ポートと*同じ* VLAN 内の候補スイッチおよびクラスタ メンバー スイッチだけを検出します。ルーテッド ポートの詳細については、「ルーテッド ポート」（P.14-4）を参照してください。

図 6-5 のレイヤ 3 クラスタ コマンド スイッチは、VLAN 9 および 62 内のスイッチは検出できますが、VLAN 4 内のスイッチは検出できません。クラスタ コマンド スイッチとクラスタ メンバー スイッチ 7 の間のルーテッド ポート パスが失われても、VLAN 9 経由の冗長パスがあるため、クラスタ メンバー スイッチ 7 との接続は維持されます。

図 6-5　ルーテッド ポート経由の検出



新しく設置されたスイッチの検出

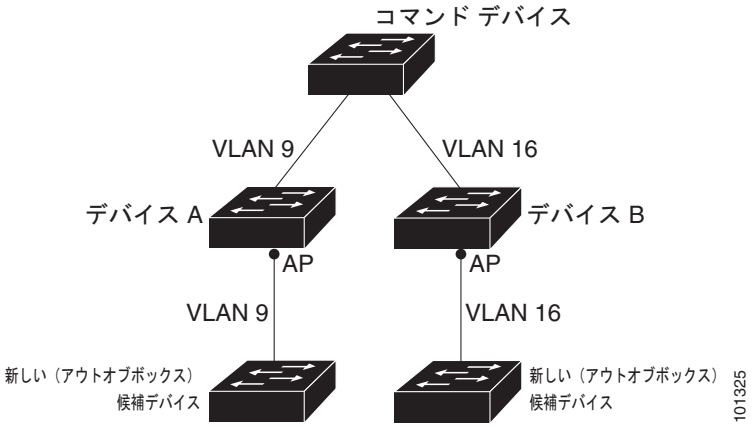
新しいスイッチをクラスタに追加するには、スイッチがいずれかのアクセス ポート経由でクラスタに接続されている必要があります。1 つのアクセス ポート（AP）は、1 つの VLAN にだけ属し、そのトラフィックを伝送します。デフォルトでは、新しいスイッチとそのアクセス ポートは、VLAN 1 に割り当てられます。

新しいスイッチをクラスタに追加すると、そのデフォルト VLAN が、直近のアップストリーム側ネイバーの VLAN に変更されます。また、新しいスイッチのアクセス ポートが、直近のアップストリーム側ネイバーの VLAN に属するように設定されます。

図 6-6 のクラスタ コマンド スイッチは VLAN 9 および 16 に属しています。新しいクラスタ対応スイッチをクラスタに追加すると、次のようになります。

- 1 台のクラスタ対応スイッチとそのアクセス ポートが VLAN 9 に割り当てられます。
- もう 1 台のクラスタ対応スイッチとそのアクセス ポートが管理 VLAN 16 に割り当てられます。

図 6-6　新しく設置されたスイッチの検出



HSRP とスタンバイ クラスタ コマンド スイッチ

スイッチは Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）をサポートしているため、スタンバイ クラスタ コマンド スイッチのグループを設定できます。クラスタ コマンド スイッチは、すべてのクラスタ メンバー スイッチへの通信情報および設定情報の転送を管理しているため、次のことを強く推奨します。

- クラスタ コマンド スイッチ スタックには、スイッチ スタック全体に障害が発生した場合に備えて、スタンバイ クラスタ コマンド スイッチが必要です。ただし、コマンド スイッチ スタックのスタック マスターだけに障害が発生した場合は、スイッチ スタックは新しいスタック マスターを選択し、クラスタ コマンド スイッチ スタックとしての役割を再開します。
- クラスタ コマンド スイッチがスタンドアロンのスイッチである場合は、プライマリ クラスタ コマンド スイッチに障害が発生した際に役割を引き継ぐ、スタンバイ クラスタ コマンド スイッチを設定します。

*クラスタ スタンバイ グループ*とは、「スタンバイ クラスタ コマンド スイッチの特性」（P.6-3）に記載されている要件を満たすコマンド対応スイッチのグループです。1 つのクラスタに割り当てることができるクラスタ スタンバイ グループは 1 つだけです。

（注）　クラスタ スタンバイ グループは HSRP グループです。HSRP をディセーブルにすると、クラスタ スタンバイ グループもディセーブルになります。

クラスタ スタンバイ グループ内のスイッチは、HSRP プライオリティに従ってランク付けされます。グループ内で最高のプライオリティを持つスイッチが、*アクティブ クラスタ コマンド スイッチ*（AC）になります。次に高いプライオリティを持つスイッチが、*スタンバイ クラスタ コマンド スイッチ*（SC）になります。クラスタ スタンバイ グループ内の他のスイッチは、*パッシブ クラスタ コマンド スイッチ*（PC）です。アクティブ クラスタ コマンド スイッチとスタンバイ クラスタ コマンド スイッチが*同時に*ディセーブルになった場合、最高のプライオリティを持つパッシブ クラスタ コマンド スイッチがアクティブ クラスタ コマンド スイッチになります。自動検出の制限事項については、「クラスタ設定の自動回復」（P.6-12）を参照してください。HSRP プライオリティ値の変更については、「HSRP プライオリティの設定」（P.45-8）を参照してください。クラスタ スタンバイ グループのメンバーとルータ冗長構成グループのメンバーのプライオリティ変更には、同じ HSRP **standby priority** インターフェイス コンフィギュレーション コマンドを使用します。

（注）　HSRP スタンバイ ホールド タイムの間隔は、hello タイムの間隔の 3 倍以上にしてください。デフォルトの HSRP スタンバイ ホールド タイムの間隔は 10 秒です。デフォルトの HSRP スタンバイ hello タイムの間隔は 3 秒です。スタンバイ ホールド タイムおよびスタンバイ hello タイムの間隔の詳細については、「HSRP の認証およびタイマーの設定」（P.45-10）を参照してください。

次に示す接続上の注意事項に従うことにより、スイッチ クラスタ、クラスタ候補、接続されたスイッチ クラスタ、およびネイバー エッジ装置が、確実に自動検出されます。これらのトピックでは、スタンバイ クラスタ コマンド スイッチの詳細についても説明します。

- 「仮想 IP アドレス」（P.6-11）
- 「クラスタ スタンバイ グループに関するその他の考慮事項」（P.6-11）
- 「クラスタ設定の自動回復」（P.6-12）

仮想 IP アドレス

クラスタ スタンバイ グループには、一意の仮想 IP アドレス、グループ番号、およびグループ名を割り当てる必要があります。この情報は、アクティブ クラスタ コマンド スイッチの特定の VLAN またはルーテッド ポートに設定する必要があります。アクティブ クラスタ コマンド スイッチは、この仮想 IP アドレス宛てのトラフィックを受信します。クラスタを管理するには、コマンド スイッチの IP アドレスからではなく、仮想 IP アドレスからアクティブ クラスタ コマンド スイッチにアクセスする必要があります これは、アクティブ クラスタ コマンド スイッチの IP アドレスがクラスタ スタンバイ グループの仮想 IP アドレスと異なる場合があるからです。

アクティブ クラスタ コマンド スイッチに障害が発生すると、スタンバイ クラスタ コマンド スイッチが仮想 IP アドレスの所有権を引き継ぎ、アクティブ クラスタ コマンド スイッチになります。クラスタ スタンバイ グループ内のパッシブ スイッチは、それぞれに割り当てられたプライオリティを比較して、新しいスタンバイ クラスタ コマンド スイッチを決定します。最も高いプライオリティを持つパッシブ スタンバイ スイッチが、スタンバイ クラスタ コマンド スイッチになります。以前のアクティブ クラスタ コマンド スイッチが再度アクティブになると、アクティブ クラスタ コマンド スイッチとしての役割を再開し、現在のアクティブ クラスタ コマンド スイッチはスタンバイ クラスタ コマンド スイッチに戻ります。スイッチ クラスタの IP アドレスの詳細については、「IP アドレス」（P.6-13）を参照してください。

クラスタ スタンバイ グループに関するその他の考慮事項

次の要件も適用されます。

- スタンバイ クラスタ コマンド スイッチは、クラスタ コマンド スイッチと同じスイッチ タイプである必要があります。たとえば、クラスタ コマンド スイッチが IE 3000 スイッチの場合は、スタンバイ クラスタ コマンド スイッチも IE 3000 スイッチにする必要があります。他のクラスタ対応スイッチのスタンバイ クラスタ コマンド スイッチの要件については、そのスイッチのコンフィギュレーション ガイドを参照してください。

  スイッチ クラスタに IE 3000 スイッチが 1 台含まれる場合は、それをクラスタ コマンド スイッチにしてください。

- 1 つのクラスタに割り当てることができるクラスタ スタンバイ グループは 1 つだけです。ルータ冗長構成スタンバイ グループは複数設定できます。

  1 つの HSRP グループを、クラスタ スタンバイ グループおよびルータ冗長構成グループの両方として設定できます。ただし、ルータ冗長構成グループがクラスタ スタンバイ グループになると、そのグループのルータ冗長性はディセーブルになります。CLI を使用すると再度イネーブルにできます。HSRP とルータ冗長構成の詳細については、第 45 章「HSRP の設定」を参照してください。

- スタンバイ グループのすべてのメンバーは、クラスタのメンバーである必要があります。

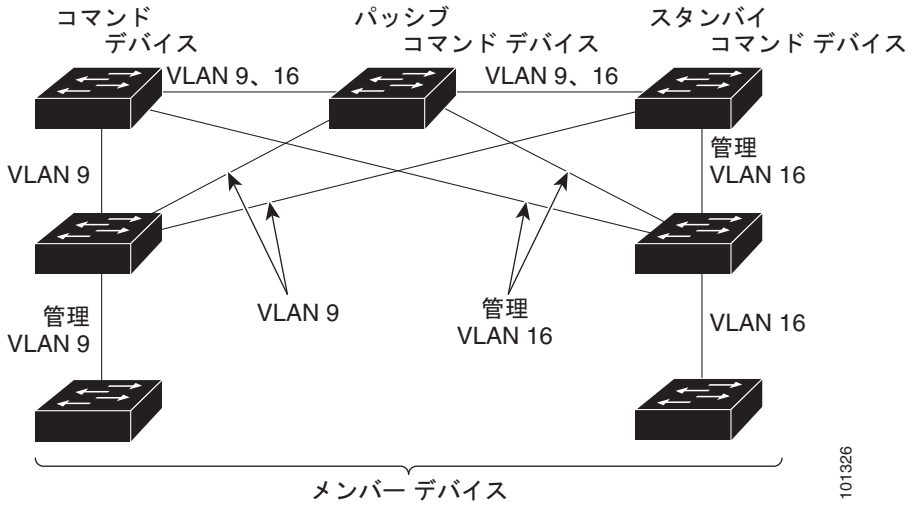
  （注）　任意の数のスイッチをスタンバイ クラスタ コマンド スイッチとして割り当てることができます。ただし、クラスタ内のスイッチの総数は 16 台以下にする必要があります。これには、アクティブ クラスタ コマンド スイッチ、スタンバイ グループ メンバー、およびクラスタ メンバー スイッチが含まれます。

- すべてのスタンバイ グループ メンバー（図 6-7）は、同じ VLAN 経由でクラスタ コマンド スイッチに接続されている必要があります。この例のクラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチは、Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 クラスタ コマンド スイッチです。また、各スタンバイ グループ メンバーは、スイッチ クラスタと共通の 1 つ以上の VLAN 経由で、互いに冗長接続されている必要があります。

Catalyst 1900、Catalyst 2820、Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL クラスタ メンバー スイッチは、管理 VLAN 経由でクラスタ スタンバイ グループに接続されている必要があります。スイッチ クラスタの VLAN の詳細については、次のセクションを参照してください。

- 「異なる VLAN 経由の検出」（P.6-7）
- 「異なる管理 VLAN 経由の検出」（P.6-7）

図 6-7　スタンバイ グループ メンバーとクラスタ メンバーの間の VLAN 接続



クラスタ設定の自動回復

アクティブ クラスタ コマンド スイッチは、クラスタの設定情報（装置の設定情報ではありません）を、スタンバイ クラスタ コマンド スイッチに絶えず転送します。そのため、アクティブ クラスタ コマンド スイッチに障害が発生しても、スタンバイ クラスタ コマンド スイッチがただちにクラスタを引き継ぐことができます。

自動検出には次の制限事項があります。

- この制限は、Catalyst 2950、Catalyst 3550、Catalyst 3560、および Catalyst 3750 のコマンド スイッチとスタンバイ クラスタ コマンド スイッチを含むクラスタにだけ適用されます。アクティブ クラスタ コマンド スイッチとスタンバイ クラスタ コマンド スイッチが*同時に*ディセーブルになった場合、最高のプライオリティを持つパッシブ クラスタ コマンド スイッチがアクティブ クラスタ コマンド スイッチになります。ただし、これはパッシブ スタンバイ クラスタ コマンド スイッチだったので、以前のクラスタ コマンド スイッチからクラスタ設定情報は転送されて*いません*。アクティブ クラスタ コマンド スイッチは、スタンバイ クラスタ コマンド スイッチに対してだけクラスタ設定情報を転送します。したがって、クラスタの再構築が必要です。
- この制限は、すべてのクラスタに適用されます。アクティブ クラスタ コマンド スイッチに障害が発生した場合、クラスタ スタンバイ グループ内にスイッチが 3 台以上あると、新しいクラスタ コマンド スイッチは、Catalyst 1900、Catalyst 2820、および Catalyst 2916M XL クラスタ メンバー スイッチを検出しません。これらのクラスタ メンバー スイッチは、クラスタに追加し直す必要があります。
- この制限は、すべてのクラスタに適用されます。アクティブ クラスタ コマンド スイッチが障害発生後に再度アクティブになった場合、そのスイッチは Catalyst 1900、Catalyst 2820、および Catalyst 2916M XL クラスタ メンバー スイッチを検出しません。これらのクラスタ メンバー スイッチを、クラスタに追加し直す必要があります。

以前のアクティブ クラスタ コマンド スイッチがその役割を再開すると、ダウン中に追加されたメンバーを含む最新のクラスタ設定情報のコピーをアクティブ クラスタ コマンド スイッチから受信します。アクティブ クラスタ コマンド スイッチは、クラスタ設定情報のコピーをクラスタ スタンバイ グループに送信します。

IP アドレス

クラスタ コマンド スイッチには IP 情報を割り当てる必要があります。クラスタ コマンド スイッチには複数の IP アドレスを割り当てることができ、コマンド スイッチのいずれの IP アドレスを使用してもクラスタにアクセスできます。クラスタ スタンバイ グループを設定する場合は、スタンバイ グループの仮想 IP アドレスを使用して、アクティブ クラスタ コマンド スイッチからクラスタを管理する必要があります。仮想 IP アドレスを使用すると、アクティブ クラスタ コマンド スイッチに障害が発生して、スタンバイ クラスタ コマンド スイッチがアクティブ クラスタ コマンド スイッチになっても、クラスタへの接続が確実に維持されます。

アクティブ クラスタ コマンド スイッチに障害が発生してスタンバイ クラスタ コマンド スイッチが役割を引き継いだ場合、クラスタにアクセスするには、スタンバイ グループの仮想 IP アドレスを使用するか、新しいアクティブ クラスタ コマンド スイッチで利用可能な IP アドレスのいずれかを使用する必要があります。

クラスタ対応スイッチには IP アドレスを割り当てることができますが、必須ではありません。クラスタ メンバー スイッチの管理、およびクラスタ メンバー スイッチ間の通信には、コマンド スイッチの IP アドレスが使用されます。固有の IP アドレスを持たないクラスタ メンバー スイッチをクラスタから削除する場合は、そのスイッチをスタンドアロン スイッチとして管理するために IP アドレスを割り当てる必要があります。

IP アドレスの詳細については、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」を参照してください。

ホスト名

クラスタ コマンド スイッチや適格なクラスタ メンバーにホスト名を割り当てる必要はありません。しかし、クラスタ コマンド スイッチにホスト名を割り当てると、スイッチ クラスタの識別に役立ちます。スイッチのデフォルトのホスト名は *Switch* です。

ホスト名を持たないスイッチをクラスタに追加するたびに、クラスタ コマンド スイッチのホスト名の後ろに一意のメンバー番号を付加した名前が、クラスタ コマンド スイッチによって順番に割り当てられます。番号は、スイッチがクラスタに追加された順序を表します。たとえば、クラスタ コマンド スイッチの名前が *eng-cluster* である場合、5 番めのクラスタ メンバーの名前は *eng-cluster-5* となります。

スイッチにホスト名が割り当てられている場合は、クラスタに追加しても、クラスタから削除しても、その名前が維持されます。

クラスタ コマンド スイッチによってホスト名が割り当てられた後、クラスタから削除されて新しいクラスタに追加されたときに、メンバー番号が同じ（*5* など）だった場合、スイッチは古いホスト名（*eng-cluster-5* など）を、新しいクラスタのクラスタ コマンド スイッチのホスト名（*mkg-cluster-5* など）で上書きします。新しいクラスタでスイッチのメンバー番号が変わる場合（*3* など）は、以前の名前（*eng-cluster-5*）が維持されます。

パスワード

クラスタ メンバーとなる個々のスイッチにパスワードを割り当てる必要はありません。クラスタに追加したスイッチは、コマンド スイッチのパスワードを継承し、クラスタから削除されてもそのパスワードを維持します。コマンド スイッチのパスワードが設定されていない場合、クラスタ メンバー スイッチはヌル パスワードを継承します。クラスタ メンバー スイッチが継承するのは、コマンド スイッチのパスワードだけです。

メンバー スイッチのパスワードをコマンド スイッチとは異なるパスワードに変更して保存した場合は、メンバー スイッチのパスワードをコマンド スイッチと同じパスワードに変更しない限り、そのスイッチはクラスタ コマンド スイッチから管理できません。メンバー スイッチを再起動しても、パスワードはコマンド スイッチのパスワードに戻りません。クラスタへの追加後は、メンバー スイッチのパスワードを変更しないことを推奨します。

パスワードの詳細については、「スイッチへの不正アクセスの防止」（P.11-1）を参照してください。

Catalyst 1900 スイッチおよび Catalyst 2820 スイッチに固有の、パスワードに関する考慮事項については、各スイッチのインストレーション ガイドおよびコンフィギュレーション ガイドを参照してください。

SNMP コミュニティ ストリング

クラスタ メンバー スイッチは、次のように、コマンド スイッチの最初の read-only（RO; 読み取り専用）コミュニティ ストリングおよび read-write（RW; 読み取りと書き込み）コミュニティ ストリングの後ろに *@esN* を付加したストリングを継承します。

- *command-switch-readonly-community-string@esN*（*N* はメンバー スイッチ番号）
- *command-switch-readwrite-community-string@esN*（*N* はメンバー スイッチ番号）

クラスタ コマンド スイッチに read-only または read-write のコミュニティ ストリングが複数ある場合、最初の read-only ストリングと read-write ストリングだけがクラスタ メンバー スイッチに使用されます。

スイッチで使用可能なコミュニティ ストリングの数と長さに制限はありません。SNMP およびコミュニティ ストリングの詳細については、第 36 章「SNMP の設定」を参照してください。

Catalyst 1900 スイッチおよび Catalyst 2820 スイッチに固有の、SNMP に関する考慮事項については、各スイッチのインストレーション ガイドおよびコンフィギュレーション ガイドを参照してください。

TACACS+ と RADIUS

Terminal Access Controller Access Control System Plus（TACACS+）をクラスタ メンバーに設定する場合は、すべてのクラスタ メンバーに設定する必要があります。同様に、RADIUS をクラスタ メンバーに設定する場合は、すべてのクラスタ メンバーに設定する必要があります。また、同じスイッチ クラスタ内に、TACACS+ を設定したメンバーと RADIUS を設定したメンバーを混在させることはできません。

TACACS+ の詳細については、「TACACS+ でのスイッチ アクセスの制御」（P.11-10）を参照してください。RADIUS の詳細については、「RADIUS でのスイッチ アクセスの制御」（P.11-17）を参照してください。

LRE プロファイル

プライベート プロファイルとパブリック プロファイルの両方を使用する Long-Reach Ethernet（LRE; 長距離イーサネット）スイッチがスイッチ クラスタ内に混在すると、設定の競合が発生します。クラスタ内の 1 台の LRE スイッチにパブリック プロファイルを割り当てる場合は、そのクラスタ内のすべての LRE スイッチに同じパブリック プロファイルを割り当てる必要があります。LRE スイッチをクラスタに追加する前に、クラスタ内の他の LRE スイッチで使用されているパブリック プロファイルを割り当ててください。

1 つのクラスタ内に、異なるプライベート プロファイルを使用する LRE スイッチを混在させることはできます。

CLI によるスイッチ クラスタの管理

最初にクラスタ コマンド スイッチにログインして、CLI からクラスタ メンバー スイッチを設定できます。**command** ユーザ EXEC コマンドとクラスタ メンバー スイッチ番号を入力して Telnet セッション（コンソールまたは Telnet 接続）を開始し、クラスタ メンバー スイッチの CLI にアクセスします。コマンド モードが変更され、Cisco IOS コマンドを通常どおり使用できるようになります。コマンド スイッチの CLI に戻るには、クラスタ メンバー スイッチで **exit** 特権 EXEC コマンドを入力します。

次に、コマンド スイッチの CLI からメンバー スイッチ 3 にログインする例を示します。

```
switch# rcommand 3
```

メンバー スイッチ番号が不明の場合は、クラスタ コマンド スイッチで **show cluster members** 特権 EXEC コマンドを入力します。**rcommand** コマンドおよびその他のクラスタ コマンドの詳細については、スイッチのコマンド リファレンスを参照してください。

Telnet セッションにより、クラスタ コマンド スイッチと同じ権限レベルでメンバー スイッチの CLI にアクセスします。Cisco IOS コマンドを通常どおり使用できるようになります。スイッチの Telnet セッションの設定手順については、「パスワード回復のディセーブル化」（P.11-5）を参照してください。

Catalyst 1900 および Catalyst 2820 の CLI に関する考慮事項

Standard Edition ソフトウェアが稼動する Catalyst 1900 および Catalyst 2820 スイッチがスイッチ クラスタに含まれている場合、クラスタ コマンド スイッチの権限レベルが 15 であれば、Telnet セッションは管理コンソール（メニュー方式インターフェイス）にアクセスします。クラスタ コマンド スイッチの権限レベルが 1 ～ 14 であれば、メニュー コンソールにアクセスするためのパスワードの入力を求められます。

コマンド スイッチの権限レベルと、Standard Edition および Enterprise Edition ソフトウェアが稼動する Catalyst 1900 および Catalyst 2820 クラスタ メンバー スイッチとの対応関係は、次のとおりです。

- コマンド スイッチの権限レベルが 1 ～ 14 である場合、クラスタ メンバー スイッチへのアクセスは権限レベル 1 で行われます。
- コマンド スイッチの権限レベルが 15 である場合、クラスタ メンバー スイッチへのアクセスは権限レベル 15 で行われます。

（注） Catalyst 1900 および Catalyst 2820 の CLI を利用できるのは、スイッチで Enterprise Edition ソフトウェアが稼動している場合に限られます。

Catalyst 1900 スイッチおよび Catalyst 2820 スイッチの詳細については、各スイッチのインストレーション ガイドおよびコンフィギュレーション ガイドを参照してください。

SNMP によるスイッチ クラスタの管理

スイッチの最初の起動時にセットアップ プログラムを使用して IP 情報を入力し、提示された設定を採用した場合、SNMP はイネーブルになります。セットアップ プログラムを使用して IP 情報を入力しておらず、SNMP がイネーブルになっていない場合は、「SNMP の設定」（P.36-6）の説明に従ってイネーブル化できます。Catalyst 1900 スイッチおよび Catalyst 2820 スイッチでは、デフォルトで SNMP がイネーブルになります。

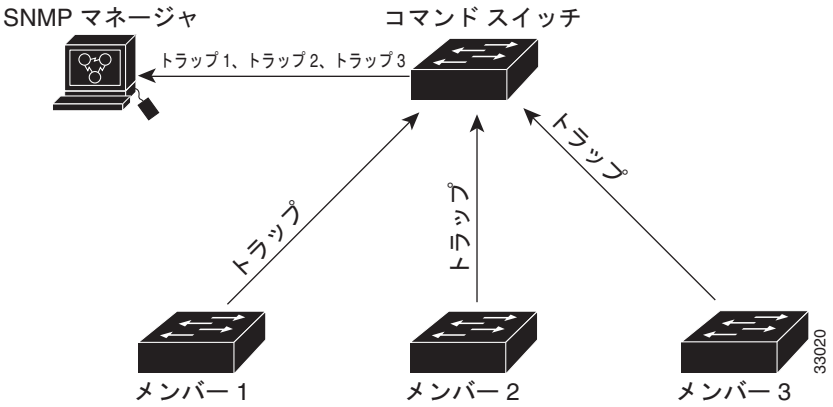
クラスタを作成すると、クラスタ コマンド スイッチが、クラスタ メンバー スイッチと SNMP アプリケーションの間のメッセージ交換を管理します。クラスタ コマンド スイッチのクラスタ ソフトウェアは、クラスタ コマンド スイッチ上で最初に設定された read-write および read-only のコミュニティ ストリングに、クラスタ メンバー スイッチ番号 *@esN*（*N* はスイッチ番号）を付加して、クラスタ メンバー スイッチに設定します。クラスタ コマンド スイッチはこのコミュニティ ストリングを使用して、SNMP 管理ステーションとクラスタ メンバー スイッチの間で、get、set、および get-next メッセージの転送を制御します。

（注）　クラスタ スタンバイ グループを設定すると、ユーザが気付かないうちにクラスタ コマンド スイッチが変更される可能性があります。クラスタにクラスタ スタンバイ グループを設定した場合は、クラスタ コマンド スイッチとの通信に、最初の read-write および read-only コミュニティ ストリングを使用してください。

クラスタ メンバー スイッチに IP アドレスがない場合、図 6-8 に示すように、クラスタ コマンド スイッチが、クラスタ メンバー スイッチからのトラップを管理ステーションにリダイレクトします。クラスタ メンバー スイッチに固有の IP アドレスとコミュニティ ストリングがある場合、クラスタ メンバー スイッチは、クラスタ コマンド スイッチを経由することなく、管理ステーションに直接トラップを送信できます。

クラスタ メンバー スイッチに固有の IP アドレスとコミュニティ ストリングがある場合、それらに加えて、クラスタ コマンド スイッチによるアクセスも利用できます。SNMP およびコミュニティ ストリングの詳細については、第 36 章「SNMP の設定」を参照してください。

図 6-8　　SNMP によるクラスタの管理



CHAPTER 7

スイッチの管理

この章では、IE 3000 スイッチを管理するための 1 回限りの手順について説明します。この章で説明する内容は、次のとおりです。

システム日時の管理

Network Time Protocol（NTP; ネットワーク タイム プロトコル）などの自動設定方法または手動設定方法を使用して、スイッチのシステム日時を管理できます。

（注） この項で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ここでは、次の設定情報について説明します。

システム クロックの概要

時刻サービスの中核となるのは、システム クロックです。このクロックは、システムが起動した瞬間から動作し、日時を追跡します。

システム クロックは、次のソースから設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供できます。

- ユーザ **show** コマンド
- ログおよびデバッグ メッセージ

システム クロックは、Universal Time Coordinated（UTC; 協定世界時）（または Greenwich Mean Time（GMT; グリニッジ標準時））に基づいて内部で時刻を追跡します。時刻が現地の時間帯に応じて正しく表示されるように、現地の時間帯と夏時間に関する情報を設定できます。

システム クロックは、時刻が*信頼できる*かどうか（時刻が信頼できると見なされる時刻源によって設定されているかどうか）を追跡します。時刻が信頼できない場合、時刻は表示目的でだけ使用でき、再配布されません。設定の詳細については、「手動での日時の設定」（P.7-11）を参照してください。

ネットワーク タイム プロトコルの概要

NTP は、装置のネットワークの時間を同期するように設計されています。NTP は、IP 上で実行される User Datagram Protocol（UDP; ユーザ データグラム プロトコル）で実行されます。NTP については、RFC 1305 で説明されています。

通常、NTP ネットワークは、タイム サーバに接続されているラジオ クロックやアトミック クロックなど信頼できる時刻源から時刻を取得します。NTP は、ネットワークを介して取得した時刻を配布します。NTP は非常に効率的です。1 分あたり 1 つのパケットを使用するだけで、2 台の装置を 1 ミリ秒以内に同期できます。

NTP は、*ストラタム*という概念を使用して、装置と信頼できる時刻源の間にある NTP ホップ数を表します。ストラタム 1 タイム サーバには、ラジオ クロックまたはアトミック クロックが直接接続され、ストラタム 2 タイム サーバは、ストラタム 1 タイム サーバから NTP 経由で時刻を受信するというように、順番に続いていきます。NTP を実行している装置は、その時刻源として、NTP を介して通信するときに使用するストラタム番号が最小の装置を自動的に選択します。この方法によって、NTP スピーカの自己編成型ツリーが効率的に構築されます。

NTP では、同期されていない装置と同期しないようにして、時刻が正確ではない可能性がある装置との同期を回避します。また、複数の装置から報告された時刻を比較し、時刻が他の装置と大幅に異なる装置とは、そのストラタム番号が小さい場合であっても同期しません。

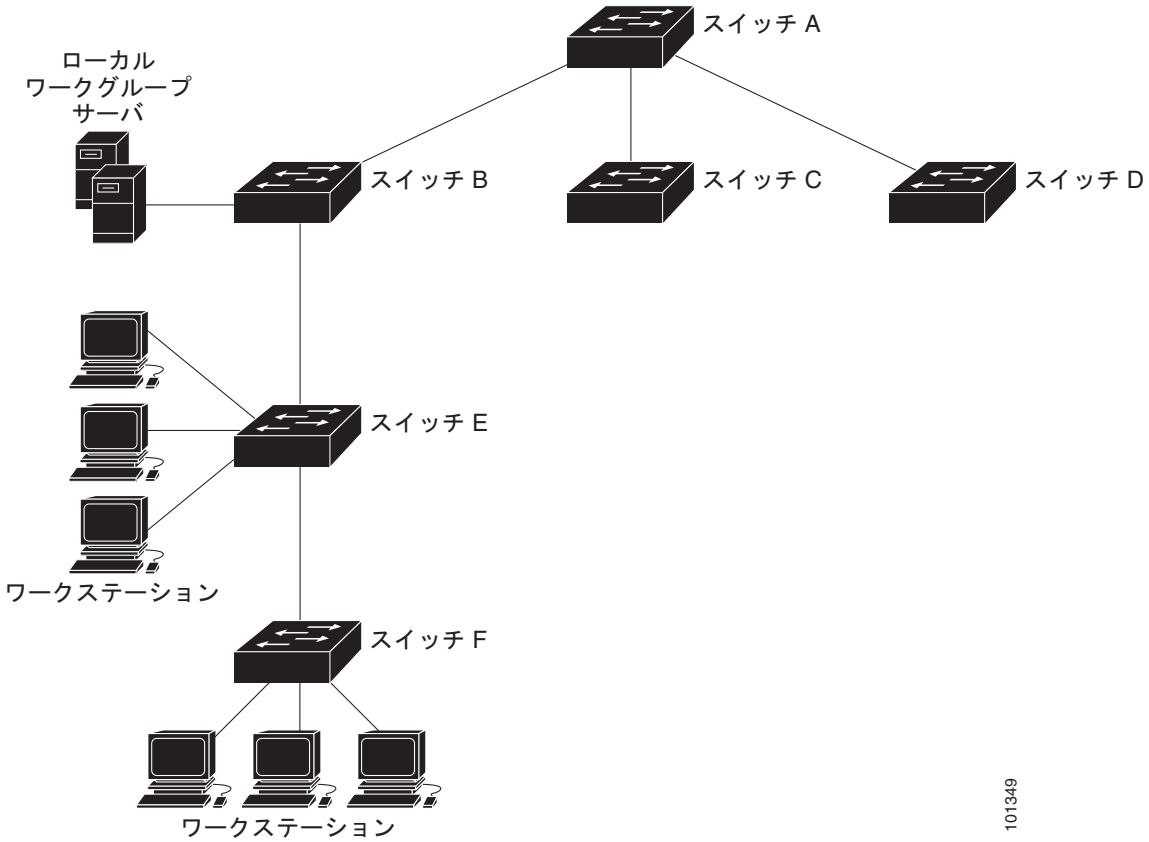
NTP を実行している装置間の通信（*アソシエーション*）は通常、スタティックに設定されます。各装置には、アソシエーションの作成に使用するすべての装置の IP アドレスが与えられます。アソシエーションのペアとなる装置間で NTP メッセージを交換することで、正確なタイムキーピングが実現されます。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。この代替の方法では、ブロードキャスト メッセージを送受信するように各装置を設定するだけなので、設定の複雑さが解消されます。ただし、この場合は、情報の流れが一方向に限定されます。

装置で維持される時刻は重要なリソースです。NTP のセキュリティ機能を使用して、誤って指定した設定や悪意ある設定で誤った時刻が設定されないようにする必要があります。2 つのメカニズムを利用できます。1 つはアクセス リストに基づく制限方式で、もう 1 つは暗号化認証メカニズムです。

シスコの NTP の実装では、ストラタム 1 サービスはサポートされていません。そのため、ラジオ クロックやアトミック クロックに接続できません。ネットワークの時刻サービスは、IP インターネットで使用できるパブリック NTP サーバから取得することを推奨します。

図 7-1 に、NTP を使用した一般的なネットワークの例を示します。スイッチ A は NTP マスターです。スイッチ B、C、D は NTP サーバ モードで設定され、スイッチ A とのサーバ アソシエーション内にあります。スイッチ E は、アップストリーム スイッチ（スイッチ B）とダウンストリーム スイッチ（スイッチ F）に対する NTP ピアとして設定されています。

図 7-1　一般的な NTP ネットワークの設定



ネットワークがインターネットに接続されていない場合、シスコの NTP の実装では、実際には他の方法で時刻を取得している場合でも、NTP を介して同期されているかのように装置を設定できます。この場合、他の装置は、NTP を介してその装置と同期します。

複数の時刻源が使用できる場合、NTP は常に他の時刻源よりも信頼が高いと見なされます。NTP の時刻は、他の方法で設定された時刻よりも優先されます。

いくつかの製造元では、自社のホスト システムに NTP ソフトウェアを組み込んでいます。また、UNIX を実行しているシステム用の公開バージョンおよびその各種派生バージョンもあります。このソフトウェアでは、ホスト システムの時刻も同期できます。

NTP の設定

スイッチには、ハードウェアでサポートされているクロックはありません。また、スイッチは、外部の NTP ソースが使用できない場合に、ペアが自身を同期する NTP マスター クロックとしても機能しません。スイッチには、カレンダーに対するハードウェアのサポートもありません。そのため、**ntp update-calendar** および **ntp master** グローバル コンフィギュレーション コマンドは使用できません。

ここでは、次の設定情報について説明します。

- 「NTP のデフォルト設定」（P.7-4）
- 「NTP 認証の設定」（P.7-4）
- 「NTP アソシエーションの設定」（P.7-5）

NTP のデフォルト設定

表 7-1 に、NTP のデフォルト設定を示します。

表 7-1　NTP のデフォルト設定

機能	デフォルト設定
NTP 認証	ディセーブル。認証キーは指定されていません。
NTP ピアおよびサーバ アソシエーション	設定なし。
NTP ブロードキャスト サービス	ディセーブル。インターフェイスは NTP ブロードキャスト パケットを送受信しません。
NTP アクセス制限	アクセス制御は指定されていません。
NTP パケット送信元 IP アドレス	送信元アドレスは、発信インターフェイスによって設定されます。

NTP は、すべてのインターフェイスでデフォルトでイネーブルになっています。すべてのインターフェイスが NTP パケットを受信します。

NTP 認証の設定

この手順は、NTP サーバの管理者と調整する必要があります。この手順で設定する情報は、スイッチが時刻を NTP サーバと同期するときに使用するサーバと一致する必要があります。

セキュリティ目的で他の装置とのアソシエーション（正確なタイムキーピングを行うために提供される、NTP を実行している装置間の通信）を認証するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp authenticate**	デフォルトではディセーブルになっている NTP 認証機能をイネーブルにします。
ステップ 3	**ntp authentication-key** *number* **md5** *value*	認証キーを定義します。デフォルトでは、認証キーは定義されていません。 • *number* には、キー番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • **md5** は、Message Digest Algorithm 5（MD5）を使用してメッセージ認証のサポートが提供されることを指定します。 • *value* には、キーの 8 文字までの任意の文字列を入力します。 スイッチと装置の両方がこれらの認証キーのいずれかを持たない限り、スイッチと装置は同期しません。また、キー番号は、**ntp trusted-key** *key-number* コマンドで指定されます。

	コマンド	目的
ステップ 4	**ntp trusted-key** *key-number*	スイッチが同期するためにピアの NTP 装置がその NTP パケットに提供する必要のある 1 つまたは複数のキー番号（ステップ 3 で定義）を指定します。 デフォルトでは、信頼できるキーは定義されていません。 *key-number* には、ステップ 3 で定義したキーを指定します。 このコマンドを指定すると、スイッチが誤って信頼できない装置と同期することがなくなります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

NTP 認証をディセーブルにするには、**no ntp authenticate** グローバル コンフィギュレーション コマンドを使用します。認証キーを削除するには、**no ntp authentication-key** *number* グローバル コンフィギュレーション コマンドを使用します。装置の ID の認証をディセーブルにするには、**no ntp trusted-key** *key-number* グローバル コンフィギュレーション コマンドを使用します。

次に、装置の NTP パケットで認証キー 42 を提供する装置とだけ同期するようスイッチを設定する例を示します。

```
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aNiceKey
Switch(config)# ntp trusted-key 42
```

NTP アソシエーションの設定

NTP アソシエーションは、ピア アソシエーション（スイッチを他の装置に同期することも、他の装置をスイッチに同期することもできる）、またはサーバ アソシエーション（スイッチだけが他の装置に同期でき、他の装置からは同期することができない）として設定できます。

別の装置との NTP アソシエーションを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp peer** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	ピアを同期するか、ピアによって同期される（ピア アソシエーション）ようにスイッチのシステム クロックを設定します。
	または	または
	ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	タイム サーバで同期される（サーバ アソシエーション）ようにスイッチのシステム クロックを設定します。 デフォルトでは、ピア アソシエーションまたはサーバ アソシエーションは定義されていません。 • ピア アソシエーションの *ip-address* には、クロック同期を提供しているピア、またはクロック同期が提供されているピアの IP アドレスを指定します。サーバ アソシエーションの場合は、クロック同期を提供しているタイム サーバの IP アドレスを指定します。 • （任意）*number* には、NTP のバージョン番号を指定します。指定できる範囲は 1 ～ 3 です。デフォルトでは、バージョン 3 が選択されています。 • （任意）*keyid* には、**ntp authentication-key** グローバル コンフィギュレーション コマンドで定義した認証キーを入力します。 • （任意）*interface* には、IP 送信元アドレスを選択するインターフェイスを指定します。デフォルトでは、送信元 IP アドレスは発信インターフェイスから取得されます。 • （任意）**prefer** キーワードを入力して、このピアまたはサーバを、同期を提供する優先ピアまたはサーバにします。このキーワードにより、ピアとサーバ間の切り替えが削減されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アソシエーションの一端の装置だけ設定する必要があります。もう一方の装置では、アソシエーションは自動的に設定されます。デフォルトの NTP バージョン（バージョン 3）を使用しているときに NTP 同期が行われない場合は、NTP バージョン 2 を使用してみてください。インターネット上の多くの NTP サーバがバージョン 2 を実行しています。

ピア アソシエーションまたはサーバ アソシエーションを削除するには、**no ntp peer** *ip-address* または **no ntp server** *ip-address* グローバル コンフィギュレーション コマンドを使用します。

次に、NTP バージョン 2 を使用して、IP アドレス 172.16.22.44 にあるピアのクロックとシステム クロックを同期するようにスイッチを設定する例を示します。

```
Switch(config)# ntp server 172.16.22.44 version 2
```

NTP ブロードキャスト サービスの設定

NTP を実行している装置間の通信（*アソシエーション*）は通常、スタティックに設定されます。各装置には、アソシエーションの作成に使用するすべての装置の IP アドレスが与えられます。アソシエーションのペアとなる装置間で NTP メッセージを交換することで、正確なタイムキーピングが実現されます。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。この代替の方法では、ブロードキャスト メッセージを送受信するように各装置を設定するだけなので、設定の複雑さが解消されます。ただし、情報の流れは一方向に限定されます。

ルータなどの NTP ブロードキャスト サーバがあり、ネットワーク上で時刻の情報をブロードキャストしている場合、スイッチはインターフェイス単位で NTP ブロードキャスト パケットを送受信できます。スイッチは NTP ブロードキャスト パケットをピアに送信して、ピアがスイッチと同期できるようにします。また、スイッチは NTP ブロードキャスト パケットを受信して独自のクロックを同期することもできます。ここでは、NTP ブロードキャスト パケットを送受信する手順について説明します。

NTP ブロードキャスト パケットをピアに送信して、ピアがそれぞれのクロックをスイッチと同期するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	NTP ブロードキャスト パケットを送信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]	NTP ブロードキャストをピアに送信するインターフェイスをイネーブルにします。 デフォルトでは、この機能はすべてのインターフェイスでディセーブルになっています。 • （任意）*number* には、NTP のバージョン番号を指定します。指定できる範囲は 1 ～ 3 です。バージョンを指定しない場合、バージョン 3 が使用されます。 • （任意）*keyid* には、パケットをピアに送信するときに使用する認証キーを指定します。 • （任意）*destination-address* には、そのクロックをこのスイッチと同期しているピアの IP アドレスを指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。
ステップ 7		次の手順で説明するように NTP ブロードキャスト パケットを受信するよう、接続されているピアを設定します。

インターフェイスによる NTP ブロードキャスト パケットの送信をディセーブルにするには、**no ntp broadcast** インターフェイス コンフィギュレーション コマンドを使用します。

次に、NTP バージョン 2 パケットを送信するようにポートを設定する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ntp broadcast version 2
```

接続されているピアから NTP ブロードキャスト パケットを受信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	NTP ブロードキャスト パケットを受信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ntp broadcast client**	NTP ブロードキャスト パケットを受信するインターフェイスをイネーブルにします。 デフォルトでは、インターフェイスは NTP ブロードキャスト パケットを受信しません。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ntp broadcastdelay** *microseconds*	（任意）スイッチと NTP ブロードキャスト サーバ間の予測されるラウンドトリップ遅延を変更します。 デフォルト値は 3000 マイクロ秒です。範囲は 1 ～ 999999 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスによる NTP ブロードキャストの受信をディセーブルにするには、**no ntp broadcast client** インターフェイス コンフィギュレーション コマンドを使用します。予測されるラウンドトリップ遅延をデフォルト値に変更するには、**no ntp broadcastdelay** グローバル コンフィギュレーション コマンドを使用します。

次に、NTP ブロードキャスト パケットを受信するようにポートを設定する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ntp broadcast client
```

NTP アクセス制限の設定

- 「アクセス グループの作成と基本 IP アクセス リストの割り当て」（P.7-9）
- 「特定のインターフェイスでの NTP サービスのディセーブル化」（P.7-10）

アクセス グループの作成と基本 IP アクセス リストの割り当て

アクセス リストを使用して NTP サービスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*	アクセス グループを作成し、基本 IP アクセス リストを適用します。 キーワードの意味は次のとおりです。 • **query-only**：NTP 制御クエリーだけ許可します。 • **serve-only**：時刻の要求だけ許可します。 • **serve**：時刻の要求と NTP 制御クエリーを許可しますが、スイッチはリモート装置と同期できません。 • **peer**：時刻の要求と NTP 制御クエリーを許可し、スイッチはリモート装置と同期できます。 *access-list-number* には、1 ～ 99 までの標準 IP アクセス リスト番号を入力します。
ステップ 3	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	アクセス リストを作成します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • **permit** キーワードを入力し、条件が一致した場合にアクセスを許可します。 • *source* の場合は、スイッチへのアクセスが許可される装置の IP アドレスを入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットを入力します。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アクセス グループ キーワードが、次の順序で（最も制限の少ないものから最も制限の大きいものへ）スキャンされます。

1. **peer**：時刻の要求と NTP 制御クエリーを許可し、スイッチはアドレスがアクセス リスト基準を満たしている装置とスイッチを同期できます。
2. **server**：時刻の要求と NTP 制御クエリーを許可しますが、スイッチはアドレスがアクセス リスト基準を満たしている装置とスイッチを同期できません。
3. **serve-only**：アドレスがアドレス リスト基準を満たす装置からの時刻の要求だけ許可します。
4. **query-only**:アドレスがアクセス リスト基準を満たす装置からの NTP 制御クエリーだけ許可します。

送信元 IP アドレスが、複数のアクセス タイプのアクセス リストと一致した場合、最初のタイプが許可されます。アクセス グループが指定されていない場合は、すべてのアクセス タイプがすべての装置に許可されます。アクセス グループが指定されている場合は、指定されたアクセス タイプだけ許可されます。

スイッチの NTP サービスへのアクセス制御を削除するには、**no ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} グローバル コンフィギュレーション コマンドを使用します。

次に、アクセス リスト 99 のピアと同期するためのスイッチを設定する例を示します。ただし、スイッチはアクセス リスト 42 からの時刻の要求だけ許可するようにアクセスを制限します。

```
Switch# configure terminal
Switch(config)# ntp access-group peer 99
Switch(config)# ntp access-group serve-only 42
Switch(config)# access-list 99 permit 172.20.130.5
Switch(config)# access list 42 permit 172.20.130.6
```

特定のインターフェイスでの NTP サービスのディセーブル化

NTP サービスは、すべてのインターフェイスでデフォルトでイネーブルになっています。

NTP パケットのインターフェイス上の受信をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、ディセーブルにするインターフェイスを指定します。
ステップ 3	**ntp disable**	NTP パケットのインターフェイス上の受信をディセーブルにします。 デフォルトでは、すべてのインターフェイスは NTP パケットを受信します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

NTP パケットのインターフェイス上の受信を再びイネーブルにするには、**no ntp disable** インターフェイス コンフィギュレーション コマンドを使用します。

NTP パケットの送信元 IP アドレスの設定

スイッチで NTP パケットを送信する場合、送信元 IP アドレスは通常、NTP パケットが送信されるときに使用されるインターフェイスのアドレスに設定されます。すべての NTP パケットで特定の送信元 IP アドレスを使用する場合は、**ntp source** グローバル コンフィギュレーション コマンドを使用します。アドレスは、指定されたインターフェイスから取得されます。このコマンドは、インターフェイス上のアドレスが、応答パケットの宛先として使用できない場合に役に立ちます。

送信元 IP アドレスが取得される特定のインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp source** *type number*	送信元 IP アドレスが取得されるインターフェイスのタイプと番号を指定します。 デフォルトでは、送信元アドレスは、発信インターフェイスによって設定されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定されたインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスに使用されます。送信元アドレスを特定のアソシエーションに使用する場合は、「NTP アソシエーションの設定」（P.7-5）の説明に従って、**ntp peer** または **ntp server** グローバル コンフィギュレーション コマンドで **source** キーワードを使用します。

NTP の設定の表示

NTP 情報を表示するには、次の 2 つの特権 EXEC コマンドを使用します。

- **show ntp associations** [**detail**]
- **show ntp status**

（注）　この出力に表示されるフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。

手動での日時の設定

他の時刻源が使用できない場合は、システムを再起動した後に、手動で日時を設定できます。次にシステムを再起動するまで、時刻は正確な状態で維持されます。手動設定は、最後の手段としてだけ使用することを推奨します。スイッチが同期できる外部の時刻源がある場合、システム クロックを手動で設定する必要はありません。

ここでは、次の設定情報について説明します。

- 「システム クロックの設定」（P.7-11）
- 「日時設定の表示」（P.7-12）
- 「時間帯の設定」（P.7-12）
- 「夏時間の設定」（P.7-13）

システム クロックの設定

NTP サーバなど、時刻サービスを提供する外部の時刻源がネットワーク上にある場合、システム クロックを手動で設定する必要はありません。

システム クロックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**clock set** *hh*:*mm*:*ss day month year* または **clock set** *hh*:*mm*:*ss month day year*	次のフォーマットのいずれか 1 つを使用して、システム クロックを手動で設定します。 • *hh*:*mm*:*ss* には、24 時間形式の時間、分、秒で時刻を指定します。指定された時刻は、設定された時間帯に基づきます。 • *day* には、月の日付を指定します。 • *month* には、月の名前を指定します。 • *year* には、年（省略なし）を指定します。

次に、システム クロックを 2001 年 7 月 23 日の午後 1 時 32 分に手動で設定する例を示します。

```
Switch# clock set 13:32:00 23 July 2001
```

日時設定の表示

日時の設定を表示するには、**show clock** [**detail**] 特権 EXEC コマンドを使用します。

システム クロックでは、時刻が信頼できる（正確であると確信できる）かどうかを示す *authoritative* フラグが維持されます。システム クロックが NTP などのタイミング ソースにより設定されている場合、フラグが設定されます。時刻が信頼できない場合、時刻は表示目的でだけ使用されます。クロックが信頼でき、*authoritative* フラグが設定されるまでは、フラグによって、ピアの時刻が無効な場合にピアはクロックと同期されません。

show clock 表示の前にある記号の意味は次のとおりです。

- *：時刻は信頼できません。
- （空白）：時刻は信頼できます。
- .：時刻は信頼できますが、NTP は同期されません。

時間帯の設定

手動で時間帯を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	時間帯を設定します。 スイッチでは、UTC の内部時刻が維持されるため、このコマンドは、表示目的および時刻を手動で設定する場合にだけ使用されます。 • *zone* には、標準時間が有効なときに表示される時間帯の名前を入力します。デフォルトは UTC です。 • *hours-offset* には、UTC からの時間のオフセットを入力します。 • （任意）*minutes-offset* には、UTC からの分のオフセットを入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

clock timezone グローバル コンフィギュレーション コマンドの *minutes-offset* 変数は、現地の時間帯が UTC との時間差を 1 時間における割合で表す場合に使用できます。たとえば、カナダ大西洋沿岸のある区域の時間帯の Atlantic Standard Time（AST; 大西洋標準時）が UTC-3.5 の場合、3 は 3 時間、.5 は 50% を意味します。この場合、必要なコマンドは **clock timezone AST -3 30** です。

時刻を UTC に設定するには、**no clock timezone** グローバル コンフィギュレーション コマンドを使用します。

夏時間の設定

毎年の特定の曜日に夏時間が開始および終了する区域に夏時間を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定された日付に開始および終了する夏時間を設定します。 夏時間はデフォルトではディセーブルになっています。パラメータを指定せずに **clock summer-time** *zone* **recurring** を指定すると、夏時間のルールはデフォルトで米国のルールに設定されます。 • *zone* には、夏時間が有効な場合に表示される時間帯の名前（PDT など）を指定します。 • （任意）*week* には、月の週（1 ～ 5 または **last**）を指定します。 • （任意）*day* には、曜日（Sunday、Monday など）を指定します。 • （任意）*month* には、月（January、February など）を指定します。 • （任意）*hh*:*mm* には、24 時間形式の時間と分を指定します。 • （任意）*offset* には、夏時間の間に追加する分数を指定します。デフォルト値は 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では、夏時間が開始される日時を指定します。2 つ目の部分では終了する日時を指定します。すべての時刻は、現地の時間帯に基づきます。開始時刻は、標準時間に基づきます。終了時刻は、夏時間に基づきます。開始月が終了月よりあとの場合は、システムでは南半球にいると見なされます。

次に、夏時間が 4 月の第 1 日曜日の 2 時に開始し、10 月の最終日曜日の 2 時に終了するように指定する例を示します。

```
Switch(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October
2:00
```

区域の夏時間が定期的なパターンに従わない（次の夏時間イベントの正確な日時を設定する）場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	最初の日付から開始し、2 つ目の日付で終了するように夏時間を設定します。 夏時間はデフォルトではディセーブルになっています。 • *zone* には、夏時間が有効な場合に表示される時間帯の名前（PDT など）を指定します。 • （任意）*week* には、月の週（1 ～ 5 または **last**）を指定します。 • （任意）*day* には、曜日（Sunday、Monday など）を指定します。 • （任意）*month* には、月（January、February など）を指定します。 • （任意）*hh*:*mm* には、24 時間形式の時間と分を指定します。 • （任意）*offset* には、夏時間の間に追加する分数を指定します。デフォルト値は 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では、夏時間が開始される日時を指定します。2 つ目の部分では終了する日時を指定します。すべての時刻は、現地の時間帯に基づきます。開始時刻は、標準時間に基づきます。終了時刻は、夏時間に基づきます。開始月が終了月よりあとの場合は、システムでは南半球にいると見なされます。

夏時間をディセーブルにするには、**no clock summer-time** グローバル コンフィギュレーション コマンドを使用します。

次に、夏時間が 2000 年 10 月 12 日の 2 時に開始し、2001 年 4 月 26 日の 2 時に終了するように設定する例を示します。

```
Switch(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

システム名とプロンプトの設定

スイッチにシステム名を設定して識別します。デフォルトでは、システム名とプロンプトは *Switch* です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字がシステム プロンプトとして使用されます。大なり記号 [>] が追加されます。システム名が変更されるたびにプロンプトが更新されます。

この項で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference*』および『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』を参照してください。

ここでは、次の設定情報について説明します。

- 「デフォルトのシステム名とプロンプトの設定」（P.7-15）
- 「システム名の設定」（P.7-15）
- 「DNS の概要」（P.7-15）

デフォルトのシステム名とプロンプトの設定

デフォルトのスイッチ システム名とプロンプトは *Switch* です。

システム名の設定

手動でシステム名を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *name*	手動でシステム名を設定します。 デフォルト設定は *switch* です。 名前は、ARPANET ホスト名のルールに従う必要があります。名前の先頭は文字で始まり、文字または数字で終わり、その間には文字、数字、およびハイフンしか使用できません。名前には最大 63 文字を使用できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

システム名を設定すると、その名前はシステム プロンプトとしても使用されます。

デフォルトのホスト名に戻すには、**no hostname** グローバル コンフィギュレーション コマンドを使用します。

DNS の概要

Domain Name System（DNS; ドメイン ネーム システム）プロトコルは、DNS を制御します。DNS は、ホスト名を IP アドレスにマッピングできる分散データベースです。スイッチ上に DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドおよび関連の Telnet サポート 操作時に、IP アドレスの代わりにホスト名を使用できます。

IP は、場所やドメインによって装置を識別できる階層型の命名方式を定義します。ドメイン名は、デリミタにピリオド (.) を使用して連結できます。たとえば、シスコシステムズは、IP が *com* というドメイン名で識別される商業組織なので、ドメイン名は *cisco.com* となります。このドメインの特定の装置、たとえば File Transfer Protocol（FTP; ファイル転送プロトコル）システムは *ftp.cisco.com* として識別されます。

ドメイン名を継続的に追跡するために、IP はドメイン ネーム サーバの概念を定義しています。このサーバには、IP アドレスにマッピングされる名前のキャッシュ（またはデータベース）が保持されます。ドメイン名を IP アドレスにマッピングするには、まずホスト名を識別し、ネットワーク上にあるネーム サーバを指定し、DNS をイネーブルにします。

ここでは、次の設定情報について説明します。

- 「DNS のデフォルト設定」（P.7-16）
- 「DNS の設定」（P.7-16）
- 「DNS の設定の表示」（P.7-17）

DNS のデフォルト設定

表 7-2 に、DNS のデフォルト設定を示します。

表 7-2　DNS のデフォルト設定

機能	デフォルト設定
DNS イネーブル ステート	イネーブル
DNS デフォルト ドメイン名	設定なし
DNS サーバ	ネーム サーバ アドレスの設定なし

DNS の設定

DNS を使用するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip domain-name** *name*	未修飾のホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 起動時に、ドメイン名は設定されませんが、BOOTP または Dynamic Host Configuration Protocol（DHCP）サーバからスイッチの設定を取得している場合は、BOOTP または DHCP サーバでデフォルトのドメイン名が設定されている可能性があります（サーバがこの情報を使用して設定されている場合）。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	名前とアドレスの解決に使用する、1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバ アドレスはスペースで区切ります。最初に指定されたサーバがプライマリ サーバです。スイッチは、最初にプライマリ サーバに DNS クエリーを送信します。そのクエリーが失敗した場合は、バックアップ サーバにクエリーが送信されます。
ステップ 4	**ip domain-lookup**	（任意）スイッチで、DNS ベースのホスト名からアドレスへの変換をイネーブルにします。この機能はデフォルトでイネーブルになっています。 使用するネットワーク装置が、名前の割り当てを制御していないネットワーク内の装置と接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、装置を一意に識別する装置名をダイナミックに割り当てることができます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチの IP アドレスをそのホスト名として使用する場合は、IP アドレスが使用され、DNS クエリーは発生しません。ピリオド（.）なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホストに追加され、そのあとで DNS クエリーが行われ、名前が IP アドレスにマッピングされます。デフォルトのドメイン名は、**ip domain-name** グローバル コンフィギュレーション コマンドによって設定される値です。ホスト名にピリオド（.）がある場合は、Cisco IOS ソフトウェアは、ホスト名にデフォルトのドメイン名を追加せずに IP アドレスを検索します。

ドメイン名を削除するには、**no ip domain-name** *name* グローバル コンフィギュレーション コマンドを使用します。ネーム サーバのアドレスを削除するには、**no ip name-server** *server-address* グローバル コンフィギュレーション コマンドを使用します。スイッチ上の DNS をディセーブルにするには、**no ip domain-lookup** グローバル コンフィギュレーション コマンドを使用します。

DNS の設定の表示

DNS 設定情報を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

バナーの作成

Message-Of-The-Day（MOTD）とログイン バナーを設定できます。MOTD バナーは、ログイン時に接続されているすべての端末に表示され、すべてのネットワーク ユーザに影響のあるメッセージ（システムのシャットダウン予告など）を送信するのに役立ちます。

ログイン バナーも、接続されているすべての端末で表示されます。表示されるのは、MOTD バナーのあとで、ログイン プロンプトが表示される前です。

（注）　この項で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

- 「バナーのデフォルト設定」（P.7-17）
- 「Message-Of-The-Day ログイン バナーの設定」（P.7-17）
- 「ログイン バナーの設定」（P.7-19）

バナーのデフォルト設定

MOTD バナーとログイン バナーは設定されません。

Message-Of-The-Day ログイン バナーの設定

ユーザがスイッチにログインしたときに画面に表示される 1 行または複数行のメッセージ バナーを作成できます。

MOTD ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner motd** *c message c*	該当の日のメッセージを指定します。 *c* には、任意のデリミタ、たとえばポンド記号（#）を入力して、Return キーを押します。デリミタは、バナー テキストの始まりと終わりを表します。終わりのデリミタのあとの文字は廃棄されます。 *message* には、最大 255 文字のバナー メッセージを入力します。メッセージにはデリミタを使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

MOTD バナーを削除するには、**no banner motd** グローバル コンフィギュレーション コマンドを使用します。

次に、ポンド記号（#）を始まりのデリミタおよび終わりのデリミタとして使用し、スイッチの MOTD バナーを設定する例を示します。

```
Switch(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
Switch(config)#
```

次に、前の設定により表示されたバナーの例を示します。

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

User Access Verification

Password:
```

ログイン バナーの設定

接続されているすべての端末でログイン バナーが表示されるように設定できます。バナーが表示されるのは、MOTD バナーのあとで、ログイン プロンプトが表示される前です。

ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner login** *c message c*	ログイン メッセージを指定します。 *c* には、任意のデリミタ、たとえばポンド記号（#）を入力して、Return キーを押します。デリミタは、バナー テキストの始まりと終わりを表します。終わりのデリミタのあとの文字は廃棄されます。 *message* には、最大 255 文字のログイン メッセージを入力します。メッセージにはデリミタを使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ログイン バナーを削除するには、**no banner login** グローバル コンフィギュレーション コマンドを使用します。

次に、ドル記号（$）を始まりのデリミタおよび終わりのデリミタとして使用し、スイッチのログイン バナーを設定する例を示します。

```
Switch(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
Switch(config)#
```

MAC アドレス テーブルの管理

Media Access Control（MAC; メディア アクセス制御）アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。アドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに関連付けられます。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス：スイッチが学習し、使用されなくなった時点で期限切れとなる送信元 MAC アドレス。
- スタティック アドレス：手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャスト アドレス。

アドレス テーブルは、宛先 MAC アドレス、関連付けられている VLAN ID、アドレスとタイプ（スタティックまたはダイナミック）に関連付けられているポート番号を示します。

（注）　この項で使用しているコマンドの構文と使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

ここでは、次の設定情報について説明します。

アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスによって、スイッチの任意のポートを各ワークステーション、リピータ、スイッチ、ルータ、その他のネットワーク装置に接続できます。各ポートで受信するパケットの送信元アドレスを学習し、アドレス テーブルにアドレスと関連付けられているポート番号を追加することにより、スイッチはダイナミックなアドレス指定を行います。ネットワークでステーションの増設または取り外しが行われると、スイッチはアドレス テーブルを更新し、新しいダイナミック アドレスを追加し、使用されていないアドレスを期限切れにします。

エージング インターバルは、グローバルに設定されます。ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）によって VLAN 単位でエージング インターバルを短縮できます。

スイッチは、受信したパケットの宛先アドレスに基づいて、組み合わせのポート間でパケットを送信します。MAC アドレス テーブルを使用して、スイッチは宛先アドレスに関連付けられているポートにだけパケットを転送します。宛先アドレスがパケットを送信したポート上にある場合は、パケットはフィルタリング処理され、転送されません。スイッチは、常にストアアンドフォワード方式を使用します。つまり、完全なパケットを保管して、エラーがないかチェックしてから転送されます。

MAC アドレスと VLAN

すべてのアドレスは VLAN に関連付けられています。1 つのアドレスを複数の VLAN に関連付け、それぞれに異なる宛先を設定できます。たとえば、ユニキャスト アドレスを VLAN 1 のポート 1 および VLAN 5 のポート 9、10、および 1 に転送できます。

VLAN ごとに、独自の論理アドレス テーブルが維持されます。ある VLAN で既知のアドレスが別の VLAN で認識されるには、別の VLAN 内のポートによって学習されるか、スタティックに関連付けられる必要があります。

プライベート VLAN が設定されている場合は、アドレス学習は MAC アドレスのタイプによって異なります。

- プライベート VLAN の 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連する VLAN に複製されます。たとえば、プライベート VLAN のセカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN に複製されます。
- プライマリ VLAN またはセカンダリ VLAN で設定されたスタティック MAC アドレスは、関連付けられている VLAN には複製されません。プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN にスタティック MAC アドレスを設定するときは、同じスタティック MAC アドレスを、関連付けられているすべての VLAN にも設定する必要があります。

プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」を参照してください。

MAC アドレス テーブルのデフォルト設定

表 7-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 7-3　MAC アドレス テーブルのデフォルト設定

機能	デフォルト設定
エージング タイム	300 秒
ダイナミック アドレス	自動的に学習
スタティック アドレス	設定なし

アドレスのエージング タイムの変更

ダイナミック アドレスは、スイッチが学習し、使用されなくなった時点で期限切れとなる送信元 MAC アドレスです。すべての VLAN または指定された VLAN のエージング タイムの設定を変更できます。

エージング タイムの設定が短すぎると、アドレスがテーブルから削除されるのが早くなります。また、スイッチで不明な宛先のパケットを受信すると、受信ポートと同じ VLAN 内のすべてのポートにパケットがフラッディングします。この不要なフラッディングによって、パフォーマンスに影響を与える可能性があります。エージング タイムの設定が長すぎると、アドレス テーブルは未使用のアドレスで一杯になり、新しいアドレスが学習されなくなります。この結果フラッディングとなり、スイッチのパフォーマンスに影響を与える可能性があります。

ダイナミック アドレス テーブルのエージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]	ダイナミック エントリが使用または更新されたあと、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ～ 1000000 秒です。デフォルト値は 300 です。0 を入力して、エージングをディセーブルにすることもできます。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 *vlan-id* に指定できる有効な ID は 1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show mac address-table aging-time**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト値に戻すには、**no mac address-table aging-time** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック アドレス エントリの削除

すべてのダイナミック エントリを削除するには、特権 EXEC モードで **clear mac address-table dynamic** コマンドを使用します。特定の MAC アドレス（**clear mac address-table dynamic address** *mac-address*）、指定された物理ポートまたはポート チャネル上のすべてのアドレス（**clear mac address-table dynamic interface** *interface-id*）、または指定された VLAN 上のすべてのアドレス（**clear mac address-table dynamic vlan** *vlan-id*）の削除もできます。

ダイナミック エントリが削除されたことを確認するには、**show mac address-table dynamic** 特権 EXEC コマンドを使用します。

MAC アドレス変更通知トラップの設定

MAC アドレス変更通知では、MAC アドレスの変更アクティビティを保存して、ネットワーク上のユーザを追跡します。スイッチが MAC アドレスを学習または削除するときに、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）通知トラップを Network Management System（NMS; ネットワーク管理システム）に送信できます。多くのユーザがネットワークに出入りしている場合は、トラップの間隔を設定して通知トラップをバンドルし、ネットワーク トラフィックを削減できます。MAC 通知履歴テーブルには、トラップが設定されている各ポートの MAC アドレス アクティビティが保存されます。MAC アドレス変更通知は、ダイナミック MAC アドレスまたはセキュア MAC アドレスについて許可されます。自アドレス、マルチキャスト アドレス、または他のスタティック アドレスについては、通知は生成されません。

MAC アドレス変更通知トラップを NMS ホストに送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前またはアドレスを指定します。 • SNMP トラップをホストに送信するには、**traps**（デフォルト）を指定します。SNMP 情報をホストに送信するには **informs** を指定します。 • サポートする SNMP バージョンを指定します。情報の場合は、デフォルトのバージョン 1 を使用できません。 • *community-string* には、通知処理で送信するストリングを指定します。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* には、**mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification change**	MAC アドレス変更通知トラップを NMS に送信するようにスイッチをイネーブルにします。
ステップ 4	**mac address-table notification change**	MAC アドレス変更通知機能をイネーブルにします。
ステップ 5	**mac address-table notification change** [**interval** *value*] [**history-size** *value*]	トラップの間隔と履歴テーブルのサイズを入力します。 • （任意）**interval** *value* には、NMS に対して生成される各トラップ セット間の通知トラップ間隔を秒単位で指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 1 秒です。 • （任意）**history-size** *value* には、MAC 通知履歴テーブルのエントリの最大数を指定します。指定できる範囲は 0 ～ 500 です。デフォルトは 1 です。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。
ステップ 7	**snmp trap mac-notification change** {**added** | **removed**}	インターフェイス上で MAC アドレス変更通知トラップをイネーブルにします。 • MAC アドレスがインターフェイスに**追加された**ときに、トラップをイネーブルにします。 • MAC アドレスがインターフェイスから**削除された**ときに、トラップをイネーブルにします。

	コマンド	目的
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mac address-table notification change interface** **show running-config**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

MAC アドレス変更通知トラップをディセーブルにするには、**no snmp-server enable traps mac-notification change** グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイス上で MAC アドレス変更通知トラップをディセーブルにするには、**no snmp trap mac-notification change** {**added** | **removed**} インターフェイス コンフィギュレーション コマンドを使用します。MAC アドレス変更通知機能をディセーブルにするには、**no mac address-table notification change** グローバル コンフィギュレーション コマンドを使用します。

次に、172.20.10.10 を NMS として指定し、MAC アドレス通知トラップを NMS に送信するようにスイッチをイネーブルにし、MAC アドレス変更通知機能をイネーブルにし、間隔を 123 秒に設定し、履歴サイズを 100 エントリまでとし、MAC アドレスが指定されたポートに追加されるたびにトラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# snmp trap mac-notification change added
```

設定を確認するには、**show mac address-table notification change interface** および **show mac address-table notification change** 特権 EXEC コマンドを入力します。

MAC アドレス移行通知トラップの設定

MAC 移行通知を設定すると、MAC アドレスが同じ VLAN 内の別のポートに移行するたびに、SNMP 通知が生成されて、ネットワーク管理システムに送信されます。

MAC アドレス移行通知トラップを NMS ホストに送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前またはアドレスを指定します。 • SNMP トラップをホストに送信するには、**traps**（デフォルト）を指定します。SNMP 情報をホストに送信するには **informs** を指定します。 • サポートする SNMP バージョンを指定します。情報の場合は、デフォルトのバージョン 1 を使用できません。 • *community-string* には、通知処理で送信するストリングを指定します。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* には、**mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification move**	MAC アドレス移行通知トラップを NMS に送信するようにスイッチをイネーブルにします。
ステップ 4	**mac address-table notification mac-move**	MAC アドレス移行通知機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show mac address-table notification mac-move** **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

MAC アドレス移行通知トラップをディセーブルにするには、**no snmp-server enable traps mac-notification move** グローバル コンフィギュレーション コマンドを使用します。MAC アドレス移行通知機能をディセーブルにするには、**no mac address-table notification mac-move** グローバル コンフィギュレーション コマンドを使用します。

次に、172.20.10.10 を NMS として設定し、MAC アドレス移行通知トラップを NMS に送信するようにスイッチをイネーブルにし、MAC アドレス移行通知機能をイネーブルにし、MAC アドレスが別のポートに移行したときにトラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification move
Switch(config)# mac address-table notification mac-move
```

設定を確認するには、**show mac address-table notification mac-move** 特権 EXEC コマンドを入力します。

MAC スレッシュホールド通知トラップの設定

MAC スレッシュホールド通知を設定すると、MAC アドレス テーブルのスレッシュホールド制限に達するか、スレッシュホールド制限を超えると、SNMP 通知が生成されて、ネットワーク管理システムに送信されます。

MAC アドレス テーブル スレッシュホールド通知トラップを NMS ホストに送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前またはアドレスを指定します。 • SNMP トラップをホストに送信するには、**traps**（デフォルト）を指定します。SNMP 情報をホストに送信するには **informs** を指定します。 • サポートする SNMP バージョンを指定します。情報の場合は、デフォルトのバージョン 1 を使用できません。 • *community-string* には、通知処理で送信するストリングを指定します。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* には、**mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification threshold**	MAC スレッシュホールド通知トラップを NMS に送信するようにスイッチをイネーブルにします。
ステップ 4	**mac address-table notification threshold**	MAC アドレススレッシュホールド通知機能をイネーブルにします。
ステップ 5	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]	MAC アドレス スレッシュホールド使用状況のモニタリングのスレッシュホールドを入力します。 • （任意）limit percentage には、MAC アドレス テーブルの使用割合を指定します。有効値は 1 ～ 100% です。デフォルト値は 50% です。 • （任意）interval time には、通知間隔を指定します。有効値は 120 秒以上です。デフォルト値は 120 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mac address-table notification threshold** **show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

MAC アドレス スレッシュホールド通知トラップをディセーブルにするには、**no snmp-server enable traps mac-notification threshold** グローバル コンフィギュレーション コマンドを使用します。MAC アドレス スレッシュホールド通知機能をディセーブルにするには、**no mac address-table notification threshold** グローバル コンフィギュレーション コマンドを使用します。

次に、172.20.10.10 を NMS として設定し、MAC アドレス スレッシュホールド通知機能をイネーブルにし、間隔を 123 秒に設定し、制限を 78% に設定する例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification threshold
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold interval 123
Switch(config)# mac address-table notification threshold limit 78
```

設定を確認するには、**show mac address-table notification threshold** 特権 EXEC コマンドを入力します。

スタティック アドレス エントリの追加と削除

スタティック アドレスには、次の特性があります。

- アドレス テーブルに手動で入力し、手動で削除する必要があります。
- ユニキャスト アドレスまたはマルチキャスト アドレスとして使用できます。
- 期限切れにならず、スイッチの再起動時に保持されます。

スタティック アドレスを追加および削除し、それらのアドレスの転送動作を定義できます。転送動作では、パケットを受信するポートがパケットを別の伝送用ポートに転送する方法を定義します。すべてのポートは少なくとも 1 つの VLAN に関連付けられているため、スイッチは指定したポートからアドレスの VLAN ID を取得します。送信元ポートごとに異なる宛先ポート リストを指定できます。

スタティックに入力されていない VLAN に、スタティック アドレスを持つパケットが着信した場合、そのパケットはすべてのポートにフラッディングされ、学習されません。

宛先 MAC ユニキャスト アドレスと受信元の VLAN を指定して、スタティック アドレスをアドレス テーブルに追加します。この宛先アドレスで受信したパケットは、*interface-id* オプションで指定されたインターフェイスに転送されます。

プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN にスタティック MAC アドレスを設定するときは、同じスタティック MAC アドレスを、関連付けられているすべての VLAN にも設定する必要があります。プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN で設定されたスタティック MAC アドレスは、関連付けられている VLAN には複製されません。プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」を参照してください。

スタティック アドレスを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	スタティック アドレスを MAC アドレス テーブルに追加します。 • *mac-addr* には、アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 • *vlan-id* には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID は、1 ～ 4094 です。 • *interface-id* には、受信されたパケットを転送するインターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポート チャネルです。スタティック マルチキャスト アドレスの場合は、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合は、一度に 1 つのインターフェイスだけ入力できます。ただし、同じ MAC アドレスと VLAN ID を使用してコマンドを複数回入力できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table static**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スタティック エントリをアドレス テーブルから削除するには、**no mac address-table static** *mac-addr* **vlan** *vlan-id* [**interface** *interface-id*] グローバル コンフィギュレーション コマンドを使用します。

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。VLAN 4 でこの MAC アドレスを宛先アドレスとしてパケットを受信すると、パケットは指定されたポートに転送されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet1/1
```

ユニキャスト MAC アドレス フィルタリングの設定

ユニキャスト MAC アドレス フィルタリングがイネーブルの場合、スイッチは、特定の送信元または宛先 MAC アドレスのパケットを廃棄します。この機能はデフォルトではディセーブルになっています。また、この機能ではユニキャスト スタティック アドレスだけサポートされます。

この機能を使用する場合、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされません。**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** グローバル コンフィギュレーション コマンドを入力するときに、これらのいずれかのアドレスを指定すると、次のいずれかのメッセージが表示されます。

  ```
  % Only unicast addresses can be configured to be dropped

  % CPU destined address cannot be configured as drop address
  ```

- CPU に転送されるパケットもサポートされません。

- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、またはその MAC アドレスを持つパケットを廃棄します。2 番めに入力したコマンドは、最初のコマンドを上書きします。

  たとえば、**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* グローバル コンフィギュレーション コマンドのあとに **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** コマンドを入力した場合は、スイッチは送信元または宛先として指定された MAC アドレスを持つパケットを廃棄します。

  mac address-table static *mac-addr* **vlan** *vlan-id* **drop** グローバル コンフィギュレーション コマンドのあとに **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* コマンドを入力した場合は、スイッチがその MAC アドレスをスタティック アドレスとして追加します。

ユニキャスト MAC アドレス フィルタリングをイネーブルにし、送信元または宛先のユニキャスト MAC アドレスと受信元の VLAN を指定して、特定のアドレスのパケットを廃棄するようにスイッチを設定します。

送信元または宛先のユニキャスト スタティック アドレスを廃棄するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、指定された送信元または宛先のユニキャスト スタティック アドレスのパケットを廃棄するようにスイッチを設定します。 • *mac-addr* には、送信元または宛先のユニキャスト MAC アドレスを指定します。この MAC アドレスを持つパケットは廃棄されます。 • *vlan-id* には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID は、1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table static**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ユニキャスト MAC アドレス フィルタリングをディセーブルにするには、**no mac address-table static** *mac-addr* **vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

次の例では、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つパケットを廃棄するようにスイッチを設定する方法を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットが廃棄されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

VLAN での MAC アドレス学習のディセーブル化

デフォルトでは、MAC アドレス学習はスイッチのすべての VLAN でイネーブルです。VLAN で MAC アドレス学習を制御して、MAC アドレスを学習できる VLAN、さらにポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。MAC アドレス学習をディセーブルにする前に、ネットワーク トポロジとスイッチ システム設定に詳しいことを確認してください。VLAN で MAC アドレス学習をディセーブルにすると、ネットワークでフラッディングを引き起こす可能性があります。

VLAN で MAC アドレス学習をディセーブルにする場合、次の注意事項に従ってください。

- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を設定済みの VLAN で MAC アドレス学習をディセーブルにする場合は十分注意してください。この場合、スイッチは、レイヤ 2 ドメインにすべての IP パケットをフラッディングします。
- MAC アドレス学習は、1 つの VLAN ID（例：**no mac address-table learning vlan 223**）または一連の VLAN ID（例 : **no mac address-table learning vlan 1-20, 15**）でディセーブルにできます。
- MAC アドレス学習のディセーブル化はポートを 2 つ含む VLAN だけで行うことを推奨します。3 つ以上のポートを含む VLAN で MAC アドレス学習をディセーブルにした場合、スイッチに着信するすべてのパケットは、その VLAN ドメインでフラッディングします。
- スイッチが内部的に使用する VLAN で MAC アドレス学習をディセーブルにできません。入力する VLAN ID が内部 VLAN である場合、スイッチはエラー メッセージを生成してコマンドを拒否します。使用している内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを使用します。
- プライベート VLAN のプライマリ VLAN として設定された VLAN で MAC アドレス学習をディセーブルにする場合、MAC アドレスは、そのプライベート VLAN に属するセカンダリ VLAN 上で引き続き学習され、プライマリ VLAN に複製されます。プライベート VLAN のプライマリ VLAN ではなくセカンダリ VLAN で MAC アドレス学習をディセーブルにする場合、プライマリ VLAN で MAC アドレス学習が実行され、セカンダリ VLAN に複製されます。
- RSPAN VLAN で MAC アドレス学習はディセーブルにできません。設定すること自体できません。
- セキュア ポートを含む VLAN で MAC アドレス学習をディセーブルにする場合、セキュア ポートで MAC アドレス学習はディセーブルになりません。ポート セキュリティをディセーブルにする場合、設定した MAC アドレス学習の状態がイネーブルになります。

VLAN で MAC アドレス学習をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no mac address-table learning vlan** *vlan-id*	指定された 1 つまたは複数の VLAN で MAC アドレス学習をディセーブルにします。1 つの VLAN ID を指定するか、一連の VLAN ID をハイフンまたはカンマで区切って指定できます。指定できる VLAN ID は、1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table learning** [**vlan** *vlan-id*]	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN で MAC アドレス学習を再びイネーブルにするには、**default mac address-table learning vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。**mac address-table learning vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力して、VLAN で MAC アドレス学習を再びイネーブルにすることもできます。1 つ目（**デフォルト**）のコマンドでは、デフォルト設定の状態に戻るため、**show running-config** コマンドを実行しても出力に表示されません。2 つ目のコマンドでは、**show running-config** 特権 EXEC コマンドの表示に設定が表示されます。

次に、VLAN 200 で MAC アドレス学習をディセーブルにする例を示します。

```
Switch(config)# no mac address-table learning vlan 200
```

すべての VLAN、または指定された VLAN の MAC アドレス学習のステータスを表示するには、**show mac-address-table learning** [**vlan** *vlan-id*] 特権 EXEC コマンドを入力します。

アドレス テーブル エントリの表示

表 7-4 で説明されている 1 つまたは複数の特権 EXEC コマンドを使用して、MAC アドレス テーブルを表示できます。

表 7-4　MAC アドレス テーブルを表示するためのコマンド

コマンド	説明
show ip igmp snooping groups	すべての VLAN または指定された VLAN のレイヤ 2 マルチキャスト エントリを表示します。
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table learning	すべての VLAN または指定された VLAN の MAC アドレス学習のステータスを表示します。
show mac address-table notification	MAC 通知パラメータと履歴テーブルを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

ARP テーブルの管理

イーサネットなどを介して装置と通信するために、ソフトウェアは最初にその装置の 48 ビットの MAC アドレスまたはローカル データ リンク アドレスを学習する必要があります。IP アドレスからローカル データ リンク アドレスを学習するプロセスは、*アドレス解決*と呼ばれます。

Address Resolution Protocol（ARP; アドレス解決プロトコル）は、ホストの IP アドレスを対応するメディアまたは MAC アドレスおよび VLAN ID に関連付けます。ARP は、IP アドレスを使用して、関連付けられた MAC アドレスを検索します。MAC アドレスが見つかると、IP と MAC アドレスの関連付けが ARP キャッシュに保存され、すぐに取得できます。次に、IP データグラムがリンクレイヤ フレームにカプセル化され、ネットワーク上で送信されます。イーサネット以外の IEEE 802 ネットワークでの IP データグラムおよび ARP 要求および応答のカプセル化は、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）で指定されます。デフォルトでは、IP インターフェイスで標準のイーサネット形式の ARP カプセル化（**arpa** キーワードで表される）はイネーブルになっています。

テーブルに手動で追加された ARP エントリは期限切れがないため、手動で削除する必要があります。

（注）　CLI の手順の詳細については、Cisco.com のページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] にある Cisco IOS Release 12.2 のマニュアルを参照してください。

CHAPTER 8

PTP の設定

この章では、Cisco IE 3000 スイッチで Precision Time Protocol（PTP; 高精度時間プロトコル）を設定する手順について説明します。

PTP の概要

IEEE 1588 標準で定義されている高精度時間プロトコル（PTP）は、ネットワーク内の装置のリアルタイム クロックをナノ秒の精度で同期します。クロックは、マスターメンバー階層に整理されます。PTP は、最も正確なクロックを持つ装置に接続されたスイッチ ポートを識別します。このクロックを、マスター クロックといいます。ネットワーク上の他のすべての装置は、自らのクロックをマスターと同期します。これらの装置を、メンバーといいます。タイミング メッセージを常に交換することにより、継続的な同期を保証します。

PTP は、装置およびテスト機器の動きや精度の制御が重要である工業オートメーション システムやプロセス制御ネットワークで特に有用です。

PTP パケットを通常のマルチキャスト トラフィックとしてスイッチを介して渡すか（転送モード）、すべてのポートをグランド マスター クロックと同期するように（エンドツーエンド トランスペアレント モード）、スイッチをグローバルに設定できます。または、境界クロック モードを設定することも可能です。このモードでは、スイッチが最良のマスター クロックを選択する処理に参加し、さらに優れたクロックが検出されない場合はマスター クロックとして機能することができます。

スイッチが PTP 転送モードまたはエンドツーエンド トランスペアレント モードの場合、PTP モードを別のモードに設定する以外は、PTP 設定を利用できません。スイッチが境界モードの場合は、ポート単位の PTP だけを設定できます。

PTP の設定

デフォルト設定

デフォルトでは、ベース スイッチ モジュールのすべてのファスト イーサネット ポートおよびギガビット イーサネット ポートで PTP がイネーブルになっています。PTP に対応できるのは、ベース スイッチ モジュールのポートだけです。スイッチ拡張モジュールは PTP をサポートしません。すべてのポートにおけるデフォルトの PTP モードは、エンドツーエンド トランスペアレントです。

表 8-1　デフォルトの PTP 設定

機能	デフォルト設定
PTP 境界モード	ディセーブル
PTP 転送モード	ディセーブル
PTP トランスペアレント モード	イネーブル
PTP priority1 および PTP priority2	デフォルトのプライオリティ番号は 128
PTP アナウンス間隔	2 秒
PTP アナウンス タイムアウト	8 秒
PTP 遅延要求間隔	32 秒
PTP 同期間隔	1 秒
PTP 同期制限	500000000 ナノ秒

PTP の設定

PTP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ptp** {**mode** {**boundary** | **e2etransparent** | **forward**} | **priority1** *value* | **priority2** *value*}	同期クロックを設定します。 • スイッチが最良のマスター クロックを選択する作業に参加できるようにするには、**boundary**（境界）モードを選択します。自らのクロックよりも優れたクロックが検出されない場合、スイッチはネットワークのグランドマスター クロックになり、接続しているすべての装置の親クロックになります。最良のマスターがスイッチに接続されたクロックであると判断された場合、スイッチはそのクロックにクロックの子として同期し、他のポートに接続された装置の親クロックとして機能します。最初の同期のあと、スイッチと接続済み装置は、タイミング メッセージを交換して、クロックのオフセットとネットワークの遅延による時間の歪みを修正します。 このモードは、過負荷または重負荷の状態により大きな遅延ジッタが生じるときに使用します。 • スイッチがすべてのスイッチ ポートをスイッチに接続されたグランド マスター クロックと同期できるようにするには、**e2etransparent**（エンドツーエンド トランスペアレント）モードを選択します。これがデフォルトのクロック モードです。スイッチは、スイッチを通過するすべてのパケットが被る遅延（「滞留時間」といいます）を修正します。 このモードでは、境界モードよりもジッタとエラーの蓄積が少なくなります。 • 着信の PTP パケットが通常のマルチキャスト トラフィックとしてスイッチを通過できるようにするには、**forward**（転送）モードを選択します。これにより、境界モードとエンドツーエンド トランスペアレント モードはディセーブルになります。 スイッチ ポートが境界モードの場合は、クロック プライオリティのプロパティを設定します。 • **priority1** 値を指定して、最良のマスター クロックを選択するためのデフォルトの条件（クロック品質、クロック クラスなど）を上書きします。値の小さいほうが優先されます。範囲はどちらも 0 ～ 255 です。デフォルト値は 128 です。 • デフォルトの条件で一致する 2 つの装置間で優先順位を決めるための方法として使用する **priority2** 値を指定します。たとえば、priority2 値を使用して、特定のスイッチが他の同等のスイッチよりも優先されるようにすることができます。範囲はどちらも 0 ～ 255 です。デフォルト値は 128 です。 これらの値により、最良のマスターを選択することを目的とした PTP ネットワークのクロック プライオリティが設定されます。
ステップ 3	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。 スイッチ ポートの番号を入力します。これには、ポート タイプ（ファスト イーサネットの *Fa*、ギガビット イーサネットの *Gi* など）、ベース スイッチ番号（1）、および特定のポート番号が含まれます。たとえば、*Fa1/1* は、ベース スイッチのファスト イーサネット ポート 1 です。

	コマンド	目的
ステップ 4	**ptp** {**announce** {**interval** *value* | **timeout** *value*} | **delay-req interval** *value* | **enable** | **sync** {**interval** *value*| **limit** *value*}}	タイミング メッセージの設定を指定します。これらのオプションは、スイッチが境界モードの場合にのみ使用できます。 • *announce interval* には、アナウンス メッセージを送信するための時間を指定します。指定できる範囲は 0 ～ 4 秒です。デフォルトは 1（2 秒）です。 • *timeout value* には、タイムアウト メッセージをアナウンスするための時間を指定します。指定できる範囲は 2 ～ 10 秒です。デフォルトは 3（8 秒）です。 • *delay request interval* には、ポートがマスター ステートのときに遅延要求メッセージを送信するために、メンバー装置に推奨される時間を指定します。指定できる範囲は –1 ～ 6 秒です。デフォルトは 5（32 秒）です。 • *sync interval* には、同期メッセージを送信するための時間を入力します。入力できる範囲は –1 ～ 1 秒です。デフォルト値は 1 秒です。 • *sync limit* には、PTP が再同期を試みる前の最大クロック オフセット値を指定します。指定できる範囲は 50 ～ 500000000 ナノ秒です。デフォルトは 500000000 ナノ秒です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

PTP 設定の表示

PTP 設定を表示するには、表 8-2 に示す 1 つ以上の特権 EXEC コマンドを使用します。

表 8-2　PTP 設定を表示するためのコマンド

コマンド	目的
show ptp clock	PTP クロック プロパティを表示します。
show ptp foreign-master-record	PTP 外部マスター データセットを表示します。
show ptp parent	親およびグランド マスター プロパティを表示します。
show ptp port	すべての PTP ポート プロパティを表示します。
show ptp FastEthernet *interface*	指定したポートの PTP ファスト イーサネット プロパティを表示します。
show ptp GigabitEthernet *interface*	指定したポートの PTP ギガビット イーサネット プロパティを表示します。
show ptp time-property	PTP 時間プロパティを表示します。

CHAPTER 9

PROFINET の設定

この章では、Cisco IE 3000 スイッチで PROFINET 機能を設定する手順について説明します。

PROFINET の概要

PROFINET は PROFIBUS International（PI）のオープンな工業イーサネット標準であり、オートメーション コントロール用に TCP/IP および IT 標準を使用しています。PROFINET は、装置およびテスト機器の動きや精度の制御が重要である工業オートメーション システムやプロセス制御ネットワークに特に有用です。PROFINET はデータ交換を重視しており、速度要件に合った通信パスを定義しています。PROFINET 通信は、次の 3 つの点でスケーラブルです。

- 標準の非リアルタイム通信では TCP/IP を使用し、約 100 ms のバス サイクル タイムが実現されます。
- リアルタイム通信では、約 10 ms のサイクル タイムが実現されます。
- 等時間隔のリアルタイム通信では、約 1 ms のサイクル タイムが実現されます。

（注） このスイッチでは、等時間隔のリアルタイム通信チャネルはサポートされていません。

PROFINET IO は、分散型オートメーション アプリケーション用のモジュラー通信フレームワークです。PROFINET IO は巡回型のデータ転送を使用して、プログラマブル コントローラ、入力/出力（I/O）装置、およびその他のオートメーション コントローラ（モーション コントローラなど）とデータ、アラーム、診断情報を交換します。

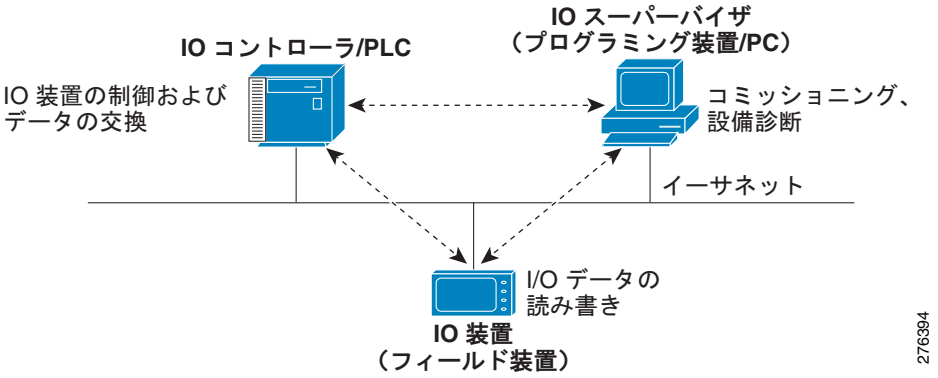
PROFINET IO は、次の 3 つのクラスの装置を認識します。

- IO 装置
- IO コントローラ
- IO スーパーバイザ

PROFINET 装置の役割

図 9-1 に、3 種類の装置の役割を示します。

図 9-1　PROFINET 装置の役割



IO コントローラは IO 装置を制御する Programmable Logic Controller（PLC; プログラマブル ロジック コントローラ）であり、オートメーション プログラムを通して設定、アラーム、IO データなどのデータを交換します。IO コントローラと IO スーパーバイザは診断情報を交換します。IO コントローラは IO 装置と設定や入力/出力情報を共有し、IO 装置からアラームを受信します。

PROFINET は、唯一またはプライマリの管理システムとして使用するよう設計されています。IO コントローラは Discovery and Configuration Protocol（DCP; 検出/コンフィギュレーション プロトコル）でスイッチを検出し、装置名と IP アドレスを設定するため、基本的な設定に Cisco IOS コマンドは必要ありません。拡張設定（QoS や DHCP などの機能）を行うには、スイッチ上で Cisco IOS コマンドを使用する必要があります。PROFINET を使用して、これらの機能の設定はできません。

IO スーパーバイザは Human Machine Interface（HMI; ヒューマン マシン インターフェイス）や PC などのエンジニアリング ステーションであり、コミッショニング、モニタリング、診断分析に使用されます。IO スーパーバイザは IO 装置と診断情報、ステータス情報、制御情報、パラメータ情報を交換します。

IO 装置は、センサー、アクチュエータ、モーション コントローラなどの分散型入力/出力装置です。

（注）　スイッチは IO 装置として動作し、IO コントローラへの PROFINET 管理接続を行います。

PROFINET IO システムでは、バス サイクル タイム 100 ms 未満のオートメーション産業要件を満たすため、すべての IO 装置がイーサネット通信ネットワークを介して通信します。このネットワークでは、データの衝突を避けるため、スイッチと全二重データ交換が使用されます。

PROFINET 装置のデータ交換

PROFINET が DCP を使用してスイッチなどの装置を検出すると、アプリケーション関係（AR）および通信関係（CR）が確立されます。接続が確立され、装置パラメータに関する情報が交換されたら、入力データと出力データが交換されます。スイッチは非リアルタイム CR を使用して、表 9-1 および表 9-2 に示すデータ属性を交換します。

表 9-1　PROFINET IO スイッチ属性

PROFINET IO スイッチ設定属性	値またはアクション
装置名	装置の名前を設定します。
TCP/IP	IP アドレス、サブネット マスク、デフォルト ゲートウェイ、SVI。
プライマリ温度アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
セカンダリ温度アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
RPS 障害アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
CF 障害アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
リレー メジャー アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
リレー マイナー アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
出荷時デフォルトへのリセット	PROFINET IO コントローラを使用して、スイッチを出荷時デフォルトにリセットします。このアクションにより、スタートアップ コンフィギュレーションが削除され、スイッチがリロードされます。
リレー メジャー設定	メジャー リレーをトリガーするポート アラーム（リンク障害など）のタイプを指定します。指定したアラーム タイプで設定された任意のポートがメジャー リレーをトリガーできます。
リレー マイナー設定	マイナー リレーをトリガーするポート アラーム（リンク障害など）のタイプを指定します。指定したアラーム タイプで設定された任意のポートがマイナー リレーをトリガーできます。

表 9-2　PROFINET IO ポート属性

PROFINET IO ポート設定属性	値またはアクション
速度	10、100、1000、自動。
デュプレックス	半二重/全二重/自動。
ポート モード	アクセス/トランク。
VLAN	VLAN 情報。
リンク ステータス	シャットダウン/シャットダウンなし。
設定レートの制限	ブロードキャスト、ユニキャスト、マルチキャストのスレッシュホールドが設定されたレベルを超えています。
ポート リンク障害アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
Port not forwarding アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
Port not operating アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
ポート FCS スレッシュホールド アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。

PROFINET 装置は General Station Description（GSD）ファイルを使用して統合されます。このファイルには、エンジニアリング用のデータや、IO コントローラ、IO スーパーバイザ、および IO 装置（スイッチなど）間のデータ交換用のデータが含まれています。各 PROFINET IO フィールド装置には、装置のプロパティが記述され、設定に必要な次の情報がすべて含まれた GSD ファイルが関連付けられている必要があります。

- 装置 ID 情報（装置 ID、ベンダー ID およびベンダー名、製品ファミリ、ポート数）。
- 着脱可能モジュールの数およびタイプ。

- Cisco IE 3000 8 ポート拡張モジュールはホットスワップ可能ではありません。拡張モジュールの接続や切断を行う前に、スイッチをオフにしてください。
- 診断情報のエラー テキスト。
- IO 装置の通信パラメータ（最小サイクル タイム、リダクション比率、ウォッチ ドッグ タイムなど）。

（注）　Cisco IE 3000 スイッチのデフォルトのリダクション比率は 128 ms ですが、スイッチに複雑な設定を使用する場合は、スイッチの CPU に対する負荷を減らすため、リダクション比率を 256 ms または 512 ms にすることを推奨します。

- IO 装置モジュールに関する設定データ（速度、デュプレックス、VLAN、ポート セキュリティ情報、アラーム、ブロードキャスト レート制限のスレッシュホールドなど）。
- 表 9-2 にリストされた属性に対して設定された、IO 装置モジュールのパラメータ。

GSD ファイルはスイッチに関するものですが、IO スーパーバイザはこのファイルを使用します。

（注）　PROFINET ネットワークを管理するには、スイッチ上の Cisco IOS リリースと関連付けられた GSD ファイルを使用する必要があります。IO スーパーバイザと Cisco IOS ソフトウェアはどちらも、GSD ファイルとスイッチの Cisco IOS ソフトウェア バージョン間の不一致を通知します。

PROFINET の設定

基本的なスイッチ設定には、IO スーパーバイザ上の PROFINET ソフトウェアか Cisco IOS ソフトウェアのいずれかを使用できます。

デフォルト設定

Cisco IOS ソフトウェア リリース 12.2(52)SE 以降、PROFINET はすべてのベース スイッチ モジュールおよび拡張ユニットのイーサネット ポート上で、デフォルトによりイネーブルになっています。PROFINET がディセーブルになっている場合は、「PROFINET のイネーブル化」（P.9-4）の手順に従ってください。

PROFINET のイネーブル化

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**profinet**	スイッチ上で PROFINET をイネーブルにします。

	コマンド	目的
ステップ 3	**profinet id** *line*	（任意）Cisco IOS ソフトウェアを使用して PROFINET 装置 ID を設定します。 最大長は 240 文字です。使用可能な特殊文字はピリオド（.）とハイフン（-）のみです。これらの文字は ID 文字列内の特定のオプションでのみ使用可能です。文字列内には複数のラベルを含めることができます。各ラベルに使用できる文字数は 1 ～ 63 文字です。複数のラベルはピリオド（.）で区切る必要があります。文字列内の末尾文字はゼロ（0）にしないでください。 PROFINET ID の設定の詳細については、PROFINET の仕様、文書番号 TC2-06-0007a、ファイル名 PN-AL-protocol_2722_V22_Oct07 を参照してください（PROFIBUS から入手できます）。
ステップ 4	**profinet vlan** *vlan id*	（任意）VLAN 番号を変更します。デフォルトの VLAN 番号は 1 です。指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチ上で PROFINET をディセーブルにするには、**no profinet** グローバル コンフィギュレーション コマンドを使用します。

PROFINET 設定の表示

show profinet 特権 EXEC コマンドを使用し、表 9-3 に示すキーワードのいずれかを指定します。

表 9-3　PROFINET の設定を表示するためのコマンド

コマンド	目的
show profinet sessions	現在接続されている PROFINET セッションを表示します。
show profinet status	PROFINET サブシステムのステータスを表示します。

PROFINET のトラブルシューティング

PLC の LED はアラームが発生すると赤になり、IO スーパーバイザのソフトウェアはこれらのアラームを反映します。

PROFINET のトラブルシューティングを行うには、**debug profinet** 特権 EXEC コマンドを使用し、表 9-4 に示すキーワードを指定します。**debug** コマンドの出力により、シリアル リンクにエラーが発生する可能性があるので注意してください。これらのコマンドを使用する際には、必ずシスコのテクニカル サポートのエンジニアの指示に従ってください。このコマンドの使用時には、シリアル ポートではなくイーサネットを使用して、Telnet で Cisco IOS の CLI（コマンドライン インターフェイス）にアクセスしてください。

表 9-4　PROFINET の設定をトラブルシューティングするためのコマンド

コマンド	目的
debug profinet alarm	アラーム ステータス（オンまたはオフ）と PROFINET アラームの内容を表示します。
debug profinet cyclic	タイム サイクル ベースの PROFINET イーサネット フレームに関する情報を表示します。
debug profinet error	PROFINET セッション エラーを表示します。
debug profinet packet ethernet	PROFINET イーサネット パケットに関する情報を表示します。
debug profinet packet udp	PROFINET Upper Layer Data Protocol（UDP）パケットに関する情報を表示します。
debug profinet platform	Cisco IOS と PROFINET 間の連携に関する情報を表示します。
debug profinet topology	受信した PROFINET トポロジ パケットを表示します。
debug profinet trace	追跡されたデバッグ出力ログのグループを表示します。

CHAPTER 10

SDM テンプレートの設定

IE 3000 スイッチのコマンド リファレンスに、コマンドの構文と使用方法の情報があります。

SDM テンプレートの概要

Switch Database Management（SDM）テンプレートを使用して、スイッチのシステム リソースを設定し、ネットワークでのスイッチの使用方法に応じて、特定の機能のサポートを最適化できます。一部の機能がシステムを最大限使用するようなテンプレートを選択したり、リソースを均衡化するデフォルト テンプレートを使用したりできます。

Ternary Content Addressable Memory（TCAM; 三値連想メモリ）リソースをさまざまな用途に割り当てるために、スイッチの SDM テンプレートでは、システム リソースに優先順位を付けて特定の機能のサポートを最適化します。次の機能を最適化する SDM テンプレートを選択できます。

- デフォルト：デフォルト テンプレートでは、レイヤ 2 のすべての機能に対してリソースを均衡化します。
- QoS：QoS テンプレートは、Quality Of Service（QoS; サービス品質）の Access Control Entries（ACE; アクセス制御エントリ）に対してシステム リソースを最大限にします。
- ルーティング：ルーティング テンプレートは、IPv4 ユニキャスト ルーティングに対してシステム リソースを最大限にします。通常、これはネットワークの中心にあるルータまたはアグリゲータに必要です。レイヤ 3 機能の IP サービス イメージを実行しているスイッチではルーティング テンプレートを使用する必要があります。

（注） スイッチでルーティング テンプレートを設定するには、Cisco IOS Release 12.2(52)SE 以降を実行している必要があります。

また、デュアル IPv4/IPv6 テンプレートを使用すると、デュアル スタック環境を実現できます。「デュアル IPv4/IPv6 SDM テンプレート」（P.10-2）を参照してください。

表 10-1　各テンプレートに割り当てられた機能のリソースの概算

リソース	デフォルト	QoS	ルーティング
ユニキャスト MAC アドレス	8 K	8 K	2 K
IGMP グループおよびマルチキャスト ルート	256	256	1 K
ユニキャスト ルート	0		4 K
• ホストに直接接続	0		2 K
• 間接ルート	0		2 K
ポリシーベース ルーティング ACE	0		512
QoS 分類 ACE	375	625	625
セキュリティの ACE	375	125	375 K
レイヤ 2 VLAN	1 K	1 K	1 K

この表の先頭から 8 つまでの行（ユニキャスト MAC からセキュリティの ACE まで）は、テンプレートが選択された場合のおおよそのハードウェア境界セットを示しています。ハードウェア リソースのセクションが満杯の場合、処理できないものはすべて CPU に送信されるため、スイッチのパフォーマンスに著しく影響します。最後の行は、スイッチ上のレイヤ 2 VLAN の数に関連するハードウェア リソース消費量を計算する際の目安です。

デュアル IPv4/IPv6 SDM テンプレート

IP バージョン 6（IPv6）をサポートする SDM テンプレートを選択できます。IPv6 の詳細および IPv6 ルーティングの設定方法については、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。

このソフトウェア リリースは、IPv6 トラフィックを転送するときに、Policy-Based Routing（PBR; ポリシーベース ルーティング）をサポートしません。IPv4 PBR は、**dual-ipv4-and-ipv6 routing** テンプレートが設定されている場合にだけサポートされます。

デュアル IPv4/IPv6 テンプレートを使用すると、スイッチをデュアル スタック環境（IPv4 と IPv6 の両方をサポートします）で使用できます。デュアル スタック テンプレートを使用すると、各リソースで使用できる TCAM の容量が少なくなります。IPv4 トラフィックだけを転送する場合は、デュアル スタック テンプレートを使用しないでください。

次の SDM テンプレートは、IPv4/IPv6 環境をサポートします。

- デュアル IPv4/IPv6 デフォルト テンプレート：IPv4 の場合はレイヤ 2、QoS、および ACL をサポートし、IPv6 の場合は、レイヤ 2、IPv6 ホスト、および ACL をサポートします。
- デュアル IPv4/IPv6 ルーティング テンプレート：IPv4 の場合は、レイヤ 2、マルチキャスト、ルーティング（ポリシーベース ルーティングを含む）、QoS、および ACL をサポートし、IPv6 の場合はレイヤ 2、ルーティング、および ACL をサポートします。

（注）　レイヤ 3 IPv6 機能の IP サービス イメージを実行しているスイッチでは、デュアル IPv4/IPv6 ルーティング テンプレートを使用する必要があります。スイッチでルーティング テンプレートを設定するには、Cisco IOS Release 12.2(52)SE 以降を実行している必要があります。

（注）　IPv4 ルートには、1 つの TCAM エントリだけが必要です。IPv6 に使用されているハードウェア圧縮スキームのため、IPv6 ルートでは複数の TCAM エントリを使用して、ハードウェアで転送されるエントリの数を削減できます。たとえば、IPv6 の直接接続された IP アドレスの場合、デスクトップ テンプレートではエントリの数が 2000 未満に制限される場合があります。

表 10-2　デュアル IPv4/IPv6 テンプレートによって許容される機能リソースの概算 [1]

リソース	IPv4/IPv6 のデフォルト設定	IPv4/IPv6 ルーティング
ユニキャスト MAC アドレス	8 K	1 K
IPv4 IGMP グループおよびマルチキャスト ルート	0.25 K	0. 5 K
IPv4 ユニキャスト ルートの合計：	0	2 K
• IPv4 ホストに直接接続	0	1 K
• 間接 IPv4 ルート	0	1 K
IPv6 マルチキャスト グループ	0.375 K	0.625 K
IPv6 ユニキャスト ルートの合計：	0	1.375 K
• 直接接続された IPv6 アドレス	0	1 K
• 間接 IPv6 ユニキャスト ルート	0	0.375 K
IPv4 ポリシー ベース ルーティング ACE	0	0.125 K
IPv4 または MAC QoS ACE（合計）	0.375 K	0.375 K
IPv4 または MAC セキュリティの ACE（合計）	0.375 K	0.125 K
IPv6 ポリシー ベース ルーティング ACE[2]	0	0.125 K
IPv6 QoS ACE	0	0.125 K
IPv6 セキュリティの ACE	0.125 K	0.125 K

1. テンプレートの概算は、8 つのルーティング対象のインターフェイスと約 1000 の VLAN に基づきます。
2. IPv6 ポリシーベース ルーティングはサポートされません。

スイッチ SDM テンプレートの設定

デフォルトの SDM テンプレート

デフォルト テンプレートがデフォルトになります。

SDM テンプレート設定時の注意事項

- SDM テンプレートを選択および設定するときは、設定が有効になるようにスイッチをリロードする必要があります。

- スイッチ上でルーティングがイネーブルになっていない場合、ルーティング テンプレートを使用しないでください。**sdm prefer routing** グローバル コンフィギュレーション コマンドを実行すると、他の機能がルーティング テンプレートのユニキャスト ルーティングに割り当てたメモリを使用するのを防ぐことができます。
- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 機能を設定しようとすると、警告メッセージが表示されます。
- デュアル スタック テンプレートを使用すると、各リソースで許容される TCAM の容量が少なくなるため、IPv4 トラフィックだけを転送する場合は、このテンプレートを使用しないでください。

SDM テンプレートの設定

SDM テンプレートを使用して機能の使用を最大限にするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer** {**default** | **dual-ipv4-and-ipv6** {**default** | **routing**} | **qos** | **routing**}	スイッチで使用する SDM テンプレートを指定します。 キーワードの意味は次のとおりです。 • **default**：すべての機能を均等に動作させます。 • **dual-ipv4-and-ipv6**：IPv4 と IPv6 両方のルーティングをサポートするテンプレートを選択します。 – **default**：IPv4/IPv6 レイヤ 2 とレイヤ 3 の機能を均等に動作させます。 – **routing**：IPv4 ポリシーベース ルーティングを含む IPv4/IPv6 ルーティングの使用率を最大限にします。 • **qos**：QoS ACE のシステム リソースを最大限にします。 • **routing**：スイッチ上の IPv4 ルーティングを最大限にします。 スイッチをデフォルト テンプレートに設定するには、**no sdm prefer** コマンドを使用します。デフォルトのテンプレートは、システム リソースを均等に使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**reload**	オペレーティング システムをリロードします。

システムの再起動後に、**show sdm prefer** 特権 EXEC コマンドを使用して新しいテンプレート設定を確認できます。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** により、使用中のテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

次に、テンプレートを変更しても、スイッチをリロードしていない場合に表示される出力の例を示します。

```
Switch# show sdm prefer
 The current template is "default" template.
The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 1024 VLANs.

number of unicast mac addresses:                  8K
```

```
  number of IPv4 IGMP groups:                        0.25K
  number of IPv4/MAC qos aces:                       0.375k
  number of IPv4/MAC security aces:                  0.375k

 On next reload, template will be "routing" template.
```

デフォルト テンプレートに戻すには、**no sdm prefer** グローバル コンフィギュレーション コマンドを使用します。

次に、ルーティング テンプレートを使用してスイッチを設定する例を示します。

```
Switch(config)# sdm prefer routing
Switch(config)# end
Switch# reload
Proceed with reload?[confirm]
```

次に、スイッチ上でデフォルトのデュアル IPv4/IPv6 テンプレートを設定する例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
Proceed with reload?[confirm]
```

SDM テンプレートの表示

パラメータを指定せずに **show sdm prefer** 特権 EXEC コマンドを使用すると、アクティブなテンプレートが表示されます。

指定したテンプレートでサポートされるリソースの数を表示するには、**show sdm prefer** [**default** | **dual-ipv4-and-ipv6** {**default** | **routing**} **qos** | **routing**] 特権 EXEC コマンドを使用します。

次に、使用中のテンプレートを表示する、**show sdm prefer** コマンドの出力例を示します。

```
Switch# show sdm prefer
 The current template is "default" template.
The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 1024 VLANs.

number of unicast mac addresses:                  8K
  number of IPv4 IGMP groups:                       0.25K
  number of IPv4/MAC qos aces:                      0.375k
  number of IPv4/MAC security aces:                 0.375k
```

次に、**show sdm prefer routing** コマンドの出力例を示します。

```
Switch# show sdm prefer routing
 "routing" template:
The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:                  2K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    4K
    number of directly-connected IPv4 hosts:        2K
    number of indirect IPv4 routes:                 2K
  number of IPv4 policy based routing aces:         0.5K
  number of IPv4/MAC qos aces:                      0.625k
  number of IPv4/MAC security aces:                 0.375k
```

CHAPTER 11

スイッチベース認証の設定

この章では、IE 3000 スイッチでのスイッチベース認証の設定方法について説明します。この章で説明する内容は、次のとおりです。

スイッチへの不正アクセスの防止

認可されていないユーザがスイッチの設定を変更したり、設定情報を表示したりすることを防止できます。通常、ネットワーク管理者にはスイッチへのアクセスを認可し、非同期ポートを通してネットワークの外部からダイヤルしてくるユーザ、シリアル ポートを通してネットワークの外部から接続してくるユーザ、またはローカル 端末またはワークステーションを通してネットワーク内から接続してくるユーザのアクセスは制限します。

スイッチへの不正アクセスを防止するには、次のセキュリティ機能を 1 つ以上設定する必要があります。

- 少なくとも、スイッチのポートごとにパスワードと権限を設定する必要があります。これらのパスワードは、スイッチにローカルに保存されます。ポートまたは回線を通してスイッチにアクセスしようとするユーザは、スイッチにアクセスする前に、そのポートまたは回線に対して指定されているパスワードを入力する必要があります。詳細については、「特権 EXEC コマンドへのアクセス保護」（P.11-2）を参照してください。
- セキュリティのレイヤを追加するには、ユーザ名とパスワードのペアを設定することもできます。この設定はスイッチにローカルに保存されます。これらのペアは回線またはポートに割り当てられ、各ユーザがスイッチにアクセスする前に、ユーザを認証します。権限レベルを定義してある場合は、ユーザ名とパスワードのペアごとに特定の権限レベル（および関連付けられている権利と権限）を割り当てることもできます。詳細については、「ユーザ名とパスワードのペアの設定」（P.11-6）を参照してください。

- ユーザ名とパスワードのペアを使用し、ローカルに保存するのではなくサーバに一元的に保存したい場合は、セキュリティ サーバのデータベースに保存できます。このようにすると、複数のネットワーキング装置が同じデータベースを使用して、ユーザ認証（および必要に応じて認可）の情報を取得できます。詳細については、「TACACS+ でのスイッチ アクセスの制御」（P.11-10）を参照してください。
- また、ログイン拡張機能をイネーブルにすることもできます。この機能は、失敗したログインの試行と成功しなかったログインの試行の両方をログに記録します。ログイン拡張機能は、一定の回数だけログインの試行が失敗したら、それ以降のログインの試行をブロックするように設定することもできます。詳細については、次の URL の『Cisco IOS Login Enhancements』ドキュメントを参照してください。
  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html

特権 EXEC コマンドへのアクセス保護

ネットワーク内の端末アクセスを制御する簡単な方法に、パスワードを使用し、権限レベルを割り当てる方法があります。パスワード保護は、ネットワークまたはネットワーク装置へのアクセスを制限します。権限レベルは、ユーザがネットワーク装置にログインしたあとで入力できるコマンドを定義します。

（注）　この項で使用するコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

- 「パスワードと権限レベルのデフォルト設定」（P.11-2）
- 「スタティック イネーブル パスワードの設定または変更」（P.11-3）
- 「イネーブル パスワードおよびイネーブル シークレット パスワードの暗号化による保護」（P.11-3）
- 「パスワード回復のディセーブル化」（P.11-5）
- 「端末回線への Telnet パスワードの設定」（P.11-6）
- 「ユーザ名とパスワードのペアの設定」（P.11-6）
- 「複数の権限レベルの設定」（P.11-7）

パスワードと権限レベルのデフォルト設定

表 11-1 に、パスワードと権限レベルのデフォルト設定を示します。

表 11-1　デフォルトのパスワードと権限レベル

機能	デフォルト設定
パスワードと権限レベルをイネーブルにする	パスワードは定義されていません。デフォルトはレベル 15（特権 EXEC レベル）です。コンフィギュレーション ファイルではパスワードは暗号化されません。
シークレット パスワードと権限レベルをイネーブルにする	パスワードは定義されていません。デフォルトはレベル 15（特権 EXEC レベル）です。パスワードはコンフィギュレーション ファイルに書き込まれる前に暗号化されます。
回線パスワード	パスワードは定義されていません。

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。スタティック イネーブル パスワードを設定または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** *password*	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトでは、パスワードは定義されていません。 *password* には、1 ～ 25 文字の英数字からなる文字列を指定します。先頭を数字にすることはできず、大文字と小文字の区別があり、スペースは使用できますが先行スペースは無視されます。パスワードを作成するとき、Crtl+v を押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、abc?123 というパスワードを作成するには、次のようにします。 **abc** と入力します。 Crtl+v を押します。 **?123** と入力します。 システムでイネーブル パスワードの入力を求められたときは、疑問符の前に Ctrl+v を押す必要はなく、パスワード プロンプトで単に abc?123 と入力できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。 イネーブル パスワードは暗号化されず、スイッチのコンフィギュレーション ファイルで読むことができます。

パスワードを削除するには、**no enable password** グローバル コンフィギュレーション コマンドを使用します。

次に、イネーブル パスワードを *l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されず、レベル 15（従来の特権 EXEC モード アクセス）へのアクセスを提供します。

```
Switch(config)# enable password l1u2c3k4y5
```

イネーブル パスワードおよびイネーブル シークレット パスワードの暗号化による保護

ネットワークで送受信されるパスワードまたは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存されるパスワードについて、セキュリティをさらに強化するには、**enable password** または **enable secret** グローバル コンフィギュレーション コマンドを使用します。どちらのコマンドも同じことを行います。つまり、ユーザが特権 EXEC モード（デフォルト）または指定されている権限レベルにアクセスするために入力する必要がある暗号化されたパスワードを設定できます。

enable secret コマンドは改善された暗号化アルゴリズムを使用するので、こちらのコマンドを使用することを推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドをイネーブルにすることはできません。

イネーブル パスワードおよびイネーブル シークレット パスワードの暗号化を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted*-password} または **enable secret** [**level** *level*] {*password* | *encryption-type encrypted*-password}	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 または 不可逆的な暗号化方式を使用して保存される、シークレット パスワードを定義します。 • （任意）*level* に指定できる範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モード権限です。デフォルトのレベルは 15（特権 EXEC モード権限）です。 • *password* には、1 ～ 25 文字の英数字からなる文字列を指定します。先頭を数字にすることはできず、大文字と小文字の区別があり、スペースは使用できますが先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。 • （任意）*encryption-type* には、シスコ独自の暗号化アルゴリズムを示すタイプ 5 だけを指定できます。暗号化タイプを指定する場合は、暗号化パスワード（別のスイッチの設定からコピーした暗号化パスワード）を指定する必要があります。 **（注）** 暗号化タイプを指定してから、クリア テキストのパスワードを入力すると、特権 EXEC モードを再び開始することができなくなります。暗号化パスワードを忘れた場合は、どのような方法でも回復できません。
ステップ 3	**service password-encryption**	（任意）パスワードを定義するとき、または設定を書き込むときに、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

イネーブル パスワードとイネーブル シークレット パスワードの両方が定義されている場合は、ユーザはイネーブル シークレット パスワードを入力する必要があります。

特定の権限レベルに対するパスワードを定義するには、**level** キーワードを使用します。レベルを指定してパスワードを設定したあと、権限レベルにアクセスする必要があるユーザだけに、パスワードを通知してください。各レベルでアクセスできるコマンドを指定するには、**privilege level** グローバル コンフィギュレーション コマンドを使用します。詳細については、「複数の権限レベルの設定」（P.11-7）を参照してください。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブル コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

パスワードとレベルを削除するには、**no enable password** [**level** *level*] または **no enable secret** [**level** *level*] のいずれかのグローバル コンフィギュレーション コマンドを使用します。パスワードの暗号化をディセーブルにするには、**no service password-encryption** グローバル コンフィギュレーション コマンドを使用します。

次に、権限レベル 2 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

パスワード回復のディセーブル化

デフォルトでは、スイッチに物理的にアクセスできるエンド ユーザは、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを失った状態から回復できます。

パスワード回復ディセーブル機能は、この機能の一部をディセーブルにすることで、スイッチのパスワードへのアクセスを保護します。この機能をイネーブルにすると、エンド ユーザは、システムをデフォルトの設定に戻すことに同意した場合にだけ、起動プロセスを中断できます。パスワード回復をディセーブルにすることにより、ユーザは起動プロセスを中断してパスワードを変更できますが、コンフィギュレーション ファイル（config.text）と VLAN データベース ファイル（vlan.dat）は削除されます。

（注） パスワード回復をディセーブルにする場合は、エンド ユーザが起動プロセスを中断してシステムの設定をデフォルト値に戻す場合に備えて、コンフィギュレーション ファイルのバックアップ コピーをセキュア サーバに保存することを推奨します。スイッチにはコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。スイッチが VTP トランスペアレント モードで動作している場合は、VLAN データベース ファイルのバックアップ コピーもセキュア サーバに保存することを推奨します。スイッチがデフォルトのシステム設定に戻されたときは、Xmodem プロトコルを使用して、保存されているファイルをスイッチにダウンロードできます。詳細については、「パスワードを忘れた場合の回復」（P.52-3）を参照してください。

パスワード回復をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no service password-recovery**	パスワード回復をディセーブルにします。 この設定はフラッシュ メモリ内のブート ローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、この領域はファイル システムの一部ではないので、ユーザはアクセスできません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show version**	コマンド出力の最後の数行を調べて、設定を確認します。

パスワード回復を再びイネーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

（注） **boot manual** グローバル コンフィギュレーション コマンドを使用してスイッチを手動で起動するように設定している場合は、パスワード回復のディセーブル化はできません。このコマンドを実行すると、スイッチの電源をオフ / オンしたあとで、ブート ローダのプロンプト（*switch:*）が表示されます。

端末回線への Telnet パスワードの設定

スイッチの電源を初めて入れると、自動セットアップ プログラムが実行して、IP 情報を割り当て、継続的な使用のためのデフォルト設定を作成します。セットアップ プログラムでは、パスワードを使用して Telnet にアクセスするようにスイッチを設定することも求められます。セットアップ プログラムでこのパスワードを設定しなかった場合は、CLI（コマンドライン インターフェイス）を使用して設定できます。

Telnet アクセス用にスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		エミュレーション ソフトウェアがインストールされている PC またはワークステーションを、スイッチのコンソール ポートに接続します。 コンソール ポートのデフォルトのデータ特性は、9600、8、1、パリティなしです。コマンドライン プロンプトを表示するため、Return キーを数回押す必要がある場合があります。
ステップ 2	**enable password** *password*	特権 EXEC モードを開始します。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**line vty 0 15**	Telnet セッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。 コマンド対応スイッチで使用できるセッションの数は 16 です。0 および 15 は、使用可能な 16 の Telnet セッションをすべて設定することを意味します。
ステップ 5	**password** *password*	回線の Telnet パスワードを入力します。 *password* には、1 ～ 25 文字の英数字からなる文字列を指定します。先頭を数字にすることはできず、大文字と小文字の区別があり、スペースは使用できますが先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。 パスワードが **line vty 0 15** コマンドの下に表示されます。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

パスワードを削除するには、**no password** グローバル コンフィギュレーション コマンドを使用します。

次に、Telnet パスワードを *let45me67in89* に設定する例を示します。

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

ユーザ名とパスワードのペアの設定

ユーザ名とパスワードのペアを設定できます。この設定はスイッチにローカルに保存されます。これらのペアは回線またはポートに割り当てられ、各ユーザがスイッチにアクセスする前に、ユーザを認証します。権限レベルを定義してある場合は、ユーザ名とパスワードのペアごとに特定の権限レベル（および関連付けられている権利と権限）を割り当てることもできます。

ログイン ユーザ名とパスワードを要求するユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ユーザごとにユーザ名、権限レベル、およびパスワードを入力します。 • *name* には、ユーザ ID として 1 語を指定します。スペースおよび引用符は使用できません。 • （任意）*level* には、ユーザがアクセスしたあとで割り当てられる権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 は特権 EXEC モード アクセスです。レベル 1 はユーザ EXEC モード アクセスです。 • *encryption-type* には、暗号化されていないパスワードが後ろに続くことを指定する場合は 0 を入力します。非表示パスワードが後ろに続くことを指定する場合は 7 を入力します。 • *password* には、スイッチにアクセスするためにユーザが入力する必要があるパスワードを指定します。パスワードは 1 ～ 25 文字でなければならず、間にスペースを含むことができ、**username** コマンドで最後に指定するオプションである必要があります。
ステップ 3	**line console 0** または **line vty 0 15**	ライン コンフィギュレーション モードを開始し、コンソール ポート（回線 0）または VTY 回線（回線 0 ～ 15）を設定します。
ステップ 4	**login local**	ログイン時のローカル パスワード検査をイネーブルにします。認証は、ステップ 2 で指定したユーザ名に基づきます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

特定のユーザのユーザ名認証をディセーブルにするには、**no username** *name* グローバル コンフィギュレーション コマンドを使用します。パスワード検査をディセーブルにし、パスワードを入力しないで接続できるようにするには、**no login** ライン コンフィギュレーション コマンドを使用します。

複数の権限レベルの設定

Cisco IOS ソフトウェアには、パスワード セキュリティのモードがデフォルトで 2 つあります。ユーザ EXEC モードと特権 EXEC モードです。各モードに、最大 16 個の階層レベルからなるコマンドを設定することができます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

たとえば、多くのユーザが **clear line** コマンドにアクセスできるようにするには、このコマンドにレベル 2 セキュリティを割り当て、レベル 2 パスワードを幅広く配布します。一方、**configure** コマンドにアクセスできるユーザを限定したい場合には、このコマンドにレベル 3 セキュリティを割り当て、限られたユーザ グループだけにパスワードを配布します。

ここでは、次の設定情報について説明します。

コマンドの権限レベルの設定

コマンド モードの権限レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**privilege** *mode* **level** *level command*	コマンドの権限レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合は **configure**、EXEC モードの場合は **exec**、インターフェイス コンフィギュレーション モードの場合は **interface**、ライン コンフィギュレーション モードの場合は **line** をそれぞれ入力します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって認可されるアクセスのレベルです。 • *command* には、アクセスを制限するコマンドを指定します。
ステップ 3	**enable password level** *level password*	権限レベルに対するイネーブル パスワードを指定します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モード権限です。 • *password* には、1 ～ 25 文字の英数字からなる文字列を指定します。先頭を数字にすることはできず、大文字と小文字の区別があり、スペースは使用できますが先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	設定を確認します。 最初のコマンドは、パスワードおよびアクセス レベルの設定を表示します。2 番めのコマンドは、権限レベルの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

コマンドを権限レベルに設定すると、構文がそのコマンドのサブセットであるすべてのコマンドも、そのレベルに設定されます。たとえば、**show ip traffic** コマンドをレベル 15 に設定した場合、**show** コマンドや **show ip** コマンドも、別のレベルに個別に設定しない限り、権限レベル 15 に自動的に設定されます。

特定のコマンドをデフォルトの権限に戻すには、**no privilege** *mode* **level** *level command* グローバル コンフィギュレーション コマンドを使用します。

次に、**configure** コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用するためにユーザが入力する必要があるパスワードとして *SecretPswd14* を定義する例を示します。

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

回線のデフォルト権限レベルの変更

回線のデフォルトの権限レベルを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line vty** *line*	アクセスを制限する仮想端末回線を選択します。
ステップ 3	**privilege level** *level*	回線のデフォルトの権限レベルを変更します。 *level* に指定できる範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって認可されるアクセスのレベルです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	設定を確認します。 最初のコマンドは、パスワードおよびアクセス レベルの設定を表示します。2 番めのコマンドは、権限レベルの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ユーザは、回線にログインして別の権限レベルをイネーブルにすることで、**privilege level** ライン コンフィギュレーション コマンドを使用して設定した権限レベルを上書きできます。**disable** コマンドを使用すると、権限レベルを下げることができます。ユーザが高い権限レベルのパスワードを知っている場合は、そのパスワードを使用して、より高い権限レベルをイネーブルにできます。コンソール回線で回線の使用を制限するために、高レベルまたは権限レベルを指定する場合があります。

デフォルトの回線権限レベルに戻すには、**no privilege level** ライン コンフィギュレーション コマンドを使用します。

権限レベルへのログインと終了

指定した権限レベルにログインしたり、指定した権限レベルを終了したりするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**enable** *level*	指定した権限レベルにログインします。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable** *level*	指定した権限レベルを終了します。 *level* に指定できる範囲は 0 ～ 15 です。

TACACS+ でのスイッチ アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus（TACACS+）をイネーブルにして設定する方法を説明します。TACACS+ は詳細なアカウント情報を提供し、認証と認可のプロセスの管理を柔軟に制御できます。TACACS+ は、Authentication、Authorization、Accounting（AAA; 認証、認可、アカウンティング）によって促進され、AAA コマンドによってだけイネーブルにすることができます。

（注）　この項で使用しているコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

- 「TACACS+ の概要」（P.11-10）
- 「TACACS+ の動作」（P.11-12）
- 「TACACS+ の設定」（P.11-12）
- 「TACACS+ の設定の表示」（P.11-17）

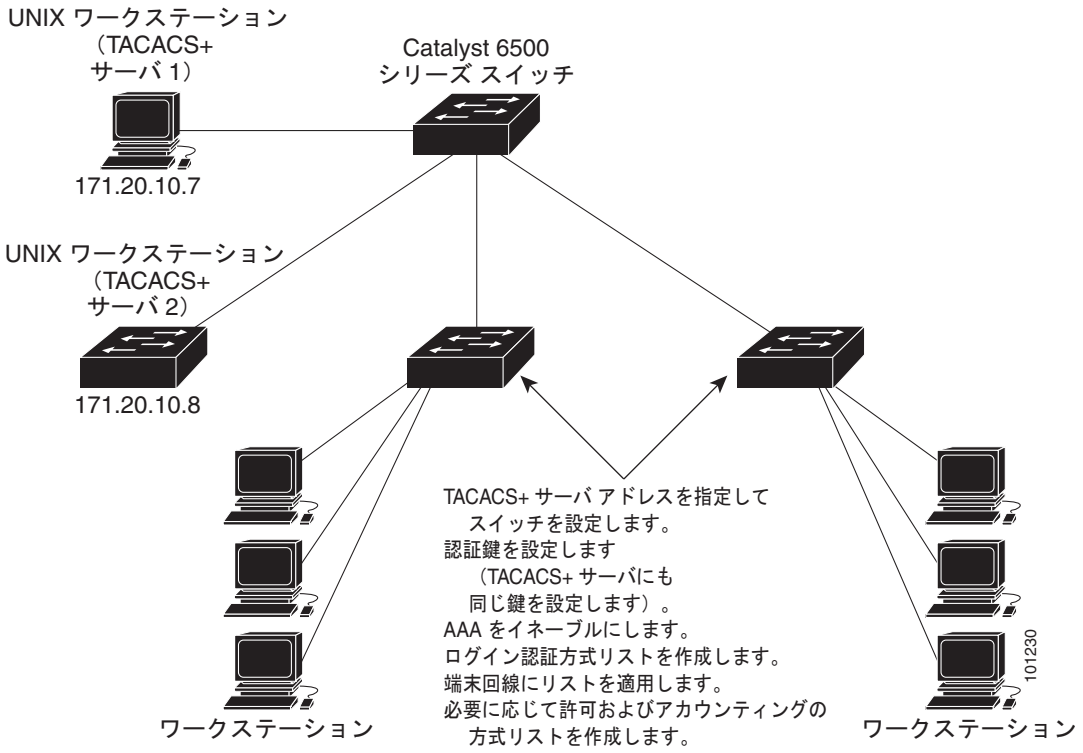
TACACS+ の概要

TACACS+ は、スイッチにアクセスを試みるユーザの検証を一元的に行うセキュリティ アプリケーションです。TACACS+ サービスは TACACS+ デーモンのデータベースで維持され、デーモンは通常は UNIX または Windows NT のワークステーション上で実行します。スイッチで TACACS+ の機能を設定するには、TACACS+ サーバにアクセスし、TACACS+ サーバを設定しておく必要があります。

TACACS+ は、独立したモジュール形式の認証、認可、アカウンティングの機能を備えています。TACACS+ では、単一のアクセス制御サーバ（TACACS+ デーモン）で、認証、認可、アカウンティングの各サービスを個別に提供できます。各サービスは専用のデータベースに結びつけられており、デーモンの機能に応じて、同じサーバ上またはネットワーク上で使用可能な他のサービスを利用できます。

TACACS+ の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理するための手段を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともに、ネットワーク アクセス サーバとして機能することができます。ネットワーク アクセス サーバは、図 11-1 で示すように、個別のユーザ、ネットワークまたはサブネットワーク、および相互接続されたネットワークへの接続を提供します。

図 11-1　一般的な TACACS+ ネットワークの設定



AAA セキュリティ サービスによって管理された TACACS+ は、次のサービスを提供できます。

- 認証：ログインおよびパスワード ダイアログ、チャレンジ アンド レスポンス、およびメッセージング サポートを通して、認証の完全な制御を提供します。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードを提供されたあとで、自宅の住所、母親の旧姓、サービスのタイプ、社会保障番号などの質問で、ユーザの身元を確認できます）。TACACS+ の認証サービスは、ユーザの画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期限ポリシーのためにパスワードを変更する必要があることを、メッセージでユーザに通知できます。

- 認可：自動コマンド、アクセス制御、セッション期間、プロトコル サポートなどの設定をはじめとする、ユーザのセッションの間のさまざまなユーザ機能を、きめ細かく制御できます。また、ユーザが実行できるコマンドを TACACS+ の認可機能で制限することもできます。

- アカウンティング：課金、監査、レポートに使用する情報を収集し、TACACS+ デーモンに送信できます。ネットワーク マネージャは、アカウンティング機能を使用して、セキュリティ監査のためにユーザのアクティビティを追跡したり、ユーザ課金のための情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始および終了時刻、実行したコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間の認証を提供します。スイッチと TACACS+ デーモンの間でのプロトコル交換はすべて暗号化されるので、機密性が保証されます。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアを実行するシステムが必要です。

TACACS+ の動作

ユーザが TACACS+ を使用してスイッチの認証を受けることで簡単な ASCII ログインを試みると、次の処理が行われます。

1. 接続が確立されると、スイッチは TACACS+ デーモンと通信し、ユーザに対して表示するユーザ名プロンプトを取得します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンと通信してパスワード プロンプトを取得します。スイッチがユーザに対してパスワード プロンプトを表示し、ユーザがパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

   デーモンがユーザを認証するために十分な情報を受け取るまで、TACACS+ はデーモンとユーザの間の対話を許可します。デーモンはユーザ名とパスワードの組み合わせの入力を求めますが、ユーザの母親の旧姓のような他の項目を含めることもできます。

2. スイッチは最終的に、次の応答のいずれかを TACACS+ デーモンから受け取ります。

   - ACCEPT：ユーザは認証され、サービスを開始できます。認可を必要とするようにスイッチが設定されている場合は、この時点で認可が開始します。
   - REJECT：ユーザは認証されませんでした。TACACS+ デーモンに応じて、ユーザのアクセスを拒否することも、ログイン シーケンスを再試行するようユーザに求めることもできます。
   - ERROR：デーモンとの認証の間のある時点で、またはデーモンとスイッチの間のネットワーク接続で、エラーが発生しました。ERROR 応答を受け取ったスイッチは、通常、代替方法を使用してユーザの認証を試みます。
   - CONTINUE：ユーザに追加の認証情報の入力を求めます。

   認証のあと、スイッチで認可がイネーブルになっている場合は、ユーザに対して追加の認可フェーズが実行されます。ユーザは、まず TACACS+ による認証が正常に完了してからでないと、TACACS+ による認可に進むことはできません。

3. TACACS+ による認可が必要な場合は、再び TACACS+ デーモンと通信し、認可に対する ACCEPT または REJECT の応答を受け取ります。ACCEPT 応答が返される場合、応答には、そのユーザに対する EXEC または NETWORK セッションを指示する属性、およびユーザがアクセスできるサービスの形式でデータが含まれます。これには、次のものがあります。

   - Telnet、Secure Shell（SSH; セキュア シェル）、rlogin、または特権 EXEC の各サービス
   - ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

TACACS+ の設定

ここでは、TACACS+ をサポートするようにスイッチを設定する方法を説明します。少なくとも、TACACS+ デーモンを維持するホストを識別し、TACACS+ による認証の方式リストを定義する必要があります。必要に応じて、TACACS+ による認可とアカウンティングの方式リストも定義できます。方式リストでは、ユーザの認証、認可、またはアカウントの保持に使用する手順と方式を定義します。方式リストを使用して、使用する 1 つまたは複数のセキュリティ プロトコルを指定でき、これにより、最初の方式が失敗した場合のバックアップ システムを設定できます。ソフトウェアは、リスト内の最初の方式を使用して、ユーザの認証、認可、またはアカウントの保持を行います。その方式が応答しない場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リストの方式による通信が成功するか、方式をすべて試し終わるまで繰り返されます。

ここでは、次の設定情報について説明します。

- 「TACACS+ のデフォルト設定」（P.11-13）
- 「TACACS+ サーバ ホストの識別と認証キーの設定」（P.11-13）
- 「TACACS+ ログイン認証の設定」（P.11-14）
- 「特権 EXEC アクセスおよびネットワーク サービスに対する TACACS+ による認可の設定」（P.11-16）
- 「TACACS+ によるアカウンティングの開始」（P.11-17）

TACACS+ のデフォルト設定

TACACS+ と AAA はデフォルトではディセーブルになっています。

セキュリティの問題を防ぐため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。イネーブルにすると、TACACS+ は CLI を使用してスイッチにアクセスするユーザを認証できます。

（注）　TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定されている HTTP 接続を認証します。

TACACS+ サーバ ホストの識別と認証キーの設定

単一のサーバまたは AAA サーバ グループを使用して既存のサーバ ホストを認証用にグループ化するように、スイッチを設定できます。サーバをグループ化することで、設定済みサーバ ホストのサブセットを選択し、それを特定のサービスに対して使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されているサーバ ホストの IP アドレスのリストを含みます。

IP ホストまたは TACACS+ サーバを維持するホストを識別し、必要に応じて暗号キーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	IP ホストまたは TACACS+ サーバを維持するホストを識別します。優先されるホストのリストを作成するには、このコマンドを複数回入力します。ソフトウェアは、ここで指定した順序でホストを検索します。 • *hostname* には、ホストの名前または IP アドレスを指定します。 • （任意）**port** *integer* には、サーバのポート番号を指定します。デフォルト値はポート 49 です。指定できる範囲は 1 ～ 65535 です。 • （任意）**timeout** *integer* には、スイッチが時間切れになってエラーを宣言するまでデーモンからの応答を待機する時間（秒単位）を指定します。デフォルト値は 5 秒です。指定できる範囲は 1 ～ 1000 秒です。 • （任意）**key** *string* には、スイッチと TACACS+ デーモンの間のすべてのトラフィックの暗号化と暗号化解除に使用する暗号キーを指定します。暗号化が成功するためには、TACACS+ デーモンでも同じキーを設定する必要があります。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 4	**aaa group server tacacs+** *group-name*	（任意）グループ名を指定して AAA のサーバ グループを定義します。 このコマンドは、スイッチをサーバ グループ サブコンフィギュレーション モードにします。
ステップ 5	**server** *ip-address*	（任意）特定の TACACS+ サーバと定義したサーバ グループを関連付けます。AAA サーバ グループ内の TACACS+ サーバごとに、このステップを繰り返します。 グループ内の各サーバは、ステップ 2 で先に定義しておく必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show tacacs**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定した TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host** *hostname* グローバル コンフィギュレーション コマンドを使用します。コンフィギュレーション リストからサーバ グループを削除するには、**no aaa group server tacacs+** *group-name* グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、**no server ip-address** サーバ グループ サブコンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義したあと、そのリストをさまざまなポートに適用します。方式リストでは、実行する認証のタイプと、実行する手順を定義します。定義した認証方式を実行するには、特定のポートにリストを適用する必要があります。唯一の例外はデフォルトの方式リストです（名前は *default* です）。方式の名前付きリストが明示的に定義されているポート以外のすべてのポートには、デフォルトの方式リストが自動的に適用されます。定義された方式リストは、デフォルトの方式リストよりも優先されます。

方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定でき、これにより、最初の方式が失敗した場合の認証のバックアップ システムを設定できます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合、つまりセキュリティ サーバまたはローカル ユーザ名データベースがユーザ アクセスを拒否する応答を返した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前を示す文字列を指定します。 • *method1...* には、認証アルゴリズムが試みる実際の方式を指定します。追加の認証方式は、前の認証方式が失敗した場合ではなく、エラーを返した場合にだけ使用されます。 次のいずれかの方式を選択します。 • **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、**enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 • **group tacacs+**：TACACS+ による認証を使用します。この認証方式を使用するには、TACACS+ サーバを設定しておく必要があります。詳細については、「TACACS+ サーバ ホストの識別と認証キーの設定」（P.11-13）を参照してください。 • **line**：回線パスワードを認証に使用します。この認証方式を使用するには、回線パスワードを定義しておく必要があります。そのためには、**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。そのためには、**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **local-case**：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用して、データベースにユーザ名情報を入力する必要があります。 • **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストを 1 つまたは複数の回線に適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成されるデフォルト リストが使用されます。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに対して TACACS+ による認証をディセーブルにするか、またはデフォルト値に戻すには、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

（注）　AAA 方式を使用して HTTP アクセスに対してスイッチを保護するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、スイッチは AAA 方式で HTTP アクセスに対して保護されません。

ip http authentication コマンドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

特権 EXEC アクセスおよびネットワーク サービスに対する TACACS+ による認可の設定

AAA 認可は、ユーザが使用できるサービスを制限します。AAA 認可をイネーブルにすると、スイッチは、ローカル ユーザ データベースまたはセキュリティ サーバにあるユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイルの情報によって許可される場合にだけ、要求したサービスにアクセスできます。

ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定するには、**aaa authorization** グローバル コンフィギュレーション コマンドで **tacacs+** キーワードを指定します。

aaa authorization exec tacacs+ local コマンドは、次の認可パラメータを設定します。

- 認証が TACACS+ を使用して実行された場合、特権 EXEC アクセスの認可には TACACS+ を使用します。
- 認証に TACACS+ が使用されなかった場合は、ローカル データベースを使用します。

（注）　認可が設定されている場合でも、CLI を使用してログインする認証済みのユーザに対しては、認可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに対して TACACS+ による認可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network tacacs+**	ネットワーク関連サービスのすべての要求に対してユーザを TACACS+ で認可するようにスイッチを設定します。
ステップ 3	**aaa authorization exec tacacs+**	ユーザが特権 EXEC アクセスを行っている場合はユーザを TACACS+ で認可するようにスイッチを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

認可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ によるアカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスしているサービス、およびユーザが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザのアクティビティをアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングに関する Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに保存されます。このデータを分析し、ネットワーク管理、クライアント課金、または監査に利用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに対して TACACS+ によるアカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa accounting network start-stop tacacs+**	すべてのネットワーク関連サービス要求に対して TACACS+ によるアカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop tacacs+**	特権 EXEC プロセスの開始時に start-record アカウンティング通知を送信し、終了時に stop-record を送信するように、TACACS+ によるアカウンティングをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

AAA サーバが到達不能のときのセッション確立

aaa accounting system guarantee-first コマンドによって、システム アカウンティングが最初のレコードになります。これは、デフォルトの状態です。システムのリロード（場合によっては 3 分以上かかることがある）が行われるまで、ユーザがコンソールまたは端末接続でセッションを開始できないことがあります。

ルータがリロードされたときに AAA サーバが到達不能の場合、ルータとコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

TACACS+ の設定の表示

TACACS+ サーバの統計情報を表示するには、**show tacacs** 特権 EXEC コマンドを使用します。

RADIUS でのスイッチ アクセスの制御

ここでは、RADIUS をイネーブルにして設定する方法を説明します。RADIUS は詳細なアカウント情報を提供し、認証と認可のプロセスの管理を柔軟に制御できます。RADIUS は、AAA によって促進され、AAA コマンドによってだけイネーブルにすることができます。

（注）　この項で使用するコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

- 「RADIUS の概要」（P.11-18）
- 「RADIUS の動作」（P.11-19）
- 「RADIUS Change of Authorization」（P.11-20）
- 「RADIUS の設定」（P.11-25）
- 「RADIUS の設定の表示」（P.11-38）

RADIUS の概要

RADIUS は、不正アクセスに対してネットワークを保護する分散クライアント/サーバ システムです。RADIUS クライアントは、サポートされる Cisco ルータおよびスイッチで動作します。クライアントは、認証要求を中央の RADIUS サーバに送信します。サーバには、ユーザの認証とネットワーク サービス アクセスに関するすべての情報が存在します。RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server Version 3.0）、Livingston、Merit、Microsoft、またはその他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。

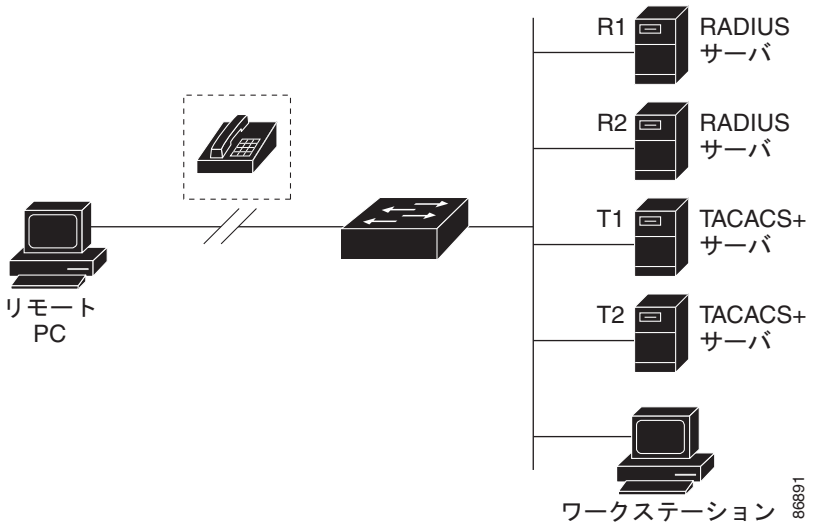
RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- 複数のベンダーのアクセス サーバが存在し、各サーバが RADIUS をサポートしているネットワーク。たとえば、複数のベンダーのアクセス サーバが、単一の RADIUS サーバベースのセキュリティ データベースを使用しているような場合です。複数のベンダーのアクセス サーバが存在する IP ベースのネットワークでは、ダイヤルイン ユーザは、Kerberos セキュリティ システムで動作するようにカスタマイズされた RADIUS サーバを使って認証されます。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。*スマート カード*アクセス制御システムを使用するアクセス環境などです。たとえば、RADIUS を Enigma のセキュリティ カードとともに使用して、ユーザを検証し、ネットワーク リソースへのアクセスを許可するような場合です。
- すでに RADIUS を使用しているネットワーク。RADIUS クライアントを含む Cisco スイッチをネットワークに追加できます。TACACS+ サーバに移行するときの最初のステップになる場合があります。図 11-2（P.11-19）を参照してください。
- ユーザがただ 1 つのサービスにアクセスする必要のあるネットワーク。RADIUS を使用すると、シングル ホスト、Telnet などの単一のユーティリティ、または IEEE 802.1x などのプロトコルを介したネットワークへのユーザ アクセスを制御できます。このプロトコルの詳細については、第 12 章「IEEE 802.1X ポートベースの認証の設定」を参照してください。
- リソースのアカウンティングが必要なネットワーク。RADIUS による認証または認可とは独立して、RADIUS によるアカウンティングを使用できます。RADIUS のアカウンティング機能を使用すると、サービスの開始時と終了時にデータを送信し、セッションの間に使用されたリソースの量（時間、パケット、バイトなど）を表示できます。インターネット サービス プロバイダーは、フリーウェアベース バージョンの RADIUS アクセス制御およびアカウンティング ソフトウェアを使用して、セキュリティや課金に関する特別なニーズを満たすことができます。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコルのアクセス環境。RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD による接続はサポートしません。
- スイッチ間またはルータ間の状況。RADIUS は双方向の認証には対応していません。RADIUS は、非シスコ デバイスが認証を必要とする場合に、ある装置から非シスコ デバイスへの認証を行うために使用できます。
- さまざまなサービスを使用するネットワーク。通常、RADIUS はユーザを 1 つのサービス モデルにバインドします。

図 11-2　RADIUS から TACACS+ サービスへの移行



RADIUS の動作

ユーザがログインし、RADIUS サーバでアクセス制御されているスイッチによる認証を試みると、次の処理が行われます。

1. ユーザは、ユーザ名とパスワードの入力を求められます。
2. ユーザ名と暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、次のいずれかの応答を RADIUS サーバから受け取ります。
   a. ACCEPT：ユーザは認証されます。
   b. REJECT：ユーザは、認証されずユーザ名とパスワードの再入力を求められるか、またはアクセスを拒否されます。
   c. CHALLENGE：チャレンジのためユーザからのデータがさらに必要です。
   d. CHALLENGE PASSWORD：応答はユーザに新しいパスワードの選択を要求しています。

ACCEPT または REJECT 応答は、特権 EXEC またはネットワーク認可に使用される追加データとバンドルされます。ユーザは、まず RADIUS による認証が正常に完了してからでないと、RADIUS による認可に進むことはできません（イネーブルになっている場合）。ACCEPT または REJECT パケットに含まれる追加データとしては次のものがあります。

- Telnet、SSH、rlogin、または特権 EXEC の各サービス
- ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

RADIUS Change of Authorization

ここでは、使用できるプリミティブなどの RADIUS インターフェイスの概要、および Change of Authorization（CoA）の間におけるその使用方法について説明します。

概要

標準的な RADIUS インターフェイスは、通常はプル モデルで使用されます。つまり、要求はネットワークに接続された装置から送信されて、応答はクエリー対象のサーバから返送されます。Catalyst スイッチは、RFC 5176 で定義されている RADIUS Change of Authorization（CoA）拡張機能をサポートします。この機能は通常はプッシュ モデルで使用され、外部の認証、認可、アカウンティング（AAA）サーバまたはポリシー サーバからのセッションのダイナミックな再設定に対応しています。

Cisco IOS Release 12.2(52)SE 以降、スイッチは次のセッション単位の CoA 要求をサポートしています。

- セッションの再認証
- セッションの終了
- セッションの終了とポートのシャットダウン
- セッションの終了とポートのバウンス

この機能は、Cisco Secure Access Control Server（ACS）5.1 に統合されています。ACS の詳細については、次の URL を参照してください。
http://cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html

Catalyst スイッチでは、RADIUS インターフェイスはデフォルトでイネーブルになっています。ただし、次の属性についていくつか基本的な設定が必要です。

- セキュリティとパスワード：『*Catalyst 3750 Switch Software Configuration Guide, Cisco Release 12.2(50)SE*』の「Configuring Switch-Based Authentication」の章の「Preventing Unauthorized Access to Your Switch」の項を参照してください。
- アカウンティング：『*Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE*』の「Configuring Switch-Based Authentication」の章の「Starting RADIUS Accounting」の項を参照してください。

Change-of-Authorization 要求

RFC 5176 で説明されているように、Change of Authorization (CoA) 要求は、セッションの識別、ホストの再認証、およびセッションの終了に対応するために、プッシュ モデルで使用されます。このモデルは、1 つの要求（CoA-Request）と 2 つの応答コードで構成されます。

- CoA 確認応答（ACK）[CoA-ACK]
- CoA 非確認応答（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS サーバまたはポリシー サーバ）から送信され、リスナーとして機能するスイッチに送られます。

ここでは、次の内容について説明します。

- 「CoA 要求の応答コード」
- 「CoA 要求コマンド」
- 「セッションの再認証」

RFC 5176 への準拠

Disconnect Request メッセージは、Packet of Disconnect（POD; パケット オブ ディスコネクト）とも呼ばれ、セッションを終了するためにスイッチによってサポートされます。

表 11-2 に、この機能のためにサポートされる Internet Engineering Task Force（IETF）属性を示します。

表 11-2　サポートされる IETF 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

表 11-3 に、Error-Cause 属性に設定される可能性のある値を示します。

表 11-3　Error-Cause の値

値	説明
201	残余セッション コンテキストが削除された
202	無効な EAP パケット（無視）
401	サポートされない属性
402	属性なし
403	NAS ID 不一致
404	無効な要求
405	サポートされないサービス
406	サポートされない拡張
407	無効な属性値
501	管理上禁止
502	要求をルーティングできない（プロキシ）
503	セッション コンテキストが見つからない
504	セッション コンテキストを削除できない
505	その他のプロキシ処理エラー
506	リソースを使用できない
507	要求が開始された
508	複数のセッションの選択はサポートされていない

前提条件

CoA インターフェイスを使用するには、セッションがすでにスイッチに存在している必要があります。CoA は、セッションを識別して接続解除要求を適用するために使用できます。更新は指定したセッションに対してだけ反映されます。

CoA 要求の応答コード

CoA 要求の応答コードを使用して、コマンドをスイッチに渡すことができます。表 11-4（P.11-23）に、サポートされるコマンドを示します。

セッションの識別

特定のセッションを対象とする接続解除要求および CoA 要求の場合、スイッチは次の属性の 1 つまたは複数に基づいてセッションを特定します。

- Calling-Station-Id（ホストの MAC アドレスを含む IETF 属性 31）
- Audit-Session-Id（Cisco Vendor-Specific Attribute（VSA; ベンダー固有属性））
- Acct-Session-Id（IETF 属性 44）

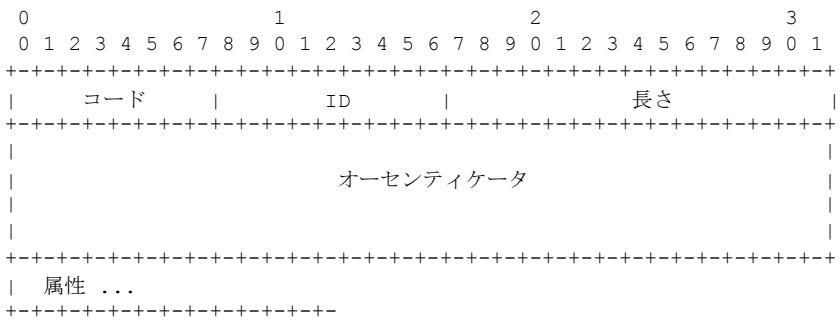
CoA メッセージに含まれるすべてのセッション識別属性がセッションと一致しない限り、スイッチは「無効な属性値」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

特定のセッションを対象とする接続解除要求および CoA 要求の場合、次のいずれかのセッション ID を使用できます。

- Calling-Station-ID（IETF 属性 31、MAC アドレスを含む必要があります）
- Audit-Session-ID（Cisco ベンダー固有属性）
- Accounting-Session-ID（IETF 属性 44）

複数のセッション識別属性がメッセージに含まれる場合、すべての属性がセッションと一致する必要があります。1 つでも一致しないものがある場合は、スイッチはエラーコード「*無効な属性値*」を含む切断否定確認応答（NAK）または CoA-NAK を返します。

RFC 5176 で定義されている CoA 要求コードのパケット形式は、コード、ID、長さ、オーセンティケータ、および属性の各フィールドで構成され、Type:Length:Value（TLV; タイプ : 長さ : 値）の形式になっています。



属性フィールドは、Cisco VSA の伝送に使用されます。

CoA ACK 応答コード

認可ステートが正常に変更されると、肯定確認応答（ACK）が送信されます。CoA ACK で返される属性は CoA 要求によって異なり、これについては個別の CoA コマンドで説明します。

CoA NAK 応答コード

否定確認応答（NAK）は認可ステートの変更が失敗したことを示し、失敗の理由を示す属性を含む場合があります。CoA が成功したかどうかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

ここでは、次の内容について説明します。

- 「セッションの再認証」
- 「セッションの終了」
- 「CoA Disconnect-Request」
- 「CoA Request: Disable Host Port」
- 「CoA Request: Bounce-Port」

Cisco IOS Release 12.2(52)SE 以降、スイッチは表 11-4 に示すコマンドをサポートします。

表 11-4　スイッチでサポートされる CoA コマンド

コマンド[1]	Cisco VSA
ホストの再認証	Cisco:Avpair="subscriber:command=reauthenticate"
セッションの終了	これは、VSA を必要としない標準の接続解除要求です。
ホスト ポートのバウンス	Cisco:Avpair="subscriber:command=bounce-host-port"
ホスト ポートのディセーブル化	Cisco:Avpair="subscriber:command=disable-host-port"

1. すべての CoA コマンドは、スイッチと CoA クライアントの間のセッション ID を含む必要があります。

セッションの再認証

AAA サーバは、通常、ID またはポスチャが不明のホストがネットワークに参加し、そのホストが制限付きアクセス認可プロファイル（ゲスト VLAN など）に関連付けられていると、セッション再認証要求を生成します。再認証要求により、クレデンシャルが不明のホストでも、適切な認可グループに配置できます。

セッションの認証を開始するために、AAA サーバは、*Cisco:Avpair="subscriber:command=reauthenticate"* という形式の Cisco ベンダー固有属性（VSA）と 1 つまたは複数のセッション識別属性を含む、標準の CoA-Request メッセージを送信します。

現在のセッションの状態により、このメッセージに対するスイッチの応答が決まります。セッションが現在 IEEE 802.1x によって認証されている場合、スイッチは Extensible Authentication Protocol over LAN（EAPOL）RequestId メッセージをサーバに送信することで応答します。

セッションが現在 MAC Authentication Bypass（MAB; MAC 認証バイパス）によって認証されている場合は、スイッチはアクセス要求をサーバに送信し、最初に成功した認証に使用したものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッションの認証が進行中の場合は、スイッチはプロセスを終了し、最初に試みるように設定されている方式で、認証手順を再開します。

セッションがまだ認可されていない場合、またはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認可されている場合は、再認証メッセージにより、最初に試みるように設定されている方式で、アクセス制御方式が再開されます。現在のセッションの認可は、再認証の結果が異なる認可になるまで維持されます。

セッションの終了

セッションを終了できる CoA 要求には 3 つの種類があります。CoA Disconnect-Request は、ホストのポートをディセーブルにしないでセッションを終了します。このコマンドは、指定したホストのオーセンティケータ ステート マシンを再初期化しますが、そのホストのネットワークへのアクセスは制限しません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA を指定した CoA 要求を使用します。このコマンドは、あるホストがネットワーク上の問題の原因であることがわかっていて、そのホストのネットワーク アクセスを直ちにブロックする必要があるときに便利です。そのポートでのネットワーク アクセスを元に戻すときは、RADIUS 以外のメカニズムを使用して再びイネーブルにします。

プリンタのようにサプリカントを持たない装置で新しい IP アドレスを取得する必要がある場合は（VLAN を変更したあとなど）、ポートバウンス（ポートを一時的にディセーブルにしてから再びイネーブルにすること）を使用して、ホストのポートでのセッションを終了します。

CoA Disconnect-Request

このコマンドは標準 Disconnect-Request です。このコマンドはセッション指向なので、「セッションの識別」（P.11-22）で説明しているセッション識別属性を 1 つまたは複数含む必要があります。セッションを特定できない場合、スイッチは「セッション コンテキストが見つからない」というエラー コード属性が設定された Disconnect-NAK メッセージを返します。セッションが *特定された* 場合は、スイッチはそのセッションを終了します。セッションが完全に削除されたあと、スイッチは Disconnect-ACK を返します。

Disconnect-ACK をクライアントに返す前にスイッチがスタンバイ スイッチにフェールオーバーした場合は、クライアントから要求が再送信されると、新しいアクティブ スイッチで処理が繰り返されます。再送信のあとでセッションが見つからない場合は、「セッション コンテキストが見つからない」というエラー コード属性を含む Disconnect-ACK が送信されます。

CoA Request: Disable Host Port

このコマンドは、次の新しい VSA を含む標準 CoA-Request メッセージで送信されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向なので、「セッションの識別」（P.11-22）で説明しているセッション識別属性を 1 つまたは複数含む必要があります。セッションを特定できない場合、スイッチは「セッション コンテキストが見つからない」というエラー コード属性が設定された CoA-NAK メッセージを返します。セッションが特定された場合は、スイッチはホストしているポートをディセーブルにして、CoA-ACK メッセージを返します。

CoA-ACK をクライアントに返す前にスイッチで障害が発生した場合は、クライアントから要求が再送信されると、新しいアクティブ スイッチで処理が繰り返されます。CoA-ACK メッセージをクライアントに返したあと、操作が完了する前にスイッチで障害が発生した場合は、操作は新しいアクティブ スイッチで再開されます。

（注）　コマンド再送信後の Disconnect-Request のエラーは、元のコマンドが発行されたあとでスタンバイ スイッチがアクティブになる前に、切り替え前のセッション終了が成功したこと（Disconnect-ACK が送信されなかった場合）、または他の手段によるセッション終了（リンク障害など）による結果である場合があります。

CoA Request: Bounce-Port

このコマンドは、次の VSA を含む標準 CoA-Request メッセージで送信されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向なので、「セッションの識別」（P.11-22）で説明しているセッション識別属性を 1 つまたは複数含む必要があります。セッションを特定できない場合、スイッチは「セッション コンテキストが見つからない」というエラー コード属性が設定された CoA-NAK メッセージを返します。セッションが特定された場合は、スイッチはホストしているポートを 10 秒間だけディセーブルにしたあと、再びイネーブルにして（ポートバウンス）、CoA-ACK を返します。

CoA-ACK をクライアントに返す前にスイッチで障害が発生した場合は、クライアントから要求が再送信されると、新しいアクティブ スイッチで処理が繰り返されます。CoA-ACK メッセージをクライアントに返したあと、操作が完了する前にスイッチで障害が発生した場合は、操作は新しいアクティブ スイッチで再開されます。

RADIUS の設定

ここでは、RADIUS をサポートするようにスイッチを設定する方法を説明します。少なくとも、RADIUS サーバ ソフトウェアを実行しているホストを識別し、RADIUS による認証の方式リストを定義する必要があります。必要に応じて、RADIUS による認可とアカウンティングの方式リストも定義できます。

方式リストでは、ユーザの認証、認可、またはアカウントの保持に使用する手順と方式を定義します。方式リストを使用して、使用する 1 つまたは複数のセキュリティ プロトコルを指定でき（TACACS+ やローカル ユーザ名検索など）、これにより、最初の方式が失敗した場合のバックアップ システムを設定できます。ソフトウェアは、リスト内の最初の方式を使用して、ユーザの認証、認可、またはアカウントの保持を行います。その方式が応答しない場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リストの方式による通信が成功するか、方式をすべて試し終わるまで繰り返されます。

スイッチで TACACS+ の機能を設定するには、RADIUS サーバにアクセスし、RADIUS サーバを設定しておく必要があります。

- 「RADIUS のデフォルト設定」（P.11-26）
- 「RADIUS サーバ ホストの識別」（P.11-26）（必須）
- 「RADIUS ログイン認証の設定」（P.11-28）（必須）
- 「AAA サーバ グループの定義」（P.11-30）（任意）
- 「ユーザ イネーブル アクセスおよびネットワーク サービスに対する RADIUS による認可の設定」（P.11-32）（任意）
- 「RADIUS によるアカウンティングの開始」（P.11-33）（任意）
- 「すべての RADIUS サーバに対する設定」（P.11-34）（任意）
- 「ベンダー固有の RADIUS 属性を使用するためのスイッチの設定」（P.11-34）（任意）
- 「ベンダー独自の RADIUS サーバ通信のためのスイッチの設定」（P.11-36）（任意）

- 「スイッチでの CoA の設定」（P.11-37）
- 「CoA 機能のモニタとトラブルシューティング」（P.11-38）
- 「RADIUS サーバのロード バランシングの設定」（P.11-38）（任意）

RADIUS のデフォルト設定

RADIUS と AAA はデフォルトではディセーブルになっています。

セキュリティの問題を防ぐため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。イネーブルにすると、RADIUS は CLI を使用してスイッチにアクセスするユーザを認証できます。

RADIUS サーバ ホストの識別

スイッチと RADIUS サーバの間の通信には、複数のコンポーネントが関係します。

- ホスト名または IP アドレス
- 認証宛先ポート
- アカウンティング宛先ポート
- キー文字列
- タイムアウト時間
- 再送信値

RADIUS セキュリティ サーバを識別するには、ホスト名または IP アドレス、ホスト名と特定の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート番号、または IP アドレスと特定の UDP ポート番号を使用します。IP アドレスと UDP ポート番号の組み合わせにより一意の ID が作成され、異なるポートを特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。この一意の ID を使用して、同じ IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（アカウンティングなど）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。この例を使用すると、最初のホスト エントリがアカウンティング サービスの提供に失敗した場合は、`%RADIUS-4-RADIUS_DEAD` メッセージが表示されたあと、スイッチは同じ装置上でアカウンティング サービス用に設定されている第 2 のホスト エントリを試します。RADIUS ホスト エントリは、設定されている順序で試行されます。

RADIUS サーバとスイッチは、共有シークレット テキスト ストリングを使用してパスワードを暗号化し、応答を交換します。AAA セキュリティ コマンドを使用するように RADIUS を設定するには、RADIUS サーバ デーモンを実行しているホストと、そのホストがスイッチと共有している秘密テキスト（キー）文字列を指定する必要があります。

タイムアウト、再送信、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに、サーバごとに、またはグローバルとサーバごとの設定の組み合わせで設定できます。これらの設定をスイッチと通信するすべての RADIUS サーバにグローバルに設定するには、それぞれに一意の 3 つのグローバル コンフィギュレーション コマンド **radius-server timeout**、**radius-server retransmit**、および **radius-server key** を使用します。これらの値を特定の RADIUS サーバに適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。

（注）　1 つのスイッチにグローバル機能とサーバごとの機能（タイムアウト、再送信、キーの各コマンド）の両方を設定した場合は、タイマー、再送信、キー値のサーバごとのコマンドがグローバルなコマンドより優先されます。すべての RADIUS サーバでこれらの設定を行う方法については、「すべての RADIUS サーバに対する設定」（P.11-34）を参照してください。

AAA サーバ グループを使用して既存のサーバ ホストを認証用にグループ化するように、スイッチを設定できます。詳細については、「AAA サーバ グループの定義」（P.11-30）を参照してください。

サーバごとの RADIUS サーバ通信を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、スイッチが再送信の前に RADIUS サーバの応答を待機する時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドの設定より優先されます。**radius-server host** コマンドでタイムアウトを設定しないと、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合またはサーバの応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数の値を設定しないと、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。 （注）　key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。キーは必ず **radius-server host** コマンドの最後の項目として設定してください。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 単一の IP アドレスに関連付けられている複数のホスト エントリを認識するようにスイッチを設定するには、必要な回数だけこのコマンドを入力し、そのたびに異なる UDP ポート番号を指定します。スイッチのソフトウェアは、ここで指定した順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定した RADIUS サーバを削除するには、**no radius-server host** *hostname* | *ip-address* グローバル コンフィギュレーション コマンドを使用します。

次に、1 つの RADIUS サーバを認証用に設定し、別のサーバをアカウンティング用に設定する例を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次に、*host1* を RADIUS サーバとして設定し、デフォルトのポートを認証とアカウンティングの両方に使用する例を示します。

```
Switch(config)# radius-server host host1
```

（注）　RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの両方で共有されるキー文字列があります。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義したあと、そのリストをさまざまなポートに適用します。方式リストでは、実行する認証のタイプと、実行する手順を定義します。定義した認証方式を実行するには、特定のポートにリストを適用する必要があります。唯一の例外はデフォルトの方式リストです（名前は *default* です）。方式の名前付きリストが明示的に定義されているポート以外のすべてのポートには、デフォルトの方式リストが自動的に適用されます。

方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定でき、これにより、最初の方式が失敗した場合の認証のバックアップ システムを設定できます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合、つまりセキュリティ サーバまたはローカル ユーザ名データベースがユーザ アクセスを拒否する応答を返した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前を示す文字列を指定します。 • *method1...* には、認証アルゴリズムが試みる実際の方式を指定します。追加の認証方式は、前の認証方式が失敗した場合ではなく、エラーを返した場合にだけ使用されます。 次のいずれかの方式を選択します。 – **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、**enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 – **group radius**：RADIUS 認証を使用します。この認証方式を使用するには、RADIUS サーバを設定しておく必要があります。詳細については、「RADIUS サーバ ホストの識別」（P.11-26）を参照してください。 – **line**：回線パスワードを認証に使用します。この認証方式を使用するには、回線パスワードを定義しておく必要があります。そのためには、**password** *password* ライン コンフィギュレーション コマンドを使用します。 – **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。そのためには、**username** *name* **password** グローバル コンフィギュレーション コマンドを使用します。 – **local-case**：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *password* グローバル コンフィギュレーション コマンドを使用して、データベースにユーザ名情報を入力する必要があります。 – **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストを 1 つまたは複数の回線に適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成されるデフォルト リストが使用されます。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに対して RADIUS 認証をディセーブルにするか、またはデフォルト値に戻すには、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

（注） AAA 方式を使用して HTTP アクセスに対してスイッチを保護するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、スイッチは AAA 方式で HTTP アクセスに対して保護されません。

ip http authentication コマンドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

AAA サーバ グループの定義

AAA サーバ グループを使用して既存のサーバ ホストを認証用にグループ化するように、スイッチを設定できます。設定済みサーバ ホストのサブセットを選択し、それを特定のサービスに対して使用します。サーバ グループは、グローバル サーバ ホスト リストとともに使用します。このリストでは、選択されているサーバ ホストの IP アドレスがリストされています。

各ホスト エントリの ID（IP アドレスと UDP ポート番号の組み合わせ）が一意であれば、サーバ グループは同じサーバに対して複数のホスト エントリを含むこともでき、異なるポートを特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリを同じサービス（アカウンティングなど）用に設定した場合、2 番めに設定したホスト エントリは、最初のホスト エントリのフェールオーバー バックアップとして動作します。

特定のサーバと定義済みのグループ サーバを関連付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。IP アドレスでサーバを指定することも、オプションの **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを指定することもできます。

AAA サーバ グループを定義し、それを特定の RADIUS サーバと関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、スイッチが再送信の前に RADIUS サーバの応答を待機する時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドの設定より優先されます。**radius-server host** コマンドでタイムアウトを設定しないと、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合またはサーバの応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数の値を設定しないと、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。キーは必ず **radius-server host** コマンドの最後の項目として設定してください。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 単一の IP アドレスに関連付けられている複数のホスト エントリを認識するようにスイッチを設定するには、必要な回数だけこのコマンドを入力し、そのたびに異なる UDP ポート番号を指定します。スイッチのソフトウェアは、ここで指定した順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa group server radius** *group-name*	グループ名を指定して AAA のサーバ グループを定義します。 このコマンドは、スイッチをサーバ グループ コンフィギュレーション モードにします。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバと定義したサーバ グループを関連付けます。AAA サーバ グループ内の RADIUS サーバごとに、このステップを繰り返します。 グループ内の各サーバは、ステップ 2 で先に定義しておく必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「RADIUS ログイン認証の設定」（P.11-28）を参照してください。

指定した RADIUS サーバを削除するには、**no radius-server host** *hostname* | *ip-address* グローバル コンフィギュレーション コマンドを使用します。コンフィギュレーション リストからサーバ グループを削除するには、**no aaa group server radius** *group-name* グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、**no server** *ip-address* サーバ グループ コンフィギュレーション コマンドを使用します。

次の例では、2 つの異なる RADIUS グループ サーバ（*group1* と *group2*）を認識するようにスイッチを設定しています。group1 では、同じサービスに対して設定されている同じ RADIUS サーバに 2 つの異なるホスト エントリがあります。2 番めのホスト エントリは、1 番めのエントリのフェールオーバー バックアップとして動作します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

ユーザ イネーブル アクセスおよびネットワーク サービスに対する RADIUS による認可の設定

AAA 認可は、ユーザが使用できるサービスを制限します。AAA 認可をイネーブルにすると、スイッチは、ローカル ユーザ データベースまたはセキュリティ サーバにあるユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイルの情報によって許可される場合にだけ、要求したサービスにアクセスできます。

ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定するには、**aaa authorization** グローバル コンフィギュレーション コマンドで **radius** キーワードを指定します。

aaa authorization exec radius local コマンドは、次の認可パラメータを設定します。

- 認証が RADIUS を使用して実行された場合、特権 EXEC アクセスの認可には RADIUS を使用します。
- 認証に RADIUS が使用されなかった場合は、ローカル データベースを使用します。

（注）　認可が設定されている場合でも、CLI を使用してログインする認証済みのユーザに対しては、認可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに対して RADIUS による認可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network radius**	ネットワーク関連サービスのすべての要求に対してユーザを RADIUS で認可するようにスイッチを設定します。
ステップ 3	**aaa authorization exec radius**	ユーザが特権 EXEC アクセスを行っている場合はユーザを RADIUS で認可するようにスイッチを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

認可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

RADIUS によるアカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスしているサービス、およびユーザが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザのアクティビティをアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングに関する Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに保存されます。このデータを分析し、ネットワーク管理、クライアント課金、または監査に利用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに対して RADIUS によるアカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa accounting network start-stop radius**	すべてのネットワーク関連サービス要求に対して RADIUS によるアカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop radius**	特権 EXEC プロセスの開始時に start-record アカウンティング通知を送信し、終了時に stop-record を送信するように、RADIUS によるアカウンティングをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

AAA サーバが到達不能のときのセッション確立

aaa accounting system guarantee-first コマンドによって、システム アカウンティングが最初のレコードになります。これは、デフォルトの状態です。システムのリロード（場合によっては 3 分以上かかることがある）が行われるまで、ユーザがコンソールまたは端末接続でセッションを開始できないことがあります。

ルータがリロードされたときに AAA サーバが到達不能の場合、ルータとコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

すべての RADIUS サーバに対する設定

スイッチとすべての RADIUS サーバの間のグローバルな通信設定を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server key** *string*	スイッチとすべての RADIUS サーバとの間で使用する共有シークレット テキスト ストリングを指定します。 （注）　key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 3	**radius-server retransmit** *retries*	中止する前にスイッチがサーバに各 RADIUS 要求を送信する回数を指定します。デフォルト値は 3 で、指定できる範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout** *seconds*	スイッチが RADIUS 要求を再送信する前に要求への応答を待機する秒数を指定します。デフォルト値は 5 秒で、指定できる範囲は 1 ～ 1000 です。
ステップ 5	**radius-server deadtime** *minutes*	認証要求に応答しない RADIUS サーバをスキップする分数を指定します。これにより、次に設定されているサーバを試行する前に要求の待機が時間切れになるのを防ぎます。デフォルト値は 0 で、指定できる範囲は 1 ～ 1440 分です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

再送信、タイムアウト、スキップ時間の設定をデフォルトに戻すには、これらのコマンドの **no** 形式を使用します。

ベンダー固有の RADIUS 属性を使用するためのスイッチの設定

Internet Engineering Task Force（IETF）のドラフト標準では、スイッチと RADIUS サーバの間でベンダー固有属性（属性 26）を使用してベンダー固有の情報を通信するための方法が指定されています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、仕様で推奨されている形式を使用して 1 つのベンダー固有属性をサポートしています。シスコのベンダー ID は 9、サポートされるオプションはベンダー タイプ 1 で、名前は *cisco-avpair* です。値は次の形式のストリングです。

```
protocol : attribute sep value *
```

protocol は、特定の認可タイプに対するシスコのプロトコル属性の値です。*attribute* および *value* はシスコの TACACS+ 仕様で定義されている適切な Attribute-Value（AV）ペアであり、*sep* は必須属性の場合は =、任意属性の場合は * です。TACACS+ による認可で使用可能なすべての機能セットを、RADIUS で使用できます。

たとえば、次の AV ペアは、（PPP IPCP アドレス割り当ての間の）IP 認可の間にシスコの *複数名 IP アドレス プール*機能をアクティブにします。

```
cisco-avpair= "ip:addr-pool=first"
```

次に、スイッチからログインするユーザがすぐに特権 EXEC コマンドにアクセスできるようにする例を示します。

```
cisco-avpair= "shell:priv-lvl=15"
```

次に、RADIUS サーバ データベースで認可された VLAN を指定する例を示します。

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

次に、この接続の期間だけインターフェイスに ASCII 形式の入力 ACL を適用する例を示します。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

次に、この接続の期間だけインターフェイスに ASCII 形式の出力 ACL を適用する例を示します。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

他のベンダーは、それぞれが独自に一意のベンダー ID、オプション、および関連する VSA を定めています。ベンダー ID と VSA の詳細については、RFC 2138『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

VSA を認識して使用するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server vsa send** [**accounting** | **authentication**]	RADIUS IETF 属性 26 で定義されている VSA を認識して使用するようにスイッチをイネーブルにします。 • （任意）認識されるベンダー固有属性のセットをアカウンティング属性だけに制限するには、**accounting** キーワードを使用します。 • （任意）認識されるベンダー固有属性のセットを認証属性だけに制限するには、**authentication** キーワードを使用します。 キーワードを指定しないでこのコマンドを入力すると、アカウンティングと認証の両方のベンダー固有属性が使用されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　RADIUS 属性の詳細なリストまたはベンダー固有属性 26 の詳細については、Cisco.com のページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] >[Command References] にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の付録「RADIUS Attributes」を参照してください。

ベンダー独自の RADIUS サーバ通信のためのスイッチの設定

RADIUS に関する IETF のドラフト標準では、スイッチと RADIUS サーバの間でベンダー独自の情報を通信するための方法が指定されていますが、独自の方法で RADIUS 属性を拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自の RADIUS 属性のサブセットをサポートします。

すでに説明したように、RADIUS を設定するには（ベンダー独自か IETF ドラフト準拠かにかかわらず）、RADIUS サーバ デーモンを実行するホストと、ホストがスイッチと共有するシークレット テキスト ストリングを指定する必要があります。RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

ベンダー独自の RADIUS サーバ ホストおよび共有シークレット テキスト ストリングを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **non-standard**	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、それが RADIUS のベンダー独自の実装を使用していることを示します。
ステップ 3	**radius-server key** *string*	スイッチとベンダー独自の RADIUS サーバの間で使用する共有シークレット テキスト ストリングを指定します。スイッチと RADIUS サーバはこの文字列を使用して、パスワードを暗号化し、応答を交換します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ベンダー独自の RADIUS ホストを削除するには、**no radius-server host** {*hostname* | *ip-address*} **non-standard** グローバル コンフィギュレーション コマンドを使用します。キーをディセーブルにするには、**no radius-server key** グローバル コンフィギュレーション コマンドを使用します。

次に、ベンダー独自の RADIUS ホストを指定し、スイッチとサーバの間で *rad124* の秘密キーを使用する例を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

スイッチでの CoA の設定

スイッチで CoA を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa server radius dynamic-author**	スイッチを認証、認可、アカウンティング（AAA）サーバとして設定し、外部ポリシー サーバとの相互通信を容易にします。
ステップ 4	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*]	ダイナミック認可ローカル サーバ コンフィギュレーション モードを開始し、装置が CoA および接続解除の要求を受け付ける RADIUS クライアントを指定します。
ステップ 5	**server-key** [**0** | **7**] *string*	装置と RADIUS クライアントの間で共有する RADIUS キーを設定します。
ステップ 6	**port** *port-number*	装置が設定済みの RADIUS クライアントからの RADIUS 要求を待ち受けるポートを指定します。
ステップ 7	**auth-type** {**any** | **all** | **session-key**}	スイッチが RADIUS クライアントに使用する認可のタイプを指定します。 クライアントが認可を受けるには、設定済みのすべての属性が一致する必要があります。
ステップ 8	**ignore session-key**	（任意）セッション キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 9	**ignore server-key**	（任意）サーバ キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 10	**authentication command bounce-port ignore**	（任意）CoA 要求を無視してセッションをホストしているポートを一時的にディセーブルにするようにスイッチを設定します。ポートを一時的にディセーブルにする目的は、VLAN の変更が発生し、変更を検出するためのサプリカントがエンドポイント上にないときに、ホストから DHCP の再ネゴシエーションをトリガーすることです。
ステップ 11	**authentication command disable-port ignore**	（任意）セッションをホストしているポートを管理的にシャットダウンすることを要求する非標準のコマンドを無視するように、スイッチを設定します。ポートをシャットダウンすると、セッションは終了します。 ポートを再びイネーブルにするには、標準の CLI コマンドまたは SNMP コマンドを使用します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show running-config**	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。スイッチの AAA サーバ機能を無効にするには、**no aaa server radius dynamic authorization** グローバル コンフィギュレーション コマンドを使用します。

CoA 機能のモニタとトラブルシューティング

次の Cisco IOS コマンドを使用して、スイッチの CoA 機能のモニタとトラブルシューティングを行います。

- **debug radius**
- **debug aaa coa**
- **debug aaa pod**
- **debug aaa subsys**
- **debug cmdhd** [**detail** | **error** | **events**]
- **show aaa attributes protocol radius**

RADIUS サーバのロード バランシングの設定

この機能を使用すると、アクセスと認証の要求を、サーバ グループ内のすべての RADIUS サーバに均等に配分できます。詳細については、次の場所にある『Cisco IOS Security Configuration Guide, Release 12.2』の「RADIUS Server Load Balancing」を参照してください。
http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrdldbl.html

RADIUS の設定の表示

RADIUS の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

Kerberos でのスイッチ アクセスの制御

ここでは、信頼できるサード パーティを使用してネットワーク リソースに対する要求を認証する Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。この機能を使用するには、暗号化バージョンのスイッチ ソフトウェアをスイッチにインストールする必要があります。

この機能を使用したり、暗号化ソフトウェアのファイルを Cisco.com からダウンロードしたりするには、許可を得る必要があります。詳細については、このリリースに対応するリリース ノートを参照してください。

ここでは、次の情報について説明します。

Kerberos の設定例については、次の URL にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Security Server Protocols」の「Kerberos Configuration Examples」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html

ここで使用するコマンドの構文および使用方法の詳細については、次の URL にある『*Cisco IOS Security Command Reference, Release 12.2*』の「Security Server Protocols」の章の「Kerberos Commands」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html

（注）　Kerberos 設定例および『*Cisco IOS Security Command Reference, Release 12.2*』では、信頼できるサード パーティは、Kerberos をサポートし、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる IE 3000 スイッチです。

Kerberos の概要

Kerberos は、Massachusetts Institute of Technology（MIT）で開発された秘密キー ネットワーク認証プロトコルです。Data Encryption Standard（DES; データ暗号化規格）暗号アルゴリズムを使用して暗号化と認証を行い、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサード パーティの概念を使用して、ユーザとサービスのセキュアな検証を実行します。この信頼できるサード パーティは、*Key Distribution Center*（KDC; キー発行局）と呼ばれます。

Kerberos は、ユーザが自分で主張するとおりのユーザであり、ユーザが使用するネットワーク サービスがそのとおりのものであることを確認します。そのために、KDC つまり信頼できる Kerberos サーバはチケットをユーザに発行します。このチケットは有効期限が限られており、ユーザのクレデンシャル キャッシュに保存されます。Kerberos サーバは、ユーザ名とパスワードの代わりにチケットを使用して、ユーザとネットワーク サービスを認証します。

（注）　Kerberos サーバは、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる IE 3000 スイッチです。

Kerberos のクレデンシャル方式は、*シングル ログオン*と呼ばれるプロセスを使用します。このプロセスは、ユーザを 1 回認証すると、そのユーザ クレデンシャルが受け付けられるすべての場所で（別のパスワードを暗号化することなく）セキュアな認証を許可します。

このソフトウェア リリースでは Kerberos 5 をサポートするので、すでに Kerberos 5 を使用している場合は、他のネットワーク ホスト（UNIX サーバや PC など）ですでに使用しているものと同じ Kerberos 認証データベースを KDC で使用できます。

このソフトウェア リリースの Kerberos は、次のネットワーク サービスをサポートします。

- Telnet
- rlogin
- remote shell protocol（rsh; リモート シェル プロトコル）

表 11-5 に Kerberos に関連する一般的な用語とその定義を示します。

表 11-5　Kerberos の用語

用語	定義
認証	ユーザまたはサービスが別のサービスに対して自分の身元を証明するプロセス。たとえば、クライアントがスイッチに対して認証したり、スイッチが別のスイッチに対して認証したりする場合があります。
認可	スイッチが、ネットワークまたはスイッチでユーザに与えられている権限およびユーザが実行できる処理を識別する手段。

表 11-5　Kerberos の用語 （続き）

用語	定義
クレデンシャル	TGT[1] やサービス クレデンシャルなどの認証チケットを表す一般的な用語。Kerberos クレデンシャルはユーザまたはサービスの ID を確認します。チケットを発行した Kerberos サーバをネットワーク サービスが信頼することにした場合、ユーザ名とパスワードを再入力する代わりにチケットを使用できます。クレデンシャルのデフォルトの有効期間は 8 時間です。
インスタンス	Kerberos プリンシパルの承認レベルのラベル。ほとんどの Kerberos プリンシパルの形式は *user@REALM*（たとえば smith@EXAMPLE.COM）です。Kerberos インスタンスを含む Kerberos プリンシパルの形式は *user/instance@REALM*（たとえば smith/admin@EXAMPLE.COM）です。Kerberos インスタンスを使用すると、認証が成功した場合にユーザの承認レベルを指定できます。各ネットワーク サービスのサーバでは Kerberos インスタンスの認可マッピングが実装され、適用されている場合がありますが、そのようにする必要はありません。 **（注）** Kerberos プリンシパルとインスタンスの名前は、すべて小文字にする*必要があります*。 **（注）** Kerberos レルム名は、すべて大文字にする*必要があります*。
KDC[2]	ネットワーク ホスト上で実行する Kerberos サーバとデータベース プログラムで構成されるキー発行局。
Kerberos 対応	Kerberos クレデンシャル インフラストラクチャをサポートするように変更されたアプリケーションおよびサービスを示す用語。
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。ユーザまたはネットワーク サービスは、Kerberos サーバを信頼することで、別のユーザやネットワーク サービスの ID を検証します。 **（注）** Kerberos レルム名は、すべて大文字にする*必要があります*。
Kerberos サーバ	ネットワーク ホスト上で実行しているデーモン。ユーザおよびネットワーク サービスは、自分の ID を Kerberos サーバに登録します。ネットワーク サービスは Kerberos サーバをクエリーして、他のネットワーク サービスに対して認証します。
KEYTAB[3]	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降では、ネットワーク サービスは、KEYTAB を使用して暗号化されたサービス クレデンシャルを復号化することで、クレデンシャルを認証します。Kerberos 5 よりも前のバージョンでは、KEYTAB は SRVTAB[4] と呼ばれていました。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバでのユーザまたはサービスの身元です。 **（注）** Kerberos プリンシパル名は、すべて小文字にする*必要があります*。
サービス クレデンシャル	ネットワーク サービスのクレデンシャル。KDC から発行されるとき、このクレデンシャルは、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。パスワードはユーザの TGT とも共有されます。

表 11-5　Kerberos の用語 （続き）

用語	定義
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降では、SRVTAB は KEYTAB と呼ばれます。
TGT	KDC が認証済みのユーザに対して発行するクレデンシャルであるチケット認可チケット。TGT を受け取ったユーザは、KDC によって表される Kerberos レルム内のネットワーク サービスに対して認証できます。

1. TGT = Ticket Granting Ticket（チケット認可チケット）
2. KDC = Key Distribution Center（キー発行局）
3. KEYTAB = Key Table（キー テーブル）
4. SRVTAB = Server Table（サーバ テーブル）

Kerberos の動作

Kerberos サーバは、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してリモート ユーザを認証できる IE 3000 スイッチです。さまざまな方法で Kerberos をカスタマイズできますが、ネットワーク サービスにアクセスを試みるリモート ユーザは、3 つのセキュリティ レイヤを通過してからでないと、ネットワーク サービスにアクセスできません。

IE 3000 スイッチを Kerberos サーバとして使用してネットワーク サービスに対して認証するには、リモート ユーザは次の手順を実行する必要があります。

1. 「境界スイッチに対する認証」（P.11-41）
2. 「KDC からの TGT の取得」（P.11-42）
3. 「ネットワーク サービスに対する認証」（P.11-42）

境界スイッチに対する認証

ここでは、リモート ユーザが通過する必要のある第 1 のセキュリティ レイヤについて説明します。ユーザは最初に境界スイッチに対して認証を行う必要があります。この処理は次のように行われます。

1. ユーザは、Kerberos 対応ではない Telnet 接続を境界スイッチに対して開きます。
2. スイッチは、ユーザにユーザ名とパスワードの入力を求めます。
3. スイッチは、このユーザに対する TGT を KDC に要求します。
4. KDC は、ユーザの ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使用して TGT の復号化を試みます。
   - 復号化が成功すると、ユーザはスイッチに対して認証されます。
   - 復号化が成功しない場合は、ユーザはユーザ名とパスワードを再入力するか（Caps Lock または Num Lock のオンまたはオフに注意してください）、または別のユーザ名とパスワードを入力して、ステップ 2 を繰り返します。

Kerberos 対応ではない Telnet セッションを開始して境界スイッチに対して認証するリモート ユーザは、ファイアウォールの内部にいますが、ネットワーク サービスにアクセスする前に、KDC に対して直接認証する必要があります。ユーザが KDC に対して認証する必要があるのは、KDC が発行する TGT はスイッチに格納され、ユーザがスイッチにログオンするまでは追加の認証に TGT を使用できないためです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過する必要のある第 2 のセキュリティ レイヤについて説明します。ユーザは次に、ネットワーク サービスにアクセスするために、KDC に対して認証して TGT を KDC から取得する必要があります。

KDC に対して認証を行う方法については、次の URL にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Security Server Protocols」の「Obtaining a TGT from a KDC」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

ネットワーク サービスに対する認証

ここでは、リモート ユーザが通過する必要のある第 3 のセキュリティ レイヤについて説明します。TGT を取得したユーザは次に、Kerberos レルム内にあるネットワーク サービスに対して認証する必要があります。

ネットワーク サービスに対して認証を行う方法については、次の URL にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Security Server Protocols」の「Authenticating to Network Services」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

Kerberos の設定

リモート ユーザがネットワーク サービスに対して認証できるためには、ユーザおよびネットワーク サービスと通信して相互に認証するように、Kerberos レルム内のホストと KDC を設定する必要があります。そのためには、ユーザとネットワーク サービスを相互に識別する必要があります。ホストのエントリを KDC 上の Kerberos データベースに追加し、KDC によって生成された KEYTAB ファイルを Kerberos レルム内のすべてのホストに追加します。また、KDC データベースにユーザのエントリを作成します。

ホストおよびユーザのエントリを追加または作成するときは、次の注意事項に従ってください。

- Kerberos プリンシパル名は、すべて小文字にする*必要があります*。
- Kerberos インスタンス名は、すべて小文字にする*必要があります*。
- Kerberos レルム名は、すべて大文字にする*必要があります*。

（注）　Kerberos サーバは、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる IE 3000 スイッチです。

Kerberos で認証されたサーバ クライアント システムを設定するには、次の手順を実行します。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

手順については、次の URL にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Security Server Protocols」の「Kerberos Configuration Task List」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

ローカルな認証と認可のためのスイッチの設定

AAA をローカル モードで実装するようにスイッチを設定することで、サーバなしで動作するように AAA を設定できます。このように設定すると、スイッチが認証と認可を処理します。この設定ではアカウンティングは使用できません。

ローカル AAA 用にスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login default local**	ローカル ユーザ名データベースを使用するように、ログイン認証を設定します。**default** キーワードは、ローカル ユーザ データベース認証をすべてのポートに適用します。
ステップ 4	**aaa authorization exec local**	AAA によるユーザの認可を設定し、ローカル データベースをチェックし、ユーザに EXEC シェルの実行を許可します。
ステップ 5	**aaa authorization network local**	ネットワーク関連サービスのすべての要求に対してユーザを AAA で認可するように設定します。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースに入り、ユーザ名に基づく認証システムを設定します。 ユーザごとにこのコマンドを繰り返します。 • *name* には、ユーザ ID として 1 語を指定します。スペースおよび引用符は使用できません。 • （任意）*level* には、ユーザがアクセスしたあとで割り当てられる権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 は特権 EXEC モード アクセスです。レベル 0 はユーザ EXEC モード アクセスです。 • *encryption-type* には、暗号化されていないパスワードが後ろに続くことを指定する場合は 0 を入力します。非表示パスワードが後ろに続くことを指定する場合は 7 を入力します。 • *password* には、スイッチにアクセスするためにユーザが入力する必要があるパスワードを指定します。パスワードは 1 ～ 25 文字でなければならず、間にスペースを含むことができ、**username** コマンドで最後に指定するオプションである必要があります。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。認可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

（注） AAA 方式を使用して HTTP アクセスに対してスイッチを保護するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、スイッチは AAA 方式で HTTP アクセスに対して保護されません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

セキュア シェル用のスイッチの設定

ここでは、セキュア シェル（SSH）機能の設定方法について説明します。この機能を使用するには、暗号化ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用したり、暗号化ソフトウェアのファイルを Cisco.com からダウンロードしたりするには、許可を得る必要があります。詳細については、このリリースに対応するリリース ノートを参照してください。

ここでは、次の情報について説明します。

SSH の設定例については、次の URL にある『*Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*』の「Configuring Secure Shell」の「SSH Configuration Examples」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html

（注）　この項で使用しているコマンドの構文および使用方法の詳細については、次の URL にあるこのリリースのコマンド リファレンスおよび Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html

SSH の概要

SSH は、装置に対するセキュアなリモート接続を提供するプロトコルです。SSH は装置の認証時に強力な暗号化を行うことにより、リモート接続に対して Telnet よりも高いセキュリティを提供します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートします。

この項で説明する内容は、次のとおりです。

SSH サーバ、統合クライアント、サポートされるバージョン

SSH の機能には、スイッチで実行するアプリケーションである SSH サーバと SSH 統合クライアントがあります。SSH クライアントを使用して、SSH サーバを実行するスイッチに接続できます。SSH サーバは、このリリースでサポートされる SSH クライアントおよびシスコ以外の SSH クライアントと連動します。また、SSH クライアントは、このリリースでサポートされる SSH サーバおよびシスコ以外の SSH サーバと連動します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは SSHv1 クライアントをサポートします。

SSH は、データ暗号化規格（DES）、Triple DES（3DES）暗号アルゴリズム、およびパスワードに基づくユーザ認証をサポートします。

SSH は、次のユーザ認証方式もサポートします。

- TACACS+（詳細については、「TACACS+ でのスイッチ アクセスの制御」（P.11-10）を参照してください）
- RADIUS（詳細については、「RADIUS でのスイッチ アクセスの制御」（P.11-17）を参照してください）
- ローカル認証と認可（詳細については、「ローカルな認証と認可のためのスイッチの設定」（P.11-43）を参照してください）

（注）　このソフトウェア リリースは IP セキュリティ（IPSec）はサポートしません。

制限事項

SSH には、次の制限事項が適用されます。

- スイッチは、Rivest、Shamir、Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバと SSH クライアントは、DES（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアだけでサポートされます。
- スイッチは、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES; 高度暗号化規格）暗号化アルゴリズムをサポートします。ただし、対称暗号 AES によるキーの暗号化はサポートしません。

SSH の設定

ここでは、次の設定情報について説明します。

- 「設定時の注意事項」（P.11-45）
- 「SSH を実行するためのスイッチの設定」（P.11-46）（必須）
- 「SSH サーバの設定」（P.11-47）（スイッチを SSH サーバとして設定する場合に限り必要）

設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定するときは、次の注意事項に従ってください。

- SSHv1 サーバによって生成された RSA キー ペアは、SSHv2 サーバで使用できます。その逆の場合も同様です。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力したあとで CLI エラー メッセージが表示される場合は、RSA キー ペアが生成されていません。ホスト名とドメインを再設定したあと、**crypto key generate rsa** コマンドを入力してください。詳細については、「SSH を実行するためのスイッチの設定」（P.11-46）を参照してください。
- RSA キー ペアを生成するとき、[No host name specified] というメッセージが表示される場合があります。その場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キー ペアを生成するとき、[No domain specified] というメッセージが表示される場合があります。その場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。

- ローカル認証および認可認証方式を設定するときは、コンソールで AAA がディセーブルになっていることを確認してください。

SSH を実行するためのスイッチの設定

SSH を実行するようにスイッチを設定するには、次の手順を実行します。

1. Cisco.com から暗号化ソフトウェア イメージをダウンロードします。このステップは必須です。詳細については、このリリースに対応するリリース ノートを参照してください。
2. スイッチのホスト名と IP ドメイン名を設定します。スイッチを SSH サーバとして設定する場合にだけ、この手順を実行してください。
3. スイッチの RSA キー ペアを生成します。SSH が自動的にイネーブルになります。スイッチを SSH サーバとして設定する場合にだけ、この手順を実行してください。
4. ローカルまたはリモート アクセス用にユーザ認証を設定します。このステップは必須です。詳細については、「ローカルな認証と認可のためのスイッチの設定」（P.11-43）を参照してください。

ホスト名と IP ドメイン名を設定し、RSA キー ペアを生成するには、特権 EXEC モードで次の手順を実行します。この手順は、スイッチを SSH サーバとして設定する場合に必要です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *hostname*	スイッチのホスト名を設定します。
ステップ 3	**ip domain-name** *domain_name*	スイッチのホスト ドメインを設定します。
ステップ 4	**crypto key generate rsa**	スイッチでローカルおよびリモート認証用の SSH サーバをイネーブルにして、RSA キー ペアを生成します。 最小モジュール サイズを 1024 ビットにすることを推奨します。 RSA キーを生成するときに、モジュールの長さの入力を求められます。モジュールを長くするほど安全性は高くなりますが、生成および使用するときの時間が長くなります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチの SSH サーバのステータスを表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

RSA キー ペアを削除するには、**crypto key zeroize rsa** グローバル コンフィギュレーション コマンドを使用します。RSA キー ペアを削除すると、SSH サーバは自動的にディセーブルになります。

SSH サーバの設定

SSH サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip ssh version** [**1** | **2**]	（任意）SSH バージョン 1 または SSH バージョン 2 を実行するようにスイッチを設定します。 • **1**：SSH バージョン 1 を実行するようにスイッチを設定します。 • **2**：SSH バージョン 2 を実行するようにスイッチを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合は、SSH サーバは SSH クライアントがサポートする最新の SSH バージョンを選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}	SSH 制御パラメータを設定します。 • タイムアウト値を秒単位で指定します。デフォルト値は 120 秒です。指定できる範囲は 0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されたあとは、スイッチは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク経由での複数の CLI ベース セッション用に、最大で 5 つの暗号化 SSH 接続を同時に使用できます（セッション 0 からセッション 4）。実行シェルが開始したあと、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントがサーバに対して再認証できる回数を指定します。デフォルト値は 3 で、指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定するときは、このステップを繰り返します。
ステップ 4	**line vty** *line_number* [*ending_line_number*] **transport input ssh**	（任意）仮想端末回線の設定を指定します。 • ライン コンフィギュレーション モードを開始して、仮想端末回線の設定を行います。*line_number* と *ending_line_number* には、回線のペアを指定します。指定できる範囲は 0 ～ 15 です。 • スイッチが SSH ではない Telnet 接続を拒否するように指定します。これにより、ルータを SSH 接続だけに制限します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチの SSH サーバ接続のステータスを表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの SSH 制御パラメータに戻すには、**no ip ssh** {**timeout** | **authentication-retries**} グローバル コンフィギュレーション コマンドを使用します。

SSH の設定とステータスの表示

SSH サーバの設定とステータスを表示するには、表 11-6 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 11-6　SSH サーバの設定とステータスを表示するためのコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、次の URL にある『*Cisco IOS Security Command Reference, Cisco IOS Release 12.2*』の「Other Security Features」の「Secure Shell Commands」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7cd.html

Secure Socket Layer HTTP 用のスイッチの設定

ここでは、HTTP 1.1 のサーバおよびクライアントに対して Secure Socket Layer（SSL）バージョン 3.0 のサポートを設定する方法を説明します。SSL は、サーバ認証、暗号化、メッセージ整合性、および HTTP クライアント認証の機能を備え、セキュアな HTTP 通信を可能にします。この機能を使用するには、暗号化ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用したり、暗号化ソフトウェアのファイルを Cisco.com からダウンロードしたりするには、許可を得る必要があります。暗号化イメージの詳細については、このリリースに対応するリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「セキュア HTTP サーバおよびクライアントの概要」（P.11-48）
- 「セキュア HTTP サーバおよびクライアントの設定」（P.11-50）
- 「セキュア HTTP のサーバとクライアントのステータスの表示」（P.11-54）

ここで使用する設定例やコマンドの構文および使用方法の詳細については、次の URL にある Cisco IOS Release 12.2(15)T の「HTTPS：HTTP Server and Client with SSL 3.0」の機能説明を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008015a4c6.html

セキュア HTTP サーバおよびクライアントの概要

セキュアな HTTP 接続では、HTTP サーバとの間でやり取りされるデータは、インターネット上で送信される前に暗号化されます。SSL 暗号化を使用する HTTP が提供するセキュアな接続を使用すると、Web ブラウザからのスイッチの設定のような機能が可能になります。セキュア HTTP サーバおよびセキュア HTTP クライアントのシスコによる実装では、SSL バージョン 3.0 の実装とアプリケーション層の暗号化を使用します。HTTP over SSL は HTTPS と略されます。セキュアな接続の URL は、http:// ではなく https:// で始まります。

HTTP セキュア サーバ（スイッチ）の主な役割は、指定されているポート（デフォルトの HTTPS ポートは 443）で HTTPS 要求を待ち受けて、要求を HTTP 1.1 Web サーバに渡すことです。HTTP 1.1 サーバは要求を処理して応答（ページ）を HTTP セキュア サーバに返送し、HTTP セキュア サーバは元の要求に応答します。

HTTP セキュア クライアント（Web ブラウザ）の主な役割は、HTTPS ユーザ エージェント サービスに対する Cisco IOS アプリケーション要求に応答し、アプリケーションに対して HTTPS ユーザ エージェント サービスを実行し、応答をアプリケーションに戻すことです。

認証局のトラストポイント

Certificate Authority（CA; 認証局）は、証明書の要求を管理し、参加しているネットワーク装置に証明書を発行します。これらのサービスは、参加している装置のためにセキュリティ キーと証明書を一元的に管理します。特定の CA サーバは*トラストポイント*と呼ばれます。

接続が試みられると、HTTPS サーバは指定された CA トラストポイントから取得した認証済みの X.509v3 証明書をクライアントに発行することで、セキュアな接続を提供します。これに対し、クライアント（通常は Web ブラウザ）は、証明書を認証できる公開キーを持っています。

セキュアな HTTP 接続のために、CA トラストポイントを設定することを強く推奨します。HTTPS サーバを実行する装置に対して CA トラストポイントを設定しないと、サーバは自分自身を認証し、必要な RSA キー ペアを生成します。自己認証（自己署名）された証明書は十分なセキュリティを提供しないので、接続しているクライアントは証明書が自己認証されていることを示す通知を生成し、ユーザは接続を許可または拒否できます。このオプションは、内部ネットワーク トポロジ（テスト用など）に適しています。

CA トラストポイントを設定していない場合、セキュア HTTP 接続をイネーブルにすると、セキュア HTTP サーバ（またはクライアント）用の一時的または永続的な自己署名証明書が、自動的に生成されます。

- スイッチにホスト名およびドメイン名を設定していない場合は、一時的な自己署名証明書が生成されます。スイッチが再起動した場合、一時的な自己署名証明書は失われ、新しい一時的な自己署名証明書が割り当てられます。
- スイッチにホスト名とドメイン名を設定してある場合は、永続的な自己署名証明書が生成されます。この証明書は、スイッチを再起動した場合、またはセキュア HTTP サーバをディセーブルにした場合でもアクティブ状態のままになり、次にセキュア HTTP 接続を再びイネーブルにするとまだ存在しています。

（注） 認証局およびトラストポイントは、装置ごとに個別に設定する必要があります。他の装置からコピーしても、コピー先のスイッチでは無効になります。

自己署名証明書が生成されている場合、この情報は **show running-config** 特権 EXEC コマンドの出力に含まれます。次の例は、このコマンドからの出力で自己署名証明書が表示されている部分です。

```
Switch# show running-config
Building configuration...

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3080755072
 revocation-check none
 rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
 certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109

<output truncated>
```

セキュア HTTP サーバをディセーブルにし、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで、この自己署名証明書を削除できます。あとでセキュア HTTP サーバを再びイネーブルにすると、新しい自己署名証明書が生成されます。

（注）　*TP self-signed* に続く値は、装置のシリアル番号によって決まります。

オプションのコマンド（**ip http secure-client-auth**）を使用することで、HTTPS サーバからクライアントに X.509v3 証明書を要求できます。クライアントを認証すると、サーバがそれ自体で認証するよりもセキュリティが向上します。

認証局の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Configuring Certification Authority Interoperability」を参照してください。

CipherSuite

CipherSuite は、SSL 接続で使用する暗号化アルゴリズムとダイジェスト アルゴリズムを指定します。HTTPS サーバに接続するときに、クライアントの Web ブラウザはサポートされる CipherSuite のリストを提供し、クライアントとサーバはリストの中で両方がサポートするものから最善の暗号化アルゴリズムを使用するようにネゴシエートします。たとえば、Netscape Communicator 4.76 は、RSA 公開キー暗号化、MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC の U.S. セキュリティをサポートします。

可能な最善の暗号化を使用するには、Microsoft Internet Explorer Version 5.5（またはそれ以降）や Netscape Communicator Version 4.76（またはそれ以降）などの 128 ビット暗号化をサポートするクライアント ブラウザを使用する必要があります。SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化ではないので、他の CipherSuite よりもセキュリティが劣ります。

より安全で複雑な CipherSuite ほど、必要な処理時間が長くなります。次に、スイッチがサポートする CipherSuite を、ルータの処理（速度）が速いものから遅いものの順に示します。

1. SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化には DES-CBC を使用し、メッセージのダイジェストには SHA を使用する RSA キー交換（RSA 公開キー暗号化）
2. SSL_RSA_WITH_RC4_128_MD5：RC4 128 ビット暗号化と MD5 のメッセージ ダイジェストを使用する RSA キー交換
3. SSL_RSA_WITH_RC4_128_SHA：RC4 128 ビット暗号化と SHA のメッセージ ダイジェストを使用する RSA キー交換
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化には 3DES と DES-EDE3-CBC を使用し、メッセージのダイジェストには SHA を使用する RSA キー交換

RSA は（指定されている暗号化とダイジェスト アルゴリズムの組み合わせとともに）、キーの生成と、SSL 接続での認証の両方に使用されます。この使用方法は、CA トラストポイントが設定されているかどうかには関係ありません。

セキュア HTTP サーバおよびクライアントの設定

SSL のデフォルト設定

標準 HTTP サーバはイネーブルです。

SSL はイネーブルです。

CA トラストポイントは設定されていません。

自己署名証明書は生成されません。

SSL 設定時の注意事項

SSL がスイッチ クラスタで使用されると、SSL セッションはクラスタ コマンダで終了します。クラスタ メンバー スイッチは標準 HTTP を実行する必要があります。

CA トラストポイントを設定する前に、システム クロックを設定する必要があります。クロックが設定されていない場合は、日付が正しくないために証明書が拒否されます。

CA トラストポイントの設定

セキュアな HTTP 接続のために、正式な CA トラストポイントを設定することを推奨します。CA トラストポイントの方が自己署名証明書よりも安全です。

CA トラストポイントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *hostname*	スイッチのホスト名を指定します（ホスト名をまだ設定していない場合に限り必要）。ホスト名はセキュリティ キーと証明書のために必要です。
ステップ 3	**ip domain-name** *domain-name*	スイッチの IP ドメイン名を指定します（IP ドメイン名をまだ設定していない場合に限り必要）。ドメイン名はセキュリティ キーと証明書のために必要です。
ステップ 4	**crypto key generate rsa**	（任意）RSA キー ペアを生成します。スイッチの証明書を取得するには、先に RSA キー ペアが必要です。RSA キー ペアは自動的に生成されます。このコマンドを使用すると、必要な場合にキーを再生成できます。
ステップ 5	**crypto ca trustpoint** *name*	CA トラストポイントのローカル設定名を指定して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	**enrollment url** *url*	スイッチが証明書要求を送信する宛先の URL を指定します。
ステップ 7	**enrollment http-proxy** *host-name port-number*	（任意）HTTP プロキシ サーバ経由で CA から証明書を取得するようにスイッチを設定します。
ステップ 8	**crl query** *url*	Certificate Revocation List（CRL; 証明書失効リスト）を要求してピアの証明書が失効していないことを確認するように、スイッチを設定します。
ステップ 9	**primary**	（任意）トラストポイントを CA 要求のプライマリ（デフォルト）トラストポイントとして使用するように指定します。
ステップ 10	**exit**	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto ca authentication** *name*	CA の公開キーを取得して CA を認証します。ステップ 5 で使用したものと同じ名前を使用します。
ステップ 12	**crypto ca enroll** *name*	指定した CA トラストポイントから証明書を取得します。このコマンドは、各 RSA キー ペアの署名付き証明書を要求します。

	コマンド	目的
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show crypto ca trustpoints**	設定を確認します。
ステップ 15	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

CA と関連付けられているすべての ID 情報および証明書を削除するには、**no crypto ca trustpoint** *name* グローバル コンフィギュレーション コマンドを使用します。

セキュア HTTP サーバの設定

証明書に認証局を使用している場合は、HTTP サーバをイネーブルにする前に、前記の手順を使用してスイッチに CA トラストポイントを設定する必要があります。CA トラストポイントを設定していない場合は、セキュア HTTP サーバを初めてイネーブルにしたときに、自己署名証明書が生成されます。サーバを設定したあとは、標準とセキュアの両方の HTTP サーバに適用されるオプション（パス、適用するアクセス リスト、最大接続数、タイムアウト ポリシー）を設定できます。

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的

ステップ 1	**show ip http server status**	（任意）HTTP サーバのステータスを表示し、セキュア HTTP サーバ機能がソフトウェアでサポートされているかどうかを確認します。出力に次のいずれかの行が表示される必要があります。
		`HTTP secure server capability: Present`
		`or`
		`HTTP secure server capability: Not present`

ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http secure-server**	ディセーブルになっている場合は、HTTPS サーバをイネーブルにします。HTTPS サーバはデフォルトでイネーブルになっています。
ステップ 4	**ip http secure-port** *port-number*	（任意）HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。有効なオプションは、443 または 1025 ～ 65535 の範囲の任意の値です。
ステップ 5	**ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する必要がない場合は、サーバとクライアントに両方がサポートする CipherSuite をネゴシエートさせます。これはデフォルトです。
ステップ 6	**ip http secure-client-auth**	（任意）接続処理の間に認証用の X.509v3 証明書をクライアントに要求するように HTTP を設定します。デフォルトでは、クライアントはサーバに証明書を要求しますが、サーバはクライアントの認証を試みません。
ステップ 7	**ip http secure-trustpoint** *name*	X.509v3 セキュリティ証明書を取得し、クライアントの証明書接続を認証するために使用する CA トラストポイントを指定します。 **（注）**　このコマンドを使用する場合は、前記の手順に従って CA トラストポイントをすでに設定してあるものと見なされます。
ステップ 8	**ip http path** *path-name*	（任意）HTML ファイルのベース HTTP パスを設定します。このパスでは、ローカル システム上の HTTP サーバ ファイルの場所を指定します（通常はシステムのフラッシュ メモリにあります）。
ステップ 9	**ip http access-class** *access-list-number*	（任意）HTTP サーバへのアクセスを許可するために使用するアクセス リストを指定します。

	コマンド	目的
ステップ 10	**ip http max-connections** *value*	（任意）HTTP サーバに対して許可する同時接続の最大数を設定します。指定できる範囲は 1 ～ 16 です。デフォルト値は 5 です。
ステップ 11	**ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value*	（任意）定義されている状況で HTTP サーバへの接続を開いておくことのできる時間の長さを指定します。 • **idle**：データを受信しない、または応答を送信できない状態の最大時間。指定できる範囲は 1 ～ 600 秒です。デフォルト値は 180 秒（3 分）です。 • **life**：接続が確立されてからの最大時間。指定できる範囲は 1 ～ 86400 秒（24 時間）です。デフォルト値は 180 秒です。 • **requests**：持続している接続で処理される要求の最大数。最大値は 86400 です。デフォルトは 1 です。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip http server secure status**	HTTP セキュア サーバのステータスを表示して、設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

標準 HTTP サーバをディセーブルにするには、**no ip http server** グローバル コンフィギュレーション コマンドを使用します。セキュア HTTP サーバをディセーブルにするには、**no ip http secure-server** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、**no ip http secure-port** および **no ip http secure-ciphersuite** グローバル コンフィギュレーション コマンドを使用します。クライアント認証を不要にするには、**no ip http secure-client-auth** グローバル コンフィギュレーション コマンドを使用します。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、https://*URL* と入力します。URL は、サーバ スイッチの IP アドレスまたはホスト名です。デフォルト ポート以外のポートを設定した場合は、URL の後ろにポート番号も指定する必要があります。次に例を示します。

```
https://209.165.129:1026
```

または

```
https://host.domain.com:1026
```

セキュア HTTP クライアントの設定

標準 HTTP クライアントとセキュア HTTP クライアントは、常にイネーブルになっています。セキュア HTTP クライアント証明書には、認証局が必要です。次の手順では、すでにスイッチに CA トラストポイントを設定してあるものと見なされます。CA トラストポイントが設定されておらず、リモート HTTPS サーバでクライアント認証が必要な場合は、セキュア HTTP クライアントへの接続は失敗します。

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip http client secure-trustpoint** *name*	（任意）リモート HTTP サーバがクライアントの認証を要求する場合は、使用する CA トラストポイントを指定します。このコマンドを使用する場合は、前記の手順を使用して CA トラストポイントをすでに設定してあるものと見なされます。クライアント認証が必要ない場合、またはプライマリ トラストポイントが設定されている場合は、このコマンドは任意です。

	コマンド	目的
ステップ 3	**ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する必要がない場合は、サーバとクライアントに両方がサポートする CipherSuite をネゴシエートさせます。これはデフォルトです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip http client secure status**	HTTP セキュア サーバのステータスを表示して、設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

クライアント トラストポイントの設定を削除するには、**no ip http client secure-trustpoint** *name* を使用します。クライアントに事前に設定されている CipherSuite の指定を削除するには、**no ip http client secure-ciphersuite** を使用します。

セキュア HTTP のサーバとクライアントのステータスの表示

SSL セキュア サーバおよびクライアントのステータスを表示するには、表 11-7 に示す特権 EXEC コマンドを使用します。

表 11-7　SSL セキュア サーバおよびクライアントのステータスを表示するためのコマンド

コマンド	目的
show ip http client secure status	HTTP セキュア クライアントの設定を表示します。
show ip http server secure status	HTTP セキュア サーバの設定を表示します。
show running-config	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

Secure Copy Protocol 用のスイッチの設定

Secure Copy Protocol（SCP）機能は、スイッチの設定またはスイッチのイメージ ファイルをコピーするためのセキュアで認証された方法を提供します。SCP は、Berkeley r-tools の代わりのセキュアな方式を提供するアプリケーションとプロトコルであるセキュア シェル（SSH）に依存します。

SSH を使用するには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは、セキュアな転送を SSH に依存する SCP と同じです。

SSH は AAA 認証に依存し、SCP も AAA 認可に依存するので、正しく設定する必要があります。

- SCP をイネーブルにする前に、スイッチに SSH、認証、および認可を正しく設定する必要があります。
- SCP はセキュアな転送を SSH に依存するので、ルータには Rivest、Shamir、Adelman（RSA）キー ペアが必要です。

（注） SCP を使用するときは、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときにパスワードを入力する必要があります。

セキュア コピーの概要

セキュア コピー機能を設定するには、次の概念を理解しておく必要があります。

SCP の動作は、Berkeley r-tools スイートに含まれるリモート コピー（rcp）の動作と似ていますが、SCP はセキュリティを SSH に依存します。また、SCP では、ユーザが正しい権限レベルを持っているかどうかをルータが判断できるように、認証、認可、アカウンティング（AAA）認可を設定する必要もあります。

適切な認可を持っているユーザは、SCP の **copy** コマンドを使用してスイッチとの間で Cisco IOS File System（IFS; IOS ファイル システム）の任意のファイルをコピーできます。認可された管理者は、ワークステーションからこれを行うこともできます。

SCP の設定および確認方法の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4*』の「Secure Copy Protocol」を参照してください。
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_copy_ps6350_TSD_Products_Configuration_Guide_Chapter.html

CHAPTER 12

IEEE 802.1X ポートベースの認証の設定

IEEE 802.1X ポートベースの認証により、認証されていない装置（クライアント）がネットワークにアクセスするのを防止します。IE 3000 スイッチのコマンド リファレンスと、『Cisco IOS Security Command Reference, Release 12.2』の「RADIUS Commands」に、コマンドの構文と使用方法の情報があります。

この章の内容は次のとおりです。

IEEE 802.1X ポートベースの認証の概要

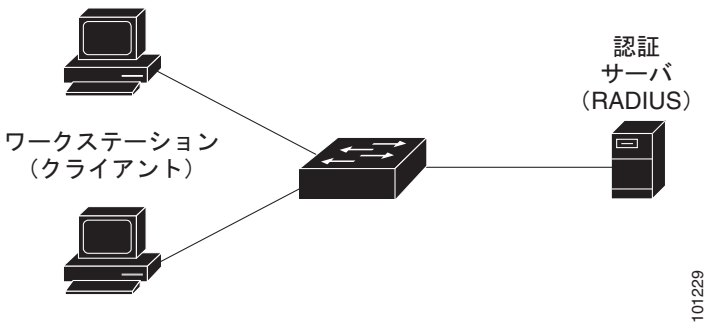
この標準は、クライアント サーバ ベースのアクセス制御と認証プロトコルを定義し、認可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを防ぎます。認証サーバは、スイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN サービスを利用できるようにします。

IEEE 802.1X アクセス制御では、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、および Spanning Tree Protocol（STP; スパニング ツリー プロトコル）トラフィックしか許可されません。認証後は、通常のトラフィックがポート経由で送受信されます。

装置の役割

802.1X ポートベースの認証での装置の役割：

図 12-1　802.1X 装置の役割



- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答する装置（ワークステーション）。ワークステーションでは、802.1X に準拠するクライアント ソフトウェア（Microsoft Windows XP オペレーティング システムで提供されるクライアント ソフトウェアなど）を実行している必要があります（クライアントは、802.1X 標準では*サプリカント*といいます）。

  （注）　Windows XP のネットワーク接続および 802.1X 認証の問題を解決するには、次の URL にあるマイクロソフト サポート技術情報の記事を参照してください。
  http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ*：クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対してトランスペアレントに行われます。このリリースでは、Extensible Authentication Protocol（EAP）拡張機能を備えた RADIUS セキュリティ システムだけが認証サーバとしてサポートされています。この認証サーバは、Cisco Secure Access Control Server Version 3.0 以降で使用可能です。RADIUS はクライアント/サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- *スイッチ*（エッジ スイッチまたはワイヤレス アクセス ポイント）：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバの間の仲介装置（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています（スイッチは、802.1X 標準では*オーセンティケータ*です）。

  スイッチが EAPOL フレームを受信して認証サーバにリレーする際、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更は行われず、認証サーバはネイティブ フレーム フォーマット内の EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

  仲介装置として動作できる装置は、IE 3000、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940 の各スイッチや、ワイヤレス アクセス ポイントなどです。これらの装置では、RADIUS クライアントおよび 802.1X 認証をサポートするソフトウェアを実行している必要があります。

認証プロセス

802.1X ポートベースの認証がイネーブルになっていて、クライアントが 802.1X に準拠するクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

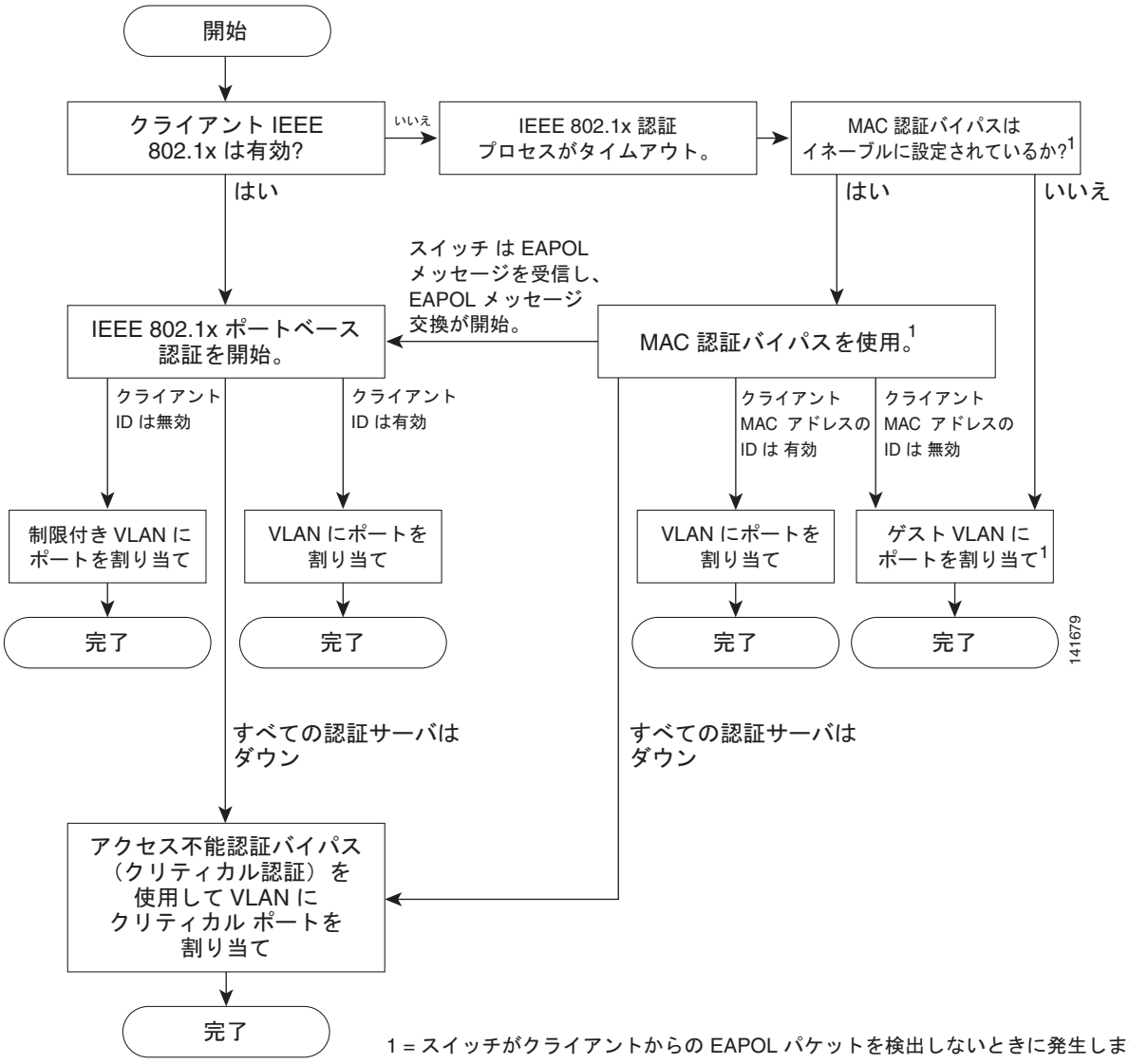
- クライアントの識別情報が有効で、802.1X 認証が成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- 802.1X 認証が EAPOL メッセージ交換を待機している間に時間切れとなり、Media Access Control（MAC; メディア アクセス制御）認証バイパスがイネーブルになっている場合、スイッチはクライアントの MAC アドレスを認証に使用できます。クライアントの MAC アドレスが有効で、認可が成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアントの MAC が無効で、認可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチは限られたサービスを提供するゲスト VLAN にクライアントを割り当てます。

- スイッチが 802.1X 対応のクライアントから無効な識別情報を取得し、制限付き VLAN が指定されている場合、スイッチは限られたサービスを提供する制限付き VLAN にクライアントを割り当てることができます。
- RADIUS 認証サーバが使用不可（ダウン）であり、アクセス不能認証バイパスがイネーブルになっている場合、スイッチは RADIUS 設定またはユーザ指定のアクセス VLAN でポートを critical-authentication ステートに置くことにより、ネットワークへのアクセスをクライアントに許可します。

（注）　アクセス不能認証バイパスは、クリティカル認証または Authentication、Authorization、Accounting（AAA; 認証、認可、アカウンティング）失敗ポリシーとも呼ばれます。

図 12-2 に認証プロセスを示します。

図 12-2　認証のフローチャート



1 = スイッチがクライアントからの EAPOL パケットを検出しないときに発生します。

スイッチは、次の状態のいずれかが発生した場合、クライアントを再認証します。

- 定期的な再認証がイネーブルになっていて、再認証タイマーが期限切れになる。

  スイッチ固有の値を使用するか、RADIUS サーバの値に基づくように、再認証タイマーを設定できます。

  RADIUS サーバを使用する 802.1X 認証を設定したあと、スイッチは Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS 属性（属性 [27]）は、再認証が行われるまでの時間を指定します。

  Termination-Action RADIUS 属性（属性 [29]）は、再認証中に実行するアクションを指定します。このアクションは、*Initialize* および *ReAuthenticate* です。*Initialize* アクションを設定した場合（属性値は *DEFAULT*）、802.1X セッションは終了し、接続は再認証中に失われます。*ReAuthenticate* アクションを設定した場合（属性値は RADIUS-Request）、セッションは再認証中に影響を受けません。

- **dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力することにより、クライアントを手動で再認証する。

ポート上で Multidomain Authentication（MDA; マルチドメイン認証）がイネーブルになっている場合、このフローを使用できますが、音声認証に適用されるいくつかの例外があります。MDA の詳細については、「マルチドメイン認証」（P.12-12）を参照してください。

認証の開始およびメッセージ交換

802.1X 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** または **dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポートで認証をイネーブルにした場合、スイッチは、リンク ステートがダウンからアップに変化したときに、またはポートがアップのままで認証されていない限り定期的に、認証を開始します。スイッチは、EAP 要求/アイデンティティ フレームをクライアントに送信して識別情報を要求します。クライアントはフレームを受信すると、EAP 応答/アイデンティティ フレームで応答します。

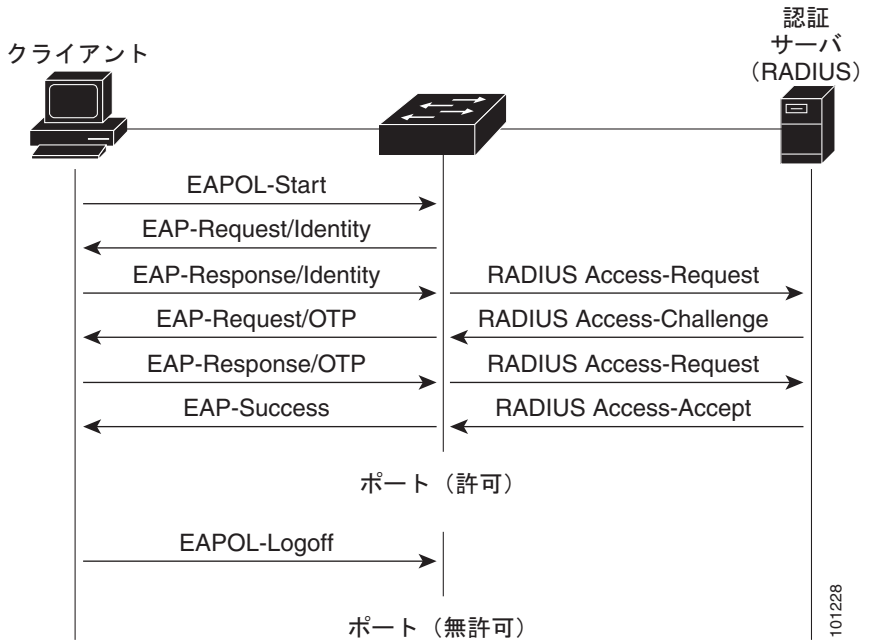
ただし、クライアントが起動時にスイッチから EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントは EAPOL 開始フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）　ネットワーク アクセス装置で 802.1X 認証がイネーブルになっていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントはポートが認可ステートであるものとしてフレームを送信します。ポートが認可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「認可ステートおよび無認可ステートのポート」（P.12-10）を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介装置としての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは認可ステートになります。認証が失敗した場合は、認証を再試行するか、限られたサービスを提供する VLAN にポートが割り当てられるか、ネットワーク アクセスが許可されません。詳細については、「認可ステートおよび無認可ステートのポート」（P.12-10）を参照してください。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 12-3 に、クライアントが RADIUS サーバとの間で One-Time-Password（OTP; ワンタイム パスワード）認証方式を使用する場合に行われるメッセージ交換を示します。

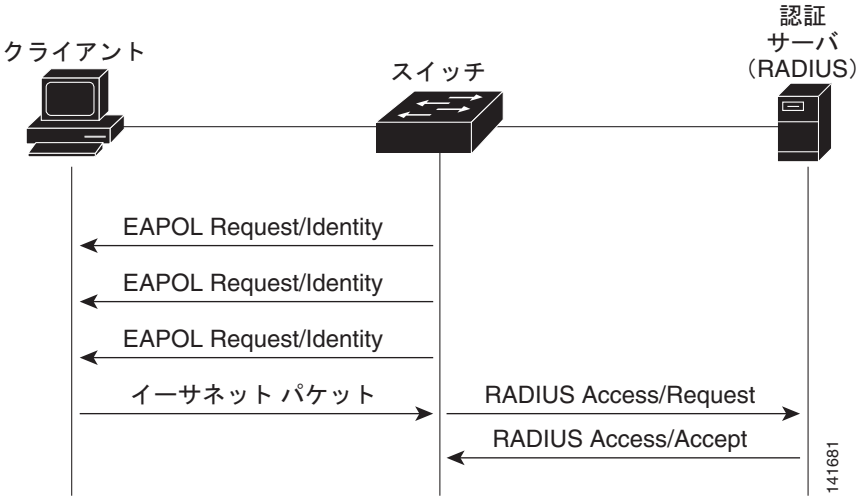
図 12-3　メッセージ交換



802.1X 認証が EAPOL メッセージ交換を待機している間に時間切れとなり、MAC 認証バイパスがイネーブルになっている場合、スイッチはクライアントからのイーサネット パケットを検出したときにクライアントを認可できます。スイッチは、クライアントの MAC アドレスを識別情報として使用し、この情報を RADIUS サーバに送信する RADIUS-access/request フレームに含めます。サーバがスイッチに RADIUS-access/accept フレームを送信したあと（認可が成功）、ポートは認可されます。認可が失敗し、ゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。スイッチがイーサネット パケットを待機しているときに EAPOL パケットを検出した場合、スイッチは MAC 認証バイパス プロセスを停止し、802.1X 認証を停止します。

図 12-4 に、MAC 認証バイパス中に行われるメッセージ交換を示します。

図 12-4　MAC 認証バイパス中のメッセージ交換



認証マネージャ

Cisco IOS Release 12.2(46)SE 以前では、このスイッチと Catalyst 6000 などの他のネットワーク装置で、CLI コマンドおよびメッセージなどの同じ認可方式を使用することはできませんでした。独立した認証設定を使用する必要がありました。Cisco IOS Release 12.2(50)SE 以降では、ネットワーク内のすべての Catalyst スイッチで同じ認可方式がサポートされます。

Cisco IOS Release 12.2(55)SE では、認証マネージャからの詳細なシステム メッセージのフィルタリングがサポートされます。詳細については、「認証マネージャの CLI コマンド」（P.12-9）を参照してください。

ポートベースの認証方式

表 12-1 に、次のホスト モードでサポートされる認証方式を示します。

- シングル ホスト：1 つのポートで 1 つのデータ ホストまたは音声ホスト（クライアント）だけを認証できます。
- マルチ ホスト：同じポートで複数のデータ ホストを認証できます（ポートがマルチホスト モードで無認可ステートになった場合、スイッチは接続されたすべてのクライアントへのネットワーク アクセスを拒否します）。
- マルチドメイン認証（MDA）：同じスイッチ ポートでデータ装置と音声装置の両方を認証できます。ポートは、データ ドメインと音声ドメインに分割されます。
- マルチ認証：データ VLAN で複数のホストを認証できます。音声 VLAN が設定されている場合、このモードでは VLAN で 1 つのクライアントが許可されます。

表 12-1　802.1X の機能

認証方式	モード			
	シングル ホスト	マルチ ホスト	MDA[1]	マルチ認証[2]
802.1X	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[4] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]	ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]	ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
スタンドアロン Web 認証[4]	プロキシ ACL、Filter-Id 属性、ダウンロード可能 ACL[2]			

表 12-1　802.1X の機能 （続き）

認証方式	モード			
	シングル ホスト	マルチ ホスト	MDA[1]	マルチ認証[2]
NAC レイヤ 2 IP 検証	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
フォールバック方式としての Web 認証[5]	プロキシ ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	プロキシ ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	プロキシ ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	プロキシ ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3]

1. MDA = マルチドメイン認証。
2. 「*multiauth*」とも呼ばれます。
3. Cisco IOS Release 12.2(50)SE 以降でサポートされます。
4. Cisco IOS Release 12.2(50)SE 以降でサポートされます。
5. 802.1X 認証をサポートしないクライアント用。

ユーザ単位 ACL と Filter-Id

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、ユーザ単位 ACL と Filter-Id は、シングルホスト モードだけでサポートされていました。Cisco IOS Release 12.2(50) では、MDA 対応ポートおよびマルチ認証対応ポートに対するサポートが追加されました。12.2(52)SE 以降では、マルチ ホスト モードのポートに対するサポートが追加されました。

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、スイッチで設定された ACL は、Catalyst 6000 スイッチなど、Cisco IOS ソフトウェアを実行する別の装置で設定された ACL と互換性がありませんでした。

Cisco IOS Release 12.2(50)SE 以降では、スイッチで設定された ACL は、Cisco IOS リリースを実行する他の装置と互換性があります。

（注）　ACL で送信元として設定できるのは **any** だけです。

（注）　マルチホスト モード用に設定されたすべての ACL では、ステートメントの送信元部分が *any* である必要があります（たとえば、**permit icmp** *any* **host 10.10.1.1**）。

定義されたすべての ACL の送信元ポートで *any* を指定する必要があります。それ以外の場合は、ACL を適用できず、認可は失敗します。シングル ホストは、下位互換性をサポートするための唯一の例外です。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。1 つのホストに適用された ACL ポリシーは、別のホストのトラフィックに影響を与えません。

マルチホスト ポートで 1 つのホストだけが認証され、他のホストは認証なしでネットワーク アクセスを取得する場合、送信元アドレスで *any* を指定することにより、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

認証マネージャの CLI コマンド

認証マネージャのインターフェイス コンフィギュレーション コマンドは、802.1X、MAC 認証バイパス、Web 認証などのすべての認証方式を制御します。認証マネージャ コマンドは、接続したホストに適用される認証方式の優先順位と順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モード、認証タイマーなどの汎用的な認証機能を制御します。汎用の認証コマンドには、**authentication host-mode**、**authentication violation**、**authentication timer** などのインターフェイス コンフィギュレーション コマンドがあります。

802.1X に固有のコマンドは、**dot1x** というキーワードで始まります。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。一方、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは、802.1X 認証をグローバルにだけイネーブルまたはディセーブルにします。

（注） 802.1X 認証をグローバルにディセーブルにした場合、Web 認証など、他の認証方式はそのポートでイネーブルのままになります。

認証マネージャ コマンドは、以前の 802.1X コマンドと同じ機能を提供します。

表 12-2　認証マネージャ コマンドと以前の 802.1X コマンド

Cisco IOS Release 12.2(50)SE 以降の認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前の相当する 802.1X コマンド	説明
authentication control-direction {both | in}	**dot1x control-direction {both | in}**	Wake-on-LAN（WoL）機能を含む認証をイネーブルにし、ポート制御を単一方向または双方向に設定します。
authentication event	**dot1x auth-fail vlan**	ポートで制限付き VLAN をイネーブルにします。
	dot1x critical (interface configuration)	アクセス不能認証バイパス機能をイネーブルにします。
	dot1x guest-vlan6	アクティブ VLAN をゲスト VLAN として指定します。
authentication fallback *fallback-profile*	**dot1x fallback** *fallback-profile*	認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode [multi-auth | multi-domain | multi-host | single-host]	**dot1x host-mode {single-host | multi-host | multi-domain}**	認可ポート上で単一のホスト（クライアント）または複数のホストを許可します。
authentication order	**dot1x mac-auth-bypass**	使用する認証方式の順序を定義する柔軟性を提供します。
authentication periodic	**dot1x reauthentication**	クライアントの定期的な再認証をイネーブルにします。
authentication port-control {auto | force-authorized | force-un authorized}	**dot1x port-control {auto | force-authorized | force-unauthorized}**	ポートの認可ステートの手動制御をイネーブルにします。

表 12-2　認証マネージャ コマンドと以前の 802.1X コマンド（続き）

Cisco IOS Release 12.2(50)SE 以降の認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前の相当する 802.1X コマンド	説明
authentication timer	**dot1x timeout**	タイマーを設定します。
authentication violation {**protect** | **restrict** | **shutdown**}	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	新しい装置がポートに接続した場合、または最大数の装置がポートに接続したあとに新しい装置がそのポートに接続した場合に発生する違反モードを設定します。

Cisco IOS Release 12.2(55)SE 以降、認証マネージャで生成された詳細なシステム メッセージをフィルタリングできるようになりました。フィルタリングされる内容は、通常、認証成功に関連しています。802.1X 認証および MAB 認証の詳細メッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドがあります。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの詳細メッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1X 認証の詳細メッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC Authentication Bypass（MAB; MAC 認証バイパス）の詳細メッセージをフィルタリングします。

詳細については、このリリースのコマンド リファレンスを参照してください。

認可ステートおよび無認可ステートのポート

802.1X 認証中に、スイッチ ポートのステートに応じて、スイッチはクライアントにネットワークへのアクセスを許可できます。ポートは最初、*無認可*ステートです。このステートの間、音声 VLAN ポートとして設定されていないポートは、802.1X 認証、CDP、および STP のパケットを除くすべての入力トラフィックと出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは*認可*ステートに変化し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、ポートはクライアントの認証が成功する前に、VoIP トラフィックおよび 802.1X プロトコル パケットを許可します。

802.1X 認証をサポートしていないクライアントが、無認可の 802.1X ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無認可ステートとなり、クライアントはネットワーク アクセスを許可されません。

一方、802.1X 対応のクライアントが、802.1X 標準を実行していないポートに接続すると、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが認可ステートであるものとしてフレーム送信を開始します。

authentication port-control または **dot1x port-control** インターフェイス コンフィギュレーション コマンドと次のキーワードを使用して、ポートの認可ステートを制御できます。

- **force-authorized**：802.1X 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを認可ステートに変化させます。ポートはクライアントの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。これは、デフォルト設定です。
- **force-unauthorized**：クライアントによる認証の試みをすべて無視し、ポートを無認可ステートのままにします。スイッチはポートを介してクライアントに認証サービスを提供できません。

- **auto**：802.1X 認証をイネーブルにします。ポートは最初、無認可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変化したとき、または EAPOL 開始フレームを受信したときに、認証プロセスが開始されます。スイッチは、クライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC アドレスを使用して、ネットワークへのアクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが認可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無認可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信できます。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL ログオフ メッセージを送信します。このメッセージにより、スイッチ ポートは無認可ステートに変化します。

ポートのリンク ステートがアップからダウンに変化した場合、または EAPOL ログオフ フレームを受信した場合に、ポートは無認可ステートに戻ります。

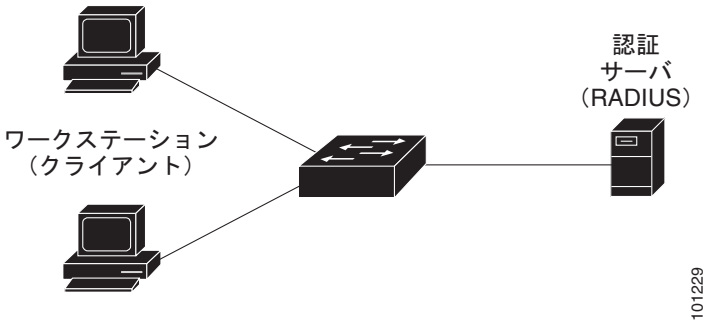
802.1X ホスト モード

802.1X ポートをシングルホスト モードまたはマルチホスト モードに設定できます。シングルホスト モード（図 12-1（P.12-2）を参照）では、1 つのクライアントだけを 802.1X 対応のスイッチ ポートに接続できます。スイッチは、ポートのリンク ステートがアップ ステートに変化したときに EAPOL フレームを送信することによりクライアントを検出します。クライアントがログオフした場合、または別のクライアントに代わった場合は、スイッチはポートのリンク ステートをダウンに変更し、ポートは無認可ステートに戻ります。

マルチホスト モードでは、単一の 802.1X 対応ポートに複数のホストを接続できます。図 12-5（P.12-11）に、ワイヤレス LAN における 802.1X ポートベースの認証を示します。このモードでは、すべてのクライアントにネットワーク アクセスを許可するために、接続されたホストのうちの 1 つを認証するだけで済みます。ポートが無認可ステートになった場合（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、スイッチは接続しているすべてのクライアントに対してネットワーク アクセスを拒否します。このトポロジでは、ワイヤレス アクセス ポイントが接続先クライアントの認証を処理し、スイッチに対するクライアントとしての役割も果たします。

マルチホスト モードがイネーブルの場合、802.1X 認証を使用してポートおよびポート セキュリティを認証し、クライアントの MAC アドレスを含むすべての MAC アドレスのネットワーク アクセスを管理できます。

図 12-5　マルチ ホスト モードの例



スイッチはマルチドメイン認証（MDA）をサポートします。MDA により、データ装置と、IP Phone（シスコ製品またはシスコ以外の製品）などの音声装置の両方で、同じスイッチ ポートに接続することが可能になります。詳細については、「マルチドメイン認証」（P.12-12）を参照してください。

マルチドメイン認証

スイッチはマルチドメイン認証（MDA）をサポートします。MDA により、データ装置と、IP Phone（シスコ製品またはシスコ以外の製品）などの音声装置を、同じスイッチ ポートで認証できます。ポートは、データ ドメインと音声ドメインに分割されます。

MDA では、装置認証の順序は強制されません。ただし、最良の結果を得るために、MDA 対応ポートでは音声装置を認証してからデータ装置を認証することを推奨します。

MDA を設定するには、次の注意事項に従ってください。

- スイッチ ポートを MDA 用に設定するには、「ホスト モードの設定」（P.12-43）を参照してください。
- ホスト モードをマルチドメインに設定する場合、IP Phone 用に音声 VLAN を設定する必要があります。詳細については、第 16 章「VLAN の設定」を参照してください。
- 音声装置を認可するには、Cisco Attribute-Value（AV）ペア属性を値 `device-traffic-class=voice` で送信するように AAA サーバを設定する必要があります。この値がない場合、スイッチは音声装置をデータ装置として扱います。
- ゲスト VLAN 機能および制限付き VLAN 機能は、MDA 対応ポートのデータ装置にだけ適用されます。スイッチは、認可に失敗した音声装置をデータ装置として扱います。
- 複数の装置がポートの音声ドメインまたはデータ ドメインで認可を試みた場合、errdisable になります。
- 装置が認可されるまで、ポートはトラフィックを廃棄します。シスコ製品ではない IP Phone または音声装置は、データ VLAN および音声 VLAN への接続を許可されます。データ VLAN では、音声装置が Dynamic Host Configuration Protocol（DHCP）サーバに接続して IP アドレスを取得し、音声 VLAN 情報を入手できます。音声装置が音声 VLAN 上での送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN でバインドしている音声装置の MAC アドレスは、ポート セキュリティの MAC アドレス制限にカウントされません。
- MDA では、MAC 認証バイパスをフォールバック メカニズムとして使用して、スイッチ ポートに 802.1X 認証をサポートしない装置を接続させることができます。詳細については、「MAC 認証バイパス」（P.12-36）を参照してください。
- ポートでデータ装置または*音声*装置が検出された場合、その装置の MAC アドレスは、認可が成功するまでブロックされます。認可が失敗した場合、MAC アドレスは 5 分間ブロックされたままになります。
- ポートが無認可ステートの間にデータ VLAN で 6 つ以上の装置が検出された場合、または*音声* VLAN で 2 つ以上の音声装置が検出された場合、ポートは errdisable になります。
- ポートのホスト モードがシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変化した場合、認可されたデータ装置は、ポートで認可されたままになります。ただし、ポートの音声 VLAN 上の Cisco IP Phone は、自動的に削除され、そのポートで再認証する必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック メカニズムは、ポートがシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変化したあとも設定されたままになります。

- ポートのホスト モードをマルチドメイン モードからシングルホスト モードまたはマルチホスト モードに切り替えると、認可されたすべての装置がポートから削除されます。
- データ ドメインを最初に認可し、ゲスト VLAN に配置した場合、802.1X に対応していない音声装置は、音声 VLAN 上でパケットをタグ付けして認証を開始する必要があります。IP Phone では、タグ付けされたトラフィックを送信する必要はありません（802.1X 対応の IP Phone でも同じです）。
- MDA 対応ポートでユーザ単位 ACL を使用することは推奨できません。ユーザ単位 ACL ポリシーを持つ認可された装置は、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与える可能性があります。ユーザ単位 ACL を強制するためにポートで使用できる装置は 1 つだけです。

詳細については、「ホスト モードの設定」（P.12-43）を参照してください。

802.1X マルチ認証モード

マルチ認証（multiauth）モードでは、データ VLAN 上で複数の認証済みクライアントを許可できます。各ホストは個別に認証されます。音声 VLAN が設定されている場合、このモードでは音声 VLAN 上でも 1 つのクライアントが許可されます（ポートが追加の音声クライアントを検出した場合、それらの音声クライアントはポートから破棄されますが、違反エラーは発生しません）。

ハブまたはアクセス ポイントが 802.1X 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。

802.1X に対応していない装置に対し、MAC 認証バイパスまたは Web 認証をホスト単位の認証フォールバック方式として使用して、1 つのポートで異なるホストを異なる方式により認証することができます。

マルチ認証ポートで認証できるデータ ホストの数に制限はありません。ただし、音声 VLAN が設定されている場合、許可される音声装置は 1 つだけです。ホスト制限が定義されておらず、違反がトリガーされないので、第 2 の音声装置が確認された場合、その装置は自動的に破棄されますが、違反はトリガーされません。

音声 VLAN 上で MDA 機能を実現するために、マルチ認証モードでは、認証サーバから受信した Vendor-Specific Attribute（VSA; ベンダー固有属性）に応じて、認証された装置がデータ VLAN または音声 VLAN に割り当てられます。

（注）　ポートがマルチ認証モードの場合、ゲスト VLAN および認証失敗 VLAN の各機能は、アクティブになりません。

クリティカル認証モードとクリティカル VLAN の詳細については、「802.1X 認証とアクセス不能認証バイパス」（P.12-23）を参照してください。

ポートでのマルチ認証モードの設定の詳細については、「ホスト モードの設定」（P.12-43）を参照してください。

MAC 移行

1 つのスイッチ ポートで MAC アドレスを認証しても、そのアドレスは、そのスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出した場合、そのアドレスは許可されません。

状況によっては、MAC アドレスを同じスイッチのあるポートから別のポートに移行する必要があります。たとえば、認証されたホストとスイッチ ポートの間に別の装置（ハブまたは IP Phone など）がある場合、そのホストを装置から接続解除し、同じスイッチの別のポートに直接接続することがあります。

装置が新しいポートで再認証されるように、MAC 移行をグローバルにイネーブルにすることができます。ホストが第 2 のポートに移行すると、最初のポートのセッションは削除され、新しいポートでホストが再認証されます。

MAC 移行は、すべてのホスト モードでサポートされます（認証されたホストは、ポートでイネーブルになっているホスト モードに関係なく、スイッチの任意のポートに移行できます）。

Cisco IOS Release 12.2(55)SE 以降、MAC 移行はポート セキュリティと共にすべてのホスト モードで設定できます。

あるポートから別のポートに MAC アドレスを移行すると、スイッチは元のポートでの認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。ポート セキュリティの動作は、MAC 移行を設定したときと同じです。

MAC 移行機能は、音声ホストとデータホストの両方に適用されます。

（注）　オープン認証モードでは、MAC アドレスは元のポートから新しいポートにすぐに移行され、新しいポートでの認証を必要としません。

詳細については、「MAC 移行のイネーブル化」（P.12-49）を参照してください。

MAC 置き換え

Cisco IOS Release 12.2(55)SE 以降、ホストが、別のホストが既に認証しているポートに接続を試行したときに発生する違反に対処するため、MAC 置き換え機能を設定できるようになりました。

（注）　マルチ認証モードでは違反がトリガーされないため、この機能はマルチ認証モードのポートには適用されません。マルチ ホスト モードでは最初のホストだけが認証を必要とするため、この機能はマルチ ホスト モードのポートには適用されません。

authentication violation インターフェイス コンフィギュレーション コマンドに **replace** キーワードを指定して設定した場合、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 新しい MAC アドレスが既存の認証済み MAC アドレスのポートで受信されます。
- 認証マネージャが、ポート上の現行データ ホストの MAC アドレスを新しい MAC アドレスで置き換えます。
- 認証マネージャが新しい MAC アドレスの認証プロセスを開始します。
- 認証マネージャが、新しいホストが音声ホストであると判断した場合、元の音声ホストが削除されます。

ポートがオープン認証モードの場合、新しい MAC アドレスはすべて、MAC アドレス テーブルにすぐに追加されます。

詳細については、「MAC 置き換えのイネーブル化」（P.12-49）を参照してください。

802.1X アカウンティング

802.1X 標準は、ネットワーク アクセスに対するユーザの認可方法および認証方法を定義しますが、ネットワークの使用状況を追跡しません。802.1X アカウンティングは、デフォルトでディセーブルになっています。802.1X アカウンティングをイネーブルにすると、802.1X 対応ポートで次のアクティビティをモニタできます。

- ユーザ認証の成功
- ユーザのログオフ
- リンクダウンの発生
- 再認証の成功
- 再認証の失敗

スイッチは 802.1X アカウンティングの情報を記録しません。代わりに、この情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定されている必要があります。

802.1X アカウンティングの Attribute-Value ペア

RADIUS サーバに送信される情報は、Attribute-Value（AV）ペアの形式で表されます。これらの AV ペアは、さまざまなアプリケーションにデータを提供します（たとえば、課金アプリケーションでは、RADIUS パケットの Acct-Input-Octets 属性または Acct-Output-Octets 属性の情報が必要になることがあります）。

AV ペアは、802.1X アカウンティング用に設定されたスイッチによって自動的に送信されます。スイッチでは、次の 3 種類の RADIUS アカウンティング パケットが送信されます。

- START：新しいユーザ セッションの開始時に送信されます。
- INTERIM：既存のセッション中に更新のために送信されます。
- STOP：セッションの終了時に送信されます。

表 12-3 に、AV ペアと、それらのペアがスイッチによって送信されるタイミングを示します。

表 12-3　アカウンティングの AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常に送信	常に送信	常に送信
属性 [4]	NAS-IP-Address	常に送信	常に送信	常に送信
属性 [5]	NAS-Port	常に送信	常に送信	常に送信
属性 [8]	Framed-IP-Address	送信なし	一部送信[1]	一部送信[1]
属性 [25]	Class	常に送信	常に送信	常に送信
属性 [30]	Called-Station-ID	常に送信	常に送信	常に送信
属性 [31]	Calling-Station-ID	常に送信	常に送信	常に送信
属性 [40]	Acct-Status-Type	常に送信	常に送信	常に送信
属性 [41]	Acct-Delay-Time	常に送信	常に送信	常に送信
属性 [42]	Acct-Input-Octets	送信なし	常に送信	常に送信
属性 [43]	Acct-Output-Octets	送信なし	常に送信	常に送信
属性 [44]	Acct-Session-ID	常に送信	常に送信	常に送信

表 12-3　アカウンティングの AV ペア （続き）

属性番号	AV ペア名	START	INTERIM	STOP
属性 [45]	Acct-Authentic	常に送信	常に送信	常に送信
属性 [46]	Acct-Session-Time	送信なし	常に送信	常に送信
属性 [49]	Acct-Terminate-Cause	送信なし	送信なし	常に送信
属性 [61]	NAS-Port-Type	常に送信	常に送信	常に送信

1. Framed-IP-Address AV ペアは、有効な Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在する場合にだけ送信されます。

スイッチによって送信されている AV ペアを表示するには、**debug radius accounting** 特権 EXEC コマンドを入力します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800872ce.html

AV ペアの詳細については、RFC 3580『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

802.1X 準備状態チェック

802.1X 準備状態チェックでは、すべてのスイッチ ポートでの 802.1X アクティビティをモニタし、802.1X をサポートするポートに接続された装置に関する情報を表示します。この機能を使用して、スイッチ ポートに接続された装置が 802.1X に対応しているかどうかを判断できます。802.1X 機能をサポートしない装置に対しては、MAC 認証バイパスや Web 認証などの代替認証を使用します。

この機能は、クライアント上のサプリカントが NOTIFY EAP 通知パケットによるクエリーをサポートする場合にだけ機能します。クライアントは、802.1X のタイムアウト値以内に応答する必要があります。

スイッチを 802.1X 準備状態チェック用に設定する方法の詳細については、「802.1X 準備状態チェックの設定」（P.12-37）を参照してください。

802.1X 認証と VLAN 割り当て

RADIUS サーバは、スイッチ ポートを設定するために VLAN 割り当てを送信します。RADIUS サーバのデータベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続しているクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声装置が認可され、RADIUS サーバが認可済みの VLAN を返した場合、ポート上の音声 VLAN は、割り当てられた音声 VLAN でパケットを送受信するように設定されます。マルチドメイン認証（MDA）対応ポートでは、音声 VLAN の割り当ては、データ VLAN の割り当てと同じように行われます。詳細については、「マルチドメイン認証」（P.12-12）を参照してください。

スイッチと RADIUS サーバで設定されている場合、802.1X 認証と VLAN 割り当てには次のような特徴があります。

- RADIUS サーバが VLAN を提供していないか、または 802.1X 認証がディセーブルの場合、ポートは認証が成功したあとにアクセス VLAN で設定されます。アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるすべてのパケットは、この VLAN に属します。
- 802.1X 認証がイネーブルになっているが、RADIUS サーバからの VLAN 情報が有効ではない場合、認可は失敗し、設定された VLAN は使用されたままになります。これにより、設定エラーによってポートが不適切な VLAN に予期せず表示されるのを防ぎます。

  設定エラーには、ルーテッド ポートへの VLAN、形式に誤りのある VLAN ID、存在しないまたは内部の（ルーテッド ポート）VLAN ID、RSPAN VLAN、シャット ダウンまたは停止している VLAN の指定などがあります。マルチドメイン ホスト ポートの場合、設定エラーは、設定済みまたは割り当て済みの音声 VLAN ID と一致するデータ VLAN の割り当て（またはその逆）を試みることによって発生することもあります。
- 802.1X 認証がイネーブルで RADIUS サーバからのすべての情報が有効の場合、認可された装置は認証後に指定した VLAN に配置されます。
- 802.1X ポートでマルチホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバによって指定されます）に配置されます。
- ポート セキュリティをイネーブルにしても、RADIUS サーバによって割り当てられた VLAN の動作に影響はありません。
- 802.1X 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1X ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置された場合、ポート アクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全に認可されていれば、同じことが音声装置に当てはまります。ただし、次の例外があります。
  - 一方の装置の VLAN 設定変更により、他方の装置が設定済みまたは割り当て済みの VLAN と一致した場合、ポート上のすべての装置の認可は中止され、マルチドメイン ホスト モードは、データ装置が設定された VLAN と音声装置が設定された VLAN が一致しない有効な設定が復元されるまで無効になります。
  - 音声装置が認可され、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除するか、設定値を *dot1p* または *untagged* に変更すると、音声装置は無認可になり、マルチドメイン ホスト モードはディセーブルになります。

ポートが強制認可、強制無認可、無認可、シャットダウンのいずれかのステートの場合、そのポートは設定済みのアクセス VLAN に配置されます。

VLAN 割り当て機能付きの 802.1X 認証は、トランク ポート、ダイナミック ポート、または VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）を使用したダイナミック アクセス ポート割り当てではサポートされていません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 認可をイネーブルにし、RADIUS サーバからのインターフェイス コンフィギュレーションを許可します。
- 802.1X 認証をイネーブルにします（VLAN 割り当て機能は、アクセス ポートで 802.1X 認証を設定すると自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802

- [81] Tunnel-Private-Group-ID = VLAN 名、VLAN ID、または VLAN-Group
- [83] Tunnel-Preference

属性 [64] は、値 *VLAN*（type 13）を含んでいる必要があります。属性 [65] は、値 *802*（type 6）を含んでいる必要があります。属性 [81] は、802.1X 認証ユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

トンネル属性の例については、「ベンダー固有の RADIUS 属性を使用するためのスイッチの設定」（P.11-34）を参照してください。

802.1X 認証とユーザ単位 ACL の使用

ユーザ単位の Access Control List（ACL; アクセス制御リスト）をイネーブルにして、802.1X 認証ユーザに異なるレベルのネットワーク アクセスおよびサービスを提供できます。RADIUS サーバは、802.1X ポートに接続したユーザを認証するときに、ユーザの識別情報に基づいて ACL 属性を取得し、それらをスイッチに送信します。スイッチは、ユーザ セッション中に、それらの属性を 802.1X ポートに適用します。スイッチは、セッションが終了したとき、認証が失敗したとき、またはリンクダウン状態が発生したときに、ユーザ単位 ACL 設定を削除します。スイッチは、RADIUS 固有の ACL を実行コンフィギュレーションには保存しません。ポートが無認可の場合、スイッチはそのポートから ACL を削除します。

同じスイッチ上で、ルータ ACL と入力ポート ACL を設定できます。ただし、ポート ACL はルータ ACL よりも優先されます。VLAN に属するインターフェイスに入力ポート ACL を適用した場合、そのポート ACL は、VLAN インターフェイスに適用された入力ルータ ACL よりも優先されます。ポート ACL が適用されたポートで受信された着信パケットは、ポート ACL によってフィルタリングされます。他のポートで受信された着信のルーティング パケットは、ルータ ACL によってフィルタリングされます。発信のルーティング パケットは、ルータ ACL によってフィルタリングされます。設定の競合を回避するには、RADIUS サーバに格納されるユーザ プロファイルを慎重に計画する必要があります。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。これらのベンダー固有属性（VSA）は、オクテット ストリング形式になっており、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用する VSA は、入力方向では `inacl#`*n*、出力方向では `outacl#`*n* です。MAC ACL は、入力方向だけでサポートされます。このスイッチは、入力方向でだけ VSA をサポートします。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。詳細については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。

拡張 ACL 構文スタイルだけを使用して、RADIUS サーバに格納されるユーザ単位設定を定義します。RADIUS サーバから定義が渡される場合、それらの定義は、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチで設定されている着信 ACL または発信 ACL を指定できます。属性には、ACL 番号と、そのあとに入力フィルタリングを示す *.in* または出力フィルタリングを示す *.out* が含まれています。RADIUS サーバが *.in* または *.out* の構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。スイッチ上では Cisco IOS アクセス リストのサポートが制限されているので、Filter-Id 属性は番号が 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL と IP 拡張 ACL）だけでサポートされています。

ユーザ単位 ACL の最大サイズは、ASCII 文字で 4000 字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズによって制限されます。

ベンダー固有属性の例については、「ベンダー固有の RADIUS 属性を使用するためのスイッチの設定」（P.11-34）を参照してください。ACL の設定の詳細については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。

（注）　ユーザ単位 ACL は、シングルホスト モードだけでサポートされます。

ユーザ単位 ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認可をイネーブルにし、RADIUS サーバからのインターフェイス コンフィギュレーションを許可します。
- 802.1X 認証をイネーブルにします。
- RADIUS サーバでユーザ プロファイルと VSA を設定します。
- 802.1X ポートをシングルホスト モード用に設定します。

設定の詳細については、「認証マネージャ」（P.12-7）を参照してください。

802.1X 認証とダウンロード可能 ACL およびリダイレクト URL

ホストの 802.1X 認証または MAC 認証バイパス中に、ACL をダウンロードし、URL を RADIUS サーバからスイッチにリダイレクトすることができます。また、Web 認証中に ACL をダウンロードすることもできます。

（注）　ダウンロード可能 ACL は、*dACL* とも呼ばれます。

複数のホストが認証され、ホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

802.1X 対応ポートに接続されているすべての装置に、ACL およびリダイレクト URL を適用できます。

802.1X 認証中に ACL がダウンロードされない場合、スイッチはスタティックなデフォルト ACL をホストへのポートに適用します。マルチ認証モードまたは MDA モードで設定されている音声 VLAN ポートでは、スイッチは認証ポリシーの一部として、電話にだけ ACL を適用します。

Cisco IOS Release 12.2(55)SE 以降、ポートにスタティックな ACL がない場合、動的な auth-default-ACL が作成され、dACL がダウンロードされて適用される前にポリシーが強制されます。

（注）　auth-default-ACL は、実行コンフィギュレーションには出現しません。

auth-default-ACL は、認証ポリシーが設定されているホストが 1 台以上、ポートで検出されたときに作成されます。auth-default-ACL は、最後の認証済みセッションが終了すると、ポートから削除されます。auth-default-ACL は、**ip access-list extended auth-default-acl** グローバル コンフィギュレーション コマンドを使用して設定できます。

（注）　auth-default-ACL では、シングル ホスト モードでの Cisco Discovery Protocol（CDP）バイパスはサポートされません。CDP バイパスをサポートするには、インターフェイスにスタティックな ACL を設定する必要があります。

802.1X および MAB 認証方式では、*オープン*と*クローズド*の 2 つの認証方式がサポートされます。*クローズド*認証モードで、ポートにスタティックな ACL がない場合、次のようになります。

- auth-default-ACL が作成されます。
- ポリシーが強制されるまで、auth-default-ACL によって、DHCP トラフィックだけが許可されます。
- 最初のホストが認証を行うと、IP アドレス挿入なしで認証ポリシーが適用されます。

- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、最初と後続のセッションのポリシーが IP アドレス挿入ありで強制されます。

*オープン*認証モードで、ポートにスタティックな ACL がない場合、以下のようになります。

- auth-default-ACL-OPEN が作成され、すべてのトラフィックを許可します。
- セキュリティ違反を防ぐために、ポリシーが IP アドレス挿入ありで強制されます。
- Web 認証は、auth-default-ACL-OPEN の対象です。

認証ポリシーがないホストのアクセスを制御するために、ディレクティブを設定できます。ディレクティブとしてサポートされる値は、*open* および *default* です。*open* ディレクティブを設定すると、すべてのトラフィックが許可されます。*default* ディレクティブでは、トラフィックは、ポートが提供するアクセスの対象になります。ディレクティブは、AAA サーバのユーザ プロファイルまたはスイッチで設定できます。AAA サーバでディレクティブを設定するには、**authz-directive =<open/default>** グローバル コマンドを使用します。スイッチでディレクティブを設定するには、**epm access-control open** グローバル コンフィギュレーション コマンドを使用します。

（注） ディレクティブのデフォルト値は、*default* です。

設定済みの ACL がないポートで、ホストが Web 認証にフォールバックした場合は、次のようになります。

- ポートがオープン認証モードの場合、auth-default-ACL-OPEN が作成されます。
- ポートがクローズド認証モードの場合、auth-default-ACL が作成されます。

フォールバック ACL の Access Control Entry（ACE; アクセス コントロール エントリ）が、ユーザ単位のエントリに変換されます。構成済みのフォールバック プロファイルにフォールバック ACL が含まれていない場合、ホストは、ポートに関連付けられた auth-default-ACL の対象になります。

（注） Web 認証でカスタム ロゴを使用していて、これが外部サーバに格納されている場合、ポート ACL によって、認証前にこの外部サーバへのアクセスを許可する必要があります。外部サーバへの適切なアクセスを提供するには、スタティックなポート ACL を設定するか、auth-default-ACL を変更する必要があります。

リダイレクト URL 用の Cisco Secure ACS および Attribute-Value ペア

このスイッチは、次の *cisco-av-pair* VSA を使用します。

- url-redirect は、HTTP から HTTPS への URL です。
- url-redirect-acl は、スイッチの ACL 名または番号です。

スイッチは、CiscoSecure-Defined-ACL の属性と値のペアを使用して、エンド ポイント装置からの HTTP 要求または HTTPS 要求を代行受信します。次に、スイッチはクライアントの Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure Access Control Server（ACS）の url-redirect の属性と値のペアには、Web ブラウザのリダイレクト先となる URL が含まれます。url-redirect-acl の属性と値のペアには、リダイレクトする HTTP トラフィックまたは HTTPS トラフィックを指定する ACL の名前または番号が含まれます。ACL 内の許可 ACE に一致するトラフィックはリダイレクトされます。

（注） URL リダイレクト ACL とデフォルト ポート ACL をスイッチで定義します。

リダイレクト URL が認証サーバ上でクライアントに対して設定されている場合、接続されているクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

ダウンロード可能 ACL 用の Cisco Secure ACS および Attribute-Value ペア

Cisco Secure ACS で RADIUS cisco-av-pair ベンダー固有属性（VSA）により CiscoSecure-Defined-ACL Attribute-Value ペアを設定できます。このペアは、#ACL#-IP-name-number 属性により、Cisco Secure ACS 上のダウンロード可能 ACL の名前を指定します。

- *name* は ACL 名です。
- *number* はバージョン番号です（たとえば、3f783768）。

ダウンロード可能 ACL が認証サーバ上でクライアントに対して設定されている場合、接続されているクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

スイッチでデフォルト ACL を設定している場合に、Cisco Secure ACS がホスト アクセス ポリシーをスイッチに送信すると、スイッチはスイッチ ポートに接続されたホストからのトラフィックに対し、このポリシーを適用します。ポリシーがトラフィックに適用されない場合は、スイッチはデフォルトの ACL を適用します。Cisco Secure ACS がスイッチにダウンロード可能 ACL を送信した場合、この ACL は、スイッチ ポートで設定されているデフォルト ACL よりも優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信した場合に、デフォルト ACL が設定されていないと、認可の失敗が宣言されます。

設定の詳細については、「認証マネージャ」（P.12-7）および「802.1X 認証とダウンロード可能 ACL およびリダイレクト URL の設定」（P.12-61）を参照してください。

VLAN ID ベースの MAC 認証

ダウンロード可能な VLAN ではなく、スタティックな VLAN ID に基づいてホストを認証する場合は、VLAN ID ベースの MAC 認証を使用できます。スイッチでスタティックな VLAN ポリシーが設定されている場合、認証用に VLAN 情報が各ホストの MAC アドレスとともに Internet Authentication Service（IAS; インターネット認証サービス）（Microsoft）RADIUS サーバに送信されます。接続ポートで設定されている VLAN ID が、MAC 認証に使用されます。VLAN ID ベースの MAC 認証を ISA サーバとともに使用することで、固定数の VLAN をネットワーク内で使用できます。

この機能は、STP によりモニタおよび処理される VLAN の数も制限します。ネットワークは、固定 VLAN として管理できます。

（注）　この機能は、Cisco ACS Server ではサポートされていません（ACS サーバは、新しいホスト用に送信された VLAN ID を無視し、MAC アドレスに基づいた認証だけを行います）。

設定の詳細については、「VLAN ID ベースの MAC 認証の設定」（P.12-64）を参照してください。その他の設定は、「MAC 認証バイパスの設定」（P.12-57）で説明している MAC 認証バイパスに似ています。

802.1X 認証とゲスト VLAN

スイッチの各 802.1X ポートにゲスト VLAN を設定して、802.1X クライアントのダウンロードなどの限られたサービスをクライアントに提供できます。これらのクライアントは、802.1X 認証のためにシステムをアップグレードしている可能性があり、Windows 98 システムなどの一部のホストは、802.1X に対応していない可能性があります。

802.1X ポートでゲスト VLAN をイネーブルにすると、スイッチは EAP 要求/アイデンティティ フレームに対する応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、クライアントをゲスト VLAN に割り当てます。

スイッチは、EAPOL パケット履歴を保持します。リンクの存続時間中に EAPOL パケットがインターフェイスで検出された場合、スイッチは、そのインターフェイスに接続されている装置が 802.1X 対応サプリカントであると判断し、インターフェイスはゲスト VLAN ステートに変更されません。インターフェイスのリンク ステータスがダウンになった場合、EAPOL 履歴は消去されます。EAPOL パケットがインターフェイスで検出されない場合、インターフェイスはゲスト VLAN ステートに変更されます。

装置がリンクの存続時間中に EAPOL パケットをスイッチに送信した場合、スイッチは認証に失敗したクライアントがゲスト VLAN にアクセスできないようにします。

スイッチが 802.1X 対応の音声装置を認可しようとしていて、AAA サーバが使用不可の場合、認可の試みは失敗しますが、EAPOL パケットが検出されたことは EAPOL 履歴に保存されます。AAA サーバが使用可能になると、スイッチは音声装置を認可します。ただし、スイッチは他の装置がゲスト VLAN にアクセスするのを許可しなくなります。この状態を避けるには、次のいずれかのコマンド シーケンスを使用します。

- **dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを入力して、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

（注）　インターフェイスがゲスト VLAN に変更されたあとで EAPOL パケットが検出された場合、インターフェイスは無認可ステートに戻り、802.1X 認証が再開されます。

スイッチ ポートがゲスト VLAN に移行すると、任意の数の 802.1X 非対応クライアントがアクセスを許可されます。802.1X 対応クライアントが、ゲスト VLAN が設定されているポートと同じポートに加わると、そのポートはユーザ設定アクセス VLAN で無認可ステートに移行し、認証が再開されます。

ゲスト VLAN は、シングルホスト モードまたはマルチホスト モードの 802.1X ポート上でサポートされます。

RSPAN VLAN、プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X のゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

スイッチは、*MAC 認証バイパス*をサポートします。MAC 認証バイパスが 802.1X ポートでイネーブルになっている場合、EAPOL メッセージ交換の待機中に 802.1X 認証が時間切れになると、スイッチはクライアントの MAC アドレスに基づいてクライアントを認可できます。スイッチは、802.1X ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。詳細については、「802.1X 認証と MAC 認証バイパス」（P.12-27）を参照してください。

詳細については、「ゲスト VLAN の設定」（P.12-51）を参照してください。

802.1X 認証と制限付き VLAN

スイッチ上の 802.1X ポートごとに制限付き VLAN（*認証失敗 VLAN* とも呼ばれます）を設定して、ゲスト VLAN にアクセスできないクライアントに限られたサービスを提供できます。これらのクライアントは、802.1X に準拠しており、認証プロセスに失敗するので別の VLAN にアクセスできません。制限付き VLAN により、認証サーバ内に有効なクレデンシャルがないユーザ（通常は企業への訪問者）が、一連の限られたサービスにアクセスできるようになります。管理者は、制限付き VLAN で利用できるサービスを制御できます。

（注）　ゲスト VLAN と制限付き VLAN の両方のタイプのユーザに同じサービスを提供する場合、1 つの VLAN をゲスト VLAN と制限付き VLAN の両方として設定できます。

この機能がなければ、クライアントは認証の試行と失敗を無制限に繰り返し、スイッチ ポートはスパニング ツリー ブロッキング ステートのままになります。この機能を使用すると、認証が指定回数（デフォルト値は 3 回）試行されたあとで、スイッチ ポートを制限付き VLAN に移行できます。

オーセンティケータが、クライアントの失敗した認証試行の回数をカウントします。このカウントが設定された最大認証試行回数を超えると、ポートは制限付き VLAN に移行します。失敗した試行のカウントは、RADIUS サーバが *EAP 失敗*または EAP パケットを含まない空の応答により応答した場合に増加します。ポートが制限付き VLAN に移行すると、失敗試行カウンタはリセットされます。

認証に失敗したユーザは、次の再認証が試行されるまで制限付き VLAN に残ります。制限付き VLAN 内のポートは、設定された間隔（デフォルトは 60 秒）で再認証を試みます。再認証が失敗した場合、ポートは制限付き VLAN に残ります。再認証が成功した場合、ポートは設定された VLAN または RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることができます。その場合、再認証プロセスが再開されるのは、ポートが *リンクダウン*イベントまたは *EAP ログオフ*イベントを受信した場合だけです。クライアントがハブを介して接続する可能性がある場合は、再認証をイネーブルのままにすることを推奨します。クライアントがハブから接続解除されたときに、ポートは *リンクダウン*イベントまたは *EAP ログオフ*イベントを受信しない可能性があります。

ポートが制限付き VLAN に移行したあと、シミュレートされた EAP 成功メッセージがクライアントに送信されます。これにより、クライアントが認証を無制限に試みるのを防ぎます。一部のクライアント（たとえば、Windows XP を実行する装置）は、EAP 成功なしでは DHCP を実装できません。

制限付き VLAN は、シングルホスト モードの 802.1X ポートおよびレイヤ 2 ポートだけでサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X の制限付き VLAN として設定できます。制限付き VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

この機能は、ポート セキュリティと連動します。ポートが認可されるとすぐに、MAC アドレスがポート セキュリティに提供されます。ポート セキュリティで MAC アドレスが許可されない場合、またはセキュア アドレス カウントの最大数に達した場合、ポートは無認可ステートおよび errdisable になります。

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査、DHCP スヌーピング、IP ソース ガードなどのその他のポート セキュリティ機能は、制限付き VLAN 上で個別に設定できます。

詳細については、「制限付き VLAN の設定」（P.12-52）を参照してください。

802.1X 認証とアクセス不能認証バイパス

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合は、*クリティカル認証*または *AAA 失敗ポリシー*とも呼ばれるアクセス不能認証バイパス機能を使用します。それらのホストを *クリティカル ポート*に接続するようにスイッチを設定できます。

新しいホストがクリティカル ポートへの接続を試みると、そのホストはユーザ指定のアクセス VLAN である *クリティカル VLAN* に移行します。管理者は、限られた認証をホストに与えます。

クリティカル ポートに接続されたホストを認証するとき、スイッチは設定された RADIUS サーバのステータスを確認します。サーバが使用可能な場合、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが使用不可の場合、スイッチはネットワーク アクセスをホストに許可し、ポートを認証ステートの特別なケースである *critical-authentication* ステートに置きます。

マルチ認証ポートでのサポート

マルチ認証（multiauth）ポートでアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan** *vlan-id* を使用します。新しいホストがクリティカル ポートへの接続を試みると、そのポートが再初期化され、接続しているすべてのホストがユーザ指定のアクセス VLAN に移行します。

authentication event server dead action reinitialize vlan *vlan-id* インターフェイス コンフィギュレーション コマンドは、すべてのホスト モードでサポートされます。

認証結果

アクセス不能認証バイパス機能の動作は、ポートの認可ステートによって異なります。

- クリティカル ポートに接続されたホストが認証を試行したときにポートが無認可で、すべてのサーバが使用不可の場合、スイッチはポートを RADIUS 設定またはユーザ指定のアクセス VLAN で critical-authentication ステートに置きます。
- ポートがすでに認可されていて、再認証が発生した場合、スイッチはクリティカル ポートを現在の VLAN で critical-authentication ステートに置きます。この VLAN は、RADIUS サーバによって事前に割り当てられたものである可能性があります。
- 認証交換中に RADIUS サーバが使用不可になった場合、現在の交換は時間切れとなり、スイッチは次回の認証試行時にクリティカル ポートを critical-authentication ステートに置きます。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、それらのホストをクリティカル VLAN から移行するように、クリティカル ポートを設定できます。このように設定した場合、critical-authentication ステートのすべてのクリティカル ポートは、自動的に再認証されます。詳細については、このリリースのコマンド リファレンスと、「アクセス不能認証バイパス機能の設定」（P.12-54）を参照してください。

機能の相互作用

アクセス不能認証バイパスは、次の機能と相互作用します。

- ゲスト VLAN：アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 802.1X ポートでイネーブルになっている場合、これらの機能は次のように相互作用します。
  - 少なくとも 1 つの RADIUS サーバが使用可能な場合、スイッチは、EAP 要求/アイデンティティ フレームに対する応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、クライアントをゲスト VLAN に割り当てます。
  - すべての RADIUS サーバが使用不可であり、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証し、クリティカル ポートを RADIUS 設定またはユーザ指定のアクセス VLAN で critical-authentication ステートに置きます。
  - すべての RADIUS サーバが使用不可であり、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていなければ、スイッチはクライアントをゲスト VLAN に割り当てない可能性があります。
  - すべての RADIUS サーバが使用不可であり、クライアントがクリティカル ポートに接続されていて事前にゲスト VLAN に割り当てられている場合、スイッチはそのポートをゲスト VLAN で維持します。
- 制限付き VLAN：ポートが制限付き VLAN ですでに認可されていて、RADIUS サーバが使用不可の場合、スイッチはクリティカル ポートを制限付き VLAN で critical-authentication ステートに置きます。
- 802.1X アカウンティング：RADIUS サーバが使用不可の場合、アカウンティングは影響を受けません。

- プライベート VLAN：プライベート VLAN ホスト ポートでアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ プライベート VLAN である必要があります。
- 音声 VLAN：アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定またはユーザ指定のアクセス VLAN と音声 VLAN は異なるものである必要があります。
- Remote Switched Port Analyzer（RSPAN; リモート スイッチド ポート アナライザ）：RSPAN VLAN をアクセス不能認証バイパス用の RADIUS 設定またはユーザ指定のアクセス VLAN として設定しないでください。

802.1X 認証と音声 VLAN ポート

音声 VLAN ポートは、次の 2 つの VLAN ID に関連付けられた特殊なアクセス ポートです。

- IP Phone との間で音声トラフィックを搬送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じてスイッチに接続されたワークステーションとの間でデータ トラフィックを搬送する PVID。PVID は、ポートのネイティブ VLAN です。

IP Phone は、ポートの認可ステートに関係なく、音声トラフィックに VVID を使用します。これにより、IP Phone は 802.1X 認証とは独立して動作できます。

シングルホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチホスト モードでは、サプリカントが PVID で認証されたあとに、追加のクライアントが音声 VLAN 上でトラフィックを送信できます。マルチホスト モードがイネーブルの場合、サプリカントの認証は、PVID と VVID に影響を与えます。

リンクが存在していれば音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取ると装置の MAC アドレスが表示されます。Cisco IP Phone は、他の装置からの CDP メッセージをリレーしません。そのため、複数の IP Phone が直列で接続されていても、スイッチは自身に直接接続された IP Phone しか認識しません。音声 VLAN ポートで 802.1X 認証がイネーブルになっている場合、スイッチは、2 ホップ以上離れた認識されていない IP Phone からのパケットを廃棄します。

ポートで 802.1X 認証がイネーブルになっている場合は、音声 VLAN と等価であるポート VLAN を設定できません。

（注）　音声 VLAN が設定されていて Cisco IP Phone が接続されているアクセス ポートで 802.1X 認証をイネーブルにした場合、Cisco IP Phone とスイッチの接続が最大 30 秒切断されます。

音声 VLAN の詳細については、第 18 章「音声 VLAN の設定」を参照してください。

802.1X 認証とポート セキュリティ

シングルホスト モードまたはマルチホスト モードのいずれかで、ポート セキュリティを含む 802.1X ポートを設定できます（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用して、ポートでポート セキュリティを設定する必要があります）。ポートでポート セキュリティおよび 802.1X 認証をイネーブルにすると、802.1X 認証によってポートが認証され、ポート セキュリティによってクライアントの MAC アドレスを含むすべての MAC アドレスについてのネットワーク アクセスが管理されます。そのあと、802.1X ポートを介してネットワークにアクセスできるクライアントの数またはグループを制限できます。

スイッチにおいて、802.1X 認証とポート セキュリティの間には次のような相互作用があります。

- クライアントが認証され、ポート セキュリティ テーブルがいっぱいになっていない場合、クライアントの MAC アドレスがセキュア ホストのポート セキュリティ リストに追加されます。すると、ポートが通常どおりアクティブになります。

  クライアントが認証され、ポート セキュリティ用に手動で設定された場合、セキュア ホスト テーブル内のエントリが保証されます（ポート セキュリティのスタティック エージングがイネーブルになっている場合を除きます）。

  クライアントが認証されても、ポート セキュリティ テーブルがいっぱいの場合は、セキュリティ違反が発生します。この状況は、セキュア ホストの最大数がスタティックに設定されているか、セキュア ホスト テーブルでのクライアントの有効期限が切れた場合に生じます。クライアントのアドレスの有効期限が切れた場合、そのクライアントのセキュア ホスト テーブル内の位置を、別のホストが使用できます。

  最初に認証されたホストによってセキュリティ違反が発生した場合、ポートは errdisable になり、すぐにシャットダウンされます。

  セキュリティ違反に対するアクションは、ポート セキュリティ違反モードによって決まります。詳細については、「セキュリティ違反」（P.29-10）を参照してください。

- 802.1X クライアントのアドレスを、**no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用してポート セキュリティ テーブルから手動で削除した場合、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを使用して 802.1X クライアントを再認証する必要があります。
- 802.1X クライアントがログオフすると、ポートは無認証ステートに変わり、クライアントのエントリを含むセキュア ホスト テーブル内のすべてのダイナミック エントリが消去されます。続いて、通常の認証が実行されます。
- ポートを管理上の理由からシャットダウンした場合、ポートは無認証ステートになり、すべてのダイナミック エントリがセキュア ホスト テーブルから削除されます。
- ポート セキュリティと音声 VLAN は、シングルホスト モードまたはマルチホスト モードの 802.1X ポートで同時に設定できます。ポート セキュリティは、音声 VLAN ID（VVID）とポート VLAN ID（PVID）の両方に適用されます。
- 新しい装置が 802.1X 対応ポートに接続したとき、または最大許可数の装置が認証されたときに、ポートをシャットダウンするか、Syslog エラーを生成するか、または新しい装置からのパケットを破棄するように、**authentication violation** または **dot1x violation-mode** インターフェイス コンフィギュレーション コマンドを設定できます。詳細については、「ポート単位で許可される装置の最大数」（P.12-37）およびこのリリースのコマンド リファレンスを参照してください。

スイッチでポート セキュリティをイネーブルにする方法の詳細については、「ポート セキュリティの設定」（P.29-9）を参照してください。

802.1X 認証と Wake-on-LAN

802.1X 認証と Wake-on-LAN（WoL）機能により、スイッチが *マジック パケット*と呼ばれる特殊なイーサネット フレームを受信したときに、休止状態の PC の電源をオンにできます。この機能は、電源がオフになっているシステムに管理者が接続する必要がある環境で使用できます。

WoL を使用するホストが 802.1X ポートを通じて接続されていて、そのホストの電源がオフになると、802.1X ポートは無認可ステートになります。ポートでは EAPOL パケットだけを送受信でき、WoL マジック パケットはホストに到達しません。PC の電源がオフになると、その PC は認可されず、スイッチ ポートは開きません。

スイッチで 802.1X 認証と WoL を使用する場合、スイッチはマジック パケットを含むトラフィックを無認可の 802.1X ポートに転送します。ポートが無認可ステートの間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストは、パケットを受信できますが、ネットワーク内の他の装置にパケットを送信することはできません。

（注）　ポートで PortFast がイネーブルになっていない場合、ポートは強制的に双方向ステートになります。

authentication control-direction in または **dot1x control-direction in** インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向として設定すると、ポートはスパニング ツリー フォワーディング ステートに変更されます。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both または **dot1x control-direction both** インターフェイス コンフィギュレーション コマンドを使用してポートを双方向として設定すると、ポートは双方向でアクセス制御されます。ポートは、ホストとの間でパケットを送受信しません。

802.1X 認証と MAC 認証バイパス

MAC 認証バイパス機能を使用することで、クライアントの MAC アドレス（図 12-2（P.12-4）を参照）に基づいてクライアントを認可するようにスイッチを設定できます。たとえば、プリンタなどの装置に接続された 802.1X ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答を待機している間に 802.1X 認証が時間切れになった場合、スイッチは MAC 認証バイパスを使用してクライアントを認可しようと試みます。

802.1X ポートで MAC 認証バイパス機能がイネーブルになっている場合、スイッチは MAC アドレスをクライアントの識別情報として使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。スイッチは、802.1X ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートをゲスト VLAN に割り当てます（設定されている場合）。

リンクの存続時間中に EAPOL パケットがインターフェイスで検出された場合、スイッチは、そのインターフェイスに接続されている装置が 802.1X 対応サプリカントであると判断し、（MAC 認証バイパスではなく）802.1X 認証を使用してインターフェイスを認可します。インターフェイスのリンク ステータスがダウンになった場合、EAPOL 履歴は消去されます。

スイッチが MAC 認証バイパスを使用してポートをすでに認可していて、802.1X サプリカントを検出した場合、スイッチはポートに接続されたクライアントを無認可にしません。再認証を行う場合、以前のセッションが Termination-Action RADIUS 属性値が DEFAULT であるために終了していれば、スイッチは 802.1X 認証を優先的な再認証プロセスとして使用します。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、802.1X で認証されたクライアントの再認証プロセスと同じです。再認証中に、ポートは以前に割り当てられた VLAN 内にとどまります。再認証に成功すると、スイッチはポートを同じ VLAN 内に維持します。再認証に失敗すると、スイッチはポートをゲスト VLAN に割り当てます（設定されている場合）。

再認証が Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）に基づいていて、Termination-Action RADIUS 属性（属性 [29]）のアクションが *Initialize* の場合（属性値は *DEFAULT*）、MAC 認証バイパス セッションは終了し、再認証中に接続が失われます。MAC 認証バイパスがイネーブルになっていて、802.1X 認証が時間切れになった場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。これらの AV ペアの詳細については、RFC 3580『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互作用します。

- 802.1X 認証：MAC 認証バイパスをイネーブルにできるのは、ポートで 802.1X 認証がイネーブルになっている場合だけです。
- ゲスト VLAN：クライアントの MAC アドレス識別情報が無効である場合、ゲスト VLAN が設定されていれば、スイッチはクライアントをゲスト VLAN に割り当てます。
- 制限付き VLAN：802.1X ポートに接続されたクライアントが MAC 認証バイパスで認証されている場合、この機能はサポートされません。
- ポート セキュリティ：「802.1X 認証とポート セキュリティ」（P.12-25）を参照してください。
- 音声 VLAN：「802.1X 認証と音声 VLAN ポート」（P.12-25）を参照してください。
- VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）：802.1X および VMPS は、相互に排他的です。
- プライベート VLAN：クライアントをプライベート VLAN に割り当てることができます。
- Network Admission Control（NAC）レイヤ 2 IP 検証：この機能は、例外リストのホストを含めて、802.1X ポートが MAC 認証バイパスで認証されたあとに有効になります。

設定の詳細については、「認証マネージャ」（P.12-7）を参照してください。

Cisco IOS Release 12.2(55)SE 以降では、詳細な MAB システム メッセージのフィルタリングがサポートされます。「認証マネージャの CLI コマンド」（P.12-9）を参照してください。

802.1X ユーザ分散

802.1X ユーザ分散を設定して、同じグループ名を持つユーザを複数の異なる VLAN に負荷分散させることができます。

VLAN は、RADIUS サーバによって提供されるか、スイッチの CLI を通じて VLAN グループ名の下に設定されます。

- ユーザに対して複数の VLAN 名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として複数の VLAN 名を送信できます。802.1X ユーザ分散では、特定の VLAN 内のすべてのユーザを追跡し、認可済みユーザを最もユーザが少ない VLAN に移動することでロード バランシングを実現します。
- ユーザに対して VLAN グループ名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として VLAN グループ名を送信できます。スイッチの CLI を使用して設定した VLAN グループ名の中から、選択した VLAN グループ名を検索できます。VLAN グループ名が見つかった場合、その VLAN グループ名の下の対応する VLAN が検索され、最もユーザが少ない VLAN が検索されます。その VLAN に対応する認可済みユーザを移動することで、ロード バランシングが実現されます。

（注）　RADIUS サーバは、VLAN-ID、VLAN 名、または VLAN グループの任意の組み合わせで VLAN 情報を送信できます。

802.1X ユーザ分散の設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされていることを確認します。
- 複数の VLAN を VLAN グループにマップできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。

- 既存の VLAN を VLAN グループ名から消去した場合、VLAN の認証済みポートは消去されませんが、マッピングは既存の VLAN グループから削除されます。
- VLAN グループ名から最後の VLAN を消去すると、VLAN グループが消去されます。
- アクティブな VLAN が VLAN グループにマッピングされているときでも、VLAN グループを消去できます。VLAN グループを消去した場合、グループ内の任意の VLAN で認証済みステートであるポートまたはユーザは消去されませんが、VLAN グループへの VLAN マッピングは消去されます。

詳細については、「802.1X ユーザ分散の設定」（P.12-58）を参照してください。

Network Admission Control レイヤ 2 802.1X 検証

スイッチは、Network Admission Control（NAC）レイヤ 2 802.1X 検証をサポートします。この検証では、エンドポイント システムまたはクライアントにネットワーク アクセスを許可する前に、それらの装置のアンチウイルス状態または*ポスチャ*をチェックします。NAC レイヤ 2 802.1X 検証では、次の作業を実行できます。

- Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）を認証サーバからダウンロードします。
- 再認証を試行する間隔の秒数を、Session-Timeout RADIUS 属性（属性 [27]）の値として設定し、クライアントに対するアクセス ポリシーを RADIUS サーバから取得します。
- Termination-Action RADIUS 属性（属性 [29]）を使用して、スイッチがクライアントの再認証を試みるときに実行するアクションを設定します。値が *DEFAULT* であるか、または設定されていない場合、セッションは終了します。値が RADIUS-Request の場合、再認証プロセスが開始されます。
- VLAN 番号または名前あるいは VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN 番号または名前あるいは VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから取得されます。
- **show authentication** または **show dot1x** 特権 EXEC コマンドを使用して、クライアントのポスチャを示す NAC ポスチャ トークンを表示します。
- セカンダリ プライベート VLAN をゲスト VLAN として設定します。

NAC レイヤ 2 802.1X 検証の設定は、802.1X ポートベース認証の設定に似ていますが、RADIUS サーバでポスチャ トークンを設定する必要があります。NAC レイヤ 2 802.1X 検証の設定については、「NAC レイヤ 2 802.1X 検証の設定」（P.12-59）および「定期的再認証の設定」（P.12-44）を参照してください。

NAC の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

設定の詳細については、「認証マネージャ」（P.12-7）を参照してください。

フレキシブルな認証順序付け

フレキシブルな認証順序付け機能を使用して、ポートが新しいホストの認証に使用する方式の順序を設定できます。MAC 認証バイパスおよび 802.1X をプライマリ認証方式またはセカンダリ認証方式に設定し、これらの認証の一方または両方が失敗したときのフォールバック方式として Web 認証を設定することができます。詳細については、「フレキシブルな認証順序付けの設定」（P.12-64）を参照してください。

Open1x 認証

Open1x 認証により、装置を認証する前に装置のポートへのアクセスを許可することができます。オープン認証を設定した場合、ポート上の新しいホストは、スイッチへのトラフィックの送信だけを行うことができます。ホストが認証されると、RADIUS サーバで設定されたポリシーがそのホストに適用されます。

オープン認証は次のシナリオで設定できます。

- シングルホスト モードとオープン認証：認証の前後で、1 人のユーザだけがネットワーク アクセスを許可されます。
- MDA モードとオープン認証：音声ドメインの 1 人のユーザと、データ ドメインの 1 人のユーザだけが許可されます。
- マルチホスト モードとオープン認証：任意のホストがネットワークにアクセスできます。
- マルチ認証モードとオープン認証：MDA に似ていますが、複数のホストを認証できます。

詳細については、「ホスト モードの設定」（P.12-43）を参照してください。

音声認識 802.1X セキュリティの使用

データ VLAN であるか音声 VLAN であるかに関係なく、セキュリティ違反が発生した VLAN だけをディセーブルにするようにスイッチを設定するには、音声認識 802.1X セキュリティ機能を使用します。以前のリリースでは、データ クライアントの認証を試みたことによりセキュリティ違反が発生した場合、ポート全体がシャットダウンされ、接続が完全に失われました。

この機能は、PC が IP Phone に接続されている場合に使用できます。データ VLAN でセキュリティ違反が見つかった場合、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは、中断せずに継続されます。

音声認識 802.1X セキュリティの設定については、「音声認識 802.1X セキュリティの設定」（P.12-38）を参照してください。

802.1X サプリカント スイッチおよびオーセンティケータ スイッチと Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）

ネットワーク エッジ アクセス トポロジ（NEAT）機能は、配線クローゼットの外部の領域（会議室など）に ID を拡張します。これにより、任意のタイプの装置をポートで認可できます。

- 802.1X スイッチ サプリカント：802.1X サプリカント機能を使用することで、スイッチを別のスイッチへのサプリカントとして機能するように設定できます。この設定は、たとえば、スイッチが配線クローゼットの外部にあり、トランク ポートを通じてアップストリーム スイッチに接続されているシナリオで役立ちます。802.1X スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のために、アップストリーム スイッチとの間で認証を行います。

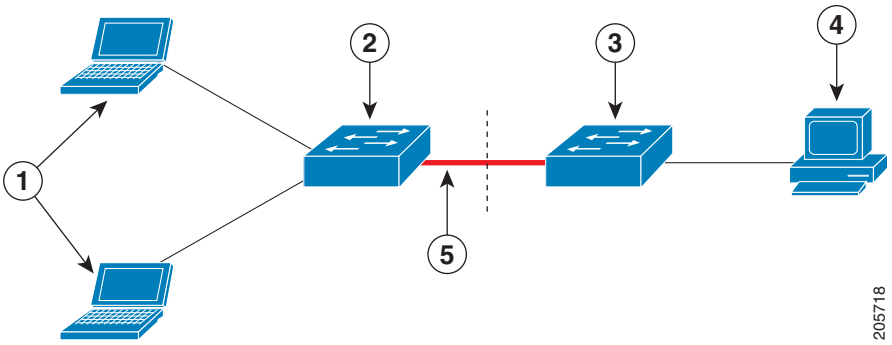
  サプリカント スイッチの認証が成功すると、ポート モードがアクセスからトランクに変更されます。
- オーセンティケータ スイッチでアクセス VLAN が設定されている場合、そのアクセス VLAN は、認証が成功したあとにトランク ポートのネイティブ VLAN になります。

1 つまたは複数のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで、MDA モードまたはマルチ認証モードをイネーブルにすることができます。マルチホスト モードは、オーセンティケータ スイッチ インターフェイスでサポートされません。

ネットワーク エッジ アクセス トポロジ（NEAT）がすべてのホスト モードで動作するようにするには、サプリカント スイッチで **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを使用します。

- ホスト認証：認可されたホスト（サプリカントによりスイッチに接続しているもの）からのトラフィックだけがネットワーク上で許可されるようにします。スイッチは、図 12-6 に示すように、Client Information Signalling Protocol（CISP）を使用して、サプリカント スイッチに接続している MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動イネーブル化：オーセンティケータ スイッチでトランク設定を自動的にイネーブルにし、サプリカント スイッチから送信される複数の VLAN からのユーザ トラフィックを許可します。ACS で、cisco-av-pair を *device-traffic-class=switch* として設定します（この設定は *group* 設定または *user* 設定で行うことができます）。

図 12-6　CISP を使用するオーセンティケータ スイッチとサプリカント スイッチ



1	ワークステーション（クライアント）	**2**	サプリカント スイッチ（配線クローゼットの外部）
3	オーセンティケータ スイッチ	**4**	Access Control Server（ACS）
5	トランク ポート		

注意事項

- 他の認証ポートと同じ設定で NEAT ポートを設定できます。サプリカント スイッチの認証時に、ポート モードは、スイッチのベンダー固有属性（VSA）に基づいて *アクセス*から *トランク*に変更されます（device-traffic-class=switch）。
- VSA は、オーセンティケータ スイッチのポート モードをアクセスからトランクに変更し、802.1X トランク カプセル化とアクセス VLAN をイネーブルにします（ネイティブ トランク VLAN に変換する場合）。VSA は、サプリカントのポート設定を変更しません。
- ホスト モードを変更し、かつオーセンティケータ スイッチ ポートに標準ポート設定を適用するには、スイッチ VSA ではなく、Auto Smartports ユーザ定義マクロを使用することもできます。これにより、オーセンティケータ スイッチ ポート上のサポートされていない設定を削除し、ポート モードを *アクセス*から *トランク*に変更できます。詳細については、第 15 章「SmartPort マクロの設定」を参照してください。

詳細については、「オーセンティケータおよびサプリカント スイッチと NEAT の設定」（P.12-60）を参照してください。

IEEE 802.1X 認証と ACL および RADIUS Filter-Id 属性の使用

スイッチは、入力ポートに適用された IP 標準および IP 拡張ポート アクセス制御リスト（ACL）をサポートします。

- ユーザが設定する ACL
- Access Control Server（ACS）からの ACL

シングルホスト モードの IEEE 802.1X ポートは、ACS からの ACL を使用して、異なるレベルのサービスを IEEE 802.1X 認証済みユーザに提供します。RADIUS サーバは、このタイプのユーザおよびポートを認証すると、ユーザの識別情報に基づいて ACL 属性をスイッチに送信します。スイッチは、ユーザ セッション中に、それらの属性をポートに適用します。セッションが終了した場合、認証が失敗した場合、またはリンクが失敗した場合、ポートは無認可ステートになり、スイッチは ACL をポートから削除します。

ACS からの IP 標準ポート ACL および IP 拡張ポート ACL だけが Filter-Id 属性をサポートします。Filter-Id 属性は、ACL の名前または番号を指定します。Filter-id 属性では、方向（着信または発信）と、ユーザまたはユーザが属するグループも指定できます。

- ユーザの Filter-Id 属性は、グループの Filter-Id 属性よりも優先されます。
- ACS からの Filter-Id 属性がすでに設定されている ACL を指定する場合、その ACL はユーザ設定の ACL よりも優先されます。
- RADIUS サーバが複数の Filter-Id 属性を送信した場合、最後の属性だけが適用されます。

Filter-Id 属性がスイッチで定義されていない場合、認証は失敗し、ポートは無認可ステートに戻ります。

共通セッション ID

認証マネージャでは、使用する認証方式に関係なく、1 つのセッション ID（共通セッション ID と呼ばれます）をクライアントに対して使用します。この ID は、show コマンドや Management Information Base（MIB; 管理情報ベース）など、すべてのレポート目的に使用されます。セッション ID は、すべてのセッション単位 Syslog メッセージとともに表示されます。

セッション ID には次のものが含まれます。

- Network Access Device（NAD; ネットワーク アクセス装置）の IP アドレス
- 単調に増加する一意の 32 ビット整数
- セッション開始時間スタンプ（32 ビット整数）

次に、**show authentication** コマンドの出力に表示されるセッション ID の例を示します。この例のセッション ID は、160000050000000B288508E5 です。

```
Switch# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

次に、Syslog 出力に表示されるセッション ID の例を示します。この例のセッション ID も、160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッション ID は、NAD、AAA サーバ、およびその他のレポート解析アプリケーションでクライアントを識別するために使用されます。ID は自動的に表示されます。したがって設定作業は不要です。

802.1X 認証の設定

802.1X 認証のデフォルト設定

表 12-4 に、802.1X 認証のデフォルト設定を示します。

表 12-4　802.1X 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1X イネーブル ステート	ディセーブル。
ポート単位の 802.1X イネーブル ステート	ディセーブル（force-authorized）。 ポートはクライアントの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。
AAA	ディセーブル。
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし。 • 1812。 • 指定なし。
ホスト モード	シングルホスト モード。
制御方向	双方向制御。
定期的再認証	ディセーブル。
再認証の試行間隔（秒）	3600 秒。
再認証回数	2 回（ポートが無認可ステートに移行する前に、スイッチが認証プロセスを再開する回数）。
待機時間	60 秒（スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数）。
再送信時間	30 秒（スイッチが要求を再送信する前に、EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数）。
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP 要求/アイデンティティ フレームを送信する回数）。
クライアント タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするときに、スイッチが要求をクライアントに再送信する前に応答を待機する時間）。
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答をサーバに再送信する前に、応答を待機する時間）。 このタイムアウト時間を変更するには、**authentication timer server** または **dot1x timeout server-timeout** インターフェイス コンフィギュレーション コマンドを使用します。
無活動タイムアウト	ディセーブル。
ゲスト VLAN	指定なし。
アクセス不能認証バイパス	ディセーブル。
制限付き VLAN	指定なし。
オーセンティケータ（スイッチ）モード	指定なし。
MAC 認証バイパス	ディセーブル。
音声認識セキュリティ	ディセーブル。

802.1X 認証の設定時の注意事項

802.1X 認証

- 802.1X 認証をイネーブルにすると、ポートが認証されてから、他のレイヤ 2 機能またはレイヤ 3 機能がイネーブルになります。
- 802.1X 対応ポートのモードを変更しようとしても（たとえば、アクセスからトランク）、エラー メッセージが表示され、ポート モードは変更されません。
- 802.1X 対応ポートが割り当てられている VLAN が変更された場合、この変更はトランスペアレントであり、スイッチに影響を与えません。たとえば、この変更は、ポートが RADIUS サーバによって割り当てられた VLAN に割り当てられていて、再認証後に異なる VLAN に割り当てられた場合に発生します。

  802.1X ポートが割り当てられている VLAN がシャットダウンするか、ディセーブルになるか、または削除された場合、ポートは無認可ステートになります。たとえば、ポートが割り当てられているアクセス VLAN がシャットダウンされるか、または削除されると、ポートは無認可になります。
- 802.1X プロトコルは、レイヤ 2 のスタティック アクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートではサポートされますが、次のポート タイプではサポートされません。
  - トランク ポート：トランク ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol [VQP]）ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
  - EtherChannel　ポート：アクティブまたはまだアクティブでない　EtherChannel　メンバーを 802.1X ポートとして設定しないでください。EtherChannel ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN; リモート SPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートで 802.1X 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先ポートとして削除されるまで、802.1X 認証はディセーブルのままです。SPAN または RSPAN 送信元ポートでは 802.1X 認証をイネーブルにすることができます。
- **dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1X 認証をスイッチでグローバルにイネーブルにする前に、802.1X 認証および EtherChannel が設定されているインターフェイスから EtherChannel 設定を削除します。
- Cisco IOS Release 12.2(55)SE 以降では、802.1X 認証に関連するシステム メッセージのフィルタリングがサポートされます。「認証マネージャの CLI コマンド」（P.12-9）を参照してください。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス

- ポートで 802.1X 認証がイネーブルになっている場合は、音声 VLAN と等価であるポート VLAN を設定できません。
- VLAN 割り当て機能付きの 802.1X 認証は、トランク ポート、ダイナミック ポート、または VMPS を使用したダイナミック アクセス ポート割り当てではサポートされていません。
- プライベート VLAN ポートで 802.1X 認証を設定することは可能ですが、プライベート VLAN ポートでポート セキュリティ、音声 VLAN、ゲスト VLAN、制限付き VLAN、またはユーザ単位 ACL とともに 802.1X 認証を設定しないでください。
- RSPAN VLAN、プライベート VLAN、または音声 VLAN 以外の任意の VLAN を、802.1X のゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。
- DHCP クライアントが接続されている 802.1X ポートのゲスト VLAN を設定したあと、DHCP サーバからホスト IP アドレスを取得することが必要な場合があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得する前に、スイッチ上の 802.1X 認証プロセスを再開するための設定を変更できます。802.1X 認証プロセスの設定を減らします（**authentication timer inactivity**（または **dot1x timeout quiet-period**）および **authentication timer reauthentication**（または **dot1x timeout tx-period**）インターフェイス コンフィギュレーション コマンド）。設定の減少量は、接続された 802.1X クライアントのタイプによって異なります。
- アクセス不能認証バイパス機能を設定するときは、次の注意事項に従ってください。
  - この機能は、シングルホスト モードおよびマルチホスト モードの 802.1X ポートでサポートされています。
  - クライアントが Windows XP を実行し、クライアントが接続されているポートが critical-authentication ステートである場合、Windows XP はインターフェイスが認証されていないと報告することがあります。
  - Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
  - アクセス不能認証バイパス機能および制限付き VLAN を 802.1X ポートで設定できます。スイッチが制限付き VLAN でクリティカル ポートの再認証を試行し、すべての RADIUS サーバが使用不可の場合、スイッチはポートのステートを critical-authentication ステートに変更し、制限付き VLAN にとどまります。
  - アクセス不能認証バイパス機能とポート セキュリティは、同じスイッチ ポートに設定できます。
- RSPAN VLAN または音声 VLAN 以外の任意の VLAN を、802.1X の制限付き VLAN として設定できます。制限付き VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

MAC 認証バイパス

- 特に言及しない限り、MAC 認証バイパスの注意事項は、802.1X 認証の注意事項と同じです。詳細については、「802.1X 認証」（P.12-35）を参照してください。
- ポートが MAC アドレスで認証されたあとで、ポートから MAC 認証バイパスをディセーブルにした場合、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。

- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAC 認証バイパスによって接続されたが非アクティブであるホストのタイムアウト時間を設定できます。指定できる範囲は 1 ～ 65535 秒です。タイムアウト値を設定する前に、ポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定」（P.29-9）を参照してください。

ポート単位で許可される装置の最大数

これは、802.1X 対応ポートで許可される装置の最大数です。

- シングルホスト モードでは、アクセス VLAN で 1 つの装置だけが許可されます。ポートが音声 VLAN でも設定されている場合、無制限の数の Cisco IP Phone が音声 VLAN を通じてトラフィックを送受信できます。
- マルチドメイン認証（MDA）モードでは、アクセス VLAN で 1 つの装置が許可され、音声 VLAN で 1 つの IP Phone が許可されます。
- マルチホスト モードでは、1 つの 802.1X サプリカントだけがポートで許可されますが、無制限の数の非 802.1X ホストがアクセス VLAN で許可されます。音声 VLAN では無制限の数の装置が許可されます。

802.1X 準備状態チェックの設定

802.1X 準備状態チェックでは、すべてのスイッチ ポートでの 802.1X アクティビティをモニタし、802.1X をサポートするポートに接続された装置に関する情報を表示します。この機能を使用して、スイッチ ポートに接続された装置が 802.1X に対応しているかどうかを判断できます。

802.1X 準備状態チェックは、802.1X 用に設定できるすべてのポートで許可されます。準備状態チェックは、**dot1x force-unauthorized** として設定されているポートでは使用できません。

スイッチで準備状態チェックをイネーブルにするには、次の注意事項に従ってください。

- 準備状態チェックは、通常はスイッチで 802.1X をイネーブルにする前に使用します。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用した場合、スイッチ スタックのすべてのポートがテストされます。
- 802.1X 対応ポートで **dot1x test eapol-capable** コマンドを設定し、リンクがアップになった場合、ポートは 802.1X 機能に関するクエリーを接続済みクライアントに送信します。クライアントが通知パケットで応答した場合、そのクライアントは 802.1X に対応しています。クライアントがタイムアウト時間内に応答した場合、Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、そのクライアントは 802.1X に対応していません。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホストを処理するポート（たとえば、IP Phone に接続されている PC）で送信できます。タイマー時間内に準備状態チェックに応答した各クライアントに対して、Syslog メッセージが生成されます。

スイッチで 802.1X 準備状態チェックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dot1x test eapol-capable** [**interface** *interface-id*]	スイッチで 802.1X 準備状態チェックをイネーブルにします。 （任意）*interface-id* には、802.1X 準備状態をチェックするポートを指定します。 **（注）** オプションの **interface** キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。
ステップ 2	**configure terminal**	（任意）グローバル コンフィギュレーション モードを開始します。
ステップ 3	**dot1x test timeout** *timeout*	（任意）EAPOL 応答の待機に使用するタイムアウトを設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 10 秒です。
ステップ 4	**end**	（任意）特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	（任意）変更したタイムアウト値を確認します。

次に、スイッチで準備状態チェックをイネーブルにしてポートにクエリーを送信する例を示します。この例は、クエリー先のポートから受信した応答も示しており、接続している装置が 802.1X 対応であることを確認しています。

```
switch# dot1x test eapol-capable interface gigabitethernet1/2

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/2 is EAPOL
capable
```

音声認識 802.1X セキュリティの設定

データ VLAN であるか音声 VLAN であるかに関係なく、セキュリティ違反が発生した VLAN だけをディセーブルにするには、スイッチで音声認識 802.1X セキュリティ機能を使用します。この機能は、PC が IP Phone に接続されている IP Phone 配置で使用できます。データ VLAN でセキュリティ違反が見つかった場合、データ VLAN だけがシャットダウンされます。音声 VLAN 上のトラフィックは、中断されずにスイッチを通過します。

スイッチで音声認識 802.1X 音声セキュリティを設定するには、次の注意事項に従ってください。

- 音声認識 802.1X セキュリティをイネーブルにするには、**errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力します。音声認識 802.1X セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。このコマンドは、スイッチのすべての 802.1X 設定ポートに適用されます。

（注） **shutdown vlan** キーワードを含めない場合、errdisable ステートになったときにポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して errdisable ステート回復を設定した場合、ポートは自動的に再びイネーブルになります。errdisable ステート回復をポートに設定していない場合は、**shutdown** および **no-shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個別の VLAN を再びイネーブルにするには、**clear errdisable interface** *interface-id* **vlan** [*vlan-list*] 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルになります。

音声認識 802.1X セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause security-violation shutdown vlan**	セキュリティ違反エラーが発生した任意の VLAN をシャットダウンします。 （注）　**shutdown vlan** キーワードを含めない場合、ポート全体が errdisable ステートになり、シャットダウンします。
ステップ 3	**errdisable recovery cause security-violation**	（任意）VLAN 単位の自動エラー回復をイネーブルにします。
ステップ 4	**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]	（任意）errdisable になっている個別の VLAN を再びイネーブルにします。 • *interface-id* には、個別の VLAN を再びイネーブルにするポートを指定します。 • （任意）*vlan-list* には、再びイネーブルにする VLAN のリストを指定します。*vlan-list* を指定しない場合は、すべての VLAN が再びイネーブルになります。
ステップ 5	**shutdown** **no-shutdown**	（任意）errdisable の VLAN を再びイネーブルにし、すべての errdisable 表示を消去します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show errdisable detect**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ギガビット イーサネット 0/2 ポートで errdisable になっているすべての VLAN を再びイネーブルにする例を示します。

```
Switch# clear errdisable interface gigabitethernet0/2 vlan
```

設定を確認するには、**show errdisable detect** 特権 EXEC コマンドを入力します。

802.1X 違反モードの設定

次の場合にポートをシャットダウンするか、Syslog エラーを生成するか、または新しい装置からのパケットを破棄するように、802.1X ポートを設定できます。

- 装置が 802.1X 対応ポートに接続したとき
- 最大許可数の装置がポートで認証されたとき

スイッチのセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1X 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバのリストを使用します。 **（注）** 他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **group radius** キーワードだけです。
ステップ 4	**interface** *interface-id*	クライアントに接続された、802.1X 認証をイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access**	ポートをアクセス モードに設定します。
ステップ 6	**authentication violation shutdown** | **restrict** | **protect** | **replace**} または **dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	違反モードを設定します。キーワードの意味は次のとおりです。 • **shutdown**：ポートを errdisable にします。 • **restrict**：Syslog エラーを生成します。 • **protect**：ポートにトラフィックを送信する任意の新しい装置からのパケットを廃棄します。 • **replace**：現行セッションを削除し、新しいホストで認証します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show authentication** または **show dot1x**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

802.1X 認証の設定

802.1X ポートベース認証を設定するには、認証、認可、アカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。

ユーザ単位 ACL または VLAN 割り当てを許可するには、AAA 認可をイネーブルにして、すべてのネットワーク関連サービス要求に対してスイッチを設定する必要があります。

802.1X AAA プロセスを次に示します。

ステップ 1　ユーザがスイッチのポートに接続します。

ステップ 2　認証が実行されます。

ステップ 3　RADIUS サーバの設定に基づいて、VLAN 割り当てが必要に応じてイネーブルにされます。

ステップ 4　スイッチがアカウンティング サーバに開始メッセージを送信します。

ステップ 5　必要に応じて、再認証が実行されます。

ステップ 6　再認証の結果に基づいて、スイッチがアカウンティング サーバに中間アカウンティング更新を送信します。

ステップ 7　ユーザがポートから接続解除します。

ステップ 8　スイッチがアカウンティング サーバに停止メッセージを送信します。

802.1X ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1X 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバのリストを使用します。 **（注）**　他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **group radius** キーワードだけです。
ステップ 4	**dot1x system-auth-control**	スイッチで 802.1X 認証をグローバルにイネーブルにします。
ステップ 5	**aaa authorization network** {**default**} **group radius**	（任意）ユーザ単位 ACL または VLAN 割り当てなどのすべてのネットワーク関連サービス要求に対してユーザ RADIUS 認可を使用するようにスイッチを設定します。 ユーザ単位 ACL に対しては、シングルホスト モードを設定する必要があります。この設定は、デフォルトです。
ステップ 6	**radius-server host** *ip-address*	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 7	**radius-server key** *string*	（任意）スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証キーおよび暗号キーを指定します。
ステップ 8	**interface** *interface-id*	クライアントに接続された、802.1X 認証をイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode access**	（任意）ステップ 6 および 7 で RADIUS サーバを設定した場合だけ、ポートをアクセス モードに設定します。
ステップ 10	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。 機能の相互作用の詳細については、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show authentication** または **show dot1x**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチと RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別されます。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同じ IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

スイッチの RADIUS サーバ パラメータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	RADIUS サーバ パラメータを設定します。 *hostname* | *ip-address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルト値は 1812 です。指定できる範囲は 0 ～ 65536 です。 **key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証キーおよび暗号キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。 **（注）** キーは、**radius-server host** コマンド構文の末尾で設定してください。これは、先頭のスペースは無視されるが、キーの文字列内または末尾のスペースは使用されるためです。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定した RADIUS サーバを消去するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次に、IP アドレスが 172.20.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を認可ポートとして使用し、暗号キーを *rad123* に設定して、RADIUS サーバ上でキーを一致させる例を示します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

radius-server host グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバに対する設定」（P.11-34）を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの両方で共有されるキー文字列があります。詳細については、RADIUS サーバのマニュアルを参照してください。

ホスト モードの設定

802.1X 認可ポートで単一のホスト（クライアント）または複数のホストを許可するには、特権 EXEC モードで次の手順を実行します。マルチドメイン認証（MDA）を設定して、同じスイッチ ポートでホストと IP Phone（シスコ製品またはシスコ以外の製品）などの音声装置の両方を認証できるようにするには、**multi-domain** キーワードを使用します。

この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server vsa send authentication**	ベンダー固有属性（VSA）を認識および使用するようにネットワーク アクセス サーバを設定します。
ステップ 3	**interface** *interface-id*	複数のホストが間接的に接続されるポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] または **dot1x host-mode** {**single-host** | **multi-host** | **multi-domain**}	キーワードの意味は次のとおりです。 • **multi-auth**：音声 VLAN 上で 1 つのクライアントを許可し、データ VLAN 上で複数の認証済みクライアントを許可します。各ホストは個別に認証されます。 （注）　**multi-auth** キーワードは、**authentication host-mode** コマンドだけで使用できます。 • **multi-host**：単一のホストが認証されたあと、802.1X 認可ポートで複数のホストを許可します。 • **multi-domain**：ホストと、IP Phone（シスコ製品またはシスコ以外の製品）などの音声装置の両方を、802.1X 認可ポートで認証できるようにします。 （注）　ホスト モードを **multi-domain** に設定する場合、IP Phone 用に音声 VLAN を設定する必要があります。詳細については、第 18 章「音声 VLAN の設定」を参照してください。 • **single-host**：802.1X 認可ポートでシングル ホスト（クライアント）を許可します。 指定するインターフェイスで、**authentication port-control** または **dot1x port-control** インターフェイス コンフィギュレーション コマンド セットが **auto** に設定されていることを確認してください。
ステップ 5	**switchport voice vlan** *vlan-id*	（任意）音声 VLAN を設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートで複数のホストをディセーブルにするには、**no authentication host-mode** または **no dot1x host-mode multi-host** インターフェイス コンフィギュレーション コマンドを使用します。

次に、802.1X 認証をイネーブルにし、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにし、ホストと音声装置の両方をポートで許可する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

定期的再認証の設定

802.1X クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証をイネーブルにする前にその間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証の試行間隔を秒数で指定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication periodic** または **dot1x reauthentication**	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルです。

	コマンド	目的
ステップ 4	**authentication timer** {{[**inactivity** | **reauthenticate**]} {**restart** *value*}} または **dot1x timeout reauth-period** {*seconds* | **server**}	再認証の間隔（秒）を指定します。 **authentication timer** キーワードには次の意味があります。 • **inactivity**：クライアントからのアクティビティがない場合に、クライアントを無認可にするまでの間隔（秒単位） • **reauthenticate**：自動再認証の試行を開始するまでの時間（秒単位） • **restart** *value*：無認可ポートの認証を試行するまでの間隔（秒単位） **dot1x timeout reauth-period** キーワードには次の意味があります。 • *seconds*：1 ～ 65535 の範囲で秒数を指定します。デフォルトは 3600 秒です。 • **server**：Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）の値に基づいて、秒数を設定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

定期的な再認証をディセーブルにするには、**no authentication periodic** または **no dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。再認証の試行間隔をデフォルトの秒数に戻すには、**no authentication timer** または **no dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、定期的な再認証をイネーブルにし、再認証の試行間隔を 4000 秒に設定する例を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

ポートに接続されたクライアントの手動再認証

dot1x re-authenticate interface *interface-id* 特権 EXEC コマンドを入力することにより、特定のポートに接続されたクライアントをいつでも手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにするには、「定期的再認証の設定」（P.12-44）を参照してください。

次に、ポートに接続されたクライアントを手動で再認証する例を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet1/2
```

待機時間の変更

クライアントを認証できない場合、スイッチは所定の時間だけアイドル状態を続け、そのあと再び認証を試みます。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドは、アイドル時間を制御します。クライアントの認証が失敗する理由としては、クライアントが無効なパスワードを提示したことなどが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x timeout quiet-period** *seconds*	スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数を設定します。 指定できる範囲は 1 ～ 65535 です。デフォルト値は 60 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの待機時間に戻すには、**no dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチの待機時間を 30 秒に設定する例を示します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

スイッチとクライアント間の再送信時間の変更

クライアントは、スイッチからの EAP 要求/アイデンティティ フレームに対し、EAP 応答/アイデンティティ フレームで応答します。この応答を受信しない場合、スイッチは所定の時間（再送信時間）だけ待機し、そのあとフレームを再送信します。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x timeout tx-period** *seconds*	スイッチが要求を再送信する前に、EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数を設定します。 指定できる範囲は 1 ～ 65535 です。デフォルト値は 5 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの再送信時間に戻すには、**no dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが要求を再送信する前に、EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する時間を 60 秒に設定する例を示します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

スイッチとクライアント間のフレーム再送信回数の設定

応答が受信されない場合に、スイッチが認証プロセスを再開する前にクライアントに EAP 要求/アイデンティティ フレームを送信する回数を変更できます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチとクライアント間のフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count*	スイッチが認証プロセスを再開する前に、EAP 要求/アイデンティティ フレームをクライアントに送信する回数を設定します。指定できる範囲は 1 ～ 10 です。デフォルト値は 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの再送信回数に戻すには、**no dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが認証プロセスを再起動する前に、EAP 要求/アイデンティティ要求を送信する回数を 5 に設定する例を示します。

```
Switch(config-if)# dot1x max-req 5
```

再認証回数の設定

ポートが無認可ステートに移行する前に、スイッチが認証プロセスを再開する回数も変更できます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count*	ポートが無認可ステートに移行する前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルト値は 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの再認証回数に戻すには、**no dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

```
Switch(config-if)# dot1x max-reauth-req 4
```

MAC 移行のイネーブル化

MAC 移行により、認証済みホストをスイッチ上のあるポートから別のポートに移行できます。

スイッチで MAC 移行をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**authentication mac-move permit**	スイッチ上で MAC 移行をイネーブルに設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	（任意）設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、スイッチで MAC 移行をグローバルにイネーブルにする例を示します。

```
Switch(config)# authentication mac-move permit
```

MAC 置き換えのイネーブル化

MAC 置き換えによって、ホストがポート上の認証済みホストを置き換えることができます。

インターフェイス上で MAC 置き換えをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**}	インターフェイスで MAC 置き換えをイネーブルにするには、**replace** キーワードを使用します。ポートは、現行セッションを削除し、新しいホストで認証を開始します。 その他のキーワードには、次の効果があります。 • **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC アドレスのパケットをドロップします。 • **restrict**：CPU によって違反パケットがドロップされ、システム メッセージが生成されます。 • **shutdown**：予期しない MAC アドレスを受信すると、ポートがエラー ディセーブル状態になります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次の例では、インターフェイス上で MAC 置き換えをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# authentication violation replace
```

802.1X アカウンティングの設定

AAA システム アカウンティングと 802.1X アカウンティングをイネーブルにすると、ロギング用にシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。これにより、サーバはすべてのアクティブ 802.1X セッションが閉じていることを推測できます。

RADIUS では信頼性の低い UDP トランスポート プロトコルを使用するので、ネットワークの状態が悪いと、アカウンティング メッセージが消失する可能性があります。設定可能なアカウンティング要求の再送信回数を超えてもスイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のシステム メッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

停止メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注）　開始メッセージ、停止メッセージ、中間更新メッセージ、およびタイム スタンプのロギングなどのアカウンティング作業を実行するように RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブで、[Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブで、[CVS RADIUS Accounting] をイネーブルにします。

AAA をスイッチでイネーブルにしたあとに、802.1X アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting dot1x default start-stop group radius**	すべての RADIUS サーバのリストを使用して 802.1X アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting system default start-stop group radius**	（任意）（すべての RADIUS サーバのリストを使用して）システム アカウンティングをイネーブルにし、スイッチがリロードしたときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アカウンティング応答メッセージを受信しない RADIUS メッセージの数を表示するには、**show radius statistics** 特権 EXEC コマンドを使用します。

次に、802.1X アカウンティングを設定する例を示します。最初のコマンドは、RADIUS サーバを設定し、アカウンティング用の UDP ポートとして 1813 を指定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

ゲスト VLAN の設定

ゲスト VLAN を設定すると、サーバが EAP 要求/アイデンティティ フレームに対する応答を受信しない場合に、802.1X に対応していないクライアントがゲスト VLAN に置かれます。802.1X に対応しているが、認証に失敗したクライアントには、ネットワーク アクセスが許可されません。スイッチは、シングルホスト モードまたはマルチホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。
ステップ 5	**dot1x guest-vlan** *vlan-id*	アクティブ VLAN を 802.1X ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X ゲスト VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ゲスト VLAN をディセーブルにして削除するには、**no dot1x guest-vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無認可ステートに戻ります。

次に、VLAN 2 を 802.1X ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x guest-vlan 2
```

次に、スイッチの待機時間を 3 秒に設定し、スイッチが要求を再送信する前に EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数を 15 秒に設定し、802.1X ポートが DHCP クライアントに接続されているときに VLAN 2 を 802.1X ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

制限付き VLAN の設定

スイッチで制限付き VLAN を設定すると、認証サーバが有効なユーザ名およびパスワードを受信しない場合に、802.1X に準拠するクライアントが制限付き VLAN に移行します。スイッチは、シングルホスト モードでだけ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize** *vlan-id*	アクティブ VLAN を 802.1X 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X 制限付き VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

制限付き VLAN をディセーブルにして削除するには、**no dot1x auth-fail vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無認可ステートに戻ります。

次に、*VLAN 2* を 802.1X 制限付き VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x auth-fail vlan 2
```

dot1x auth-fail max-attempts インターフェイス コンフィギュレーション コマンドを使用して、ユーザが制限付き VLAN に割り当てられる前に許可される最大認証試行回数を設定できます。許容可能な認証試行回数の範囲は 1 ～ 3 回です。デフォルト値は 3 回です。

認証試行の最大許容回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。
ステップ 5	**dot1x auth-fail vlan** *vlan-id*	アクティブ VLAN を 802.1X 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X 制限付き VLAN として設定できます。
ステップ 6	**dot1x auth-fail max-attempts** *max attempts*	ポートが制限付き VLAN に移行する前に許可する認証試行の回数を指定します。指定できる範囲は 1 ～ 3 です。デフォルト値は 3 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト値に戻すには、**no dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが制限付き VLAN に移行する前に許可される認証試行の回数を *2* 回に設定する例を示します。

```
Switch(config-if)# dot1x auth-fail max-attempts 2
```

アクセス不能認証バイパス機能の設定

クリティカル認証または AAA 失敗ポリシーとも呼ばれるアクセス不能バイパス機能を設定できます。

ポートをクリティカル ポートとして設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server dead-criteria time** *time* **tries** *tries*	（任意）RADIUS サーバが使用不可または*停止状態*であると判断するために使用する条件を設定します。 *time* の範囲は 1 ～ 120 秒です。スイッチは、10 ～ 60 秒のデフォルトの *seconds* 値をダイナミックに決定します。 *tries* の範囲は 1 ～ 100 です。スイッチは、10 ～ 100 のデフォルトの *tries* パラメータをダイナミックに決定します。
ステップ 3	**radius-server deadtime** *minutes*	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。デフォルト値は 0 分です。
ステップ 4	**radius-server host** *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]	（任意）次のキーワードを使用して RADIUS サーバのパラメータを設定します。 • **acct-port** *udp-port :* RADIUS アカウンティング サーバ用の UDP ポートを指定します。UDP ポート番号の範囲は、0 ～ 65536 です。デフォルト値は 1646 です。 • **auth-port** *udp-port :* RADIUS 認証サーバ用の UDP ポートを指定します。UDP ポート番号の範囲は、0 ～ 65536 です。デフォルト値は 1645 です。 **（注）** RADIUS アカウンティング サーバ用の UDP ポートと、RADIUS 認証サーバ用の UDP ポートは、デフォルト以外の値に設定する必要があります。 • **test username** *name* : RADIUS サーバ ステータスの自動テストをイネーブルにし、使用するユーザ名を指定します。 • **idle-time** *time :* スイッチがサーバにテスト パケットを送信したあとの間隔を分単位で設定します。設定できる範囲は 1 ～ 35791 分です。デフォルト値は 60 分（1 時間）です。 • **ignore-acct-port** *:* RADIUS サーバのアカウンティング ポートのテストをディセーブルにします。 • **ignore-auth-port** *:* RADIUS サーバの認証ポートのテストをディセーブルにします。 • **key** *string :* スイッチと RADIUS デーモンの間のすべての RADIUS 通信のための認証キーおよび暗号キーを指定します。 **（注）** キーは、**radius-server host** コマンド構文の末尾で設定してください。これは、先頭のスペースは無視されるが、キーの文字列内または末尾のスペースは使用されるためです。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 **radius-server key** {**0** *string* | **7** *string* | *string*} グローバル コンフィギュレーション コマンドを使用して、認証キーおよび暗号キーを設定することもできます。

	コマンド	目的
ステップ 5	**dot1x critical** {**eapol** | **recovery delay** *milliseconds*}	（任意）アクセス不能認証バイパス用のパラメータを設定します。 **eapol**：スイッチがクリティカル ポートを正常に認証したときに EAPOL-Success メッセージを送信するように指定します。 **recovery delay** *milliseconds*：使用不可の RADIUS サーバが使用可能になったときにスイッチがクリティカル ポートの再初期化を待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 1000 ミリ秒です（ポートを 1 秒おきに再初期化できます）。
ステップ 6	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 7	**authentication event server dead action [authorize | reinitialize] vlan** *vlan-id*	RADIUS サーバに到達できない場合にポート上のホストを移行するには、次のキーワードを使用します。 • **authorize**：認証を試みるすべての新しいホストを、ユーザ指定のクリティカル VLAN に移行します。 • **reinitialize**：ポート上のすべての認可済みホストをユーザ指定のクリティカル VLAN に移行します。
ステップ 8	**dot1x critical** [**recovery action reinitialize** | **vlan** *vlan-id*]	アクセス不能認証バイパス機能をイネーブルにし、次のキーワードを使用してこの機能を設定します。 • **recovery action reinitialize**：回復機能をイネーブルにし、認証サーバが使用可能の場合に回復アクションによりポートを認証するよう指定します。 • **vlan** *vlan-id*：スイッチがクリティカル ポートを割り当てることができるアクセス VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスのデフォルト設定に戻すには、**no dot1x critical** {**eapol** | **recovery delay**} グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスをディセーブルにするには、**no dot1x critical** インターフェイス コンフィギュレーション コマンドを使用します。

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 1/1
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
```

```
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

802.1X 認証と WoL の設定

802.1X 認証と WoL をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**authentication control-direction {both | in}** または **dot1x control-direction** {**both** | **in**}	ポートで 802.1X 認証と WoL をイネーブルにし、次のキーワードを使用してポートを双方向または単一方向に設定します。 • **both**：ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。 • **in**：ポートを単一方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

802.1X 認証と WoL をディセーブルにするには、**no authentication control-direction** または **no dot1x control-direction** インターフェイス コンフィギュレーション コマンドを使用します。

次に、802.1X 認証と WoL をイネーブルにし、ポートを双方向に設定する例を示します。

```
Switch(config-if)# authentication control-direction both
```

または

```
Switch(config-if)# dot1x control-direction both
```

MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。
ステップ 4	**dot1x mac-auth-bypass** [**eap** | **timeout activity** {*value*}]	MAC 認証バイパスをイネーブルにします。 （任意）認可に EAP を使用するようにスイッチを設定するには、**eap** キーワードを使用します。 （任意）接続されているホストを無認可ステートにする前に非アクティブにできる秒数を設定するには、**timeout activity** キーワードを使用します。指定できる範囲は 1 ～ 65535 です。 タイムアウト値を設定する前に、ポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定」（P.29-9）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

MAC 認証バイパスをディセーブルにするには、**no dot1x mac-auth-bypass** インターフェイス コンフィギュレーション コマンドを使用します。

次に、MAC 認証バイパスをイネーブルにする方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass
```

802.1X ユーザ分散の設定

VLAN グループを設定し、その VLAN グループに VLAN をマッピングするには、グローバル コンフィギュレーションで次の手順を実行します。

	コマンド	目的
ステップ 1	**vlan group** *vlan-group-name* ***vlan-list*** *vlan-list*	VLAN グループを設定し、そのグループに 1 つの VLAN または VLAN の範囲をマッピングします。
ステップ 2	**show vlan group all** *vlan-group-name*	設定を確認します。
ステップ 3	**no vlan group** ***vlan-group-name*** **vlan-list** *vlan-list*	VLAN グループ設定または VLAN グループ設定の要素を消去します。

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ設定および指定した VLAN へのマッピングを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 10

switch(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
switch# show dot1x vlan-group all
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
hr-dept                         20
```

次に、既存の VLAN グループに VLAN を追加し、VLAN が追加されたことを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10,30
```

次に、VLAN グループから VLAN を削除する例を示します。

```
switch# no vlan group eng-dept vlan-list 10
```

次に、VLAN グループからすべての VLAN を消去したときに、VLAN グループを消去する例を示します。

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

switch(config)# show vlan group group-name eng-dept
```

次に、すべての VLAN グループを消去する例を示します。

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

NAC レイヤ 2 802.1X 検証の設定

NAC レイヤ 2 802.1X 検証を設定できます。この機能は、RADIUS サーバによる 802.1X 認証とも呼ばれます。

NAC レイヤ 2 802.1X 認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x guest-vlan** *vlan-id*	アクティブ VLAN を 802.1X ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X ゲスト VLAN として設定できます。
ステップ 4	**authentication periodic** または **dot1x reauthentication**	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルです。
ステップ 5	**dot1x timeout reauth-period** {*seconds* | **server**}	再認証の間隔（秒）を指定します。 キーワードの意味は次のとおりです。 • *seconds*：1 ～ 65535 の秒数を設定します。デフォルト値は 3600 秒です。 • **server**：Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）の値に基づいて、秒数を設定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	802.1X 認証の設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、NAC レイヤ 2 802.1X 検証を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

オーセンティケータおよびサプリカント スイッチと NEAT の設定

この機能を設定するには、配線クローゼットの外部にある 1 つのスイッチをサプリカントとして設定し、オーセンティケータ スイッチに接続する必要があります。

概要については、「802.1X サプリカント スイッチおよびオーセンティケータ スイッチと Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）」（P.12-30）を参照してください。

（注）　ACS で *cisco-av-pairs* を *device-traffic-class=switch* として設定する必要があります。これにより、サプリカントが正常に認証されたあとにインターフェイスがトランクとして設定されます。

スイッチをオーセンティケータとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	ポート モードを **access** に設定します。
ステップ 5	**authentication port-control auto**	ポート認証モードを自動に設定します。
ステップ 6	**dot1x pae authenticator**	インターフェイスを Port Access Entity（PAE; ポート アクセス エンティティ）オーセンティケータとして設定します。
ステップ 7	**spanning-tree portfast**	1 つのワークステーションまたはサーバに接続されたアクセス ポートで PortFast をイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id*	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、スイッチを 802.1X オーセンティケータとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

スイッチをサプリカントとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile*	802.1X クレデンシャル プロファイルを作成します。このクレデンシャル プロファイルは、サプリカントとして設定されたポートに割り当てる必要があります。
ステップ 4	**username** *suppswitch*	ユーザ名を作成します。

	コマンド	目的
ステップ 5	**password** *password*	新しいユーザ名用のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast**	スイッチに対し、ユニキャスト パケットまたはマルチキャスト パケットを受信したときにマルチキャスト EAPOL パケット*だけ*を送信するように強制します。 これにより、すべてのホスト モードのサプリカント スイッチで NEAT を動作させることも可能になります。
ステップ 7	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport trunk encapsulation dot1q**	ポートをトランク モードに設定します。
ステップ 9	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant**	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name*	802.1X クレデンシャル プロファイルをインターフェイスに割り当てます。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show running-config interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

Smartports マクロでの NEAT の設定

スイッチ VSA の代わりに Smartports ユーザ定義マクロを使用してオーセンティケータ スイッチを設定することもできます。詳細については、第 15 章「SmartPort マクロの設定」を参照してください。

802.1X 認証とダウンロード可能 ACL およびリダイレクト URL の設定

スイッチでの 802.1X 認証の設定に加えて、ACS を設定する必要があります。詳細については、Cisco Secure ACS の各種コンフィギュレーション ガイドを参照してください。

（注）　ダウンロード可能 ACL をスイッチにダウンロードする前に、ACS 上でダウンロード可能 ACL を設定する必要があります。

ポートでの認証後に、**show ip access-list** 特権 EXEC コマンドを使用してポート上のダウンロード可能 ACL を表示できます。

ダウンロード可能 ACL の設定

ポリシーは、クライアントが認証され、クライアントの IP アドレスが IP 装置追跡テーブルに追加されたあとに有効になります。次に、スイッチはダウンロード可能 ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking**	IP 装置追跡テーブルを設定します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa authorization network default group radius**	認可方式をローカルに設定します。認可方式を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 5	**radius-server vsa send authentication**	RADIUS VSA 送信認証を設定します。
ステップ 6	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip access-group** *acl-id* **in**	input 方向のポートでデフォルト ACL を設定します。 **（注）**　*acl-id* は、アクセス リストの名前または番号です。
ステップ 8	**show running-config interface** *interface-id*	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ダウンロード可能ポリシーの設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **deny source** *source-wildcard* **log**	送信元アドレスとワイルドカードを使用して、デフォルトのポート ACL を定義します。 access-list-number 値は、1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にアクセスを拒否するのか許可するのかを指定します。 *source* 値は、パケットを送信するネットワークまたはホストの送信元アドレスであり、次のようなものになります。 • ドット付き 10 進表記による 32 ビット長の値。 • source、および source-wildcard 値 0.0.0.0 255.255.255.255 の略を意味するキーワード any。source-wildcard 値を入力する必要はありません。 • source および source-wildcard 値 source 0.0.0.0 の略を意味するキーワード host。 （任意）source-wildcard を使用して、ワイルドカード ビットを送信元アドレスに適用します。 （任意）log を入力すると、エントリと一致するパケットの詳細を示すロギング メッセージがコンソールに送信されます。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip access-group** *acl-id* **in**	input 方向のポートでデフォルト ACL を設定します。 **（注）**　*acl-id* は、アクセス リストの名前または番号です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**aaa new-model**	AAA をイネーブルにします。
ステップ 7	**aaa authorization network default group radius**	認可方式をローカルに設定します。認可方式を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 8	**ip device tracking**	IP 装置追跡テーブルをイネーブルにします。 IP 装置追跡テーブルをディセーブルにするには、**no ip device tracking** グローバル コンフィギュレーション コマンドを使用します。
ステップ 9	**ip device tracking probe** [**count** | **interval** | **use-svi**]	（任意）IP 装置追跡テーブルを設定します。 • **count** *count*：スイッチが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 5 です。デフォルト値は 3 です。 • **interval** *interval*：スイッチが ARP プローブを再送信する前に、応答を待機する秒数を設定します。指定できる範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。 • **use-svi**：Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）IP アドレスを ARP プローブの送信元として使用します。
ステップ 10	**radius-server vsa send authentication**	ベンダー固有属性を認識および使用するようにネットワーク アクセス サーバを設定します。 **（注）**　ダウンロード可能 ACL が動作可能である必要があります。
ステップ 11	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 12	**show ip device tracking all**	IP 装置追跡テーブル内の各エントリの情報を表示します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ダウンロード可能ポリシー用にスイッチを設定する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

VLAN ID ベースの MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mab request format attribute 32 vlan access-vlan**	VLAN ID ベースの MAC 認証をイネーブルにします。
ステップ 3	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN ID ベースの MAC 認証のステータスを確認する show コマンドはありません。**debug radius accounting** 特権 EXEC コマンドを使用すると、RADIUS 属性 32 を確認できます。このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。
http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_q1.html#wp1123741

次に、スイッチで VLAN ID ベースの MAC 認証をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# mab request format attribute 32 vlan access-vlan
Switch(config-if)# exit
```

フレキシブルな認証順序付けの設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**authentication order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポートで使用する認証方式の順序を設定します。
ステップ 4	**authentication priority** [**dot1x** | **mab**] | {**webauth**}	（任意）認証方式をポート プライオリティ リストに追加します。
ステップ 5	**show authentication**	（任意）設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ポートが最初に 802.1X 認証を試行し、次に Web 認証をフォールバック方式として試行するように設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config)# authentication order dot1x webauth
```

Open1x の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication control-direction {both | in}**	（任意）ポート制御を単一方向または双方向に設定します。
ステップ 4	**authentication fallback** *name*	（任意）802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようにポートを設定します。
ステップ 5	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	（任意）ポートで認可マネージャ モードを設定します。
ステップ 6	**authentication open**	（任意）ポートでオープン アクセスをイネーブルまたはディセーブルにします。
ステップ 7	**authentication order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポートで使用する認証方式の順序を設定します。
ステップ 8	**authentication periodic**	（任意）ポートで再認証をイネーブルまたはディセーブルにします。
ステップ 9	**authentication port-control** {**auto** | **force-authorized** | **force-un authorized**}	（任意）ポートの認可ステートの手動制御をイネーブルにします。
ステップ 10	**show authentication**	（任意）設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ポートで Open1x を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config)# authentication control-direction both
Switch(config)# au ten tic at ion fallback profile1
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

ポートでの 802.1X 認証のディセーブル化

ポートで 802.1X 認証をディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1X 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no dot1x pae**	ポートで 802.1X 認証をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートを 802.1X ポート アクセス エンティティ（PAE）オーセンティケータとして設定し、ポートで 802.1X をイネーブルにしてポートに接続したクライアントが許可されないようにするには、**dot1x pae authenticator** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートで 802.1X 認証をディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no dot1x pae authenticator
```

802.1X 認証設定のデフォルト値へのリセット

802.1X 認証設定をデフォルト値にリセットするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	**dot1x default**	802.1X パラメータをデフォルト値にリセットします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

802.1X 統計情報およびステータスの表示

すべてのポートの 802.1X 統計情報を表示するには、**show dot1x all statistics** 特権 EXEC コマンドを使用します。特定のポートの 802.1X 統計情報を表示するには、**show dot1x statistics interface** *interface-id* 特権 EXEC コマンドを使用します。

スイッチの 802.1X 管理ステータスおよび動作ステータスを表示するには、**show dot1x all** [**details** | **statistics** | **summary**] 特権 EXEC コマンドを使用します。特定のポートの 802.1X 管理ステータスおよび動作ステータスを表示するには、**show dot1x interface** *interface-id* 特権 EXEC コマンドを使用します。

Cisco IOS Release 12.2(55)SE 以降、**no dot1x logging verbose** グローバル コンフィギュレーション コマンドを使用して、詳細な 802.1X 認証メッセージをフィルタリングできるようになりました。「認証マネージャの CLI コマンド」（P.12-9）を参照してください。

これらの出力に表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 13

Web ベースの認証の設定

この章では、Web ベースの認証の設定方法を説明します。この章で説明する内容は、次のとおりです。

（注） この章で使用しているスイッチ コマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

Web ベースの認証の概要

Web ベースの認証機能（*Web 認証プロキシ*）を使用して、IEEE 802.1x サプリカントを実行していないホスト システムでエンド ユーザを認証します。

（注） Web ベースの認証はレイヤ 2 およびレイヤ 3 インターフェイスに設定できます。

HTTP セッションを開始すると、Web ベースの認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザに HTML ログイン ページを送信します。ユーザがそれぞれのクレデンシャルを入力すると、Web ベースの認証機能はそれらのクレデンシャルを Authentication、Authorization、Accounting（AAA; 認証、認可、アカウンティング）サーバに送信して認証します。

認証が成功すると、Web ベースの認証はログイン成功 HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗すると、Web ベースの認証はログイン失敗 HTML ページをユーザに転送し、ユーザにログインの再試行を求めるメッセージを表示します。ユーザが最大試行回数を超えると、Web ベースの認証は、ログイン期限切れ HTML ページをホストに転送し、ユーザは待機期間の間ウォッチ リストに置かれます。

次の項では、AAA の一部としての Web ベースの認証の役割について説明します。

- 「Web 認証のカスタマイズ可能 Web ページ」（P.13-6）
- 「Web ベースの認証と他の機能との相互作用」（P.13-7）

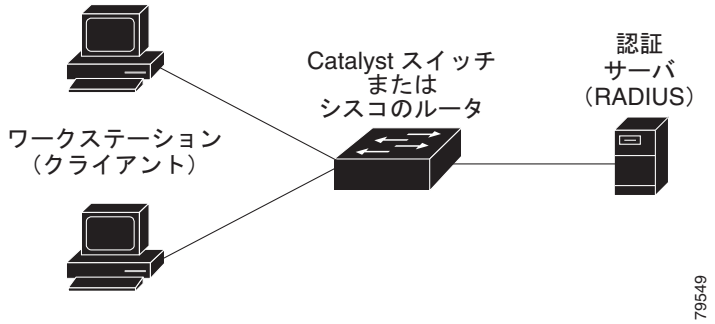
装置の役割

Web ベースの認証では、ネットワーク内の装置は次の特定の役割を持ちます。

- *クライアント*：LAN およびサービスへのアクセスを要求し、スイッチからの要求に応答する装置（ワークステーション）。ワークステーションでは、Java スクリプトがイネーブルの HTML ブラウザを実行している必要があります。
- *認証サーバ*：クライアントを認証します。認証サーバはクライアントの ID を検証し、クライアントが LAN およびスイッチ サービスへのアクセスが許可されたこと、またはクライアントが拒否されたことをスイッチに通知します。
- *スイッチ*：クライアントの認証ステータスに基づいてネットワークへの物理的なアクセスを制御します。スイッチはクライアントと認証サーバの間の仲介装置（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

図 13-1 に、ネットワークでのこれらの装置の役割を示します。

図 13-1　Web ベースの認証装置の役割



ホストの検出

スイッチは、検出されたホストに関する情報を格納する IP 装置追跡テーブルを維持します。

（注） デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベースの認証を使用するには、IP 装置追跡機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスの場合、Web ベースの認証は次のメカニズムを使用して IP ホストを検出します。

- ARP ベースのトリガー：Address Resolution Protocol（ARP; アドレス解決プロトコル）リダイレクト Access Control List（ACL; アクセス制御リスト）を使用すると、Web ベースの認証は、スタティック IP アドレスまたはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション。
- DHCP スヌーピング：スイッチがホストの Dynamic Host Configuration Protocol（DHCP）バインディング エントリを作成すると、Web ベースの認証に通知されます。

セッションの作成

Web ベースの認証で新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストの確認

  ホスト IP が例外リストに含まれている場合、例外リストのエントリのポリシーが適用され、セッションが確立されます。

- 認可バイパスの確認

  ホスト IP が例外リストにない場合、Web ベースの認証では、nonresponsive-host（NRH; 非応答ホスト）要求がサーバに送信されます。

  サーバの応答が *access accepted* である場合、このホストの認可はバイパスされます。セッションが確立されます。

- HTTP インターセプト ACL の設定

  NRH 要求に対するサーバの応答が *access rejected* である場合、HTTP インターセプト ACL がアクティブになり、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベースの認証をイネーブルにすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信されて、認可が開始されます。スイッチがログイン ページをユーザに送信します。ユーザがユーザ名とパスワードを入力すると、スイッチは認証サーバにエントリを送信します。
- 認証に成功すると、スイッチは認証サーバからユーザのアクセス ポリシーをダウンロードして、アクティブにします。ログイン成功ページがユーザに送信されます。
- 認証に失敗すると、スイッチはログイン失敗ページを送信します。ユーザはログインを再試行します。最大試行回数だけ失敗すると、スイッチはログイン期限切れページを送信し、ホストはウォッチ リストに置かれます。ウォッチ リストが時間切れになったあと、ユーザは認証プロセスを再試行できます。
- 認証サーバがスイッチに応答しない場合、および AAA 失敗ポリシーが設定されている場合、スイッチはホストにアクセス失敗ポリシーを適用します。ログイン成功ページがユーザに送信されます（「ローカルの Web 認証バナー」（P.13-4）を参照）。
- スイッチは、ホストがレイヤ 2 インターフェイスで ARP プローブに応答しない場合、またはレイヤ 3 インターフェイスでホストがアイドル タイムアウト内にトラフィックを送信しない場合に、クライアントを再認証します。
- この機能では、ダウンロードされたタイムアウトまたはローカルで設定されたセッション タイムアウトが適用されます。
- 終端アクションが RADIUS である場合、この機能では、非応答ホスト（NRH）要求がサーバに送信されます。終端アクションは、サーバからの応答に含まれます。
- 終端アクションがデフォルトである場合、セッションは終了し、適用されたポリシーは削除されます。

ローカルの Web 認証バナー

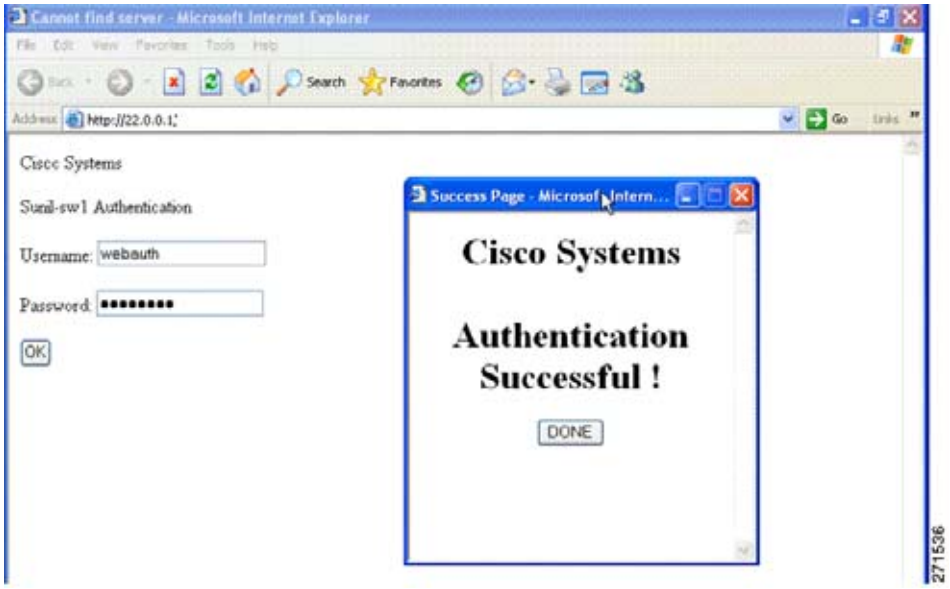
Web 認証を使用してスイッチにログインするときに表示されるバナーを作成できます。

バナーはログイン ページと認証結果ポップアップ ページの両方に表示されます。

- *Authentication Successful*
- *Authentication Failed*
- *Authentication Expired*

ip admission auth-proxy-banner http グローバル コンフィギュレーション コマンドを使用して、バナーを作成できます。デフォルトのバナー「*Cisco Systems*」および「*Switch host-name Authentication*」はログイン ページに表示されます。「*Cisco Systems*」は認証結果のポップアップ ページに表示されます（図 13-2 を参照）。

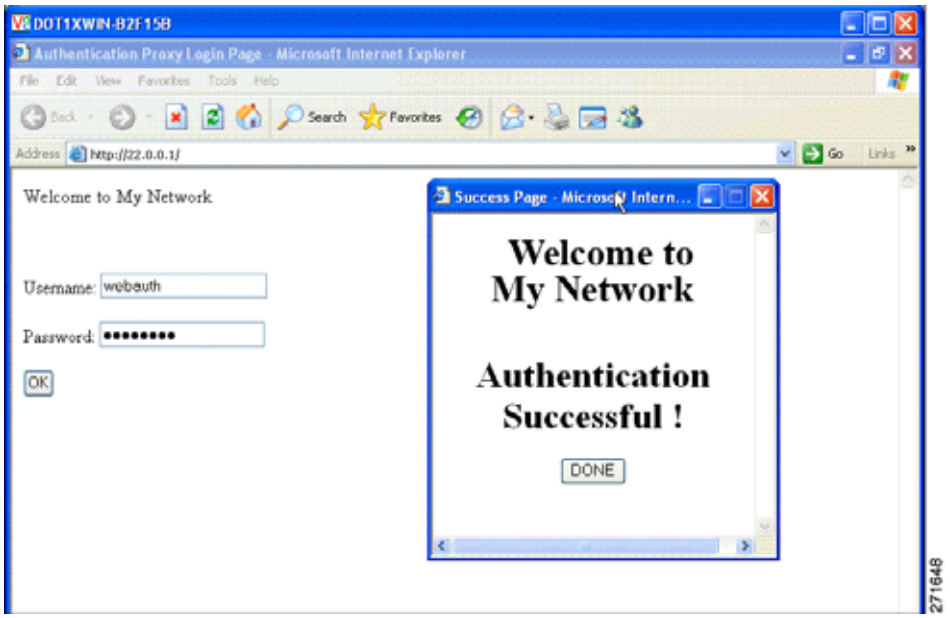
図 13-2　Authentication Successful バナー



また、バナーをカスタマイズすることもできます（図 13-3 を参照）。

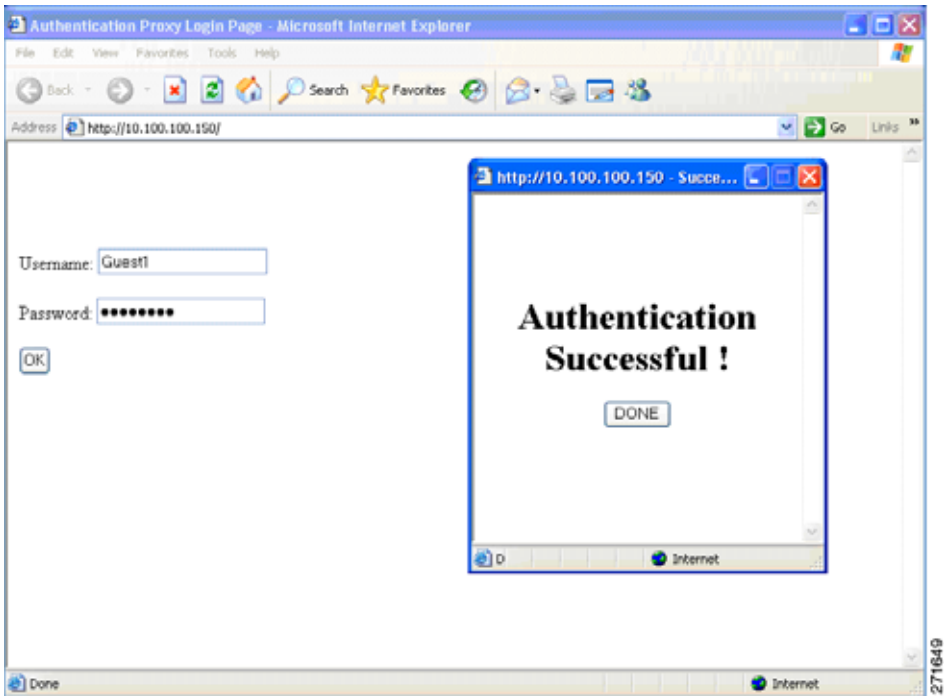
- スイッチ、ルータ、または会社名をバナーに追加するには、**ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用します。
- ロゴまたはテキスト ファイルをバナーに追加するには、**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。

図 13-3　カスタマイズされた Web バナー



バナーをイネーブルにしない場合、図 13-4 に示すように、スイッチへのログイン時に Web 認証のログイン画面にはユーザ名とパスワードのダイアログ ボックスだけが表示され、バナーは表示されません。

図 13-4　バナーのないログイン画面



詳細については、『Cisco IOS Security Command Reference』および「Web 認証ローカル バナーの設定」（P.13-16）を参照してください。

Web 認証のカスタマイズ可能 Web ページ

Web ベースの認証プロセス中、スイッチの内部 HTTP サーバが、4 つの HTML ページをホストして、認証するクライアントに配信します。サーバはこれらのページを使用して、次の 4 つの認証プロセスのステートを通知します。

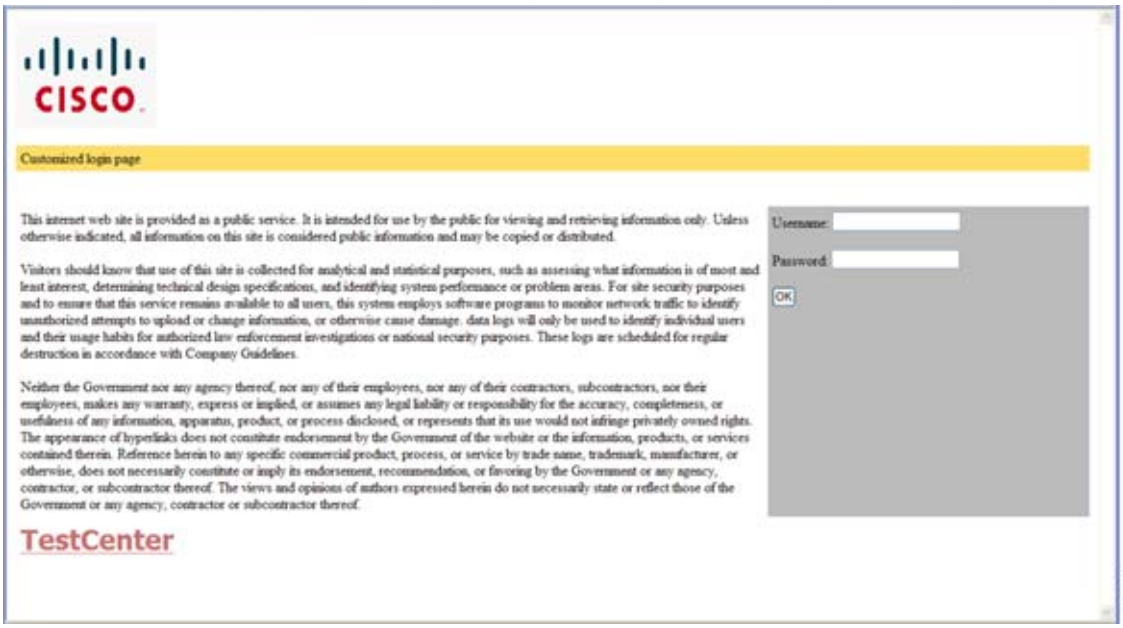
- ログイン：クレデンシャルが要求されています。
- 成功：ログインが成功しました。
- 失敗：ログインが失敗しました。
- 期限切れ：ログインに何度も失敗しているため、ログイン セッションの期限が切れました。

注意事項

- デフォルトの内部 HTML ページを独自の HTML ページに置き換えることができます。
- *ログイン*、*成功*、*失敗*、および*期限切れ* Web ページでロゴを使用したり、テキストを指定したりできます。
- バナー ページでは、ログイン ページのテキストを指定できます。
- ページは HTML 形式になります。
- 成功ページに、特定の URL にアクセスするための HTML リダイレクト コマンドを含める必要があります。
- URL ストリングは有効な URL（http://www.cisco.com など）にする必要があります。不完全な URL を指定すると、*page not found* などのエラーが Web ブラウザに表示される場合があります。
- HTTP 認証用に Web ページを設定する場合は、適切な HTML コマンド（ページのタイムアウトを設定したり、非表示パスワードを設定したり、同じページが 2 回送信されていないか確認したりするなど）を含める必要があります。
- ユーザを特定の URL にリダイレクトする CLI（コマンドライン インターフェイス）コマンドは、設定されたログイン フォームがイネーブルな場合は使用できません。管理者は、Web ページにリダイレクションが設定されていることを確認する必要があります。
- 認証が行われたあとにユーザを特定の URL にリダイレクトする CLI コマンドが入力されてから、Web ページを設定するコマンドが入力されると、ユーザを特定の URL にリダイレクトする CLI コマンドは無効になります。
- 設定された Web ページは、スイッチのブート フラッシュまたはフラッシュにコピーできます。
- 設定されたページには、スタック マスターまたはメンバー上のフラッシュからアクセスできます。
- ログイン ページは 1 つのフラッシュに格納でき、成功ページと失敗ページは別のフラッシュ（たとえば、スタック マスターまたはメンバーのフラッシュ）に格納できます。
- 4 つのページをすべて設定する必要があります。
- バナー ページは Web ページで設定されている場合、無効です。
- システム ディレクトリ（flash、disk0、または disk）に格納され、ログイン ページに表示する必要のあるすべてのロゴ ファイル（イメージ、フラッシュ、オーディオ、ビデオなど）では、ファイル名として *web_auth_<filename>* を使用する必要があります。
- 設定された認証プロキシ機能は、HTTP と Secure Socket Layer（SSL）の両方をサポートします。

デフォルトの内部 HTML ページを独自の HTML ページに置き換えることができます（図 13-5 (P.13-7) を参照）。また、認証が行われたあとにユーザがリダイレクトされる URL を指定することもできます。この URL は内部の成功ページを置き換えます。

図 13-5　認証ページのカスタマイズ



詳細については、「認証プロキシ Web ページのカスタマイズ」（P.13-13）を参照してください。

Web ベースの認証と他の機能との相互作用

- 「ポート セキュリティ」（P.13-7）
- 「LAN ポート IP」（P.13-7）
- 「ゲートウェイ IP」（P.13-8）
- 「ACL」（P.13-8）
- 「コンテキスト ベースのアクセス制御」（P.13-8）
- 「802.1x 認証」（P.13-8）
- 「EtherChannel」（P.13-8）

ポート セキュリティ

Web ベースの認証とポート セキュリティは、同じポートに設定できます。Web ベースの認証はポートを認証し、ポート セキュリティはクライアントの Media Access Control（MAC; メディア アクセス制御）アドレスを含むすべての MAC アドレスのネットワーク アクセスを管理します。そのあと、ポートを介してネットワークにアクセスできるクライアントの数またはグループを制限できます。

ポート セキュリティをイネーブルにする方法の詳細については、「ポート セキュリティの設定」（P.29-9）を参照してください。

LAN ポート IP

LAN Port IP（LPIP; LAN ポート IP）およびレイヤ 2 の Web ベースの認証は、同じポートに設定できます。ホストは最初に Web ベースの認証を使用して認証され、そのあとに LPIP ポスチャ検証が行われます。LPIP ホスト ポリシーは、Web ベースの認証ホスト ポリシーよりも優先されます。

Web ベースの認証のアイドル タイマーが時間切れになると、Network Admission Control（NAC）ポリシーが削除されます。ホストが認証され、ポスチャが再検証されます。

ゲートウェイ IP

Web ベースの認証が VLAN 内のスイッチ ポートのいずれかに設定されている場合、レイヤ 3 インターフェイスに Gateway IP（GWIP; ゲートウェイ IP）を設定することはできません。

Web ベースの認証は、ゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアでは両方の機能のホスト ポリシーが適用されます。GWIP ポリシーは、Web ベースの認証ホスト ポリシーよりも優先されます。

ACL

インターフェイスに VLAN ACL または Cisco IOS ACL を設定している場合は、Web ベースの認証ホスト ポリシーの適用後に限り ACL がホスト トラフィックに適用されます。

レイヤ 2 の Web ベースの認証の場合は、ポートに接続されているホストからの入力トラフィックに対するデフォルトのアクセス ポリシーとして Port ACL（PACL; ポート ACL）を設定する必要があります。認証後、Web ベースの認証ホスト ポリシーは、PACL よりも優先されます。

同じインターフェイスに MAC ACL と Web ベースの認証を設定することはできません。

アクセス VLAN が VACL キャプチャに設定されているポートには、Web ベースの認証を設定できません。

コンテキスト ベースのアクセス制御

Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）がポート VLAN のレイヤ 3 VLAN インターフェイスに設定されている場合、Web ベースの認証をレイヤ 2 ポートに設定することはできません。

802.1x 認証

フォールバック認証方式を除き、802.1x 認証と同じポートに Web ベースの認証を設定することはできません。

EtherChannel

レイヤ 2 EtherChannel インターフェイスに Web ベースの認証を設定できます。Web ベースの認証設定は、すべてのメンバー チャネルに適用されます。

Web ベースの認証の設定

Web ベースの認証のデフォルト設定

表 13-1 に、Web ベースの認証のデフォルト設定を示します。

表 13-1　Web ベースの認証のデフォルト設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし • 1812 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベースの認証設定時の注意事項および制約事項

- Web ベースの認証は、入力だけの機能です。
- Web ベースの認証は、アクセス ポートにだけ設定できます。Web ベースの認証は、トランク ポート、EtherChannel メンバー ポートまたはダイナミック トランク ポートではサポートされません。
- Web ベースの認証を設定する前に、インターフェイスにデフォルトの ACL を設定する必要があります。レイヤ 2 インターフェイスの場合はポート ACL を設定し、レイヤ 3 インターフェイスの場合は Cisco IOS ACL を設定します。
- スタティック ARP キャッシュ 割り当てを使用するレイヤ 2 インターフェイスではホストを認証できません。これらのホストは ARP メッセージを送信しないため、Web ベースの認証機能で検出されません。
- デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベースの認証を使用するには、IP 装置追跡機能をイネーブルにする必要があります。
- スイッチの HTTP サーバを実行する IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホストの IP アドレスに到達するためのルートを設定する必要もあります。HTTP サーバは HTTP ログイン ページをホストに送信します。

- Spanning Tree Protocol（STP; スパニング ツリー プロトコル）トポロジの変更によってホストのトラフィックが別のポートに届いた場合、複数のホップ先にあるホストではトラフィックが中断される場合があります。このようなトラフィックの中断は、レイヤ 2（STP）トポロジが変更されたあとに、ARP と DHCP の更新が送信できない場合があるために生じます。
- Web ベースの認証は、ダウンロード可能なホスト ポリシーとして VLAN 割り当てをサポートしません。
- Web ベースの認証は、IPv6 トラフィックでサポートされません。

Web ベースの認証設定のタスク リスト

認証のルールとインターフェイスの設定

	コマンド	目的
ステップ 1	**ip admission name** *name* **proxy http**	Web ベースの認可の認証ルールを設定します。
ステップ 2	**interface** *type slot/port*	インターフェイス コンフィギュレーション モードを開始し、Web ベースの認証でイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 *type* には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 3	**ip access-group** *name*	デフォルトの ACL を適用します。
ステップ 4	**ip admission** *name*	指定したインターフェイスに Web ベースの認証を設定します。
ステップ 5	**exit**	コンフィギュレーション モードに戻ります。
ステップ 6	**ip device tracking**	IP 装置追跡テーブルをイネーブルにします。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip admission configuration**	設定を表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ポート FastEthernet 5/1 で Web ベースの認証をイネーブルにする例を示します。

```
Switch(config)# ip admission name webauth1 proxy http
Switch(config)# interface fastethernet 5/1
Switch(config-if)# ip admission webauth1
Switch(config-if)# exit
Switch(config)# ip device tracking
```

次に、設定を確認する例を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name webauth1
    http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 認証の設定

	コマンド	目的
ステップ 1	**aaa new-model**	AAA 機能をイネーブルにします。
ステップ 2	**aaa authentication login default group** {*tacacs+* | *radius*}	ログイン時に認証方式のリストを定義します。
ステップ 3	**aaa authorization auth-proxy default group** {*tacacs+* | *radius*}	Web ベースの認可の認可方式のリストを作成します。
ステップ 4	**tacacs-server host** {*hostname* | *ip_address*}	AAA サーバを指定します。RADIUS サーバについては、「スイッチと RADIUS サーバ間の通信設定」（P.13-11）を参照してください。
ステップ 5	**tacacs-server key** {*key-data*}	スイッチと TACACS サーバとの間で使用する認証キーおよび暗号キーを設定します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、AAA をイネーブルにする例を示します。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group tacacs+
Switch(config)# aaa authorization auth-proxy default group tacacs+
```

スイッチと RADIUS サーバ間の通信設定

RADIUS セキュリティ サーバは次のもので識別されます。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同じ IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。

RADIUS サーバ パラメータを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	**ip radius source-interface** *interface_name*	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **test username** *username*	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username** *username* オプションを指定すると、RADIUS サーバ接続の自動テストがイネーブルになります。指定された *username* は有効なユーザ名である必要はありません。 **key** オプションでは、スイッチと RADIUS サーバとの間で使用する認証キーおよび暗号キーを指定します。 複数の RADIUS サーバを使用するには、サーバごとにこのコマンドを再入力します。
ステップ 3	**radius-server key** *string*	スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証キーおよび暗号キーを設定します。
ステップ 4	**radius-server vsa send authentication**	RADIUS サーバからの ACL のダウンロードをイネーブルにします。この機能は、Cisco IOS Release 12.2(50)SG でサポートされます。
ステップ 5	**radius-server dead-criteria tries** *num-tries*	サーバが非アクティブと見なされるまでの RADIUS サーバに対する非応答送信メッセージの数を指定します。*num-tries* に指定できる値の範囲は 1 ～ 100 です。

RADIUS サーバ パラメータを設定するには、次の手順を実行します。

- 別のコマンドラインには、**key** *string* を指定します。
- **key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証キーおよび暗号キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。
- **key** *string* を指定する場合、キーの途中および末尾のスペースを使用します。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。
- **radius-server host** グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、次の URL の 『*Cisco IOS Security Configuration Guide*』*Release 12.2* および『 *Cisco IOS Security Command Reference*』*Release 12.2* を参照してください。
  http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

（注）　RADIUS サーバには、スイッチ IP アドレス、サーバとスイッチの両方で共有するキー文字列、Downloadable ACL（DACL; ダウンロード可能 ACL）などのいくつかの設定を行う必要があります。詳細については、RADIUS サーバのマニュアルを参照してください。

次に、スイッチで RADIUS サーバ パラメータを設定する例を示します。

```
Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.120.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(config)# radius-server dead-criteria tries 2
```

HTTP サーバの設定

Web ベースの認証を使用するには、スイッチ内で HTTP サーバをイネーブルにする必要があります。HTTP または HTTPS のいずれかに対してサーバをイネーブルにできます。

	コマンド	目的
ステップ 1	**ip http server**	HTTP サーバをイネーブルにします。Web ベースの認証機能では、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
ステップ 2	**ip http secure-server**	HTTPS をイネーブルにします。

カスタムの認証プロキシ Web ページを設定するか、ログインの成功を示すリダイレクション URL を指定できます。

（注）　**ip http secure-secure** コマンドの入力時にセキュアな認証を行うために、ユーザが HTTP 要求を送信する場合でも、ログイン ページは常に HTTPS（セキュア HTTP）形式になります。

- 「認証プロキシ Web ページのカスタマイズ」
- 「ログインの成功を示すリダイレクション URL の設定」

認証プロキシ Web ページのカスタマイズ

Web ベースの認証の実行時にスイッチのデフォルト HTML ページの代わりとなる 4 つの HTML ページが表示されるように、Web 認証を設定できます。

カスタムの認証プロキシ Web ページの使用を指定するには、まずカスタムの HTML ファイルをスイッチのフラッシュ メモリに格納し、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	**ip admission proxy http login page file** *device:login-filename*	デフォルトのログイン ページの代わりに使用するカスタムの HTML ファイルのスイッチ メモリ ファイル システムにおける場所を指定します。*device:* はフラッシュ メモリです。
ステップ 2	**ip admission proxy http success page file** *device:success-filename*	デフォルトのログイン成功ページの代わりに使用するカスタムの HTML ファイルの場所を指定します。

	コマンド	目的
ステップ 3	**ip admission proxy http failure page file** *device:fail-filename*	デフォルトのログイン失敗ページの代わりに使用するカスタムの HTML ファイルの場所を指定します。
ステップ 4	**ip admission proxy http login expired page file** *device:expired-filename*	デフォルトのログイン期限切れページの代わりに使用するカスタムの HTML ファイルの場所を指定します。

カスタマイズされた認証プロキシ Web ページを設定する場合は、次の注意事項に従ってください。

- カスタムの Web ページ機能をイネーブルにするには、4 つのカスタム HTML ファイルをすべて指定します。4 つよりも少ない数のファイルを指定すると、内部のデフォルト HTML ページが使用されます。
- 4 つのカスタム HTML ファイルは、スイッチのフラッシュ メモリに格納する必要があります。各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページのイメージはすべてアクセス可能な HTTP サーバに格納する必要があります。アドミッション ルール内でインターセプト ACL を設定します。
- カスタム ページからの外部リンクには、アドミッション ルール内にインターセプト ACL を設定する必要があります。
- 有効な Domain Name System（DNS; ドメイン ネーム システム）サーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、アドミッション ルール内にインターセプト ACL を設定する必要があります。
- カスタムの Web ページ機能がイネーブルの場合、設定された auth-proxy-banner は使用されません。
- カスタムの Web ページ機能がイネーブルの場合、ログイン成功機能のリダイレクション URL は使用できません。
- カスタム ファイルの指定を削除するには、このコマンドの **no** 形式を使用します。

カスタムのログイン ページはパブリック Web フォームであるため、このページについては次の点に注意してください。

- ログイン フォームはユーザ名とパスワードのユーザ エントリを受け入れる必要があります。また、それらのユーザ名とパスワードは **uname** および **pwd** として表示される必要があります。
- カスタムのログイン ページは、ページ タイムアウト、非表示パスワード、冗長な送信の回避など、Web フォームのベスト プラクティスに従う必要があります。

次に、カスタムの認証プロキシ Web ページを設定する例を示します。

```
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
```

次に、カスタムの認証プロキシ Web ページの設定を検証する例を示します。

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
 Success page         : flash:success.htm
 Fail Page            : flash:fail.htm
 Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

ログインの成功を示すリダイレクション URL の設定

認証後にユーザがリダイレクトされる URL を指定できます。この URL は内部の*成功* HTML ページを置き換えます。

コマンド	目的
ip admission proxy http success redirect *url-string*	デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。

ログインの成功を示すリダイレクション URL を設定する場合は、次の点に注意してください。

- カスタムの認証プロキシ Web ページ機能がイネーブルの場合、リダイレクション URL 機能はディセーブルになり、CLI で使用できません。カスタムのログイン成功ページでリダイレクションを実行できます。
- リダクレイション URL 機能がイネーブルの場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を削除するには、このコマンドの **no** 形式を指定します。

次に、ログインの成功を示すリダクレイション URL を設定する例を示します。

```
Switch(config)# ip admission proxy http success redirect www.cisco.com
```

次に、ログインの成功を示すリダクレイション URL を検証する例を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 失敗ポリシーの設定

	コマンド	目的
ステップ 1	**ip admission name** *rule-name* **proxy http event timeout aaa policy identity** *identity_policy_name*	AAA 失敗ルールを作成し、AAA サーバに到達できない場合にセッションに適用されるアイデンティティ ポリシーを関連付けます。 **（注）** ルールを削除するには、**no ip admission name** *rule-name* **proxy http event timeout aaa policy identity** グローバル コンフィギュレーション コマンドを使用します。
ステップ 2	**ip admission ratelimit aaa-down** *number_of_sessions*	（任意）AAA ダウン ステートでのホストからの認証試行回数をレート制限して、サービスに戻るときの AAA サーバのフラッディングを回避します。

次に、AAA 失敗ポリシーを適用する例を示します。

```
Switch(config)# ip admission name AAA_FAIL_POLICY proxy http event timeout aaa policy
identity GLOBAL_POLICY1
```

次に、接続されているホストが AAA ダウン ステートかどうかを確認する例を示します。

```
Switch# show ip admission cache
Authentication Proxy Cache
 Client IP 209.165.201.11 Port 0, timeout 60, state ESTAB (AAA Down)
```

次に、ホスト IP アドレスに基づいて特定のセッションに関する詳細情報を表示する例を示します。

```
Switch# show ip admission cache 209.165.201.11
Address              : 209.165.201.11
MAC Address          : 0000.0000.0000
Interface            : Vlan333
Port                 : 3999
Timeout              : 60
Age                  : 1
State                : AAA Down
AAA Down policy      : AAA_FAIL_POLICY
```

Web ベースの認証パラメータの設定

クライアントが待機期間にウォッチ リストに置かれるまでのログイン失敗最大試行回数を設定できます。

	コマンド	目的
ステップ 1	**ip admission max-login-attempts** *number*	ログイン失敗最大試行回数を設定します。指定できる範囲は 1 ～ 2147483647 回です。デフォルト値は 5 です。
ステップ 2	**end**	特権 EXEC モードに戻ります。
ステップ 3	**show ip admission configuration**	認証プロキシ設定を表示します。
ステップ 4	**show ip admission cache**	認証エントリのリストを表示します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ログイン失敗最大試行回数を 10 に設定する例を示します。

```
Switch(config)# ip admission max-login-attempts 10
```

Web 認証ローカル バナーの設定

Web 認証が設定されているスイッチにローカル バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*]	ローカル バナーをイネーブルにします。 （任意）*C banner-text C* を入力してカスタム バナーを作成します。ここで、*C* はデリミタを示します。または、file-path でバナーに表示されるファイル（ロゴやテキスト ファイルなど）を指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、カスタム メッセージ「*My Switch*」を含むローカル バナーを設定する例を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
```

ip auth-proxy auth-proxy-banner コマンドの詳細については、Cisco.com にある『*Cisco IOS Security Command Reference*』の「Authentication Proxy Commands」を参照してください。

Web ベースの認証キャッシュ エントリの削除

コマンド	目的
clear ip auth-proxy cache {* | *host ip address*}	認証プロキシ エントリを削除します。すべてのキャッシュ エントリを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、特定の IP アドレスを入力します。
clear ip admission cache {* | *host ip address*}	認証プロキシ エントリを削除します。すべてのキャッシュ エントリを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、特定の IP アドレスを入力します。

次に、IP アドレス 209.165.201.1 にあるクライアントの Web ベースの認証セッションを削除する例を示します。

```
Switch# clear ip auth-proxy cache 209.165.201.1
```

Web ベースの認証ステータスの表示

すべてのインターフェイスまたは特定のポートの Web ベースの認証設定を表示するには、次の作業を実行します。

	コマンド	目的
ステップ 1	**show authentication sessions** [**interface** *type slot/port*]	Web ベースの認証設定を表示します。 type = fastethernet、gigabitethernet または tengigabitethernet （任意）特定のインターフェイスの Web ベースの認証設定を表示するには、**interface** キーワードを使用します。

次に、グローバルな Web ベースの認証ステータスだけを表示する例を示します。

```
Switch# show authentication sessions
```

次に、ギガビット インターフェイス 3/27 の Web ベースの認証設定を表示する例を示します。

```
Switch# show authentication sessions interface gigabitethernet 3/27
```

CHAPTER 14

インターフェイスの特性の設定

この章では、IE 3000 インターフェイスのタイプを定義し、それを設定する方法について説明します。

（注） この章で使用しているコマンドの構文と使用方法の詳細については、このリリースのスイッチのコマンド リファレンスおよび Cisco.com ページの [Documentation] > [Cisco IOS Software Release] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Interface Command Reference, Release 12.2*』を参照してください。

インターフェイス タイプの概要

ここでは、サポートされるさまざまなインターフェイス タイプを、これらのインターフェイスの設定に関する詳細情報を含む章と関連付けて説明します。

ポートベースの VLAN

VLAN は、ユーザの物理的な位置にかかわりなく、機能、チーム、またはアプリケーション単位で論理的なセグメントに分割したスイッチド ネットワークです。VLAN の詳細については、第 16 章「VLAN の設定」を参照してください。ポートで受信したパケットは、受信ポートと同じ VLAN に属するポートだけに転送されます。異なる VLAN でのネットワーク装置が相互に通信するには、VLAN 間のトラフィックをルーティングするためにレイヤ 3 装置を使用する必要があります。

VLAN パーティションによって VLAN のトラフィックに堅固なファイアウォールが提供され、各 VLAN が独自の MAC アドレス テーブルを持つようになります。VLAN が成立するのは、VLAN と関連付けるためにローカル ポートが設定された場合、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）がトランク上のネイバーから VLAN の存在を認識した場合、またはユーザが VLAN を作成した場合です。

VLAN を設定するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して、VLAN コンフィギュレーション モードを開始します。標準範囲 VLAN（VLAN ID は 1 ～ 1005）に対応する VLAN 設定は、VLAN データベースに保存されます。VTP のバージョンが 1 または 2 の場合、拡張範囲 VLAN（VLAN ID は 1006 ～ 4094）を設定するには、まず、VTP モードをトランスペアレントに設定する必要があります。トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに追加されるのではなく、スイッチの実行コンフィギュレーションに保存されます。VTP バージョン 3 を使用すると、クライアント モードまたはサーバ モードで拡張範囲 VLAN を作成できます。これらの VLAN は、VLAN データベースに保存されます。

switchport インターフェイス コンフィギュレーション コマンドを使用してポートを VLAN に追加するには、次の手順を実行します。

- インターフェイスを識別します。
- トランク ポートには、トランクの特性を設定し、必要に応じて VLAN をその所属先に定義します。
- アクセス ポートには、VLAN をその所属先に設定および定義します。
- トンネル ポートには、カスタマー固有の VLAN タグに VLAN ID を設定および定義します。第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

スイッチ ポート

スイッチ ポートはレイヤ 2 限定のインターフェイスであり、物理ポートに関連付けられます。スイッチ ポートは 1 つまたは複数の VLAN に属します。スイッチ ポートを使用して、物理インターフェイスと関連するレイヤ 2 プロトコルを管理します。スイッチ ポートでは、ルーティングまたはブリッジングが処理されません。

スイッチ ポートは、アクセス ポート、トランク ポート、またはトンネル ポートとして使用できます。ポートをアクセス ポートまたはトランク ポートとして設定するか、Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）をポート単位で動作させ、リンクの反対側にあるポートとネゴシエートすることでスイッチポート モードを設定できます。トンネル ポートは、IEEE 802.1Q トランク ポートに接続する非対称リンクの一部として、手動で設定する必要があります。

スイッチ ポートを設定するには、**switchport** インターフェイス コンフィギュレーション コマンドを使用します。

レイヤ 3 モードにあるインターフェイスをレイヤ 2 モードにするには、キーワードを指定せずに **switchport** コマンドを使用します。

（注） レイヤ 3 インターフェイスをレイヤ 2 モードに変更すると、影響を受けるインターフェイスに関連する設定情報が失われる可能性があり、インターフェイスはデフォルト設定に戻ります。

アクセス ポートおよびトランク ポートの特性の設定に関する詳細については、第 16 章「VLAN の設定」を参照してください。トンネル ポートの詳細については、第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

アクセス ポート

アクセス ポートは、所属先となる 1 つの VLAN のトラフィックだけを伝送します（音声 VLAN ポートとして設定された場合は例外となります）。トラフィックは VLAN タギングのないネイティブ形式で送受信されます。アクセス ポートで受信されるトラフィックは、ポートに割り当てられた VLAN に属すると想定されます。

アクセス ポートで 802.1Q タグ付きパケットが受信される場合、パケットは廃棄され、送信元アドレスも認識されません。

サポートされるアクセス ポートは、次のとおりです。

- スタティック アクセス ポートは、手動（または IEEE 802.1x と併用する RADIUS サーバを介して）で VLAN に割り当てられます。詳細については、「802.1X 認証と VLAN 割り当て」（P.12-16）を参照してください。
- ダイナミック アクセス ポートの VLAN メンバーシップは、着信パケットによって認識されます。ダイナミック アクセス ポートは、デフォルトで VLAN のメンバーではありません。ポートの VLAN メンバーシップが検出された場合に限り、このポートを転送先および転送元とするトラフィック転送がイネーブルになります。スイッチ上のダイナミック アクセス ポートは、VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）によって VLAN に割り当てられます。VMPS を Catalyst 6500 シリーズ スイッチにすることはできます。IE 3000 スイッチは VMPS サーバとして使用できません。

また、接続された Cisco IP Phone を使用してアクセス ポートを設定し、1 つの VLAN を音声トラフィック用に、別の VLAN を IP Phone に接続された装置からのデータ トラフィック用にすることもできます。音声 VLAN ポートの詳細については、第 18 章「音声 VLAN の設定」を参照してください。

トランク ポート

トランク ポートは複数の VLAN のトラフィックを伝送し、デフォルトで VLAN データベースに存在するすべての VLAN のメンバーになります。

このスイッチは、802.1Q トランク ポートだけをサポートします。802.1Q トランク ポートは、タグ付きおよびタグなしのトラフィックを同時にサポートします。トランク ポートは、デフォルトの Port VLAN ID（PVID; ポート VLAN ID）に割り当てられ、すべてのタグなしトラフィックはポートのデフォルト PVID 上を流れます。すべてのタグなしトラフィックと、VLAN ID が NULL のタグ付きトラフィックは、デフォルトの PVID のポートに属します。発信ポートのデフォルトの PVID と同じ VLAN ID が含まれるパケットは、タグなしで送信されます。他のすべてのトラフィックは VLAN タグ付きで送信されます。

デフォルトで、トランク ポートは VTP が認識した各 VLAN のメンバーになりますが、トランク ポートごとの VLAN に許可リストを設定して、VLAN メンバーシップを制限できます。許可された VLAN のリストは、関連付けられたトランク ポートだけに影響を与えます。デフォルトで、可能性のあるすべての VLAN（VLAN ID 1 ～ 4094）が許可リストに含まれます。トランク ポートは、VTP が VLAN を認識し、VLAN がイネーブルの場合に限り、VLAN のメンバーになることができます。VTP によって新しいイネーブル状態の VLAN が認識され、この VLAN が許可リストに含まれる場合、トランク ポートは自動的にその VLAN のメンバーになります。トラフィックはその VLAN のトランク ポートに送受信されます。VTP によってイネーブル状態の VLAN が認識されても、その VLAN がトランク ポートの許可リストに含まれない場合、このポートは VLAN のメンバーにならないため、VLAN のトラフィックはポートで送受信されません。

トランク ポートの詳細については、第 16 章「VLAN の設定」を参照してください。

トンネル ポート

トンネル ポートは、サービス プロバイダー ネットワークにおけるカスタマーのトラフィックを、同じ VLAN 番号を使用する他のカスタマーから分離するために IEEE 802.1Q トンネリングで使用します。非対称リンクは、サービス プロバイダー エッジ スイッチ上のトンネル ポートから、カスタマー スイッチ上の IEEE 802.1Q トランク ポートまでの範囲に設定します。エッジ スイッチにトンネル ポートを入力するパケットは、すでにカスタマー VLAN によって IEEE 802.1Q タグが付けられており、サービス プロバイダー ネットワークで各カスタマーに固有の VLAN ID を含む、別のレイヤの IEEE 802.1Q タグ（メトロ タグと呼ばれる）によってカプセル化されます。この二重タグ付きのパケットは、元のカスタマーの VLAN とその他のカスタマーの VLAN を分離しながら、サービス プロバイダー ネットワークを通過します。アウトバンド インターフェイスとトンネル ポートでは、メトロ タグが削除され、カスタマー ネットワークでの元の VLAN 番号が取得されます。

（注）　トンネル ポートは、IP サービス イメージが稼動しているスイッチでだけサポートされます。

トンネル ポートは、トランク ポートまたはアクセス ポートにはできません。各カスタマーに固有の VLAN に属している必要があります。

トンネル ポートの詳細については、第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

ルーテッド ポート

ルーテッド ポートは物理ポートであり、ルータ上でポートのように機能しますが、ルータに接続する必要はありません。ルーテッド ポートは、アクセス ポートと異なり、特定の VLAN に関連付けられません。ルーテッド ポートは、標準のルータ インターフェイスのように動作しますが、VLAN サブインターフェイスをサポートしない点が異なります。ルーテッド ポートは、レイヤ 3 ルーティング プロトコルを使用して設定できます。ルーテッド ポートはレイヤ 3 インターフェイス限定であるため、DTP および STP などのレイヤ 2 プロトコルをサポートしません。ルーテッド ポートは、IP サービス イメージを稼動するスイッチでだけサポートされます。

no switchport インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスをレイヤ 3 モードにすることで、ルーテッド ポートを設定します。次に、ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、**ip routing** および **router** *protocol* グローバル コンフィギュレーション コマンドを使用して、ルーティング プロトコルの特性を割り当てます。

（注）　**no switchport** インターフェイス コンフィギュレーション コマンドを入力して、インターフェイスをシャットダウンしてから再びイネーブルにすると、インターフェイスの接続先となる装置上でメッセージが生成される場合もあります。レイヤ 2 モードにあるインターフェイスをレイヤ 3 モードにすると、影響を受けるインターフェイスに関連する以前の設定情報が失われる可能性があります。

ユーザが設定可能なルーテッド ポートの数は、ソフトウェアによって制限されません。ただし、ハードウェアの制限によって、この数と、設定されている他の機能の数との関係が、CPU のパフォーマンスに影響を与える場合もあります。ハードウェアのリソースが制限に達したときの動作の詳細については、「レイヤ 3 インターフェイスの設定」（P.14-21）を参照してください。

IP ユニキャストおよび IP マルチキャストのルーティングとルーティング プロトコルの詳細については、第 41 章「IP ユニキャスト ルーティングの設定」および第 49 章「IP マルチキャスト ルーティングの設定」を参照してください。

スイッチ仮想インターフェイス

Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）は、スイッチ ポートの VLAN を、システム上のルーティングまたはブリッジング機能へのインターフェイスとして表します。1 つの VLAN に関連付けることができる SVI は、1 つだけです。VLAN 間でのルーティング、VLAN 間での非ルーティング プロトコルのフォールバック ブリッジング、またはスイッチに対する IP ホスト接続を実現する場合にだけ、1 つの VLAN に 1 つの SVI を設定します。

（注）　SVI は、IP サービス イメージが稼動しているスイッチでだけサポートされます。

デフォルトの VLAN（VLAN 1）がリモート スイッチを管理できるように、デフォルトで SVI が作成されます。追加の SVI を明示的に設定する必要があります。

（注）　インターフェイス VLAN 1 は削除できません。

SVI によって IP ホストはこのシステムだけに接続するようになります。レイヤ 3 モードでは、SVI 全体にルーティングを設定できます。スイッチは、合計 1005 の VLAN（および SVI）をサポートしますが、ハードウェアの制限により、SVI とルーテッド ポートの数と、設定されているその他機能の数との関係が、CPU のパフォーマンスに影響を与える可能性があります。ハードウェアのリソースが制限に達したときの動作の詳細については、「レイヤ 3 インターフェイスの設定」（P.14-21）を参照してください。

SVI は、初めて VLAN インターフェイスに **vlan** インターフェイス コンフィギュレーション コマンドを入力したときに作成されます。この VLAN が対応するのは、カプセル化トランク ポート上のデータフレームに関連付けられた VLAN タグ、またはアクセス ポートに設定された VLAN ID です。トラフィックをルーティングする各 VLAN に VLAN インターフェイスを設定し、それに IP アドレスを割り当てます。詳細については、「手動での IP 情報の割り当て」（P.4-15）を参照してください。

（注）　SVI を作成しても、物理ポートと関連付けられるまで、アクティブにはなりません。

SVI は、ルーティング プロトコルおよびブリッジング設定をサポートします。IP ルーティングの設定については、第 41 章「IP ユニキャスト ルーティングの設定」、第 49 章「IP マルチキャスト ルーティングの設定」、および第 51 章「フォールバック ブリッジングの設定」を参照してください。

SVI 自動ステート除外機能

VLAN 上で複数のポートを含む SVI ライン ステートは、次の条件に一致するとアップ ステートになります。

- スイッチ上の VLAN データベースに VLAN が存在し、アクティブな状態である。
- VLAN インターフェイスが存在し、管理上のダウン状態になっていない。
- レイヤ 2（アクセスまたはトランク）のポートが少なくとも 1 つ存在し、VLAN 上にアップ ステートのリンクが含まれ、VLAN でスパニング ツリー フォワーディング ステートになっている。

（注）　VLAN インターフェイスのプロトコル リンク ステートがアップ状態になるのは、対応する VLAN リンクに属する最初のスイッチポートがアップ状態になって、STP フォワーディング ステートである場合です。

VLAN に複数のポートが含まれる場合のデフォルト動作では、VLAN のすべてのポートがダウンすると SVI もダウンします。SVI 自動ステート除外機能を使用すると、SVI ラインステートのアップおよびダウンの計算に含まれないようにポートを設定できます。たとえば、VLAN で唯一アクティブなポートがモニタリング ポートの場合、そのポートに自動ステート除外機能を設定して、他のポートがすべてダウンすると VLAN もダウンするように指定できます。ポートでイネーブルになると、**自動ステート除外**はそのポートでイネーブルになっているすべての VLAN に適用されます。

VLAN インターフェイスが立ち上がるのは、VLAN の 1 つのレイヤ 2 ポートで収束する時間がある場合です（STP リスニングまたはラーニング ステートから、フォワーディング ステートへ移行する）。これにより、ルーティング プロトコルなどの機能が、まるで十分に動作可能であるかのように VLAN インターフェイスを使用することを防ぎます。また、ルーティング ブラック ホールなどの他の問題が最小限になります。自動ステート除外の設定については、「SVI 自動ステート除外の設定」（P.14-23）を参照してください。

EtherChannel ポート グループ

EtherChannel ポート グループは、複数のスイッチ ポートを 1 つのスイッチ ポートとして処理します。EtherChannel ポート グループは、スイッチ間、またはスイッチおよびサーバ間で高帯域接続を行う単一論理ポートとして動作します。EtherChannel は、トラフィックの負荷をチャネルのリンク全体に分散させます。EtherChannel 内のリンクで障害が発生すると、障害リンク上でそれまで伝送されていたトラフィックは、残りのリンクに変更されます。複数のトランク ポートを 1 つの論理トランク ポートにグループ化したり、複数のアクセス ポートを 1 つの論理アクセス ポートにグループ化したり、複数のトンネル ポートを 1 つの論理トンネル ポートにグループ化したり、複数のルーテッド ポートを 1 つの論理ルーテッド ポートにグループ化したりできます。

ほとんどのプロトコルは、単一ポートまたは集約スイッチ ポートのいずれかで動作し、ポート グループ内の物理ポートを認識しません。DTP、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）は、物理ポート上でしか動作しません。

EtherChannel を設定する場合、ポートチャネル論理インターフェイスを作成し、EtherChannel にインターフェイスを割り当てます。**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスをダイナミックに作成します。このコマンドにより、物理ポートおよび論理ポートが同時にバインドされます。

レイヤ 3 インターフェイスの場合、**interface port-channel** グローバル コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成します。次に、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを手動で EtherChannel に割り当てます。

詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

デュアルパーパス アップリンク ポート

一部のスイッチは、デュアルパーパス アップリンク ポートをサポートします。各アップリンク ポートは、RJ-45 コネクタと Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュール コネクタのデュアル フロントエンドを備えた単一のインターフェイスと見なされます。デュアル フロントエンドは冗長インターフェイスではなく、スイッチはこのペアの一方のコネクタしかアクティブにしません。

デフォルトで、スイッチは最初にリンクがアップされたインターフェイス タイプをダイナミックに選択します。ただし、**media-type** インターフェイス コンフィギュレーション コマンドを使用すると、手動で RJ-45 コネクタまたは SFP モジュール コネクタを選択できます。デュアルパーパス アップリンクの速度とデュプレックスの設定については、「インターフェイス速度とデュプレックス パラメータの設定」（P.14-17）を参照してください。

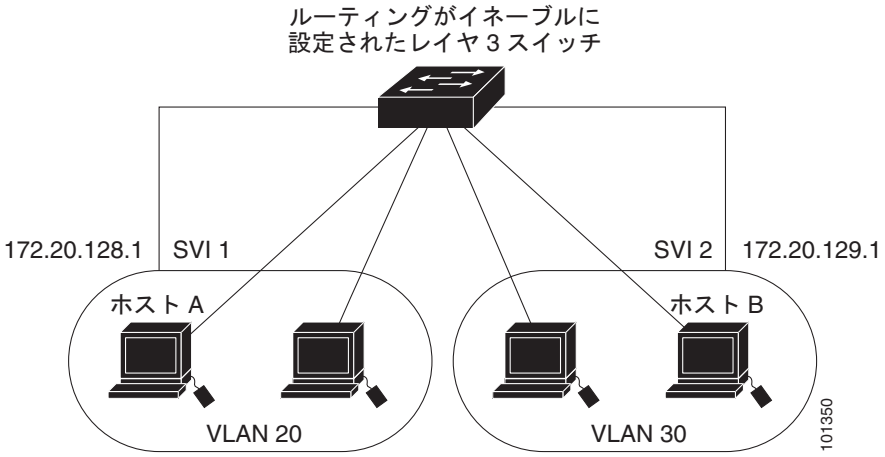
各アップリンク ポートには 2 つの LED があります。1 つは RJ-45 ポートのステータスを示し、もう 1 つは SFP モジュール ポートのステータスを示します。ポート LED は、どのコネクタがアクティブであっても点灯しています。LED の詳細については、ハードウェア インストレーション ガイドを参照してください。

インターフェイスの接続

単一の VLAN 内の装置は、任意のスイッチを介して直接通信できます。異なる VLAN のポートは、ルーティング装置を経由しないとデータを交換できません。

標準レイヤ 2 スイッチを使用する場合、異なる VLAN のポートで情報を交換するにはルータを経由する必要があります。ルーティングがイネーブルになった状態のスイッチを使用して、VLAN 20 および VLAN 30 の両方に IP アドレスが割り当てられた SVI を設定する場合、ホスト A からのパケットを、スイッチ経由でホスト B へ直接送信できます。外部ルータ（図 14-1）を使用する必要はありません。

図 14-1　　レイヤ 3 スイッチと VLAN の接続



IP サービス イメージを使用する場合、スイッチは、インターフェイス間にトラフィックを転送する 2 つの方法として、ルーティングとフォールバック ブリッジングをサポートします。高度なパフォーマンスを維持するため、可能な場合はいつでもスイッチ ハードウェアによる転送が行われます。ただし、Ethernet II のカプセル化を使用する IP Version 4 のパケットだけが、ハードウェアにルーティングされます。非 IP トラフィックおよび他の方法でカプセル化されたトラフィックは、ハードウェアによってフォールバック ブリッジングできます。

- ルーティング機能は、すべての SVI およびルーテッド ポートでイネーブルにできます。スイッチは IP トラフィックだけをルーティングします。IP ルーティング プロトコル パラメータおよびアドレス設定が SVI またはルーテッド ポートに追加されると、これらのポートから受信した IP トラフィックはすべてルーティングされます。詳細については、第 41 章「IP ユニキャスト ルーティングの設定」、第 49 章「IP マルチキャスト ルーティングの設定」、および第 50 章「MSDP の設定」を参照してください。

- フォールバック ブリッジングでは、スイッチがルーティングしなかったトラフィックや、DECnet などの非ルーティング プロトコルに属するトラフィックを転送します。フォールバック ブリッジングは、複数の SVI またはルーテッド ポート間をブリッジすることで、複数の VLAN を 1 つのブリッジ ドメインに接続します。フォールバック ブリッジングを設定する場合、SVI またはルーテッド ポートを、各 SVI が含まれるブリッジ グループ、または 1 つのブリッジ グループにだけ割り当てられたルーテッド ポートに割り当てます。同じグループ内のすべてのインターフェイスは、同じブリッジ ドメインに属します。詳細については、第 51 章「フォールバック ブリッジングの設定」を参照してください。

インターフェイス コンフィギュレーション モードの使用

スイッチは次のインターフェイス タイプをサポートします。

- 物理ポート：スイッチ ポートおよびルーテッド ポート
- VLAN：スイッチ仮想インターフェイス
- ポート チャネル：EtherChannel インターフェイス

また、インターフェイスの範囲を設定できます（「インターフェイスの範囲設定」（P.14-10）を参照）。

物理インターフェイス（ポート）を設定するには、インターフェイス タイプ、モジュール番号、およびスイッチ ポート番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

- *タイプ：ポート タイプはスイッチ上でサポートされるタイプに依存します。可能性のあるタイプは次のとおりです。*10/100 Mbps イーサネット対応のファスト イーサネット（fastethernet または fa）、10/100/1000 Mbps イーサネット ポート対応のギガビット イーサネット（gigabitethernet または gi）、10,000 Mbps 対応の 10 ギガビット イーサネット（tengigabitethernet または te）、または着脱可能小型フォーム ファクタ（SFP）モジュール ギガビット イーサネット インターフェイス。
- モジュール番号：スイッチ上のモジュール番号。モジュール番号（1 ～ 3）は、モジュールがスイッチまたは他のモジュールと接続する方法によって異なります。
  - IE-3000-4TC および IE-3000-8TC スイッチに対応するモジュール番号は 1 です。
  - スイッチに直接接続するモジュールに対応するモジュール番号は 2 です。
  - 別のモジュールに接続するモジュールに対応するモジュール番号は 3 です。
- ポート番号：スイッチ上の物理インターフェイスの番号。ファスト イーサネット ポートでの IE-3000-4TC スイッチ モジュールのポート数は 1 ～ 4 であり、ギガビット イーサネット ポートの場合は 1 ～ 2 です。ファスト イーサネット ポートでの IE-3000-8TC スイッチ モジュールのポート数は 1 ～ 8 であり、ギガビット イーサネット ポートの場合は 1 ～ 2 です。表 14-1 に、スイッチとモジュールの組み合わせおよびインターフェイス番号を示します。

表 14-1　スイッチ インターフェイス番号

スイッチのモデル	モジュール番号	インターフェイスの番号付け方式
IE-3000-4TC スイッチ	1	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2

表 14-1　スイッチ インターフェイス番号 （続き）

IE-3000-8TC スイッチ	1	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ファスト イーサネット 1/5、ファスト イーサネット 1/6、ファスト イーサネット 1/7、ファスト イーサネット 1/8、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2
IEM-3000-8TM 拡張モジュール（スイッチに接続済み）	2	ファスト イーサネット 2/1、ファスト イーサネット 2/2、ファスト イーサネット 2/3、ファスト イーサネット 2/4、ファスト イーサネット 2/5、ファスト イーサネット 2/6、ファスト イーサネット 2/7、およびファスト イーサネット 2/8
IEM-3000-8TM 拡張モジュール（別のモジュールに接続済み）	3	ファスト イーサネット 3/1、ファスト イーサネット 3/2、ファスト イーサネット 3/3、ファスト イーサネット 3/4、ファスト イーサネット 3/5、ファスト イーサネット 3/6、ファスト イーサネット 3/7、およびファスト イーサネット 3/8

スイッチを確認すると、物理インターフェイスを特定できます。また、**show** 特権 EXEC コマンドを使用して、特定のインターフェイスまたはすべてのインターフェイスに関する情報を表示できます。この章の残りの部分では、主に物理インターフェイスの設定手順を示します。

（注）　このマニュアルの設定例および出力例は、特にスタック メンバー番号が存在するかどうかに関して、実際のスイッチと異なる場合があります。

インターフェイスの設定手順

次の一般的な手順は、すべてのインターフェイス設定に適用されます。

ステップ 1　特権 EXEC プロンプトで、**configure terminal** コマンドを入力します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

ステップ 2　**interface** グローバル コンフィギュレーション コマンドを入力します。

インターフェイス タイプとインターフェイス番号を指定します。この例では、ギガビット イーサネット ポート 1 です。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)#
```

（注）　任意で、インターフェイス タイプとインターフェイス番号の間にスペースを入れます。

ステップ 3　各 **interface** コマンドのあとに、インターフェイスに必要なコンフィギュレーション コマンドを指定します。入力するコマンドによって、そのインターフェイス上で実行されるプロトコルとアプリケーションが決まります。別の interface コマンドを入力するか、**end** を入力して特権 EXEC モードに戻ると、コマンドが収集されてインターフェイスに適用されます。

また、**interface range** または **interface range macro** グローバル コンフィギュレーション コマンドを使用して、インターフェイスの範囲を設定することもできます。範囲内に設定されたインターフェイスは同じタイプにし、同じ機能オプションを設定する必要があります。

ステップ 4　インターフェイスの設定後に、「インターフェイスのモニタおよびメンテナンス」（P.14-26）に記載されている **show** 特権 EXEC コマンドを使用して、インターフェイスのステータスを確認します。

スイッチ上またはスイッチに設定された全インターフェイスのリストを参照するには、**show interfaces** 特権 EXEC コマンドを入力します。レポートは、装置がサポートするインターフェイスごと、または特定のインターフェイスに対して出力されます。

インターフェイスの範囲設定

同じ設定パラメータで複数のインターフェイスを設定するには、**interface range** グローバル コンフィギュレーション コマンドを使用します。インターフェイス レンジ コンフィギュレーション モードを開始すると、このモードを終了するまで、入力するすべてのコマンド パラメータがその範囲内の全インターフェイスに適用されます。

同じパラメータでインターフェイスの範囲を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** {*port-range* | **macro** *macro_name*}	設定するインターフェイス（VLAN または物理ポート）の範囲を指定し、インターフェイス レンジ コンフィギュレーション モードを開始します。 • **interface range** コマンドを使用して、ポートの範囲を最大 5 つ設定するか、定義済みのマクロを設定できます。 • **macro** 変数については、「インターフェイス レンジ マクロの設定および使用」（P.14-11）を参照してください。 • カンマ区切りで *port-range* を指定する場合、エントリごとにインターフェイス タイプを入力し、カンマの前後にスペースを入力する必要があります。 • ハイフン区切りで *port-range* を指定する場合、インターフェイス タイプを再入力する必要はありませんが、ハイフンの前にスペースを入力します。
ステップ 3		標準のコンフィギュレーション コマンドを使用して、範囲内のすべてのインターフェイスに設定パラメータを適用します。各コマンドは入力するたびに実行されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** [*interface-id*]	範囲内のインターフェイス設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

interface range グローバル コンフィギュレーション コマンドを使用する場合は、次の注意事項を確認してください。

- *port-range* に有効なエントリは、スイッチ上のポート タイプによって決まります。
  - **vlan** *vlan-ID* - *vlan-ID*（VLAN ID の範囲は 1 ～ 4094）

- module は常に 0
- **fastethernet** module/{first *port*} - {*last port*}（module は常に 0）
- **gigabitethernet** module/{*first port*} - {*last port*}（module は常に 0）
- **port-channel** *port-channel-number - port-channel-number*（*port-channel-number* は 1 ～ 6）

（注）　ポート チャネルで **interface range** コマンドを使用する場合、最初と最後のポートチャネル番号をアクティブなポート チャネルにする必要があります。

- **interface range** コマンドを使用するときは、最初のインターフェイス番号とハイフンの間にスペースを入れる必要があります。

  たとえば、**interface range gigabitethernet1/1 - 2** は有効な範囲指定ですが、**interface range gigabitethernet 1/1-2** は無効です。
- **interface range** コマンドは、**interface vlan** コマンドを使用して設定された VLAN インターフェイスに限定して機能します。**show running-config** 特権 EXEC コマンドは、設定済みの VLAN インターフェイスを表示します。**show running-config** コマンドによって表示されない VLAN インターフェイスは、**interface range** コマンドで使用できません。
- 1 つの範囲内にあるすべてのインターフェイスは同じタイプ（すべてファスト イーサネット ポート、すべてギガビット イーサネット ポート、すべて EtherChannel ポート、またはすべて VLAN）にする必要がありますが、コマンド内に複数の範囲を入力できます。

次に、**interface range** グローバル コンフィギュレーション コマンドを使用して、ポート 1 ～ 2 の速度を 100 Mbps に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 - 2
Switch(config-if-range)# speed 100
```

次に、カンマを使用して異なるインターフェイス タイプ ストリングを範囲に追加し、ファスト イーサネット ポート 1 ～ 3 とギガビット イーサネット ポート 1 と 2 をイネーブルにして、フロー制御のポーズ フレームを受信する例を示します。

```
Switch# configure terminal
Switch(config)# interface range fastethernet1/1 - 3, gigabitethernet1/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

インターフェイス レンジ モードの実行中に複数のコンフィギュレーション コマンドを入力する場合は、入力するたびに各コマンドが実行されます。コマンドはインターフェイス レンジ モードの終了後に一括して実行されるわけではありません。コマンドの実行中にインターフェイス レンジ コンフィギュレーション モードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスに実行されない場合があります。コマンド プロンプトが再表示されるのを確認してから、インターフェイス レンジ コンフィギュレーション モードを終了してください。

インターフェイス レンジ マクロの設定および使用

インターフェイス レンジ マクロを作成し、設定するインターフェイスの範囲を自動的に選択することができます。**macro** キーワードを **interface range macro** グローバル コンフィギュレーション コマンド ストリングで使用するには、**define interface-range** グローバル コンフィギュレーション コマンドを使用してマクロを定義する必要があります。

インターフェイス レンジ マクロを定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**define interface-range** *macro_name interface-range*	インターフェイス レンジ マクロを定義して、NVRAM（不揮発性 RAM）に保存します。 • *macro_name* は最大 32 文字の文字列です。 • 1 つのマクロには、カンマで区切ってインターフェイス範囲を最大 5 つ含めることができます。 • 各 *interface-range* は同じポート タイプで構成されます。
ステップ 3	**interface range macro** *macro_name*	設定するインターフェイス範囲を選択するには、*macro_name* と呼ばれるインターフェイス レンジ マクロに保存された値を使用します。 これで、標準のコンフィギュレーション コマンドを使用して、定義されたマクロ内の全インターフェイスに設定を適用できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config | include define**	定義済みのインターフェイス レンジ マクロの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

マクロを削除するには、**no define interface-range** *macro_name* グローバル コンフィギュレーション コマンドを使用します。

define interface-range グローバル コンフィギュレーション コマンドを使用する場合は、次の注意事項を確認してください。

- *interface-range* に有効なエントリは、スイッチ上のポート タイプによって決まります。
  - **vlan** *vlan-ID* - *vlan-ID*（VLAN ID の範囲は 1 ～ 4094）
  - **fastethernet** module/{first *port*} - {*last port*}（module は常に 0）
  - **gigabitethernet** module/{*first port*} - {*last port*}（module は常に 0）
  - **port-channel** *port-channel-number* - *port-channel-number*（*port-channel-number* は 1 ～ 6）

  （注） ポート チャネルで **interface range** コマンドを使用する場合、最初と最後のポートチャネル番号をアクティブなポート チャネルにする必要があります。

- *interface-range* を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れる必要があります。

  たとえば、**gigabitethernet1/1 - 2** は有効な範囲指定ですが、**gigabitethernet 1/1-2** は無効です。
- VLAN インターフェイスは、**interface vlan** コマンドを使用して設定する必要があります。**show running-config** 特権 EXEC コマンドは、設定済みの VLAN インターフェイスを表示します。**show running-config** コマンドによって表示されない VLAN インターフェイスは、*interface-range* として使用できません。
- 1 つの範囲内にあるすべてのインターフェイスは同じタイプ（すべてファスト イーサネット ポート、すべてギガビット イーサネット ポート、すべて EtherChannel ポート、またはすべて VLAN）にする必要がありますが、マクロ内で複数のインターフェイス タイプを組み合わせることができます。

次に、*enet_list* という名前のインターフェイス範囲を定義してポート 1 と 2 に含め、マクロ設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet1/1 - 2
Switch(config)# end
Switch# show running-config | include define
Switch# define interface-range enet_list gigabitethernet1/1 - 2
```

次に、*macro1* という名前で、複数のインターフェイス マクロを作成する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range macro1 fastethernet1/1 - 2, gigabitethernet1/1 - 2
Switch(config)# end
```

次に、インターフェイス レンジ マクロ *enet_list* でインターフェイス レンジ コンフィギュレーション モードを開始する例を示します。

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

次に、インターフェイス レンジ マクロ *enet_list* を削除し、削除されたことを確認する例を示します。

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

イーサネット インターフェイスの設定

ここでは、次の設定情報について説明します。

イーサネット インターフェイスのデフォルト設定

表 14-2 に、イーサネット インターフェイスのデフォルト設定を示します。表に記載されている VLAN パラメータの詳細については、第 16 章「VLAN の設定」を参照してください。ポートへのトラフィック制御の詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。

（注）　レイヤ 2 パラメータを設定するには、インターフェイスがレイヤ 3 モードである場合は、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。この操作で、インターフェイスをシャットダウンしてから再びイネーブルにすると、インターフェイスの接続先である装置上にメッセージが生成される場合があります。レイヤ 3 モードにあるインターフェイスをレイヤ 2 モードにすると、影響を受けるインターフェイスに関連する以前の設定情報が失われる可能性があり、インターフェイスはデフォルト設定に戻ります。

表 14-2　レイヤ 2 イーサネット インターフェイスのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ 2 またはスイッチング モード（**switchport** コマンド）。
VLAN 許容範囲	VLAN 1 ～ 4094。
デフォルトの VLAN（アクセス ポート用）	VLAN 1（レイヤ 2 インターフェイス限定）。
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1（レイヤ 2 インターフェイス限定）。
VLAN トランキング	スイッチポート モード dynamic auto（DTP をサポート）（レイヤ 2 インターフェイス限定）。
ポート イネーブル ステート	すべてのポートがイネーブル。
ポートの説明	定義なし。
速度	自動ネゴシエーション。
デュプレックス モード	自動ネゴシエーション。
フロー制御	フロー制御は **receive off** に設定されます。送信パケットは常に off になります。
EtherChannel（PAgP）	すべてのイーサネット ポート上でディセーブル。第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
ポート ブロッキング（不明なマルチキャスト トラフィックおよび不明なユニキャスト トラフィック）	ディセーブル（非ブロック）（レイヤ 2 インターフェイス限定）。「ポート ブロッキングの設定」（P.29-7）を参照してください。
ブロードキャスト、マルチキャスト、およびユニキャストのストーム制御	ディセーブル。「ストーム制御のデフォルト設定」（P.29-3）を参照してください。
保護ポート	ディセーブル（レイヤ 2 インターフェイス限定）。「保護ポートの設定」（P.29-6）を参照してください。
ポート セキュリティ	ディセーブル（レイヤ 2 インターフェイス限定）。「ポート セキュリティのデフォルト設定」（P.29-11）を参照してください。
PortFast	ディセーブル。「オプションのスパニング ツリーのデフォルト設定」（P.23-9）を参照してください。
Auto-MDIX	イネーブル。 **（注）** 受電装置がクロス ケーブルを経由してスイッチに接続している場合、スイッチは、Cisco IP Phone などの先行標準の受電装置や、IEEE 802.3af をフル サポートしていないアクセス ポイントをサポートしない場合があります。これは、スイッチ ポート上で Auto-MDIX がイネーブルになっているかどうかに関係しません。
キープアライブ メッセージ	SFP モジュール ポート上ではディセーブルですが、その他すべてのポート上ではイネーブルです。

デュアルパーパス アップリンク ポート タイプの設定

（注）　デュアルパーパス アップリンク ポートを備えているのは、Catalyst 2960 スイッチだけです。

一部のスイッチは、デュアルパーパス アップリンク ポートをサポートします。デフォルトで、スイッチは最初にリンクがアップされたインターフェイス タイプをダイナミックに選択します。ただし、**media-type** インターフェイス コンフィギュレーション コマンドを使用すると、手動で RJ-45 コネクタまたは SFP モジュール コネクタを選択できます。詳細については、「デュアルパーパス アップリンク ポート」（P.14-6）を参照してください。

デュアルパーパス アップリンクを選択し、速度とデュプレックスを設定できるようにアクティブにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するデュアルパーパス アップリンク ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**media-type** {**auto-select** | **rj45** | **sfp**}	デュアルパーパス アップリンク ポートのインターフェイスとタイプを選択します。キーワードの意味は次のとおりです。 • **auto-select**：スイッチはタイプをダイナミックに選択します。リンクの確立が完了すると、スイッチはアクティブ リンクが終了するまでの間、もう一方のタイプをディセーブルにします。アクティブ リンクが終了すると、スイッチはいずれかのリンクが確立されるまでの間、両方のタイプをイネーブルにします。auto-select モードでは、スイッチはいずれのタイプも速度とデュプレックスの自動ネゴシエーションに基づいて設定します（デフォルト）。インストールされた SFP モジュールのタイプによっては、スイッチがタイプをダイナミックに選択できない場合もあります。詳細については、この手順の最後の情報を参照してください。 • **rj45**：スイッチは SFP モジュール インターフェイスをディセーブルにします。SFP モジュールをこのポートに接続すると、RJ-45 側でリンクがダウンしていたり、接続していない場合でも、リンクは確立できません。このモードでは、デュアルパーパス ポートは 10/100/1000BASE-TX インターフェイスと同様に動作します。このインターフェイス タイプに合った速度とデュプレックスが設定できます。 • **sfp**：スイッチは RJ-45 インターフェイスをディセーブルにします。RJ-45 ポートにケーブルを接続すると、SFP モジュール側がダウンしている場合や、SFP モジュールが存在しない場合でも、リンクは確立できません。搭載された SFP モジュール タイプに応じて、このインターフェイス タイプに合った速度とデュプレックスが設定できます。 速度とデュプレックスの設定の詳細については、「速度およびデュプレックス設定時の注意事項」（P.14-17）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show interfaces** *interface-id* **transceiver properties**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**media-type auto interface** または **no media-type** インターフェイス コンフィギュレーション コマンドを使用します。

速度とデュプレックス（デフォルト）を自動ネゴシエートするには、スイッチによって両方のタイプを設定します。**auto-select** を設定した場合、**speed** および **duplex** インターフェイス コンフィギュレーション コマンドは設定できません。

スイッチの電源投入時、または **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドでデュアルパーパス アップリンク ポートをイネーブルにした場合は、SFP モジュール インターフェイスが優先されます。それ以外の場合は、最初にリンクが確立されたタイプがスイッチによって選択されます。

このスイッチと 100BASE-*x*（-*x* は -BX、-FX、-FE、-LX のいずれか）SFP モジュールを併用すると、次のように動作します。

- 100BASE -*x* SFP モジュールがモジュール スロットに挿入され、RJ-45 側にリンクが存在しない場合には、スイッチは RJ-45 インターフェイスをディセーブルにして SFP モジュール インターフェイスを選択します。SFP モジュール側にケーブルが接続されておらず、リンクが存在しない場合でも、このような動作になります。
- 100BASE-*x* SFP モジュールが挿入されており、RJ-45 側にリンクが存在する場合には、スイッチはそのリンクを使用します。リンクがダウンすると、スイッチは RJ-45 側をディセーブルにし、SFP モジュール インターフェイスを選択します。
- 100BASE-*x* SFP モジュールが取り外されると、スイッチは再度タイプをダイナミックに選択（**auto-select**）し、RJ-45 側を再度イネーブルにします。

スイッチは 100BASE-FX-GE SFP モジュールに対しては、このような動作はしません。

インターフェイス速度およびデュプレックス モードの設定

サポートするポート タイプによっては、スイッチ上のイーサネット インターフェイスは 10、100、1000 Mbps、または 10,000 Mbps の速度で動作し、半二重モードまたは全二重モードのいずれかになります。全二重モードでは、2 つのステーション間でトラフィックの送受信を同時に行うことができます。通常、10 Mbps のポートは半二重モードで動作します。つまり、ステーションはトラフィックの送信または受信のいずれか一方を行います。

スイッチ モデルには、次の組み合わせを含めることができます。ファスト イーサネット（10/100 Mbps）ポート、ギガビット イーサネット（10/100/1000 Mbps）ポート、10 ギガビット モジュール ポート、および着脱可能小型フォーム ファクタ（SFP）モジュールをサポートする SFP モジュール スロット。

ここでは、インターフェイス速度およびデュプレックス モードの設定手順について説明します。

- 「速度およびデュプレックス設定時の注意事項」（P.14-17）
- 「インターフェイス速度とデュプレックス パラメータの設定」（P.14-17）

速度およびデュプレックス設定時の注意事項

インターフェイス速度とデュプレックス モードを設定する際は、次の注意事項を確認してください。

- ファスト イーサネット（10/100 Mbps）ポートは、すべての速度とデュプレックス オプションをサポートします。
- ギガビット イーサネット（10/100/1000 Mbps）ポートは、すべての速度とデュプレックス オプション（自動、半二重、全二重）をサポートします。ただし、1000 Mbps で動作するギガビット イーサネット ポートは、半二重モードをサポートしません。
- SFP モジュール ポートの場合、速度とデュプレックス CLI オプションは、SFP モジュールのタイプによって変化します。
  - 1000BASE-*x*（-*x* は -BX、-CWDM、-LX、-SX、および -ZX）SFP モジュール ポートは、**speed** インターフェイス コンフィギュレーション コマンドにある **nonegotiate** キーワードをサポートします。デュプレックス オプションはサポートされません。
  - 1000BASE-T SFP モジュール ポートは、10/100/1000 Mbps ポートと同じ速度とデュプレックス オプションをサポートします。
  - 100BASE-*x*（-*x* は -BX、-CWDM、-LX、-SX、および -ZX）SFP モジュール ポートは、100 Mbps しかサポートしません。これらのモジュールは、全二重および半二重のデュプレックス オプションをサポートしますが、自動ネゴシエーションはサポートしません。

  ご使用のスイッチでサポートされている SFP モジュールについては、製品のリリース ノートを参照してください。
- ラインの両端が自動ネゴシエーションをサポートしている場合、デフォルトの **auto** ネゴシエーション設定を使用することを推奨します。
- 片方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定しても、サポートしている側で **auto** 設定を使用しないでください。
- STP がイネーブルになっていてポートが再設定されている場合、スイッチはループを確認するために最大 30 秒かけることができます。ポート LED は、STP の再設定中にオレンジになります。

注意　インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再度イネーブルになる場合があります。

インターフェイス速度とデュプレックス パラメータの設定

物理インターフェイスに速度とデュプレックス モードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**speed** {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}	インターフェイスに適切な速度パラメータを入力します。 • **10**、**100**、または **1000** を入力し、インターフェイスに特定の速度を設定します。**1000** キーワードは、10/100/1000 Mbps のポートだけに利用可能です。 • **auto** を入力してインターフェイスをイネーブルにし、接続先装置と速度を自動ネゴシエートします。**10**、**100**、または **1000** キーワードと **auto** キーワードを併用する場合、ポートは指定した速度に限定して自動ネゴシエートします。 • **nonegotiate** キーワードは、SFP モジュール ポートだけに利用可能です。SFP モジュール ポートは 1000 Mbps に限定して動作するため、接続先の装置が自動ネゴシエーションをサポートしない場合は、ネゴシエーションを設定できません。 速度設定の詳細については、「速度およびデュプレックス設定時の注意事項」（P.14-17）を参照してください。
ステップ 4	**duplex** {**auto** | **full** | **half**}	インターフェイスにデュプレックス パラメータを入力します。 半二重モードをイネーブルにします（10 Mbps または 100 Mbps に限定して動作するインターフェイス用）。1000 Mbps で動作するインターフェイスには、半二重モードを設定できません。 デュプレックス設定の詳細については、「速度およびデュプレックス設定時の注意事項」（P.14-17）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id*	インターフェイスの速度およびデュプレックス モードの設定を表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

no speed および **no duplex** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスをデフォルトの速度とデュプレックスの設定に戻します（自動ネゴシエーション）。すべてのインターフェイスをデフォルト設定に戻すには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス速度を 10 Mbps に設定し、デュプレックス モードを 10/100 Mbps ポート上で半二重モードに設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fasttethernet1/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

次に、10/100/1000 Mbps ポート上でインターフェイス速度を 100 Mbps に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/2
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# speed 100
```

IEEE 802.3x フロー制御の設定

フロー制御によって、接続されたイーサネット ポートをイネーブルにし、輻輳したノードの一端でリンクの動作を休止させることで、輻輳中のトラフィック レートを制御します。一方のポートが輻輳しており、それ以上のトラフィックを受信できない場合、その状態がクリアされるまで送信を停止するために、ポーズ フレームを送信してもう片方のポートに通知します。ポーズ フレームを受信すると、送信元の装置がデータ パケットの送信を停止するため、輻輳期間中にデータ パケットが失われるのを防ぎます。

（注）　スイッチ上のポートはポーズ フレームを受信できますが、送信はできません。

flowcontrol インターフェイス コンフィギュレーション コマンドを使用して、ポーズ フレームを**受信**するインターフェイスの機能を、**on**、**off**、または **desired** に設定できます。デフォルトのステートは **off** です。

ステートが **desired** に設定された場合、フロー制御パケットを送信する必要がある接続装置、またはフロー制御パケットを送信する必要はないが送信可能な接続装置を、インターフェイスとともに動作できます。

次のルールは、装置上のフロー制御設定に適用されます。

- **receive on**（または **desired**）：ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要のある接続装置、またはポーズ フレームを送信可能な接続装置とともに動作できます。ポートはポーズ フレームを受信できます。
- **receive off**：フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置もポーズ フレームの送受信を行いません。

（注）　コマンド設定と、その結果となるローカル ポートとリモート ポートでのフロー制御解決の詳細については、このリリースのコマンド リファレンスの **flowcontrol** インターフェイス コンフィギュレーション コマンドを参照してください。

インターフェイス上でフロー制御を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**flowcontrol** {**receive**} {**on** | **off** | **desired**}	フロー制御モードをポートに設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id*	インターフェイスのフロー制御設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フロー制御をディセーブルにするには、**flowcontrol receive off** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートでフロー制御を有効にする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)# end
```

インターフェイスでの Auto-MDIX の設定

Automatic Medium-Dependent Interface Crossover（Auto-MDIX）がインターフェイス上でイネーブルな場合、インターフェイスは必要なケーブルの接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定します。Auto-MDIX 機能を使用せずにスイッチを接続する場合、サーバ、ワークステーション、またはルータなどの装置に接続するにはストレート ケーブルを使用し、その他のスイッチまたはリピータに接続するにはクロス ケーブルを使用します。Auto-MDIX がイネーブルの場合、いずれかのタイプのケーブルを使用してその他の装置に接続すると、インターフェイスによって不適切なケーブル接続が自動的に修正されます。ケーブル接続要件の詳細については、ハードウェア インストレーション ガイドを参照してください。

Auto-MDIX はデフォルトでイネーブルになっています。Auto MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイス速度とデュプレックスも **auto** に設定する必要があります。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mbps インターフェイスでサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

表 14-3 に、Auto-MDIX の設定と適切および不適切なケーブル接続の結果によるリンク ステートを示します。

表 14-3　リンク条件と Auto-MDIX 設定

ローカル側の Auto-MDIX	リモート側の Auto-MDIX	適切なケーブル接続	不適切なケーブル接続
点灯	点灯	リンクアップ	リンクアップ
点灯	消灯	リンクアップ	リンクアップ
消灯	点灯	リンクアップ	リンクアップ
消灯	消灯	リンクアップ	リンクダウン

インターフェイス上に Auto-MDIX を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**speed auto**	インターフェイスが接続先装置と速度を自動ネゴシエートするように設定します。
ステップ 4	**duplex auto**	インターフェイスが接続先装置とデュプレックス モードを自動ネゴシエートするように設定します。
ステップ 5	**mdix auto**	インターフェイス上で Auto-MDIX をイネーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show controllers ethernet-controller** *interface-id* **phy**	インターフェイス上の Auto-MDIX 機能の動作ステートを確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

Auto-MDIX をディセーブルにするには、**no mdix auto** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
```

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

インターフェイスに関する説明の追加

インターフェイスの機能をわかりやすくするため、インターフェイスに関する説明を追加できます。説明は、**show configuration**、**show running-config**、および **show interfaces** 特権 EXEC コマンドの出力に表示されます。

インターフェイスに関する説明を追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	説明を追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**description** *string*	インターフェイスに関する説明（最大 240 文字）を追加します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **description** または **show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

説明を削除するには、**no description** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上に説明を追加し、説明を確認する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/2 description
Interface Status         .Protocol Description
Gi1/2   admin down     down     Connects to Marketing
```

レイヤ 3 インターフェイスの設定

スイッチは、次のタイプのレイヤ 3 インターフェイスをサポートします。

- SVI：トラフィックをルーティングするすべての VLAN に SVI を設定する必要があります。**interface vlan** グローバル コンフィギュレーション コマンドのあとに VLAN ID を入力すると、SVI が作成されます。SVI を削除するには、**no interface vlan** グローバル コンフィギュレーション コマンドを使用します。インターフェイス VLAN 1 は削除できません。

（注）　物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。レイヤ 2 ポートを VLAN に割り当てる方法の詳細については、第 16 章「VLAN の設定」を参照してください。

SVI を設定する場合、SVI 自動ステート除外を SVI のポートに設定すると、そのポートが SVI ラインステート ステータスの判断に含まれないようにすることができます。「SVI 自動ステート除外の設定」（P.14-23）を参照してください。

- ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドの使用してレイヤ 3 モードに設定された物理ポートです。
- レイヤ 3 EtherChannel ポート：EtherChannel インターフェイスは、ルーテッド ポートで構成されます。

  EtherChannel ポートのインターフェイスについては、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

レイヤ 3 スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。

1 つのスイッチに設定可能な SVI とルーテッド ポートの数は制限が定義されていません。ただし、ハードウェアの制限により、SVI とルーテッド ポートの数と、設定されている他の機能の数との関係が、CPU 使用率に影響を与える可能性があります。スイッチがハードウェア リソースを最大限に使用している場合、ルーテッド ポートまたは SVI の作成を試行すると次のような結果になります。

- 新しいルーテッド ポートを作成する場合、インターフェイスをルーテッド ポートに変換するリソースが十分でないというメッセージがスイッチによって生成され、インターフェイスはスイッチ ポートのままになります。
- 拡張範囲 VLAN の作成を試行すると、エラー メッセージが生成されて拡張範囲 VLAN は拒否されます。
- VLAN トランキング プロトコル（VTP）によって、スイッチに新しい VLAN の生成が通知されると、スイッチは、利用可能なハードウェア リソースが不足しているというメッセージを送信し、VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力には、VLAN が中断ステートになっていることが示されます。
- ハードウェアがサポート可能な VLAN とルーテッド ポートを超える設定でスイッチの起動を試行すると、VLAN は作成されますが、ルーテッド ポートがシャットダウンされます。この原因はハードウェア リソースの不足であるというメッセージが、スイッチから送信されます。

すべてのレイヤ 3 インターフェイスは、トラフィックをルーティングするための IP アドレスを必要とします。この手順では、インターフェイスをレイヤ 3 インターフェイスとして設定し、インターフェイスに IP アドレスを割り当てる方法を示します。

（注） 物理ポートがレイヤ 2 モード（デフォルト）である場合、**no switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 3 モードにする必要があります。**no switchport** コマンドを入力してインターフェイスをディセーブルにしてから再びイネーブルにすると、接続先となる装置上でメッセージが生成される場合があります。また、レイヤ 2 モードにあるインターフェイスをレイヤ 3 モードにすると、影響を受けるインターフェイスに関連する以前の設定情報が失われる可能性があり、インターフェイスがデフォルト設定に戻ります。

レイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** {{**fastethernet** | **gigabitethernet**} *interface-id*} | {**vlan** *vlan-id*} | {**port-channel** *port-channel-number*}	レイヤ 3 インターフェイスとして設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport**	物理ポートだけの場合は、レイヤ 3 モードを入力します。

	コマンド	目的
ステップ 4	**ip address** *ip_address subnet_mask*	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**no shutdown**	インターフェイスをイネーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **show ip interface** [*interface-id*] **show running-config interface** [*interface-id*]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスから IP アドレスを削除するには、**no ip address** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをルーテッド ポートとして設定し、ポートに IP アドレスを割り当てる例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
Switch(config-if)# no shutdown
```

SVI 自動ステート除外の設定

SVI 自動ステート除外を SVI のアクセス ポートまたはトランク ポートに設定すると、同じ VLAN に属していても、SVI のステータス（ライン ステートのアップまたはダウン）の計算にそのポートが含まれなくなります。除外されたポートがアップ ステートであり、VLAN 内の他のポートがすべてダウン ステートである場合、SVI ステートはダウンに変更されます。

VLAN では少なくとも 1 つのポートをアップにする必要があるため、SVI ライン ステートのアップの維持は除外されません。このコマンドを使用して、SVI のステータスを判断する際に、モニタリング ポートのステータスを除外できます。

SVI ステート変更の計算からポートを除外するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レイヤ 2 インターフェイス（物理ポートまたはポート チャネル）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport autostate exclude**	SVI ライン ステート（アップまたはダウン）のステータスを定義する際に、アクセス ポートまたはトランク ポートを除外します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running config interface** *interface-id* **show interface** *interface-id* **switchport**	（任意）実行コンフィギュレーションを表示します。 設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ステータスの計算に含まれないように SVI 内にアクセス ポートまたはトランク ポートを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport autostate exclude
Switch(config-if)# exit
```

システム最大伝送ユニット（MTU）の設定

フレームを受信して全インターフェイス上に伝送するための Maximum Transmission Unit（MTU; 最大伝送ユニット）のデフォルト サイズは、1500 バイトです。10 Mbps または 100 Mbps で稼動するすべてのインターフェイス用に MTU サイズを増加させるには、**system mtu** グローバル コンフィギュレーション コマンドを使用します。MTU サイズを増加させてすべてのギガビット イーサネット インターフェイス上でジャンボ フレームをサポートするには、**system mtu jumbo** グローバル コンフィギュレーション コマンドを使用します。

ルーテッド ポート用に MTU サイズを変更するには、**system mtu routing** グローバル コンフィギュレーション コマンドを使用します。

（注）　システム MTU サイズを超えるルーティング MTU サイズは設定できません。システム MTU サイズを現在設定されているルーティング MTU サイズより小さい値に変更すると、設定変更は受け入れられますが、次にスイッチをリセットするまで適用されません。設定変更が有効になると、ルーティング MTU サイズは自動的に新しいシステム MTU サイズのデフォルトになります。

ギガビット イーサネット ポートは **system mtu** コマンドの影響を受けず、10/100 ポートは **system mtu jumbo** コマンドの影響を受けません。**system mtu jumbo** コマンドを設定しない場合、**system mtu** コマンドの設定がすべてのギガビット イーサネット インターフェイスに適用されます。

MTU サイズは個別のインターフェイスに設定できないため、10/100 インターフェイスのすべて、またはギガビット イーサネット インターフェイスのすべてに設定します。システム MTU またはジャンボ MUT のサイズを変更する場合、新しい設定内容を反映させるには、スイッチをリセットする必要があります。**system mtu routing** コマンドの場合、変更内容を反映させるためにスイッチをリセットする必要はありません。

スイッチ CPU が受信可能なフレーム サイズは 1998 バイトに制限されます。これは、**system mtu** または **system mtu jumbo** コマンドによって入力された値に関係しません。通常、転送またはルーティングされるフレームは CPU で受信されませんが、制御トラフィック、SNMP、Telnet、またはルーティング プロトコルへ送信されるトラフィックなど、パケットが CPU へ送信される場合もあります。

ルーテッド パケットは、出力ポートで MTU のチェックを受けます。ルーテッド ポートに使用される MTU 値は、適用済みの **system mtu** 値（**system mtu jumbo** 値ではない）から派生します。つまり、ルーテッド MTU 値が、すべての VLAN に対応するシステム MTU 値より大きくなることはありません。ルーティング プロトコルは、隣接やリンクの MTU をネゴシエートする場合は、システム MTU 値を使用します。たとえば、ピア ルータとの隣接を設定するには、Open Shortest Path First（OSPF）プロトコルにこの MTU 値が使用されます。特定の VLAN に対応するルーテッド パケットの MTU 値を表示するには、**show platform port-asic mvid** 特権 EXEC コマンドを使用します。

（注）　レイヤ 2 ギガビット イーサネット インターフェイスを設定して 10/100 インターフェイスより大きいフレームを受け入れる場合は、レイヤ 2 ギガビット イーサネット インターフェイスで受信し、レイヤ 2 の 10/100 インターフェイスで送信されたジャンボ フレームが廃棄されます。

すべての 10/100 またはギガビット イーサネット インターフェイスに対応する MTU サイズを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**system mtu** *bytes*	（任意）10 Mbps または 100 Mbps で動作するスイッチ上のすべてのインターフェイスに対する MTU サイズを変更します。 指定できる範囲は 1500 ～ 1998 バイトです。デフォルトは 1500 バイトです。
ステップ 3	**system mtu jumbo** *bytes*	（任意）スイッチ上のすべてのギガビット イーサネット インターフェイスに対応する MTU サイズを変更します。 指定できる範囲は 1500 ～ 9000 バイトです。デフォルトは 1500 バイトです。
ステップ 4	**system mtu routing** *bytes*	（任意）ルーテッド ポートのシステム MTU サイズを変更します。指定できる範囲は 1500 ～システム MTU 値です。システム MTU 値は、すべてのポートにルーティングできる最大 MTU です。 より大きいパケットも受け入れられますが、ルーティングはできません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	設定をコンフィギュレーション ファイルに保存します。
ステップ 7	**reload**	オペレーティング システムをリロードします。

特定のインターフェイス タイプに許容範囲外の値を入力すると、値が拒否されます。

スイッチがリロードされると、**show system mtu** 特権 EXEC コマンドを入力して、設定を確認できます。

次に、ギガビット イーサネット ポートの最大パケット サイズを 1800 バイトに設定する例を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

次に、ギガビット イーサネット インターフェイスに範囲外の数値を設定しようとした場合の応答の例を示します。

```
Switch(config)# system mtu jumbo 25000
                                 ^
% Invalid input detected at '^' marker.
```

インターフェイスのモニタおよびメンテナンス

ここでは、インターフェイスのモニタおよびメンテナンスの情報について説明します。

インターフェイス ステータスのモニタ

特権 EXEC プロンプトに入力したコマンドによって、ソフトウェアとハードウェアのバージョン、設定、インターフェイスの統計情報など、インターフェイスに関する情報が表示されます。表 14-4 に、インターフェイス モニタ コマンドの一部を示します（**show** コマンドの全リストは、特権 EXEC プロンプトで **show ?** コマンドを使用して表示できます）。これらのコマンドの詳細な説明については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Interface Command Reference, Release 12.2*』を参照してください。

表 14-4　インターフェイスの show コマンド

コマンド	目的
show interfaces [*interface-id*]	（任意）すべてのインターフェイスまたは特定のインターフェイスについて、ステータスと設定を表示します。
show interfaces *interface-id* **status** [**err-disabled**]	（任意）インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。
show interfaces [*interface-id*] **switchport**	（任意）スイッチング ポートの管理ステータスおよび動作ステータスを表示します。このコマンドを使用して、ポートがルーティング モードまたはスイッチング モードにあるかどうかを確認できます。
show interfaces [*interface-id*] **description**	（任意）1 つのインターフェイスまたはすべてのインターフェイスに設定された説明とインターフェイス ステータスを表示します。
show ip interface [*interface-id*]	（任意）IP ルーティングに設定されたすべてのインターフェイスまたは特定のインターフェイスのユーザビリティ ステータスを表示します。
show interface [*interface-id*] **stats**	（任意）インターフェイスのスイッチング パスによる入出力パケットを表示します。
show interfaces transceiver properties	（任意）インターフェイスの速度とデュプレックスの設定を表示します。
show interfaces transceiver detail	（任意）インターフェイス上の温度、電圧、または電流量を表示します。
show interfaces [*interface-id*] [{**transceiver properties** | **detail**}] *module number*]	SFP モジュールに関する物理ステータスと動作ステータスを表示します。
show running-config interface [*interface-id*]	インターフェイスに対応する RAM の実行コンフィギュレーションを表示します。
show version	ハードウェア設定、ソフトウェアのバージョン、コンフィギュレーション ファイル名と送信元、およびブート イメージを表示します。
show controllers ethernet-controller *interface-id* **phy**	インターフェイス上の Auto-MDIX 機能の動作ステートを表示します。

インターフェイスとカウンタのクリアとリセット

表 14-5 に示す特権 EXEC モードの **clear** コマンドを使用してカウンタをクリアし、インターフェイスをリセットできます。

表 14-5　インターフェイスの clear コマンド

コマンド	目的
clear counters [*interface-id*]	インターフェイス カウンタをクリアします。
clear interface *interface-id*	インターフェイスのハードウェア論理をリセットします。
clear line [*number* | **console 0** | **vty** *number*]	非同期シリアル ラインのハードウェア論理をリセットします。

show interfaces 特権 EXEC コマンドで表示されたインターフェイス カウンタをクリアするには、**clear counters** 特権 EXEC コマンドを使用します。**clear counters** コマンドを使用すると、インターフェイスから現在のインターフェイス カウンタをすべてクリアします。ただし、オプションの引数を指定して、特定のインターフェイス番号から特定のインターフェイス タイプだけをクリアする場合は例外となります。

（注）　**clear counters** 特権 EXEC コマンドでは、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して取得したカウンタをクリアしませんが、これらのカウンタが認識されるのは、**show interface** 特権 EXEC コマンドを使用する場合だけです。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定したインターフェイス上の全機能がディセーブルになり、そのインターフェイスはすべてのモニタ コマンド表示で使用不能に指定されます。この情報は、あらゆるダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。そのインターフェイスは、すべてのルーティング アップデートにも含まれなくなります。

インターフェイスをシャットダウンするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** {**vlan** *vlan-id*} | {{**fastethernet** | **gigabitethernet**} *interface-id*} | {**port-channel** *port-channel-number*}	設定するインターフェイスを選択します。
ステップ 3	**shutdown**	インターフェイスをシャットダウンします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。

CHAPTER 15

SmartPort マクロの設定

IE 3000 スイッチのコマンド リファレンスに、コマンドの構文と使用方法の情報があります。

SmartPort マクロの概要

SmartPort マクロを使用すると、共通の設定を簡単に保存および共有できます。SmartPort マクロを使用して、ネットワーク内のスイッチの場所に基づいて機能や設定をイネーブルにしたり、ネットワーク上で大規模な設定の配置を行うことができます。

各 SmartPort マクロは、定義する一連の CLI コマンドです。SmartPort マクロには、新しい CLI コマンドは含まれていません。SmartPort マクロは、単なる既存の CLI コマンドのグループです。

SmartPort マクロをインターフェイスに適用すると、マクロ内の CLI コマンドがインターフェイスに設定されます。マクロがインターフェイスに適用された場合、既存のインターフェイス設定は失われません。新しいコマンドはインターフェイスに追加され、実行コンフィギュレーション ファイルに保存されます。

SmartPort マクロの設定

SmartPort のデフォルト設定

スイッチで SmartPort マクロはイネーブルになっていません。

表 15-1　デフォルト SmartPort マクロ

マクロ名[1]	説明
cisco-ie-global	このグローバル コンフィギュレーション マクロを使用して、スイッチの設定を工業用イーサネットの環境に合わせてスイッチの設定を行います。このマクロは、Express Setup を使用してスイッチを初期設定するときに自動的に適用されます。 （注）　**cisco-ethernetip** マクロが適切に動作するために、まず **cisco-ie-global** マクロを適用する必要があります。
cisco-ie-desktop	このインターフェイス コンフィギュレーション マクロを使用して、PC などのデスクトップ装置をスイッチ ポートに接続しているときのネットワーク セキュリティと信頼性を高めます。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-phone	このインターフェイス コンフィギュレーション マクロは、Cisco IP Phone を使用している PC などのデスクトップ装置をスイッチ ポートに接続している場合に使用します。このマクロは、**cisco-ie-desktop** マクロの拡張で、同じセキュリティと復元力機能を備えていますが、遅延に影響されやすい音声トラフィックを正しく処理できるように専用の音声 VLAN が追加されています。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-switch	このインターフェイス コンフィギュレーション マクロは、アクセス スイッチとディストリビューション スイッチを接続している場合や、Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュールを使用して接続されているアクセス スイッチ間で接続している場合に使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-router	このインターフェイス コンフィギュレーション マクロは、スイッチと WAN ルータを接続しているときに使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-wireless	このインターフェイス コンフィギュレーション マクロは、スイッチとワイヤレス アクセス ポイントを接続しているときに使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ethernetip	このインターフェイス コンフィギュレーション マクロは、スイッチを EtherNet IP 装置に接続しているときに使用します。 （注）　**cisco-ethernetip** マクロが適切に動作するために、まず **cisco-ie-global** マクロを適用する必要があります。

1. シスコ デフォルト SmartPort マクロは、スイッチで実行されているソフトウェア バージョンによって異なります。

SmartPort 設定時の注意事項

- マクロがスイッチまたはスイッチ インターフェイスにグローバルに適用されている場合、インターフェイス上の既存のすべての設定が保持されます。これは、設定の差分を適用する場合に役立ちます。
- 構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドを適用します。**macro global trace** *macro-name* グローバル コンフィギュレーション コマンドまたは **macro trace** *macro-name* インターフェイス コンフィギュレーション コマンドを使用して、構文または設定エラーを判別するためにマクロを適用およびデバッグできます。
- 一部の CLI コマンドは、特定のインターフェイス タイプに固有です。設定を受け入れないインターフェイスにマクロを適用すると、マクロが構文または設定のチェックに失敗し、スイッチはエラー メッセージを返します。
- マクロをインターフェイスの範囲に適用することは、マクロを単一のインターフェイスに適用することと同じです。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。あるインターフェイスでマクロ コマンドが失敗した場合、残りのインターフェイスに適用されていきます。

- マクロをスイッチまたはスイッチ インターフェイスに適用する場合、マクロ名が自動的にスイッチまたはインターフェイスに追加されます。**show running-config** ユーザ EXEC コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

SmartPort マクロの適用

SmartPort マクロを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**show parser macro**	スイッチ ソフトウェアに埋め込まれているシスコ デフォルト SmartPort マクロを表示します。
ステップ 2	**show parser macro name** *macro-name*	適用する特定のマクロを表示します。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**macro global** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	**macro global apply** *macro-name* を入力して、マクロで定義された個々のコマンドをスイッチに適用します。**macro global trace** *macro-name* を指定して、構文または設定エラーを判別するためにマクロを適用およびデバッグします。 **parameter** *value* キーワードを使用して、必要な値をマクロに追加します。**$** で始まるキーワードには、一意のパラメータ値が必要です。 **macro global apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。 （任意）スイッチに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。
ステップ 5	**interface** *interface-id*	（任意）インターフェイス コンフィギュレーション モードを開始し、マクロを適用するインターフェイスを指定します。
ステップ 6	**default interface** *interface-id*	（任意）指定されたインターフェイスからすべての設定を消去します。
ステップ 7	**macro** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	**macro global apply** *macro-name* を入力して、マクロで定義された個々のコマンドをポートに適用します。**macro global trace** *macro-name* を指定して、構文または設定エラーを判別するためにマクロを適用およびデバッグします。 **parameter** *value* キーワードを使用して、必要な値をマクロに追加します。**$** で始まるキーワードには、一意のパラメータ値が必要です。 **macro global apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。 （任意）スイッチに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**show running-config interface** *interface-id*	マクロがインターフェイスに適用されていることを確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

マクロに含まれる各コマンドの **no** バージョンを入力したときにだけ、スイッチで適用されたグローバル マクロ設定を削除できます。**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを入力すれば、ポートで適用されたマクロの設定を削除できます。

次に、**cisco-ie-desktop** マクロを表示する例、およびインターフェイス上でマクロを適用し、アクセス VLAN ID を 25 に設定する例を示します。

```
Switch# show parser macro name cisco-ie-desktop
-------------------------------------------------------------
Macro name : cisco-ie-desktop
Macro type : default interface
# macro keywords ACCESS_VLAN
#macro name cisco-ie-desktop
switchport mode access
switchport access vlan ACCESS_VLAN
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
spanning-tree bpduguard enable
no macro description
macro description cisco-ie-desktop
-------------------------------------------------------------
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet1/4
Switch(config-if)# macro apply cisco-ie-desktop $AVID 25
```

次に、**cisco-ethernetip** マクロを表示する例と、このマクロをインターフェイスに適用する例を示します。

```
Switch# show parser macro name cisco-ethernetip
Macro name : cisco-ie-global
Macro type : default interface
#macro name cisco-ethernetip
#macro keywords ACCESS_VLAN
#macro description cisco-ethernetip
switchport host
switchport access vlan ACCESS-VLAN
storm-control broadcast level 3.00 1.00
service-policy input CIP-Traffic
#service-policy input 1588

Switch# configure terminal
Switch(config)# interface fastethernet 1/1
Switch(config-if)# macro apply cisco-ethernetip ACCESS_VLAN 1
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

SmartPort マクロの表示

SmartPort マクロを表示するには、表 15-2 の 1 つまたは複数の特権 EXEC コマンドを使用します。

表 15-2　SmartPort マクロを表示するためのコマンド

コマンド	目的
show parser macro	すべての SmartPort マクロを表示します。
show parser macro name *macro-name*	特定の SmartPort マクロを表示します。
show parser macro brief	SmartPort マクロの名前を表示します。
show parser macro description [**interface** *interface-id*]	すべてのインターフェイスまたは特定のインターフェイスに関する SmartPort マクロの説明を表示します。

CHAPTER 16

VLAN の設定

この章では、IE 3000 スイッチに標準範囲 VLAN（VLAN ID 1 ～ 1005）および拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を設定する手順について説明します。VLAN メンバーシップ モード、VLAN コンフィギュレーション モード、VLAN トランク、および VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）からのダイナミック VLAN 割り当てについても説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

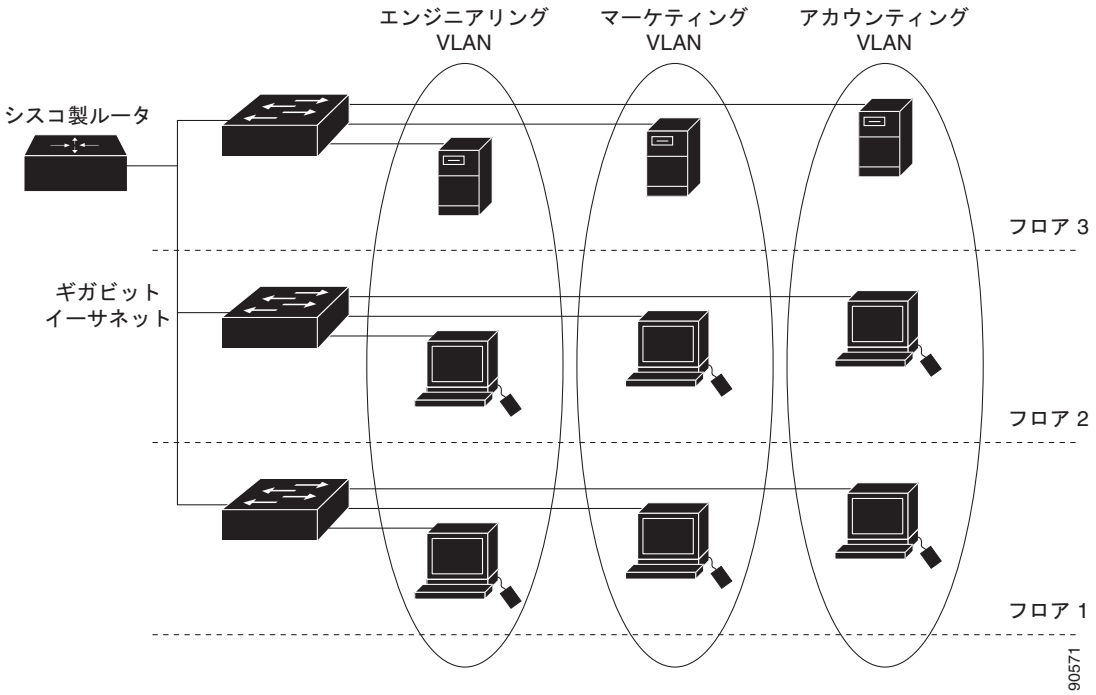
VLAN の概要

VLAN は、ユーザの物理的な位置にかかわりなく、機能、プロジェクト チーム、またはアプリケーション単位で論理的なセグメントに分割したスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、物理的に同じ LAN セグメントに置かれていないエンド ステーションでもグループ化することができます。VLAN には任意のスイッチ ポートを設定でき、ユニキャスト パケット、ブロードキャスト パケット、マルチキャスト パケットは VLAN 内のエンド ステーションだけに転送およびフラッディングされます。各 VLAN は 1 つの論理ネットワークと見なされます。VLAN に属さないステーション宛てのパケットは、フォールバック ブリッジングをサポートするルータまたはスイッチを介して転送されます（図 16-1 を参照）。VLAN は個別の論理ネットワークと見なされるため、独自のブリッジ Management Information Base（MIB; 管理情報ベース）情報を保持し、独自のスパニング ツリーを実装できます。第 21 章「STP の設定」を参照してください。

（注） VLAN を作成する前に、ネットワークのグローバル VLAN 設定の管理に VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）を使用するかどうかを決定する必要があります。VTP の詳細については、第 17 章「VTP の設定」を参照してください。

図 16-1 は、論理的に定義されたネットワークにセグメント化される VLAN の例を示しています。

図 16-1　論理的に定義されたネットワークの VLAN



VLAN は、多くの場合、IP サブネットワークと関連付けます。たとえば、特定の IP サブネットに含まれるすべてのエンド ステーションを同じ VLAN に属させる場合などです。スイッチ上のインターフェイスの VLAN メンバーシップは、インターフェイス単位に手動で割り当てます。この方法でスイッチ インターフェイスを VLAN に割り当てる場合に、インターフェイス ベース（スタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングまたはフォールバック ブリッジングする必要があります。スイッチは、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を使用して、VLAN 間のトラフィックをルーティングできます。SVI は明示的に設定し、VLAN 間のトラフィックをルーティングする IP アドレスを割り当てる必要があります。詳細については、「スイッチ仮想インターフェイス」（P.14-5）および「レイヤ 3 インターフェイスの設定」（P.14-21）を参照してください。

（注） スイッチ上に多数の VLAN を設定し、ルーティングをイネーブルにしない場合は、**sdm prefer vlan** グローバル コンフィギュレーション コマンドを使用すると、Switch Database Management（SDM）機能を VLAN テンプレートに設定できます。これによって、ユニキャスト MAC アドレスの最大数をサポートするシステム リソースを設定できます。SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」またはこのリリースのコマンド リファレンスで **sdm prefer** コマンドを参照してください。

サポートされる VLAN

このスイッチでは、VTP クライアント モード、VTP サーバ モード、および VTP トランスペアレント モードの VLAN がサポートされます。VLAN は、1 ～ 4094 の番号で識別されます。VLAN ID 1002 ～ 1005 は、トークン リング VLAN および FDDI VLAN 用に予約されています。

VTP バージョン 1 およびバージョン 2 では、標準範囲 VLAN（VLAN ID 1 ～ 1005）だけがサポートされます。これらのバージョンでは、1006 ～ 4094 の範囲の VLAN ID を作成する場合に、スイッチを VTP トランスペアレント モードで使用する必要があります。Cisco IOS Release 12.2(52)SE 以降では、VTP バージョン 3 がサポートされます。VTP バージョン 3 では、VLAN の全範囲（VLAN 1 ～ 4094）がサポートされます。拡張範囲 VLAN（VLAN 1006 ～ 4094）は、VTP バージョン 3 でだけサポートされます。ドメイン内に拡張 VLAN が設定されている場合、VTP バージョン 3 から VTP バージョン 2 に変換できません。

スイッチでは、計 1005（標準範囲および拡張範囲）の VLAN がサポートされますが、ルーテッド ポートの数、SVI、およびその他の設定済みの機能がスイッチのハードウェアの使用法に影響を及ぼします。

スイッチでは、最大 128 のスパニング ツリー インスタンスで Per-VLAN Spanning Tree Plus（PVST+）および Rapid PVST+ がサポートされます。VLAN 単位で 1 つのスパニング ツリー インスタンスが許可されます。スパニング ツリー インスタンス数と VLAN 数については、「標準範囲 VLAN 設定時の注意事項」（P.16-6）を参照してください。

VLAN ポートのメンバーシップ モード

VLAN に属するポートを設定するには、ポートが伝送するトラフィックの種類と、ポートが所属できる VLAN の数を指定するメンバーシップ モードを割り当てます。表 16-1 に各メンバーシップ モード、メンバーシップの特性、および VTP の特性を示します。

表 16-1　ポートのメンバーシップ モードおよび特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、1 つの VLAN に所属でき、該当の VLAN に手動で割り当てます。 詳細については、「VLAN へのスタティック アクセス ポートの割り当て」（P.16-10）を参照してください。	VTP は必須ではありません。VTP を使用してグローバルに情報を伝播する必要がない場合、VTP モードをトランスペアレント モードに設定します。VTP に参加するには、スイッチの少なくとも 1 つのトランク ポートが 2 番めのスイッチのトランク ポートに接続されている必要があります。
トランク（ISL または IEEE 802.1Q）	トランク ポートは、デフォルトで拡張範囲 VLAN を含むすべての VLAN のメンバーですが、許可 VLAN リストを設定することによってメンバーシップを制限することができます。プルーニング適格リストを変更して、リストに含まれるトランク ポート上で VLAN へのフラッディング トラフィックをブロックすることもできます。 トランク ポートの設定については、「イーサネット インターフェイスのトランク ポートとしての設定」（P.16-17）を参照してください。	VTP は推奨されますが、必須ではありません。VTP は、ネットワーク全体での VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランク リンク経由で他のスイッチと VLAN 設定メッセージを交換します。

表 16-1　ポートのメンバーシップ モードおよび特性 （続き）

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
ダイナミック アクセス	ダイナミック アクセス ポートは 1 つの VLAN（VLAN ID 1 ～ 4094）に属することができ、VMPS によってダイナミックに割り当てられます。VMPS には、たとえば Catalyst 5000 または Catalyst 6500 シリーズのスイッチが使用できますが、IE 3000 スイッチは使用できません。IE 3000 スイッチは VMPS クライアントです。 同じスイッチ上にダイナミック アクセス ポートとトランク ポートを設定できます。ただし、ダイナミック アクセス ポートは、エンド ステーションまたはハブに接続する必要があり、別のスイッチに接続できません。 設定の詳細については、「VMPS クライアント上でのダイナミック アクセス ポートの設定」（P.16-29）を参照してください。	VTP は必須です。 VMPS とクライアントを同じ VTP ドメイン名で設定します。 VTP に参加するには、スイッチの少なくとも 1 つのトランク ポートが 2 番めのスイッチのトランク ポートに接続されている必要があります。
音声 VLAN	音声 VLAN ポートは、音声トラフィック用に 1 つの VLAN を使用し、電話に接続された装置からのデータ トラフィック用に別の VLAN を使用するよう設定された Cisco IP Phone に付属するアクセス ポートの 1 つです。 音声 VLAN ポートの詳細については、第 18 章「音声 VLAN の設定」を参照してください。	VTP は必須ではなく、音声 VLAN にはまったく影響を及ぼしません。
プライベート VLAN	プライベート VLAN ポートは、プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN に属するホスト ポートまたはプロミスキャス ポートです。 プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」を参照してください。	VTP バージョン 1 および 2 では、プライベート VLAN を設定する場合に、スイッチを VTP トランスペアレント モードにする必要があります。スイッチ上にプライベート VLAN が設定されている場合は、VTP モードをトランスペアレントからクライアントまたはサーバ モードに変更しないでください。VTP バージョン 3 では、任意のモードでプライベート VLAN がサポートされます。
トンネル（**dot1q-tunnel**）	トンネル ポートは IEEE 802.1Q において、サービス プロバイダー ネットワーク全体でカスタマー VLAN の完全性を維持するために使用されます。サービス プロバイダー ネットワークのエッジ スイッチにトンネル ポートを設定して、カスタマー インターフェイスの IEEE 802.1Q トランク ポートに接続し、非対称リンクを構成します。トンネル ポートは、トンネリング専用の単一の VLAN に属します。 トンネル ポートの詳細については、第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。	VTP は必須ではありません。トンネル ポートを手動で VLAN に割り当てるには、**switchport access vlan** インターフェイス コンフィギュレーション コマンドを使用します。

アクセス モードおよびトランク モードの定義と機能の詳細については、表 16-4（P.16-16）を参照してください。

ポートが VLAN に属する場合、スイッチは VLAN 単位でポートに関連付けられたアドレスを学習して管理します。詳細については、「MAC アドレス テーブルの管理」（P.7-19）を参照してください。

標準範囲 VLAN の設定

標準範囲 VLAN は、VLAN ID 1 ～ 1005 の VLAN です。スイッチが VTP サーバ モードまたは VTP トランスペアレント モードの場合、VLAN 2 ～ 1001 の設定を VLAN データベースに追加、変更、削除できます（VLAN ID 1 および 1002 ～ 1005 は自動的に作成され、削除できません）。

VTP バージョン 1 および 2 では、拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を作成する場合に、スイッチを VTP トランスペアレント モードにする必要がありますが、これらの VLAN は VLAN データベースに保存されません。VTP バージョン 3 では、VTP サーバ モードおよび VTP トランスペアレント モードで拡張範囲 VLAN がサポートされます。「拡張範囲 VLAN の設定」（P.16-11）を参照してください。

VLAN ID 1 ～ 1005 の設定は、ファイル *vlan.dat*（VLAN データベース）に書き込まれ、**show vlan** 特権 EXEC コマンドを入力すると情報を表示できます。*vlan.dat* ファイルはフラッシュ メモリに保存されます。

注意　*vlan.dat* ファイルを手動で削除しようとすると、VLAN データベースに矛盾が生じる可能性があります。VLAN 設定を変更する場合、ここで説明するコマンドおよびこのリリースのコマンド リファレンスに記載されたコマンドを使用します。VTP 設定を変更するには、第 17 章「VTP の設定」を参照してください。

ポート メンバーシップ モードを定義したり、VLAN のポートを追加および削除するには、インターフェイス コンフィギュレーション モードを使用します。これらのコマンドの結果は、実行コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

標準範囲 VLAN の新規作成時または VLAN データベースに既存の VLAN の変更時に、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ（イーサネット、Fiber Distributed Data Interface（FDDI; ファイバ分散データ インターフェイス）、FDDI Network Entity Title（NET）、TrBRF、または TrCRF、トークン リング、トークン リング NET）
- VLAN ステート（アクティブまたは中断）
- VLAN の Maximum Transmission Unit（MTU; 最大伝送ユニット）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN の Spanning Tree Protocol（STP; スパニング ツリー プロトコル）タイプ
- 1 つの VLAN タイプから別の VLAN タイプに変換する VLAN 番号

（注）　ここでは、これらのパラメータの大部分について、設定の詳細は説明しません。VLAN 設定を制御するコマンドおよびパラメータの詳細については、このリリースのコマンド リファレンスを参照してください。

ここでは、次の標準範囲 VLAN 設定について説明します。

トークン リング VLAN

このスイッチではトークン リング接続がサポートされていませんが、サポートされるスイッチのいずれかから、トークン リング接続された Catalyst 5000 シリーズ スイッチなどのリモート装置を管理できます。VTP バージョン 2 を実行するスイッチは、次のトークン リング VLAN に関する情報をアドバタイズします。

- トークン リング TrBRF VLAN
- トークン リング TrCRF VLAN

トークン リング VLAN の設定の詳細については、『*Catalyst 5000 Series Software Configuration Guide*』を参照してください。

標準範囲 VLAN 設定時の注意事項

ネットワークで標準範囲 VLAN を作成および変更する場合、次の注意事項に従ってください。

- このスイッチは、VTP クライアント モード、VTP サーバ モード、および VTP トランスペアレント モードで 1005 の VLAN をサポートします。
- 標準範囲 VLAN は 1 ～ 1001 の範囲の番号で識別します。VLAN 番号 1002 ～ 1005 は、トークン リング VLAN および FDDI VLAN 用に予約されています。
- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに保存されます。VTP モードがトランスペアレント モードの場合、VTP および VLAN の設定がスイッチの実行コンフィギュレーション ファイルにも保存されます。
- VTP バージョン 1 および 2 では、スイッチは VTP トランスペアレント モード（VTP はディセーブル）でのみ VLAN ID 1006 ～ 4094 をサポートします。これらは拡張範囲 VLAN で、設定オプションが制限されます。VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播もされません。VTP バージョン 3 では拡張範囲 VLAN（VLAN 1006 ～ 4094）データベースの伝播がサポートされます。拡張 VLAN が設定されている場合、VTP バージョン 3 からバージョン 1 または 2 に変換できません。「拡張範囲 VLAN の設定」（P.16-11）を参照してください。

- VLAN を作成する前に、スイッチを VTP サーバ モードまたは VTP トランスペアレント モードにする必要があります。スイッチが VTP サーバの場合、VTP ドメインを定義しないと VTP が機能しません。
- スイッチでは、トークン リングまたは FDDI のメディアがサポートされていません。スイッチは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを転送するのではなく、VTP を介して VLAN 設定を伝播します。
- スイッチでは 128 のスパニング ツリー インスタンスがサポートされます。スイッチに、サポートされるスパニング ツリー インスタンスよりも多くのアクティブ VLAN がある場合、スパニング ツリーは 128 の VLAN でイネーブルにでき、残りの VLAN ではディセーブルになります。スイッチで使用可能なすべてのスパニング ツリー インスタンスを使用している場合、VTP ドメイン内の任意の場所に別の VLAN を追加すると、スパニング ツリーが動作していないスイッチ上に VLAN が作成されます。該当のスイッチのトランク ポートにデフォルトの許可リストがある場合（すべての VLAN を許可する）、新しい VLAN はすべのトランク ポートで伝送されます。ネットワークのトポロジによっては、このために新しい VLAN に切断できないループが発生する可能性があります。特に、スパニング ツリー インスタンスをすべて使い果たした隣接スイッチが複数ある場合です。スパニング ツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定すると、この可能性を排除できます。

  スイッチ上の VLAN 数が、サポートされているスパニング ツリー インスタンスの数を超えている場合、スイッチに IEEE 802.1s の Multiple STP（MSTP）を設定して、複数の VLAN を 1 つのスパニング ツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 22 章「MSTP の設定」を参照してください。

標準範囲 VLAN の設定

vlan グローバル コンフィギュレーション コマンドで VLAN ID を入力して VLAN を設定します。VLAN を作成するには新しい VLAN ID を入力し、VLAN を変更するには既存の VLAN ID を入力します。デフォルトの VLAN 設定（表 16-2）を使用することも、複数のコマンドを入力して VLAN を設定することもできます。このモードで使用可能なコマンドについては、このリリースのコマンド リファレンスで **vlan** グローバル コンフィギュレーション コマンドの説明を参照してください。設定が完了した後、設定を有効にするには VLAN コンフィギュレーション モードを終了する必要があります。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN ID 1 ～ 1005 の設定は常に VLAN データベース（vlan.dat ファイル）に保存されます。VTP モードがトランスペアレント モードの場合、設定はスイッチの実行コンフィギュレーション ファイルにも保存されます。**copy running-config startup-config** 特権 EXEC コマンドを入力すると、設定をスタートアップ コンフィギュレーション ファイルに保存できます。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN および VTP の情報（拡張範囲 VLAN 設定の情報を含む）をスタートアップ コンフィギュレーション ファイルに保存してスイッチを再起動する場合、スイッチ設定は次のように選択されます。

- スタートアップ コンフィギュレーションで VTP モードがトランスペアレントになっていて、VLAN データベースと、VLAN データベースの VTP ドメイン名がスタートアップ コンフィギュレーション ファイルの情報と一致する場合、VLAN データベースは無視（消去）され、スタートアップ コンフィギュレーション ファイルの VTP および VLAN の設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーションの VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 の VLAN のドメイン名、VTP モードおよび設定は VLAN データベースの情報を使用します。
- VTP バージョン 1 および 2 で、VTP モードがサーバ モードの場合、ドメイン名と VLAN 設定は最初の 1005 の VLAN だけに VLAN データベースの情報を使用します。VTP バージョン 3 では VLAN 1006 ～ 4094 もサポートされます。

デフォルトのイーサネット VLAN 設定

表 16-2 にイーサネット VLAN のデフォルト設定を示します。

（注）　このスイッチは排他的にイーサネット インターフェイスをサポートします。FDDI およびトークン リング VLAN はローカルにサポートされないため、FDDI およびトークン リング メディア固有の特性は、別のスイッチに対する VTP グローバル アドバタイズに限って設定します。

表 16-2　イーサネット VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1	1 ～ 4094 （注）　拡張範囲 VLAN（VLAN ID 1006 ～ 4094）は、VTP バージョン 3 でのみ VLAN データベースに保存されます。
VLAN 名	*VLANxxxx*。ここで、*xxxx* は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。	範囲なし
IEEE 802.10 SAID	100001（100000 + VLAN ID）	1 ～ 4294967294
MTU サイズ	1500	1500 ～ 18190
トランスレーショナル ブリッジ 1	0	0 ～ 1005
トランスレーショナル ブリッジ 2	0	0 ～ 1005
VLAN ステート	アクティブ	アクティブ、中断
リモート SPAN	ディセーブル	イネーブル、ディセーブル
プライベート VLAN	設定なし	2 ～ 1001、1006 ～ 4094

イーサネット VLAN の作成または変更

VLAN データベース内の各イーサネット VLAN には、1 ～ 1001 の 4 桁の一意の ID が設定されています。VLAN ID 1002 ～ 1005 は、トークン リング VLAN および FDDI VLAN 用に予約されています。標準範囲 VLAN を作成して VLAN データベースに追加するには、VLAN に番号と名前を割り当てます。

（注）　VTP バージョン 1 および 2 では、スイッチが VTP トランスペアレント モードの場合、1006 より大きい VLAN ID を割り当てることはできますが、VLAN データベースには追加されません。「拡張範囲 VLAN の設定」（P.16-11）を参照してください。

VLAN を追加する際に割り当てられるデフォルトのパラメータについては、「標準範囲 VLAN の設定」（P.16-5）を参照してください。

イーサネット VLAN を作成または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。VLAN を作成するには新しい VLAN ID を入力し、VLAN を変更するには既存の VLAN ID を入力します。 **（注）** このコマンドで指定できる VLAN ID 範囲は 1 ～ 4094 です。1005 より大きい VLAN ID を追加するには（拡張範囲 VLAN）、「拡張範囲 VLAN の設定」（P.16-11）を参照してください。
ステップ 3	**name** *vlan-name*	（任意）VLAN の名前を入力します。VLAN の名前を入力しない場合、VLAN という文字列に *vlan-id*（先行ゼロを伴う）を付加したデフォルト名が使用されます。たとえば、VLAN0004 が VLAN 4 のデフォルトの VLAN 名となります。
ステップ 4	**mtu** *mtu-size*	（任意）MTU サイズ（または他の VLAN 特性）を変更します。
ステップ 5	**remote-span**	**（注）** （任意）VLAN をリモート SPAN セッションの RSPAN VLAN として設定します。リモート SPAN の詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	設定を確認します。
ステップ 8	**copy running-config startup config**	（任意）スイッチが VTP トランスペアレント モードの場合、VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。これによって、設定がスイッチ スタートアップ コンフィギュレーション ファイルに保存されます。

VLAN 名をデフォルト設定に戻すには、**no name**、**no mtu**、または **no remote-span** コマンドを使用します。

この例は、イーサネット VLAN 20 を作成し、*test20* という名前を設定し、VLAN データベースに追加する方法を示しています。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

VLAN の削除

VTP サーバ モードのスイッチから VLAN を削除する場合、VLAN は VTP ドメイン内のすべてのスイッチの VLAN データベースから削除されます。VTP トランスペアレント モードのスイッチから VLAN を削除する場合、VLAN は特定のスイッチ上でのみ削除されます。

イーサネット VLAN 1 と FDDI またはトークン リング VLAN 1002 ～ 1005 のように、異なるメディア タイプのデフォルトの VLAN は削除できません。

注意　VLAN を削除すると、その VLAN に割り当てられているポートは非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブのまま）関連付けられています。

スイッチ上で VLAN を削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no vlan** *vlan-id*	VLAN ID を入力して、VLAN を削除します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vlan brief**	VLAN が削除されたことを確認します。
ステップ 5	**copy running-config startup config**	（任意）スイッチが VTP トランスペアレント モードの場合、VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。これによって、設定がスイッチ スタートアップ コンフィギュレーション ファイルに保存されます。

VLAN へのスタティック アクセス ポートの割り当て

VTP をディセーブルにする（VTP トランスペアレント モード）と、VTP でグローバルに VLAN 設定情報を伝播せずに、スタティック アクセス ポートを VLAN に割り当てられます。

クラスタ メンバー スイッチのポートを VLAN に割り当てる場合、最初に **rcommand** 特権 EXEC コマンドを使用して、クラスタ メンバー スイッチにログインします。

（注）　存在しない VLAN へのインターフェイスを指定すると、新しい VLAN が作成されます（「イーサネット VLAN の作成または変更」（P.16-8）を参照）。

VLAN データベースに存在する VLAN にポートを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	VLAN に追加するインターフェイスを入力します。
ステップ 3	**switchport mode access**	ポートの VLAN メンバーシップ モードを定義します（レイヤ 2 アクセス ポート）。
ステップ 4	**switchport access vlan** *vlan-id*	ポートを VLAN に割り当てます。指定できる VLAN ID は、1 ～ 4094 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id*	インターフェイスの VLAN メンバーシップ モードを確認します。
ステップ 7	**show interfaces** *interface-id* **switchport**	*Administrative Mode* フィールドと *Access Mode VLAN* フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスをデフォルトの設定に戻すには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートを VLAN 2 のアクセス ポートとして設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

拡張範囲 VLAN の設定

VTP バージョン 1 およびバージョン 2 で、スイッチが VTP トランスペアレント モードである（VTP はディセーブル）場合、拡張範囲 VLAN（1006 ～ 4094）を作成できます。VTP バージョン 3 では、サーバ モードまたはトランスペアレント モードで拡張範囲 VLAN がサポートされます。拡張範囲 VLAN を使用すると、サービス プロバイダーはインフラストラクチャをさらに多くのカスタマーに拡張できます。拡張範囲 VLAN ID は、VLAN ID を許可するすべての switchport コマンドで使用できます。

VTP バージョン 1 および 2 では、拡張範囲 VLAN 設定は VLAN データベースに保存されませんが、VTP モードがトランスペアレント モードなので、スイッチの実行コンフィギュレーション ファイルに保存されます。また、**copy running-config startup-config** 特権 EXEC コマンドを使用すると、設定をスタートアップ コンフィギュレーション ファイルに保存できます。VTP バージョン 3 で作成された拡張範囲 VLAN は、VLAN データベースに保存されます。

（注）　スイッチは 4094 の VLAN ID をサポートしますが、実際にサポートされる VLAN の数については「サポートされる VLAN」（P.16-2）を参照してください。

ここでは、拡張範囲 VLAN 設定の情報について説明します。

VLAN のデフォルト設定

イーサネット VLAN のデフォルト設定については、表 16-2（P.16-8）を参照してください。変更できるのは、拡張範囲 VLAN の MTU サイズ、プライベート VLAN、およびリモート SPAN 設定のステートです。他のすべての特性はデフォルト ステートのままにしておく必要があります。

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN を作成する場合、次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、スイッチが VTP バージョン 3 で稼動していない限り、VLAN データベースに保存されず、VTP から認識されません。
- 拡張範囲 VLAN をプルーニングに適格な範囲に設定できません。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN を作成する場合に、スイッチを VTP トランスペアレント モードにする必要があります。VTP モードがサーバ モードまたはクライアント モードである場合、エラー メッセージが生成され、拡張範囲 VLAN は拒否されます。VTP バージョン 3 はサーバ モードおよびトランスペアレント モードで拡張 VLAN をサポートします。

- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで VTP モードをトランスペアレントに設定できます。「VTP モードの設定」（P.17-11）を参照してください。スイッチを VTP トランスペアレント モードで起動させるには、この設定をスタートアップ コンフィギュレーションに保存する必要があります。保存しないと、スイッチがリセットされた場合に拡張範囲 VLAN 設定が失われます。拡張範囲 VLAN を VTP バージョン 3 で 作成すると、VTP バージョン 1 または 2 に変換できなくなります。
- STP は拡張範囲 VLAN 上でデフォルトでイネーブルに設定されていますが、**no spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用してディセーブルにできます。スイッチがスパニング ツリー インスタンスの最大数に達している場合、新たに作成されるすべての VLAN でスパニング ツリーはディセーブルになります。スイッチ上の VLAN 数が、スパニング ツリー インスタンスの数を超えている場合、スイッチに IEEE 802.1s の Multiple STP（MSTP）を設定して、複数の VLAN を 1 つのスパニング ツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 22 章「MSTP の設定」を参照してください。
- スイッチ上の各ルーテッド ポートは、内部的に使用する内部 VLAN を作成します。内部 VLAN は拡張範囲 VLAN の番号を使用し、内部 VLAN として使用されている ID は拡張範囲 VLAN として使用できなくなります。すでに内部 VLAN に割り当てられている VLAN ID で拡張範囲 VLAN を作成しようとすると、エラー メッセージが生成され、コマンドは拒否されます。
  - 内部 VLAN ID は拡張範囲の下位部分を使用するので、内部 VLAN ID と重なる可能性を低くするために、拡張範囲 VLAN の作成時に最上位の値（4094）から最下位の値（1006）に向かって降順に番号を使用することを推奨します。
  - 拡張範囲 VLAN を設定する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、内部 VLAN として割り当て済みの VLAN を確認します。
  - 必要に応じて、内部 VLAN に割り当てられたルーテッド ポートをシャットダウンして内部 VLAN を解放した後で、拡張範囲 VLAN を作成してポートを再度イネーブルにすると、内部 VLAN として別の VLAN が使用されます。「内部 VLAN ID を使用する拡張範囲 VLAN の作成」（P.16-14）を参照してください。
- スイッチでは、計 1005（標準範囲および拡張範囲）の VLAN がサポートされますが、ルーテッド ポートの数、SVI、およびその他の設定済みの機能がスイッチのハードウェアの使用法に影響を及ぼします。拡張範囲 VLAN を作成しようとして、使用可能なハードウェア リソースが十分でない場合、エラー メッセージが生成されて拡張範囲 VLAN は拒否されます。

拡張範囲 VLAN の作成

拡張範囲 VLAN を作成するには、グローバル コンフィギュレーション モードで **vlan** グローバル コンフィギュレーション コマンドに 1006 から 4094 の VLAN ID を指定します。拡張範囲 VLAN は、デフォルトのイーサネット VLAN の特性（表 16-2 を参照）を持ち、変更可能なパラメータは MTU サイズ、プライベート VLAN、および RSPAN の設定だけです。すべてのパラメータのデフォルト設定については、コマンド リファレンスで **vlan** グローバル コンフィギュレーション コマンドの説明を参照してください。VTP バージョン 1 または 2 では、スイッチが VTP トランスペアレント モードでない状態で拡張範囲 VLAN ID を入力すると、VLAN コンフィギュレーション モードの終了時にエラー メッセージが生成され、拡張範囲 VLAN は作成されません。

VTP バージョン 1 および 2 では、拡張範囲 VLAN は VLAN データベースには保存されず、スイッチの実行コンフィギュレーション ファイルに保存されます。拡張範囲 VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。VTP バージョン 3 では、拡張範囲 VLAN が VLAN データベースに保存されます。

（注）　拡張範囲 VLAN を作成する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、VLAN ID が内部的に使用されていないことを確認できます。内部的に使用されている VLAN ID を解放するには、拡張範囲 VLAN を作成する前に「内部 VLAN ID を使用する拡張範囲 VLAN の作成」（P.16-14）を参照してください。

拡張範囲 VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp mode transparent**	スイッチを VTP トランスペアレント モードに設定し、VTP をディセーブルにします。 （注）　VTP バージョン 3 の場合、このステップは不要です。
ステップ 3	**vlan** *vlan-id*	拡張範囲 VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ～ 4094 です。
ステップ 4	**mtu** *mtu-size*	（任意）MTU サイズを変更して、VLAN の設定を変更します。 （注）　CLI ヘルプにはすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされるのは **mtu** *mtu-size*、**private-vlan**、および **remote-span** コマンドだけです。
ステップ 5	**remote-span**	（任意）VLAN を RSPAN VLAN として設定します。「RSPAN VLAN としての VLAN の設定」（P.30-18）を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show vlan id** *vlan-id*	VLAN が作成されたことを確認します。
ステップ 8	**copy running-config startup config**	スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。拡張範囲 VLAN 設定を保存するには、VTP トランスペアレント モード設定および拡張範囲 VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存する必要があります。保存しないと、スイッチがリセットされた場合にデフォルトのサーバ モードに戻り、拡張範囲 VLAN ID は保存されません。 （注）　VTP バージョン 3 では、VLAN 設定は VLAN データベースにも保存されます。

拡張範囲 VLAN を削除するには、**no vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

拡張範囲 VLAN にスタティック アクセス ポートを割り当てる手順は、標準範囲 VLAN の場合と同じです。「VLAN へのスタティック アクセス ポートの割り当て」（P.16-10）を参照してください。

次に、すべての特性がデフォルトである拡張範囲 VLAN を新規作成し、VLAN コンフィギュレーション モードを開始して、新規 VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する例を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

内部 VLAN ID を使用する拡張範囲 VLAN の作成

すでに内部 VLAN に割り当てられる拡張範囲 VLAN ID を入力すると、エラー メッセージが生成され、拡張範囲 VLAN は拒否されます。内部 VLAN ID を手動で解放するには、その内部 VLAN ID を使用しているルーテッド ポートを一時的にシャットダウンする必要があります。

内部 VLAN に割り当てられている VLAN ID を解放し、同じ ID で拡張範囲 VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**show vlan internal usage**	スイッチが内部的に使用している VLAN ID を表示します。該当の VLAN ID が内部 VLAN の場合、その VLAN ID を使用しているルーテッド ポートが表示されます。ステップ 3 でポート番号を入力します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	VLAN ID を使用しているルーテッド ポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**shutdown**	内部 VLAN ID を解放するポートをシャットダウンします。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**vtp mode transparent**	拡張範囲 VLAN を作成するために VTP モードをトランスペアレント モードに設定します。 **（注）** VTP バージョン 3 の場合、このステップは不要です。
ステップ 7	**vlan** *vlan-id*	新しい拡張範囲 VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。
ステップ 8	**exit**	VLAN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *interface-id*	ステップ 4 でシャットダウンしたルーテッド ポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**no shutdown**	ルーテッド ポートを再度イネーブルにします。新しい内部 VLAN ID が割り当てられます。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**copy running-config startup config**	スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。拡張範囲 VLAN 設定を保存するには、VTP トランスペアレント モード設定および拡張範囲 VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存する必要があります。保存しないと、スイッチがリセットされた場合にデフォルトのサーバ モードに戻り、拡張範囲 VLAN ID は保存されません。 **（注）** VTP バージョン 3 の場合、VLAN が VLAN データベースに保存されるため、このステップは不要です。

VLAN の表示

拡張範囲 VLAN を含む、スイッチ上のすべての VLAN のリストを表示するには、**show vlan** 特権 EXEC コマンドを使用します。VLAN のステータス、ポート、および設定情報が表示されます。

表 16-3 に VLAN をモニタする特権 EXEC コマンドを示します。

表 16-3　VLAN のモニタ コマンド

コマンド	目的
show interfaces [**vlan** *vlan-id*]	スイッチ上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。
show vlan [**id** *vlan-id*]	スイッチ上のすべての VLAN または特定の VLAN のパラメータを表示します。

show コマンドのオプションおよび出力フィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

VLAN トランクの設定

ここでは、次の概念情報について説明します。

- 「トランキングの概要」（P.16-15）
- 「レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定」（P.16-17）
- 「イーサネット インターフェイスのトランク ポートとしての設定」（P.16-17）
- 「ロード シェアリングを目的としたトランク ポートの設定」（P.16-22）

トランキングの概要

トランクとは、1 つまたは複数のイーサネット スイッチ インターフェイスと、ルータやスイッチなど別のネットワーキング装置の間のポイントツーポイント リンクです。イーサネット トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。スイッチは IEEE 802.1Q カプセル化をサポートします。

1 つのイーサネット インターフェイスまたは EtherChannel バンドルに対してトランクを設定できます。EtherChannel の詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

イーサネット トランク インターフェイスは、数種類のトランキング モードをサポートしています（表 16-4 を参照）。インターフェイスをトランキングまたは非トランキングとして、またはネイバー インターフェイスとトランキングをネゴシエートするように設定できます。トランキングを自動ネゴシエートするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、ポイントツーポイント プロトコルである Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）によって管理されます。ただし、一部のインターネットワーキング装置によって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

この事態を避けるには、DTP をサポートしない装置に接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンクを介してトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていない装置でトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

（注） DTP はプライベート VLAN ポートまたはトンネル ポートではサポートされません。

表 16-4　レイヤ 2 インターフェイス モード

モード	機能
switchport mode access	インターフェイス（アクセス ポート）は永続的な非トランキング モードになり、リンクを非トランク リンクに変換するようにネゴシエートします。ネイバー インターフェイスがトランク インターフェイスであるかどうかにかかわらず、インターフェイスは非トランク インターフェイスになります。
switchport mode dynamic auto	インターフェイスがリンクからトランク リンクに変換できるようにします。ネイバー インターフェイスが *trunk* または *desirable* モードに設定されると、インターフェイスはトランク インターフェイスになります。すべてのイーサネット インターフェイスに対するデフォルトのスイッチポート モードは、**dynamic auto** です。
switchport mode dynamic desirable	リンクからトランク リンクへの変換をインターフェイスにアクティブに試行させます。ネイバー インターフェイスが *trunk*、*desirable*、または *auto* モードに設定されると、インターフェイスはトランク インターフェイスになります。
switchport mode trunk	インターフェイスは永続的なトランキング モードになり、ネイバー リンクをトランク リンクに変換するようにネゴシエートします。ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスはトランク インターフェイスになります。
switchport nonegotiate	インターフェイスが DTP フレームを生成するのを防ぎます。このコマンドを使用できるのは、インターフェイス スイッチポート モードが **access** または **trunk** である場合だけです。トランク リンクを確立するには、ネイバー インターフェイスを手動でトランク インターフェイスとして設定する必要があります。
switchport mode dot1q-tunnel	IEEE 802.1Q トランク ポートと非対称リンクで接続するために、インターフェイスをトンネル（非トランキング）ポートとして設定します。IEEE 802.1Q トンネリングは、サービス プロバイダー ネットワーク全体でカスタマー VLAN の完全性を維持するために使用されます。トンネル ポートの詳細については、第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

（注） このスイッチはレイヤ 3 トランクをサポートしていません。同等の機能を備えたレイヤ 2 トランクおよびレイヤ 3 VLAN インターフェイスをサポートします。

IEEE 802.1Q 設定に関する考慮事項

IEEE 802.1Q トランクを使用する場合に、ネットワークのトランキングの構築方法が次のように制限されます。

- IEEE 802.1Q トランクを使用して接続している Cisco スイッチのネットワークでは、トランク上で許容される VLAN ごとに 1 つのスパニング ツリー インスタンスが維持されます。非シスコ デバイスはすべての VLAN に対して 1 つのスパニング ツリー インスタンスをサポートしている可能性があります。

  IEEE 802.1Q トランクを介して Cisco スイッチを非シスコ デバイスに接続する場合、Cisco スイッチはトランクの VLAN のスパニング ツリー インスタンスと他社製の IEEE 802.1Q スイッチのスパニング ツリー インスタンスを結合します。ただし、各 VLAN のスパニング ツリーの情報は、他社製の IEEE 802.1Q スイッチのクラウドと切り離して、Cisco スイッチが維持します。Cisco スイッチを分離する他社製の 802.1Q 装置のクラウドは、スイッチ間の単一トランク リンクとして処理されます。

- IEEE 802.1Q トランクのネイティブ VLAN がトランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と他端のネイティブ VLAN が異なると、スパニング ツリー ループの原因になります。

- ネットワーク上のすべての VLAN についてスパニング ツリーをディセーブルにせずに、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニング ツリーをディセーブルにすると、スパニング ツリー ループが発生することがあります。IEEE 802.1Q トランクのネイティブ VLAN 上のスパニング ツリーをイネーブルのままにするか、ネットワーク上のすべての VLAN のスパニング ツリーをディセーブルにすることを推奨します。スパニング ツリーをディセーブルにする場合には、事前にネットワークにループが存在しないことを確認してください。

レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

表 16-5 にレイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定を示します。

表 16-5　レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
インターフェイス モード	**switchport mode dynamic auto**
VLAN 許容範囲	VLAN 1 ～ 4094
プルーニングに適格な VLAN 範囲	VLAN 2 ～ 1001
デフォルトの VLAN（アクセス ポート用）	VLAN 1
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1

イーサネット インターフェイスのトランク ポートとしての設定

トランク ポートは VTP アドバタイズを送受信するため、VTP を使用するには、スイッチ上に少なくとも 1 つのトランク ポートが設定されていて、このトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。

ここでは、次の設定情報について説明します。

- 「他の機能との相互作用」（P.16-18）
- 「トランク上で許可される VLAN の定義」（P.16-20）
- 「プルーニング適格リストの変更」（P.16-21）
- 「タグなしトラフィック用のネイティブ VLAN の設定」（P.16-22）

（注）　デフォルトで、インターフェイスはレイヤ 2 モードです。レイヤ 2 インターフェイスのデフォルト モードは、**switchport mode dynamic auto** です。ネイバー インターフェイスがトランキングをサポートしていて、トランキングを許可するよう設定されている場合、リンクはレイヤ 2 トランクになります。または、インターフェイスがレイヤ 3 モードである場合、**switchport** インターフェイス コンフィギュレーション コマンドを入力すると、レイヤ 2 トランクになります。

他の機能との相互作用

トランキングは次のように他の機能と相互に作用します。

- トランク ポートはセキュア ポートにできません。
- トランク ポートはトンネル ポートにできません。
- トランク ポートは、EtherChannel ポート グループにグループ化できますが、グループ内のすべてのトランクが同じ設定である必要があります。グループを初めて作成したときは、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかの設定を変更すると、スイッチは入力した設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト
  - 各 VLAN の STP ポート プライオリティ
  - STP PortFast 設定
  - トランクのステータス：ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- 設定するトランク ポートは、PVST モードでは 24 まで、MST モードでは 40 までにすることを推奨します。
- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、トランク ポートへの変更をネイバーとネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

トランク ポートの設定

ポートをトランク ポートとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	トランキング用に設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートである場合、またはトランキング モードを設定する場合に限り必要）。 • **dynamic auto**:ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクに設定します。これはデフォルトです。 • **dynamic desirable** : ネイバー インターフェイスが trunk、desirable または auto モードに設定されている場合に、インターフェイスをトランク リンクに設定します。 • **trunk** : インターフェイスを永続的なトランキング モードに設定し、ネイバー インターフェイスがトランク インターフェイスでない場合でも、リンクのトランク リンクへの変換をネゴシエートします。
ステップ 4	**switchport access vlan** *vlan-id*	（任意）インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。
ステップ 5	**switchport trunk native vlan** *vlan-id*	IEEE 802.1Q トランクのネイティブ VLAN を指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id* **switchport**	インターフェイスのスイッチポート コンフィギュレーションを *Administrative Mode* フィールドと *Administrative Trunking Encapsulation* フィールドに表示します。
ステップ 8	**show interfaces** *interface-id* **trunk**	インターフェイスのトランクの設定を表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスをデフォルトの設定に戻すには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。トランキング インターフェイスのトランキング特性をすべてデフォルトにリセットするには、**no switchport trunk** インターフェイス コンフィギュレーション コマンドを使用します。トランキングをディセーブルにするには、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、ポートをスタティック アクセス ポートとして設定します。

次に、ポートを IEEE 802.1Q トランクとして設定する例を示します。この例では、ネイバー インターフェイスが IEEE 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```

トランク上で許可される VLAN の定義

デフォルトで、トランク ポートはすべての VLAN との間でトラフィックを送受信します。各トランク上で 1 ～ 4094 のすべての VLAN ID が許可されます。ただし、許可リストから VLAN を削除すると、該当の VLAN からのトラフィックがトランクを通過することを防止できます。トラフィックがトランクを伝送されないようにするには、**switchport trunk allowed vlan remove** *vlan-list* インターフェイス コンフィギュレーション コマンドを使用して、特定の VLAN を許可リストから削除します。

（注）　VLAN 1 は、全 Cisco スイッチのすべてのトランク ポートのデフォルト VLAN で、以前は VLAN 1 がすべてのトランク リンク上で常にイネーブルであることが要件となっていました。ユーザ トラフィック（スパニング ツリーのアドバタイズを含む）が VLAN 1 上を送受信されないように、個々の VLAN トランク リンク上で VLAN 1 をディセーブルにして VLAN 1 の最小化機能を使用できます。

スパニング ツリー ループまたはストームの危険性を減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにします。トランク ポートから VTP 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）、Link Aggregation Control Protocol（LACP）、DTP、および VLAN 1 の VTP）を送受信し続けます。

VLAN 1 がディセーブルになったトランク ポートが非トランク ポートに変換されると、アクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、**switchport trunk allowed** 設定に関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている VLAN についても同様です。

VLAN がイネーブルになっていて、VTP が VLAN を認識し、VLAN がポートの許可リストにある場合、トランク ポートは VLAN のメンバーになることができます。VTP が新たにイネーブルになった VLAN を検出し、その VLAN がトランク ポートの許可リストにある場合、自動的にトランク ポートはイネーブルになった VLAN のメンバーになります。VTP が新たに VLAN を検出し、その VLAN がトランク ポートの許可リストにない場合、トランク ポートは新しい VLAN のメンバーになりません。

トランクの許可リストを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 4	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*	（任意）トランク上で許可される VLAN のリストを設定します。 **add**、**all**、**except**、および **remove** キーワードの使用の詳細については、このリリースに対応するコマンド リファレンスを参照してください。 *vlan-list* パラメータは、1 ～ 4094 の範囲の単一の VLAN 番号、または 2 つの VLAN 番号（小さい番号が先、ハイフンで区切る）で指定する VLAN 範囲です。カンマで区切った VLAN パラメータの間、またはハイフンで指定した範囲の間には、スペースを入れないでください。 デフォルトでは、すべての VLAN が許可されます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport**	*Trunking VLANs Enabled* フィールドの設定を画面で確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

すべての VLAN のデフォルト許可 VLAN リストに戻すには、**no switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上で許可 VLAN リストから VLAN 2 を削除する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

プルーニング適格リストの変更

プルーニング適格リストは、トランク ポートにだけ適用されます。トランク ポートごとに独自の適格リストがあります。この手順を有効にするには、VTP プルーニングをイネーブルにする必要があります。「VTP プルーニングのイネーブル化」（P.17-15）では、VTP プルーニングをイネーブルにする方法を説明しています。

トランク ポートのプルーニング適格リストから VLAN を削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	VLAN をプルーニングするトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan*[,*vlan*[,,,]]	トランクからのプルーニングが許容される VLAN のリストを設定します（「VTP プルーニング」（P.17-6）を参照）。 **add**、**except**、**none**、および **remove** キーワードの詳細については、このリリースに対応するコマンド リファレンスを参照してください。 連続しない VLAN ID は、スペースを入れずにカンマで区切ります。ID の範囲を指定するにはハイフンを使用します。有効な ID は、2 ～ 1001 です。拡張範囲 VLAN（VLAN ID 1006 ～ 4094）はプルーニングできません。 プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。 デフォルトでは、プルーニングが許容される VLAN のリストには、2 ～ 1001 の範囲の VLAN が含まれます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	*Pruning VLANs Enabled* フィールドの設定を画面で確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

すべての VLAN のデフォルトのプルーニング適格リストに戻すには、**no switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します。

タグなしトラフィック用のネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックとタグなしトラフィックのいずれも受信できます。デフォルトで、スイッチはポートに設定されたネイティブ VLAN でタグなしトラフィックを転送します。ネイティブ VLAN は、デフォルトでは VLAN 1 です。

（注）　ネイティブ VLAN は任意の VLAN ID に割り当てることができます。

IEEE 802.1Q の設定上の問題については、「IEEE 802.1Q 設定に関する考慮事項」（P.16-17）を参照してください。

IEEE 802.1Q トランク上にネイティブ VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	IEEE 802.1Q トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport trunk native vlan** *vlan-id*	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 *vlan-id* では、指定できる範囲は 1 ～ 4094 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	*Trunking Native Mode VLAN* フィールドの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのネイティブ VLAN である VLAN 1 に戻すには、**no switchport trunk native vlan** インターフェイス コンフィギュレーション コマンドを使用します。

パケットの VLAN ID が発信ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。

ロード シェアリングを目的としたトランク ポートの設定

ロード シェアリングによって、スイッチを接続するパラレル トランクが供給する帯域幅が分割されます。STP は通常、ループを回避するために、スイッチ間で 1 つを残してすべてのパラレル リンクをブロックします。ロード シェアリングを採用すると、トラフィックが属する VLAN によって、リンク間のトラフィックを分割します。

トランク ポート上にロード シェアリングを設定する際には、STP ポート プライオリティまたは STP パス コストを使用します。STP ポート プライオリティを使用するロード シェアリングでは、両方のロード シェアリング リンクを同じスイッチに接続する必要があります。STP パス コストを使用するロード シェアリングでは、各ロード シェアリング リンクを同じスイッチに接続することも、2 つの異なるスイッチに接続することもできます。STP の詳細については、第 21 章「STP の設定」を参照してください。

STP ポート プライオリティを使用するロード シェアリング

同じスイッチ上の 2 つのポートがループを形成する場合、スイッチは STP ポート プライオリティを使用して、どちらのポートがイネーブルで、どちらのポートがブロッキング ステートかを決定します。ポートが特定の VLAN 宛てのすべてのトラフィックを伝送するように、パラレル トランク ポートにプライオリティを設定できます。特定の VLAN について高いプライオリティ（小さい数値）を持つトランク ポートは、その VLAN 宛てのトラフィックを転送します。同じ VLAN について低いプライオリティ（大きい数値）を持つトランク ポートは、その VLAN に対してブロッキング ステートのままです。1 つのトランク ポートは、その VLAN に対してすべてのトラフィックを送受信します。

図 16-2 に、サポートされるスイッチを接続する 2 つのトランクを示します。この例では、スイッチは次のように設定されています。

- VLAN 8 ～ 10 は、トランク 1 にポート プライオリティ 16 が割り当てられている。
- VLAN 3 ～ 6 は、トランク 1 がデフォルト ポート プライオリティ 128 のままである。
- VLAN 3 ～ 6 は、トランク 2 にポート プライオリティ 16 が割り当てられている。
- VLAN 8 ～ 10 は、トランク 2 がデフォルト ポート プライオリティ 128 のままである。

このようにして、トランク 1 は VLAN 8 ～ 10 宛てのトラフィックを伝送し、トランク 2 は VLAN 3 ～ 6 宛てのトラフィックを伝送します。アクティブなトランクに障害が発生すると、低いプライオリティを持つトランクが処理を引き継いで、VLAN のすべてのトラフィックを伝送します。トランク ポート上でトラフィックの重複は発生しません。

図 16-2　STP ポート プライオリティを使用するロード シェアリング

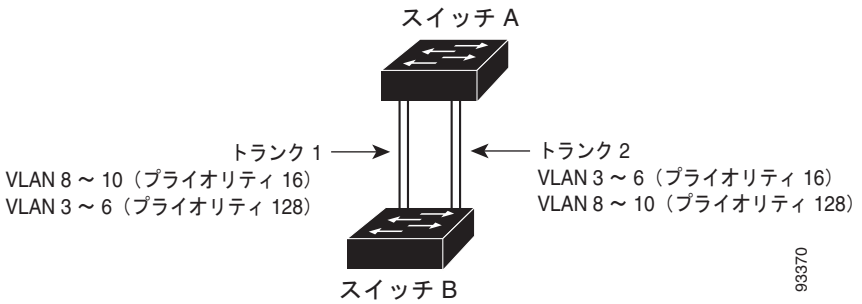


図 16-2 に示すネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	スイッチ A でグローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp domain** *domain-name*	VTP 管理ドメインを設定します。 ドメイン名は 1 ～ 32 文字です。
ステップ 3	**vtp mode server**	スイッチ A を VTP サーバとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status**	スイッチ A とスイッチ B の VTP 設定を確認します。 表示で、*VTP Operating Mode* フィールドと *VTP Domain Name* フィールドを確認します。
ステップ 6	**show vlan**	VLAN がスイッチ A のデータベースに存在することを確認します。
ステップ 7	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 8	**interface** *interface-id_1*	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show interfaces** *interface-id_1* **switchport**	VLAN の設定を確認します。
ステップ 12		スイッチの 2 番めのポートについて、スイッチ A 上でステップ 7 ～ 10 を繰り返します。
ステップ 13		スイッチ B 上でステップ 7 ～ 10 を繰り返し、スイッチ A 上に設定されたトランク ポートに接続するトランク ポートを設定します。
ステップ 14	**show vlan**	トランク リンクがアップすると、VTP は VTP と VLAN の情報をスイッチ B に渡します。スイッチ B が VLAN 設定を学習したことを確認します。
ステップ 15	**configure terminal**	スイッチ A でグローバル コンフィギュレーション モードを開始します。
ステップ 16	**interface** *interface-id_1*	STP ポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 17	**spanning-tree vlan 8-10 port-priority 16**	VLAN 8 ～ 10 にポート プライオリティ 16 を割り当てます。
ステップ 18	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 19	**interface** *interface-id_2*	STP ポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 20	**spanning-tree vlan 3-6 port-priority 16**	VLAN 3 ～ 6 にポート プライオリティ 16 を割り当てます。
ステップ 21	**end**	特権 EXEC モードに戻ります。
ステップ 22	**show running-config**	設定を確認します。
ステップ 23	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

STP パス コストを使用するロード シェアリング

トランク上に異なるパス コストを設定して異なる VLAN セットと関連付け、別の VLAN 用のポートをブロックすることによって VLAN トラフィックを共有するようパラレル トランクを設定できます。VLAN はトラフィックを個別に維持し、リンクが失われた場合に冗長性を保ちます。

図 16-3 で、トランク ポート 1 および 2 は 100BASE-T ポートとして設定されています。VLAN パス コストは次のように割り当てられています。

- VLAN 2 ～ 4 は、トランク ポート 1 にパス コスト 30 が割り当てられている。
- VLAN 8 ～ 10 は、トランク ポート 1 がデフォルトの 100BASE-T パス コスト 19 のままである。
- VLAN 8 ～ 10 は、トランク ポート 2 にパス コスト 30 が割り当てられている。
- VLAN 2 ～ 4 は、トランク ポート 2 がデフォルトの 100BASE-T パス コスト 19 のままである。

図 16-3　パス コストによってトラフィックを分散させるロード シェアリング トランク

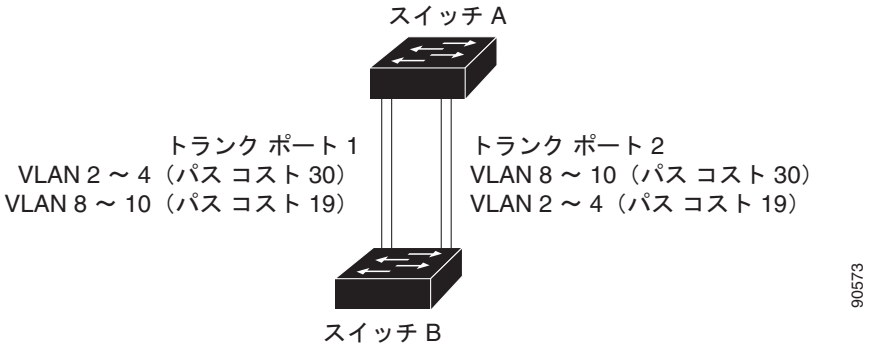


図 16-3 に示すネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	スイッチ A でグローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id_1*	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5		スイッチ A の 2 番めのインターフェイスでステップ 2 ～ 4 を繰り返します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。表示で、インターフェイスがトランク ポートとして設定されていることを確認します。
ステップ 8	**show vlan**	トランク リンクがアップすると、スイッチ A は他のスイッチから VTP 情報を受信します。スイッチ A が VLAN 設定を学習したことを確認します。
ステップ 9	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface** *interface-id_1*	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**spanning-tree vlan 2-4 cost 30**	VLAN 2 ～ 4 にスパニング ツリー パス コスト 30 を設定します。
ステップ 12	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 13		スイッチ A 上に設定された他のトランク インターフェイスでステップ 9 ～ 12 を繰り返し、VLAN 8、9、および 10 にスパニング ツリー パス コスト 30 を設定します。
ステップ 14	**exit**	特権 EXEC モードに戻ります。
ステップ 15	**show running-config**	設定を確認します。表示で、パス コストが両方のトランク インターフェイスに正しく設定されていることを確認します。
ステップ 16	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VMPS の設定

VLAN Query Protocol（VQP）は、ダイナミック アクセス ポートをサポートするために使用されます。ダイナミック アクセス ポートは、VLAN に永続的に割り当てられるのではなく、ポート上で確認される MAC 送信元アドレスに基づいて VLAN に割り当てられます。未知の MAC アドレスが認識されるたびに、スイッチは VQP クエリーをリモート VMPS に送信します。VQP クエリーには、新たに認識された MAC アドレスと、認識したポートの情報が含まれます。VMPS はポートへの VLAN 割り当てで応答します。スイッチは、VMPS サーバにはなりませんが、VMPS のクライアントとして動作し、VQP を介して通信できます。

ここでは、次の情報について説明します。

VMPS の概要

クライアント スイッチは新しいホストの MAC アドレスを受信するたびに、VQP クエリーを VMPS に送信します。VMPS はこのクエリーを受信すると、データベースを検索して MAC アドレスと VLAN のマッピングを探します。サーバはこのマッピングと、サーバがオープン モードであるかセキュア モードであるかに基づいて応答します。セキュア モードでは、不正なホストが検出されると、サーバはポートをシャットダウンします。オープン モードでは、サーバはポートへのホスト アクセスを単に拒否します。

ポートが現在*未割り当て*の（つまり、まだ VLAN 割り当てがない）場合、VMPS は次のいずれかの応答をします。

- ホストがポート上で許可されている場合、VMPS は割り当てられた VLAN 名を含み、ホストへのアクセスを許可する *vlan-assignment* 応答をクライアントに送信します。
- ホストがポート上で許可されておらず、VMPS がオープン モードの場合、VMPS は *access-denied* 応答を送信します。
- VLAN がポート上で許可されておらず、VMPS がセキュア モードの場合、VMPS は *port-shutdown* 応答を送信します。

ポートにすでに VLAN 割り当てがある場合、VMPS は次のいずれかの応答をします。

- データベースにある VLAN がポート上の現在の VLAN と一致する場合、VMPS はホストへのアクセスを許可する *success* 応答を送信します。
- データベースにある VLAN がポート上の現在の VLAN と一致せず、アクティブなホストがポート上に存在する場合、VMPS はセキュア モードによって *access-denied* または *port-shutdown* 応答を送信します。

スイッチは VMPS からの *access-denied* 応答を受信すると、該当のホスト MAC アドレスに対するトラフィックのブロックを継続します。スイッチは、ポートに転送されたパケットを引き続きモニタし、新しいホスト アドレスを認識すると VMPS にクエリーを送信します。スイッチは VMPS からの *port-shutdown* 応答を受信すると、ポートをディセーブルにします。ポートを再度イネーブルにするには、手動で Network Assistant、CLI、または SNMP を使用する必要があります。

ダイナミック アクセス ポート VLAN メンバーシップ

ダイナミック アクセス ポートは、1 ～ 4094 の ID を持つ 1 つの VLAN だけに属することができます。リンクがアップしたとき、VMPS が VLAN 割り当てを行うまで、スイッチはこのポートにトラフィックを転送しません。VMPS は、ダイナミック アクセス ポートに接続された新しいホストの最初のパケットから送信元 MAC アドレスを取り出し、VMPS データベースにある VLAN の MAC アドレスと突き合わせます。

一致するエントリがある場合、VMPS はポートの VLAN 番号を送信します。クライアント スイッチがまだ設定されていない場合、トランク ポート上で VMPS から受信した最初の VTP パケットにあるドメイン名を使用します。クライアント スイッチがすでに設定されている場合、VLAN 番号を取得するための VMPS へのクエリー パケットにドメイン名が挿入されます。VMPS は、要求を受け入れる前にパケットのドメイン名がそれ自体のドメイン名と一致することを確認し、クライアントに割り当てた VLAN 番号をクライアントに応答します。一致するエントリがない場合、VMPS は要求を拒否するか、ポートをシャットダウンします（VMPS セキュア モード設定に依存します）。

1 つのダイナミック アクセス ポートで、同じ VLAN にある複数のホスト（MAC アドレス）をアクティブにできます。ただし、ポート上で 20 を超えるホストがアクティブになっている場合、VMPS はダイナミック アクセス ポートをシャットダウンします。

ダイナミック アクセス ポートのリンクがダウンすると、ポートは VLAN に属さない独立した状態に戻ります。このポートを介してオンライン状態になるホストがあれば、ポートを VLAN に割り当てる前に、VQP によって再度 VMPS に確認されます。

ダイナミック アクセス ポートは、ホストの直接接続に使用することも、ネットワークに接続することもできます。スイッチ上のポートごとに最大 20 の MAC アドレスが許可されます。ダイナミック アクセス ポートが属することができる VLAN は一度に 1 つだけですが、認識される MAC アドレスによって随時 VLAN を変更できます。

VMPS クライアントのデフォルト設定

表 16-6 に、クライアント スイッチ上の VMPS およびダイナミック アクセス ポートのデフォルト設定を示します。

表 16-6　VMPS クライアントおよびダイナミック アクセス ポートのデフォルト設定

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認間隔	60 分
VMPS サーバの再試行回数	3
ダイナミック アクセス ポート	設定なし

VMPS 設定時の注意事項

ダイナミック アクセス ポート VLAN メンバーシップには、次の注意事項および制約事項が適用されます。

- ポートをダイナミック アクセス ポートとして設定する前に、VMPS を設定する必要があります。
- ポートをダイナミック アクセス ポートとして設定すると、そのポートでスパニング ツリー PortFast 機能が自動的にイネーブルになります。PortFast モードでは、ポートをフォワーディング ステートにする処理が加速されます。

- IEEE 802.1x ポートは、ダイナミック アクセス ポートとして設定できません。ダイナミック アクセス（VQP）ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- トランク ポートをダイナミック アクセス ポートにすることはできませんが、トランク ポートに **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力できます。この場合、スイッチは設定を保持し、あとでポートがアクセス ポートとして設定された場合に設定を適用します。

  ダイナミック アクセス設定を有効にする前に、ポートのトランキングをオフにする必要があります。
- ダイナミック アクセス ポートをモニタ ポートにすることはできません。
- セキュア ポートをダイナミック アクセス ポートにすることはできません。ダイナミックにする前に、ポート上のポート セキュリティをディセーブルにする必要があります。
- プライベート VLAN ポートをダイナミック アクセス ポートにすることはできません。
- ダイナミック アクセス ポートを EtherChannel グループのメンバーにすることはできません。
- ポート チャネルはダイナミック アクセス ポートとして設定できません。
- ダイナミック アクセス ポートは、フォールバック ブリッジングに参加できます。
- VMPS クライアントの VTP 管理ドメインと VMPS サーバの VTP 管理ドメインは、同じである必要があります。
- VMPS サーバ上に設定される VLAN は、音声 VLAN にしないでください。

VMPS クライアントの設定

VMPS（サーバ）を使用してダイナミック VLAN を設定します。スイッチを VMPS クライアントにすることはできますが、VMPS サーバにすることはできません。

VMPS の IP アドレスの入力

スイッチをクライアントとして設定するには、まず、サーバの IP アドレスを入力する必要があります。

（注）　VMPS をスイッチのクラスタに定義する場合、コマンド スイッチのアドレスを入力します。

VMPS の IP アドレスを入力するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vmps server** *ipaddress* **primary**	プライマリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。
ステップ 3	**vmps server** *ipaddress*	（任意）セカンダリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。 セカンダリ サーバのアドレスは最大 3 つまで入力できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show vmps**	*VMPS Domain Server* フィールドの設定を画面で確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　ダイナミック アクセス ポートが動作するには VMPS への IP 接続が必要です。IP 接続をテストするには、VMPS の IP アドレスに ping を使用し、応答が返ることを確認します。

VMPS クライアント上でのダイナミック アクセス ポートの設定

クラスタ メンバー スイッチのポートをダイナミック アクセス ポートとして設定する場合、最初に **rcommand** 特権 EXEC コマンドを使用して、クラスタ メンバー スイッチにログインします。

注意　ダイナミック アクセス ポート VLAN メンバーシップは、エンド ステーション、またはエンド ステーションに接続されたハブ用です。ダイナミック アクセス ポートを他のスイッチに接続すると、接続が切断されることがあります。

VMPS クライアント スイッチ上にダイナミック アクセス ポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	エンド ステーションに接続されたスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access**	ポートをアクセス モードに設定します。
ステップ 4	**switchport access vlan dynamic**	ダイナミック VLAN メンバーシップに適格としてポートを設定します。 ダイナミック アクセス ポートはエンド ステーションに接続する必要があります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport**	*Operational Mode* フィールドの設定を画面で確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスをデフォルトの設定に戻すには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスをデフォルトのスイッチポート モード（dynamic auto）に戻すには、**no switchport mode** インターフェイス コンフィギュレーション コマンドを使用します。アクセス モードをスイッチのデフォルト VLAN にリセットするには、**no switchport access vlan** インターフェイス コンフィギュレーション コマンドを使用します。

VLAN メンバーシップの再確認

スイッチが VMPS から受信したダイナミック アクセス ポート VLAN メンバーシップの割り当てを確認するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**vmps reconfirm**	ダイナミック アクセス ポート VLAN メンバーシップを再確認します。
ステップ 2	**show vmps**	ダイナミック VLAN 再確認のステータスを確認します。

再確認間隔の変更

VMPS クライアントは、VMPS から受信する VLAN メンバーシップ情報を定期的に再確認します。再確認を実行する間隔を分数で設定できます。

クラスタ メンバー スイッチを設定する場合、このパラメータはコマンド スイッチ再確認の設定値以上にする必要があります。また、最初に **rcommand** 特権 EXEC コマンドを使用して、メンバー スイッチにログインする必要があります。

再確認間隔を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vmps reconfirm** *minutes*	ダイナミック VLAN メンバーシップの再確認の間隔を分数で入力します。指定できる範囲は 1 ～ 120 です。デフォルト値は 60 分です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vmps**	*Reconfirm Interval* フィールドでダイナミック VLAN 再確認のステータスを画面で確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no vmps reconfirm** グローバル コンフィギュレーション コマンドを使用します。

再試行回数の変更

スイッチが次のサーバに照会する前に VMPS に接続を試みる回数を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vmps retry** *count*	再試行回数を変更します。指定できる範囲は 1 ～ 10 です。デフォルト値は 3 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vmps**	*Server Retry Count* フィールドの設定を画面で確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no vmps retry** グローバル コンフィギュレーション コマンドを使用します。

VMPS のモニタ

VMPS の情報を表示するには、**show vmps** 特権 EXEC コマンドを使用します。スイッチは VMPS に関する次の情報を表示します。

- VMPS VQP Version：VMPS との通信に使用する VQP のバージョン。スイッチは VQP バージョン 1 を使用する VMPS に照会します。
- Reconfirm Interval：スイッチが VLAN と MAC アドレスの割り当てを再確認するまでに待機する分数。
- Server Retry Count：VQP が VMPS にクエリーを再送信する回数。この回数の試行後に応答が受信できない場合、スイッチはセカンダリ VMPS への照会を開始します。
- VMPS domain server：設定された VLAN メンバーシップ ポリシー サーバの IP アドレス。スイッチは、*current* とマーキングされたサーバにクエリーを送信します。*primary* とマーキングされたサーバはプライマリ サーバです。
- VMPS Action：最後に試行した再確認の結果。再確認の試行は、再確認間隔が経過すると自動的に実行されます。また、**vmps reconfirm** 特権 EXEC コマンドを入力するか、Network Assistant または SNMP と同等の機能を使用すると強制的に実行できます。

次に、**show vmps** 特権 EXEC コマンドの出力例を示します。

```
Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         other
```

ダイナミック アクセス ポート VLAN メンバーシップのトラブルシューティング

VMPS は、次の条件でダイナミック アクセス ポートをシャットダウンします。

- VMPS がセキュア モードであり、ホストのポートへの接続を許可していない場合。ホストがネットワークに接続するのを防ぐために、VMPS はポートをシャットダウンします。
- ダイナミック アクセス ポート上のアクティブなホストが 20 を超えている場合。

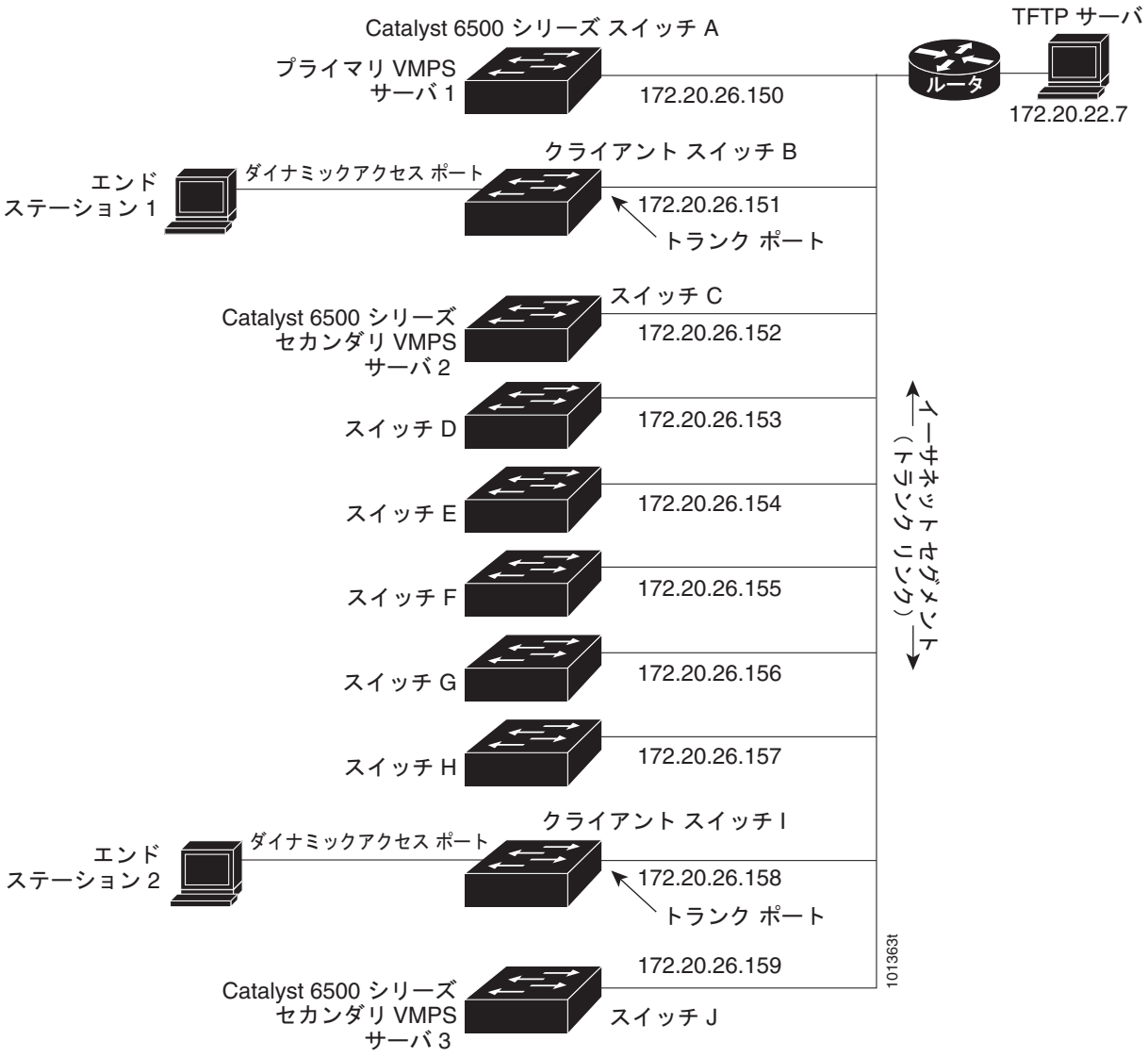
ディセーブルになっているダイナミック アクセス ポートを再びイネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドを入力したあとに、**no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

VMPS の設定例

図 16-4 に、ダイナミック アクセス ポートを持つ VMPS サーバ スイッチおよび VMPS クライアント スイッチのあるネットワークを示します。この例では、次の前提を適用しています。

- VMPS サーバと VMPS クライアントが別のスイッチである。
- Catalyst 6500 シリーズのスイッチ A がプライマリ VMPS サーバである。
- Catalyst 6500 シリーズのスイッチ C とスイッチ J はセカンダリ VMPS サーバである。
- エンド ステーションがクライアントのスイッチ B とスイッチ I に接続されている。
- データベース コンフィギュレーション ファイルは、IP アドレス 172.20.22.7 の TFTP サーバに格納されている。

図 16-4　　ダイナミック ポート VLAN メンバーシップの設定



CHAPTER 17

VTP の設定

この章では、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）と VLAN データベースを使用して、IE 3000 スイッチで VLAN を管理する方法について説明します。この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

VTP の概要

VTP はレイヤ 2 のメッセージング プロトコルであり、ネットワーク全体にわたって VLAN（仮想 LAN）の追加、削除、名前変更などを管理することにより、VLAN 設定の整合性を維持します。VTP を使用すると、VLAN 名の重複、無効な VLAN タイプの指定、セキュリティ違反などの問題を引き起こす可能性がある設定の誤りや設定の矛盾を最小限に抑えることができます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 つまたは複数のスイッチ上で集中的に設定の変更を行い、その変更をネットワーク上の他のスイッチに自動的に伝達することができます。VTP を使用しない場合、VLAN に関する情報を他のスイッチに送信できません。

VTP は、更新が 1 つのスイッチ上で行われ、VTP を介してドメイン内の他のスイッチに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同じドメイン内の複数のスイッチ上で同時に行われ、その結果、VLAN データベースに矛盾が生じる環境では、VTP は適切に動作しません。

スイッチでは、1005 個の VLAN がサポートされます。ただし、ルーテッド ポートの数、SVI、およびその他の設定済み機能がスイッチ ハードウェアの使用法に影響を及ぼします。使用可能な最大数のハードウェア リソースをすでに使用しているスイッチが新しい VLAN の VTP から通知を受けた場合、そのスイッチは使用可能なハードウェアが不足していることを示すメッセージを送信し、VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力には、VLAN が中断ステートになっていることが示されます。

VTP バージョン 1 およびバージョン 2 では、標準範囲 VLAN（VLAN ID 1 ～ 1005）だけがサポートされます。Cisco IOS Release 12.2(52)SE 以降では、VTP バージョン 3 がサポートされます。VTP バージョン 3 では、VLAN の全範囲（VLAN 1 ～ 4094）がサポートされます。拡張範囲 VLAN（VLAN 1006 ～ 4094）は、VTP バージョン 3 でだけサポートされます。ドメイン内に拡張 VLAN が設定されている場合、VTP バージョン 3 から VTP バージョン 2 に変換できません。

ここでは、次の概念情報について説明します。

VTP ドメイン

VTP ドメイン（別名、VLAN 管理ドメイン）は、1 つのスイッチ、または共通管理下にあり、同じ VTP ドメイン名を共有する、相互接続された複数のスイッチで構成されます。1 つのスイッチが所属できる VTP ドメインは 1 つだけです。ドメインのグローバル VLAN 設定を変更します。

デフォルトでは、スイッチはトランク リンク（複数の VLAN のトラフィックを伝送するリンク）を介してドメインに関するアドバタイズを受信するか、またはユーザがドメイン名を設定しない限り、VTP 非管理ドメイン ステートのままです。管理ドメイン名が指定されるか、または学習されるまで、VTP サーバ上で VLAN を作成または変更できず、VLAN 情報は ネットワーク上に伝播されません。

スイッチは、トランク リンクを介して VTP アドバタイズを受信すると、管理ドメイン名および VTP 設定のリビジョン番号を継承します。スイッチは、別のドメイン名または古い設定のリビジョン番号が指定されたアドバタイズについては無視します。

注意　VTP ドメインに VTP クライアント スイッチを追加する前に、その VTP 設定リビジョン番号が、VTP ドメイン内の他のスイッチの設定リビジョン番号よりも小さいことを必ず確認してください。VTP ドメイン内のスイッチは、VTP 設定リビジョン番号が最も大きいスイッチの VLAN 設定を常に使用します。VTP ドメインのリビジョン番号よりも大きいリビジョン番号を持つスイッチを追加した場合、そのスイッチは VTP サーバおよび VTP ドメインからの VLAN 情報をすべて消去する可能性があります。VTP 設定リビジョン番号を確認およびリセットする手順については、「VTP ドメインへの VTP クライアント スイッチの追加」（P.17-16）を参照してください。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのスイッチに伝播されます。VTP アドバタイズは、IEEE 802.1Q を含むすべての IEEE トランク接続を介して送信されます。VTP は、複数の LAN タイプの VLAN に、一意の名前と内部インデックスの対応付けをダイナミックにマッピングします。このマッピングにより、ネットワーク管理者が装置を管理するための作業負担が大幅に軽減されます。

スイッチを VTP トランスペアレント モードに設定した場合、VLAN の作成および変更は可能ですが、その変更はドメイン内の他のスイッチには送信されず、個々のスイッチにだけ適用されます。ただし、スイッチが VTP トランスペアレント モードのときに行われた設定変更は、スイッチの実行コンフィギュレーションに保存されます。また、スイッチのスタートアップ コンフィギュレーション ファイルに保存することもできます。

ドメイン名とパスワードの設定時の注意事項については、「VTP 設定時の注意事項」（P.17-8）を参照してください。

VTP のモード

サポートされているスイッチは、表 17-1 に示すいずれかの VTP モードに設定できます。

表 17-1　VTP のモード

VTP モード	説明
VTP サーバ	VTP サーバ モードでは、VLAN の作成、変更、および削除を行うことができます。また、VTP ドメイン全体に対して他の設定パラメータ（VTP バージョンなど）を指定できます。VTP サーバは、同一 VTP ドメイン内の他のスイッチに VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて VLAN 設定を他のスイッチと同期化します。 VTP サーバがデフォルトのモードです。 **（注）** VTP サーバ モードでは、VLAN 設定は NVRAM（不揮発性 RAM）に保存されます。スイッチが NVRAM に設定を書き込むときに障害を検出した場合、VTP モードは自動的にサーバ モードからクライアント モードに切り替わります。この場合、NVRAM が正常に動作するまで、スイッチを VTP サーバ モードに戻すことはできません。
VTP クライアント	VTP クライアントは、VTP サーバと同様に動作し、VTP 更新をトランクで送受信しますが、VTP クライアント上で VLAN の作成、変更、または削除を行うことはできません。VLAN は、サーバ モードになっている、ドメイン内の別のスイッチで設定します。 VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM に保存されません。VTP バージョン 3 のクライアント モードでは、VLAN 設定は NVRAM に保存されます。
VTP トランスペアレント	VTP トランスペアレント スイッチは、VTP に関与しません。VTP トランスペアレント スイッチは、VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて同期化することもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレント スイッチは、トランク インターフェイスを介して他のスイッチから受信した VTP アドバタイズを転送します。VTP トランスペアレント モードのスイッチでは、VLAN の作成、変更、および削除を行うことができます。 VTP バージョン 1 および 2 で拡張範囲 VLAN を作成する場合は、スイッチが VTP トランスペアレント モードになっている必要があります。VTP バージョン 3 では、クライアント モードまたはサーバ モードでの拡張範囲 VLAN の作成もサポートされます。「拡張範囲 VLAN の設定」（P.16-11）を参照してください。 VTP バージョン 1 および 2 でプライベート VLAN を作成する場合は、スイッチが VTP トランスペアレント モードになっている必要があります。また、プライベート VLAN を設定するときに、VTP モードをトランスペアレント モードからクライアント モードまたはサーバ モードに変更できません。VTP バージョン 3 では、クライアント モードおよびサーバ モードでのプライベート VLAN もサポートされます。第 19 章「プライベート VLAN の設定」を参照してください。 スイッチが VTP トランスペアレント モードになっている場合、VTP および VLAN の設定は NVRAM に保存されますが、他の スイッチにはアドバタイズされません。このモードでは、VTP モードおよびドメイン名はスイッチの実行コンフィギュレーション ファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。
VTP オフ	VTP オフ モードのスイッチは、トランク上でアドバタイズを転送しないことを除いて、VTP トランスペアレント スイッチと同様に機能します。

VTP アドバタイズ

VTP ドメイン内の各スイッチは、予約されたマルチキャスト アドレスに対して、各トランク ポートからグローバル コンフィギュレーション アドバタイズを定期的に送信します。ネイバー スイッチは、このアドバタイズを受信し、必要に応じて各自の VTP および VLAN 設定を更新します。

（注）　VTP アドバタイズはトランク ポートで送受信されるので、少なくとも 1 つのトランク ポートがスイッチに設定されていること、およびそのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。トランク ポートの詳細については、「VLAN トランクの設定」（P.16-15）を参照してください。

VTP アドバタイズは、次のグローバル ドメイン情報を配布します。

- VTP ドメイン名
- VTP 設定のリビジョン番号
- 更新 ID および更新タイムスタンプ
- 各 VLAN の Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズを含めた MD5 ダイジェスト VLAN 設定
- フレーム形式

VTP アドバタイズは、設定済みの各 VLAN に対して、次のグローバル ドメイン情報を配布します。

- VLAN ID（IEEE 802.1Q）
- VLAN 名
- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、プライマリ サーバ ID、インスタンス番号、および開始インデックスも VTP アドバタイズに含まれます。

VTP バージョン 2

ネットワークで VTP を使用する場合は、使用する VTP のバージョンを決定する必要があります。デフォルトでは、VTP はバージョン 1 で動作します。

VTP バージョン 2 では、バージョン 1 ではサポートされない次の機能がサポートされます。

- トークン リング サポート：VTP バージョン 2 では、Token Ring Bridge Relay Function（TrBRF; トークン リング ブリッジ リレー機能）および Token Ring Concentrator Relay Function（TrCRF; トークン リング コンセントレータ リレー機能）VLAN がサポートされます。トークン リング VLAN の詳細については、「標準範囲 VLAN の設定」（P.16-5）を参照してください。
- 認識不能な Type-Length-Value（TLV）のサポート：VTP サーバまたはクライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。スイッチが VTP サーバ モードで動作している場合、認識不能な TLV は NVRAM に保存されます。
- バージョン依存型トランスペアレント モード：VTP バージョン 1 の場合、VTP トランスペアレント スイッチは、VTP メッセージの中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限ってメッセージを転送します。VTP バージョン 2 では、1 つのドメインだけがサポートされます。そのため、トランスペアレント モードでは、バージョンとドメイン名を調べずに VTP メッセージを転送します。

- 整合性検査：VTP バージョン 2 では、CLI または SNMP を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

VTP バージョン 3

VTP バージョン 3 では、バージョン 1 またはバージョン 2 ではサポートされない次の機能がサポートされます。

- 拡張認証：認証を **hidden** または **secret** として設定できます。**hidden** の場合、パスワードの秘密キーは VLAN データベースに保存されますが、コンフィギュレーションのプレーン テキストには表示されません。代わりに、パスワードに関連付けられているキーが 16 進数形式で実行コンフィギュレーションに保存されます。ドメイン内でテイクオーバー コマンドを入力する場合は、パスワードを再入力する必要があります。**secret** キーワードを入力すると、パスワードの秘密キーを直接設定できます。
- 拡張範囲 VLAN（VLAN 1006 ～ 4094）データベース伝播のサポート。VTP バージョン 1 および 2 では、VLAN 1 ～ 1005 だけが伝播されます。拡張 VLAN が設定されている場合、VTP バージョン 3 からバージョン 1 または 2 に変換できません。

（注）　VTP プルーニングは、依然として VLAN 1 ～ 1005 にだけ適用されます。また、VLAN 1002 ～ 1005 は引き続き予約されており、変更できません。

- プライベート VLAN のサポート。
- ドメイン内の任意のデータベースに対するサポート。バージョン 3 では、VTP 情報だけでなく、Multiple Spanning Tree（MST; 多重スパニング ツリー）プロトコル データベース情報も伝播されます。VTP プロトコルのインスタンスは、VTP を使用する VTP プロトコルごとに個別に実行されます。
- VTP プライマリ サーバおよび VTP セカンダリ サーバ。VTP プライマリ サーバは、データベース情報を更新し、システム内のすべての装置で受け入れられる更新を送信します。VTP セカンダリ サーバは、更新された VTP 設定をプライマリ サーバから受信し、それを NVRAM にバックアップすることしかできません。

  デフォルトでは、装置はすべてセカンダリ サーバとして起動します。プライマリ サーバを指定するには、**vtp primary** 特権 EXEC コマンドを入力します。プライマリ サーバ ステータスが必要になるのは、管理者がデータベースを更新するためにドメイン内でテイクオーバー メッセージを発行するときだけです。VTP ドメインは、プライマリ サーバなしでも正常に機能します。装置のリロードまたはドメイン パラメータの変更が行われると、スイッチでパスワードが設定されている場合でも、プライマリ サーバ ステータスが失われます。
- トランク（ポート）単位で VTP のオン / オフを切り替えるオプション。[**no**] **vtp** インターフェイス コンフィギュレーション コマンドを入力すると、ポート単位で VTP をイネーブルおよびディセーブルにできます。トランキング ポートの VTP をディセーブルにすると、そのポートの VTP インスタンスがすべてディセーブルになります。同じポート上で、MST データベースの VTP を *オフ* に設定し、VLAN データベースの VTP を *オン* に設定できません。

  VTP モードをグローバルにオフに設定すると、システム内のすべてのトランキング ポートにその設定が適用されます。ただし、VTP インスタンス単位でオン / オフを指定できます。たとえば、MST データベースの VTP を *オフ* にした状態で、スイッチを VLAN データベースの VTP サーバとして設定することができます。

VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先装置に到達するために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、ネットワークで使用可能な帯域幅が増えます。VTP プルーニングを使用しない場合、スイッチは、ブロードキャスト トラフィック、マルチキャスト トラフィック、および不明なユニキャスト トラフィックを、受信スイッチがそれらのトラフィックを廃棄した場合でも、VTP ドメイン内のすべてのトランク リンクにフラッディングします。VTP プルーニングは、デフォルトではディセーブルに設定されています。

VTP プルーニングは、プルーニング適格リストに指定された、トランク ポート上の VLAN への不要なフラッディング トラフィックをブロックします。プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、VLAN 2 ～ 1001 がプルーニング適格のトランク ポートです。VLAN がプルーニング不適格として設定されている場合は、フラッディングが継続します。VTP プルーニングは、すべての VTP バージョンでサポートされます。

図 17-1 に、VTP プルーニングを使用しない場合のスイッチド ネットワークを示します。スイッチ A のポート 1 およびスイッチ D のポート 2 は、Red という VLAN に割り当てられています。スイッチ A に接続されたホストからブロードキャストが送信された場合、スイッチ A はこのブロードキャストをフラッディングします。Red VLAN にポートを持たないスイッチ C、E、F も含めて、ネットワーク内のすべてのスイッチがこのブロードキャストを受信します。

図 17-1　VTP プルーニングを使用しない場合のフラッディング トラフィック

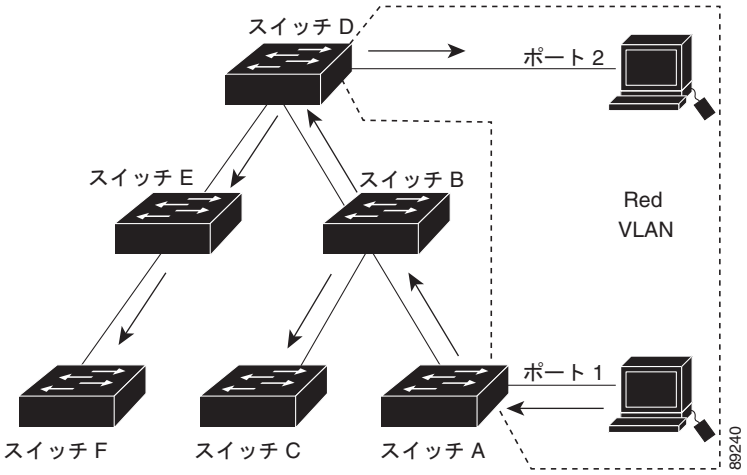
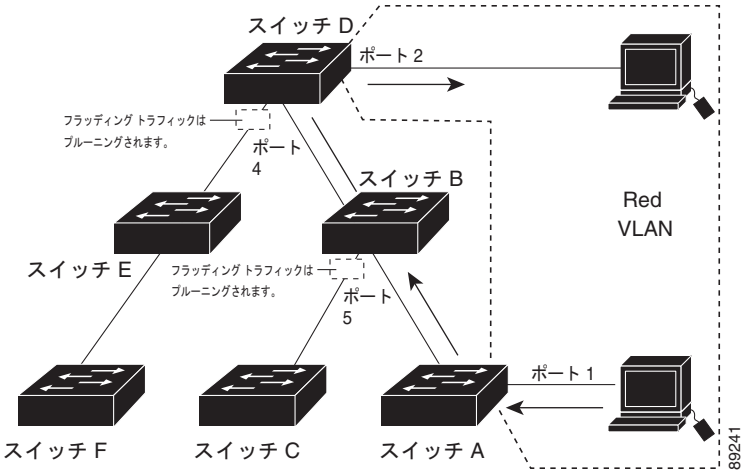


図 17-2 に、VTP プルーニングをイネーブルにした場合のスイッチド ネットワークを示します。Red VLAN のトラフィックは図に示すリンク（スイッチ B のポート 5、スイッチ D のポート 4）でプルーニングされるので、スイッチ A からのブロードキャスト トラフィックは、スイッチ C、E、F には転送されません。

図 17-2　VTP プルーニングで最適化されたフラッディング トラフィック



VTP サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。VLAN をプルーニング適格または不適格にした場合、その VLAN のプルーニング適格性の影響を受けるのはそのトランクだけです（VTP ドメイン内のすべてのスイッチに影響するわけではありません）。

「VTP プルーニングのイネーブル化」（P.17-15）を参照してください。VTP プルーニングは、イネーブルにしてから数秒後に有効になります。プルーニング不適格の VLAN からのトラフィックは、VTP プルーニングの対象になりません。VLAN 1 および VLAN 1002 ～ 1005 は常にプルーニング不適格です。これらの VLAN からのトラフィックをプルーニングできません。拡張範囲 VLAN（VLAN ID が 1006 以上）もプルーニング不適格です。

VTP プルーニングは、VTP トランスペアレント モードで動作するように設計されていません。ネットワーク内の 1 つまたは複数のスイッチが VTP トランスペアレント モードになっている場合は、次のいずれかを実行する必要があります。

- ネットワーク全体で VTP プルーニングをオフにする。
- VTP トランスペアレント スイッチのアップストリームにあるスイッチのトランク上の VLAN をすべてプルーニング不適格にすることで、VTP プルーニングをオフにする。

インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します（「プルーニング適格リストの変更」（P.16-21）を参照）。VTP プルーニングは、インターフェイスがトランキングを実行している場合に動作します。VTP ドメインに対して VTP プルーニングが設定されているかどうか、指定された VLAN が存在しているかどうか、およびインターフェイスがトランキングを現在実行しているかどうかに関係なく、VLAN プルーニング適格性を設定できます。

VTP の設定

ここでは、次の設定情報について説明します。

- 「VTP プルーニングのイネーブル化」（P.17-15）
- 「ポート単位での VTP の設定」（P.17-16）
- 「VTP ドメインへの VTP クライアント スイッチの追加」（P.17-16）

VTP のデフォルト設定

表 17-2 に、VTP のデフォルト設定を示します。

表 17-2　VTP のデフォルト設定

機能	デフォルト設定
VTP ドメイン名	ヌル。
VTP モード（VTP バージョン 1 およびバージョン 2）	サーバ。
VTP モード（VTP バージョン 3）	このモードは、バージョン 3 に変換する前の VTP バージョン 1 およびバージョン 2 のモードと同じです。
VTP バージョン	バージョン 1。
MST データベース モード	トランスペアレント。
VTP バージョン 3 サーバ タイプ	セカンダリ。
VTP パスワード	なし。
VTP プルーニング	ディセーブル。

VTP 設定時の注意事項

VTP パスワード、バージョン、VTP ファイル名、更新された VTP 情報を提供するインターフェイス、ドメイン名、およびモードを設定したり、プルーニングをディセーブルまたはイネーブルにするには、**vtp** グローバル コンフィギュレーション コマンドを使用します。使用可能なキーワードの詳細については、このリリースに対応するコマンド リファレンスのコマンドの説明を参照してください。VTP 情報は、VTP VLAN データベースに保存されます。VTP モードがトランスペアレントである場合、VTP ドメイン名とモードはスイッチの実行コンフィギュレーション ファイルにも保存されます。**copy running-config startup-config** 特権 EXEC コマンドを入力すると、この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存できます。スイッチをリセットする場合に VTP モードをトランスペアレントとして保存するときは、このコマンドを使用する必要があります。

VTP 情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存してスイッチを再起動した場合、設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベースの VTP モードがトランスペアレントで、VLAN データベースの VTP ドメイン名がスタートアップ コンフィギュレーション ファイルと一致する場合、VLAN データベースは無視（消去）されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーションの VTP モードまたはドメイン名が VLAN データベースと一致しない場合、ドメイン名、VTP モード、および最初の 1005 個の VLAN の設定には、VLAN データベースの情報が使用されます。

ドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。VTP ドメイン内のすべてのスイッチに同じドメイン名を設定する必要があります。VTP トランスペアレント モードのスイッチは、他のスイッチと VTP メッセージを交換しません。したがって、それらのスイッチについては、VTP ドメイン名を設定する必要はありません。

（注） NVRAM および DRAM のストレージが十分にある場合は、VTP ドメイン内のすべてのスイッチを VTP サーバ モードにしてください。

注意 すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメインを設定しないでください。VTP ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の 1 つ以上のスイッチを VTP サーバ モードに設定してください。

パスワード

VTP ドメインのパスワードを設定できますが、パスワードは必須ではありません。ドメインのパスワードを設定する場合は、すべてのドメイン スイッチで同じパスワードを使用する必要があります。また、管理ドメイン内の各スイッチでパスワードを設定する必要があります。パスワードが設定されていないスイッチ、または誤ったパスワードが設定されたスイッチは、VTP アドバタイズを拒否します。

ドメインにパスワードを設定した場合、VTP 設定なしで起動したスイッチは、正しいパスワードが設定されない限り、VTP アドバタイズを受け入れません。設定後、スイッチは同じパスワードおよびドメイン名を使用する VTP アドバタイズを次から受け入れます。

VTP 機能を備えた既存のネットワークに新しいスイッチを追加した場合、新しいスイッチは、適切なパスワードが設定された後にだけ、ドメイン名を取得します。

注意 ドメイン内の各スイッチに管理ドメイン パスワードを割り当てていない場合、VTP ドメイン パスワードを設定するときに、管理ドメインが正常に機能しません。

VTP バージョン

実装する VTP バージョンを決定するときには、次の注意事項に従ってください。

- VTP ドメイン内のすべてのスイッチで、同じドメイン名を使用する必要がありますが、同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応スイッチは、バージョン 2 がディセーブルになっている場合（デフォルトではバージョン 2 はディセーブル）、VTP バージョン 1 が稼動しているスイッチと同一の VTP ドメイン内で動作可能です。
- VTP バージョン 1 が稼動している VTP バージョン 2 対応スイッチが VTP バージョン 3 のアドバタイズを受信した場合、そのスイッチは自動的に VTP バージョン 2 に移行します。
- VTP バージョン 3 が稼動しているスイッチが、VTP バージョン 1 が稼動しているスイッチに接続されている場合、VTP バージョン 1 スイッチは VTP バージョン 2 に移行します。VTP バージョン 3 スイッチは、VTP バージョン 2 スイッチがデータベースを更新できるように、縮小バージョンの VTP パケットを送信します。
- VTP バージョン 3 が稼動しているスイッチは、拡張 VLAN が設定されている場合、バージョン 1 または 2 に移行できません。

- 同一 VTP ドメイン内のすべてのスイッチがバージョン 2 に対応する場合を除いて、スイッチ上で VTP バージョン 2 をイネーブルにしないでください。スイッチ上でバージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応スイッチでバージョン 2 がイネーブルになります。バージョン 1 専用のスイッチがある場合、そのスイッチはバージョン 2 がイネーブルになっているスイッチとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 のスイッチは、VTP バージョン 3 のアドバタイズを転送しないので、ネットワークのエッジに配置することを推奨します。
- 使用環境に TrBRF および TrCRF トークン リング ネットワークが含まれている場合、トークン リング VLAN スイッチングを正しく機能させるためには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークン リングおよびトークン リング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 では、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報は伝播されません。これらの VLAN は、各装置上で手動で設定する必要があります。VTP バージョン 3 では、拡張範囲 VLAN がサポートされます。拡張 VLAN が設定されている場合、VTP バージョン 3 から VTP バージョン 2 に変換できません。
- VTP バージョン 3 装置は、VTP バージョン 2 装置からのメッセージをトランク ポートで受信すると、そのトランク上で縮小バージョンの VLAN データベースを VTP バージョン 2 形式で送信します。VTP バージョン 3 装置は、トランク ポートで VTP バージョン 2 パケットを受信しない限り、そのトランク上で VTP バージョン 2 形式のパケットを送信しません。
- VTP バージョン 3 装置は、トランク ポート上で VTP バージョン 2 装置を検出すると、バージョン 2 およびバージョン 3 のネイバーが同じトランク上で共存できるように、VTP バージョン 2 パケットに加えて VTP バージョン 3 パケットの送信を続行します。
- VTP バージョン 3 装置は、VTP バージョン 2 または VTP バージョン 1 装置からの設定情報を受け入れません。
- 2 つの VTP バージョン 3 領域は、トランスペアレント モードで VTP バージョン 1 またはバージョン 2 領域を介してのみ通信できます。
- VTP バージョン 1 専用の装置は、VTP バージョン 3 装置と相互運用できません。

設定の要件

VTP を設定するときには、スイッチがドメイン内の他のスイッチとの間で VTP アドバタイズを送受信できるように、トランク ポートを設定する必要があります。

詳細については、「VLAN トランクの設定」（P.16-15）を参照してください。

クラスタ メンバー スイッチ上の VTP を VLAN に設定する場合は、**rcommand** 特権 EXEC コマンドを使用してメンバー スイッチにログインします。このコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

VTP バージョン 1 および 2 で拡張範囲 VLAN をスイッチ上に設定する場合は、スイッチが VTP トランスペアレント モードになっている必要があります。VTP バージョン 3 では、クライアント モードまたはサーバ モードでの拡張範囲 VLAN の作成もサポートされます。

VTP バージョン 1 および 2 では、プライベート VLAN はサポートされません。プライベート VLAN を設定する場合は、スイッチが VTP トランスペアレント モードになっている必要があります。スイッチ上にプライベート VLAN が設定されている場合は、VTP モードをトランスペアレントからクライアントまたはサーバ モードに変更しないでください。VTP バージョン 3 では、プライベート VLAN がサポートされます。

VTP モードの設定

VTP モードは次のいずれかに設定できます。

- スイッチが VTP サーバ モードになっている場合は、VLAN 設定を変更し、それをネットワーク全体に伝播することができます。
- スイッチが VTP クライアント モードになっている場合は、VLAN 設定を変更できません。クライアント スイッチは、VTP ドメイン内の VTP サーバから VTP 更新を受信し、それに従って設定を変更します。
- スイッチを VTP トランスペアレント モードに設定すると、そのスイッチで VTP がディセーブルになります。スイッチは、VTP 更新を送信せず、他のスイッチから受信した VTP 更新に従って動作することもありません。ただし、VTP バージョン 2 が稼動している VTP トランスペアレント スイッチは、受信した VTP アドバタイズをトランク リンク上で転送します。
- VTP オフ モードは、VTP アドバタイズが転送されないことを除いて、VTP トランスペアレント モードと同じです。

次の注意事項に従ってください。

- VTP バージョン 1 およびバージョン 2 で、拡張範囲 VLAN がスイッチ上に設定されている場合は、VTP モードをクライアントまたはサーバに変更できません。エラー メッセージが表示され、設定は許可されません。VTP バージョン 1 およびバージョン 2 では、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報は伝播されません。これらの VLAN は、各装置上で手動で設定する必要があります。

（注） VTP バージョン 1 および 2 では、拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を作成する前に、**vtp mode transparent** グローバル コンフィギュレーション コマンドを使用して VTP モードをトランスペアレントに設定する必要があります。スイッチが VTP トランスペアレント モードで起動するように、この設定をスタートアップ コンフィギュレーションに保存します。そうしないと、スイッチがリセットされて VTP サーバ モード（デフォルト）で起動した場合に、拡張範囲 VLAN 設定が失われます。

- VTP バージョン 3 では、拡張範囲 VLAN がサポートされます。拡張 VLAN が設定されている場合、VTP バージョン 3 から VTP バージョン 2 に変換できません。
- スイッチを VTP クライアント モードに設定すると、そのスイッチで VLAN データベース ファイル（vlan.dat）が作成されなくなります。その後でスイッチの電源を切断すると、スイッチの VTP 設定がデフォルトにリセットされます。スイッチの再起動後も VTP 設定が VTP クライアント モードに維持されるようにするには、VTP モードの前に VTP ドメイン名を設定する必要があります。

注意 すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメイン名を設定しないでください。VTP ドメイン名を設定すると、そのドメインの VLAN 設定を変更できなくなります。そのため、少なくとも 1 つのスイッチを VTP サーバに設定してください。

VTP モードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp domain** *domain-name*	VTP 管理ドメイン名を設定します。1 ～ 32 文字の名前を使用できます。共通管理下にある VTP サーバ モードまたはクライアント モードのスイッチはすべて、同じドメイン名に設定する必要があります。 サーバ モード以外のモードでは、このコマンドを省略できます。VTP サーバ モードでは、ドメイン名が必要です。スイッチが VTP ドメインにトランク接続されている場合、そのスイッチはドメイン内の VTP サーバからドメイン名を取得します。 他の VTP パラメータを設定する前に、VTP ドメインを設定する必要があります。
ステップ 3	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}	スイッチに VTP モード（クライアント、サーバ、トランスペアレント、またはオフ）を設定します。 （任意）データベースを設定します。 • **vlan**：設定済みのデータベースがない場合は、VLAN データベースがデフォルトになります。 • **mst**：多重スパニング ツリー（MST）データベース。 • **unknown**：不明なデータベース タイプ。
ステップ 4	**vtp password** *password*	（任意）VTP ドメインのパスワードを設定します。8 ～ 64 文字のパスワードを使用できます。VTP パスワードを設定する場合、ドメイン内の各スイッチに同じパスワードを割り当てないと、VTP ドメインは正常に機能しません。 VTP バージョン 3 で使用できるオプションについては、「VTP バージョン 3 パスワードの設定」（P.17-13）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show vtp status**	*VTP Operating Mode* フィールドおよび *VTP Domain Name* フィールドの設定を画面で確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をスタートアップ コンフィギュレーション ファイルに保存します。 **（注）**　スイッチの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードとドメイン名だけです。

設定したドメイン名は削除できません。スイッチを別のドメインに再度割り当てるしかありません。

別のモードのスイッチを VTP サーバ モードに戻すには、**no vtp mode** グローバル コンフィギュレーション コマンドを使用します。スイッチをパスワードのない状態に戻すには、**no vtp password** グローバル コンフィギュレーション コマンドを使用します。

次に、ドメイン名 *eng_group* とパスワード *mypassword* を使用して、スイッチを VTP サーバとして設定する例を示します。

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
Switch(config)# vtp password mypassword
```

```
Setting device VLAN database password to mypassword.
Switch(config)# end
```

VTP バージョン 3 パスワードの設定

VTP バージョン 3 を使用している場合にパスワードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp password** *password* [**hidden** | **secret**]	（任意）VTP ドメインのパスワードを設定します。8 ～ 64 文字のパスワードを使用できます。 • （任意）**hidden**：パスワード文字列から生成された秘密キーが nvam:vlan.dat ファイルに保存されるようにするには、**hidden** と入力します。VTP プライマリ サーバを設定してテイクオーバーを設定すると、パスワードを再入力するように求められます。 • （任意）**secret**：パスワードを直接設定するには、**secret** と入力します。secret として設定されるパスワードは、32 個の 16 進数文字を含んでいる必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vtp password**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をスタートアップ コンフィギュレーション ファイルに保存します。

パスワードを消去するには、**no vtp password** グローバル コンフィギュレーション コマンドを入力します。

次に、hidden としてパスワードを設定する例と、設定したパスワードが表示される例を示します。

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

VTP バージョン 3 プライマリ サーバの設定

VTP サーバを VTP プライマリ サーバとして設定するには、特権 EXEC モードから開始して、目的の VTP サーバで次の手順を実行します（バージョン 3 のみ）。この手順を実行すると、テイクオーバー操作が開始されます。

	コマンド	目的
ステップ 1	**vtp primary-server** [**vlan** | **mst**] [**force**]	スイッチの動作ステートをセカンダリ サーバ（デフォルト）からプライマリ サーバに変更し、その設定をドメインにアドバタイズします。スイッチのパスワードが **hidden** として設定されている場合は、パスワードを再入力するように求められます。 • （任意）**vlan**：VLAN データベースをテイクオーバー機能として選択します。これはデフォルトです。 • （任意）**mst**：多重スパニング ツリー（MST）データベースをテイクオーバー機能として選択します。 • （任意）**force**：**force** と入力すると、競合するサーバの設定が上書きされます。**force** と入力しなかった場合は、テイクオーバーの前に確認を求められます。

次に、hidden パスワードまたは secret パスワードが設定されている場合に、スイッチを VLAN データベース（デフォルト）のプライマリ サーバとして設定する例を示します。

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- --------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

VTP バージョンのイネーブル化

VTP バージョン 2 およびバージョン 3 は、デフォルトでディセーブルに設定されています。

- スイッチで VTP バージョン 2 をイネーブルにすると、VTP ドメイン内のすべての VTP バージョン 2 対応スイッチでバージョン 2 がイネーブルになります。VTP バージョン 3 をイネーブルにするには、各スイッチで手動で設定する必要があります。
- VTP バージョン 1 および 2 では、VTP サーバまたはトランスペアレント モードのスイッチでのみ、バージョンを設定できます。VTP バージョン 3 が稼動しているスイッチでは、拡張 VLAN およびプライベート VLAN が存在せず、hidden パスワードが設定されていない場合に限り、クライアント モードのときにバージョン 2 に変更できます。

注意　同一 VTP ドメイン内のスイッチで、VTP バージョン 1 と VTP バージョン 2 を相互運用できません。VTP ドメイン内のすべてのスイッチが VTP バージョン 2 をサポートしている場合を除いて、VTP バージョン 2 をイネーブルにしないでください。

- TrCRF および TrBRF トークン リング環境でトークン リング VLAN スイッチングを正しく機能させるためには、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があります。トークン リングおよびトークン リング Net の場合は、VTP バージョン 2 をディセーブルにする必要があります。
- VTP バージョン 3 は、Cisco IOS Release 12.2(52) SE 以降が実行されているスイッチでサポートされます。

注意　VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのインスタンス上で共存できます。

VTP バージョン設定時の注意事項については、「VTP バージョン」（P.17-9）を参照してください。

VTP バージョンを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp version** {**1** | **2** | **3**}	スイッチで VTP バージョンをイネーブルにします。デフォルトは VTP バージョン 1 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vtp status**	設定済みの VTP バージョンがイネーブルかどうかを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をスタートアップ コンフィギュレーション ファイルに保存します。

デフォルトの VTP バージョン 1 に戻すには、**no vtp version** グローバル コンフィギュレーション コマンドを使用します。

VTP プルーニングのイネーブル化

プルーニングを使用すると、トラフィックが宛先装置にアクセスするために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能な帯域幅が増えます。VTP プルーニングは、VTP サーバ モードのスイッチでだけイネーブルにできます。

VTP ドメインで VTP プルーニングをイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp pruning**	VTP 管理ドメインでプルーニングをイネーブルにします。 デフォルトでは、プルーニングはディセーブルに設定されています。プルーニングをイネーブルにする必要があるのは、VTP サーバ モードのスイッチ 1 台だけです。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vtp status**	*VTP Pruning Mode* フィールドの設定を画面で確認します。

VTP プルーニングをディセーブルにするには、**no vtp pruning** グローバル コンフィギュレーション コマンドを使用します。

VTP バージョン 1 および 2 では、VTP サーバでプルーニングをイネーブルにすると、VTP ドメイン全体でプルーニングがイネーブルになります。VTP バージョン 3 では、ドメイン内の各スイッチで手動でプルーニングをイネーブルにする必要があります。

プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、VLAN 2 ～ 1001 がトランク ポート上でプルーニング適格です。予約 VLAN および拡張範囲 VLAN はプルーニングできません。プルーニング適格の VLAN を変更するには、「プルーニング適格リストの変更」（P.16-21）を参照してください。

ポート単位での VTP の設定

VTP バージョン 3 では、ポート単位で VTP をイネーブルまたはディセーブルにできます。VTP をイネーブルにできるのは、トランク モードのポートだけです。着信および発信 VTP トラフィックはブロックされ、転送されません。

ポート上で VTP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**vtp**	指定されたポートで VTP をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config interface** *interface-id*	ポートへの変更を確認します。
ステップ 6	**show vtp status**	設定を確認します。

インターフェイスで VTP をディセーブルにするには、**no vtp** インターフェイス コンフィギュレーション コマンドを使用します。

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# vtp
Switch(config-if)# end
```

VTP ドメインへの VTP クライアント スイッチの追加

VTP ドメインに VTP クライアントを追加する前に、その VTP 設定リビジョン番号が、VTP ドメイン内の他のスイッチの設定リビジョン番号よりも小さいことを必ず確認してください。VTP ドメイン内のスイッチは、VTP 設定リビジョン番号が最も大きいスイッチの VLAN 設定を常に使用します。VTP バージョン 1 および 2 では、VTP ドメインのリビジョン番号よりも大きいリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからの VLAN 情報がすべて消去される場合があります。VTP バージョン 3 では、VLAN 情報は消去されません。

スイッチを VTP ドメインに追加する*前に*、スイッチの VTP 設定リビジョン番号を確認してリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**show vtp status**	VTP 設定リビジョン番号を確認します。 番号が 0 の場合は、VTP ドメインにスイッチを追加します。 番号が 0 よりも大きい場合は、次の手順を実行します。 **a.** ドメイン名をメモします。 **b.** 設定リビジョン番号をメモします。 **c.** 次の手順に進んでスイッチの設定リビジョン番号をリセットします。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain** *domain-name*	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。
ステップ 4	**end**	スイッチの VLAN 情報が更新され、設定リビジョン番号が 0 にリセットされます。特権 EXEC モードに戻ります。
ステップ 5	**show vtp status**	設定リビジョン番号が 0 にリセットされたことを確認します。
ステップ 6	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**vtp domain** *domain-name*	スイッチの元のドメイン名を入力します。
ステップ 8	**end**	スイッチの VLAN 情報が更新され、特権 EXEC モードに戻ります。
ステップ 9	**show vtp status**	（任意）ドメイン名がステップ 1 のものと同じであること、および設定リビジョン番号が 0 であることを確認します。

設定リビジョン番号をリセットしたら、VTP ドメインにスイッチを追加します。

（注）　**vtp mode transparent** グローバル コンフィギュレーション コマンドを使用すると、スイッチの VTP をディセーブルにしてから、VTP ドメイン内の他のスイッチに影響を与えることなく、スイッチの VLAN 情報を変更することができます。

VTP のモニタ

VTP をモニタするには、VTP 設定情報（ドメイン名、現在の VTP リビジョン、および VLAN 数）を表示します。スイッチで送受信されたアドバタイズに関する統計情報も表示できます。

表 17-3 に、VTP のアクティビティをモニタするための特権 EXEC コマンドを示します。

表 17-3　VTP モニタ コマンド

コマンド	目的
show vtp counters	送受信された VTP メッセージに関するカウンタを表示します。
show vtp devices [**conflict**]	ドメイン内のすべての VTP バージョン 3 装置に関する情報を表示します。conflict には、プライマリ サーバと競合する VTP バージョン 3 装置を指定します。スイッチがトランスペアレントまたはオフ モードになっている場合は、**show vtp devices** コマンドを実行しても、情報は表示されません。

表 17-3　VTP モニタ コマンド（続き）

コマンド	目的
show vtp interface [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスの VTP ステータスおよび設定を表示します。
show vtp password	VTP パスワードを表示します。表示されるパスワードの形式は、**hidden** キーワードが入力されたかどうか、およびスイッチで暗号化がイネーブルになっているかどうかによって異なります。
show vtp status	VTP スイッチ設定情報を表示します。

CHAPTER 18

音声 VLAN の設定

この章では、IE 3000 スイッチで音声 VLAN 機能を設定する方法について説明します。音声 VLAN は、Catalyst 6500 ファミリ スイッチの一部のマニュアルでは *補助 VLAN* と呼ばれています。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

音声 VLAN の概要

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。スイッチを Cisco 7960 IP Phone に接続すると、レイヤ 3 IP precedence 値とレイヤ 2 Class of Service（CoS; サービス クラス）値を使用して、IP Phone から音声トラフィックが送信されます。デフォルトでは、どちらの値も 5 に設定されます。データの送信が均質でない場合、IP Phone 通話の音質が低下することがあります。そのため、このスイッチでは、IEEE 802.1p CoS に基づく Quality of Service（QoS; サービス品質）をサポートしています。QoS では、分類およびスケジューリングを使用して、スイッチからのネットワーク トラフィックを予測可能な方法で送信します。QoS の詳細については、第 39 章「QoS の設定」を参照してください。

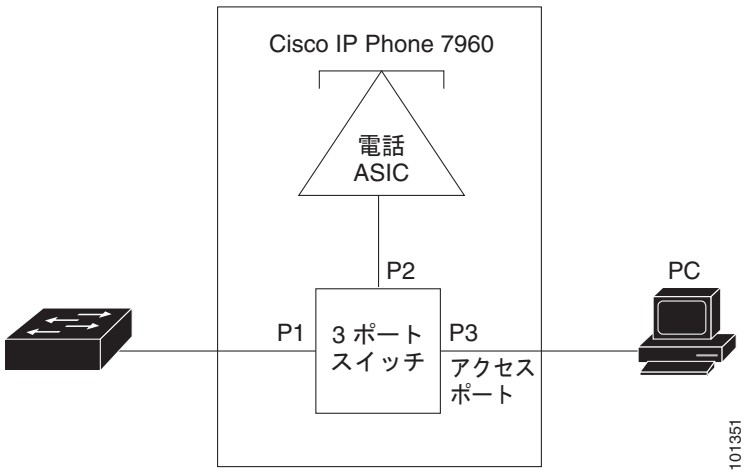
Cisco 7960 IP Phone は設定可能な装置であり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィック プライオリティを信頼するように、または上書きするようにスイッチを設定できます。

Cisco IP Phone は、図 18-1 に示すように、統合型 3 ポート内蔵 10/100 スイッチを装備しています。各ポートは、次の装置との接続専用です。

- ポート 1 は、スイッチまたはその他の Voice over IP（VoIP）装置に接続します。
- ポート 2 は、内蔵 10/100 インターフェイスで、IP Phone トラフィックを伝送します。
- ポート 3（アクセス ポート）は、PC またはその他の装置に接続します。

図 18-1 に、Cisco 7960 IP Phone の接続方法の例を示します。

図 18-1　スイッチに接続された Cisco 7960 IP Phone



Cisco IP Phone の音声トラフィック

接続された Cisco IP Phone を使用してアクセス ポートを設定し、1 つの VLAN を音声トラフィック用に、別の VLAN を IP Phone に接続された装置からのデータ トラフィック用にすることができます。スイッチのアクセス ポートを、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）パケットを送信するように設定することができます。CDP パケットは、接続する IP Phone に対して、次のいずれかの方法でスイッチに音声トラフィックを送信するように指示します。

- レイヤ 2 CoS プライオリティ値によるタグ付きの音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値によるタグ付きのアクセス VLAN による送信
- タグなしのアクセス VLAN（レイヤ 2 CoS プライオリティ値なし）による送信

（注） すべての設定において、音声トラフィックはレイヤ 3 IP precedence 値を伝送します（デフォルト値は音声トラフィックについては 5、音声制御トラフィックについては 3）。

Cisco IP Phone のデータ トラフィック

このスイッチでは、Cisco IP Phone のアクセス ポートに接続されている装置（図 18-1 を参照）からのタグ付きデータ トラフィック（IEEE 802.1Q フレーム タイプまたは IEEE 802.1p フレーム タイプのトラフィック）を処理することもできます。スイッチのレイヤ 2 アクセス ポートを、CDP パケットを送信するように設定することができます。CDP パケットは、接続する IP Phone に対して、IP Phone のアクセス ポートを次のいずれかのモードに設定するように指示します。

- 信頼モードでは、Cisco IP Phone のアクセス ポート経由で受信したすべてのトラフィックは、そのまま IP Phone を通過します。
- 信頼できないモードでは、Cisco IP Phone のアクセス ポート経由で受信した IEEE 802.1Q フレームまたは IEEE 802.1p フレームのすべてのトラフィックは、設定されたレイヤ 2 CoS 値を受け取ります。デフォルトのレイヤ 2 CoS 値は 0 です。信頼できないモードがデフォルト設定です。

（注）　Cisco IP Phone に接続されている装置からのタグなしトラフィックは、IP Phone のアクセス ポートの信頼状態にかかわらず、そのまま IP Phone を通過します。

音声 VLAN の設定

ここでは、次の設定情報について説明します。

音声 VLAN のデフォルト設定

音声 VLAN 機能は、デフォルトではディセーブルに設定されています。

音声 VLAN 機能がイネーブルに設定されている場合、タグなしのすべてのトラフィックは、ポートのデフォルトの CoS プライオリティに従って送信されます。

IEEE 802.1p または IEEE 802.1Q のタグ付きトラフィックでは、CoS 値は信頼されません。

音声 VLAN 設定時の注意事項

音声 VLAN の設定時の注意事項を次に示します。

- 音声 VLAN の設定はスイッチのアクセス ポート上でだけサポートされます。トランク ポート上では音声 VLAN の設定はサポートされません。音声 VLAN は、レイヤ 2 ポート上にだけ設定できます。

（注）　トランク ポートでは、通常の VLAN と同様に、任意の数の音声 VLAN を伝送できます。トランク ポートには音声 VLAN の設定は必要ありません。

- IP Phone が音声 VLAN 上で適切に通信するためには、音声 VLAN がスイッチ上に存在し、アクティブになっている必要があります。VLAN が存在するかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します（リストで表示されます）。VLAN がリストにない場合に音声 VLAN を作成する方法については、第 16 章「VLAN の設定」を参照してください。
- プライベート VLAN ポートには音声 VLAN を設定しないでください。
- 音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチの QoS をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力して信頼するポート信頼状態を設定することを推奨します。auto-QoS 機能を使用すると、これらの設定は自動的に指定されます。詳細については、第 39 章「QoS の設定」を参照してください。
- Cisco IP Phone に設定を送信するには、IP Phone に接続されたスイッチ ポートで CDP をイネーブルする必要があります（デフォルトでは、CDP はすべてのスイッチ インターフェイスでグローバルにイネーブルです）。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

- Cisco IP Phone とその IP Phone に接続されている装置が同じ VLAN にある場合、両方とも同じ IP サブネットに属している必要があります。次の条件にあてはまる場合、両方とも同じ VLAN にあります。
  - 両方が IEEE 802.1p フレームまたはタグなしフレームを使用する場合
  - Cisco IP Phone が IEEE 802.1p フレームを使用し、装置はタグなしフレームを使用する場合
  - Cisco IP Phone がタグなしフレームを使用し、装置は IEEE 802.1p フレームを使用する場合
  - Cisco IP Phone は IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである場合
- Cisco IP Phone とその IP Phone に接続されている装置は、同じ VLAN とサブネット内に存在していても、異なるフレーム タイプを使用する場合は、通信できません。同じサブネット内のトラフィックはルーティングされないからです（フレーム タイプが違う場合はルーティングされません）。
- 音声 VLAN では、スタティック セキュア MAC アドレスを設定できません。
- 音声 VLAN ポートは、次のポート タイプにすることもできます。
  - ダイナミック アクセス ポート。詳細については、「VMPS クライアント上でのダイナミック アクセス ポートの設定」（P.16-29）を参照してください。
  - IEEE 802.1x 認証ポート。詳細については、「802.1X 準備状態チェックの設定」（P.12-37）を参照してください。

  （注）　音声 VLAN が設定されていて Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1X をイネーブルにした場合、Cisco IP Phone とスイッチの接続が最大 30 秒切断されます。

  - 保護ポート。詳細については、「保護ポートの設定」（P.29-6）を参照してください。
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）または Remote SPAN（RSPAN; リモート SPAN）セッションの送信元ポートまたは宛先ポート。
  - セキュア ポート。詳細については、「ポート セキュリティの設定」（P.29-9）を参照してください。

  （注）　音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を、アクセス VLAN で許容されるセキュア アドレスの最大数に 2 を足した数に設定する必要があります。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが最大で 2 つ必要になります。IP Phone のアドレスは音声 VLAN 上で学習され、アクセス VLAN 上でも学習される場合があります。PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

Cisco 7960 IP Phone に接続されたポートの設定

Cisco 7960 IP Phone は、PC または他の装置との接続もサポートしているので、スイッチを Cisco IP Phone に接続するポートでは、混在トラフィックを伝送できます。ポートを設定して、Cisco IP Phone による音声トラフィックおよびデータ トラフィックの伝送方法を決定できます。

ここでは、次の設定情報について説明します。

- 「Cisco IP Phone の音声トラフィックの設定」（P.18-5）
- 「着信データ フレームのプライオリティの設定」（P.18-6）

Cisco IP Phone の音声トラフィックの設定

Cisco IP Phone に接続されたポートを、CDP パケットを IP Phone に送信するように設定できます。これにより、IP Phone による音声トラフィックの送信方法を設定することができます。IP Phone では、レイヤ 2 CoS 値を使用して、指定された音声 VLAN に IEEE 802.1Q フレームの音声トラフィックを伝送できます。IEEE 802.1p のプライオリティ タギングを使用すると、音声トラフィックにさらに高いプライオリティを設定し、すべての音声トラフィックをネイティブ（アクセス）VLAN 経由で転送できます。Cisco IP Phone では、タグなしの音声トラフィックを送信することも、独自の設定を使用してアクセス VLAN の音声トラフィックを送信することもできます。すべての設定において、音声トラフィックはレイヤ 3 IP precedence 値（デフォルトは 5）を伝送します。

ポート上で音声トラフィックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	IP Phone に接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**mls qos trust cos**	パケットの CoS 値を使用して着信トラフィック パケットを分類するように、インターフェイスを設定します。タグなしパケットの場合、ポートのデフォルト CoS 値が使用されます。 **（注）** ポートの信頼状態を設定する前に、**mls qos** グローバル コンフィギュレーション コマンドを使用して、QoS をグローバルにイネーブルにしておく必要があります。
ステップ 4	**switchport voice** {**detect cisco-phone** [**full-duplex**] | **vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}}	Cisco IP Phone による音声トラフィックの伝送方法を設定します。 • **detect** : Cisco IP Phone を検出して認識するようにインターフェイスを設定します。 • **cisco-phone** : switchport voice detect コマンドを初めて実装する場合、使用できるオプションはこのオプションだけです。デフォルトは、**no switchport voice detect cisco-phone** [**full-duplex**] です。 • **full-duplex** :（任意）全二重 Cisco IP Phone だけを受け入れるようにスイッチを設定します。 • *vlan-id* : すべての音声トラフィックが指定された VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。指定できる VLAN ID は、1 ～ 4094 です。 • **dot1p** : 音声トラフィックに IEEE 802.1p プライオリティ タギングを使用し、デフォルトのネイティブ VLAN（VLAN 0）を使用してすべてのトラフィックを伝送するように、IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。 • **none** : IP Phone が独自の設定を使用してタグなしの音声トラフィックを送信できるようにします。 • **untagged** : タグなしの音声トラフィックを送信するように IP Phone を設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show interfaces** *interface-id* **switchport** または	音声 VLAN の設定を確認します。
	show running-config interface *interface-id*	QoS および音声 VLAN の設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、Cisco IP Phone に接続されたポートを設定する例を示します。CoS 値を使用して着信トラフィックを分類し、音声トラフィックに IEEE 802.1p プライオリティ タギングを使用し、デフォルトのネイティブ VLAN（VLAN 0）を使用してすべてのトラフィックを伝送するように、ポートを設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

ポートをデフォルト設定に戻すには、**no switchport voice vlan** インターフェイス コンフィギュレーション コマンドを使用します。

次に、Cisco IP Phone 上で **switchport voice detect** をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport voice?
detect         detection enhancement keyword
vlan           VLAN for voice traffic
Switch(config-if)# switchport voice detect?
cisco-phone    Cisco IP Phone
Switch(config-if)# switchport voice detect cisco-phone?
full-duplex    Cisco IP Phone

Switch(config-if)# switchport voice detect cisco-phone full-duplex
full-duplex    full duplex keyword

Switch(config-if)# end
```

次に、Cisco IP Phone 上で **switchport voice detect** をディセーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# no switchport voice detect cisco-phone
Switch(config-if)# no switchport voice detect cisco-phone full-duplex
```

着信データ フレームのプライオリティの設定

Cisco IP Phone のポートには PC またはその他のデータ装置を接続できます。タグ付きデータ トラフィック（IEEE 802.1Q フレームまたは IEEE 802.1p フレーム）を処理するために、CDP パケットを送信するようにスイッチを設定して、Cisco IP Phone のアクセス ポートに接続する装置からのデータ パケットの送信方法を IP Phone に指示できます。PC では、CoS 値が割り当てられたパケットを生成できます。接続先装置から IP Phone のポートに送信されたフレームのプライオリティを変更しない（信頼する）または上書きする（信頼しない）ように、IP Phone を設定できます。

Cisco IP Phone の非音声ポートから受信したデータ トラフィックのプライオリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	Cisco IP Phone に接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport priority extend** {**cos** *value* | **trust**}	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを設定します。 • **cos** *value* : PC または接続先装置から受信したプライオリティを指定された CoS 値で上書きするように、IP Phone を設定します。指定できる値は 0 ～ 7 の数値です。7 が最も高いプライオリティです。デフォルトのプライオリティは **cos** 0 です。 • **trust** : PC または接続先装置から受信したプライオリティを信頼するように、IP Phone のアクセス ポートを設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、PC または接続先装置から受信したフレームのプライオリティを変更しないように、Cisco IP Phone に接続されたポートを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport priority extend trust
Switch(config-if)# end
```

ポートをデフォルト設定に戻すには、**no switchport priority extend** インターフェイス コンフィギュレーション コマンドを使用します。

音声 VLAN の表示

インターフェイスの音声 VLAN 設定を表示するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを使用します。

CHAPTER 19

プライベート VLAN の設定

この章では、IE 3000 スイッチにプライベート VLAN を設定する手順について説明します。プライベート VLAN は、IP サービス イメージが稼動しているスイッチでだけサポートされます。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

（注） プライベート VLAN を設定する場合は、スイッチが VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）トランスペアレント モードになっている必要があります。第 17 章「VTP の設定」を参照してください。

プライベート VLAN の概要

プライベート VLAN 機能では、サービス プロバイダーが VLAN を使用する際に直面する 2 つの問題に対処します。

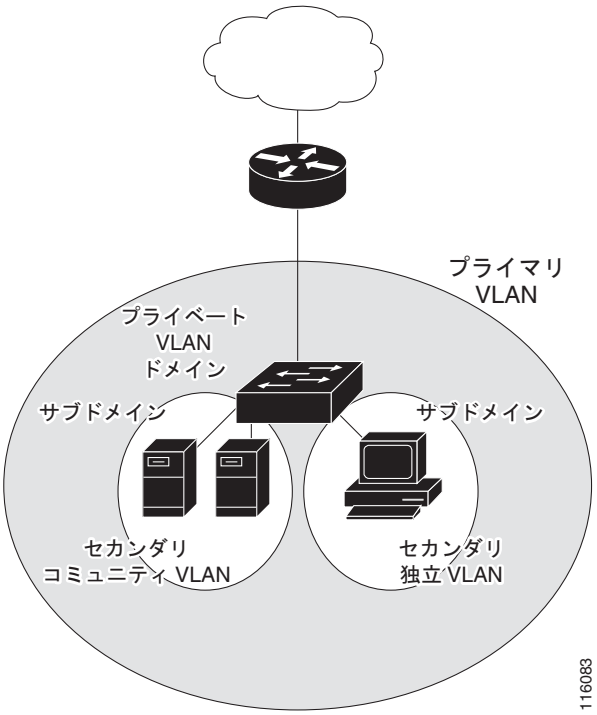
- スケーラビリティ：スイッチは最大 1005 個のアクティブ VLAN をサポートします。サービス プロバイダーがカスタマーごとに 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数は制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てます。これにより未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が生じます。

プライベート VLAN を使用することにより、スケーラビリティの問題が対処され、サービス プロバイダーにとっては IP アドレスの管理が便利になり、カスタマーにはレイヤ 2 セキュリティが提供されます。

プライベート VLAN では、通常の VLAN ドメインがサブドメインに分割され、複数の VLAN ペア（サブドメインごとに 1 つのペア）を設定できます。サブドメインは、*プライマリ* VLAN と *セカンダリ* VLAN で表されます。

プライベート VLAN 内のすべての VLAN ペアは、同じプライマリ VLAN を共有します。セカンダリ VLAN ID では、あるサブドメインを他のサブドメインと区別します。図 19-1 を参照してください。

図 19-1　プライベート VLAN ドメイン



セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN：独立 VLAN 内のポートは、レイヤ 2 レベルで相互に通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは、相互に通信できますが、レイヤ 2 レベルの他のコミュニティ上のポートとは通信できません。

プライベート VLAN は、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートには、次の 3 種類のアクセス ポートがあります。

- プロミスキャス：プロミスキャス ポートはプライマリ VLAN に属し、プライマリ VLAN に関連付けられているセカンダリ VLAN に属するコミュニティ ホスト ポートおよび独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立：独立ポートは、独立セカンダリ VLAN に属するホスト ポートです。このポートは、プロミスキャス ポート以外の、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN は、プロミスキャス ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、プロミスキャス ポートにだけ転送されます。
- コミュニティ：コミュニティ ポートは、コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN 内の他のポートおよびプロミスキャス ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートからレイヤ 2 で分離されています。

（注）　トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも伝送します。

プライマリ VLAN およびセカンダリ VLAN には、次のような特性があります。

- プライマリ VLAN：プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、単一方向のトラフィックのダウンストリームをプロミスキャス ポートから（独立およびコミュニティ）ホスト ポートおよび他のプロミスキャス ポートに伝送します。
- 独立 VLAN：プライベート VLAN には、独立 VLAN を 1 つだけ設定できます。独立 VLAN は、ホストからの単一方向トラフィック アップストリームを混合ポートおよびゲートウェイへ伝送するセカンダリ VLAN です。
- コミュニティ VLAN：コミュニティ VLAN は、アップストリーム トラフィックをコミュニティ ポートからプロミスキャス ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。1 つのプライベート VLAN 内に複数のコミュニティ VLAN を設定できます。

プロミスキャス ポートでは、1 つのプライマリ VLAN、1 つの独立 VLAN、および複数のコミュニティ VLAN だけを処理できます。レイヤ 3 ゲートウェイは、通常プロミスキャス ポート経由でスイッチに接続されます。プロミスキャス ポートを使用すると、さまざまな装置をアクセス ポイントとしてプライベート VLAN に接続できます。たとえば、プロミスキャス ポートを使用すると、管理ワークステーションからすべてのプライベート VLAN サーバをモニタまたはバックアップできます。

スイッチング環境では、個々のエンド ステーションまたは共通グループのエンド ステーションに、個別のプライベート VLAN や、関連付けられている IP サブネットを割り当てることができます。エンド ステーションがプライベート VLAN の外部と通信するには、デフォルト ゲートウェイだけと通信する必要があります。

プライベート VLAN を使用すると、エンド ステーションへのアクセスを次のように制御できます。

- エンド ステーションに接続された特定のインターフェイスを独立ポートとして設定すると、レイヤ 2 での通信が禁止されます。たとえば、エンド ステーションがサーバの場合は、サーバ間のレイヤ 2 通信が禁止されます。
- デフォルト ゲートウェイおよび選択されたエンド ステーション（たとえば、バックアップ サーバなど）に接続されたインターフェイスをプロミスキャス ポートとして設定すると、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできます。

複数の装置にわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他の装置にトランキングします。使用するプライベート VLAN の設定のセキュリティを確保して、プライベート VLAN として設定された VLAN が他の目的に使用されないようにするには、プライベート VLAN ポートがない装置を含めて、すべての中間装置でプライベート VLAN を設定します。

プライベート VLAN による IP アドレッシング方式

カスタマーごとに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

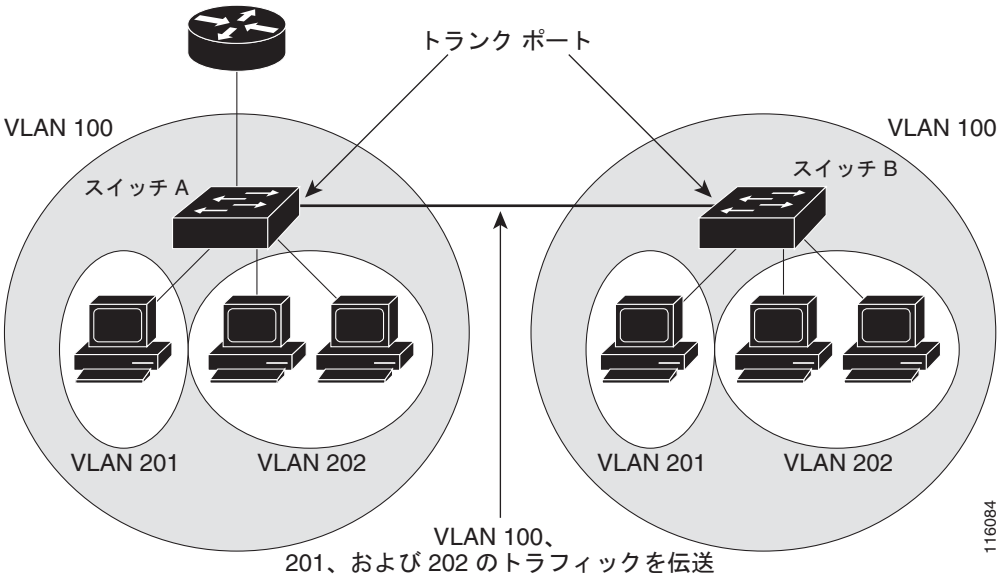
- カスタマー VLAN に アドレス ブロックを割り当てると、未使用の IP アドレスが生じます。
- VLAN 内の装置数が増加した場合、割り当てられるアドレス数はそれに対応できるほど多くはない場合があります。

これらの問題は、プライベート VLAN を使用することで軽減されます。この場合、プライベート VLAN 内のすべてのメンバーは、プライマリ VLAN に割り当てられる共通のアドレス空間を共有します。ホストはセカンダリ VLAN に接続され、Dynamic Host Configuration Protocol（DHCP）サーバが プライマリ VLAN に割り当てられたアドレス ブロックから IP アドレスを割り当てます。同じプライマリ VLAN 内の別のセカンダリ VLAN 内のカスタマー装置に後続の IP アドレスを割り当てられます。新しい装置が追加された場合、DHCP サーバはサブネット アドレスの大きなプールから次に使用可能なアドレスを装置に割り当てます。

複数のスイッチにまたがるプライベート VLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートは、プライマリ VLAN およびセカンダリ VLAN をネイバー スイッチに伝送します。トランク ポートは、プライベート VLAN を他の VLAN として扱います。複数のスイッチにまたがるプライベート VLAN の機能では、スイッチ A の独立ポートからのトラフィックは、スイッチ B の独立ポートに到達しません。図 19-2 を参照してください。

図 19-2　　複数のスイッチにまたがるプライベート VLAN



VLAN 100 = プライマリ VLAN
VLAN 201 = セカンダリ独立 VLAN
VLAN 202 = セカンダリ コミュニティ VLAN

VTP は、プライベート VLAN をサポートしないので、レイヤ 2 ネットワークのすべてのスイッチではプライベート VLAN を手動で設定する必要があります。ネットワーク内の一部のスイッチにプライマリ VLAN とセカンダリ VLAN のアソシエーションを設定しない場合、これらのスイッチ内のレイヤ 2 データベースは結合されません。これより、これらのスイッチ上のプライベート VLAN トラフィックが不要にフラッディングする可能性があります。

（注） スイッチにプライベート VLAN を設定するときには、ユニキャスト ルートとレイヤ 2 エントリとの間のシステム リソースのバランスを取るために、必ずデフォルトの Switch Database Management（SDM）テンプレートを使用してください。別の SDM テンプレートが設定されている場合は、**sdm prefer default** グローバル コンフィギュレーション コマンドを使用してデフォルトのテンプレートを設定します。第 10 章「SDM テンプレートの設定」を参照してください。

プライベート VLAN の他の機能との相互作用

プライベート VLAN には、次の各項で説明するように、他の機能との特殊な相互作用があります。

- 「プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック」（P.19-5）
- 「プライベート VLAN および SVI」（P.19-5）

「プライベート VLAN 設定時の注意事項」の「セカンダリ VLAN およびプライマリ VLAN の設定」（P.19-7）も参照してください。

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN 内の装置はレイヤ 2 レベルで相互に通信できますが、異なる VLAN のインターフェイスに接続されている装置とは、レイヤ 3 レベルで通信する必要があります。プライベート VLAN では、プロミスキャス ポートはプライマリ VLAN のメンバーで、ホスト ポートはセカンダリ VLAN に属しています。セカンダリ VLAN はプライマリ VLAN に関連付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで相互に通信できます。

通常の VLAN では、ブロードキャストはその VLAN 内のすべてのポートに転送されます。プライベート VLAN のブロードキャスト転送は、ブロードキャストを送信するポートにより異なります。

- 独立ポートは、ブロードキャストをプロミスキャス ポートまたはトランク ポートにだけ送信します。
- コミュニティ ポートは、ブロードキャストをすべてのプロミスキャス ポート、トランク ポート、および同じコミュニティ VLAN 内のポートに送信します。
- プロミスキャス ポートは、ブロードキャストをプライベート VLAN 内のすべてのポート（他のプロミスキャス ポート、トランク ポート、独立ポート、およびコミュニティ ポート）に送信します。

マルチキャスト トラフィックは、プライベート VLAN 境界を越えて、単一のコミュニティ VLAN 内でルーティングまたはブリッジングされます。マルチキャスト トラフィックは、同じ独立 VLAN 内のポート間または異なるセカンダリ VLAN 内のポート間で転送されません。

プライベート VLAN および SVI

レイヤ 3 スイッチでは、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）が VLAN のレイヤ 3 インターフェイスを表します。レイヤ 3 装置は、セカンダリ VLAN ではなく、プライマリ VLAN を介してだけプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイスはプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

- アクティブな SVI が設定された VLAN をセカンダリ VLAN として設定しようとする場合、SVI をディセーブルにしなければ設定は許可されません。
- セカンダリ VLAN として設定されている VLAN 上に SVI を作成しようとした場合、セカンダリ VLAN がレイヤ 3 ですでにマッピングされていると、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 でマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされます。

プライマリ VLAN がセカンダリ VLAN に関連付けられていて、マッピングされている場合、プライマリ VLAN 上のすべての設定はセカンダリ VLAN の SVI に伝播されます。たとえば、プライマリ VLAN の SVI に IP サブネットを割り当てる場合、このサブネットはプライベート VLAN 全体の IP サブネット アドレスとなります。

プライベート VLAN の設定

ここでは、次の設定情報について説明します。

プライベート VLAN の設定作業

プライベート VLAN を設定するには、次の手順を実行します。

ステップ 1　VTP モードをトランスペアレントに設定します。

ステップ 2　プライマリ VLAN およびセカンダリ VLAN を作成して、これらを関連付けします。「VLAN の設定およびプライベート VLAN への関連付け」（P.19-10）を参照してください。

（注）　VLAN がまだ作成されていない場合は、プライベート VLAN の設定プロセスを実行して、VLAN を作成します。

ステップ 3　インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」（P.19-12）を参照してください。

ステップ 4　インターフェイスをプロミスキャス ポートに設定して、プロミスキャス ポートをプライマリ VLAN およびセカンダリ VLAN のペアにマッピングします。「プライベート VLAN プロミスキャス ポートとしてのレイヤ 2 インターフェイスの設定」（P.19-13）を参照してください。

ステップ 5　VLAN 間ルーティングを使用している場合は、プライマリ SVI を設定して、セカンダリ VLAN をプライマリにマッピングします。「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」（P.19-14）を参照してください。

ステップ 6　プライベート VLAN の設定を確認します。

プライベート VLAN のデフォルト設定

プライベート VLAN は設定されていません。

プライベート VLAN 設定時の注意事項

プライベート VLAN 設定時の注意事項は、次のカテゴリに分類されます。

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定時には、次の注意事項に従ってください。

- スイッチで VTP バージョン 1 または 2 が稼動している場合は、VTP をトランスペアレント モードに設定する必要があります。プライベート VLAN を設定したあとで、VTP モードをクライアントまたはサーバに変更できません。VTP の詳細については、第 17 章「VTP の設定」を参照してください。VTP バージョン 3 では、すべてのモードでプライベート VLAN がサポートされます。
- VTP バージョン 1 または 2 では、プライベート VLAN を設定したあと、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレント モード設定およびプライベート VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存します。そうしないと、スイッチをリセットしたときにデフォルトの VTP サーバ モードになり、プライベート VLAN がサポートされなくなります。VTP バージョン 3 では、プライベート VLAN がサポートされます。
- VTP バージョン 1 およびバージョン 2 では、プライベート VLAN 設定が伝播されません。装置で VTP バージョン 3 が稼動していない場合は、プライベート VLAN ポートを使用する装置ごとに、プライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）は、プライベート VLAN に属することができます。
- プライマリ VLAN には、1 つの隔離 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行されるのは 1 つの Spanning Tree Protocol（STP; スパニング ツリー プロトコル）インスタンスだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。
- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにする場合、セカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定する際、プライマリ VLAN がすでに設定されている場合は、設定が有効になりません。
- プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- プライベート VLAN でトラフィックを伝送しない装置のトランクから、プライベート VLAN をプルーニングすることを推奨します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS; サービス品質）を適用できます。
- スティッキ ARP
  - スティッキ ARP エントリは、SVI およびレイヤ 3 インターフェイスで学習されるエントリです。これらのエントリは、期限切れになりません。

  - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属している SVI でだけサポートされます。
  - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、次のものでだけサポートされます。

    レイヤ 3 インターフェイス

    通常の VLAN に属している SVI

    プライベート VLAN に属している SVI

  ip sticky-arp *グローバル* コンフィギュレーション コマンドと **ip sticky-arp** *インターフェイス* コンフィギュレーション コマンドの使用の詳細については、このリリースのコマンド リファレンスを参照してください。

- プライマリ VLAN およびセカンダリ VLAN では VLAN マップを設定できます（「VLAN マップの設定」（P.38-31）を参照）。ただし、プライベート VLAN のプライマリ VLAN とセカンダリ VLAN には、同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内でレイヤ 2 転送される場合、入力側と出力側で同じ VLAN マップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップは入力側で適用されます。
  - ホスト ポートからプロミスキャス ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN で設定された VLAN マップが適用されます。
  - プロミスキャス ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN で設定された VLAN マップが適用されます。

  プライベート VLAN の特定の IP トラフィックをフィルタリングするには、プライマリ VLAN とセカンダリ VLAN の両方に VLAN マップを適用する必要があります。
- ルータ ACL はプライマリ VLAN SVI にだけ適用できます。ACL はプライマリ VLAN およびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを独立していても、ホストはレイヤ 3 で相互に通信できます。
- プライベート VLAN では、次の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能をサポートしています。
  - プライベート VLAN ポートを SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN-based SPAN（VSPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別にモニタすることができます。

プライベート VLAN ポートの設定

プライベート VLAN ポートの設定時には、次の注意事項に従ってください。

- ポートをプライマリ VLAN、独立 VLAN、またはコミュニティ VLAN に割り当てる場合は、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- Port Aggregation Protocol（PAgP; ポート集約プロトコル）または Link Aggregation Control Protocol（LACP）EtherChannel に属するポートを、プライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN 設定に含まれていると、ポートの EtherChannel 設定が非アクティブになります。

- 設定ミスによって STP ループが発生しないようにするため、および STP コンバージェンスを高速化するためには独立ホスト ポートおよびコミュニティ ホスト ポート上で PortFast および Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガードをイネーブルにします（第 23 章「オプションのスパニング ツリー機能の設定」を参照）。STP をイネーブルに設定すると、STP によってすべての PortFast 設定済みレイヤ 2 LAN ポートに BPDU ガード機能が適用されます。プロミスキャス ポートでは、PortFast および BPDU をイネーブルにしないでください。
- プライベート VLAN の設定で使用される VLAN を削除すると、この VLAN に関連付けられたプライベート VLAN ポートが非アクティブになります。
- プライベート VLAN ポートは、ネットワーク装置をトランク接続し、トランクからプライマリ VLAN およびセカンダリ VLAN が削除されていない限りさまざまなネットワーク装置上で使用できます。

他の機能との制限事項

プライベート VLAN を設定する場合、他の機能との間で次のような制限があることに留意してください。

（注）　場合によっては、エラー メッセージなしで設定が受け入れられますが、コマンドは無効になります。

- プライベート VLAN が設定されたスイッチにフォールバック ブリッジングを設定しないでください。
- スイッチで IGMP スヌーピングがイネーブルになっている場合（デフォルト）、スイッチでサポートされるプライベート VLAN ドメインは 20 個までです。
- Remote SPAN（RSPAN; リモート SPAN）VLAN をプライベート VLAN のプライマリ VLAN またはセカンダリ VLAN として設定しないでください。

  SPAN の詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。
- 次のその他の機能が設定されているインターフェイスに、プライベート VLAN ポートを設定しないでください。
  - ダイナミック アクセス ポート VLAN メンバーシップ
  - ダイナミック トランキング プロトコル（DTP）
  - ポート集約プロトコル（PagP）
  - Link Aggregation Control Protocol（LACP）
  - マルチキャスト VLAN レジストレーション（MVR）
  - 音声 VLAN
  - Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）
- プライベート VLAN ポートはセキュア ポートにはなれないので、保護ポートとして設定はできません。
- プライベート VLAN ポートに IEEE 802.1x ポートベース認証を設定できますが、IEEE 802.1x をポート セキュリティ、音声 VLAN、またはユーザ単位 ACL と一緒にプライベート VLAN ポートに設定しないでください。
- プライベート VLAN ホストまたはプロミスキャス ポートは、SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートとして設定した場合、ポートは非アクティブとなります。

- プライマリ VLAN のプロミスキャス ポート上でスタティック MAC アドレスを設定する場合は、すべての関連するセカンダリ VLAN にこれと同じスタティック アドレスを追加する必要があります。セカンダリ VLAN のホスト ポート上でスタティック MAC アドレスを設定する場合は、関連するプライマリ VLAN にこれと同じスタティック MAC アドレスを追加する必要があります。プライベート VLAN ポートからスタティック MAC アドレスを削除した場合は、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要があります。

（注）　プライベート VLAN の 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連する VLAN に複製されます。たとえば、セカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN に複製されます。元のダイナミック MAC アドレスが削除されるか、期限切れになった場合は、複製されたアドレスは MAC アドレス テーブルから削除されます。

- レイヤ 3 VLAN インターフェイスはプライマリ VLAN にだけ設定してください。

VLAN の設定およびプライベート VLAN への関連付け

プライベート VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

（注）　**private-vlan** コマンドは、VLAN コンフィギュレーション モードを終了するまで有効になりません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp mode transparent**	VTP モードをトランスペアレントに設定します（VTP をディセーブルにします）。
ステップ 3	**vlan** *vlan-id*	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定または作成します。VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan primary**	VLAN をプライマリ VLAN として指定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**vlan** *vlan-id*	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定または作成します。VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 7	**private-vlan isolated**	VLAN を独立 VLAN として指定します。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**vlan** *vlan-id*	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 10	**private-vlan community**	VLAN をコミュニティ VLAN として指定します。
ステップ 11	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**vlan** *vlan-id*	ステップ 2 で指定したプライマリ VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 13	**private-vlan association** [**add** | **remove**] *secondary_vlan_list*	セカンダリ VLAN をプライマリ VLAN に関連付けます。
ステップ 14	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 15	**show vlan private-vlan** [**type**] または **show interfaces status**	設定を確認します。
ステップ 16	**copy running-config startup config**	スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。プライベート VLAN 設定を保存するには、スイッチ スタートアップ コンフィギュレーション ファイルに VTP トランスペアレント モード設定とプライベート VLAN 設定を保存する必要があります。そうしないと、スイッチをリセットしたときにデフォルトの VTP サーバ モードになり、プライベート VLAN がサポートされなくなります。

セカンダリ VLAN をプライマリ VLAN と関連付ける際には、次の構文情報に注意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- *secondary_vlan_list* パラメータには、複数のコミュニティ VLAN ID を含めることができますが、独立 VLAN ID は 1 つしか含めることができません。
- セカンダリ VLAN をプライマリ VLAN に関連付けるには、*secondary_vlan_list* を入力するか、または *secondary_vlan_list* を指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN の関連付けを消去するには、*secondary_vlan_list* を指定して **remove** キーワードを使用します。
- これらのコマンドは、VLAN コンフィギュレーション モードを終了するまで有効になりません。

次に、VLAN 20 をプライマリ VLAN に、VLAN 501 を独立 VLAN に、VLAN 502 および 503 をコミュニティ VLAN に設定し、それらの VLAN をプライベート VLAN に関連付けて、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
20      503       community
20      504       non-operational
```

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定し、それをプライマリ VLAN およびセカンダリ VLAN に関連付けるには、特権 EXEC モードで次の手順を実行します。

（注）　独立 VLAN およびコミュニティ VLAN はセカンダリ VLAN です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するレイヤ 2 インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode private-vlan host**	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id*	レイヤ 2 ポートをプライベート VLAN に関連付けます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] **switchport**	設定を確認します。
ステップ 7	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスをプライベート VLAN ホスト ポートとして設定し、それをプライマリ VLAN のペアに関連付けて、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigatibethernet1/2
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 25
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/2 switchport
Name: Gi1/2
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 (VLAN0020) 25 (VLAN0025)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)

<output truncated>
```

プライベート VLAN プロミスキャス ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN プロミスキャス ポートとして設定し、それをプライマリ VLAN およびセカンダリ VLAN にマッピングするには、特権 EXEC モードで次の手順を実行します。

（注）　独立 VLAN およびコミュニティ VLAN はセカンダリ VLAN です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するレイヤ 2 インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode private-vlan promiscuous**	レイヤ 2 ポートをプライベート VLAN プロミスキャス ポートとして設定します。
ステップ 4	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list*	プライベート VLAN プロミスキャス ポートをプライマリ VLAN、および選択したセカンダリ VLAN にマッピングします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] **switchport**	設定を確認します。
ステップ 7	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 インターフェイスをプライベート VLAN プロミスキャス ポートとして設定する際には、次の構文情報に注意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- セカンダリ VLAN をプライベート VLAN プロミスキャス ポートにマッピングするには、*secondary_vlan_list* を入力するか、または *secondary_vlan_list* を指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライベート VLAN プロミスキャス ポートの間のマッピングを消去するには、*secondary_vlan_list* を指定して **remove** キーワードを使用します。

次に、インターフェイスをプライベート VLAN プロミスキャス ポートとして設定し、それをプライベート VLAN にマッピングする例を示します。インターフェイスは、プライマリ VLAN 20 のメンバーで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
Switch# configure terminal
Switch(config)# interface gigatibethernet1/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

プライマリ VLAN およびセカンダリ VLAN とスイッチ上のプライベート VLAN ポートを表示するには、**show vlan private-vlan** または **show interface status** 特権 EXEC コマンドを使用します。

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定して、セカンダリ VLAN を SVI にマッピングできます。

（注）　独立 VLAN およびコミュニティ VLAN はセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングして、プライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *primary_vlan_id*	プライマリ VLAN のインターフェイス コンフィギュレーション モードを開始し、VLAN を SVI として設定します。VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 3	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list*	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interface private-vlan mapping**	設定を確認します。
ステップ 6	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

（注）　**private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされるプライベート VLAN トラフィックにだけ作用します。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際には、次の構文情報に注意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- セカンダリ VLAN をプライマリ VLAN にマッピングするには、*secondary_vlan_list* を入力するか、または *secondary_vlan_list* を指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN の間のマッピングを消去するには、*secondary_vlan_list* を指定して **remove** キーワードを使用します。

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。プライマリ VLAN 10 では、プライベート VLAN 501 から 502 へのセカンダリ VLAN 入力トラフィックのルーティングが許可されます。

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
```

```
vlan10    501            isolated
vlan10    502            community
```

プライベート VLAN のモニタ

表 19-1　プライベート VLAN のモニタ コマンド

コマンド	目的
show interfaces status	所属する VLAN を含むインターフェイスのステータスを表示します。
show vlan private-vlan [**type**]	スイッチのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。

次に、**show vlan private-vlan** コマンドの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated           Gi1/1, Gi1/3
10      502       community          Gi1/5, Gi1/4

10      503       non-operational
```

CHAPTER 20

IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定

Virtual Private Network（VPN; 仮想私設網）は、共有インフラストラクチャにおいて、多くの場合はイーサネットベースで、複数のプライベート ネットワークでの同一のセキュリティ、プライオリティ、信頼性、および管理性の要件を使用して、企業規模の接続を提供します。トンネリングは、ネットワークを介して複数のカスタマーのトラフィックを伝送し、他のカスタマーのトラフィックに影響を与えずにカスタマーごとの VLAN と レイヤ 2 プロトコルの設定を維持する必要があるサービス プロバイダーのために設計された機能です。IE 3000 スイッチは、IP サービス イメージを稼動している場合に、IEEE 802.1Q トンネリングとレイヤ 2 プロトコル トンネリングをサポートします。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章の内容は次のとおりです。

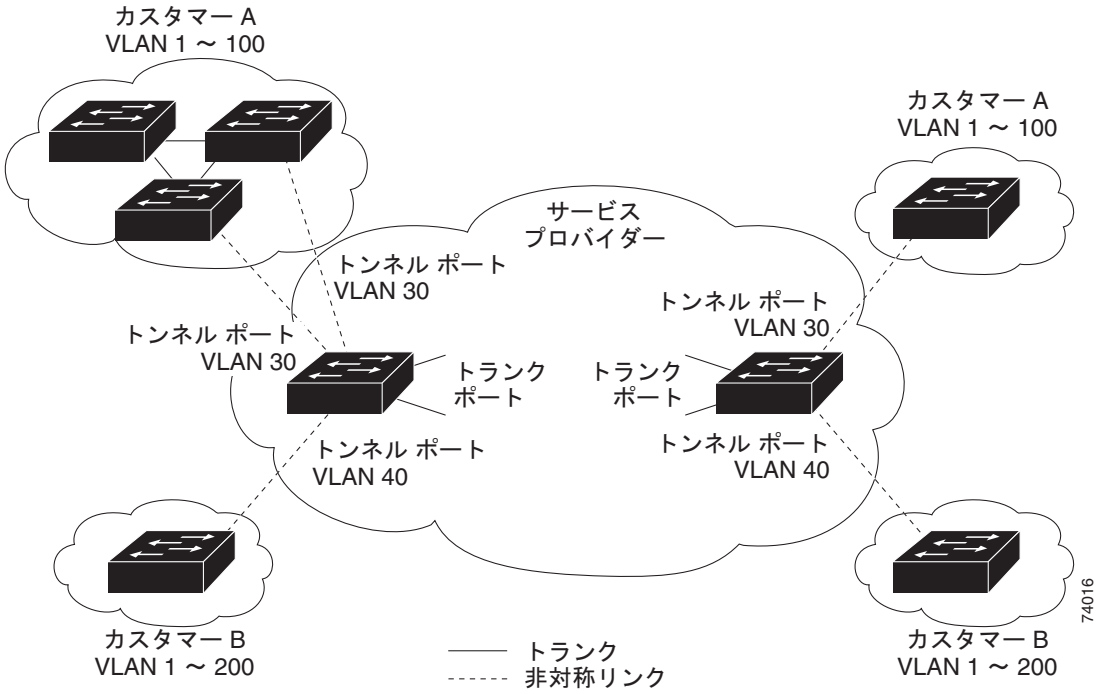
IEEE 802.1Q トンネリングの概要

サービス プロバイダーのビジネス カスタマーは多くの場合、サポートする VLAN ID と VLAN の番号に対する特定の要件を持っています。同じサービス プロバイダー ネットワーク内のさまざまなカスタマーによって必要とされる VLAN の範囲は重複する可能性があり、インフラストラクチャを通したカスタマーのトラフィックは混合される可能性があります。カスタマーごとに VLAN ID の一意の範囲を割り当てることによって、カスタマー設定が制限され、簡単に IEEE 802.1Q の仕様である VLAN 制限（4096）を超える場合があります。

IEEE 802.1Q トンネリング機能を使用することにより、サービス プロバイダーは単一の VLAN を使用して複数の VLAN があるカスタマーをサポートできます。カスタマー VLAN ID は保持され、別のカスタマーからのトラフィックは同じ VLAN 内にあるように表示されている場合でもサービス プロバイダー ネットワーク内で分離されます。IEEE 802.1Q トンネリングを使用することによって、VLAN 内 VLAN 階層構造を使用し、タグ付きパケットを再タグ付けして VLAN スペースを拡張します。IEEE 802.1Q トンネリングをサポートするように設定されたポートは、*トンネル ポート*といいます。トンネリングを設定する場合は、トンネル ポートをトンネリング専用の VLAN ID に割り当てます。カスタマーごとに個別のサービス プロバイダー VLAN ID が必要ですが、この VLAN ID でカスタマーの VLAN をすべてサポートできます。

通常の方法で適切な VLAN ID にタグ付けされたカスタマー トラフィックはカスタマー装置上の IEEE 802.1Q トランク ポートから発信し、サービス プロバイダー エッジ スイッチ上のトンネル ポートに着信します。カスタマー装置とエッジ スイッチの間のリンクは非対称です。これは、一端が IEEE 802.1Q トランク ポートとして設定され、もう一端がトンネル ポートとして設定されているからです。カスタマーごとに一意のアクセス VLAN ID に、トンネル ポート インターフェイスを割り当てます。図 20-1 を参照してください。

図 20-1　サービス プロバイダー ネットワークにおける IEEE 802.1Q トンネル ポート

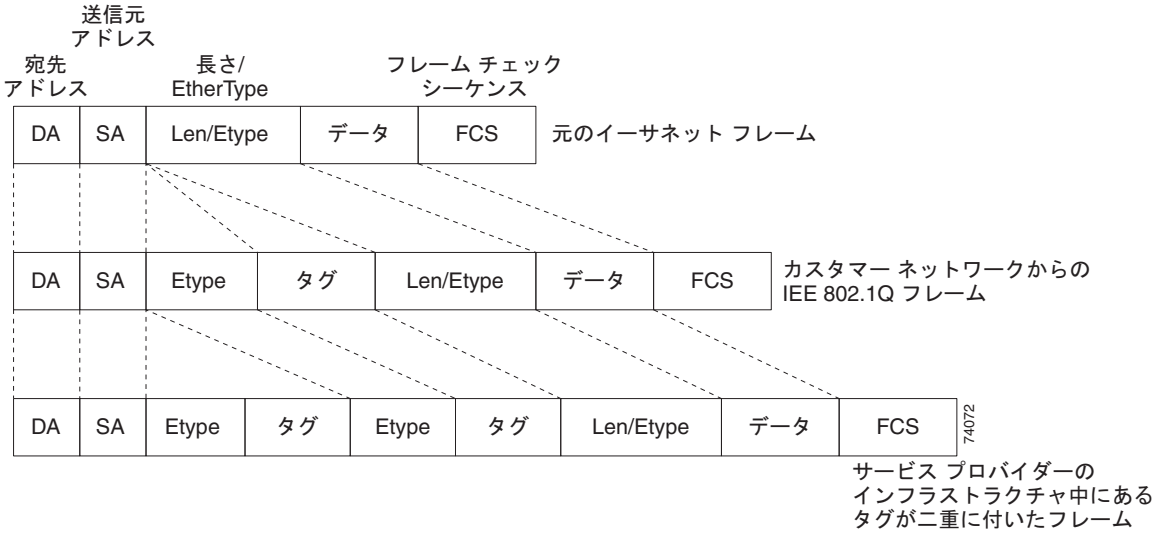


カスタマー トランク ポートからトンネル ポートに送信されるパケットは、サービス プロバイダー エッジ スイッチは通常は適切な VLAN ID でタグを付けられた IEEE 802.1Q です。タグ付きパケットは、スイッチの内部でそのまま残り、トランク ポートからサービス プロバイダー ネットワークから送信されるときに、カスタマーに一意の VLAN ID を含む IEEE 802.1Q タグ（*メトロ タグ*と呼ばれます）の別のレイヤを使用してカプセル化されます。元のカスタマー IEEE 802.1Q タグは、カプセル化されたパケット内に保持されます。したがって、サービス プロバイダー ネットワークに着信するパケットは、カスタマーのアクセス VLAN ID が含まれる外部（メトロ）タグと着信トラフィックの内部のタグである VLAN ID を使用した二重タグ付きです。

二重タグ付きパケットがサービス プロバイダー コア スイッチ内の別のトランク ポートで受信される場合、スイッチがそのパケットを処理するときに外部タグが取り除かれます。パケットが同じコア スイッチの別のトランク ポートから送信される場合、同じメトロ タグが再びそのパケットにタグ付けされます。図 20-2 に、二重タグ付きパケットのタグ構造を示します。

（注）　カプセル化された着信パケットはトランクポートを errdisable に変更するため、そのトランクポートからレイヤ 2 プロトコル設定を削除します。カプセル化された発信 VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）の Cisco Discovery Protocol（CDP; シスコ検出プロトコル）と Spanning Tree Protocol（STP; スパニング ツリー プロトコル）パケットは、そのトランク上で廃棄されます。

図 20-2　元の（標準の）、IEEE 802.1Q、および二重タグ付きイーサネット パケット形式



パケットがサービス プロバイダー 出力スイッチのトランク ポートで受信される場合、スイッチが内部でパケットを処理するときに外部タグが再び取り除かれます。ただし、パケットがエッジ スイッチ上のトンネル ポートからカスタマー ネットワークに送信されるときには、メトロ タグは追加されません。パケットはカスタマー ネットワーク内の元の VLAN 番号を保持するために標準の IEEE 802.1Q タグ付きフレームとして送信されます。

図 20-1 では、カスタマー A は VLAN 30 が割り当てられ、カスタマー B は VLAN 40 が割り当てられています。IEEE 802.1Q タグを使用してエッジ スイッチ トンネル ポートで受信されるパケットは、VLAN ID 30 または 40 を含んでいる外部タグ、および VLAN 100 などの元の VLAN 番号 を含んでいる内部タグを適切に使用して、サービス プロバイダー ネットワークに着信するときに、二重タグが付いています。カスタマー A と B の両方のネットワーク内に VLAN 100 がある場合、外部タグが異なるため、トラフィックはサービス プロバイダー ネットワーク 内で分離されたままになります。各カスタマーは、他のカスタマーによって使用される VLAN 番号付けスペースとサービス プロバイダー ネットワークによって使用される VLAN 番号付けスペースから独立した独自の VLAN 番号付けスペースを管理します。

アウトバウンド トンネル ポートでは、カスタマーのネットワークの元の VLAN 番号が回復されます。このリリースでは、トンネリングとタグ付けは複数のレベルにできますが、スイッチは 1 つのレベルだけをサポートします。

カスタマー ネットワークから送信されるトラフィックは、タグ付きではない（ネイティブ VLAN フレームである）場合、これらのパケットは標準のパケットとしてブリッジされるかルーティングされます。エッジ スイッチ上のトンネル ポートを経由してサービス プロバイダー ネットワークに着信するすべてのパケットは、すでに IEEE 802.1Q ヘッダーを使用してタグ付けされている場合もそうではない場合も、タグなしパケットとして扱われます。パケットは IEEE 802.1Q トランク ポート上のサービス プロバイダー ネットワークを通って送信されるときに、（トンネル ポートのアクセス VLAN に設定された）メトロ タグ VLAN ID を使用してカプセル化されます。メトロ タグ上のプライオリティ フィールドは、トンネル ポート上で設定されたインターフェイス Class of Service（CoS; サービス クラス）に設定されます（none に設定されている場合、デフォルトは 0 です）。

IEEE 802.1Q トンネリングの設定

ここでは、次の設定情報について説明します。

デフォルトの IEEE 802.1Q トンネリングの設定

デフォルトでは、デフォルト スイッチポート モードが dynamic auto であるため、IEEE 802.1Q トンネリングはディセーブルになっています。すべての IEEE 802.1Q トランク ポートは IEEE 802.1Q ネイティブ VLAN パケットのタグ付けもディセーブルです。

IEEE 802.1Q トンネリングの設定時の注意事項

IEEE 802.1Q トンネリングを設定する場合、カスタマー装置のポートは IEEE 802.1Q トランク ポートとして設定し、エッジ スイッチ ポートはトンネル ポートとして設定して、カスタマー装置とエッジ スイッチの間で常に非対称リンクを使用する必要があります。

トンネル ポートはトンネリングに使用する VLAN だけに割り当てます。

ネイティブ VLAN に対する設定の要件と Maximum Transmission Unit（MTU; 最大伝送ユニット）に対する設定の要件は、次の項以降で説明します。

ネイティブ VLAN

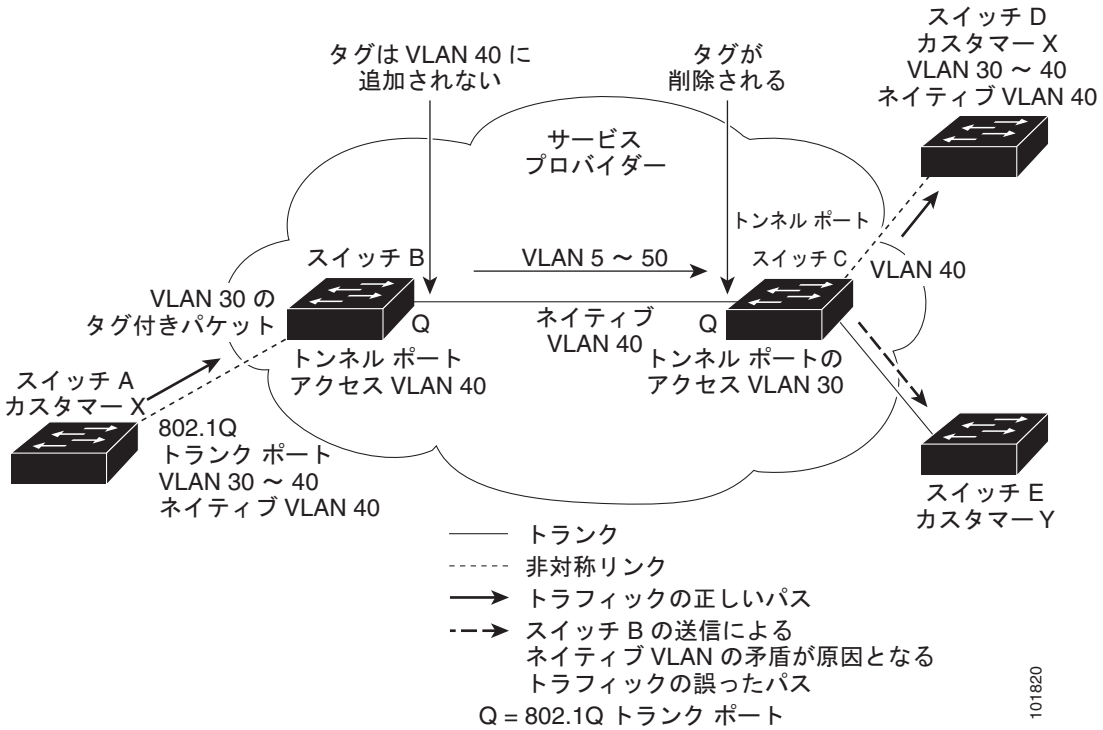
エッジ スイッチ上の IEEE 802.1Q トンネリングを設定する場合、サービス プロバイダー ネットワーク内へのパケットの送信には IEEE 802.1Q トランク ポートを使用する必要があります。ただし、サービス プロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL（スイッチ間リンク）トランク、または非トランキング リンクを通して伝送される可能性があります。これらのコア スイッチ内で IEEE 802.1Q トランクが使用される場合、IEEE 802.1Q トランクのネイティブ VLAN は、ネイティブ VLAN 上のトラフィックは IEEE 802.1Q 送信トランク ポートでタグ付けされないため、同一のスイッチ上の非トランキング（トンネリング）ポートのどのネイティブ VLAN とも一致しないようにする必要があります。

図 20-3 を参照してください。VLAN 40 は、サービス プロバイダー ネットワーク（スイッチ B）内の入力エッジ スイッチで、カスタマー X からの IEEE 802.1Q トランク ポートのネイティブ VLAN として設定されます。カスタマー X のスイッチ A は、アクセス VLAN 40 に属するサービス プロバイダー ネットワーク内のスイッチ B の入力トンネル ポートに VLAN 30 でタグ付きパケットを送信します。トンネル ポートのアクセス VLAN（VLAN 40）は、エッジ スイッチ トランク ポートのネイティブ VLAN（VLAN 40）と同じであるため、メトロ タグはトンネル ポートから受信したタグ付きパケットに付加されません。パケットは VLAN 30 タグだけをサービス プロバイダー ネットワークを通して出力エッジ スイッチ（スイッチ C）のトランク ポートに伝送し、出力スイッチ トンネル ポートを通してカスタマー Y に誤って送信されます。

次に、この問題を解決する方法を示します。

- **vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用して、ネイティブ VLAN を含む、IEEE 802.1Q トランクから出るすべてのパケットがタグ付けされるようにエッジ スイッチを設定します。スイッチがすべての IEEE 802.1Q トランク上のネイティブ VLAN パケットにタグを付けるように設定されている場合、そのスイッチはタグなしパケットを受け入れますが、タグ付きパケットだけを送信します。
- エッジ スイッチ トランク ポート上のネイティブ VLAN ID がカスタマー VLAN の範囲内ではないことを確認します。たとえば、トランク ポートが VLAN 100 から 200 までのトラフィックを伝送する場合、ネイティブ VLAN にその範囲外の番号を割り当てます。

図 20-3　IEEE 802.1Q トンネリングとネイティブ VLAN に関する潜在的な問題



システム MTU

スイッチ上のトラフィックのデフォルト システム MTU は 1500 バイトです。**system mtu** グローバル コンフィギュレーション コマンドを使用して、ファスト イーサネット ポートを 1500 バイトより大きいフレームをサポートするように設定できます。**system mtu jumbo** グローバル コンフィギュレーション コマンドを使用して、1500 バイトより大きいフレームをサポートするようにギガビット イーサネット ポートを設定できます。IEEE 802.1Q トンネリング機能は、メトロ タグを付加するときにフレーム サイズを 4 バイトずつ大きくするため、スイッチ システム MTU サイズを最小でも 1504 バイトにすることによって、最大のフレームを処理できるようにサービス プロバイダー ネットワーク内のすべてのスイッチを設定する必要があります。ギガビット イーサネット インターフェイスに使用可能な最大のシステム MTU は 9000 バイトであり、ファスト イーサネット インターフェイスの最大システム MTU は 1998 バイトです。

IEEE 802.1Q トンネリングと他の機能

IEEE 802.1Q トンネリングはレイヤ 2 パケット スイッチングに対して適切に機能しますが、一部のレイヤ 2 機能とレイヤ 3 スイッチングとの間に非互換性の問題があります。

- トンネル ポートはルーテッド ポートにはできません。
- IP ルーティングは IEEE 802.1Q ポートを含む VLAN 上ではサポートされません。トンネル ポートから受信したパケットは、レイヤ 2 情報だけに基づいて転送されます。トンネル ポートを含む Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）上でルーティングがイネーブルになっている場合は、トンネル ポートから受信されたタグなし IP パケットは、スイッチによって認識され、ルーティングされます。カスタマーは各自のネイティブ VLAN を通してインターネットにアクセスできます。このアクセスが必要ではない場合は、トンネル ポートを含む VLAN 上で SVI を設定しないようにする必要があります。
- フォールバック ブリッジングはトンネル ポートではサポートされません。トンネル ポートから受信したすべての IEEE 802.1Q タグ付きパケットは、非 IP パケットとして扱われるため、フォールバック ブリッジングはトンネル ポートが設定された VLAN 上でイネーブルになっている場合、IP パケットは VLAN にわたって不適切にブリッジされます。したがって、トンネル ポートがある VLAN 上ではフォールバック ブリッジングをイネーブルにしないようにする必要がります。
- トンネル ポートでは IP Access Control List（ACL; アクセス制御リスト）をサポートしません。
- レイヤ 3 QoS（Quality Of Service）ACL およびレイヤ 3 に関連するその他の QoS 機能の情報は、トンネル ポートでサポートされません。Media Access Control（MAC; メディア アクセス制御）ベースの QoS はトンネル ポートでサポートされます。
- EtherChannel ポート グループは、IEEE 802.1Q 設定が EtherChannel ポート グループ内で一貫している限りトンネル ポートと互換性があります。
- Port Aggregation Protocol（PAgP; ポート集約プロトコル）、Link Aggregation Control Protocol（LACP）、および UniDirectional Link Detection（UDLD; 単一方向リンク検出）は IEEE 802.1Q トンネル ポート上でサポートされます。
- Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）は、トンネル ポートとトランク ポートを使用して手動で非対称リンクに設定する必要があるため、IEEE 802.1Q と互換性がありません。
- VLAN トランキング プロトコル（VTP）は、トンネルを介して通信する非対称リンクまたは装置によって接続された装置間で機能しません。
- ループバック検出は、IEEE 802.1Q トンネル ポート上でサポートされます。

- IEEE 802.1Q トンネル ポートとしてポートが設定されている場合、スパニング ツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）フィルタリングは、インターフェイス上で自動的にイネーブルになります。シスコ検出プロトコル（CDP）と Link Layer Discovery Protocol（LLDP）は、インターフェイス上で自動的にディセーブルになります。

IEEE 802.1Q トンネリング ポートの設定

IEEE 802.1Q トンネル ポートとしてポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	トンネル ポートとして設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワーク内のエッジ ポートである必要があります。有効なインターフェイスには、物理インターフェイスとポートチャネル論理インターフェイス（ポート チャネル 1 ～ 48）が含まれます。
ステップ 3	**switchport access vlan** *vlan-id*	インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。この VLAN ID は特定のカスタマーに固有です。
ステップ 4	**switchport mode dot1q-tunnel**	インターフェイスを IEEE 802.1Q トンネル ポートとして設定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**vlan dot1q tag native**	（任意）すべての IEEE 802.1Q トランク ポートでネイティブ VLAN パケットのタグ付けをイネーブルにするようにスイッチを設定します。これを設定せず、カスタマー VLAN ID がネイティブ VLAN と同じである場合、トランク ポートはメトロ タグを適用せず、パケットは誤った宛先に送信される可能性があります。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** **show dot1q-tunnel**	IEEE 802.1Q トンネリング用に設定されたポートを表示します。 トンネル モードになっているポートを表示します。
ステップ 9	**show vlan dot1q tag native**	IEEE 802.1Q ネイティブ VLAN タギング ステータスを表示します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

no switchport mode dot1q-tunnel インターフェイス コンフィギュレーション コマンドを使用して、dynamic desirable のデフォルト状態にポートを戻します。**no vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用して、ネイティブ VLAN パケットのタグ付けをディセーブルにします。

次に、トンネル ポートとしてインターフェイスを設定して、ネイティブ VLAN パケットのタグ付けをイネーブルにし、設定を確認する例を示します。ギガビット イーサネット インターフェイス 7 に接続されているカスタマーの VLAN ID は VLAN 22 です。

```
Switch(config)# interface gigabitethernet1/7
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet1/7
Port
```

```
-----
Gi1/1Port

-----
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

レイヤ 2 プロトコル トンネリングの概要

サービス プロバイダー ネットワークにわたって接続されている さまざまなサイトにおけるカスタマーは、さまざまなレイヤ 2 プロトコルを使用し、すべてのリモート サイトとローカル サイが含まれるようにトポロジを拡張する必要があります。STP は適切に実行する必要があり、各 VLAN はサービス プロバイダー ネットワークのローカル サイトとすべてのリモート サイトを含む適切なスパニング ツリーを構築する必要があります。シスコ検出プロトコル（CDP）は、ローカル サイトとリモート サイトからネイバー シスコ デバイスを検出する必要があります。VLAN トランキング プロトコル（VTP）は、カスタマー ネットワーク内のすべてのサイトにわたって一貫した VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルである場合、サービス プロバイダー ネットワークの着信側のエッジ スイッチはレイヤ 2 プロトコル パケットを特別な MAC アドレスを使用してカプセル化し、それらをサービス プロバイダー ネットワークにわたって送信します。ネットワーク内のコア スイッチは、これらのパケットを処理しませんが、それらを標準のパケットとして転送します。CDP、STP、または VTP のレイヤ 2 プロトコル Protocol Data Unit（PDU; プロトコル データ ユニット）は、サービス プロバイダー ネットワークをわたり、サービス プロバイダー ネットワークの発信側のカスタマー スイッチに配信されます。同じパケットは、同じ VLAN 上のすべてのカスタマー ポートで受信され、次のような結果になります。

- 各カスタマー サイトのユーザは STP を適切に実行し、すべての VLAN はローカル サイトだけではなくすべてのサイトからのパラメータに基づいた適切なスパニング ツリーを構築できます。
- CDP はサービス プロバイダー ネットワークを通して接続された他のシスコ デバイスについての情報を検出して表示します。
- VTP はサービス プロバイダーを介してすべてのスイッチに伝播し、カスタマー ネットワーク全体に一貫した VLAN 設定を提供します。

（注） サードパーティ ベンダーに相互運用性を提供するには、レイヤ 2 プロトコルトンネル バイパス機能を使用します。バイパス モードは、さまざまな方法でプロトコル トンネリングを制御するベンダー スイッチに制御 PDU がトランスペアレントに転送されます。出力トランク ポート上でレイヤ 2 プロトコル トンネリングをイネーブルにすることによってバイパス モードを実装します。トランク ポート上でレイヤ 2 プロトコル トンネリングがイネーブルである場合、カプセル化されたトンネル MAC アドレスは削除され、プロトコル パケットは標準の MAC アドレスを持ちます。

レイヤ 2 プロトコル トンネリングは個別に使用でき、IEEE 802.1Q トンネリングを拡張できます。プロトコル トンネリングが IEEE 802.1Q トンネリング ポートでイネーブルでない場合、サービス プロバイダー ネットワークの受信側のリモート スイッチは PDU を受信せず、STP、CDP、VTP を適切に実行できません。プロトコル トンネリングがイネーブル*である*場合、各カスタマー ネットワーク内のレイヤ 2 プロトコルは、サービス プロバイダー ネットワーク内で実行されているプロトコルから完全に分離しています。サービス プロバイダー ネットワークを通じ、IEEE 802.1Q トンネリングを使用してトラフィックを送信するさまざまのサイトのカスタマー スイッチでは、カスタマー VLAN が完全に認識されます。IEEE 802.1Q トンネリングを使用しない場合は、アクセス ポートを通してカスタマー スイッチに接続することによって、およびサービス プロバイダー アクセス ポート上でトンネリングをイネーブルにすることによって、レイヤ 2 プロトコル トンネリングをイネーブルにできます。

たとえば、図 20-4 では、カスタマー X には、サービス プロバイダー ネットワークを通して接続されている同一 VLAN 上に 4 つのスイッチがあります。ネットワークが PDU のトンネリングを行わない場合は、ネットワークの遠端上のスイッチは STP、CDP、VTP を適切に実行できません。たとえば、カスタマー X のスイッチの VLAN の STP は、サイト 2 のカスタマー X のスイッチに基づいたコンバージェンス パラメータを考慮せずに、サイト 1 がそのサイトのスイッチにスパニング ツリーを構築します。この結果、図 20-5 のようなトポロジとなる可能性があります。

図 20-4　レイヤ 2 プロトコル トンネリング

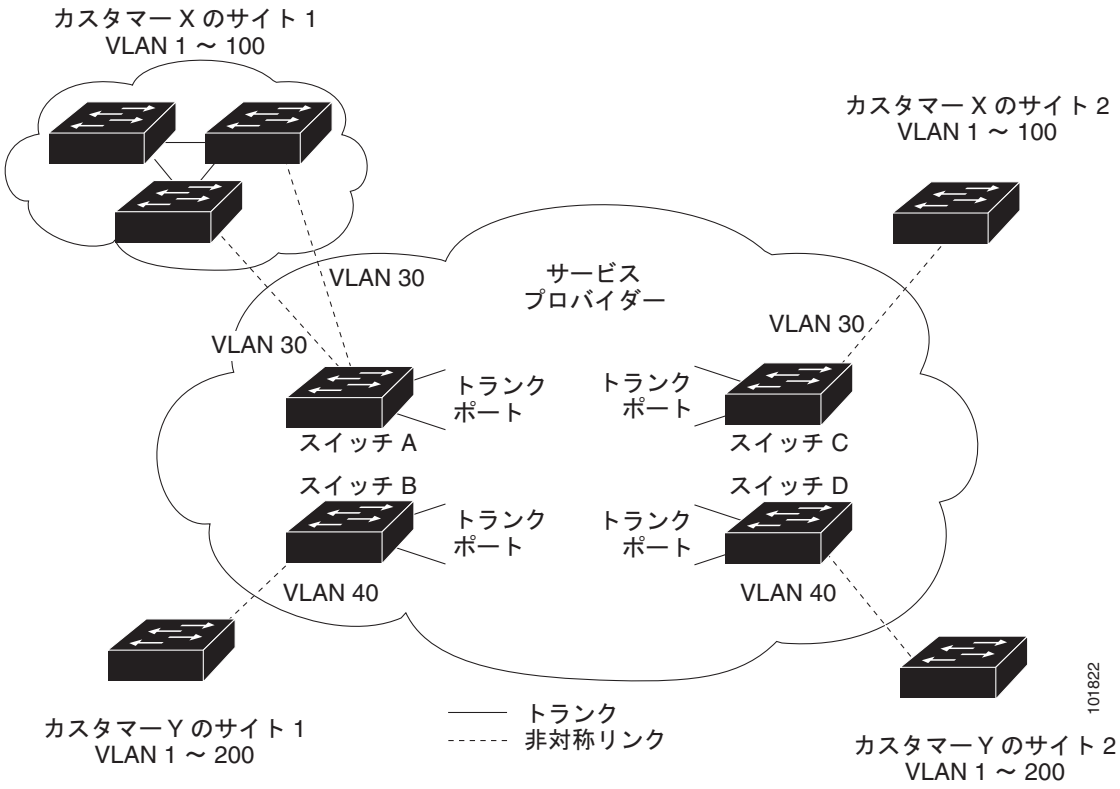
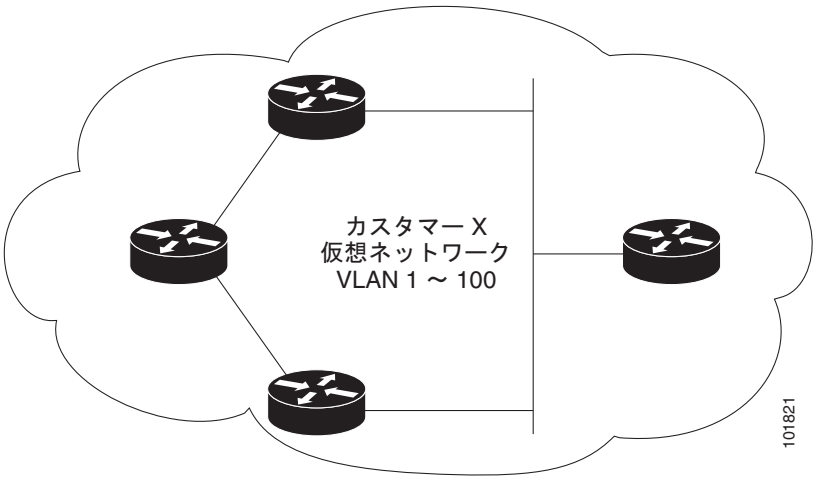


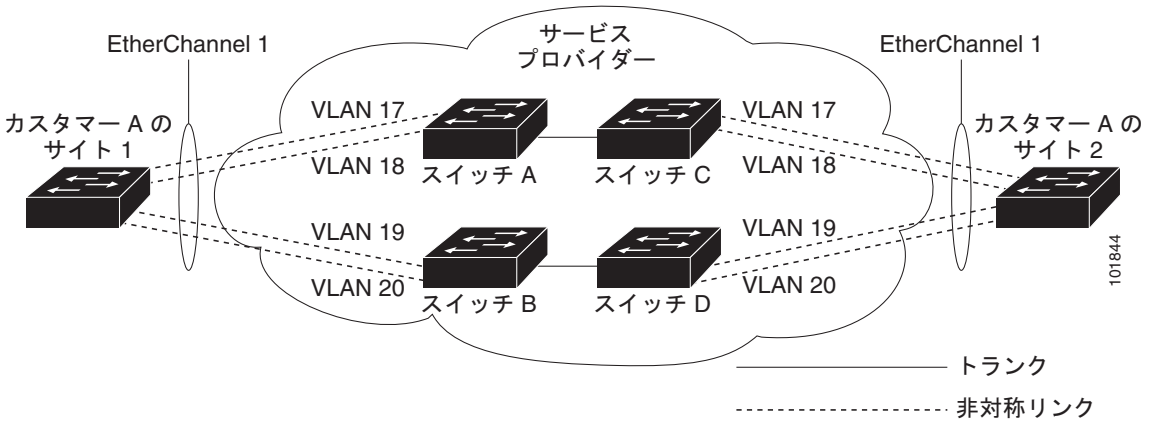
図 20-5　適切なコンバージェンスがないレイヤ 2 ネットワーク トポロジ



Service-Provider（SP; サービス プロバイダー）ネットワークでは、ポイントツーポイント ネットワーク トポロジをエミュレートして EtherChannel の作成を強化するのに、レイヤ 2 プロトコル トンネリングを使用できます。プロトコル トンネリング（PAgP または LACP）を SP スイッチでイネーブルにする場合、リモート カスタマー スイッチは、PDU を受信し、EtherChannel の自動作成をネゴシエートできます。

たとえば、図 20-6 では、カスタマー A には、SP ネットワークを通して接続されている同一 VLAN 上に 2 つのスイッチがあります。ネットワークが PDU のトンネリングを行う場合、ネットワークの遠端上のスイッチは専用線を必要としないで EtherChannel の自動作成をネゴシエートできます。手順については、「EtherChannel のレイヤ 2 トンネリングの設定」（P.20-14）を参照してください。

図 20-6　EtherChannel のレイヤ 2 プロトコル トンネリング



レイヤ 2 プロトコル トンネリングの設定

サービス プロバイダー ネットワークのエッジ スイッチのカスタマーに接続されているポート上で レイヤ 2 プロトコル トンネリングを（プロトコルによって）イネーブルにできます。カスタマー スイッチに接続されているサービス プロバイダー エッジ スイッチは、トンネリングのプロセスを実行します。エッジ スイッチ トンネル ポートは、カスタマー IEEE 802.1Q トランク ポートに接続されます。エッジ スイッチ アクセス ポートはカスタマー アクセス ポートに接続されます。カスタマー スイッチに接続されているエッジ スイッチは、トンネリングのプロセスを実行します。

アクセス ポートまたはトンネル ポートとして設定されたポート上のレイヤ 2 プロトコル トンネリングをイネーブルにできます。**switchport mode dynamic auto（デフォルト モード）**または **switchport mode dynamic desirable** で設定されたポート上のレイヤ 2 プロトコル トンネリングをイネーブルにできません。

スイッチは CDP、STP、および VTP のレイヤ 2 プロトコル トンネリングをサポートします。エミュレートされたポイントツーポイント ネットワーク トポロジの場合は、PAgP、LACP、および UDLD プロトコルもサポートします。スイッチは LLDP のレイヤ 2 プロトコル トンネリングをサポートしません。

注意　PAgP、LACP、および UDLD プロトコル トンネリングは、ポイントツーポイント トポロジをエミュレートすることだけを目的としています。設定を間違えたことによりトンネリング パケットが多くのポートに送信されると、ネットワーク障害が発生する可能性があります。

レイヤ 2 プロトコルがイネーブルのポートを通ってサービス プロバイダーの着信側エッジ スイッチに入ったレイヤ 2 PDU が、トランク ポートを通ってサービス プロバイダー ネットワークに出力する場合、そのスイッチカスタマー PDU 宛先 MAC アドレスがシスコの既知の独自マルチキャスト アドレス（01-00-0c-cd-cd-d0）で上書きされます。IEEE 802.1Q トンネリングがイネーブルの場合、パケットも二重タグ付きになります。外部タグはカスタマー メトロ タグであり、内部タグはカスタマー VLAN タグです。コア スイッチは内部タグを無視してパケットを同じメトロ VLAN 内のすべてのトランク ポートに転送します。発信側のエッジ スイッチは、適切なレイヤ 2 プロトコルと MAC アドレス情報を元に戻し、同じメトロ VLAN 内のすべてのトンネル ポートまたはアクセス ポートにパケットを転送します。したがって、レイヤ 2 PDU はそのまま残り、サービス プロバイダー インフラストラクチャを介して反対側のカスタマー ネットワークに配信されます。

カスタマー X とカスタマー Y がそれぞれアクセス VLAN 30 と 40 にある図 20-4 を参照してください。非対称リンクはサイト 1 内のカスタマーをサービス プロバイダー ネットワーク内のエッジ スイッチに接続します。サイト 1 内のカスタマー Y からスイッチ 2 に入るレイヤ 2 PDU（BPDU など）は、宛先 MAC アドレスとして既知の MAC アドレスが付いた状態で二重タグ付きパケットとしてインフラストラクチャに転送されます。これらの二重タグ付きパケットにはメトロ VLAN タグ 40 と内部 VLAN タグ（VLAN 100 など）があります。二重タグ付きパケットがスイッチ D に入ると、外部 VLAN タグ 40 は削除され、既知の MAC アドレスはそれぞれのレイヤ 2 プロトコル MAC アドレスに置き換えられ、パケットは VLAN 100 内の一重タグ付きフレームとしてサイト 2 のカスタマー Y に送信されます。

カスタマー スイッチ上のアクセス ポートまたはトランク ポートに接続されたエッジ スイッチ上のアクセス ポート上でレイヤ 2 プロトコル トンネリングをイネーブルにすることもできます。この場合、カプセル化プロセスとカプセル化解除プロセスは、パケットがサービス プロバイダー ネットワーク内では二重タグ付きではないことを除いて、前の段落で説明したプロセスと同じです。一重タグは、カスタマー固有のアクセス VLAN タグです。

ここでは、次の設定情報について説明します。

- 「レイヤ 2 プロトコル トンネリングのデフォルト設定」（P.20-11）
- 「レイヤ 2 プロトコル トンネリングの設定時の注意事項」（P.20-12）
- 「レイヤ 2 プロトコル トンネリングの設定」（P.20-13）
- 「EtherChannel のレイヤ 2 トンネリングの設定」（P.20-14）

レイヤ 2 プロトコル トンネリングのデフォルト設定

表 20-1 に、レイヤ 2 プロトコル トンネリングのデフォルト設定を示します。

表 20-1　レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
レイヤ 2 プロトコル トンネリング	ディセーブル。
シャットダウン スレッシュホールド	設定なし。
廃棄スレッシュホールド	設定なし。
CoS 値	インターフェイスに CoS 値が設定されている場合は、その値がレイヤ 2 プロトコル トンネリングの BPDU CoS 値を設定するために使用されます。CoS 値がインターフェイス レベルで設定されていない場合は、L2 プロトコル トンネリング BPDU の CoS マーキングのデフォルト値は 5 です。これはデータ トラフィックには適用されません。

レイヤ 2 プロトコル トンネリングの設定時の注意事項

次に、レイヤ 2 プロトコル トンネリングの設定時の注意事項と動作特性を示します。

- スイッチは、CDP、Multiple STP（MSTP）を含む STP、および VTP のトンネリングをサポートします。プロトコル トンネリングはデフォルトではディセーブルになっていますが、IEEE 802.1Q トンネル ポートまたはアクセス ポート上の個別のプロトコルに対してはイネーブルにできます。
- スイッチは、**switchport mode dynamic auto** または **dynamic desirable** であるポート上ではレイヤ 2 プロトコル トンネリングをサポートしません。
- DTP はレイヤ 2 プロトコル トンネリングと互換性がありません。
- サービス プロバイダー ネットワークの発信側のエッジ スイッチは、適切なレイヤ 2 プロトコルと MAC アドレス情報を元に戻し、同じメトロ VLAN 内のすべてのトンネル ポートとアクセス ポートにパケットを転送します。
- サード パーティ ベンダーのスイッチとの相互運用性のために、スイッチはレイヤ 2 プロトコル トンネル バイパス 機能をサポートします。バイパス モードは、さまざまな方法でプロトコル トンネリングを制御するベンダー スイッチに制御 PDU をトランスペアレントに転送します。レイヤ 2 プロトコル トンネリングがスイッチ上の入力ポートでイネーブルにされる場合、出力トランク ポートは特別なカプセル化を使用してトンネリング パケットを転送します。出力トランク ポート上でもレイヤ 2 プロトコル トンネリングをイネーブルにした場合は、この動作がバイパスされ、スイッチはどのような処理や変更も行わずに制御 PDU を転送します。
- スイッチはエミュレートされたポイントツーポイント ネットワーク トポロジに対する PAgP、LACP、および UDLD のトンネリングをサポートします。プロトコル トンネリングはデフォルトではディセーブルになっていますが、IEEE 802.1Q トンネル ポートまたはアクセス ポート上の個別のプロトコルに対してはイネーブルにできます。
- PAgP または LACP トンネリングをイネーブルにした場合、リンク障害検出を高速化するために、インターフェイス上で UDLD もイネーブルにすることを推奨します。
- ループバック検出は、PAgP、LACP、または UDLD パケットのレイヤ 2 プロトコル トンネリングではサポートされません。
- EtherChannel ポート グループは、IEEE 802.1Q 設定が EtherChannel ポート グループ内で一貫している場合はトンネル ポートと互換性があります。
- 独自の宛先 MAC アドレスを持つカプセル化された PDU がレイヤ 2 トンネリングがイネーブルにされたトンネル ポートまたはアクセス ポートから受信された場合、トンネル ポートがループを防止するためにシャットダウンされます。ポートは、プロトコルに対して設定されたシャットダウン スレッシュホールドに達した場合もシャットダウンされます。ポートは、手動で（**shutdown** および **no shutdown** のコマンド シーケンスを入力することによって）再びイネーブルにできます。errdisable recovery がイネーブルの場合、指定された間隔のあとに動作が再試行されます。
- カプセル化が解除された PDU だけがカスタマー ネットワークに転送されます。サービス プロバイダー ネットワーク上で実行されているスパニング ツリー インスタンスは、BPDU をトンネル ポートに転送しません。CDP パケットはトンネル ポートから転送されません。
- インターフェイス上でプロトコル トンネリングがイネーブルである場合、カスタマー ネットワークによって生成された PDU のプロトコルごと、ポートごとのシャットダウン スレッシュホールドを設定できます。制限を超えた場合、ポートはシャットダウンします。トンネル ポート上の QoS ACL とポリシー マップを使用して BPDU レートを制限することもできます。
- インターフェイス上でプロトコル トンネリングがイネーブルである場合、カスタマー ネットワークによって生成された PDU のプロトコルごと、ポートごとの廃棄スレッシュホールドを設定できます。制限を超えた場合は、PDU を受信するレートが廃棄スレッシュホールドより小さくなるまでポートは PDU を廃棄します。

- トンネリングされた PDU（特に STP BPDU）は、カスタマーの仮想ネットワークが正常に動作するようにすべてのリモート サイトに配信される必要があるため、サービス プロバイダー ネットワーク内で同じトンネル ポートから受信したデータ パケットよりも PDU に高いプライオリティを設定できます。デフォルトでは、PDU は同じ CoS 値をデータ パケットとして使用します。

レイヤ 2 プロトコル トンネリングの設定

レイヤ 2 プロトコル トンネリング用にポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	トンネル ポートとして設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワーク内のエッジ ポートである必要があります。有効なインターフェイスは、物理インターフェイスとポートチャネル論理インターフェイス（ポート チャネル 1 ～ 48）です。
ステップ 3	**switchport mode access** または **switchport mode dot1q-tunnel**	インターフェイスをアクセス ポートまたは IEEE 802.1Q トンネル ポートとして設定します。
ステップ 4	**l2protocol-tunnel** [**cdp** | **stp** | **vtp**]	目的のプロトコルのプロトコル トンネリングをイネーブルにします。キーワードが入力されていない場合は、3 つのレイヤ 2 プロトコルすべてに対してトンネリングがイネーブルになります。
ステップ 5	**l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] *value*	（任意）カプセル化用に受け入れられる秒単位のパケット数についてのスレッシュホールドを設定します。設定されたスレッシュホールドを超えた場合、インターフェイスはディセーブルになります。プロトコルのオプションが設定されていない場合は、スレッシュホールドが各トンネリング レイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ～ 4096 です。デフォルトでは、スレッシュホールドが設定されていません。 **（注）** インターフェイスに廃棄スレッシュホールドも設定する場合は、シャットダウン スレッシュホールドが廃棄スレッシュホールド以上でなければなりません。
ステップ 6	**l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *value*	（任意）カプセル化用に受け入れられる秒単位のパケット数についてのスレッシュホールドを設定します。設定されたスレッシュホールドを超えた場合、インターフェイスはパケットを廃棄します。プロトコルのオプションが設定されていない場合は、スレッシュホールドが各トンネリング レイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ～ 4096 です。デフォルトでは、スレッシュホールドが設定されていません。 インターフェイスにシャットダウン スレッシュホールドも設定する場合は、廃棄スレッシュホールドがシャットダウン スレッシュホールド以下でなければなりません。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**errdisable recovery cause l2ptguard**	（任意）インターフェイスが再びイネーブルにされ再試行するためのレイヤ 2 最大レート エラーからの回復メカニズムを設定します。errdisable recovery がデフォルトでディセーブルである場合、デフォルト間隔は 300 秒です。

	コマンド	目的
ステップ 9	**l2protocol-tunnel cos** *value*	（任意）すべてのトンネリング レイヤ 2 PDU の CoS 値を設定します。範囲 0 ～ 7 です。デフォルトはインターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show l2protocol**	設定されたプロトコル、スレッシュホールド、およびカウンタを含む、スイッチ上のレイヤ 2 トンネル ポートを表示します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのプロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel** [**cdp** | **stp** | **vtp**] インターフェイス コンフィギュレーション コマンドを使用します。シャットダウン スレッシュホールドと廃棄スレッシュホールドをデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] および **no l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] コマンドを使用します。

次に、CDP、STP、および VTP に対して、レイヤ 2 プロトコル トンネリングを設定し、その設定を確認する例を示します。

```
Switch(config)# interface fastethernet1/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
Port      Protocol Shutdown  Drop      Encapsulation Decapsulation Drop
                   Threshold Threshold Counter       Counter       Counter
-------   -------- --------- --------- ------------- ------------- -------------
Fa1/11    cdp           1500      1000 2288          2282          0
          stp           1500      1000 116           13            0
          vtp           1500      1000 3             67            0
          pagp          ----      ---- 0             0             0
          lacp          ----      ---- 0             0             0
          udld          ----      ---- 0             0             0
```

EtherChannel のレイヤ 2 トンネリングの設定

レイヤ 2 ポイントツーポイント トンネリングを設定して EtherChannel を自動的に作成するには、SP エッジ スイッチとカスタマー スイッチの両方を設定する必要があります。

SP エッジ スイッチの設定

EtherChannel のレイヤ 2 プロトコル トンネリング用に SP エッジ スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	トンネル ポートとして設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチに接続する SP ネットワーク内のエッジ ポートである必要があります。有効なインターフェイスは物理ポートです。
ステップ 3	**switchport mode dot1q-tunnel**	インターフェイスを IEEE 802.1Q トンネル ポートとして設定します。
ステップ 4	**l2protocol-tunnel point-to-point** [**pagp** | **lacp** | **udld**]	（任意）目的のプロトコルのポイントツーポイント プロトコル トンネリングをイネーブルにします。キーワードが入力されていない場合は、3 つのプロトコルすべてに対してトンネリングがイネーブルになります。 **注意** ネットワーク障害を回避するには、PAgP、LACP、または UDLD パケットのトンネリングをイネーブルにする前に、ネットワークがポイントツーポイント トポロジであることを確認します。
ステップ 5	**l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*	（任意）カプセル化用に受け入れられる秒単位のパケット数についてのスレッシュホールドを設定します。設定されたスレッシュホールドを超えた場合、インターフェイスはディセーブルになります。プロトコルのオプションが設定されていない場合は、スレッシュホールドが各トンネリング レイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ～ 4096 です。デフォルトでは、スレッシュホールドが設定されていません。 **（注）** インターフェイスに廃棄スレッシュホールドも設定する場合は、シャットダウン スレッシュホールドが廃棄スレッシュホールド以上でなければなりません。
ステップ 6	**l2protocol-tunnel drop-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*	（任意）カプセル化用に受け入れられる秒単位のパケット数についてのスレッシュホールドを設定します。設定されたスレッシュホールドを超えた場合、インターフェイスはパケットを廃棄します。プロトコルのオプションが設定されていない場合は、スレッシュホールドが各トンネリング レイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ～ 4096 です。デフォルトでは、スレッシュホールドが設定されていません。 **（注）** インターフェイスにシャットダウン スレッシュホールドも設定する場合は、廃棄スレッシュホールドがシャットダウン スレッシュホールド以下でなければなりません。
ステップ 7	**no cdp enable**	インターフェイスで CDP をディセーブルにします。
ステップ 8	**spanning-tree bpdufilter enable**	インターフェイスで BPDU フィルタリングをイネーブルにします。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**errdisable recovery cause l2ptguard**	（任意）インターフェイスが再びイネーブルにされ再試行するためのレイヤ 2 最大レート エラーからの回復メカニズムを設定します。errdisable recovery がデフォルトでディセーブルである場合、デフォルト間隔は 300 秒です。
ステップ 11	**l2protocol-tunnel cos** *value*	（任意）すべてのトンネリング レイヤ 2 PDU の CoS 値を設定します。範囲 0 ～ 7 です。デフォルトはインターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。

	コマンド	目的
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show l2protocol**	設定されたプロトコル、スレッシュホールド、およびカウンタを含む、スイッチ上のレイヤ 2 トンネル ポートを表示します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのポイントツーポイント プロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel** [**point-to-point** [**pagp** | **lacp** | **udld**]] インターフェイス コンフィギュレーション コマンドを使用します。シャットダウン スレッシュホールドと廃棄スレッシュホールドをデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] および **no l2protocol-tunnel drop-threshold** [[**point-to-point** [**pagp** | **lacp** | **udld**]] コマンドを使用します。

カスタマー スイッチの設定

SP エッジ スイッチを設定したあとに、EtherChannel のレイヤ 2 プロトコル トンネリング用にカスタマー スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。これはカスタマー スイッチ ポートである必要があります。
ステップ 3	**switchport trunk encapsulation dot1q**	トランキング カプセル化フォーマットを IEEE 802.1Q に設定します。
ステップ 4	**switchport mode trunk**	インターフェイス上でトランキングをイネーブルにします。
ステップ 5	**udld enable**	インターフェイス上の**通常**モードで UDLD をイネーブルにします。
ステップ 6	**channel-group** *channel-group-number* **mode desirable**	インターフェイスをチャネル グループに割り当て、PAgP モードに **desirable** を指定します。EtherChannel の設定の詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface port-channel** *port-channel number*	ポートチャネル インターフェイス モードを開始します。
ステップ 9	**shutdown**	インターフェイスをシャットダウンします。
ステップ 10	**no shutdown**	インターフェイスをイネーブルにします。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show l2protocol**	設定されたプロトコル、スレッシュホールド、およびカウンタを含む、スイッチ上のレイヤ 2 トンネル ポートを表示します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスをデフォルトの設定に戻すには、**no switchport mode trunk**、**no udld enable**、および **no channel group** *channel-group-number* **mode desirable** インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel の場合、レイヤ 2 プロトコル トンネリング用に SP エッジ スイッチとカスタマー スイッチの両方を設定する必要があります（図 20-6（P.20-10）を参照）。

次に、SP のエッジ スイッチと 1 とエッジ スイッチ 2 を設定する例を示します。VLAN 17、18、19、および 20 はアクセス VLAN、ファスト イーサネット インターフェイス 1 および 2 は PAgP および UDLD がイネーブルになっているポイントツーポイント トンネル ポート、廃棄スレッシュホールドは 1000、ファスト イーサネット イーサネット 3 はトランク ポートです。

SP エッジ スイッチ 1 の設定は次のとおりです。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

SP エッジ スイッチ 2 の設定は次のとおりです。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

次に、サイト 1 のカスタマー スイッチを設定する例を示します。ファスト イーサネット インターフェイス 1、2、3、および 4 が IEEE 802.1Q トランキング用に設定され、UDLD がイネーブルにされ、EtherChannel グループ 1 がイネーブルにされ、ポート チャネルがシャットダウンされてからイネーブルにされて EtherChannel 設定がアクティブになります。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/3
Switch(config-if)# switchport trunk encapsulation dot1q
```

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

トンネリング ステータスのモニタおよびメンテナンス

表 20-2 に、IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングのモニタとメンテナンスのための特権 EXEC コマンドを示します。

表 20-2　トンネリングのモニタおよびメンテナンスのためのコマンド

コマンド	目的
clear l2protocol-tunnel counters	レイヤ 2 プロトコル トンネリング ポートのプロトコル カウンタを消去します。
show dot1q-tunnel	スイッチ上の IEEE 802.1Q トンネル ポートを表示します。
show dot1q-tunnel interface *interface-id*	特定のインターフェイスがトンネル ポートであるかどうかを確認します。
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
show errdisable recovery	レイヤ 2 プロトコル トンネル errdisable ステートからの回復タイマーがイネーブルかどうかを確認します。
show l2protocol-tunnel interface *interface-id*	特定のレイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
show l2protocol-tunnel summary	レイヤ 2 プロトコル サマリー情報だけを表示します。
show vlan dot1q tag native	スイッチ上でネイティブ VLAN タギングのステータスを表示します。

これらの表示の詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 21

STP の設定

この章では、IE3000 スイッチのポートベース VLAN で Spanning Tree Protocol（STP; スパニング ツリー プロトコル）を設定する方法について説明します。スイッチでは、IEEE 802.1D 標準とシスコ独自の拡張機能に基づく Per-VLAN Spanning-Tree Plus（PVST+）プロトコル、または IEEE 802.1W 標準に基づく Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルを使用できます。Multiple Spanning-Tree Protocol（MSTP; 多重スパニング ツリー プロトコル）と、複数の VLAN を同じスパニング ツリー インスタンスにマッピングする方法の詳細については、第 22 章「MSTP の設定」を参照してください。PortFast、UplinkFast、ルート ガードなどの他のスパニング ツリー機能の詳細については、第 23 章「オプションのスパニング ツリー機能の設定」を参照してください。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

スパニング ツリー機能の概要

ここでは、次の概念情報について説明します。

- 「STP および IEEE 802.1Q トランク」（P.21-10）
- 「VLAN ブリッジ スパニング ツリー」（P.21-11）

設定の詳細については、「スパニング ツリー機能の設定」（P.21-11）を参照してください。

オプションのスパニング ツリー機能の詳細については、第 23 章「オプションのスパニング ツリー機能の設定」を参照してください。

STP の概要

STP は、ネットワークのループを排除しながらパスの冗長性を提供する、レイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正常に動作するには、2 つのステーション間で存在できるアクティブ パスは 1 つだけです。エンド ステーション間に複数のアクティブ パスがあると、ネットワーク内でループが発生する原因になります。ネットワークにループが存在する場合、エンド ステーションが重複したメッセージを受信する可能性があります。また、スイッチが複数のレイヤ 2 インターフェイス上のエンド ステーション MAC アドレスを学習する可能性があります。このような状況が、不安定なネットワーク環境につながります。スパニング ツリーの動作はトランスペアレントなので、エンド ステーションが単一の LAN セグメントに接続されているのか、それとも複数のセグメントからなるスイッチド LAN に接続されているのかを、エンド ステーションは検知できません。

STP では、スパニング ツリー アルゴリズムを使用して、冗長接続されたネットワークの 1 つのスイッチをスパニング ツリーのルートとして選択します。このアルゴリズムは、アクティブ トポロジにおけるポートのロールに基づいて各ポートにロールを割り当てることにより、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニング ツリー トポロジに対して選定された転送ポート
- 指定：各スイッチド LAN セグメントに対して選定された転送ポート
- 代替：スパニング ツリーのルート ブリッジへの代替パスを提供するブロックされたポート
- バックアップ：ループバック設定におけるブロックされたポート

*すべて*のポートが指定ロールまたはバックアップ ロールであるスイッチは、ルート スイッチです。少なくとも *1* つのポートが指定ロールであるスイッチは、指定スイッチと呼ばれます。

スパニング ツリーは、冗長データ パスを強制的にスタンバイ（ブロック）ステートにします。スパニング ツリーの 1 つのネットワーク セグメントで障害が発生し、冗長パスが存在する場合、スパニング ツリー アルゴリズムはスパニング ツリー トポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）と呼ばれるスパニング ツリー フレームを一定の間隔で送受信します。スイッチは、これらのフレームを転送するのではなく、ループフリー パスの構築に使用します。BPDU には、送信元のスイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。スパニング ツリーでは、この情報を使用して、スイッチド ネットワークのルート スイッチとルート ポートを選定し、各スイッチド セグメントのルート ポートと指定ポートを選定します。

スイッチの 2 つのポートがループの一部になっている場合、どちらのポートがフォワーディング ステートになり、どちらのポートがブロッキング ステートになるかは、スパニング ツリーのポート プライオリティおよびパス コストの設定によって制御されます。スパニング ツリーのポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置を表すとともに、ポートがトラフィックを渡すのにどの程度適した位置にあるかを表します。パス コスト値は、メディア速度を表します。

（注）　デフォルトでは、スイッチは Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュールを持たないインターフェイスでだけキープアライブ メッセージを（接続がアップ状態であることを確認するために）送信します。[**no**] **keepalive** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのデフォルトを変更できます。

スパニング ツリー トポロジと BPDU

スイッチド ネットワークの安定したアクティブなスパニング ツリー トポロジは、次の要素によって制御されます。

- 各スイッチの各 VLAN に関連付けられた一意のブリッジ ID（スイッチ プライオリティと MAC アドレス）。
- ルート スイッチへのスパニング ツリー パス コスト。
- 各レイヤ 2 インターフェイスに関連付けられたポート ID（ポート プライオリティと MAC アドレス）。

ネットワーク内のスイッチの電源を入れると、それぞれのスイッチがルート スイッチとして機能します。各スイッチは、すべてのポートを通じてコンフィギュレーション BPDU を送信します。BPDU は、スパニング ツリー トポロジを伝達および計算します。各コンフィギュレーション BPDU には、次の情報が含まれます。

- 送信元スイッチがルート スイッチとして識別するスイッチの一意のブリッジ ID
- ルートへのスパニング ツリー パス コスト
- 送信元スイッチのブリッジ ID
- メッセージ エージ
- 送信元インターフェイスの ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

*優位*の情報（ブリッジ ID が小さい、パス コストが小さいなど）を含むコンフィギュレーション BPDU を受信すると、スイッチはそのポートの情報を格納します。この BPDU をスイッチのルート ポートで受信した場合、スイッチは自らが指定スイッチであるすべての接続 LAN に、その BPDU を更新メッセージとともに転送します。

当該のポートに対して現在格納されている情報よりも *下位*の情報を含むコンフィギュレーション BPDU を受信すると、スイッチはその BPDU を破棄します。スイッチが下位の BPDU の送信元である LAN の指定スイッチである場合、スイッチはその LAN に当該のポートに対して格納されている最新情報を含む BPDU を送信します。これにより、下位の情報が破棄され、優位の情報がネットワークで伝播されます。

BPDU 交換によって次の処理が実行されます。

- ネットワーク内の 1 つのスイッチがルート スイッチ（スイッチド ネットワークにおけるスパニング ツリー トポロジの論理上の中心）として選定されます。

  VLAN ごとに、最高のスイッチ プライオリティ（数値的に最小のプライオリティ値）を持つスイッチがルート スイッチとして選定されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合は、VLAN 内で MAC アドレスが最小のスイッチがルート スイッチになります。スイッチ プライオリティ値は、表 21-1（P.21-4）に示すように、ブリッジ ID の最上位ビットを占めます。
- 各スイッチ（ルート スイッチを除く）のルート ポートが選択されます。このポートは、スイッチがルート スイッチにパケットを転送するときの最適パス（最小コスト）を提供します。
- パス コストに基づいて、ルート スイッチまでの最短距離がスイッチごとに計算されます。

- LAN セグメントごとに指定スイッチが選択されます。指定スイッチは、その LAN からルート スイッチにパケットを転送するときの最小パス コストとなります。指定スイッチが LAN に接続されるポートを指定ポートと呼びます。

スイッチド ネットワーク内のどの場所からもルート スイッチに到達するために必要とされないパスは、すべてスパニング ツリー ブロッキング モードになります。

ブリッジ ID、スイッチ プライオリティ、および拡張システム ID

IEEE 802.1D 標準では、各スイッチがルート スイッチの選択を制御する一意のブリッジ識別情報（ブリッジ ID）が必要です。各 VLAN は PVST+ と Rapid PVST+ で異なる*論理ブリッジ*と見なされるため、同じスイッチが設定済み VLAN ごとに異なるブリッジ ID を持っている必要があります。スイッチの各 VLAN は、一意の 8 バイト ブリッジ ID を持ちます。最上位の 2 バイトはスイッチ プライオリティに使用され、残りの 6 バイトはスイッチの MAC アドレスから取得されます。

スイッチは IEEE 802.1t スパニング ツリー拡張をサポートし、以前はスイッチ プライオリティに使用されていた一部のビットが、現在は VLAN ID として使用されます。その結果、ブリッジ ID の一意性を維持しつつ、スイッチ用に予約された MAC アドレスは減り、サポートできる VLAN ID の範囲は増えています。表 21-1 に示すように、以前はスイッチ プライオリティに使用されていた 2 バイトは、4 ビットのプライオリティ値と、VLAN ID と等価である 12 ビットの拡張システム ID 値に割り当てが変更されました。

表 21-1　スイッチ プライオリティ値と拡張システム ID

スイッチ プライオリティ値				拡張システム ID（VLAN ID と同設定）											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニング ツリーは、ブリッジ ID が VLAN ごとに一意になるように、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニング ツリー MAC アドレスを使用します。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティを手動で設定する方法に影響が生じます。たとえば、スイッチ プライオリティ値を変更すると、スイッチがルート スイッチとして選定される確率が変わります。大きな値を設定すると確率が低くなり、小さな値を設定すると確率が高くなります。詳細については、「ルート スイッチの設定」（P.21-15）、「セカンダリ ルート スイッチの設定」（P.21-17）、および 「VLAN のスイッチ プライオリティの設定」（P.21-20）を参照してください。

スパニング ツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジの変化が発生します。インターフェイスがスパニング ツリー トポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成される可能性があります。インターフェイスは新しいトポロジ情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。古いトポロジで転送されたフレームの存続時間を満了させることも必要です。

スパニング ツリーを使用するスイッチの各レイヤ 2 インターフェイスは、次のステートのいずれかになります。

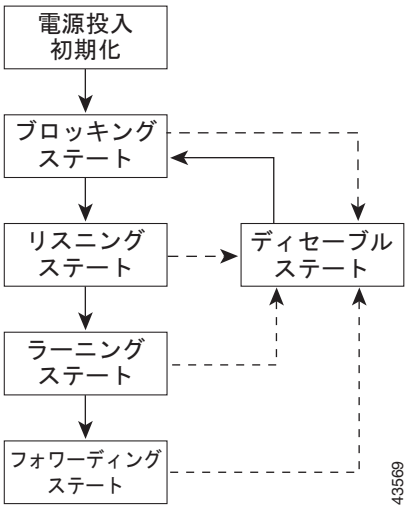
- ブロッキング：インターフェイスはフレーム転送に参加しません。
- リスニング：インターフェイスがフレーム転送に参加する必要があるとスパニング ツリーが判断した場合に、ブロッキング ステートのあとで最初に開始する移行ステートです。
- ラーニング：インターフェイスはフレーム転送に参加する準備をしています。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：ポートがシャットダウンしているか、ポートにリンクが存在しないか、ポートでスパニング ツリー インスタンスが実行されていないため、インターフェイスはスパニング ツリーに参加していません。

インターフェイスは次のステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 21-1 に、インターフェイスがどのようにステートを移行するかを示します。

図 21-1　スパニング ツリー インターフェイス ステート



スイッチの電源を入れると、スパニング ツリーがデフォルトでイネーブルになり、スイッチ、VLAN、またはネットワークのすべてのインターフェイスは、ブロッキング ステートを経て、移行ステートであるリスニングとラーニングに進みます。スパニング ツリーは、各インターフェイスをフォワーディング ステートまたはブロッキング ステートで安定させます。

スパニング ツリー アルゴリズムによってレイヤ 2 インターフェイスがフォワーディング ステートになると、次の処理が行われます。

1. スパニング ツリーがインターフェイスをブロッキング ステートに移行するためにプロトコル情報を待機する間、インターフェイスはリスニング ステートになります。

2. スパニング ツリーは転送遅延タイマーが期限切れになるのを待機する間、インターフェイスをラーニング ステートに移行し、転送遅延タイマーをリセットします。
3. ラーニング ステートで、インターフェイスはフレーム転送を引き続きブロックしながら、スイッチは転送データベースのエンド ステーションのロケーション情報を学習します。
4. 転送遅延タイマーが期限切れになると、スパニング ツリーはインターフェイスをフォワーディング ステートに移行し、学習とフレーム転送がイネーブルになります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスは、フレーム転送に参加しません。初期化後、各スイッチ インターフェイスに BPDU が送信されます。スイッチは、他のスイッチと BPDU を交換するまで、最初はルートとして機能します。BPDU の交換により、ネットワークのどのスイッチがルートまたはルート スイッチであるかが確定します。ネットワークにスイッチが 1 つしか存在しない場合、BPDU の交換は行われず、転送遅延タイマーは時間切れとなり、インターフェイスはリスニング ステートに移行します。スイッチが初期化したあと、インターフェイスは必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイスで受信したフレームを破棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを破棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、レイヤ 2 インターフェイスがブロッキング ステートのあとに最初に移行するステートです。インターフェイスは、そのインターフェイスがフレーム転送に参加する必要があるとスパニング ツリーが判断したときに、このステートに移行します。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイスで受信したフレームを破棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを破棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレーム転送に参加するための準備を行います。インターフェイスは、リスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイスで受信したフレームを破棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを破棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。インターフェイスは、ラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイスで受信したフレームを受信し、転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ディセーブル ステートのレイヤ 2 インターフェイスは、フレーム転送またはスパニング ツリーに参加しません。ディセーブル ステートのインターフェイスは、動作を行いません。

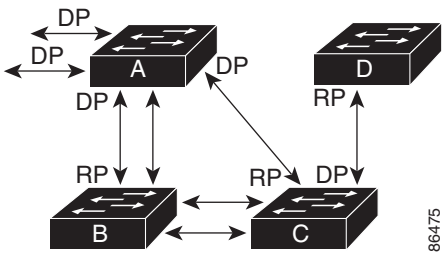
ディセーブルのインターフェイスは、次の機能を実行します。

- インターフェイスで受信したフレームを破棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを破棄します。
- アドレスを学習しません。
- BPDU を受信しません。

スイッチまたはポートがルート スイッチまたはルート ポートになる仕組み

ネットワーク内のすべてのスイッチがデフォルトのスパニング ツリー設定でイネーブルになっている場合、MAC アドレスが最小のスイッチがルート スイッチになります。図 21-2 では、スイッチ A がルート スイッチに選定されます。これは、すべてのスイッチのスイッチ プライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるためです。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチであるとは限りません。最適なスイッチのプライオリティを上げ（数値を下げ）、そのスイッチをルート スイッチにすることで、スパニング ツリーの再計算で最適なスイッチをルートとする新しいトポロジが形成されるようにすることができます。

図 21-2　スパニング ツリー トポロジ



RP = ルート ポート
DP = 指定ポート

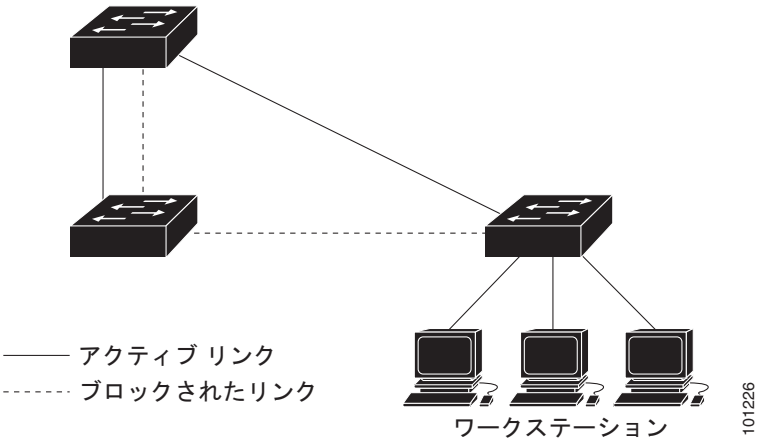
スパニング ツリー トポロジをデフォルトのパラメータに基づいて計算すると、スイッチド ネットワーク上の送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない可能性があります。たとえば、ルート ポートよりも数値が大きいインターフェイスに高速リンクを接続すると、ルート ポートが変更される場合があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B の 1 つのポートがギガビット イーサネット リンクであり、同じスイッチの別のポート（10/100 リンク）がルート ポートであると仮定します。この場合、ネットワーク トラフィックをギガビット イーサネット リンクに流した方が効率的です。ギガビット イーサネット ポートのスパニング ツリー ポート プライオリティをルート ポートよりも上げる（数値を下げる）ことにより、ギガビット イーサネット ポートが新しいルート ポートになります。

スパニング ツリーと冗長接続

図 21-3 に示すように、2 つのスイッチ インターフェイスを別の装置または 2 つの異なる装置に接続することにより、スパニング ツリーで冗長バックボーンを作成できます。スパニング ツリーは、一方のインターフェイスを自動的にディセーブルにしますが、もう一方のインターフェイスに障害が発生した場合は、そのインターフェイスをイネーブルにします。一方のリンクが高速であり、もう一方のリンクが低速である場合、低速のリンクがつねにディセーブルになります。速度が同じである場合、ポート プライオリティとポート ID が加算され、その値が最小であるリンクがスパニング ツリーによってディセーブルに設定されます。

図 21-3　　スパニング ツリーと冗長接続



EtherChannel グループを使用して、スイッチ間に冗長リンクを作成することもできます。詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

スパニング ツリーのアドレス管理

IEEE 802.1D では、異なるブリッジ プロトコルで使用するマルチキャスト アドレスとして、0x00180C2000000 から 0x0180C2000010 までの 17 個を指定しています。これらのアドレスは、削除できないスタティック アドレスです。

スパニング ツリー ステートに関係なく、各スイッチは、0x0180C2000000 から 0x0180C200000F までのアドレスを宛先とするパケットを受信しますが、転送はしません。

スパニング ツリーがイネーブルの場合、スイッチの CPU は、0x0180C2000000 から 0x0180C2000010 までを宛先とするパケットを受信します。スパニング ツリーがディセーブルの場合、スイッチはこれらのパケットを不明なマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、**mac address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルト設定です。ただし、スパニング ツリーの再設定により、多数のステーションの場所が変更されることがあります。これらのステーションは再設定中、5 分以上到達不能になる可能性があるため、アドレス テーブルからステーション アドレスを廃棄して再学習できるように、アドレスエージング タイムが短縮されます。スパニング ツリーの再設定時に短縮されるエージング タイムは、転送遅延パラメータ値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN は個別のスパニング ツリー インスタンスであるため、スイッチは VLAN 単位でエージング タイムを短縮します。ある VLAN でスパニング ツリーが再設定されると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、スイッチに対して設定されたエージング タイムがそのまま適用されます。

スパニング ツリー モードおよびプロトコル

スイッチは、次のスパニング ツリー モードおよびプロトコルをサポートします。

- PVST+：このスパニング ツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に基づいています。すべてのイーサネット ポートベース VLAN で使用されるデフォルトのスパニング ツリー モードです。PVST+ は、スイッチ上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

  PVST+ は、実行される VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用して異なる論理トポロジを作成し、すべてのリンクが使用され、1 つのリンクがオーバーサブスクライブ状態にならないようにすることができます。VLAN 上の PVST+ の各インスタンスに、1 つのルート スイッチがあります。このルート スイッチは、その VLAN に関連するスパニング ツリー情報を、ネットワーク内の他のすべてのスイッチに伝播します。このプロセスにより、各スイッチがネットワークに関する同じ情報を持つようになるため、ネットワーク トポロジが維持されることが保証されます。

- Rapid PVST+：このスパニング ツリー モードは、PVST+ と同じですが、IEEE 802.1w 標準に基づく高速コンバージェンスを使用します。高速コンバージェンスを提供するために、Rapid PVST+ では、トポロジの変更を受信したときに、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。これに対し、PVST+ では、ダイナミックに学習した MAC アドレス エントリに対して、短いエージング タイムを使用します。

  Rapid PVST+ では、PVST+ と同じ設定を使用しているので（指摘した部分を除く）、スイッチで最小限の追加設定を行うだけで済みます。Rapid PVST+ の利点は、複雑な MSTP 設定を学習したり、ネットワークの再プロビジョニングをしたりすることなく、大規模な PVST+ インストール ベースを Rapid PVST+ に移行できることです。Rapid PVST+ モードでは、サポートされる最大数を上限として、各 VLAN が独自のスパニング ツリー インスタンスを実行します。

- MSTP：このスパニング ツリー モードは、IEEE 802.1s 標準に基づいています。複数の VLAN を同じスパニング ツリー インスタンスにマッピングできます。これにより、多数の VLAN をサポートするために必要なスパニング ツリー インスタンスの数が減少します。MSTP は、Rapid Spanning-Tree Protocol（RSTP）（IEEE 802.1w に基づく）上で実行されます。RSTP は、転送遅延をなくし、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行することにより、スパニング ツリーの高速コンバージェンスを実現します。RSTP なしでは MSTP を実行できません。

MSTP の最も一般的な初期配置は、レイヤ 2 スイッチド ネットワークのバックボーン レイヤおよびディストリビューション レイヤへの配置です。詳細については、第 22 章「MSTP の設定」を参照してください。

サポートされるスパニング ツリー インスタンス数の詳細については、次の項を参照してください。

サポートされるスパニング ツリー インスタンス

PVST+ モードまたは Rapid PVST+ モードでは、スイッチは最大 128 のスパニング ツリー インスタンスをサポートします。

MSTP モードでは、スイッチは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数は制限されていません。

スパニング ツリーと VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）の相互運用の詳細については、「スパニング ツリー設定時の注意事項」（P.21-12）を参照してください。

スパニング ツリーの相互運用性と下位互換性

表 21-2 に、ネットワークでサポートされるスパニング ツリー モード間の相互運用性と互換性を示します。

表 21-2　PVST+、MSTP、および Rapid PVST+ の相互運用性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり（制限付き）	あり（PVST+ に戻る）
MSTP	あり（制限付き）	あり	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	あり

MSTP と PVST+ が混在するネットワークでは、Common Spanning Tree（CST; 共通スパニング ツリー）ルートが MST バックボーンの内部に存在する必要があります。また、PVST+ スイッチは複数の MST 領域に接続できません。

ネットワークに Rapid PVST+ を実行するスイッチと PVST+ を実行するスイッチが含まれる場合は、Rapid PVST+ スイッチと PVST+ スイッチを異なるスパニング ツリー インスタンスに設定することを推奨します。Rapid PVST+ スパニング ツリー インスタンスでは、ルート スイッチが Rapid PVST+ スイッチである必要があります。PVST+ インスタンスでは、ルート スイッチが PVST+ スイッチである必要があります。PVST+ スイッチがネットワークのエッジに位置している必要があります。

STP および IEEE 802.1Q トランク

VLAN トランクの IEEE 802.1Q 標準は、ネットワークのスパニング ツリー構築方法にいくつかの制限をもたらします。この標準では、トランクで許可される *すべての* VLAN に対して、スパニング ツリー インスタンスは 1 つしか要求されません。ただし、IEEE 802.1Q トランクを使用して接続している Cisco スイッチのネットワークでは、トランク上で許容される *各* VLAN ごとに 1 つのスパニング ツリー インスタンスが維持されます。

IEEE 802.1Q トランクを使用して Cisco スイッチを非シスコ デバイスに接続すると、Cisco スイッチは PVST+ を使用してスパニング ツリーの相互運用性を提供します。Rapid PVST+ がイネーブルの場合、スイッチは PVST+ の代わりに Rapid PVST+ を使用します。スイッチは、トランクの IEEE 802.1Q VLAN のスパニング ツリー インスタンスと、他社製の IEEE 802.1Q スイッチのスパニング ツリー インスタンスを結合します。

ただし、すべての PVST+ 情報または Rapid PVST+ 情報は、他社製の IEEE 802.1Q スイッチのクラウドにより分離された Cisco スイッチが維持します。Cisco スイッチを分離する他社製の 802.1Q 装置のクラウドは、スイッチ間の単一トランク リンクとして処理されます。

PVST+ は IEEE 802.1Q トランクで自動的にイネーブルとなり、ユーザによる設定は不要です。アクセス ポートおよび Inter-Switch Link（ISL; スイッチ間リンク）トランク ポートでの外部スパニング ツリー動作は、PVST+ の影響を受けません。

IEEE 802.1Q トランクの詳細については、第 16 章「VLAN の設定」を参照してください。

VLAN ブリッジ スパニング ツリー

シスコの VLAN ブリッジ スパニング ツリーは、2 つ以上の VLAN ブリッジ ドメインまたはルーテッド ポート間で DECnet などの非 IP プロトコルを転送するフォールバック ブリッジング機能（ブリッジ グループ）で使用されます。VLAN ブリッジ スパニング ツリーにより、個別の VLAN スパニング ツリー上にブリッジ グループでスパニング ツリーを形成して、VLAN 間に複数の接続が存在する場合にループが形成されるのを防ぐことができます。また、ブリッジされている VLAN の個別のスパニング ツリーが崩れて 1 つのスパニング ツリーになることもなくなります。

VLAN ブリッジ スパニング ツリーをサポートするために、一部のスパニング ツリー タイマーが増加します。フォールバック ブリッジング機能を使用するには、IP サービス イメージをスイッチにインストールする必要があります。詳細については、第 51 章「フォールバック ブリッジングの設定」を参照してください。

スパニング ツリー機能の設定

ここでは、次の設定情報について説明します。

スパニング ツリーのデフォルト設定

表 21-3 に、スパニング ツリーのデフォルト設定を示します。

表 21-3　スパニング ツリーのデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 でイネーブル 詳細については、「サポートされるスパニング ツリー インスタンス」（P.21-10）を参照してください。
スパニング ツリー モード	PVST+（Rapid PVST+ および MSTP がディセーブル）
スイッチ プライオリティ	32768
スパニング ツリー ポート プライオリティ（インターフェイス単位で設定可能）	128.
スパニング ツリー ポート コスト（インターフェイス単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニング ツリー VLAN ポート プライオリティ（VLAN 単位で設定可能）	128.
スパニング ツリー VLAN ポート コスト（VLAN 単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニング ツリー タイマー	hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒 伝送ホールド カウント：6 BPDU

スパニング ツリー設定時の注意事項

スパニング ツリー インスタンスの数より多い VLAN が VTP で定義されている場合、スイッチで PVST+ または Rapid PVST+ をイネーブルにできる VLAN は 128 に限られます。残りの VLAN は、スパニング ツリーがディセーブルの状態で動作します。ただし、MSTP を使用して、複数の VLAN を同じスパニング ツリー インスタンスにマッピングできます。詳細については、第 22 章「MSTP の設定」を参照してください。

スパニング ツリーの 128 のインスタンスがすでに使用されている場合、いずれかの VLAN でスパニング ツリーをディセーブルにし、スパニング ツリーを実行したい VLAN でイネーブルにすることができます。特定の VLAN でスパニング ツリーをディセーブルにするには、**no spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。目的の VLAN でスパニング ツリーをイネーブルにするには、**spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

注意　スパニング ツリーを実行していないスイッチも、スパニング ツリー インスタンスを実行している VLAN 上の他のスイッチがループを切断できるように、受信した BPDU を転送します。したがって、スパニング ツリーは、ネットワークのすべてのループを切断するのに十分な数のスイッチで実行されている必要があります。たとえば、少なくとも VLAN 内の各ループで 1 つのスイッチがスパニング ツリーを実行している必要があります。VLAN 内のすべてのスイッチでスパニング ツリーを実行する必要はありません。ただし、スイッチの最小限のセットだけでスパニング ツリーを実行している場合、ネットワークに不注意に変更を加えることで VLAN に別のループをもたらし、ブロードキャスト ストームが発生することがあります。

（注）　スイッチで使用可能なすべてのスパニング ツリー インスタンスをすでに使用している場合、VTP ドメイン内の任意の場所に別の VLAN を追加すると、スパニング ツリーを実行していないスイッチ上に VLAN が作成されます。該当のスイッチのトランク ポートにデフォルトの許可リストがある場合、新しい VLAN はすべてのトランク ポートで伝送されます。ネットワークのトポロジによっては、このために新しい VLAN に切断できないループが発生する可能性があります。特に、スパニング ツリー インスタンスをすべて使い果たした隣接スイッチが複数ある場合です。スパニング ツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定すると、この可能性を排除できます。許可リストの設定は、ネットワークに別の VLAN を追加する作業が煩雑になる可能性があるため、多くの場合は必要ありません。

スパニング ツリー コマンドは、VLAN スパニング ツリー インスタンスの設定を制御します。スパニング ツリー インスタンスは、VLAN にインターフェイスを割り当てるときに作成します。スパニング ツリー インスタンスは、最後のインターフェイスを別の VLAN に移動すると削除されます。スパニング ツリー インスタンスを作成する前に、スイッチおよびポートのパラメータを設定できます。これらのパラメータは、スパニング ツリー インスタンスを作成したときに適用されます。

スイッチは PVST+、Rapid PVST+、および MSTP をサポートしますが、一度にアクティブにできるバージョンは 1 つだけです（たとえば、すべての VLAN が PVST+ を実行するか、すべての VLAN が Rapid PVST+ を実行するか、またはすべての VLAN が MSTP を実行します）。さまざまなスパニング ツリー モードとそれらの相互運用の詳細については、「スパニング ツリーの相互運用性と下位互換性」（P.21-10）を参照してください。

UplinkFast および BackboneFast の設定時の注意事項については、「オプションのスパニング ツリー設定時の注意事項」（P.23-10）を参照してください。

注意　ループ ガードは、ポイントツーポイント リンクでだけ機能します。リンクの両端に、STP を実行している装置を直接接続することを推奨します。

スパニング ツリー モードの変更

スイッチは、PVST+、Rapid PVST+、および MSTP の 3 つのスパニング ツリー モードをサポートします。デフォルトでは、スイッチは PVST+ プロトコルを実行します。

スパニング ツリー モードを変更するには、特権 EXEC モードで次の手順を実行します。デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}	**（注）**　スパニング ツリー モードを設定します。 • PVST+（デフォルト設定）をイネーブルにするには、**pvst** を選択します。 • MSTP（および RSTP）をイネーブルにするには、**mst** を選択します。詳細な設定手順については、第 22 章「MSTP の設定」を参照してください。 • Rapid PVST+ をイネーブルにするには、**rapid-pvst** を選択します。
ステップ 3	**interface** *interface-id*	（Rapid PVST+ モードの場合だけ推奨）設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスとしては、物理ポート、VLAN、およびポート チャネルがあります。指定できる VLAN ID の範囲は 1 ～ 4094 です。指定できるポート チャネル範囲は 1 ～ 6 です。
ステップ 4	**spanning-tree link-type point-to-point**	（Rapid PVST+ モードの場合だけ推奨）このポートのリンク タイプがポイントツーポイントであることを指定します。 このポート（ローカル ポート）を、ポイントツーポイント リンクを介してリモート ポートに接続した場合、ローカル ポートが指定ポートになると、スイッチはリモート ポートとネゴシエートし、ローカル ポートをフォワーディング ステートにすばやく変更します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**clear spanning-tree detected-protocols**	（Rapid PVST+ モードの場合だけ推奨）スイッチのいずれかのポートがレガシー IEEE 802.1D スイッチのポートに接続されている場合、スイッチ全体でプロトコル移行プロセスを再開します。 このステップは、このスイッチが Rapid PVST+ を実行していることを指定スイッチが検出した場合のオプションです。
ステップ 7	**show spanning-tree summary** および **show spanning-tree interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no spanning-tree mode** グローバル コンフィギュレーション コマンドを使用します。ポートをデフォルト設定に戻すには、**no spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用します。

スパニング ツリーのディセーブル化

スパニング ツリーは、デフォルトでは、VLAN 1 と、新たに作成されたすべての VLAN でイネーブルになります（「サポートされるスパニング ツリー インスタンス」（P.21-10）で示されたスパニング ツリー制限を上限とします）。ネットワーク トポロジにループが存在しないことが確実である場合にだけ、スパニング ツリーをディセーブルにします。

注意　スパニング ツリーがディセーブルになっていて、トポロジにループが存在する場合、過剰なトラフィックと無制限のパケット重複により、ネットワークのパフォーマンスが大幅に低下する可能性があります。

スパニング ツリーを VLAN 単位でディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no spanning-tree vlan** *vlan-id*	*vlan-id* では、指定できる範囲は 1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スパニング ツリーを再びイネーブルにするには、**spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

ルート スイッチの設定

スイッチは、そのスイッチで設定されたアクティブ VLAN ごとに個別のスパニング ツリー インスタンスを維持します。各インスタンスには、スイッチ プライオリティおよびスイッチの MAC アドレスで構成されるブリッジ ID が対応付けられます。VLAN ごとに、最小のブリッジ ID を持つスイッチが、その VLAN のルート スイッチになります。

指定した VLAN のルートになるようにスイッチを設定するには、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値（32768）から非常に小さな値へと変更します。このコマンドを入力すると、各 VLAN のルート スイッチのスイッチ プライオリティが確認されます。拡張システム ID がサポートされているため、スイッチは指定された VLAN のスイッチ プライオリティを 24576 に設定します。これは、この値によってこのスイッチが指定された VLAN のルートになる場合です。

指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です。表 21-1（P.21-4）を参照してください）。

（注）　ルート スイッチになるために必要な値が 1 より小さい場合は、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドは失敗します。

（注）　ネットワークが拡張システム ID をサポートするスイッチとサポートしないスイッチで構成される場合、拡張システム ID をサポートするスイッチがルート ブリッジになることはほぼありません。拡張システム ID によって、古いソフトウェアを実行している接続スイッチのプライオリティよりも VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

（注）　各スパニング ツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリビューション スイッチである必要があります。アクセス スイッチをスパニング ツリーのプライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク内の任意の 2 つのエンド ステーション間における最大スイッチ ホップ数）を指定するには、**diameter** キーワードを使用します。ネットワークの直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

（注）　スイッチをルート スイッチとして設定したあとで、**spanning-tree vlan** *vlan-id* **hello-time**、**spanning-tree vlan** *vlan-id* **forward-time**、および **spanning-tree vlan** *vlan-id* **max-age** の各グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、および最大エージング タイムを手動で設定しないでください。

指定した VLAN のルートになるようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定した VLAN のルートになるようにスイッチを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間における最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。 • （任意）**hello-time** *seconds* には、ルート スイッチによって設定メッセージが生成される間隔を秒単位で指定します。指定できる範囲は 1 ～ 10 です。デフォルト値は 2 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree detail**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

スイッチをセカンダリ ルートとして設定すると、スイッチ プライオリティがデフォルト値（32768）から 28672 に変更されます。これにより、プライマリ ルート スイッチに障害が発生した場合に、このスイッチが指定した VLAN のルート スイッチになる可能性が高くなります。ただし、他のネットワーク スイッチがデフォルトのスイッチ プライオリティである 32768 を使用していて、ルート スイッチになる可能性が低いことが前提です。

このコマンドを複数のスイッチに対して実行すると、複数のバックアップ ルート スイッチを設定できます。プライマリ ルート スイッチ を設定したときに使用したものと同じネットワーク直径と hello タイム値を **spanning-tree vlan** *vlan_id* **root primary** グローバル コンフィギュレーション コマンドで使用してください。

指定した VLAN のセカンダリ ルートになるようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定した VLAN のセカンダリ ルートになるようにスイッチを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間における最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。 • （任意）**hello-time** *seconds* には、ルート スイッチによって設定メッセージが生成される間隔を秒単位で指定します。指定できる範囲は 1 ～ 10 です。デフォルト値は 2 です。 プライマリ ルート スイッチを設定したときに使用したものと同じネットワーク直径と hello タイム値を使用してください。「ルート スイッチの設定」（P.21-15）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree detail**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生すると、スパニング ツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させるインターフェイスには高いプライオリティ（小さい数値）を与え、最後に選択させるインターフェイスには低いプライオリティ（大きい数値）を付けます。すべてのインターフェイスが同じプライオリティ値を使用している場合には、スパニング ツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにし、残りのインターフェイスをブロックします。

インターフェイスのポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートやポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）が含まれます。
ステップ 3	**spanning-tree port-priority** *priority*	インターフェイスのポート プライオリティを設定します。 *priority* に対して、指定できる範囲は 16 単位で、0 ～ 240 です。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 4	**spanning-tree vlan** *vlan-id* **port-priority** *priority*	VLAN のポート プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* に対して、指定できる範囲は 16 単位で、0 ～ 240 です。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show spanning-tree interface** *interface-id* または **show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　**show spanning-tree interface** *interface-id* 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能ステートの場合だけです。それ以外は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認します。

デフォルト設定に戻すには、**no spanning-tree** [**vlan** *vlan-id*] **port-priority** インターフェイス コンフィギュレーション コマンドを使用します。スパニング ツリー ポート プライオリティを使用してトランク ポート上にロード シェアリングを設定する方法については、「ロード シェアリングを目的としたトランク ポートの設定」（P.16-22）を参照してください。

パス コストの設定

スパニング ツリー パス コストのデフォルト値は、インターフェイスのメディア速度から抽出されます。ループが発生すると、スパニング ツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたいインターフェイスには低いコスト値を、最後に選択させたいインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスが同じコスト値を使用している場合には、スパニング ツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにし、残りのインターフェイスをブロックします。

インターフェイスのコストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポートやポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）が含まれます。
ステップ 3	**spanning-tree cost** *cost*	インターフェイスのコストを設定します。 ループが発生すると、スパニング ツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストの低い方が高速で伝送されます。 *cost* に対して、指定できる範囲は 1 ～ 200000000 で、デフォルト値は、インターフェイスのメディア速度から抽出されます。
ステップ 4	**spanning-tree vlan** *vlan-id* **cost** *cost*	VLAN のコストを設定します。 ループが発生すると、スパニング ツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストの低い方が高速で伝送されます。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *cost* に対して、指定できる範囲は 1 ～ 200000000 で、デフォルト値は、インターフェイスのメディア速度から抽出されます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show spanning-tree interface** *interface-id* または **show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　**show spanning-tree interface** *interface-id* 特権 EXEC コマンドは、リンクアップ動作可能ステートのポートの情報だけを表示します。それ以外は、**show running-config** 特権 EXEC コマンドを使用して設定を確認します。

デフォルト設定に戻すには、**no spanning-tree** [**vlan** *vlan-id*] **cost** インターフェイス コンフィギュレーション コマンドを使用します。スパニング ツリー パス コストを使用してトランク ポート上にロード シェアリングを設定する方法については、「ロード シェアリングを目的としたトランク ポートの設定」（P.16-22）を参照してください。

VLAN のスイッチ プライオリティの設定

スイッチ プライオリティを設定して、そのスイッチがルート スイッチに選択されるようにできます。

（注）　このコマンドを使用する場合には注意が必要です。スイッチ プライオリティを変更するには、ほとんどの状況で **spanning-tree vlan** *vlan-id* **root primary** および **spanning-tree vlan** *vlan-id* **root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

VLAN のスイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **priority** *priority*	VLAN のスイッチ プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* に対して、指定できる範囲は 4096 単位で、0 ～ 61440 です。デフォルトは 32768 です。より小さい番号のスイッチが、ルート スイッチとして選択される可能性があります。 有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。それ以外の値はすべて拒否されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **priority** グローバル コンフィギュレーション コマンドを使用します。

スパニング ツリー タイマーの設定

表 21-4 に、スパニング ツリーの全体的なパフォーマンスに影響するタイマーを示します。

表 21-4　スパニング ツリー タイマー

変数	説明
hello タイマー	スイッチから他のスイッチへ hello メッセージをブロードキャストする頻度を制御します。
転送遅延タイマー	インターフェイスが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を制御します。
最大エージング タイマー	インターフェイスで受信したプロトコル情報をスイッチが格納する時間を制御します。
伝送ホールド カウント	1 秒間の一時停止の前に送信できる BPDU の数を制御します。

ここでは、設定の手順を示します。

hello タイムの設定

hello タイムを変更することで、ルート スイッチにより設定メッセージが生成される間隔を設定できます。

（注）　このコマンドを使用する場合には注意が必要です。hello タイムを変更するには、ほとんどの状況で **spanning-tree vlan** *vlan-id* **root primary** および **spanning-tree vlan** *vlan-id* **root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

VLAN の hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **hello-time** *seconds*	VLAN の hello タイムを設定します。hello タイムは、ルート スイッチにより設定メッセージが生成される間隔です。これらのメッセージは、スイッチが動作していることを示します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に対して、指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **hello-time** グローバル コンフィギュレーション コマンドを使用します。

VLAN の転送遅延時間の設定

VLAN の転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **forward-time** *seconds*	VLAN の転送時間を設定します。転送遅延は、スパニング ツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでにインターフェイスが待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に対して、指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **forward-time** グローバル コンフィギュレーション コマンドを使用します。

VLAN の最大エージング タイムの設定

VLAN の最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **max-age** *seconds*	VLAN の最大エージング タイムを設定します。最大エージング タイムは、スイッチがスパニング ツリーの設定メッセージを受信せずに再設定を試行するまで待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に対して、指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **max-age** グローバル コンフィギュレーション コマンドを使用します。

伝送ホールド カウントの設定

伝送ホールド カウントの値を変更することで、BPDU バースト サイズを設定できます。

（注）　このパラメータを大きい値に変更すると、特に Rapid PVST モードの場合に、CPU 使用率に大きな影響が及ぶことがあります。この値を小さくすると、特定のシナリオでコンバージェンスが遅くなることがあります。デフォルト設定を維持することを推奨します。

伝送ホールド カウントを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree transmit hold-count** *value*	1 秒間の一時停止の前に送信できる BPDU の数を設定します。 *value* に対して、指定できる範囲は 1 ～ 20 です。デフォルトは 6 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree detail**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no spanning-tree transmit hold-count** *value* グローバル コンフィギュレーション コマンドを使用します。

スパニング ツリー ステータスの表示

スパニング ツリー ステータスを表示するには、表 21-5 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 21-5　スパニング ツリー ステータスを表示するコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスのスパニング ツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニング ツリー情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示するか、または STP ステート セクションの総行数を表示します。

スパニング ツリー カウンタを消去するには、**clear spanning-tree** [**interface** *interface-id*] 特権 EXEC コマンドを使用します。

show spanning-tree 特権 EXEC コマンドの他のキーワードの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 22

MSTP の設定

この章では、IE 3000 スイッチ上に IEEE 802.1s Multiple Spanning Tree Protocol（MSTP; 多重スパニング ツリー プロトコル）のシスコ実装を設定する方法について説明します。

（注） 多重スパニング ツリー（MST）は、IEEE 802.1s 標準に基づいて実装されます。

MSTP を使用すると、複数の VLAN を同一のスパニング ツリー インスタンスにマッピングできるため、多数の VLAN のサポートに必要なスパニング ツリーのインスタンスの数が減少します。MSTP はデータ トラフィック用に複数の転送パスを提供し、ロード バランシングをイネーブルにします。1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）には影響しないため、ネットワークのフォールトトレランスが改善されます。MSTP の最も一般的な初期配置は、レイヤ 2 スイッチド ネットワークのバックボーン レイヤおよびディストリビューション レイヤへの配置です。この配置により、サービス プロバイダー環境に必要な高可用性ネットワークを提供します。

スイッチが MST モードの場合、IEEE 802.1w に基づく Rapid Spanning Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）が自動的にイネーブルになります。RSTP は、明示的なハンドシェイクによってスパニング ツリーの高速コンバージェンスを提供しています。これにより、IEEE 802.1D の転送遅延が解消し、ルート ポートと宛先ポートを迅速にフォワーディング ステートに移行できます。

MSTP および RSTP のどちらもスパニング ツリーの動作を改善し、（元の）IEEE 802.1D スパニング ツリー、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存の Cisco Per-VLAN Spanning-Tree Plus（PVST+）と Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）に基づく装置との後方互換性を維持します。PVST+ および Rapid PVST+ 機能の詳細については、第 21 章「STP の設定」を参照してください。PortFast、UplinkFast、ルート ガードなどの他のスパニング ツリー機能の詳細については、第 23 章「オプションのスパニング ツリー機能の設定」を参照してください。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

MSTP の概要

MSTP は高速コンバージェンス用に RSTP を使用し、複数の VLAN を 1 つのスパニング ツリー インスタンスにグループ化します。各インスタンスには、他のスパニング ツリーに依存しないスパニング ツリー トポロジがあります。このアーキテクチャにより、データ トラフィック用に複数の転送パスが提供され、ロード バランシングが使用可能になり、多数の VLAN のサポートに必要なスパニング ツリー インスタンスの数が減少します。

ここでは、MSTP の機能について説明します。

- 「多重スパニング ツリー領域」（P.22-2）
- 「IST、CIST、および CST」（P.22-2）
- 「ホップ カウント」（P.22-6）
- 「境界ポート」（P.22-6）
- 「IEEE 802.1s の実装」（P.22-7）
- 「IEEE 802.1D STP との相互運用性」（P.22-8）

設定の詳細については、「MSTP 機能の設定」（P.22-14）を参照してください。

多重スパニング ツリー領域

スイッチが多重スパニング ツリー（MST）のインスタンスに参加するには、常に同じ MST 設定情報を使用してスイッチを設定する必要があります。同じ MST 設定を持つ相互接続されたスイッチの集合体が MST 領域を構成します（図 22-1（P.22-4）を参照）。

MST 設定は、各スイッチが属する MST 領域を制御します。この設定には、領域名、リビジョン番号、MST VLAN/インスタンス間の割り当てマップが含まれています。領域にスイッチを設定するには、**spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用します。その後、スイッチが MST コンフィギュレーション モードを開始します。このモードで、**instance** MST コンフィギュレーション コマンドを使用して複数の VLAN を 1 つの MST インスタンスにマップし、**name** MST コンフィギュレーション コマンドを使用して領域名を指定し、**revision** MST コンフィギュレーション コマンドを使用してリビジョン番号を設定します。

領域は、同じ MST 設定を使用して 1 つまたは複数のメンバーを持つことができます。各メンバーは、RSTP Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を処理する機能を持つ必要があります。ネットワーク内の MST 領域数には制限がありませんが、各領域は最大で 65 のスパニング ツリー インスタンスをサポートできます。インスタンスは、0 ～ 4094 の範囲で任意の数値を特定できます。1 つの VLAN を同時に割り当てることのできるスパニング ツリー インスタンスは 1 つだけです。

IST、CIST、および CST

すべてのスパニング ツリー インスタンスが独立している PVST+ と Rapid PVST+ とは異なり、MSTP は次の 2 つのタイプのスパニング ツリーを確立し、維持します。

- Internal Spanning tree（IST）は、MST 領域で実行されるスパニング ツリーです。

  各 MST 領域内では、MSTP は多重スパニング ツリー インスタンスを維持しています。インスタンス 0 は領域の特殊インスタンスで、Internal Spanning tree（IST）と呼ばれています。他のすべての MST インスタンスは 1 ～ 4094 の番号が付いています。

IST は BPDU を送受信する唯一のスパニング ツリー インスタンスです。他のすべてのスパニング ツリー インスタンス情報は、M レコードに含まれていて、MSTP BPDU 内でカプセル化されています。MSTP BPDU はすべてのインスタンスの情報を伝送するため、多重スパニング ツリー インスタンスをサポートする処理に必要な BPDU の数が大幅に削減されます。

同じ領域内にあるすべての MST インスタンスは同じプロトコル タイマーを共有していますが、各 MST インスタンスにはルート スイッチ ID、ルート パス コストなどの独自のトポロジ パラメータがあります。デフォルトでは、すべての VLAN は IST に割り当てられています。

MST インスタンスは領域に対してローカルです。たとえば、領域 A と B が相互接続されている場合でも、領域 A の MST インスタンス 1 は 領域 B の MST インスタンス 1 から独立しています。

- Common And Internal Spanning Tree（CIST）は、各 MST 領域における IST と MST 領域および単一のスパニング ツリーと相互接続する Common Spanning Tree（CST）の集合体です。

  1 つの領域内で計算されたスパニング ツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーとして認識されます。CIST は IEEE 802.1w、IEEE 802.1s、IEEE 802.1D 標準をサポートするスイッチ間で動作するスパニング ツリー アルゴリズムによって形成されます。MST 領域内にある CIST は領域外にある CST と同じです。

詳細については、「MST 領域内の動作」（P.22-3）および「MST 領域間の動作」（P.22-3）を参照してください。

（注）　IEEE 802.1s 標準の実装により、MST 実装に関連する用語の一部が変更されます。これらの変更点については、表 21-1（P.21-4）を参照してください。

MST 領域内の動作

IST は領域内のすべての MSTP スイッチを接続します。IST が収束する際に、IST のルートは CIST リージョナル ルート（IEEE 802.1s 標準の実装前には *IST* マスターと呼ばれていた）となります（図 22-1（P.22-4）を参照）。このスイッチは、最小のスイッチ ID と CIST ルートへのパス コストが指定された領域内に存在します。CIST リージョナル ルートは、ネットワーク内に領域が 1 つしかない場合は CIST ルートでもあります。CIST ルートが領域外にある場合、領域の境界にある MSTP スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MSTP スイッチが初期化されると、自身が CIST と CIST リージョナル ルートであると主張する BPDU を送信し、CIST ルートと CIST リージョナル ルートに対する両方のパス コストを 0 に設定します。また、スイッチはすべての MST インスタンスも初期化し、自身がこれらすべてのルートであると主張します。スイッチが現在ポートに格納されているものよりも上位の MST ルート情報（小さいスイッチ ID、低いパス コストなど）を受信すると、CIST リージョナル ルートとしての主張を撤回します。

初期化中に、領域内に独自の CIST リージョナル ルートを持つ多くのサブ領域が形成される場合があります。スイッチが上位の IST 情報を受信すると、古いサブ領域を脱退させ、真の CIST リージョナル ルートを持つ新しいサブ領域を加入させます。このように、真の CIST リージョナル ルートを持つサブ領域を除いて、すべてのサブ領域が縮小します。

正しく動作するために、MST 領域内のすべてのスイッチは同じ CIST リージョナル ルートを承認する必要があります。したがって、領域内にある任意の 2 つのスイッチは、共通の CIST リージョナル ルートに収束する場合、MST インスタンスに対するポート ロールだけを同期します。

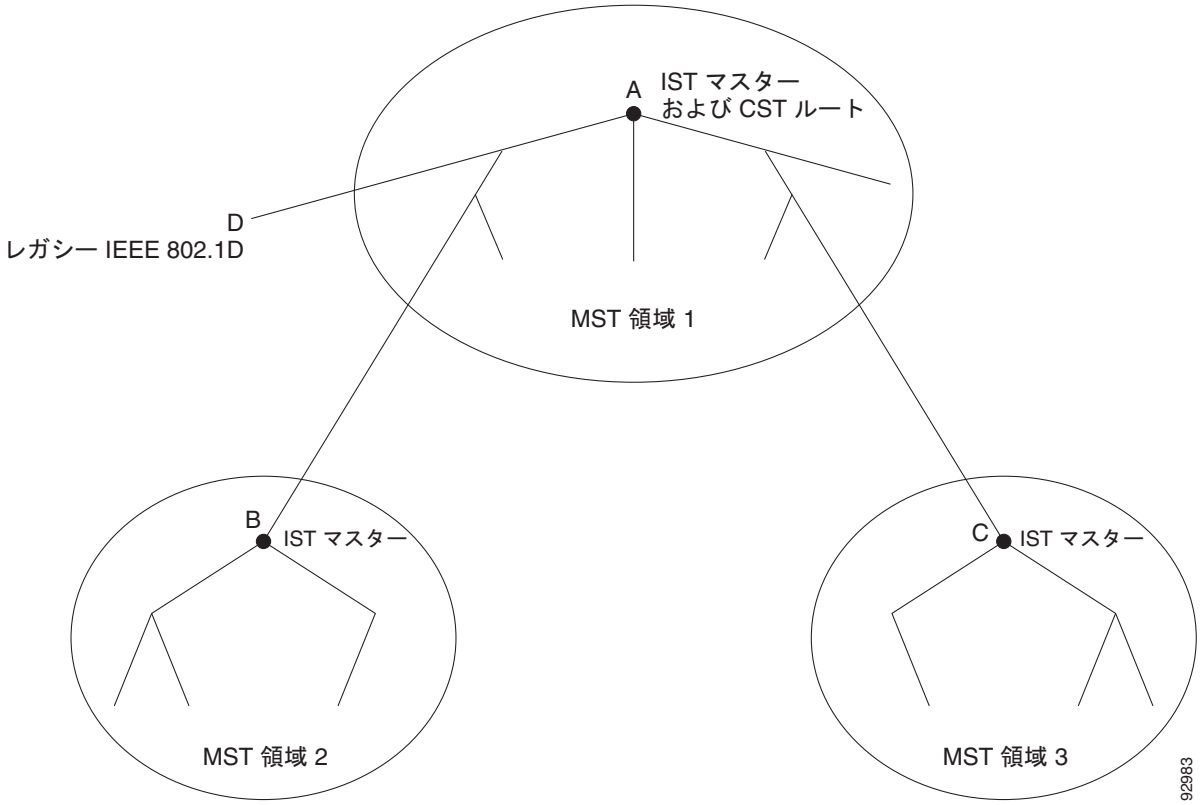
MST 領域間の動作

複数の領域またはレガシー IEEE 802.1D スイッチがネットワーク内に存在する場合、MSTP は CST を確立して維持します。これには、ネットワーク内のすべての MST 領域とすべてのレガシー STP スイッチが含まれます。MST インスタンスは、領域の境界で IST と結合して CST になります。

IST は領域内のすべての MSTP スイッチを接続し、スイッチド ドメイン全体を網羅する CIST 内のサブツリーとして認識されます。サブツリーのルートは CIST リージョナル ルートです。MST 領域は、隣接する STP スイッチおよび MST 領域への仮想スイッチとして認識されます。

図 22-1 に、3 つの MST 領域およびレガシー IEEE 802.1D スイッチ（D）を備えたネットワークを示します。領域 1 の CIST リージョナル ルート（A）は CIST ルートでもあります。領域 2 の CIST リージョナル ルート（B）および領域 3 の CIST リージョナル ルート（C）は、CIST 内の各サブツリーのルートです。すべての領域で RSTP が実行されます。

図 22-1　MST 領域、CIST マスター、および CST ルート



BPDU を送受信するのは CST インスタンスだけで、MST インスタンスはスパニング ツリー情報を BPDU に追加してネイバー スイッチと相互作用し、最終的なスパニング ツリー トポロジを計算します。このため、BPDU 送信に関連したスパニング ツリー パラメータ（たとえば hello タイム、転送時間、最大エージング タイム、最大ホップ数など）は、CST インスタンスだけに設定されますが、すべての MST インスタンスに影響します。スパニング ツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は CST インスタンスと MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用してレガシー IEEE 802.1D スイッチと通信します。MSTP スイッチは MSTP BPDU を使用して MSTP スイッチと通信します。

IEEE 802.1s 用語

シスコ先行標準実装で使用されている MST 命名規則の一部は、*内部*パラメータまたは *リージョナル* パラメータを識別するために変更されています。これらのパラメータは、ネットワーク全体に関連する外部パラメータとは異なり、MST 領域内に限定して重要になります。CIST はネットワーク全体にまたがる唯一のスパニング ツリー インスタンスなので、CIST パラメータだけは、内部修飾子や領域の修飾子ではなく、外部修飾子が必要です。

- CIST ルートは、ネットワーク全体にまたがる一意のインスタンスである CIST のルート スイッチです。
- CIST 外部ルート パス コストは、CIST ルートのコストです。このコストは、MST 領域内では変化しません。MST 領域は CIST に対して単一のスイッチのように見えることに注意してください。CIST 外部ルート パス コストは、これらの仮想スイッチと、どの領域にも属さないスイッチとの間で計算されたルート パス コストです。
- CIST リージョナル ルートは、先行標準実装では IST マスターと呼ばれていました。CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。それ以外の場合は、領域内で CIST ルートに最も近いスイッチが CIST リージョナル ルートになります。CIST リージョナル ルートは IST のルート スイッチとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートのコストです。このコストが関連するのは IST（インスタンス 0）だけです。

表 22-1（P.22-5）では、IEEE 標準の用語とシスコ先行標準の用語とを比較します。

表 22-1　先行標準用語と標準用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

ホップ カウント

IST および MST インスタンスは、スパニング ツリー トポロジを計算するために、コンフィギュレーション BPDU 内のメッセージ エージと最大エージング タイム情報を使用しません。その代わりに、ルートへのパス コストおよび IP Time to Live（TTL）メカニズムに似たホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することで、領域内の最大ホップを設定してそれをその領域内にある IST およびすべての MST インスタンスに適用できます。ホップ カウントは、メッセージ エージ情報と同じ結果（再設定の開始）となります。インスタンスのルート スイッチは、常にコストを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。スイッチがこの BPDU を受信すると、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、この値を伝播します。ホップ カウントが 0 になると、スイッチは BPDU を廃棄して、ポートに維持された情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ エージおよび最大エージング タイム情報は、領域全体で同じままになります。境界にある領域の指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準実装の場合、境界ポートは MST 領域を、RSTP を実行中の単一スパニング ツリー領域、PVST+ または Rapid PVST+ を実行中の単一スパニング ツリー領域、または異なる MST 設定を使用した別の MST 領域に接続します。境界ポートは LAN にも接続されています。LAN の指定スイッチは、単一のスパニング ツリー スイッチ、または異なる MST 設定を持つスイッチのいずれかです。

IEEE 802.1s 標準には境界ポートの定義はありません。IEEE 802.1Q-2002 標準では、ポートが受信できる 2 種類のメッセージとして、内部（同一領域内から発信）と外部を識別します。メッセージが外部の場合、CIST だけが受信します。CIST の役割がルートまたは代替ルートの場合、または外部 BPDU がトポロジ変更の場合、MST インスタンスに影響する可能性があります。メッセージが内部の場合、CIST が CIST 部分を受信し、各 MST インスタンスが各 M レコードを受信します。シスコ先行標準実装では、外部メッセージを受信するポートを境界ポートとして扱います。つまり、ポートでは内部メッセージと外部メッセージの両方を受信できません。

MST 領域には、スイッチと LAN の両方が含まれます。セグメントは、その指定ポートの領域に属します。したがって、セグメントの指定ポートとは異なる領域にあるポートが境界ポートとなります。この定義により、領域の内側にある 2 つのポートが異なる領域に属するポートとセグメントを共有できるので、内部メッセージと外部メッセージの両方をポートで受信できる可能性があります。

シスコ先行標準実装からの主な変更点は、指定ポートが STP 互換モードで動作しない場合は境界ポートとして定義されないことです。

（注）　セグメントにレガシー STP スイッチがある場合、メッセージは常に外部として認識されます。

その他の先行標準実装からの変更点は、CIST リージョナル ルート スイッチ ID フィールドが、RSTP またはレガシー IEEE 802.1Q スイッチが送信側スイッチ ID を持つ場所に挿入されたことです。一貫した送信側スイッチ ID をネイバー スイッチに送信することで、領域全体が単一の仮想スイッチのように実行されます。この例では、A または B がセグメントで指定されているかどうかにかかわらず、スイッチ C はルートの一貫した送信側スイッチ ID が同一の BPDU を受信します。

IEEE 802.1s の実装

IEEE MST 標準のシスコ実装には、標準を満たすために必要な機能と、現在公表されている標準にまだ採用されていない先行標準機能の中で、望ましい機能の一部が含まれています。

ポート ロール命名の変更

境界の役割は最終 MST 標準に含まれなくなりましたが、この境界の概念はシスコ実装でも維持されています。ただし、領域の境界にある MST インスタンス ポートが、対応する CIST ポートのステートに従わない可能性があります。次の 2 つの場合があります。

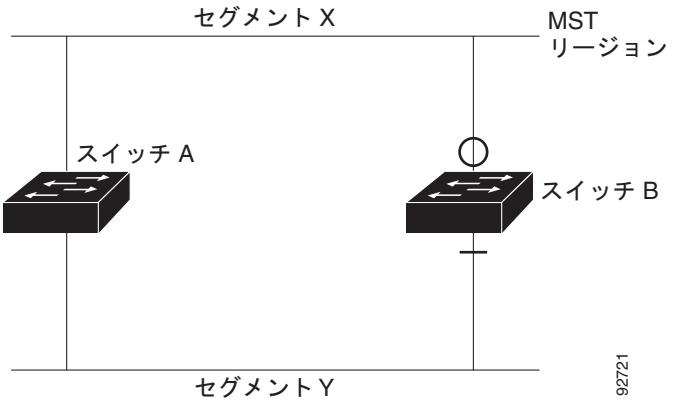
- 境界ポートが CIST リージョナル ルートのルート ポートである場合 : CIST インスタンス ポートが提案されて同期されている場合、すべての対応 MSTI ポートで同期化された（したがって転送された）あとにだけ合意を送り返してフォワーディング ステートに移行することができます。ここで MSTI ポートに、マスターの役割が含まれます。
- 境界ポートが CIST リージョナル ルートのルート ポートではない場合 : MSTI ポートが CIST ポートのステートと役割に従います。標準で提供される情報が少ないので、BPDU（M レコード）を受信しないときに、代わりに MSTI ポートがブロックできる理由を理解するのが難しい場合もあります。この場合、境界の役割がすでに存在していなくても、**show** コマンドを入力すると、出力の *type* カラムで境界としてポートが識別されます。

レガシー スイッチと標準スイッチとの間の相互運用

先行標準スイッチの自動検出が失敗することもあるため、インターフェイス コンフィギュレーション コマンドを使用して先行標準ポートを識別できます。標準スイッチおよび先行標準スイッチとの間で領域を形成することはできませんが、CIST を使用することで相互運用が可能になります。この特定のケースでは、さまざまなインスタンスに対するロード バランシング機能だけが失われます。ポートが先行標準 BPDU を受信する際に、CLI（コマンドライン インターフェイス）はポート設定に応じてさまざまなフラグを表示します。先行標準 BPDU 伝送用に設定されていないポートでスイッチが最初に先行標準 BPDU を受信する際に Syslog メッセージも表示されます。

図 22-2 に、このシナリオを示します。A は標準スイッチ、B は先行標準スイッチで、いずれも同じ領域に設定されているとします。A は CIST のルート スイッチであり、B はセグメント X 上にルート ポート（BX）、セグメント Y 上に代替ポート（BY）を持っています。単一の先行標準 BPDU を送信する前に、セグメント Y がフラップし BY 上のポートが代替になる場合、AY は先行標準スイッチが Y に接続していることを検出できず、標準 BPDU の送信を続けます。ポート BY は境界に固定されるため、スイッチ A と B の間でロード バランシングが実行できません。セグメント X 上には同じ問題が存在しますが、スイッチ B はトポロジ変更を送信します。

図 22-2　標準スイッチおよび先行標準スイッチの相互運用



（注）　標準 MST 実装と先行標準 MST 実装との間では、相互運用を最小限にすることを推奨します。

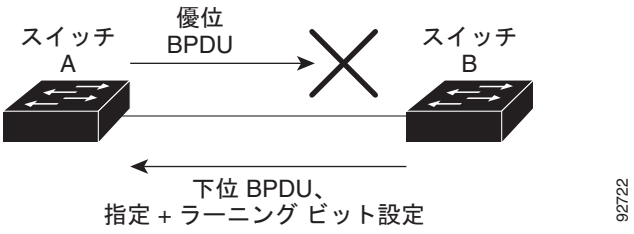
単一方向リンク障害の検出

この機能は IEEE MST 標準には存在しませんが、Cisco IOS リリースには含まれています。ブリッジング ループが発生する可能性のある単一方向リンク障害を検出するために、ソフトウェアが受信した BPDU のポート ロールとステートの一貫性をチェックします。

指定ポートが矛盾を検出すると役割は維持されますが、状態は廃棄ステートに戻ります。これは、接続に矛盾が生じた場合、ブリッジング ループを開始するよりも接続を中断する方が好ましいためです。

図 22-3 に、一般的にブリッジング ループを作成する単一方向リンク障害を示します。スイッチ A はルート スイッチであり、その BPDU はスイッチ B へのリンク上で失われます。RSTP および MST BPDU には、送信ポートの役割とステートが含まれます。この情報を使用して、スイッチ A は、自身が送信した上位 BPDU にスイッチ B が反応しないこと、スイッチ B が指定スイッチであり、ルート スイッチではないことを検出できるようになります。この結果、スイッチ A はそのポートをブロックする（またはブロックし続ける）ため、ブリッジング ループが回避されます。

図 22-3　単一方向リンク障害の検出



IEEE 802.1D STP との相互運用性

MSTP を実行するスイッチは、レガシー IEEE 802.1D スイッチとの相互運用を実現する内蔵プロトコル移行メカニズムをサポートします。このスイッチがレガシー IEEE 802.1D のコンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信すると、そのポートの IEEE 802.1D BPDU だけを送信します。MSTP スイッチは、レガシー BPDU、異なる領域に関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信する際に、ポートが領域の境界にあることも検出できます。

ただし、スイッチは、IEEE 802.1D BPDU を受信しなくなった場合でも、自動的に MSTP モードには戻りません。これは、レガシー スイッチが指定スイッチでない限り、自身がリンクから削除されたかどうかを検出できないためです。また、このスイッチの接続先のスイッチがその領域に加入している場合、引き続きポートに境界の役割を割り当て続ける場合もあります。プロトコル移行プロセスを再起動する（ネイバー スイッチと強制的に再ネゴシエートする）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー スイッチが RSTP スイッチの場合、RSTP BPDU のように MSTP BPDU を処理できます。したがって、MSTP スイッチは、バージョン 0 コンフィギュレーションと TCN BPDU、または境界ポート上のバージョン 3 MSTP BPDU のいずれかを送信します。境界ポートは、LAN、境界ポートの指定が単一のスパニング ツリー スイッチ、または異なる MST 設定を持つスイッチに接続されます。

RSTP の概要

RSTP は、ポイントツーポイント配線を活用してスパニング ツリーの高速コンバージェンスを実現します。スパニング ツリーの再設定は 1 秒以内に実行できます（IEEE 802.1D スパニング ツリーのデフォルト設定の場合は 50 秒かかります）。

ここでは、RSTP の機能について説明します。

- 「ポート ロールとアクティブ トポロジ」（P.22-9）
- 「高速コンバージェンス」（P.22-10）
- 「ポート ロールの同期化」（P.22-11）
- 「ブリッジ プロトコル データ ユニットの形式と処理」（P.22-12）

設定の詳細については、「MSTP 機能の設定」（P.22-14）を参照してください。

ポート ロールとアクティブ トポロジ

RSTP では、ポート ロールを割り当ててアクティブ トポロジを学習することで、スパニング ツリーの高速コンバージェンスを実現しています。「スパニング ツリー トポロジと BPDU」（P.21-3）で説明しているように、RSTP は IEEE 802.1D STP 上に構築されて、最高のスイッチ プライオリティ（最小プライオリティ値）を持つスイッチをルート スイッチとして選択します。次に RSTP は、各ポートに次のいずれかのポート ロールを割り当てます。

- ルート ポート：スイッチがルート スイッチにパケットを転送する際に最適なパス（最小コスト）を提供します。
- 指定ポート：指定スイッチに接続すると、LAN からルート スイッチにパケットを転送する際にパス コストが最小になります。指定スイッチが LAN に接続されるポートを指定ポートと呼びます。
- 代替ポート：現在のルート ポートが提供するルート ブリッジへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供する、スパニング ツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートは、2 つのポートがループバック内でポイントツーポイント リンクで接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が複数ある場合にだけ存在できます。
- ディセーブル ポート：スパニング ツリーの動作中の役割が指定されていないポートです。

ルート ポートまたは指定のポート ロールを割り当てられたポートは、アクティブ トポロジに含まれます。代替ポートまたはバックアップのポート ロールを割り当てられたポートは、アクティブ トポロジから除外されます。

ネットワーク全体でポート ロールが一貫している安定したトポロジでは、RSTP により各ルート ポートおよび指定ポートは即座にフォワーディング ステートに移行し、すべての代替ポートおよびバックアップ ポートは必ず廃棄ステートになります（IEEE 802.1D でのブロッキングと同様）。ポート ステートは、転送および学習処理の動作を制御します。表 22-2 に、IEEE 802.1D と RSTP のポート ステートの比較を示します。

表 22-2　ポート ステートの比較

動作ステータス	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	アクティブ トポロジ内のポートの有無
イネーブル	ブロッキング	廃棄	不可
イネーブル	リスニング	廃棄	不可
イネーブル	ラーニング	ラーニング	あり
イネーブル	フォワーディング	フォワーディング	あり
ディセーブル	ディセーブル	廃棄	不可

シスコの STP 実装製品との整合性をはかるために、このマニュアルではポートの*廃棄*ステートを*ブロッキング*と定義します。指定ポートは、リスニング ステートから開始します。

高速コンバージェンス

RSTP には、スイッチ、スイッチ ポート、または LAN に障害が発生したあとに、短時間で接続を回復する機能があります。エッジ ポート、新規ルート ポート、およびポイントツーポイント リンクで接続されたポートに対して、次のような高速コンバージェンス機能を提供します。

- エッジ ポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して RSTP スイッチにあるエッジ ポートとしてポートを設定した場合、エッジ ポートは即座にフォワーディング ステートに移行します。エッジ ポートは PortFast 対応ポートと同様に、これをイネーブルにできるのは、単一のエンド ステーションに接続されているポート上だけです。
- ルート ポート：RSTP が新規ルート ポートを選択した場合、古いルート ポートをブロックし、即座に新規ルート ポートがフォワーディング ステートに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクを介してポートを別のポートに接続し、ローカル ポートを指定ポートにする場合、ループのないトポロジを実現するために、提案合意ハンドシェイクを使用して相手側ポートと高速移行をネゴシエートします。

  スイッチ A はポイントツーポイント リンクを介してスイッチ B に接続されており、すべてのポートがブロッキング ステートになります（図 22-4 を参照）。スイッチ A のプライオリティは、スイッチ B のプライオリティより少ない数値であるとします。スイッチ A は、自身が指定スイッチであることを提案する、提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）をスイッチ B に送信します。

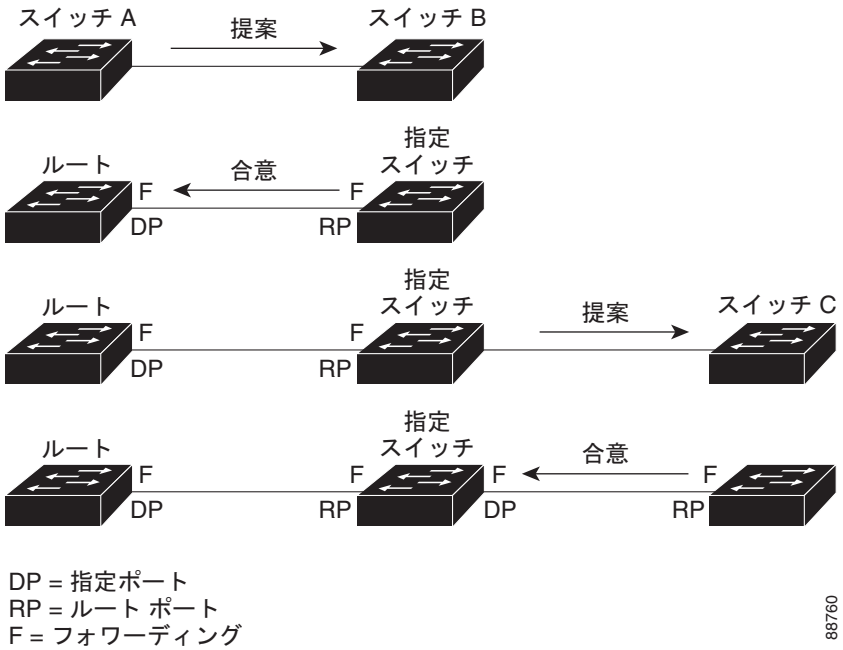
  スイッチ B が提案メッセージを受信すると、提案メッセージの受信元ポートを新しいルート ポートとして選択し、すべての非エッジ ポートを強制的にブロッキング ステートにします。さらに、その新しいルート ポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

  スイッチ A は、スイッチ B から合意メッセージを受信すると、すぐに自身の指定ポートをフォワーディング ステートにします。スイッチ B はそのすべての非エッジ ポートをブロックしており、さらにスイッチ A とスイッチ B はポイントツーポイント リンクで接続されているため、ネットワークにループが形成されません。

スイッチ C がスイッチ B に接続された場合も、同様の一連のハンドシェイク メッセージが交換されます。スイッチ C はスイッチ B に接続されたポートをルート ポートとして選択し、両端のポートはすぐにフォワーディング ステートに移行します。このハンドシェイク プロセスの繰り返しによってアクティブ トポロジに 1 つのスイッチが追加されます。ネットワークが収束するにつれて、この提案合意ハンドシェイクがルートからスパニング ツリーのリーフに進みます。

スイッチは、ポートのデュプレックス モードからリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重ポートは共有接続と見なされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用して、デュプレックス設定で制御されたデフォルト設定を上書きできます。

図 22-4　高速コンバージェンスの提案合意ハンドシェイク



ポート ロールの同期化

スイッチのポート上で 1 つで提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、RSTP は他のすべてのポートを新しいルート情報と強制的に同期させます。

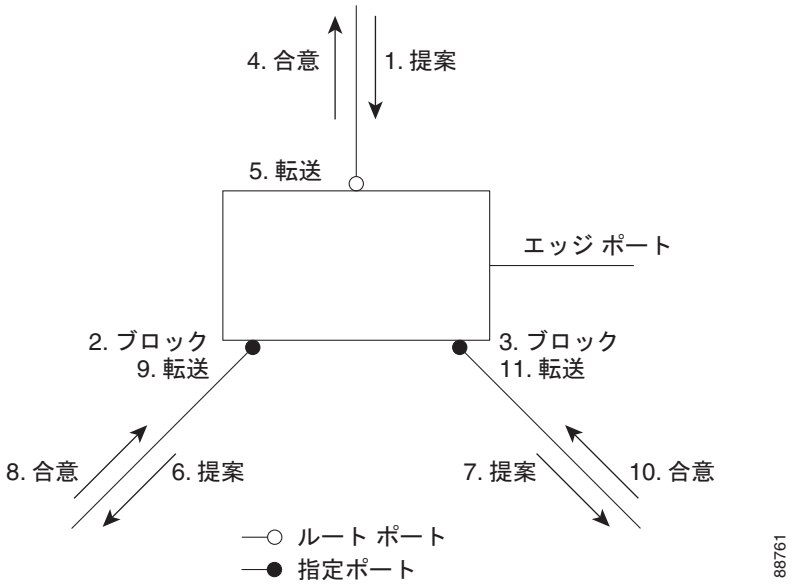
他のポートがすべて同期されると、スイッチはルート ポートで受信した上位のルート情報と同期されます。次のような場合、スイッチ上の個別のポートが同期されます。

- ポートがブロッキング ステートの場合
- エッジ ポート（ネットワークのエッジ上に設定されているポート）の場合

指定ポートがフォワーディング ステートでエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報と強制的に同期されると、その指定ポートはブロッキング ステートに移行します。一般に、RSTP がポートをルート情報と強制的に同期させ、ポートが上記のどの条件も満たしていない場合、そのポートのステートはブロッキングに設定されます。

スイッチはすべてのポートが同期されたことを確認すると、そのルート ポートに対応する指定スイッチに合意メッセージを送信します。ポイントツーポイント リンクによって接続されたスイッチがそれぞれのポート ロールについて合意すると、RSTP はポートのステートをすぐにフォワーディング ステートに移行させます。図 22-5 に、このイベント シーケンスを示します。

図 22-5　高速コンバージェンス時のイベント シーケンス



ブリッジ プロトコル データ ユニットの形式と処理

RSTP BPDU 形式は、プロトコル バージョンが 2 に設定されている点を除いて IEEE 802.1D の BPDU 形式と同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。つまり、バージョン 1 のプロトコル情報が存在しないことを意味します。表 22-3 に、RSTP フラグ フィールドを示します。

表 22-3　RSTP BPDU フラグ

ビット	機能
0	Topology Change（TC; トポロジの変更）
1	提案
2 ～ 3	ポート ロール
00	不明
01	代替ポート
10	ルート ポート
11	指定ポート
4	ラーニング
5	フォワーディング
6	合意
7	Topology Change Acknowledgement（TCA; トポロジ変更の確認）

送信スイッチは、自身をその LAN の指定スイッチとして提案する提案フラグを RSTP BPDU に設定します。提案メッセージでは、ポート ロールは常に指定ポートに設定されます。

送信スイッチは、前の提案を受け入れる合意フラグを RSTP BPDU に設定します。合意メッセージ内のポート ロールは、常にルート ポートに設定されます。

RSTP には、個別の Topology Change Notification（TCN; トポロジ変更通知）BPDU が含まれます。トポロジの変更を示すには、TC フラグを使用します。ただし、IEEE 802.1D スイッチと相互接続性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニング フラグとフォワーディング フラグは、送信ポートのステートに応じて設定されます。

上位 BPDU 情報の処理

ポートが、現在ポートに格納されているものよりも上位のルート情報（小さいスイッチ ID、低いパス コストなど）を受信すると、RSTP が再設定を開始します。そのポートが新しいルート ポートとして提案され選択されると、RSTP は他のすべてのポートを強制的に同期します。

受信した BPDU が提案フラグの設定された RSTP BPDU である場合、スイッチは他のすべてのポートを同期してから合意メッセージを送信します。BPDU が IEEE 802.1D BPDU の場合、スイッチは提案フラグを設定せずにポートの転送遅延タイマーを開始します。新しいルート ポートは、フォワーディング ステートに移行するために 2 倍の転送遅延時間を必要とします。

ポートで上位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる場合、RSTP はポートをブロッキング ステートに設定しますが、合意メッセージを送信しません。指定ポートは、転送遅延タイマーの期限が切れるまで、提案フラグの設定された BPDU の送信を続けます。タイマーの期限が切れると、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

指定ポートが下位の BPDU（現在ポートに格納されているものよりも大きいスイッチ ID、高いパス コストなど）を指定ポート ロールとともに受信すると、すぐにポート自身の情報を返信します。

トポロジの変更

ここでは、スパニング ツリー トポロジ変更を処理する際の RSTP と IEEE 802.1D との相違点を説明します。

- 検出 : IEEE 802.1D では、*どのような*ブロッキング ステートとフォワーディング ステートとの間の移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が発生するのは、ブロッキング ステートからフォワーディング ステートに移行する場合*だけ*です（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジ ポートでステートが変更されても、トポロジの変更は発生しません。RSTP スイッチがトポロジの変更を検出すると、TC 通知を受信するポートを除く、すべての非エッジ ポートから学習済みの情報を削除します。
- 通知 : TCN BPDU を使用する IEEE 802.1D とは異なり、RSTP では使用しません。ただし、IEEE 802.1D との相互接続性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。
- 確認 : RSTP スイッチは、指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信すると、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D スイッチに接続されたルート ポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU を受信した場合、TC 時間タイマーがリセットされます。

  この動作は、IEEE 802.1D スイッチをサポートする場合にだけ必要です。RSTP の BPDU には、TCA ビットが設定されません。

- 伝播：RSTP スイッチが指定ポートまたはルート ポート経由で別のスイッチから TC メッセージを受信すると、そのすべての非エッジ ポート、指定ポート、およびルート ポート（受信ポートを除く）にトポロジ変更が伝播されます。スイッチは、これらのすべてのポートの TC 時間タイマーを開始し、これらのポート上で学習した情報をフラッシュします。
- プロトコルの移行：IEEE 802.1D スイッチとの下位互換性を保つために、RSTP は IEEE 802.1D コンフィギュレーション BPDU と TCN BPDU をポート単位で選択的に送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU を送信する最短時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブの間、スイッチは目的のポートで受信されたすべての BPDU を処理し、プロトコル タイプを無視します。

  ポート移行遅延タイマーの期限が切れたあと、スイッチが IEEE 802.1D BPDU を受信した場合、スイッチは IEEE 802.1D スイッチと接続していると見なし、IEEE 802.1D BPDU だけの使用を開始します。ただし、RSTP スイッチがポートで IEEE 802.1D BPDU を使用していて、タイマーの期限切れのあとに RSTP BPDU を受信した場合、スイッチはタイマーを再起動し、そのポートで RSTP BPDU の使用を開始します。

MSTP 機能の設定

ここでは、次の設定情報について説明します。

MSTP のデフォルト設定

表 22-4 に、MSTP のデフォルト設定を示します。

表 22-4　MSTP のデフォルト設定

機能	デフォルト設定
スパニング ツリー モード	PVST+（Rapid PVST+ および MSTP がディセーブル）
スイッチ プライオリティ（CIST ポート単位に設定可能）	32768
スパニング ツリー ポート プライオリティ（CIST ポート単位に設定可能）	128
スパニング ツリー ポート コスト（CIST ポート単位に設定可能）	1000 Mbps：4 100 Mbps：19 10 Mbps：100
hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

サポートされるスパニング ツリー インスタンス数の詳細については、「サポートされるスパニング ツリー インスタンス」（P.21-10）を参照してください。

MSTP 設定時の注意事項

MSTP 設定時の注意事項を次に示します。

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- 複数のスイッチを同じ MST 領域に設定するには、同じ VLAN/インスタンス間マッピング、同じ設定リビジョン番号、および同じ名前を設定する必要があります。
- スイッチは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数は制限されていません。
- PVST+、Rapid PVST+、および MSTP はサポートされていますが、同時にアクティブにできるバージョンは 1 つだけです（たとえば、すべての VLAN で PVST+ を実行、すべての VLAN で Rapid PVST+ を実行、またはすべての VLAN で MSTP を実行する）。詳細については、「スパニング ツリーの相互運用性と下位互換性」（P.21-10）を参照してください。推奨されるトランク ポート設定の詳細については、「他の機能との相互作用」（P.16-18）を参照してください。
- VTP による MST 設定の伝播はサポートされていません。ただし、CLI（コマンドライン インターフェイス）または SNMP サポートを使用して、MST 領域内にある各スイッチ上で、MST 設定（領域名、リビジョン番号、VLAN/インスタンス間マッピング）を手動で設定することができます。
- ネットワーク内の冗長パス全体でロード バランシングを機能させるためには、すべての VLAN/インスタンス間マッピングの割り当てを一致させる必要があります。一致しない場合、すべてのトラフィックが単一リンクに流れます。

- PVST+ および MST クラウド、または Rapid-PVST+ と MST クラウドとの間でロード バランシングを実現するには、すべての MST の境界ポートがフォワーディング ステートである必要があります。そのためには、MST クラウドの IST マスターも CST のルートにする必要があります。MST クラウドが複数の MST 領域で構成されている場合、MST 領域の 1 つに CST ルートが含まれていなければならず、その他のすべての MST 領域には MST クラウド内に含まれるルートへのパスが、PVST+ または Rapid-PVST+ クラウドよりも良好なものである必要があります。クラウドにスイッチを手動で設定する必要がある場合もあります。
- ネットワークを多数の領域に分割することは推奨しません。ただし、そのような状況が避けられないような場合には、スイッチド LAN をルータまたは非レイヤ 2 装置と相互接続された小規模な LAN に分割することを推奨します。
- UplinkFast、BackboneFast、および cross-stack UplinkFast の設定時の注意事項については、「オプションのスパニング ツリー設定時の注意事項」（P.23-10）を参照してください。
- スイッチが MST モードの場合、ロング パス コスト計算方式（32 ビット）を使用してパス コスト値を計算します。ロング パス コスト計算方式では、次のパス コスト値がサポートされます。

速度	パス コスト値
10 Mbps	2,000,000
100 Mbps	200,000
1 Gbps	20,000
10 Gbps	2,000
100Gbps	200

MST 領域設定の指定と MSTP のイネーブル化

複数のスイッチを同じ MST 領域に設定するには、同じ VLAN/インスタンス間マッピング、同じ設定リビジョン番号、および同じ名前を設定する必要があります。

1 つの領域には、同じ MST 設定を持つ 1 つまたは複数のメンバーを含めることができ、各メンバーには RSTP BPDU を処理する能力が必要となります。ネットワーク内の MST 領域数には制限がありませんが、各領域は最大で 65 のスパニング ツリー インスタンスだけをサポートできます。1 つの VLAN を同時に割り当てることのできるスパニング ツリー インスタンスは 1 つだけです。

MST 領域設定を指定し、MSTP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst configuration**	MST コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**instance** *instance-id* **vlan** *vlan-range*	VLAN を MST インスタンスにマッピングします。 • *instance-id* の場合、範囲は 0 ～ 4094 です。 • **vlan** *vlan-range* の場合、範囲は 1 ～ 4094 です。 VLAN を MST インスタンスにマッピングすると、マッピングは差分で、コマンドに指定された VLAN は以前にマッピングされた VLAN に追加されるか、または VLAN から削除されます。 VLAN 範囲を指定する場合にはハイフンを使用します。たとえば VLAN 1 ～ 63 を MST インスタンス 1 にマッピングする場合は、**instance 1 vlan 1-63** とします。 連続した VLAN を指定する場合には、カンマを使用します。たとえば VLAN 10、20、30 を MST インスタンス 1 にマッピングする場合は、**instance 1 vlan 10, 20, 30** とします。
ステップ 4	**name** *name*	設定名を指定します。*name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。
ステップ 5	**revision** *version*	設定のリビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
ステップ 6	**show pending**	保留中の設定を表示して、確認します。
ステップ 7	**exit**	すべての変更を適用し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**spanning-tree mode mst**	MSTP をイネーブルにします。RSTP もイネーブルになります。 **注意** スパニング ツリー モードを変更すると、すべてのスパニング ツリー インスタンスが以前のモードのために停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+、または MSTP と Rapid PVST+ を同時に実行できません。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config**	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの MST 領域設定に戻るには、**no spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用します。デフォルトの VLAN/インスタンス間マッピングに戻すには、**no instance** *instance-id* [**vlan** *vlan-range*] MST コンフィギュレーション コマンドを使用します。デフォルトの名前に戻すには、**no name** MST コンフィギュレーション コマンドを使用します。デフォルトのリビジョン番号に戻すには、**no revision** MST コンフィギュレーション コマンドを使用します。PVST+ を再度イネーブルにするには、**no spanning-tree mode** または **spanning-tree mode pvst** グローバル コンフィギュレーション コマンドを使用します。

次の例では、MST コンフィギュレーション モードを開始して VLAN 10 ～ 20 を MST インスタンス 1 にマッピングし、領域に *region1* と名前を付けて、構成リビジョンを 1 に設定します。変更確認前の構成を表示して変更を適用し、グローバル コンフィギュレーション モードに戻る方法を示します。

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
```

```
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  --------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

ルート スイッチの設定

スイッチは、マッピングされた VLAN グループのスパニング ツリー インスタンスを維持します。各インスタンスには、スイッチ プライオリティおよびスイッチの MAC アドレスで構成されるスイッチ ID が対応付けられます。VLAN のグループでは、最小のスイッチ ID を持つスイッチがルート スイッチとなります。

スイッチがルート スイッチとなるように設定するには、**spanning-tree mst** *instance-id* **root** グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値（32768）から非常に小さい値に変更します。これにより、このスイッチが指定されたスパニング ツリー インスタンスに対するルート スイッチになります。このコマンドを入力する際に、スイッチがルート スイッチのプライオリティを確認します。拡張システム ID がサポートされているため、スイッチは指定されたインスタンスのスイッチ プライオリティを 24576 に設定します。これは、この値によってこのスイッチが指定されたスパニング ツリー インスタンスのルートになる場合です。

指定インスタンスのルート スイッチに、24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です。表 21-1（P.21-4）を参照してください）。

ネットワークが拡張システム ID をサポートするスイッチとサポートしないスイッチで構成される場合、拡張システム ID をサポートするスイッチがルート ブリッジになることはほぼありません。拡張システム ID によって、古いソフトウェアを実行している接続スイッチのプライオリティよりも VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

各スパニング ツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリビューション スイッチである必要があります。アクセス スイッチをスパニング ツリーのプライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間における最大スイッチ ホップ数）を指定するには、MST インスタンス 0 にだけ使用できる **diameter** キーワードを使用します。ネットワークの直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

（注）　スイッチをルート スイッチとして設定したあとで、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、および最大エージング タイムを手動で設定しないでください。

スイッチをルート スイッチとして設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst** *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	スイッチをルート スイッチとして設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、カンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンドステーション間における最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 の場合だけ使用できます。 • （任意）**hello-time** *seconds* には、ルート スイッチによって設定メッセージが生成される間隔を秒単位で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst** *instance-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	(任意)設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **root** グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

スイッチをセカンダリ ルートとして拡張システム ID サポートとともに設定する場合、スイッチ プライオリティはデフォルト値（32768）から 28672 に変更されます。これにより、プライマリ ルート スイッチに障害が発生した場合に、このスイッチが指定したインスタンスのルート スイッチになる可能性が高くなります。ただし、他のネットワーク スイッチがデフォルトのスイッチ プライオリティである 32768 を使用していて、ルート スイッチになる可能性が低いことが前提です。

このコマンドを複数のスイッチに対して実行すると、複数のバックアップ ルート スイッチを設定できます。プライマリ ルート スイッチ を設定したときに使用したものと同じネットワーク直径と hello タイム値を **spanning-tree mst** *instance-id* **root primary** グローバル コンフィギュレーション コマンドで使用してください。

スイッチをセカンダリ ルート スイッチとして設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst** *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	スイッチをセカンダリ ルート スイッチとして設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、カンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間における最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 の場合だけ使用できます。 • （任意）**hello-time** *seconds* には、ルート スイッチによって設定メッセージが生成される間隔を秒単位で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。 プライマリ ルート スイッチを設定したときに使用したものと同じネットワーク直径と hello タイム値を使用してください。「ルート スイッチの設定」（P.22-18）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst** *instance-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **root** グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生すると、MSTP はポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させるインターフェイスには高いプライオリティ（小さい数値）を与え、最後に選択させるインターフェイスには低いプライオリティ（大きい数値）を付けます。すべてのインターフェイスが同じプライオリティ値を使用している場合には、MSTP はインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにし、残りのインターフェイスをブロックします。

インターフェイスの MSTP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートおよびポート チャネル論理インターフェイスが含まれます。指定できるポート チャネル範囲は 1 ～ 6 です。

	コマンド	目的
ステップ 3	**spanning-tree mst** *instance-id* **port-priority** *priority*	ポート プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、カンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* に対して、指定できる範囲は 16 単位で、0 ～ 240 です。デフォルト値は 128 です。値が小さいほど、プライオリティが高くなります。 プライオリティ値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree mst interface** *interface-id* または **show spanning-tree mst** *instance-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　**show spanning-tree mst interface** *interface-id* 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能ステートの場合だけです。それ以外は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認します。

インターフェイスをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **port-priority** インターフェイス コンフィギュレーション コマンドを使用します。

パス コストの設定

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度から抽出されます。ループが発生すると、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたいインターフェイスには低いコスト値を、最後に選択させたいインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスが同じコスト値を使用している場合には、MSTP はインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにし、残りのインターフェイスをブロックします。

インターフェイスの MSTP コストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポートおよびポートチャネル論理インターフェイスが含まれます。指定できるポート チャネル範囲は 1 ～ 6 です。

	コマンド	目的
ステップ 3	**spanning-tree mst** *instance-id* **cost** *cost*	コストを設定します。 ループが発生すると、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストの低い方が高速で伝送されます。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、カンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *cost* に対して、指定できる範囲は 1 ～ 200000000 で、デフォルト値は、インターフェイスのメディア速度から抽出されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree mst interface** *interface-id* または **show spanning-tree mst** *instance-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　**show spanning-tree mst interface** *interface-id* 特権 EXEC コマンドは、リンクアップ動作可能ステートのポートの情報だけを表示します。それ以外は、**show running-config** 特権 EXEC コマンドを使用して設定を確認します。

インターフェイスをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **cost** インターフェイス コンフィギュレーション コマンドを使用します。

スイッチ プライオリティの設定

スイッチ プライオリティを設定して、そのスイッチがルート スイッチに選択されるようにできます。

（注）　このコマンドを使用する場合には注意が必要です。スイッチ プライオリティを変更するには、ほとんどの状況で **spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

スイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst** *instance-id* **priority** *priority*	スイッチ プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、カンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* に対して、指定できる範囲は 4096 単位で、0 ～ 61440 です。デフォルトは 32768 です。より小さい番号のスイッチが、ルート スイッチとして選択される可能性があります。 プライオリティ値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。それ以外の値はすべて拒否されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst** *instance-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	(任意) 設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **priority** グローバル コンフィギュレーション コマンドを使用します。

hello タイムの設定

hello タイムを変更することで、ルート スイッチにより設定メッセージが生成される間隔を設定できます。

MST インスタンスに hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst hello-time** *seconds*	すべての MST インスタンスに対して hello タイムを設定します。hello タイムは、ルート スイッチにより設定メッセージが生成される間隔です。これらのメッセージは、スイッチが動作していることを示します。 *seconds* に対して、指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst**	設定を確認します。
ステップ 5	**copy running-config startup-config**	(任意) 設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst hello-time** グローバル コンフィギュレーション コマンドを使用します。

転送遅延時間の設定

すべての MST インスタンスに転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst forward-time** *seconds*	すべての MST インスタンスに対して転送時間を設定します。転送遅延は、スパニング ツリー ラーニングおよびリスニング ステートからフォワーディング ステートに移行するまでにポートが待機する秒数です。 *seconds* に対して、指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst forward-time** グローバル コンフィギュレーション コマンドを使用します。

最大エージング タイムの設定

すべての MST インスタンスに最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst max-age** *seconds*	すべての MST インスタンスに対して最大エージング タイムを設定します。最大エージング タイムは、スイッチがスパニング ツリーの設定メッセージを受信せずに再設定を試行するまで待機する秒数です。 *seconds* に対して、指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用します。

最大ホップ カウントの設定

すべての MST インスタンスに最大ホップ カウントを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst max-hops** *hop-count*	BPDU が廃棄され、ポートで維持されていた情報が期限切れになるまでのホップ数を領域内に指定します。 *hold_count* に対して、指定できる範囲は 1 ～ 255 です。デフォルトは 20 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst max-hops** グローバル コンフィギュレーション コマンドを使用します。

リンク タイプの指定による高速移行

「高速コンバージェンス」（P.22-10）で説明しているように、ポイントツーポイント リンクを介してポートを別のポートに接続し、ローカル ポートを指定ポートにする場合、ループのないトポロジを実現するために、提案合意ハンドシェイクを使用して別のポートへの高速移行をネゴシエートします。

デフォルトで、インターフェイスのデュプレックス モードからリンク タイプが制御されます。全二重ポートはポイントツーポイント接続として見なされ、半二重ポートは共有接続として見なされます。MSTP を実行しているリモート スイッチの単一ポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きしてフォワーディング ステートへの高速移行をイネーブルにできます。

デフォルトのリンクタイプ設定を上書きするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポート、VLAN、およびポートチャネル論理インターフェイスが含まれます。指定できる VLAN ID の範囲は 1 ～ 4094 です。指定できるポート チャネル範囲は 1 ～ 6 です。
ステップ 3	**spanning-tree link-type point-to-point**	ポートのリンク タイプがポイントツーポイントになるように指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree mst interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートをデフォルト設定に戻すには、**no spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用します。

ネイバー タイプの指定

トポロジには、先行標準および IEEE 802.1s 標準準拠装置を含めることができます。デフォルトでは、ポートは自動的に先行標準装置を検出しますが、標準および先行標準 BPDU の両方を受信し続けます。装置とネイバー間で不一致が生じた場合、CIST だけがインターフェイスで動作します。

先行標準 BPDU だけを送信するようにポートの設定を選択できます。ポートが STP 互換性モードになっていても、すべての show コマンドで先行標準フラグが表示されます。

デフォルトのリンクタイプ設定を上書きするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 3	**spanning-tree mst pre-standard**	ポートが先行標準 BPDU だけを送信できるように指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree mst interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートをデフォルト設定に戻すには、**no spanning-tree mst prestandard** インターフェイス コンフィギュレーション コマンドを使用します。

プロトコル移行プロセスの再起動

MSTP を実行するスイッチは、レガシー IEEE 802.1D スイッチとの相互運用を実現する内蔵プロトコル移行メカニズムをサポートします。このスイッチがレガシー IEEE 802.1D のコンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信すると、そのポートの IEEE 802.1D BPDU だけを送信します。MSTP スイッチは、レガシー BPDU、異なる領域に関連付けられている MST BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信する際に、ポートが領域の境界にあることも検出できます。

ただし、スイッチは、IEEE 802.1D BPDU を受信しなくなった場合でも、自動的に MSTP モードには戻りません。これは、レガシー スイッチが指定スイッチでない限り、自身がリンクから削除されたかどうかを検出できないためです。スイッチは、接続先のスイッチがその領域に加入している場合、引き続きポートに境界の役割を割り当て続ける可能性もあります。

スイッチ上でプロトコル移行プロセスを再起動する（ネイバー スイッチと強制的に再ネゴシエートする）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

特定のインターフェイスでプロトコル移行プロセスを再起動するには、**clear spanning-tree detected-protocols interface** *interface-id* 特権 EXEC コマンドを使用します。

MST 設定とステータスの表示

スパニング ツリー ステータスを表示するには、表 22-5 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 22-5　MST ステータスを表示するコマンド

コマンド	目的
show spanning-tree mst configuration	MST 領域の設定を表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれる MD5 ダイジェストを表示します。
show spanning-tree mst *instance-id*	指定インスタンスの MST 情報を表示します。
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。

show spanning-tree 特権 EXEC コマンドの他のキーワードの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 23

オプションのスパニング ツリー機能の設定

この章では、IE 3000 スイッチでオプションのスパニング ツリー機能を設定する方法について説明します。スイッチで Per-VLAN Spanning-Tree Plus（PVST+）が稼動している場合は、これらの機能をすべて設定できます。スイッチで Multiple Spanning Tree Protocol（MSTP; 多重スパニング ツリー プロトコル）または Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルが稼動している場合は、明記されている機能だけを設定できます。PVST+ および Rapid PVST+ の設定の詳細については、第 21 章「STP の設定」を参照してください。Multiple Spanning-Tree Protocol（MSTP）の詳細および複数の VLAN を同じスパニング ツリー インスタンスにマッピングする方法については、第 22 章「MSTP の設定」を参照してください。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

オプションのスパニング ツリー機能の概要

ここでは、次の概念情報について説明します。

PortFast の概要

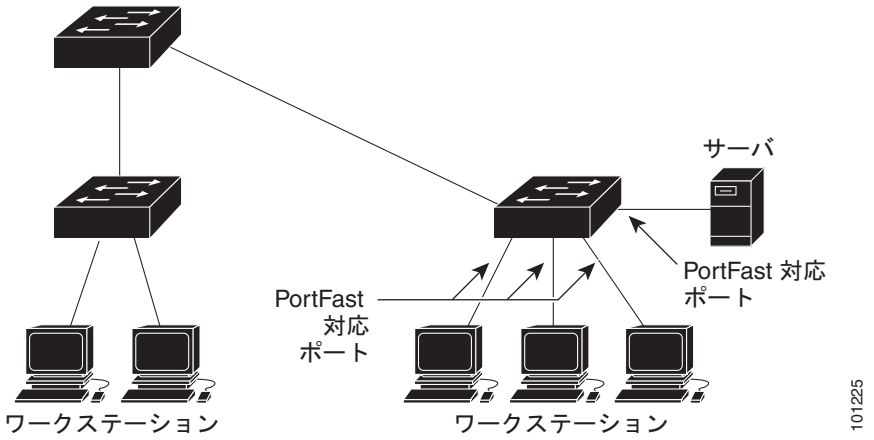
PortFast を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートからフォワーディング ステートに直接移行します。1 台のワークステーションまたはサーバに接続されたインターフェイス上で PortFast を使用すると、図 23-1 に示すように、スパニング ツリーが収束するのを待たずに、ただちに装置をネットワークに接続できます。

1 台のワークステーションまたはサーバに接続されたインターフェイスが Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信しないようにする必要があります。PortFast がイネーブルに設定されているインターフェイスは、スイッチが再起動したときに、通常のスパニング ツリー ステータスのサイクルを遷移します。

（注）　PortFast の目的は、インターフェイスがスパニング ツリーの収束を待機する時間を最小限に抑えることです。したがって、PortFast は、エンド ステーションに接続されたインターフェイス上で使用する場合にだけ有効になります。別のスイッチに接続されたインターフェイスで PortFast をイネーブルにすると、スパニング ツリーのループが発生するおそれがあります。

この機能をイネーブルにするには、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドまたは **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用します。

図 23-1　PortFast 対応インターフェイス



BPDU ガードの概要

BPDU ガード機能は、スイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、グローバル レベルとポート レベルでは、BPDU ガード機能の動作にいくつかの違いがあります。

グローバル レベルでは、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、PortFast 対応ポートで BPDU ガードをイネーブルにします。PortFast 動作ステートのポートが BPDU を受信すると、スパニング ツリーはそれらのポートをシャットダウンします。有効な設定では、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合、認可されていない装置の接続などの無効な設定が存在することを示しており、BPDU ガード機能はそのポートを errdisable ステートにします。この状況が発生した場合、スイッチは違反が発生したポート全体をシャットダウンします。

ポートのシャットダウンを防止するには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用して、違反が発生したポートで問題となっている VLAN だけをシャットダウンします。

インターフェイス レベルでは、PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにできます。ポートは、BPDU を受信すると、errdisable ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービス プロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。

BPDU フィルタリングの概要

BPDU フィルタリング機能は、スイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、グローバル レベルとインターフェイス レベルでは、BPDU ガード機能の動作にいくつかの違いがあります。

グローバル レベルでは、**spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用して、PortFast 対応インターフェイスで BPDU フィルタリングをイネーブルにできます。このコマンドを実行すると、PortFast 動作ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。このインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

インターフェイス レベルでは、PortFast 機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネーブルにできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

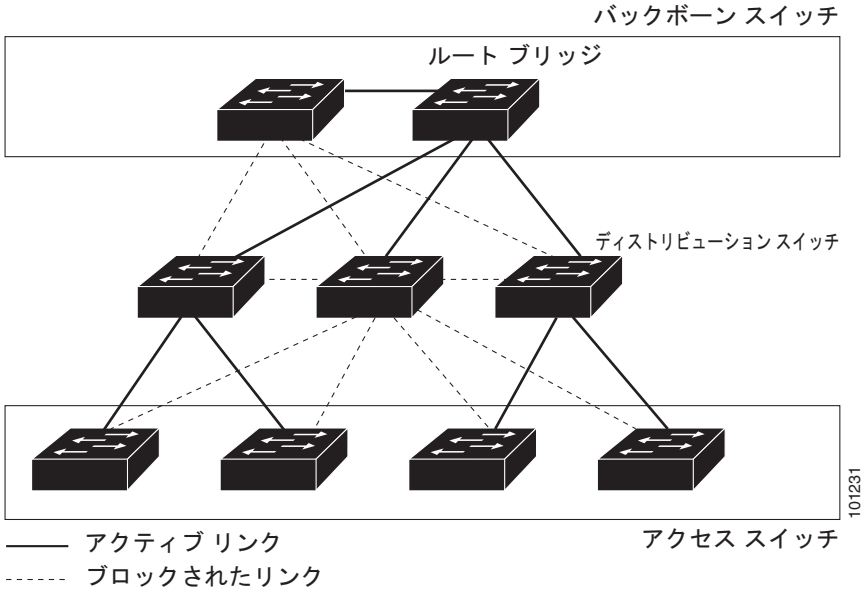
注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが発生することがあります。

BPDU フィルタリング機能は、スイッチ全体または 1 つのインターフェイスでイネーブルにできます。

UplinkFast の概要

階層ネットワークのスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。図 23-2 に、1 つ以上の冗長リンクがディストリビューション スイッチとアクセス スイッチに設定されている複雑なネットワークの例を示します。冗長リンクは、ループを防止するために、スパニング ツリーによってブロックされています。

図 23-2　　階層ネットワークのスイッチ



スイッチは、接続が切断された場合、スパニング ツリーが新しいルート ポートを選択するとすぐに代替パスの使用を開始します。**spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用して UplinkFast をイネーブルにすると、リンクやスイッチに障害が発生した場合、またはスパニング ツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択できます。ルート ポートは、通常のスパニング ツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

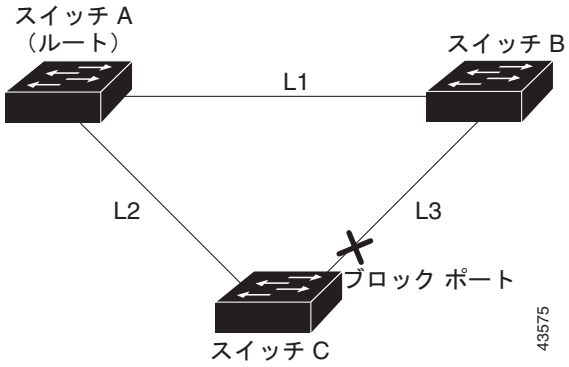
スパニング ツリーが新しいルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングします。このパケットは、インターフェイス上で学習された各アドレスに送信されます。max-update-rate パラメータ（デフォルト値は 150 パケット/秒）の値を小さくすると、このマルチキャスト トラフィックのバーストを制限できます。ただし、0 を入力すると、ステーションを学習するフレームが生成されなくなり、接続の切断後にスパニング ツリー トポロジが収束する速度が遅くなります。

（注）　UplinkFast は、ネットワークのアクセスまたはエッジにある配線クローゼット スイッチで使用するのが最も効果的です。バックボーン装置には適していません。それ以外の用途には、この機能は有用でない場合もあります。

UplinkFast は、直接接続されたリンクの障害発生後高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実現します。アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、どの時点でも、その中の 1 つのインターフェイスだけが転送を行います。つまり、アップリンク グループは、（転送を行う）ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

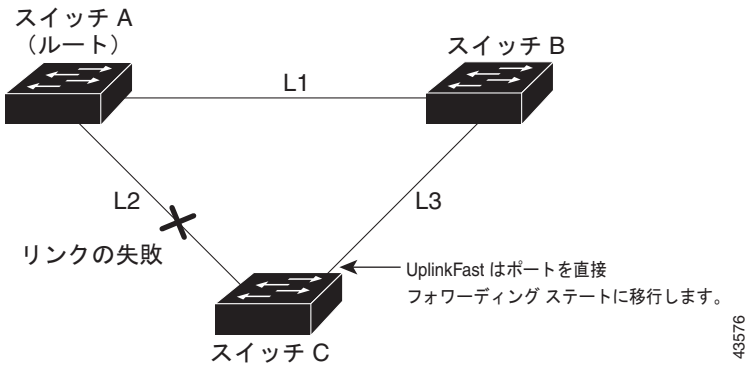
図 23-3 に、リンク障害が発生していないトポロジの例を示します。スイッチ A（ルート スイッチ）は、リンク L1 を通じてスイッチ B に、リンク L2 を通じてスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 23-3　直接リンク障害が発生する前の UplinkFast の例



スイッチ C が、現在アクティブ リンクであるルート ポート上の L2 でリンク障害（*直接*リンク障害）を検出すると、UplinkFast はスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、ただちにフォワーディング ステートに移行させます（図 23-4 を参照）。この切り替えに要する時間は 1 ～ 5 秒です。

図 23-4　直接リンク障害が発生したあとの UplinkFast の例



BackboneFast の概要

BackboneFast は、バックボーンのコアにおける間接障害を検出します。BackboneFast は、アクセス スイッチに直接接続されたリンクの障害に対応する UplinkFast 機能を補完するテクノロジーです。BackboneFast は、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間を制御する最大エージング タイマーを最適化します。スイッチが別のスイッチの指定ポートから下位 BPDU を受信した場合、BPDU は他のスイッチでルートへのパスが失われた可能性があることを示すシグナルとなり、BackboneFast はルートへの代替パスを見つけようとします。

BackboneFast は、**spanning-tree backbonefast** グローバル コンフィギュレーション コマンドでイネーブルになり、スイッチ上のルート ポートまたはブロック インターフェイスが指定スイッチから下位 BPDU を受信すると開始します。下位 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（*間接*リンク）で障害が発生したことを意味します（指定スイッチとルート スイッチ間の接続が切断されています）。スイッチは、スパニング ツリーのルールに従って、**spanning-tree vlan** *vlan-id max-age* グローバル コンフィギュレーション コマンドによって設定された最大エージング タイムの間、下位 BPDU を無視します。

スイッチは、ルート スイッチへの代替パスの有無を判別します。下位 BPDU がブロック インターフェイスに到達した場合は、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート スイッチへの代替パスになります（セルフループ ポートは、ルート スイッチへの代替パスとは見なされません）。下位 BPDU がルート ポートに到達した場合は、すべてのブロック インターフェイスがルート スイッチへの代替パスになります。下位 BPDU がルート ポートに到達し、かつブロック インターフェイスがない場合は、スイッチはルート スイッチへの接続が切断されたものと見なし、ルート ポートの最大エージング タイムを満了させ、通常のスパニング ツリー ルールに従ってルート スイッチになります。

スイッチにルート スイッチへの代替パスがある場合、スイッチはそれらの代替パスを使用して、Root Link Query（RLQ; ルート リンク クエリー）要求を送信します。スイッチは、すべての代替パスに RLQ 要求を送信し、ネットワーク内の他のスイッチからの RLQ 応答を待機します。

ルートへの代替パスがまだ存在していることが判明すると、スイッチは、下位 BPDU を受信したインターフェイスの最大エージング タイムを満了させます。ルート スイッチへのすべての代替パスが、スイッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは、RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルート スイッチに引き続き接続できる場合、スイッチは、下位 BPDU を受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートから、リスニング ステートおよびラーニング ステートを経て、フォワーディング ステートに移行させます。

図 23-5 に、リンク障害が発生していないトポロジの例を示します。スイッチ A（ルート スイッチ）は、リンク L1 を通じてスイッチ B に、リンク L2 を通じてスイッチ C に直接接続しています。スイッチ B に直接接続しているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 23-5　　間接リンク障害が発生する前の BackboneFast の例

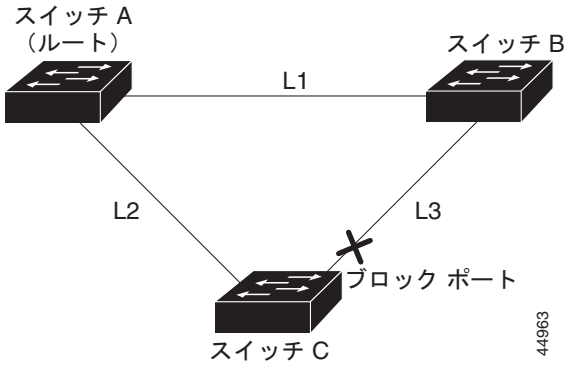


図 23-6 のリンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。一方、スイッチ B は、L1 を通じてルート スイッチに直接接続されているので、この障害を検出できます。障害を検出したスイッチ B は、自身をルートに選定し、スイッチ C への BPDU の送信を開始して、自身がルートであることを通知します。スイッチ C は、スイッチ B から下位 BPDU を受信すると、間接障害が発生したと見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを設定します。ルート スイッチの選定には 30 秒ほどかかります。これは転送遅延時間の 2 倍です（転送遅延時間がデフォルトの 15 秒に設定されている場合）。図 23-6 に、リンク L1 で障害が発生した場合に BackboneFast がトポロジを再構成する例を示します。

図 23-6　間接リンク障害が発生したあとの BackboneFast の例

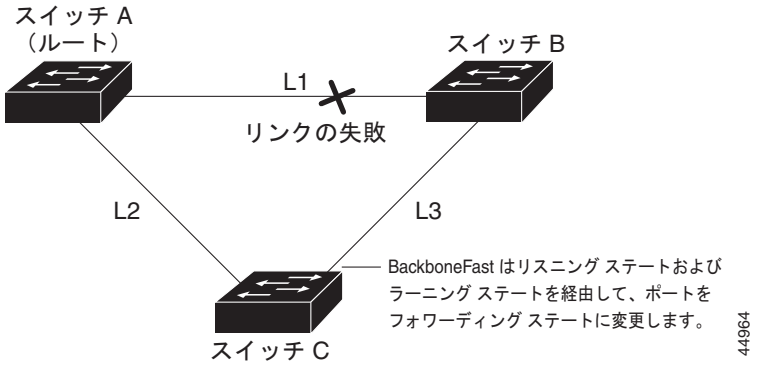
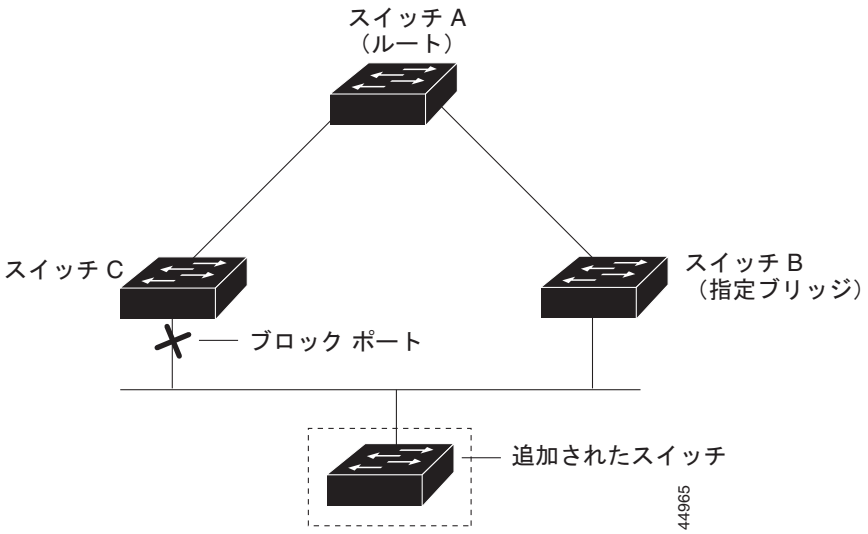


図 23-7 に示すメディア共有型トポロジに新しいスイッチが組み込まれた場合、BackboneFast はアクティブになりません。これは、認識している指定スイッチ（スイッチ B）から下位 BPDU が着信していないためです。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。しかし、他のスイッチはこれらの下位 BPDU を無視します。その結果、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。

図 23-7　メディア共有型トポロジにおけるスイッチの追加



EtherChannel ガードの概要

EtherChannel ガードを使用すると、スイッチと接続装置の間での EtherChannel の設定の矛盾を検出できます。EtherChannel にスイッチ インターフェイスが設定されているにもかかわらず、他の装置のインターフェイスが設定されていない場合、設定の矛盾が生じることがあります。設定の矛盾は、EtherChannel の両端でチャネル パラメータが異なる場合にも生じます。EtherChannel 設定時の注意事項については、「EtherChannel 設定時の注意事項」（P.40-10）を参照してください。

スイッチが他の装置の設定の矛盾を検出した場合、EtherChannel ガードはスイッチ インターフェイスを errdisable ステートにし、エラー メッセージを表示します。

この機能をイネーブルにするには、**spanning-tree etherchannel guard misconfig** グローバル コンフィギュレーション コマンドを使用します。

ルート ガードの概要

Service Provider（SP; サービス プロバイダー）のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多数含まれている場合があります。このようなトポロジでは、図 23-8 に示すように、スパニング ツリーが再設定され、*カスタマー スイッチ*がルート スイッチとして選択されることがあります。カスタマー ネットワーク内のスイッチに接続されている SP スイッチ インターフェイスでルート ガード機能をイネーブルにすると、このような状況を防ぐことができます。スパニング ツリーの計算によってカスタマー ネットワーク内のインターフェイスがルート ポートとして選択された場合、ルート ガードは、カスタマーのスイッチがルート スイッチになったり、ルートへのパスに組み込まれたりしないように、そのインターフェイスを root-inconsistent（ブロック）ステートにします。

SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ（root-inconsistent ステート）、スパニング ツリーによって新しいルート スイッチが選択されます。カスタマーのスイッチがルート スイッチになったり、ルートへのパスに組み込まれたりすることはありません。

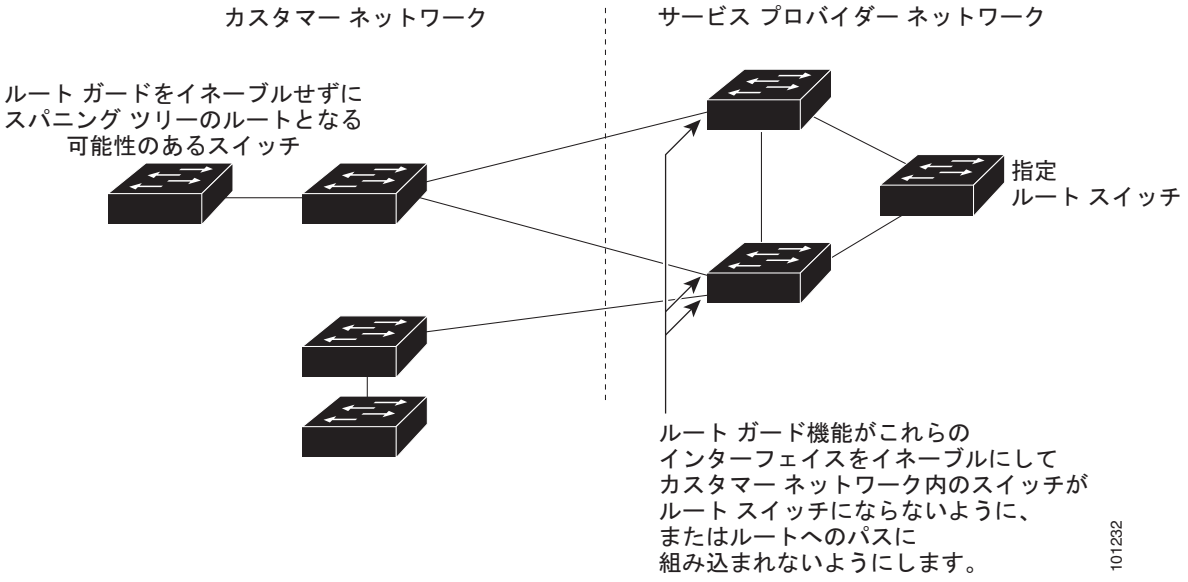
スイッチが Multiple Spanning-Tree（MST; 多重スパニング ツリー）モードで動作している場合、ルート ガードはインターフェイスを強制的に指定ポートにします。ルート ガードによって境界ポートが Internal Spanning-Tree（IST; 内部スパニング ツリー）インスタンスでブロックされた場合、インターフェイスもすべての MST インスタンスでブロックされます。境界ポートは、IEEE 802.1D スイッチまたは異なる MST 領域設定を持つスイッチのいずれかが指定スイッチである LAN に接続されるインターフェイスです。

あるインターフェイスでイネーブルに設定されたルート ガードは、そのインターフェイスが属するすべての VLAN に適用されます。VLAN は、グループ化して MST インスタンスにマッピングできます。

この機能をイネーブルにするには、**spanning-tree guard root** インターフェイス コンフィギュレーション コマンドを使用します。

注意　ルート ガードの使い方を誤ると、接続が切断されることがあります。

図 23-8　サービス プロバイダー ネットワークのルート ガード



ループ ガードの概要

ループ ガードを使用すると、単一方向リンクの原因となる障害によって代替ポートまたはルート ポートが指定ポートになるのを防ぐことができます。この機能は、スイッチド ネットワーク全体でイネーブルにした場合に最も効果があります。ループ ガードを使用すると、代替ポートとルート ポートが指定ポートになるのが防止され、スパニング ツリーがルート ポートまたは代替ポートで BPDU を送信することがなくなります。

この機能をイネーブルにするには、**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドを使用します。

スイッチが PVST+ モードまたは Rapid PVST+ モードで稼動している場合、ループ ガードを使用すると、代替ポートとルート ポートが指定ポートになるのが防止され、スパニング ツリーがルート ポートまたは代替ポートで BPDU を送信することがなくなります。

スイッチが MST モードで稼動している場合は、すべての MST インスタンスでインターフェイスがループ ガードによってブロックされている場合にだけ、非境界ポートで BPDU が送信されなくなります。境界ポートでは、すべての MST インスタンスでインターフェイスがループ ガードによってブロックされます。

オプションのスパニング ツリー機能の設定

ここでは、次の設定情報について説明します。

- 「オプションのスパニング ツリーのデフォルト設定」（P.23-9）
- 「オプションのスパニング ツリー設定時の注意事項」（P.23-10）
- 「PortFast のイネーブル化」（P.23-10）（任意）
- 「BPDU ガードのイネーブル化」（P.23-11）（任意）
- 「BPDU フィルタリングのイネーブル化」（P.23-12）（任意）
- 「冗長リンク用 UplinkFast のイネーブル化」（P.23-13）（任意）
- 「BackboneFast のイネーブル化」（P.23-14）（任意）
- 「EtherChannel ガードのイネーブル化」（P.23-15）（任意）
- 「ルート ガードのイネーブル化」（P.23-15）（任意）
- 「ループ ガードのイネーブル化」（P.23-16）（任意）

オプションのスパニング ツリーのデフォルト設定

表 23-1 に、オプションのスパニング ツリーのデフォルト設定を示します。

表 23-1　オプションのスパニング ツリーのデフォルト設定

機能	デフォルト設定
PortFast、BPDU フィルタリング、BPDU ガード	グローバルにディセーブル（インターフェイス単位で個別に設定されている場合を除く）
UplinkFast	グローバルにディセーブル
BackboneFast	グローバルにディセーブル
EtherChannel ガード	グローバルにイネーブル

表 23-1　オプションのスパニング ツリーのデフォルト設定 （続き）

機能	デフォルト設定
ルート ガード	すべてのインターフェイスでディセーブル
ループ ガード	すべてのインターフェイスでディセーブル

オプションのスパニング ツリー設定時の注意事項

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、PortFast、BPDU ガード、BPDU フィルタリング、EtherChannel ガード、ルート ガード、またはループ ガードを設定できます。

UplinkFast または BackboneFast 機能は、Rapid PVST+ または MSTP 用に設定できます。ただし、スパニング ツリー モードを PVST+ に変更するまで、これらの機能はディセーブル（非アクティブ）のままです。

PortFast のイネーブル化

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、ただちにスパニング ツリー フォワーディング ステートに移行されます。

注意　PortFast は、単一のエンド ステーションをアクセス ポートまたはトランク ポートに接続する場合に限って使用してください。スイッチまたはハブに接続されているインターフェイスでこの機能をイネーブルにすると、スパニング ツリーがネットワーク ループを検出および抑制できなくなり、その結果、ブロードキャスト ストームが発生したり、アドレス学習の問題が生じたりすることがあります。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。詳細については、第 18 章「音声 VLAN の設定」を参照してください。

この機能は、スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合にイネーブルにできます。

PortFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**spanning-tree portfast** [**trunk**]	1 つのワークステーションまたはサーバに接続されたアクセス ポートで PortFast をイネーブルにします。**trunk** キーワードを指定すると、トランク ポートで PortFast をイネーブルにできます。 **（注）** トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポートでは機能しません。 **注意** トランク ポートで PortFast をイネーブルにする前に、トランク ポートとワークステーションまたはサーバの間にネットワーク ループがないことを確認してください。 デフォルトでは、PortFast はすべてのインターフェイスでディセーブルになっています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree interface** *interface-id* **portfast**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注） **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用すると、すべての非トランキング ポートで PortFast 機能をグローバルにイネーブルにできます。

PortFast 機能をディセーブルにするには、**spanning-tree portfast disable** インターフェイス コンフィギュレーション コマンドを使用します。

BPDU ガードのイネーブル化

PortFast 対応ポート（PortFast 動作ステートのポート）で BPDU ガードをグローバルにイネーブルにした場合、スパニング ツリーはそれらのポート上で動作を継続します。ポートは、BPDU を受信しない限り、アップ状態のままです。

有効な設定では、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合、認可されていない装置の接続などの無効な設定が存在することを示しており、BPDU ガード機能はそのポートを errdisable ステートにします。この状況が発生した場合、スイッチは違反が発生したポート全体をシャットダウンします。

ポートのシャットダウンを防止するには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用して、違反が発生したポートで問題となっている VLAN だけをシャットダウンします。

BPDU ガード機能は無効な設定に対する安全対策になります。手動でポートを再び動作させなければならないからです。サービス プロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。

注意　PortFast は、エンド ステーションに接続するポートに限って設定してください。そうしないと、偶発的なトポロジ ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

spanning-tree bpduguard enable インターフェイス コンフィギュレーション コマンドを使用して、PortFast 機能をイネーブルにせずに、任意のポートで BPDU ガードをイネーブルにすることもできます。ポートは、BPDU を受信すると、errdisable ステートになります。

BPDU ガード機能は、スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合にイネーブルにできます。

BPUD ガード機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree portfast bpduguard default**	BPDU ガードをグローバルにイネーブルにします。 デフォルトでは、BPDU ガードはディセーブルになっています。
ステップ 3	**interface** *interface-id*	エンド ステーションに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree portfast**	PortFast 機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BPDU ガードをディセーブルにするには、**no spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用します。

no spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用します。

BPDU フィルタリングのイネーブル化

PortFast 対応インターフェイスで BPDU フィルタリングをグローバルにイネーブルにすると、PortFast 動作ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。このインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

注意　PortFast は、エンド ステーションに接続するインターフェイスに限って設定します。そうしないと、偶発的なトポロジ ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

spanning-tree bpdufilter enable インターフェイス コンフィギュレーション コマンドを使用して、PortFast 機能をイネーブルにせずに、任意のインターフェイスで BPDU フィルタリングをイネーブルにすることもできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが発生することがあります。

BPDU フィルタリング機能は、スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合にイネーブルにできます。

BPUD フィルタリング機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree portfast bpdufilter default**	BPDU フィルタリングをグローバルにイネーブルにします。 デフォルトでは、BPDU フィルタリングはディセーブルになっています。
ステップ 3	**interface** *interface-id*	エンド ステーションに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree portfast**	PortFast 機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BPDU フィルタリングをディセーブルにするには、**no spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用します。

no spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用します。

冗長リンク用 UplinkFast のイネーブル化

スイッチ プライオリティが設定されている VLAN では、UplinkFast をイネーブルにできません。スイッチ プライオリティが設定されている VLAN で UplinkFast をイネーブルにするには、まず **no spanning-tree vlan** *vlan-id* **priority** グローバル コンフィギュレーション コマンドを使用して、VLAN のスイッチ プライオリティをデフォルト値に戻します。

（注）　UplinkFast をイネーブルにすると、スイッチ上のすべての VLAN に影響します。個々の VLAN について UplinkFast を設定することはできません。

UplinkFast 機能は、Rapid PVST+ または MSTP 用に設定できます。ただし、スパニング ツリー モードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

UplinkFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*]	UplinkFast をイネーブルにします。 （任意）*pkts-per-second* に指定できる範囲は 0 ～ 32000 パケット / 秒です。デフォルト値は 150 です。 0 に設定すると、ステーションを学習するフレームが生成されなくなり、接続の切断後にスパニング ツリー トポロジが収束する速度が遅くなります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree summary**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティが 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上に変更した場合、パス コストは変更されません）。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低下します。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

アップデート パケット レートをデフォルト設定に戻すには、**no spanning-tree uplinkfast max-update-rate** グローバル コンフィギュレーション コマンドを使用します。UplinkFast をディセーブルにするには、**no spanning-tree uplinkfast** コマンドを使用します。

BackboneFast のイネーブル化

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニング ツリーの再設定をより早く開始できます。

（注）　BackboneFast を使用する場合は、ネットワーク内のすべてのスイッチで BackboneFast をイネーブルにする必要があります。BackboneFast は、トークン リング VLAN ではサポートされません。この機能は、サードパーティ製のスイッチと組み合わせて使用することができます。

BackboneFast 機能は、Rapid PVST+ または MSTP 用に設定できます。ただし、スパニング ツリー モードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

BackboneFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree backbonefast**	BackboneFast をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show spanning-tree summary**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BackboneFast 機能をディセーブルにするには、**no spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。

EtherChannel ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合は、EtherChannel ガードをイネーブルにして、EtherChannel の設定の矛盾を検出できます。

EtherChannel ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree etherchannel guard misconfig**	EtherChannel ガードをイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree summary**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

EtherChannel ガード機能をディセーブルにするには、**no spanning-tree etherchannel guard misconfig** グローバル コンフィギュレーション コマンドを使用します。

show interfaces status err-disabled 特権 EXEC コマンドを使用すると、EtherChannel の設定の矛盾が原因でディセーブルになっているスイッチ ポートを表示できます。リモート装置では、**show etherchannel summary** 特権 EXEC コマンドを入力して、EtherChannel の設定を確認できます。

設定を修正したあと、誤って設定されていたポートチャネル インターフェイスで、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

ルート ガードのイネーブル化

あるインターフェイスでイネーブルに設定されたルート ガードは、そのインターフェイスが属するすべての VLAN に適用されます。UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロッキング ステートの）バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

（注）　ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

この機能は、スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合にイネーブルにできます。

インターフェイスでルート ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree guard root**	インターフェイスでルート ガードをイネーブルにします。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルになっています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルート ガードをディセーブルにするには、**no spanning-tree guard** インターフェイス コンフィギュレーション コマンドを使用します。

ループ ガードのイネーブル化

ループ ガードを使用すると、単一方向リンクの原因となる障害によって代替ポートまたはルート ポートが指定ポートになるのを防ぐことができます。この機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。ループ ガードは、スパニング ツリーがポイントツーポイントと見なすインターフェイス上でだけ動作します。

（注）　ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

この機能は、スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合にイネーブルにできます。

ループ ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**show spanning-tree active** または **show spanning-tree mst**	どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default**	ループ ガードをイネーブルにします。 デフォルトでは、ループ ガードはディセーブルになっています。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ループ ガードをグローバルにディセーブルにするには、**no spanning-tree loopguard default** グローバル コンフィギュレーション コマンドを使用します。**no spanning-tree loopguard default** グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** インターフェイス コンフィギュレーション コマンドを使用します。

スパニング ツリー ステータスの表示

スパニング ツリー ステータスを表示するには、表 23-2 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 23-2　スパニング ツリー ステータスを表示するコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスのスパニング ツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニング ツリー情報を表示します。
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示するか、またはスパニング ツリー ステート セクションの総行数を表示します。

スパニング ツリー カウンタを消去するには、**clear spanning-tree** [**interface** *interface-id*] 特権 EXEC コマンドを使用します。

show spanning-tree 特権 EXEC コマンドの他のキーワードの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 24

Resilient Ethernet Protocol の設定

この章では、IE 3000 スイッチで Resilient Ethernet Protocol（REP）を使用する方法について説明します。REP はシスコ独自のプロトコルで、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジング ループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

この章の内容は次のとおりです。

REP の概要

1 REP セグメントは、相互接続しているポートのチェーンで、セグメント ID が設定されています。各セグメントは、標準（非エッジ）セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。1 スイッチに、同じセグメントに属することができるポートは 2 つまでで、各セグメント ポートにある外部ネイバーは 1 つだけです。セグメントは共有メディアを通過できますが、どのリンクであっても同じセグメントに属することができるのは 2 ポートだけです。REP は、レイヤ 2 トランク インターフェイスだけでサポートされます。

図 24-1 に、4 つのスイッチにまたがる 6 つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジ ポートとして設定されています。（左側のセグメントのように）すべてのポートが動作可能の場合、斜線で表しているように単一ポートがブロックされます。右側の図のようにネットワークに障害が発生すると、ブロックされたポートがフォワーディング ステートに復帰して、ネットワークの中断を最小限にします。

図 24-1　REP オープン セグメント

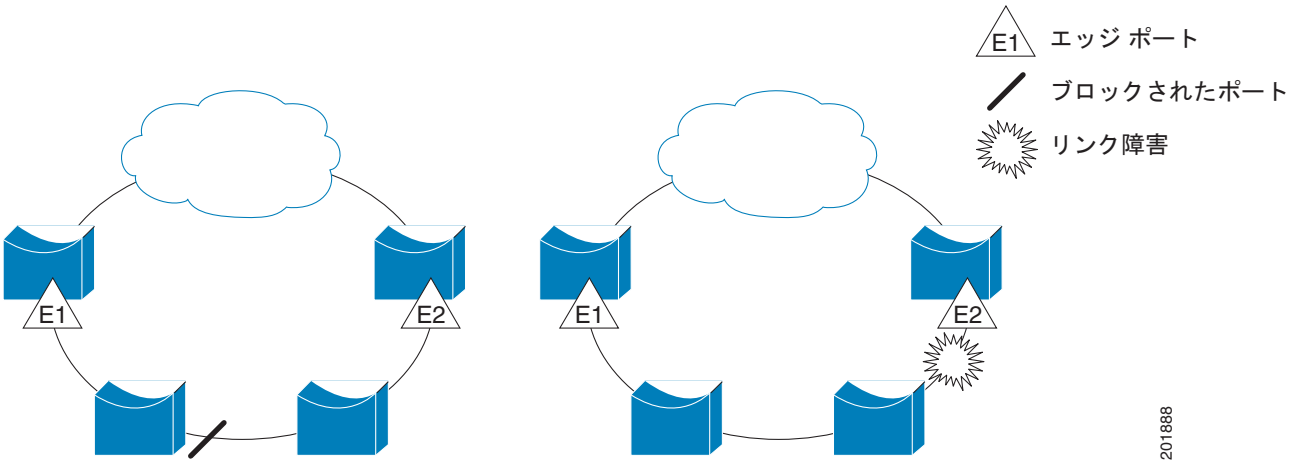
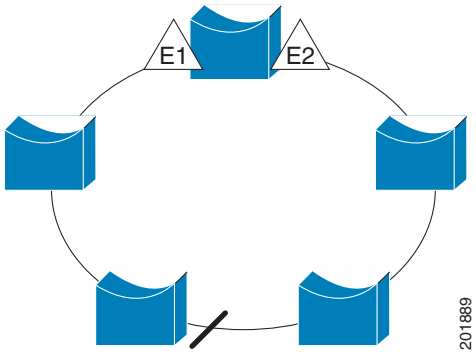


図 24-1 に示されたセグメントは、オープン セグメントで、2 つのエッジ ポート間は接続されていません。REP セグメントは、ブリッジング ループとなる可能性がなく、セグメント エッジが安全に任意のネットワークに接続されます。セグメント内のスイッチに接続されているすべてのホストには、エッジ ポートを通じて残りのネットワークに接続する方法が 2 つありますが、いつでもアクセス可能なのは 1 つだけです。障害により、ホストが通常のゲートウェイにアクセスできない場合、REP がすべてのポートのブロックを解除して、他のゲートウェイを通じた接続を確保します。

図 24-2 で示しているセグメントは、両方のエッジ ポートが同じスイッチ内にあるリング セグメントです。この設定では、セグメントを通じてエッジ ポートと接続します。この設定を使用すると、セグメント内の任意の 2 スイッチ間で冗長接続を形成することができます。

図 24-2　REP リング セグメント



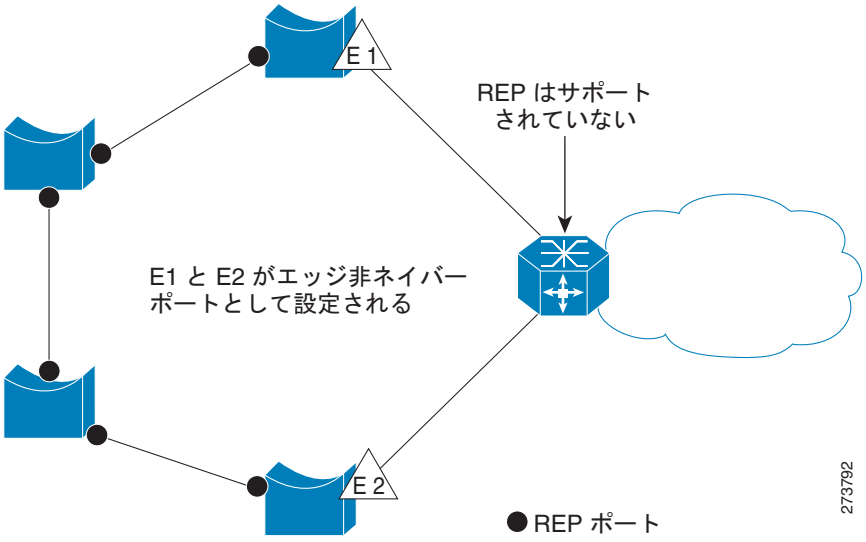
REP セグメントには次のような特徴があります。

- セグメント内の全ポートが動作可能な場合、1 ポート（*代替*ポートと呼ばれる）が各 VLAN でブロック ステートとなります。VLAN ロード バランシングが設定された場合、セグメント内の 2 ポートが VLAN のブロック ステートを制御します。
- セグメント内の 1 つまたは複数のポートが動作不能になると、リンク障害が発生して、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えながら論理的にブロックされるポートが VLAN ごとに選択されます。

REP セグメントに基づいて、ほとんどのネットワーク タイプを構成することができます。また REP は、プライマリ エッジ ポートで制御されているが、セグメント内の任意のポートで発生する、VLAN ロード バランシングをサポートしています。

アクセス リング トポロジでは、ネイバー スイッチで REP がサポートされていない場合があります（図 24-3 を参照）。その場合、そのスイッチ側のポート（E1 と E2）を非ネイバー エッジ ポートとして設定できます。これらのポートは、エッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。たとえば、STP や REP のトポロジ変更通知を集約スイッチに送信するように設定することもできます。その場合、送信される STP Topology Change Notice（TCN; トポロジ変更通知）は、Multiple Spanning-Tree（MST; 多重スパニング ツリー）STP メッセージになります。

図 24-3　　非ネイバー エッジ ポート



REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディング ループが発生します。
- REP はセグメント内の単一障害ポートだけを管理できます。REP セグメント内の複数ポート障害の場合、ネットワークの接続が中断します。
- 冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性を確認するためにエッジ ポート間でエンドツーエンド ポーリング メカニズムを使用していません。ローカル リンク障害検出を実装しています。REP Link Status Layer（LSL; リンク ステータス レイヤ）が REP 対応ネイバーを検出して、セグメント内の接続性を確立します。すべての VLAN は、ネイバーが検出されるまでインターフェイス上でブロックされます。ネイバーが特定されたあと、REP が代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内の各ポートは一意のポート ID を持っています。ポート ID フォーマットは、スパニング ツリー アルゴリズムで使用されるものと類似しており、ポート番号（ブリッジ上で一意）と、関連 MAC アドレス（ネットワーク内で一意）から構成されます。セグメント ポートが起動すると、ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。ポートは、同じセグメント内のネイバーとのスリーウェイ ハンドシェイクを実行したあとで、動作可能と宣言されます。

次のような場合、セグメント ポートは動作可能になりません。

- ネイバーに同じセグメント ID がない
- 複数のネイバーに同じセグメント ID がある
- ネイバーがピアとして、ローカル ポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。ネイバー関係が確立されると、ポートがセグメントの 1 つのブロックされたポート（代替ポート）を決定するようにネゴシエートします。その他のポートのブロックは解除されます。デフォルトで、REP パケットは Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）クラス MAC アドレスに送信されます。パケットは、シスコ マルチキャスト アドレスにも送信できますが、セグメントに障害が発生した場合に Blocked Port Advertisement（BPA; ブロックされたポートのアドバタイズ）メッセージの送信だけに使用されます。パケットは、REP が動作していない装置によって廃棄されます。

高速コンバージェンス

REP が物理リンク ベースで動作し、VLAN 単位ベースで動作しないため、必要なのは全 VLAN で 1 Hello メッセージだけなので、プロトコルの負荷が低減します。指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッディングすることも可能です。これらのメッセージは Hardware Flood Layer（HFL; ハードウェア フラッド レイヤ）で動作し、REP セグメントだけではなくネットワーク全体にフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体で専用の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

ファイバ インターフェイスのコンバージェンス復旧時間の推定値は、200 の VLAN が設定されたローカル セグメントで 200 ミリ秒未満です。VLAN ロード バランシングのコンバージェンスは 300 ミリ秒以下です。

VLAN ロード バランシング

REP セグメント内の 1 エッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジ ポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックすることで実行されます。VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

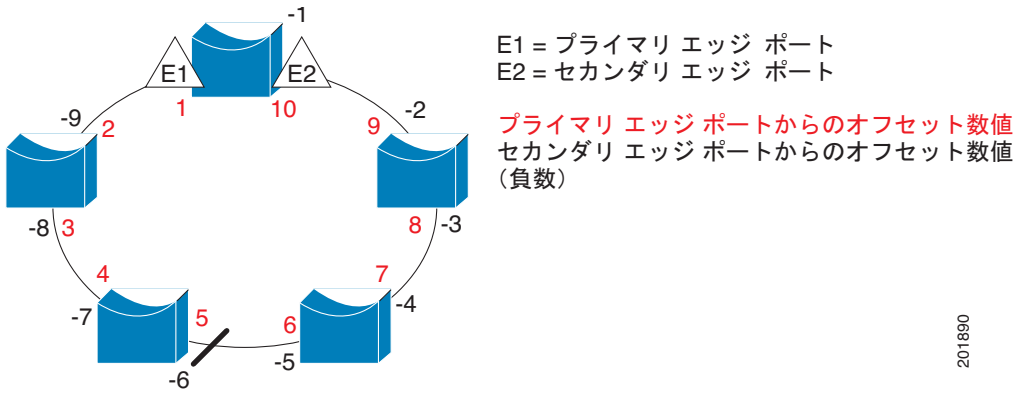
- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep detail** インターフェイス コンフィギュレーション コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ～ +256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

（注）　プライマリ（またはセカンダリ）エッジ ポートからポートのダウンストリーム位置を識別することで、プライマリ エッジ ポートのオフセット番号を設定します。番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

図 24-4 に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートの場合の、セグメントのネイバー オフセット番号を示します。リングの内側にある赤い番号は、プライマリ エッジ ポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリ エッジ ポートからのオフセット番号です。正のオフセット番号（プライマリ エッジ ポートからのダウンストリーム位置）または負のオフセット番号（セカンダリ エッジ ポートからのダウンストリーム位置）のいずれかにより、（プライマリ エッジ ポートを除く）全ポートを識別することができます。E2 がプライマリ エッジ ポートになるとオフセット番号 1 となり、E1 のオフセット番号が -1 になります。

- **preferred** キーワードを入力します。これにより、**rep segment** *segment-id* **preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。

図 24-4　　セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN ロード バランシングを設定する際には、次の 2 種類の方法のいずれかを使用してトリガーを設定する必要もあります。

- プライマリ エッジ ポートのあるスイッチ上で **rep preempt segment** *segment-id* 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- **rep preempt delay** *seconds* インターフェイス コンフィギュレーション コマンドを入力すると、プリエンプション遅延時間を設定できます。リンク障害が発生して回復すると、設定されたプリエンプション期間の経過後に VLAN ロード バランシングが開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。

（注）　VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および回復によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリ ポートで受信されると、これがネットワークに反映され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジ ポートだけによって VLAN ロード バランシングが開始され、セグメントが各エンドでエッジ ポートによって終端されていない場合開始することができません。プライマリ エッジ ポートは、ローカル VLAN ロード バランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。ロード バランシング設定を変更すると、プライマリ エッジ ポートでは、再び **rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済プリエンプト遅延期間が経過してから、新規設定が実行されます。エッジ ポートを通常セグメント ポートに変更しても、既存の VLAN ロード バランシング ステータスは変更されません。新規エッジ ポートを設定すると、新規トポロジ設定になる可能性があります。

スパニング ツリー インタラクション

REP は、STP とも Flex Link 機能とも対話しませんが、どちらとも共存できます。セグメントに属しているポートはスパニング ツリーの制御から削除されるため、セグメント ポートでは STP BPDU の送受信は行われません。したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジ ポートの場所まで両方向に設定されたら、次にエッジ ポートを設定します。

REP ポート

REP セグメント内のポートは、障害、オープン、代替のいずれかになります。

- 通常セグメント ポートとして設定されているポートは、障害ポートとして開始されます。
- ネイバー との隣接関係が確立されると、ポートは代替ポート ステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが発生して、セグメントが安定すると、ブロックされたポートのうちの 1 つが代替ロールのままになって他のすべてのポートがオープン ポートになります。
- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。代替ポートが障害通知を受信すると、オープン ステートに変更され、すべての VLAN を転送します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジ ポートを通常セグメント ポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングの場合、セグメント内に 2 つのエッジ ポートを設定する必要があります。

スパニング ツリー ポートとして再設定されたセグメント ポートは、スパニング ツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキング ポートです。PortFast が設定されていたり、STP がディセーブルの場合、ポートはフォワーディング ステートになります。

REP の設定

セグメントは、チェーンで相互接続しているポートの集合で、セグメント ID が設定されています。REP セグメントを設定するには、REP 管理 VLAN を設定し（またはデフォルト VLAN 1 を使用し）、次にインターフェイス コンフィギュレーション モードを使用してセグメントにポートを追加します。2 つのエッジ ポートをセグメント内に設定して、1 つをプライマリ エッジ ポート、もう 1 つをデフォルトでセカンダリ エッジ ポートにします。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。

別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。オプションで、Segment Topology Change Notice（STCN; セグメント トポロジ変更通知）および VLAN ロード バランシングを送信する場所を設定することもできます。

REP のデフォルト設定

REP はすべてのインターフェイス上でディセーブルです。イネーブルにする際に、エッジ ポートとして設定されていなければインターフェイスは通常セグメント ポートになります。

REP をイネーブルにする際に、STCN の送信はディセーブルで、すべての VLAN はブロックされ、管理 VLAN は VLAN 1 になります。

VLAN ロード バランシングがイネーブルの場合、デフォルトは手動でのプリエンプションで、遅延タイマーはディセーブルになっています。VLAN ロード バランシングが設定されていない場合、手動でのプリエンプション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

- まず 1 ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接するポートを設定することを推奨します。
- 外部ネイバーが設定されておらずセグメント内では 3 つ以上のポートに障害が発生した場合、1 ポートがデータ パス用のフォワーディング ステートになり、設定中の接続性の維持に役立ちます。show rep interface 特権 EXEC コマンド出力では、このポートのポート ロールは *Fail Logical Open* と表示され、他の障害ポートのポート ロールは *Fail No Ext Neighbor* と表示されます。障害ポートの外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行して、代替ポート選定メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままになります。
- REP ポートは、レイヤ 2 トランク ポートである必要があります。
- Telnet 接続を通じて REP を設定する際には注意してください。別の REP インターフェイスがメッセージを送信してブロック解除するまで REP はすべての VLAN をブロックするため、同じインターフェイスを通じてスイッチにアクセスする Telnet セッションで REP をイネーブルにすると、スイッチへの接続が失われる可能性があります。
- REP と STP または REP と Flex Link を同じセグメントやインターフェイスで実行できません。
- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを確認してください。エッジで実行されていない STP 接続は、REP セグメントでは STP が実行されないため、ブリッジング ループが発生する可能性があります。すべての STP BPDU は、REP インターフェイスで廃棄されます。
- 同じ許容 VLAN セットでセグメント内のすべてのトランク ポートを設定する必要があります。そうでない場合、設定ミスが発生します。

- REP ポートは以下の規則に従います。
  - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
  - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。
  - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジ ポートであるか、両方のポートが通常セグメント ポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。
  - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメント ポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われます。
- REP インターフェイスがブロック ステートになり、ブロック解除しても安全であると通知されるまでブロック ステートのままになります。突然の接続切断を避けるために、これを意識しておく必要があります。
- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコ マルチキャスト アドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままどのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。**rep lsl-age-time**r *value* インターフェイス コンフィギュレーション コマンドを使用して、120 ～ 10000 ミリ秒の時間を設定します。LSL hello タイマーは、このエージング タイマーの値を 3 で割った値に設定されます。通常の動作では、ピア スイッチのエージング タイマーが満了になって hello メッセージが確認されるまでに LSL hello が 3 回送信されます。
  - Cisco IOS Release 12.2(52)SE では、LSL エージング タイマーの範囲が 3000 ～ 10000 ミリ秒（500 ミリ秒単位）から 120 ～ 10000 ミリ秒（40 ミリ秒単位）に変更されています。REP ネイバー装置で Cisco IOS release 12.2(52)SE 以降が実行されていない場合は、タイマーの値を 3000 ミリ秒未満に設定しないでください。3000 ミリ秒未満の値を設定すると、要求されている時間内にネイバー スイッチが応答しないため、ポートがシャットダウンします。
  - EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。
- REP LSL エージング タイマーを設定するときには、リンクの両端で同じ値を設定するようにしてください。リンクの両端で同じ値が設定されていないと、REP リンク フラップが発生します。
- REP ポートは、これらのポート タイプのいずれかに設定できません。
  - SPAN 宛先ポート
  - トンネル ポート
  - アクセス ポート
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。
- スイッチごとに最大で 64 REP セグメントです。

REP 管理 VLAN の設定

ロード バランシング時のリンク障害や VLAN ブロッキングの通知のメッセージをソフトウェアでリレーすることによって発生する遅延を回避するために、REP は HFL で通常のマルチキャスト アドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。ドメイン全体の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- 1 つのスイッチと 1 つのセグメントで 1 つの管理 VLAN だけが可能です。ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rep admin vlan** *vlan-id*	管理 VLAN を指定します。指定できる範囲は 2 ～ 4094 です。デフォルトは VLAN 1 です。管理 VLAN を 1 に設定するには、**no rep admin vlan** グローバル コンフィギュレーション コマンドを実行します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show interface** [*interface-id*] **rep detail**	REP インターフェイスのいずれか 1 つの設定を確認します。
ステップ 5	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、管理 VLAN を VLAN 100 として設定して、REP インターフェイスの 1 つに **show interface rep detail** コマンドを入力して設定を確認する例を示します。

```
Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end
Switch# show interface gigabitethernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
```

```
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

REP インターフェイスの設定

REP 動作の場合、各セグメント インターフェイスでこれをイネーブルにして、セグメント ID を指定します。このステップは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

インターフェイス上で REP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）を指定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**switchport mode trunk**	インターフェイスをレイヤ 2 トランク ポートとして設定します。

	コマンド	目的
ステップ 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]	インターフェイスで REP をイネーブルにして、セグメント番号を指定します。指定できるセグメント ID の範囲は 1 ～ 1024 です。これらの任意のキーワードは利用可能です。 **（注）** 各セグメントに 1 つのプライマリ エッジ ポートを含めて、2 つのエッジ ポートを設定する必要があります。 • **edge** を入力して、ポートをエッジ ポートとして設定します。**primary** キーワードなしで **edge** を入力すると、ポートがセカンダリ エッジ ポートとして設定されます。各セグメントにあるエッジ ポートは 2 つだけです。 • （任意）エッジ ポート上で、**primary** を入力してポートをプライマリ エッジ ポートとして設定し、VLAN ロード バランシングを設定するポートを設定することができます。 • （任意）**no-neighbor** を入力して、外部 REP ネイバーを持たないポートをエッジ ポートとして設定します。そのポートはエッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。 **（注）** 各セグメントにあるプライマリ エッジ ポートは 1 つだけですが、2 つの異なるスイッチにエッジ ポートを設定して **primary** キーワードを両方のスイッチに入力しても、その設定は許容されます。ただし、REP ではセグメント プライマリ エッジ ポートとして 1 つのポートだけが選択されます。**show rep topology** 特権 EXEC コマンドを入力すると、セグメントのプライマリ エッジ ポートを指定することができます。 • （任意）**preferred** を入力して、ポートが優先代替ポートであるか、VLAN ロード バランシングの優先ポートであるのかを示します。 **（注）** ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。
ステップ 5	**rep stcn** {**interface** *interface-id* | **segment** *id-list* | **stp**}	（任意）STCN を送信するようにエッジ ポートを設定します。 • **interface** *interface-id* を入力して、STCN を受信するための物理インターフェイスまたはポート チャネルを指定します。 • **segment** *id-list* を入力して、STCN を受信するための 1 つまたは複数のセグメントを指定します。有効範囲は 1 ～ 1024 です。 • **stp** を入力して、STCN を STP ネットワークに送信します。

	コマンド	目的
ステップ 6	**rep block port** {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**}	（任意）プライマリ エッジ ポートに VLAN ロード バランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。 • **id** *port-id* を入力して、ポート ID で代替ポートを指定します。セグメント内の各ポートにポート ID が自動的に生成されます。**show interface** *interface-id* **rep** [**detail**] 特権 EXEC コマンドを入力して、インターフェイス ポート ID を表示できます。 • *neighbor_offset* 番号を入力して、代替ポートをエッジ ポートからのダウンストリーム ネイバーとして指定します。有効範囲は -256 ～ 256 で、負数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。値 **0** は無効です。**-1** を入力して、セカンダリ エッジ ポートを代替ポートとして識別します。ネイバー オフセット番号付けの例については、図 24-4 (P.24-5) を参照してください。 **（注）** プライマリ エッジ ポート（オフセット番号 1）にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力しません。 • **preferred** を入力して、すでに VLAN ロード バランシングの優先代替ポートとして指定されている通常セグメント ポートを選択します。 • **vlan** *vlan-list* を入力して、1 VLAN または VLAN 範囲をブロックします。 • **vlan all** を入力して、すべての VLAN をブロックします。 **（注）** REP プライマリ エッジ ポートだけに、このコマンドを入力します。
ステップ 7	**rep preempt delay** *seconds*	（任意）リンク障害および回復後に自動的に VLAN ロード バランシングをトリガーする場合、このコマンドを入力して、プリエンプション遅延時間を設定する必要があります。遅延時間の範囲は 15 ～ 300 秒です。デフォルトは、遅延時間のない手動によるプリエンプションです。 **（注）** REP プライマリ エッジ ポートだけに、このコマンドを入力します。
ステップ 8	**rep lsl-age-timer** *value*	（任意）ネイバーからの hello が受信されないままどのくらいの時間（ミリ秒）が経過すると REP インターフェイスがダウンするかを設定します。 指定できる範囲は 120 ～ 10000 ミリ秒（40 ミリ秒単位）です。デフォルト値は 5000 ミリ秒（5 秒）です。 **（注）** ネイバー装置で Cisco IOS Release 12.2(52)SE 以降が実行されていない場合は、指定できる範囲が 3000 ～ 10000 ミリ秒（500 ミリ秒単位）になります。EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。
ステップ 9	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 10	**show interface** [*interface-id*] **rep** [**detail**]	REP インターフェイス コンフィギュレーションを確認します。
ステップ 11	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各コマンドの **no** 形式を使用します。**show rep topology** 特権 EXEC コマンドを入力して、セグメント内のどのポートがプライマリ エッジ ポートなのかを確認します。

次に、インターフェイスをセグメント 1 のプライマリ エッジ ポートに設定し、STCN をセグメント 2 ～ 5 に送信し、代替ポートをポート ID 0009001818D68700 のポートとして設定して、セグメント ポート障害および回復後の 60 秒のプリエンプション遅延後にすべての VLAN をブロックする例を示します。このインターフェイスは、ネイバーからの hello が受信されないまま 6000 ミリ秒が経過するとダウンするように設定されています。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end
```

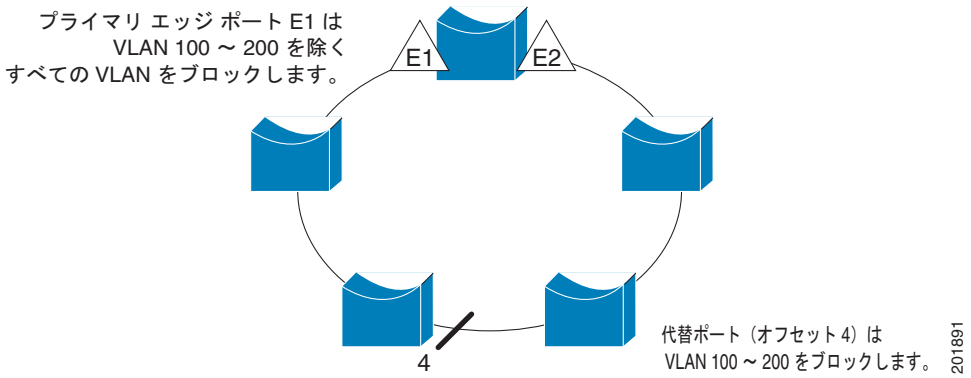
次に、インターフェイスに外部 REP ネイバーがない場合の同じ設定の例を示します。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
```

次に、図 24-5 の、VLAN ブロッキング コンフィギュレーションを設定する例を示します。代替ポートは、ネイバー オフセット番号 4 のネイバーです。手動によるプリエンプションのあとに、VLAN 100 ～ 200 がこのポートでブロックされ、その他のすべての VLAN がプライマリ エッジ ポート E1（ギガビット イーサネット ポート 1/0/1）でブロックされます。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

図 24-5　VLAN ブロッキングの例



VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリ エッジ ポートでプリエンプション遅延時間を設定する **rep preempt delay** *seconds* インターフェイス コンフィギュレーション コマンドを入力しない場合、デフォルトでは、セグメントでの VLAN ロード バランシングのトリガーは手動になっています。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。**rep preempt segment** *segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

	コマンド	目的
ステップ 1	**rep preempt segment** *segment-id*	手動により、セグメント上の VLAN ロード バランシングをトリガーします。 実行前にコマンドを確認する必要があります。
ステップ 2	**show rep topology**	REP トポロジ情報を表示します。

REP の SNMP トラップ設定

リンク動作ステータス変更およびポート ロール変更について SNMP サーバに通知するために、REP 固有のトラップの送信をスイッチに設定できます。REP トラップを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp mib rep trap-rate** *value*	REP トラップを送信するようにスイッチでイネーブルにして、1 秒あたりのトラップの送信数を設定します。範囲は 0 ～ 1000 です。デフォルトは 0（制限なし、発生するたびにトラップが送信される）です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	REP トラップ コンフィギュレーションを確認します。
ステップ 5	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

トラップを削除するには、**no snmp mib rep trap-rate** グローバル コンフィギュレーション コマンドを入力します。

1 秒あたり 10 の割合で REP トラップを送信するようにスイッチを設定する例を示します。

```
Switch(config)# snmp mib rep trap-rate 10
```

REP のモニタ

表 24-1　REP モニタ コマンド

コマンド	目的
show interface [*interface-id*] **rep** [**detail**]	特定のインターフェイスまたはすべてのインターフェイスの REP の設定とステータスを表示します。
show rep topology [**segment** *segment_id*] [**archive**] [**detail**]	セグメント内のプライマリおよびセカンダリ エッジ ポートを含む、1 セグメントまたは全セグメントの REP トポロジ情報を表示します。

CHAPTER 25

Flex Link および MAC アドレス テーブル移行更新機能の設定

この章では、Flex Link の設定方法について説明します。これは、相互バックアップを提供する IE 3000 スイッチ上のインターフェイスのペアです。また、Media Access Control（MAC; メディア アクセス制御）アドレス テーブル移行更新機能の設定についても説明します。これは、Flex Link 双方向高速コンバージェンス機能とも呼ばれます。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

Flex Link および MAC アドレス テーブル移行更新の概要

ここでは、次の情報について説明します。

Flex Link

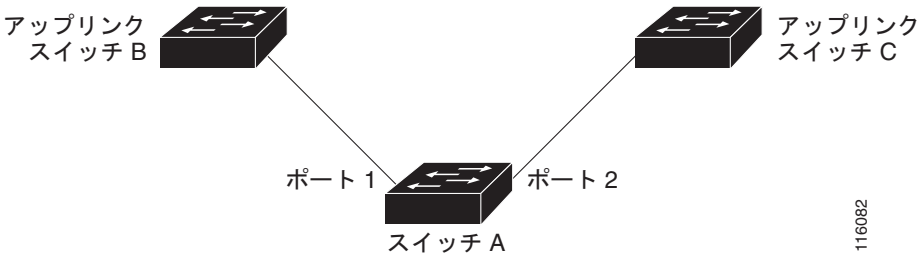
Flex Link は、レイヤ 2 インターフェイス（スイッチ ポートまたはポート チャネル）のペアで、1 つのインターフェイスがもう一方のインターフェイスのバックアップとして機能するように設定されています。この機能は Spanning Tree Protocol（STP; スパニング ツリー プロトコル）の代わりに提供され、ユーザが STP をディセーブルにした場合でも基本的なリンク冗長性を維持できます。一般的にカスタマーがスイッチで STP を実行したくないサービス プロバイダー ネットワークまたは企業ネットワーク内に設定されます。スイッチが STP を実行中の場合、STP がすでにリンク レベルの冗長性またはバックアップを提供しているので Flex Link の設定は必要ありません。

別のレイヤ 2 インターフェイスを Flex Link またはバックアップ リンクとして割り当てることで、1 つのレイヤ 2 インターフェイス（アクティブ リンク）に Flex Link を設定します。リンクの 1 つがアップでトラフィックを転送しているときは、もう一方のリンクがスタンバイ モードで、もう一方のリンクがシャット ダウンした場合にトラフィックの転送を開始できるように準備しています。どの時点でも、1 つのインターフェイスだけがリンク アップ ステートでトラフィックを転送しています。プライマリ リンクがシャットダウンすると、スタンバイ リンクがトラフィックの転送を開始します。アクティブ リンクが再びアップすると、これがスタンバイ モードになり、トラフィックの転送は行いません。STP は、Flex Link インターフェイスではディセーブルになります。

図 25-1 では、アップリンク スイッチ B および C に、スイッチ A のポート 1 およびポート 2 が接続されています。これらは Flex Link として設定されているので、1 つのインターフェイスだけがトラフィックを転送し、もう一方はスタンバイ モードになっています。ポート 1 がアクティブ リンクの場合、ポート 1 とスイッチ B との間でトラフィックの転送が開始され、ポート 2（バックアップ リンク）とスイッチ C との間ではトラフィックは転送されません。ポート 1 がダウンした場合、ポート 2 がアップになりスイッチ C へのトラフィックの転送を開始します。ポート 1 が再びアップすると、これがスタンバイ モードになり、トラフィックの転送は行いません。ポート 2 が引き続きトラフィックを転送します。

また、トラフィック転送に優先ポートを指定して、プリエンプション メカニズムを設定するように選択できます。たとえば図 25-1 の例では、Flex Link ペアをプリエンプション モードで設定できます。このシナリオでは、ポート 1 が再びアップしたときにポート 1 の帯域幅がポート 2 よりも大きい場合、ポート 1 は 60 秒後に転送を開始します。ポート 2 はスタンバイ ポートになります。これは、**switchport backup interface preemption mode bandwidth** および **switchport backup interface preemption delay** インターフェイス コンフィギュレーション コマンドを入力することによって、実行されます。

図 25-1　　Flex Link の設定例



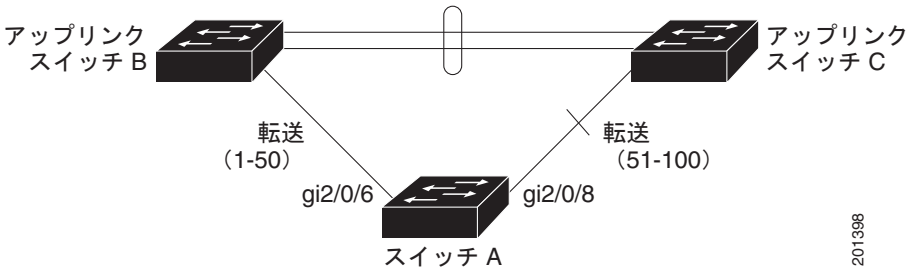
プライマリ（転送）リンクがダウンすると、トラップがこれをネットワーク管理ステーションに通知します。スタンバイ リンクがダウンすると、トラップはユーザに通知します。

Flex Link は レイヤ 2 ポートとポート チャネルだけでサポートされ、VLAN やレイヤ 3 ポートではサポートされません。

VLAN Flex Link のロード バランシングおよびサポート

VLAN Flex Link のロード バランシングにより、両方のポートが相互に排他的な VLAN のトラフィックを同時に転送するように、Flex Link ペアを設定できます。たとえば、Flex Link ポートが 1 ～ 100 の VLAN に設定されている場合、最初の 50 個の VLAN のトラフィックを 1 つのポートで転送し、残りのトラフィックを他のポートで転送することができます。1 つのポートに障害が発生した場合、もう 1 つのアクティブなポートがすべてのトラフィックを転送します。障害が発生したポートが復旧すると、優先 VLAN のトラフィックの転送が再開されます。このように、冗長性の提供とは別に、この Flex Link ペアは、ロード バランシングに使用できます。また、Flex Link VLAN のロード バランシングでは、アップリンク スイッチが制限されません。

図 25-2　VLAN Flex Link のロード バランシングの設定例



Flex Link のマルチキャスト高速コンバージェンス

Flex Link に障害が発生したあと、Flex Link のマルチキャスト高速コンバージェンスを使用すると、マルチキャスト トラフィックのコンバージェンスに要する時間が短縮されます。この機能は次のソリューションを組み合わせて実行されます。

- 「mrouter ポートとしての他の Flex Link ポートの学習」（P.25-3）
- 「IGMP レポートの生成」（P.25-3）
- 「IGMP レポートのリーク」（P.25-4）
- 「設定例」（P.25-4）

mrouter ポートとしての他の Flex Link ポートの学習

一般的なマルチキャスト ネットワークでは、VLAN ごとにクエリアがあります。ネットワークのエッジに配置されたスイッチには、クエリーを受信する Flex Link ポートの 1 つがあります。Flex Link ポートも常に転送しています。

クエリーを受信する Flex Link ポートは、スイッチ上の *mrouter* ポートとして追加されます。mrouter ポートは、スイッチが学習するすべてのマルチキャスト グループに属します。切り替え後、クエリーは別の Flex Link ポートによって受信されます。別の Flex Link ポートは mrouter ポートとして学習されます。切り替え後、マルチキャスト トラフィックは別の Flex Link ポート内を通過します。トラフィックの高速コンバージェンスを実現するため、いずれかの Flex Link ポートが mrouter ポートとして学習されるときは、両方の Flex Link ポートが mrouter ポートとして学習されます。両方の Flex Link ポートは必ずマルチキャスト グループに属します。

両方の Flex Link ポートは通常の動作モードでグループに属しますが、バックアップ ポートのすべてのトラフィックはブロックされます。したがって、通常のマルチキャスト データ フローは、mrouter ポートとしてバックアップ ポートを追加しても影響を受けません。切り替えが発生すると、バックアップ ポートのブロックは解除され、トラフィックを送信できます。この場合、バックアップ ポートのブロックが解除されるとすぐに、アップストリーム マルチキャスト データが送信されます。

IGMP レポートの生成

切り替え後にバックアップ リンクがアップすると、アップストリームの新しいディストリビューション スイッチはマルチキャスト データの転送を開始しません。アップストリーム ルータ上のポートは、ブロックされた Flex Link ポートに接続されており、マルチキャスト グループに属していないからです。バックアップ リンクがブロックされているので、マルチキャスト グループのレポートは、ダウンストリーム スイッチによって転送されませんでした。このポートがマルチキャスト グループを学習するまで、データはポート上で送信されません。これはポートがレポートを受信したあとにだけ発生します。

一般的なクエリーを受信すると、レポートはホストによって送信されます。一般的なクエリーは通常のシナリオでは 60 秒以内に送信されます。バックアップ リンクが転送を開始すると、マルチキャスト データの高速コンバージェンスを実現するため、ダウンストリーム スイッチは、一般的なクエリーを待つことなく、このポート上のすべての学習済みグループに対して、ただちにプロキシ レポートを送信します。

IGMP レポートのリーク

最小の損失でマルチキャスト トラフィック コンバージェンスを実現するには、Flex Link アクティブ リンクがダウンする前に、冗長データ パスを設定する必要があります。これは、Flex Link バックアップ リンク上の IGMP レポート パケットだけをリークすることで実現できます。リークした IGMP レポート メッセージは、アップストリーム ディストリビューション ルータによって処理されるので、マルチキャスト データ トラフィックはバックアップ インターフェイスに転送されます。バックアップ インターフェイスのすべての着信トラフィックは、アクセス スイッチの入力で廃棄されるので、重複したマルチキャスト トラフィックはホストによって受信されません。Flex Link アクティブ リンクに障害が発生すると、アクセス スイッチはバックアップ リンクからのトラフィックの受信をただちに開始します。この方式の唯一の欠点は、ディストリビューション スイッチの間のリンク上と、ディストリビューション スイッチとアクセス スイッチの間のバックアップ リンク上で帯域幅を消費することです。この機能はデフォルトではディセーブルで、**switchport backup interface *interface-id* multicast fast-convergence** コマンドを使用して設定できます。

切り替え時にこの機能がイネーブルになると、スイッチはバックアップ ポートでプロキシ レポートを生成せず、転送ポートになります。

設定例

次に、Flex Link ポートを GigabitEthernet1/1 および GigabitEthernet1/2 に設定したときに他の Flex Link ポートを mrouter ポートとして学習する例と、**show interfaces switchport backup** コマンドの出力を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface Gi1/2
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet1/1 GigabitEthernet1/2 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi1/1), 100000 Kbit (Gi1/2)
Mac Address Move Update Vlan : auto
```

次の出力では、GigabitEthernet1/1 を介してスイッチに到達するクエリーを持つ、VLAN 1 および 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier
Vlan    IP Address      IGMP Version       Port
-----------------------------------------------------------
1       1.1.1.1         v2                 Gi1/1
401     41.41.41.1      v2                 Gi1/1
```

次に、VLAN 1 および 401 の **show ip igmp snooping mrouter** コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
1       Gi1/1(dynamic), Gi1/2(dynamic)
401     Gi1/1(dynamic), Gi1/2(dynamic)
```

同様に、両方の Flex Link ポートも学習済みグループに属します。この例では、GigabitEthernet1/1 は VLAN 1 のレシーバー / ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups
Vlan    Group       Type    Version     Port List
------------------------------------------------------------------------
1       228.1.5.1   igmp    v2          Gi1/1, Gi1/2, Fa2/1
1       228.1.5.2   igmp    v2          Gi1/1, Gi1/2, Fa2/1
```

ホストが一般的なクエリーに応答すると、スイッチは mrouter ポート上でこのレポートを転送します。この例では、ホストがグループ 228.1.5.1 のレポートを送信するとき、バックアップ ポート GigabitEthernet1/2 はブロックされているので、レポートは GigabitEthernet1/1 でだけ送信されます。アクティブ リンクの GigabitEthernet1/1 がダウンすると、バックアップ ポートの GigabitEthernet1/2 が転送を開始します。

このポートが転送を開始するとすぐに、スイッチがホストの代わりにグループ 228.1.5.1 および 228.1.5.2 のプロキシ レポートを送信します。アップストリーム ルータはグループを学習し、マルチキャスト データの転送を開始します。これは、Flex Link のデフォルトの動作です。ユーザが **switchport backup interface gigabitEthernet** 1/2 **multicast fast-convergence** コマンドを使用して高速コンバージェンスを設定すると、この動作は変更されます。次に、この機能をオンにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# switchport backup interface gigabitethernet 1/2 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active                Interface             Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/1 GigabitEthernet1/2 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi1/1), 100000 Kbit (Gi1/2)
Mac Address Move Update Vlan : auto
```

次の出力では、GigabitEthernet1/1 を介してスイッチに到達するクエリーを持つ、VLAN 1 および 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier
Vlan        IP Address     IGMP Version   Port
-----------------------------------------------------------
1           1.1.1.1        v2             Gi1/1
401         41.41.41.1     v2             Gi1/1
```

次に、VLAN 1 および 401 の **show ip igmp snooping mrouter** コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter
Vlan        ports
----        -----
1           Gi1/1(dynamic), Gi1/2(dynamic)
401         Gi1/1(dynamic), Gi1/2(dynamic)
```

同様に、両方の Flex Link ポートも学習済みグループに属します。この例では、GigabitEthernet1/1 は VLAN 1 のレシーバー / ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups
Vlan    Group       Type    Version     Port List
------------------------------------------------------------------
1       228.1.5.1   igmp    v2          Gi1/1, Gi1/2, Gi1/1
1       228.1.5.2   igmp    v2          Gi1/1, Gi1/2, Gi1/1
```

ホストが一般的なクエリーに応答するたびに、スイッチは mrouter ポート上でこのレポートを転送します。コマンドライン ポートを介してこの機能をオンにし、レポートが GigabitEthernet1/1 上のスイッチによって転送されると、レポートはバックアップ ポート GigabitEthernet1/2 にもリークされます。アップストリーム ルータはグループを学習し、マルチキャスト データの転送を開始します。GigabitEthernet1/2 はブロックされているので、このデータは入力で廃棄されます。アクティブ リンクの GigabitEthernet1/1 がダウンすると、バックアップ ポートの GigabitEthernet1/2 が転送を開始します。マルチキャスト データはすでにアップストリーム ルータによって転送されているので、プロキシ レポートを送信する必要はありません。レポートをバックアップ ポートにリークすると冗長マルチキャスト パスが設定され、マルチキャスト トラフィック コンバージェンスに要する時間が最小限になります。

MAC アドレス テーブル移行更新

MAC アドレス テーブル移行更新機能により、プライマリ（転送）リンクがダウンし、スタンバイ リンクがトラフィックの転送を開始した場合、スイッチは高速双方向コンバージェンスを提供できます。

図 25-3 では、スイッチ A はアクセス スイッチで、スイッチ A のポート 1 および 2 は Flex Link ペアを介してアップリンク スイッチ B および D と接続されています。ポート 1 がトラフィックを転送し、ポート 2 はバックアップ ステートです。PC からサーバへのトラフィックは、ポート 1 からポート 3 に転送されます。PC の MAC アドレスは、スイッチ C のポート 3 で学習されます。サーバから PC へのトラフィックは、ポート 3 からポート 1 に転送されます。

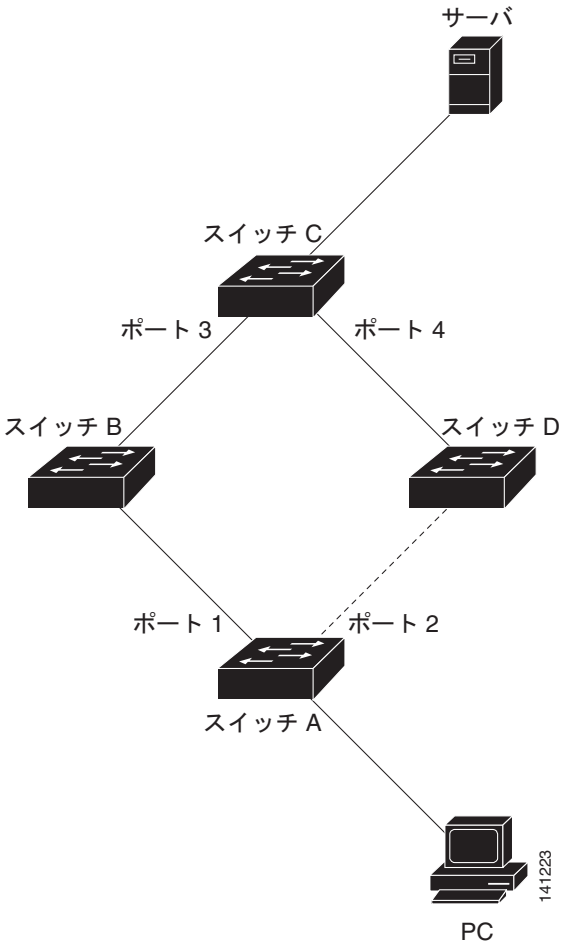
MAC アドレス テーブル移行更新機能が設定されていない場合にポート 1 がダウンすると、ポート 2 がトラフィックの転送を開始します。ただし、スイッチ C はポート 3 を介してサーバから PC へのトラフィックの転送を一時的に維持します。また、ポート 1 がダウンしているため、PC はトラフィックを受け取りません。スイッチ C がポート 3 上の PC の MAC アドレスを削除し、ポート 4 上で再学習すると、ポート 2 を介してサーバから PC へトラフィックを転送できます。

図 25-3 のスイッチで、MAC アドレス テーブル移行更新機能が設定されていて、イネーブルの場合に、ポート 1 がダウンすると、ポート 2 が PC からサーバへのトラフィックの転送を開始します。スイッチは、ポート 2 から MAC アドレス テーブル移行更新パケットを送信します。スイッチ C はポート 4 でこのパケットを受け取り、ただちにポート 4 上で PC の MAC アドレスを学習します。これにより、再コンバージェンス時間が短縮されます。

アクセス スイッチであるスイッチ A が、MAC アドレス テーブル移行更新メッセージを*送信する*ように設定できます。また、アップリンク スイッチ B、C、および D が、MAC アドレス テーブル移行更新メッセージを*受信して*、処理するように設定できます。スイッチ C が、スイッチ A から MAC アドレス テーブル移行更新メッセージを受信すると、スイッチ C はポート 4 で PC の MAC アドレスを学習します。スイッチ C は、PC の転送テーブルのエントリを含む MAC アドレス テーブルを更新します。

スイッチ A は、MAC アドレス テーブルの更新を待機する必要はありません。スイッチがポート 1 で障害を検出し、新しい転送ポートであるポート 2 からのサーバ トラフィックの転送をただちに開始します。この変更は 100 ミリ秒（ms）以内に発生します。PC はスイッチ A に直接接続され、接続ステータスは変更されません。スイッチ A は、MAC アドレス テーブル内の PC エントリを更新する必要はありません。

図 25-3　MAC アドレス テーブル移行更新の例



Flex Link および MAC アドレス テーブル移行更新の設定

ここでは、次の情報について説明します。

デフォルト設定

Flex Link は設定されておらず、バックアップ インターフェイスは定義されていません。

プリエンプション モードはオフです。

プリエンプション遅延は 35 秒です。

MAC アドレス テーブル移行更新機能は、スイッチで設定されていません。

設定時の注意事項

Flex Link の設定時には、次の注意事項に従ってください。

- 設定できるバックアップ リンクは、最大で 16 個です。
- アクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスは、1 つのアクティブ リンクに対してだけバックアップ リンクになれます。アクティブ リンクは別の FLex Link ペアに属することはできません。
- いずれのリンクも EtherChannel に属するポートにはなれません。ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルと物理インターフェイスを Flex Link として設定でき、ポート チャネルまたは物理インターフェイスをアクティブ リンクにできます。
- バックアップ リンクはアクティブ リンクと同じタイプ（ファスト イーサネット、ギガビット イーサネット、またはポート チャネル）でなくてもかまいません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の FLex Link を似たような特性で設定する必要があります。
- Flex Link ポートでは、STP はディセーブルです。ポートの VLAN に STP が設定されていても、Flex Link ポートは STP に参加しません。STP がイネーブルでない場合、設定されているトポロジでループが発生していないことを確認してください。Flex Link の設定を削除すると、STP がポートで再びイネーブルになります。

Flex Link 機能に VLAN ロード バランシングを設定するときは、次の注意事項に従ってください。

- Flex Link VLAN ロード バランシングでは、バックアップ インターフェイスで優先 VLAN を選択する必要があります。
- 同じ Flex Link ペアに対して、プリエンプション メカニズムと VLAN ロード バランシングを設定することはできません。

MAC アドレス テーブル移行更新機能を設定するときは、次の注意事項に従ってください。

- アクセス スイッチでこの機能をイネーブルにして設定すると、MAC アドレス テーブル移行更新を*送信*できます。
- アップリンク スイッチでこの機能をイネーブルにして設定すると、MAC アドレス テーブル移行更新を*受信*できます。

Flex Link の設定

Flex Link のペアを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）を指定できます。ポート チャネル範囲は 1 ～ 6 です。
ステップ 3	**switchport backup interface** *interface-id*	物理レイヤ 2 インターフェイス（またはポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** [*interface-id*] **switchport backup**	設定を確認します。
ステップ 6	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

Flex Link バックアップ インターフェイスをディセーブルにするには、**no switchport backup interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。

次に、バックアップ インターフェイスを持つインターフェイスを設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)# switchport backup interface gigabitethernet1/2
Switch(conf-if)# end

Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/1    GigabitEthernet1/2 Active Standby/Backup Up
Vlans Preferred on Active Interface: 1-3,5-4094
        Vlans Preferred on Backup Interface: 4
```

Flex Link のペアにプリエンプション スキームを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）を指定できます。ポート チャネル範囲は 1 ～ 6 です。
ステップ 3	**switchport backup interface** *interface-id*	物理レイヤ 2 インターフェイス（またはポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**switchport backup interface** *interface-id* **preemption mode** [**forced** | **bandwidth** | **off**]	Flex Link のインターフェイス ペアに、プリエンプション メカニズムおよびプリエンプション遅延を設定します。プリエンプションは、次のように設定できます。 • forced：アクティブ インターフェイスが常に、バックアップをプリエンプトします。 • bandwidth：より高い帯域幅を持つインターフェイスが常に、アクティブ インターフェイスとして動作します。 • off：アクティブからバックアップへのプリエンプションは発生しません。
ステップ 5	**switchport backup interface** *interface-id* **preemption delay** *delay-time*	特定のポートが別のポートをプリエンプトするまでの遅延時間を設定します。 **（注）**　遅延時間の設定は、forced および bandwidth モードでだけ機能します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport backup**	設定を確認します。
ステップ 8	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

プリエンプション スキームを削除するには、**no switchport backup interface** *interface-id* **preemption mode** インターフェイス コンフィギュレーション コマンドを使用します。遅延時間をデフォルトにリセットするには、**no switchport backup interface** *interface-id* **preemption delay** インターフェイス コンフィギュレーション コマンドを使用します。

次に、バックアップ インターフェイス ペアに対して、プリエンプション モードを *forced* として設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)#switchport backup interface gigabitethernet1/2 preemption mode forced
Switch(conf-if)#switchport backup interface gigabitethernet1/2 preemption delay 50
Switch(conf-if)# end

Switch# show interfaces switchport backup detail
Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/1 GigabitEthernet1/2 Active Up/Backup Standby
```

```
Interface Pair : Gi1/1, Gi1/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi1/1), 100000 Kbit (Gi1/2)
Mac Address Move Update Vlan : auto
```

Flex Link での VLAN ロード バランシングの設定

Flex Link に VLAN ロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）を指定できます。ポート チャネル範囲は 1 ～ 6 です。
ステップ 3	**switchport backup interface** *interface-id* ***prefer vlan*** *vlan-range*	物理レイヤ 2 インターフェイス（またはポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定し、インターフェイス上で伝送された VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** [*interface-id*] **switchport backup**	設定を確認します。
ステップ 6	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

VLAN ロード バランシング機能をディセーブルにするには、**no switchport backup interface** *interface-id* **prefer vlan** *vlan-range* インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、スイッチで VLAN 1 ～ 50、60、100 ～ 120 が設定されています。

```
Switch(config)#interface gigabitEthernet 1/2
Switch(config-if)#switchport backup interface gigabitEthernet 1/2 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合は、Gi1/1 が VLAN 60 および VLAN 100 ～ 120 のトラフィックを転送し、Gi1/2 が VLAN 1 ～ 50 のトラフィックを転送します。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/1 GigabitEthernet1/2 Active Up/Backup Up
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gi1/1 がダウンすると、Gi1/2 が Flex Link ペアのすべての VLAN を伝送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
```

```
GigabitEthernet1/1 GigabitEthernet1/2 Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gi1/1 がアップになると、このインターフェイスで優先される VLAN がピア インターフェイス Gi1/2 でブロックされ、Gi1/1 で転送されます。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/1      GigabitEthernet1/2 Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

Switch#show interfaces switchport backup detail
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet1/3         FastEthernet1/4       Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode  : off
Bandwidth : 10000 Kbit (Fa1/3), 100000 Kbit (Fa1/4)
Mac Address Move Update Vlan : auto
```

MAC アドレス テーブル移行更新機能の設定

ここでは、次の情報について説明します。

- スイッチの MAC アドレス テーブル移行更新の送信設定
- スイッチの MAC アドレス テーブル移行更新の受信設定

MAC アドレス テーブル移行更新を送信するようにアクセス スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）を指定できます。ポート チャネル範囲は 1 ～ 6 です。

	コマンド	目的
ステップ 3	**switchport backup interface** *interface-id* または **switchport backup interface** *interface-id* **mmu primary vlan** *vlan-id*	物理レイヤ 2 インターフェイス（またはポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。MAC アドレス テーブル移行更新の VLAN は、インターフェイス上で最も小さい VLAN ID です。 物理レイヤ 2 インターフェイス（またはポート チャネル）を設定して、MAC アドレス テーブル移行更新の送信に使用される、インターフェイス上の VLAN ID を指定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**mac address-table move update transmit**	プライマリ リンクがダウンして、スイッチがスタンバイ リンクを介してトラフィックの転送を開始する場合に、アクセス スイッチをイネーブルにして、ネットワーク内の他のスイッチに MAC アドレス テーブル移行更新を送信するようにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mac address-table move update**	設定を確認します。
ステップ 8	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブル移行更新機能をディセーブルにするには、**no mac address-table move update transmit** インターフェイス コンフィギュレーション コマンドを使用します。MAC アドレス テーブル移行更新情報を表示するには、**show mac address-table move update** 特権 EXEC コマンドを使用します。

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)# switchport backup interface gigabitethernet1/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次に、設定を確認する例を示します。

```
Switch# show mac-address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
```

```
Xmt last interface : None
```

MAC アドレス テーブル移行更新メッセージを受信して処理するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table move update receive**	スイッチをイネーブルにして、MAC アドレス テーブル移行更新を受信して処理するようにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table move update**	設定を確認します。
ステップ 5	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブル移行更新機能をディセーブルにするには、**no mac address-table move update receive** コンフィギュレーション コマンドを使用します。MAC アドレス テーブル移行更新情報を表示するには、**show mac address-table move update** 特権 EXEC コマンドを使用します。

次に、スイッチが MAC アドレス テーブル移行更新メッセージを受信して処理するように設定する例を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

Flex Link および MAC アドレス テーブル移動更新機能のモニタリング

表 25-1 に、Flex Link 設定および MAC アドレス テーブル移行更新情報をモニタするための特権 EXEC コマンドを示します。

表 25-1　Flex Link および MAC アドレス テーブル移行更新をモニタするためのコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport backup**	インターフェイスに設定されている Flex Link バックアップ インターフェイス、または設定されているすべての Flex Link と、アクティブ インターフェイスおよびバックアップ インターフェイスのステート（アップまたはスタンバイ モード）を表示します。VLAN ロード バランシングがイネーブルの場合、出力にアクティブ インターフェイスおよびバックアップ インターフェイスの優先 VLAN が表示されます。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

CHAPTER 26

DHCP 機能と IP ソース ガード機能の設定

この章では、IE 3000 スイッチに、DHCP スヌーピング機能、DHCP Option 82 データ挿入機能、および DHCP サーバのポートベースのアドレス割り当て機能を設定する方法について説明します。また、IP ソース ガード機能の設定方法についても説明します。

（注） この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、および Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』の「DHCP Commands」を参照してください。

この章で説明する内容は、次のとおりです。

DHCP スヌーピングの概要

DHCP は、中央のサーバからホストの IP アドレスをダイナミックに割り当てるために、LAN 環境で広範に使用されている機能です。この機能により、IP アドレス管理のオーバーヘッドを大幅に軽減できます。また、DHCP を使用すると、IP アドレスをホストに永続的に割り当てる必要がなくなり、ネットワークに接続しているホストだけが IP アドレスを使用するようになるので、限られた IP アドレス空間を節約するのに役立ちます。

ここでは、次の情報について説明します。

- 「Option 82 データ挿入」（P.26-3）
- 「Cisco IOS DHCP サーバ データベース」（P.26-6）
- 「DHCP スヌーピング バインディング データベース」（P.26-7）

DHCP クライアントの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』の「*IP Addressing and Services*」の「*Configuring DHCP*」を参照してください。

DHCP サーバ

DHCP サーバは、スイッチまたはルータにある指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当てて管理します。DHCP サーバが要求された設定パラメータをデータベースから DHCP クライアントに付与できない場合、その要求は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに転送されます。

DHCP リレー エージェント

DHCP リレー エージェントは、DHCP パケットをクライアントとサーバの間で転送するレイヤ 3 装置です。リレー エージェントは、クライアントとサーバが同じ物理サブネット上にない場合に、両者の間で要求と応答の転送を行います。リレー エージェント転送は、IP データグラムがネットワークの間でトランスペアレントにスイッチングされる通常のレイヤ 2 転送とは異なります。リレー エージェントは DHCP メッセージを受信し、新しい DHCP メッセージを生成して出力インターフェイスで送信します。

DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージをフィルタリングし、DHCP スヌーピング バインディング データベース（DHCP スヌーピング バインディング テーブルとも呼ばれる）を構築および維持することでネットワーク セキュリティを実現するセキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバ間のファイアウォールのように機能します。DHCP スヌーピングを使用すると、エンド ユーザに接続された信頼できないインターフェイスと、DHCP サーバまたは他のスイッチに接続された、信頼できるインターフェイスとを差別化できます。

（注）　DHCP スヌーピングが正しく機能するには、すべての DHCP サーバが、信頼できるインターフェイスを介してスイッチに接続されている必要があります。

信頼できない DHCP メッセージとは、ネットワークまたはファイアウォールの外部から受信したメッセージです。DHCP スヌーピングをサービス プロバイダー環境で使用する場合は、信頼できないメッセージは、サービス プロバイダー ネットワーク内には存在しない装置（カスタマーのスイッチなど）から送信されたものです。不明な装置からのメッセージは、この装置がトラフィック攻撃の起点である可能性もあるため、信頼できません。

DHCP スヌーピング バインディング データベースには、Media Access Control（MAC; メディア アクセス制御）アドレス、IP アドレス、リース期間、バインディングの種類、virtual LAN（VLAN; LAN）番号、およびインターフェイス情報が保存されます。インターフェイス情報は、スイッチの信頼できないローカル インターフェイスに対応する情報です。これには、信頼できるインターフェイスに相互接続しているホストに関する情報はありません。

サービス プロバイダー ネットワークでは、信頼できるインターフェイスは、同じネットワーク内にある装置のポートに接続されています。信頼できないインターフェイスは、ネットワーク内の信頼できないインターフェイス、またはネットワーク内には存在しない装置のインターフェイスに接続されています。

スイッチが信頼できないインターフェイス上でパケットを受信し、このインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルにされている場合、スイッチは送信元 MAC アドレスを DHCP クライアント ハードウェアのアドレスと比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットを廃棄します。

スイッチは、次のような状況が発生した場合に DHCP パケットを廃棄します。

- ネットワークまたはファイアウォール外部の DHCP サーバから、DHCPOFFER、DHCPACK、DHCPNAK、DHCPLEASEQUERY などのパケットを受信した場合。
- 信頼できないインターフェイスでパケットを受信し、送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合。
- DHCP スヌーピング バインディング データベース内の MAC アドレスを持つ DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信したが、バインディング データベース内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。
- DHCP リレー エージェントが 0.0.0.0 でないリレー エージェント IP アドレスが含まれる DHCP パケットを転送するか、またはリレー エージェントが Option 82 情報が含まれるパケットを信頼できないポートに転送する場合。

スイッチが DHCP スヌーピングをサポートする集約スイッチであり、DHCP Option 82 情報を挿入するエッジ スイッチに接続されている場合、スイッチは、信頼できないインターフェイスでパケットを受信すると、Option 82 情報を含むパケットを廃棄します。DHCP スヌーピングがイネーブルで、信頼できるポートでパケットを受信した場合、集約スイッチは、接続先装置の DHCP スヌーピング バインディングを学習せず、完全な DHCP スヌーピング バインディング データベースを構築できません。

信頼できないインターフェイスを介して集約スイッチをエッジ スイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スイッチから Option 82 情報を含むパケットを受け付けます。集約スイッチは信頼できないスイッチ インターフェイスを介して接続されたホストのバインディングを学習します。ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査や IP ソース ガードなどの DHCP セキュリティ機能は、スイッチが、ホストが接続されている信頼できない入力インターフェイスで Option 82 情報を含むパケットを受信している間でも、集約スイッチ上でイネーブルにできます。集約スイッチに接続されるエッジ スイッチ上のポートは、信頼できるインターフェイスとして設定する必要があります。

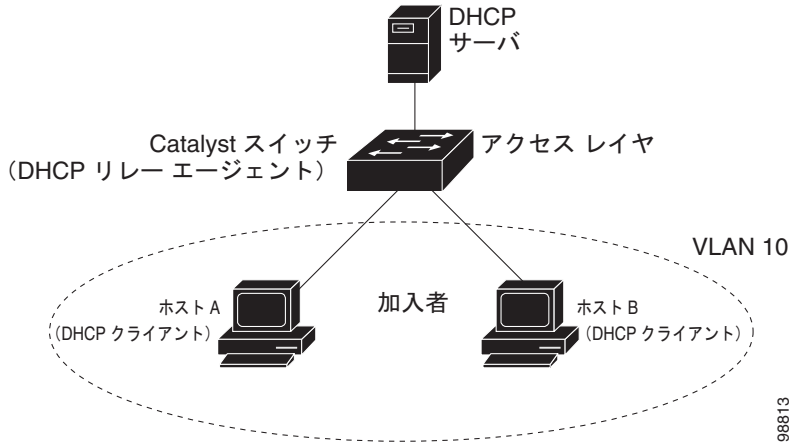
Option 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、この装置をネットワークに接続するスイッチ ポートによっても識別されます。加入者 LAN 上の複数のホストをアクセス スイッチの同一ポートに接続でき、これらは一意に識別されます。

（注）　Option 82 機能は、この機能を使用する加入者の装置が割り当てられている VLAN で DHCP スヌーピングがグローバルにイネーブルになっている場合だけサポートされます。

図 26-1 は、メトロポリタン イーサネット ネットワーク内において、アクセス レイヤのスイッチに接続されている各加入者の IP アドレスを、一元的な DHCP サーバが割り当てる例を示しています。各 DHCP クライアントと、これらに関連付けられた DHCP サーバは、同一の IP ネットワークまたはサブネット内に存在しません。したがって、DHCP リレー エージェント（Catalyst スイッチ）をヘルパー アドレスによって設定することで、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 26-1　メトロポリタン イーサネット ネットワークにおける DHCP リレー エージェント



スイッチで DHCP スヌーピング情報の Option 82 をイネーブルにすると、次の一連のイベントが発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチはこの DHCP 要求を受信すると、パケット内に Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションはスイッチの MAC アドレスで、回線 ID サブオプションはパケットの受信ポートの ID である **vlan-mod-port** です。
- リレー エージェントの IP アドレスが設定されている場合、スイッチは DHCP パケット内にこの IP アドレスを追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。サーバが Option 82 に対応している場合は、リモート ID、回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシー（単一のリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するなど）の実装を行うことができます。また、DHCP サーバは、DHCP 応答に含まれるオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データが挿入されていることを確認します。スイッチは、オプション 82 フィールドを削除し、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

デフォルトのサブオプション設定では、上記の一連のイベントが発生したときに、図 26-2 にある次のフィールドの値は変更されません。

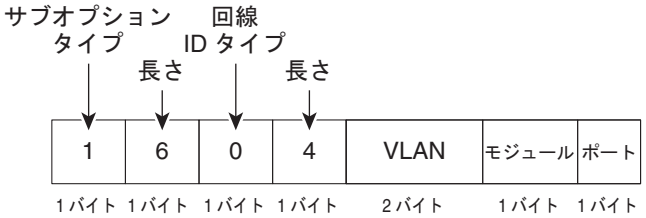
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります。たとえば、8 つの 10/100 ポートと Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュール スロットを備えたスイッチでは、ポート 3 が Fast Ethernet 1/1 ポート、ポート 4 が Fast Ethernet 1/2 ポートなどのようになります。ポート 11 は SFP モジュール スロット 1/1 などになります。

図 26-2 に、デフォルト設定のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力された場合に、このパケット形式を使用します。

図 26-2　　サブオプションのパケット形式

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット

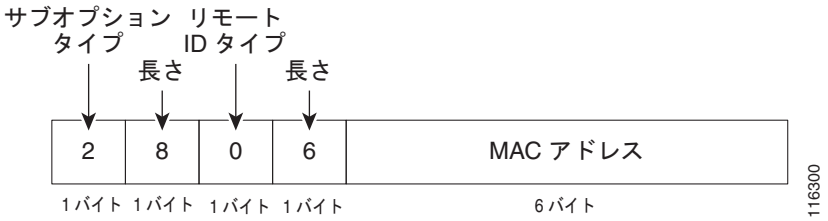


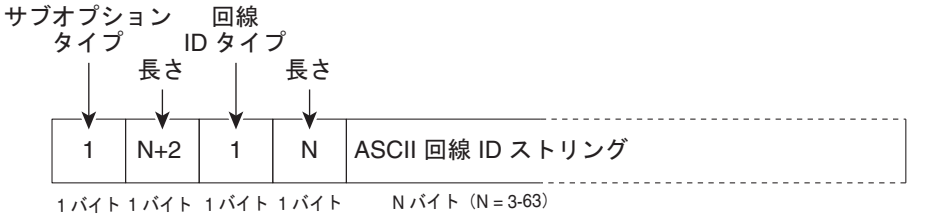
図 26-3 に、ユーザ設定のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドと **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドが入力された場合に、このパケット形式を使用します。

リモート ID サブオプションと回線 ID サブオプションを設定すると、パケットの次のフィールドの値がデフォルト値から変更されます。

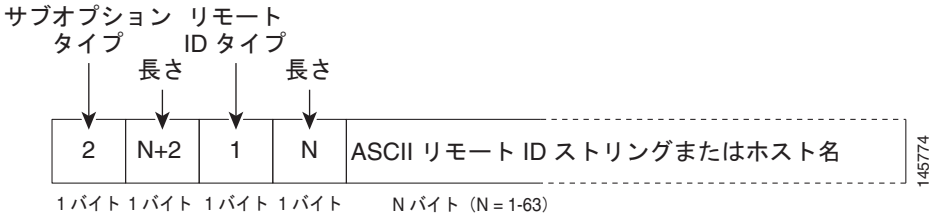
- 回線 ID サブオプション フィールド
  - 回線 ID タイプは 1 です。
  - 長さの値は変数で、設定するストリングの長さにより変わります。
- リモート ID サブオプション フィールド
  - リモート ID タイプは 1 です。
  - 長さの値は変数で、設定するストリングの長さにより変わります。

図 26-3　ユーザ設定サブオプションのパケット形式

回線 ID サブオプション フレーム フォーマット（ユーザ設定のストリング）：



リモート ID サブオプション フレーム フォーマット（ユーザ設定のストリング）：



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定された DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。このデータベースには、IP アドレス、*アドレス バインディング*、ブート ファイルなどの設定パラメータが格納されています。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスは手動で割り当てることも、DHCP サーバを使用して DHCP アドレス プールから割り当てることもできます。手動および自動アドレス バインディングの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングがイネーブルの場合、スイッチは DHCP スヌーピング バインディング データベースを使用して、信頼できないインターフェイスに関する情報を保存します。データベースには、8192 のバインディングを含めることができます。

各データベース エントリ（*バインディング*）には、IP アドレス、関連付けられた MAC アドレス、リース時間（16 進数形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN が含まれます。データベース エージェントは、設定された場所のファイルにバインディングを保存します。各エントリの最後に示されるチェックサムは、ファイルの冒頭から、エントリに関連付けられたすべてのバイトの合計に基づいて計算されます。各エントリは 72 バイトで、そのあとにスペースとチェックサム値が続きます。

スイッチがリロードされたときにバインディングを維持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP 検査または IP ソース ガードがイネーブルであり、DHCP スヌーピング バインディング データベースにダイナミック バインディングがある場合は、スイッチの接続が切断されます。エージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである場合は、スイッチの接続は切断されませんが、DHCP スヌーピングが DCHP スプーフィング攻撃を防止できないことがあります。

リロード時に、スイッチは DHCP スヌーピング バインディング データベースを構築するためにバインディング ファイルを読み込みます。スイッチは、データベースの変更時にファイルを更新します。

スイッチは、新しいバインディングを学習した場合や、バインディングを消失した場合には、データベース内のエントリを更新します。スイッチはまた、バインディング ファイル内のエントリも更新します。ファイルを更新する頻度は、設定可能な遅延に基づいて決定され、更新はバッチ処理されます。ファイルが（write-delay および abort-timeout 値によって設定された）指定の時間に更新されない場合は、更新が停止します。

バインディングを含むファイルのフォーマットは次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

ファイル内の各エントリには、スイッチがファイルを読み込んだときにエントリの確認に使用するチェックサム値がタグ付けされます。1 行めの *initial-checksum* エントリは、最新のファイル更新に関連するエントリと前のファイル更新に関連するエントリを区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E interface-id 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB interface-id 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB interface-id 584a38f0
END
```

スイッチが開始され、計算されたチェックサム値が保存されているチェックサム値と等しい場合、スイッチはバインディング ファイルからエントリを読み取って、バインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スイッチがエントリを読み取って、計算されたチェックサム値が保存されているチェックサム値と異なる場合。そのエントリとそのあとのエントリが無視されます。
- エントリに期限切れのリース時間がある場合（リース時間が期限切れになっても、スイッチはバインディング エントリを削除しない場合があります）。
- エントリ内のインターフェイスがシステムに存在しない場合。
- インターフェイスがルーテッド インターフェイスまたは DHCP スヌーピングの信頼できるインターフェイスの場合。

DHCP スヌーピングの設定

ここでは、次の設定情報について説明します。

DHCP スヌーピングのデフォルト設定

表 26-1 に、DHCP スヌーピングのデフォルト設定を示します。

表 26-1　DHCP スヌーピングのデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアでイネーブル。設定が必要です。[1]
DHCP リレー エージェント	イネーブル。[2]
DHCP パケット転送アドレス	設定なし。
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄されます）。[2]
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置き換えます。[2]
グローバルにイネーブルにされる DHCP スヌーピング	ディセーブル。
DHCP スヌーピング情報オプション	イネーブル。
信頼できない入力インターフェイスでパケットを受け付ける DHCP スヌーピング オプション[3]	ディセーブル。
DHCP スヌーピング レート制限	設定なし。
DHCP スヌーピング信頼状態	信頼しない。
DHCP スヌーピング VLAN	ディセーブル。
DHCP スヌーピングの MAC アドレス検証	イネーブル。

表 26-1　DHCP スヌーピングのデフォルト設定 （続き）

機能	デフォルト設定
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアでイネーブル。設定が必要です。 （注）　スイッチは、DHCP サーバとして設定されている装置からだけネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアでイネーブル。設定が必要です。この機能は、宛先が設定されている場合にだけ使用できます。

1. スイッチは、DHCP サーバとして設定されている場合にだけ DHCP 要求に応答します。
2. スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）上に設定されている場合にだけ DHCP パケットをリレーします。
3. この機能は、スイッチがエッジ スイッチから Option 82 情報を含むパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

ここでは、DHCP スヌーピングの設定時の注意事項を説明します。

- スイッチで DHCP スヌーピングをグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN 上で DHCP スヌーピングをイネーブルにしない限りアクティブになりません。
- スイッチで DHCP スヌーピングをグローバルにイネーブルにするには、DHCP サーバおよび DHCP リレー エージェントとして機能する装置を、事前に設定してイネーブルにしておく必要があります。
- スイッチに DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能する装置を必ず設定してください。たとえば、DHCP サーバによる割り当てまたは除外が可能な IP アドレスを指定したり、装置に DHCP オプションを設定したりする必要があります。
- スイッチに多数の回線 ID を設定する場合は、長い文字列が NVRAM またはフラッシュ メモリに与える影響を考慮してください。サーキット ID 設定がその他のデータと組み合わされた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、エラー メッセージが表示されます。
- スイッチに DHCP リレー エージェントを設定する前に、DHCP サーバとして機能する装置を必ず設定してください。たとえば、DHCP サーバによる割り当てまたは除外が可能な IP アドレスを指定したり、装置に DHCP オプションを設定したり、データベース エージェントを設定したりする必要があります。
- DHCP リレー エージェントがイネーブルでも、DHCP スヌーピングがディセーブルの場合、DHCP Option 82 データ挿入機能はサポートされません。
- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定します。
- スイッチ ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定します。
- DHCP スヌーピング バインディング データベースを設定する場合は、次の注意事項に従ってください。
  - NVRAM とフラッシュ メモリの両方のストレージ容量には限りがあるため、バインディング ファイルを Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ上に保存することを推奨します。

  - ネットワークベースの URL（TFTP や FTP など）の場合、設定した URL のバインディング ファイルにスイッチがバインディングを書き込めるようにするには、その URL に空のファイルを作成する必要があります。最初にサーバで空のファイルを作成する必要があるかどうかを判断するには、使用している TFTP サーバのマニュアルを参照してください。一部の TFTP サーバは、この方法で設定できません。
  - データベース内のリース時間を正確な時間にするには、NTP をイネーブルにして設定することを推奨します。詳細については、「NTP の設定」（P.7-3）を参照してください。
  - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容を書き込みます。
- 信頼できない装置が接続された集約スイッチに **ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できない装置がオプション 82 情報をスプーフィングする可能性があります。
- DHCP スヌーピング統計情報を表示するには、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力します。スヌーピング統計情報を消去するには、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力します。

（注） RSPAN VLAN で Dynamic Host Configuration Protocol（DHCP）スヌーピングをイネーブルにしないでください。RSPAN VLAN で DHCP スヌーピングをイネーブルにすると、DHCP パケットが RSPAN の宛先ポートに到達しなくなることがあります。

DHCP リレー エージェントの設定

スイッチで DHCP リレー エージェントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service dhcp**	スイッチで DHCP サーバとリレー エージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

DHCP サーバとリレー エージェントをディセーブルにするには、**no service dhcp** グローバル コンフィギュレーション コマンドを使用します。

次の手順については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」の「*Configuring DHCP*」を参照してください。

- リレー エージェント情報の確認（検証）
- リレー エージェント転送ポリシーの設定

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合は、**ip helper-address** *address* インターフェイス コンフィギュレーション コマンドを使用してスイッチを設定する必要があります。一般的な規則は、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで使用するアドレスには、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスを指定できます。ネットワーク アドレスを使用すると、すべての DHCP サーバが要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id*	VLAN ID を入力してスイッチ仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスと IP サブネットを使用してインターフェイスを設定します。
ステップ 4	**ip helper-address** *address*	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスには、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスを指定できます。ネットワーク アドレスを使用すると、他のサーバが DHCP 要求に応答できるようになります。 複数のサーバがある場合は、サーバごとに 1 つのヘルパー アドレスを設定できます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface range** *port-range* または **interface** *interface-id*	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス レンジ コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス レンジ コンフィギュレーション モードを開始します。
ステップ 7	**switchport mode access**	ポートの VLAN メンバーシップ モードを定義します。
ステップ 8	**switchport access vlan** *vlan-id*	ステップ 2 で設定した VLAN にポートを割り当てます。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config**	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

DHCP パケット転送アドレスを削除するには、**no ip helper-address** *address* インターフェイス コンフィギュレーション コマンドを使用します。

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチで DHCP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp snooping**	DHCP スヌーピングをグローバルにイネーブルにします。
ステップ 3	**ip dhcp snooping vlan** *vlan-range*	VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力できます。これらはスペースで区切ります。
ステップ 4	**ip dhcp snooping information option**	スイッチをイネーブルにして、DHCP サーバに転送される DHCP 要求メッセージの DHCP リレー情報（Option 82 フィールド）を挿入または削除します。これは、デフォルト設定です。
ステップ 5	**ip dhcp snooping information option format remote-id [string** *ASCII-string* **|** *hostname*]	（任意）リモート ID サブオプションを設定します。 リモート ID は次のいずれかに設定することができます。 • 63 文字までの ASCII 文字列（スペースなし） • スイッチの設定済みホスト名 **（注）** ホスト名が 63 文字を超える場合、リモート ID 設定では 64 文字以降が切り捨てられます。 デフォルトのリモート ID はスイッチの MAC アドレスです。
ステップ 6	**ip dhcp snooping information option allow-untrusted**	（任意）スイッチがエッジ スイッチに接続された集約スイッチの場合、スイッチが Option 82 情報を含む着信 DHCP スヌーピング パケットをエッジ スイッチから受け入れることができるようにします。 デフォルト設定は、ディセーブルです。 **（注）** このコマンドは、集約スイッチが信頼できる装置に接続されている場合にだけ入力してください。
ステップ 7	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id** [**override**] **string** *ASCII-string*	（任意）指定したインターフェイスの回線 ID サブオプションを設定します。 VLAN およびポート ID を、1 ～ 4094 の範囲の VLAN ID を使用して指定します。デフォルトの回線 ID は、**vlan-mod-port** という形式のポート ID です。 回線 ID は、3 ～ 63 文字の ASCII 文字（スペースなし）を使用して設定できます。 （任意）TLV 形式の回線 ID サブオプションを挿入せずに加入者情報を定義する場合は、**override** キーワードを使用します。
ステップ 9	**ip dhcp snooping trust**	（任意）インターフェイスを信頼できる状態または信頼できない状態に設定します。信頼できないクライアントからメッセージを受信するようにインターフェイスを設定するには、**no** キーワードを使用します。デフォルト設定は untrusted です。

	コマンド	目的
ステップ 10	**ip dhcp snooping limit rate** *rate*	（任意）インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。指定できる範囲は 1 ～ 2048 です。デフォルトでは、レート制限は設定されていません。 **（注）** 信頼できないインターフェイスでのレートは、100 パケット/秒以下に制限することを推奨します。信頼できるインターフェイスにレート制限を設定する場合、ポートが、DHCP スヌーピングをイネーブルにしている複数の VLAN に割り当てられたトランク ポートであれば、レート制限を高い値に設定するとこを推奨します。
ステップ 11	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**ip dhcp snooping verify mac-address**	（任意）信頼できないポートで受信された DHCP パケットの送信元 MAC アドレスが、パケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show running-config**	設定を確認します。
ステップ 15	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用します。VLAN または VLAN 範囲で DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、**no ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。エッジ スイッチからの Option 82 情報を含む着信 DHCP スヌーピング パケットを廃棄するように集約スイッチを設定するには、**no ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 10 で DHCP スヌーピングをグローバルにイネーブルにし、ポート上でレート制限を 100 パケット/秒に設定する例を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

プライベート VLAN での DHCP スヌーピングのイネーブル化

DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。DHCP スヌーピングをイネーブルにすると、その設定はプライマリ VLAN およびそれに関連付けられているセカンダリ VLAN の両方に伝播します。プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、セカンダリ VLAN でも DHCP スヌーピングがイネーブルになります。

プライマリ VLAN で DHCP スヌーピングがすでに設定されていて、セカンダリ VLAN で DHCP スヌーピングを別の値で設定した場合、セカンダリ VLAN の設定は有効になりません。DHCP スヌーピングは、プライマリ VLAN で設定する必要があります。プライマリ VLAN で DHCP スヌーピングが設定されていない場合に、VLAN 200 などのセカンダリ VLAN で DHCP スヌーピングを設定しようとすると、次のメッセージが表示されます。

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not take
effect on secondary vlan 200.DHCP Snooping configuration on secondary vlan is derived from
its primary vlan.
```

show ip dhcp snooping 特権 EXEC コマンドの出力には、DHCP スヌーピングがイネーブルになっているすべての VLAN（プライマリおよびセカンダリ プライベート VLAN を含む）が示されます。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』の「Configuring DHCP」の「DHCP Configuration Task List」を参照してください。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチで DHCP スヌーピング バインディング データベース エージェントをイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp snooping database** {**flash:**/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** | **rcp:**//*user@host*/*filename*}| **tftp:**//*host*/*filename*	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイル用の URL を指定します。 • **flash:**/*filename* • **ftp:**//*user*:*password*@*host*/*filename* • **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** • **rcp:**//*user@host*/*filename* • **tftp:**//*host*/*filename*
ステップ 3	**ip dhcp snooping database timeout** *seconds*	データベース転送プロセスを打ち切るまでの時間（秒）を指定します。 デフォルト値は 300 秒です。指定できる範囲は 0 ～ 86400 です。無期限の期間を定義するには、0 を使用します。これは、転送を無期限に続けることを意味します。
ステップ 4	**ip dhcp snooping database write-delay** *seconds*	バインディング データベースが変更されたあとに、転送を遅らせる期間を指定します。指定できる範囲は 15 ～ 86400 秒です。デフォルトは 300 秒（5 分）です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*	（任意）DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。*vlan-id* に指定できる範囲は 1 ～ 4904 です。*seconds* に指定できる範囲は 1 ～ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。 **（注）** このコマンドは、スイッチをテストまたはデバッグするときに使用します。

	コマンド	目的
ステップ 7	**show ip dhcp snooping database** [**detail**]	DHCP スヌーピング バインディング データベース エージェントのステータスと統計情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

データベース エージェントおよびバインディング ファイルの使用を停止するには、**no ip dhcp snooping database** グローバル コンフィギュレーション コマンドを使用します。タイムアウト値または遅延値をリセットするには、**ip dhcp snooping database timeout** *seconds* または **ip dhcp snooping database write-delay** *seconds* グローバル コンフィギュレーション コマンドを使用します。

DHCP スヌーピング バインディング データベース エージェントの統計情報を消去するには、**clear ip dhcp snooping database statistics** 特権 EXEC コマンドを使用します。データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

DHCP スヌーピング バインディング データベースからエントリを削除するには、**no ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* 特権 EXEC コマンドを使用します。このコマンドは、削除するエントリごとに入力し 1 ます。

DHCP スヌーピング情報の表示

DHCP スヌーピング情報を表示するには、表 26-2 に示す各特権 EXEC コマンドを使用します。

表 26-2　DHCP 情報を表示するためのコマンド

コマンド	目的
show ip dhcp snooping	スイッチの DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	バインディング テーブルとも呼ばれる DHCP スヌーピング バインディング データベースの中から、ダイナミックに設定されたバインディングだけを表示します。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスと統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報をサマリー形式または詳細形式で表示します。
show ip source binding	ダイナミックおよびスタティックに設定されたバインディングを表示します。

（注）　DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、スタティックに設定されたバインディングは削除されません。

IP ソース ガード（IPSG）の概要

IPSG は、DHCP スヌーピング バインディング データベースと手動で設定された IP 送信元バインディングに基づいてトラフィックをフィルタリングすることで、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックを制限するセキュリティ機能です。IP ソース ガードを使用すると、ホストがネイバーの IP アドレスを使用しようとした場合のトラフィック攻撃を防ぐことができます。

IP ソース ガードは、信頼できないインターフェイスで DHCP スヌーピングがイネーブルになっている場合にイネーブルにできます。インターフェイスで IPSG をイネーブルにすると、スイッチは、インターフェイスで受信した IP トラフィックを、DHCP スヌーピングで許可された DHCP パケットを除いてすべてブロックします。インターフェイスには、ポート Access Control List（ACL; アクセス制御リスト）が適用されます。ポート ACL により、IP 送信元バインディング テーブル内の送信元 IP アドレスを持つ IP トラフィックだけが許可され、他のトラフィックがすべて拒否されます。

（注）　ポート ACL は、同じインターフェイスに影響を与える ルータ ACL または VLAN マップよりも優先されます。

IP 送信元バインディング テーブルのバインディングは、DHCP スヌーピングによって学習されたバインディングか、手動で設定されたバインディング（スタティック IP 送信元バインディング）です。このテーブルのエントリには、IP アドレスと、それに関連付けられた MAC アドレスおよび VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルの場合だけ、IP 送信元バインディング テーブルを使用します。

IPSG は、アクセス ポートやトランク ポートなどのレイヤ 2 ポートでだけサポートされます。IPSG は、送信元 IP アドレス フィルタリングまたは送信元 IP および MAC アドレス フィルタリングを使用して設定できます。

- 「送信元 IP アドレス フィルタリング」（P.26-16）
- 「送信元 IP および MAC アドレス フィルタリング」（P.26-17）
- 「スタティック ホストの IP ソース ガード」（P.26-17）

送信元 IP アドレス フィルタリング

このオプションを使用して IPSG をイネーブルにした場合、IP トラフィックは送信元 IP アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP アドレスが DHCP スヌーピング バインディング データベースのエントリまたは IP 送信元バインディング テーブル内のバインディングと一致した場合に IP トラフィックを転送します。

DHCP スヌーピング バインディングまたはスタティック IP 送信元バインディングがインターフェイスで追加、変更、または削除された場合、スイッチは、IP 送信元バインディングを変更してポート ACL を修正し、そのポート ACL をインターフェイスに再度適用します。

IP 送信元バインディング（DHCP スヌーピングでによってダイナミックに学習されるか、手動で設定される）が設定されていないインターフェイスで IPSG をイネーブルにすると、スイッチは、インターフェイス上のすべての IP トラフィックを拒否するポート ACL を作成して適用します。IP ソース ガードをディセーブルにすると、スイッチはポート ACL をインターフェイスから削除します。

送信元 IP および MAC アドレス フィルタリング

IP トラフィックは、送信元 IP および MAC アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP アドレスおよび MAC アドレスが IP 送信元バインディング テーブルのエントリと一致した場合にトラフィックを転送します。

アドレス フィルタリングがイネーブルの場合、スイッチは IP および非 IP トラフィックをフィルタリングします。IP または非 IP パケットの送信元 MAC アドレスが有効な IP 送信元バインディングと一致する場合、スイッチはパケットを転送します。スイッチは、DHCP パケット以外のパケットをすべて廃棄します。

スイッチは、ポート セキュリティを使用して送信元 MAC アドレスをフィルタリングします。ポート セキュリティ違反が発生した場合は、インターフェイスをシャット ダウンできます。

スタティック ホストの IP ソース ガード

（注） アップリンク ポートまたはトランク ポートでは、スタティック ホストの IPSG（IP ソース ガード）を使用しないでください。

スタティック ホストの IPSG は、IPSG 機能を、DHCP が使用されないスタティックな環境に拡張します。以前の IPSG では、DHCP スヌーピングによって作成されたエントリを使用して、スイッチに接続されたホストを検証しました。有効な DHCP バインディング エントリがないホストからのトラフィックはすべて廃棄されます。このセキュリティ機能は、ルーティングされないレイヤ 2 インターフェイス上のトラフィックを制限します。トラフィックは、DHCP スヌーピング バインディング データベースと手動で設定された IP 送信元バインディングに基づいてフィルタリングされます。以前のバージョンの IPSG では、IPSG を機能させるために DHCP 環境が必要でした。

スタティック ホストの IPSG を使用すると、DHCP なしで IPSG を機能させることができます。スタティック ホストの IPSG では、ポート ACL のインストールに IP 装置追跡テーブルのエントリが使用されます。スイッチは、ARP 要求またはその他の IP パケットに基づいてスタティック エントリを作成し、指定のポートの有効なホストのリストを保持します。指定のポートへのトラフィックの送信を許可するホストの数を指定することもできます。これはレイヤ 3 のポート セキュリティに相当します。

スタティック ホストの IPSG では、ダイナミック ホストもサポートされます。ダイナミック ホストが IP DHCP スヌーピング テーブルで使用可能な DHCP 割り当て IP アドレスを受信した場合、同じエントリが IP 装置追跡テーブルによって学習されます。**show ip device tracking all** EXEC コマンドを入力すると、IP 装置追跡テーブルでエントリが ACTIVE と表示されます。

（注） 複数のネットワーク インターフェイスを備えた一部の IP ホストは、一部の無効パケットをネットワーク インターフェイスに送信することがあります。この無効パケットには、ホストの別のネットワーク インターフェイスの IP または MAC アドレスが送信元アドレスとして含まれています。この無効パケットにより、スタティック ホストの IPSG がホストに接続し、無効な IP または MAC アドレス バインディングを学習して、有効なバインディングを拒否することがあります。無効パケットの送信を防ぐ方法については、対応するオペレーティング システムおよびネットワーク インターフェイスのベンダーに問い合わせてください。

スタティック ホストの IPSG は、最初に ACL ベースのスヌーピング メカニズムを介して IP または MAC バインディングをダイナミックに学習します。IP または MAC バインディングは、ARP および IP パケットを介してスタティック ホストから学習され、装置追跡データベースに保存されます。指定のポートでダイナミックに学習された IP アドレス、またはスタティックに設定された IP アドレスの数が上限に達すると、ハードウェアは新しい IP アドレスを持つパケットをすべて廃棄します。スタ

ティック ホストの IPSG では、何らかの理由で移動または除去されたホストを解決するために、IP 装置追跡を使用して、ダイナミックに学習した IP アドレス バインディングを期限切れにします。この機能は DHCP スヌーピングと併用できます。DHCP ホストとスタティック ホストの両方に接続されているポートでは、複数のバインディングが設定されます。たとえば、バインディングは装置追跡データベースと DHCP スヌーピング データベースの両方に保存されます。

IP ソース ガードの設定

IP ソース ガードのデフォルト設定

デフォルトでは、IP ソース ガードはディセーブルに設定されています。

IP ソース ガード設定時の注意事項

- スタティック IP バインディングは、非ルーテッド ポートでだけ設定できます。ルーテッド インターフェイスで **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを入力すると、次のエラー メッセージが表示されます。

  ```
  Static IP source binding can only be configured on switch port.
  ```

- インターフェイスで送信元 IP フィルタリングによる IP ソース ガードをイネーブルにする場合は、そのインターフェイスのアクセス VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- 複数の VLAN があるトランク インターフェイスで IP ソース ガードをイネーブルにしていて、すべての VLAN で DHCP スヌーピングがイネーブルになっている場合は、送信元 IP アドレス フィルタがすべての VLAN に適用されます。

  （注）　IP ソース ガードがイネーブルになっている場合に、トランク インターフェイス上の VLAN で DHCP スヌーピングをイネーブルまたはディセーブルにすると、スイッチのトラフィック フィルタリングが正しく動作しなくなることがあります。

- 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにする場合は、インターフェイスで DHCP スヌーピングとポート セキュリティをイネーブルにする必要があります。また、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力して、DHCP サーバで Option 82 がサポートされるようにする必要があります。MAC アドレス フィルタリングによる IP ソース ガードがイネーブルになっている場合、DHCP ホストの MAC アドレスは、ホストにリースが付与されるまで学習されません。DHCP スヌーピングは、サーバからホストにパケットを転送するときに、Option 82 データを使用してホストのポートを識別します。
- プライベート VLAN が設定されているインターフェイスで IP ソース ガードを設定する場合、ポート セキュリティはサポートされません。
- IP ソース ガードは、EtherChannel ではサポートされません。
- この機能は、802.1X ポートベースの認証がイネーブルの場合にイネーブルにできます。

- ternary content addressable memory（TCAM; 三値連想メモリ）のエントリの数が上限を超えると、CPU の使用率が上昇します。

IP ソース ガードのイネーブル化

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip verify source** または **ip verify source port-security**	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して、IP ソース ガードとポート セキュリティの両方をイネーブルにする場合は、次の 2 つの点に注意してください。 • DHCP サーバは Option 82 をサポートしている必要があります。そうでない場合は、クライアントに IP アドレスが割り当てられません。 • DHCP パケットの MAC アドレスは、セキュア アドレスとして学習されます。DHCP クライアントの MAC アドレスは、スイッチが非 DHCP データ トラフィックを受信するときにだけ、セキュア アドレスとして学習されます。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **inteface** *interface-id*	スタティック IP 送信元バインディングを追加します。 このコマンドは、スタティック バインディングごとに入力します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip verify source** [**interface** *interface-id*]	IP ソース ガードの設定を確認します。
ステップ 8	**show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**inteface** *interface-id*] [**vlan** *vlan-id*]	（任意）スイッチ、特定の VLAN、または特定のインターフェイス上の IP 送信元バインディングを表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

送信元 IP アドレス フィルタリングによる IP ソース ガードをディセーブルにするには、**no ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

スタティック IP 送信元バインディング エントリを削除するには、**no ip source** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 10 および VLAN 11 で送信元 IP および MAC フィルタリングによる IP ソース ガードをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet1/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/1
Switch(config)# end
```

スタティック ホストの IP ソース ガードの設定

レイヤ 2 アクセス ポートでのスタティック ホストの IP ソース ガードの設定

（注）　スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。IP 装置追跡のグローバルなイネーブル化またはインターフェイス上での IP 装置の上限の設定を行わずに、ポートでこのコマンドの設定だけを行った場合、スタティック ホストの IPSG は、そのインターフェイスからの IP トラフィックをすべて拒否します。この要件は、プライベート VLAN ホスト ポート上のスタティック ホストの IPSG にも適用されます。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking**	IP ホスト テーブルをオンにし、IP 装置追跡をグローバルにイネーブルにします。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	ポートを アクセス ポートに設定します。
ステップ 5	**switchport access vlan** *vlan-id*	このポートの VLAN を設定します。

	コマンド	目的
ステップ 6	**ip verify source tracking port-security**	MAC アドレス フィルタリングによるスタティック ホストの IPSG をイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して、IP ソース ガードとポート セキュリティの両方をイネーブルにする場合は、次の 2 つの点に注意してください。 • DHCP サーバは Option 82 をサポートしている必要があります。そうでない場合は、クライアントに IP アドレスが割り当てられません。 • DHCP パケットの MAC アドレスは、セキュア アドレスとして学習されます。DHCP クライアントの MAC アドレスは、スイッチが非 DHCP データトラフィックを受信するときにだけ、セキュア アドレスとして学習されます。
ステップ 7	**ip device tracking maximum** *number*	IP 装置追跡テーブルで許可される、ポート上のスタティック IP 数の上限を設定します。指定できる範囲は 1 ～ 10 です。最大数は 10 です。 （注）　**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 8	**switchport port-security**	（任意）このポートのポート セキュリティをアクティブにします。
ステップ 9	**switchport port-security maximum** *value*	（任意）このポートの MAC アドレスの上限を設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip verify source interface** *interface-id*	設定を確認し、スタティック ホストの IPSG の許可 ACL を表示します。
ステップ 12	**show ip device track all [active | inactive] count**	スイッチ インターフェイス上の指定されたホストの IP と MAC のバインディングを表示して、設定を確認します。 • **all active**：アクティブな IP または MAC バインディング エントリだけを表示します。 • **all inactive**：非アクティブな IP または MAC バインディング エントリだけを表示します。 • **all**:アクティブおよび非アクティブな IP または MAC バインディング エントリを表示します。

次に、インターフェイスでスタティック ホストの IPSG を停止する例を示します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

次に、ポートでスタティック ホストの IPSG をイネーブルにする例を示します。

```
Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security
```

次に、レイヤ 2 アクセス ポートで IP フィルタによる IPSG イネーブルにし、インターフェイス Gi0/3 上の有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip trk       active       40.1.1.24                           10
Gi0/3      ip trk       active       40.1.1.20                           10
Gi0/3      ip trk       active       40.1.1.21                           10
```

次に、レイヤ 2 アクセス ポートで IP-MAC フィルタによる IPSG イネーブルにし、インターフェイス Gi0/3 上の有効な IP-MAC バインディングを確認して、このインターフェイス上のバインディング数が上限に達していることを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Gi0/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Gi0/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Gi0/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Gi0/3      ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  1
```

次に、すべてのインターフェイスの IP または MAC バインディング エントリをすべて表示する例を示します。CLI には、アクティブなエントリと非アクティブなエントリがすべて表示されます。インターフェイスでホストが学習されると、新しいエントリはアクティブとマークされます。同じホストがそのインターフェイスから切断され、別のインターフェイスに接続された場合、新しい IP または MAC バインディングは、ホストが検出されるとすぐにアクティブと表示されます。前のインターフェイス上のこのホストの古いエントリは、非アクティブとマークされます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface             STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
```

```
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

次に、すべてのインターフェイスのアクティブな IP または MAC バインディング エントリをすべて表示する例を示します。

```
Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
```

次に、すべてのインターフェイスの非アクティブな IP または MAC バインディング エントリをすべて表示する例を示します。ホストは、最初に GigabitEthernet 0/1 で学習され、次に GigabitEthernet 0/2 に移動されます。GigabitEthernet 0/1 で学習された IP または MAC アドレスは、非アクティブとマークされます。

```
Switch# show ip device tracking all inactive
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

次に、すべてのインターフェイスの IP 装置追跡のホスト エントリの合計数を表示する例を示します。

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
-----------------------------------------------------------------------
  Interface           Maximum Limit           Number of Entries
-----------------------------------------------------------------------
Gi0/3                  5
```

プライベート VLAN ホスト ポートでのスタティック ホストの IP ソース ガードの設定

（注） スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。IP 装置追跡のグローバルなイネーブル化またはインターフェイス上での IP 装置の上限の設定を行わずに、ポートでこのコマンドの設定だけを行った場合、スタティック ホストの IPSG は、そのインターフェイスからの IP トラフィックをすべて拒否します。この要件は、レイヤ 2 アクセス ポート上のスタティック ホストの IPSG にも適用されます。

レイヤ 2 アクセス ポート上で IP フィルタによるスタティック ホストの IPSG を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id1*	VLAN コンフィギュレーション モードを開始します。
ステップ 3	**private-vlan primary**	プライベート VLAN ポートにプライマリ VLAN を設定します。
ステップ 4	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 5	**vlan** *vlan-id2*	別の VLAN のコンフィギュレーション VLAN モードを開始します。
ステップ 6	**private-vlan isolated**	プライベート VLAN ポートに独立 VLAN を設定します。
ステップ 7	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 8	**vlan** *vlan-id1*	コンフィギュレーション VLAN モードを開始します。
ステップ 9	**private-vlan association 201**	独立プライベート VLAN ポート上の VLAN を関連付けます。
ステップ 10	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 11	**interface fastEthernet** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**switchport mode private-vlan host**	（任意）ポートをプライベート VLAN ホストとして設定します。
ステップ 13	**switchport private-vlan host-association** *vlan-id1 vlan-id2*	（任意）このポートを対応するプライベート VLAN に関連付けます。
ステップ 14	**ip device tracking maximum** *number*	IP 装置追跡テーブルで許可される、ポート上のスタティック IP 数の上限を設定します。 最大数は 10 です。 **（注）** スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *number* インターフェイス コマンドをグローバルに設定する必要があります。
ステップ 15	**ip verify source tracking [port-security]**	このポートで MAC アドレス フィルタリングによるスタティック ホストの IPSG をアクティブにします。
ステップ 16	**end**	インターフェイス コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 17	**show ip device tracking all**	設定を確認します。
ステップ 18	**show ip verify source interface** *interface-id*	IP ソース ガードの設定を確認します。スタティック ホストの IPSG の許可 ACL を表示します。

次に、プライベート VLAN ホスト ポートで IP フィルタによるスタティック ホストの IPSG をイネーブルにする例を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int fastEthernet 4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface               STATE
-----------------------------------------------------------------------
40.1.1.24       0000.0000.0304  200  FastEthernet0/3         ACTIVE
40.1.1.20       0000.0000.0305  200  FastEthernet0/3         ACTIVE
40.1.1.21       0000.0000.0306  200  FastEthernet0/3         ACTIVE
40.1.1.22       0000.0000.0307  200  FastEthernet0/3         ACTIVE
40.1.1.23       0000.0000.0308  200  FastEthernet0/3         ACTIVE
```

この出力は、インターフェイス Fa0/3 で学習された 5 つの有効な IP-MAC バインディングを示しています。プライベート VLAN の場合、バインディングはプライマリ VLAN ID に関連付けられます。したがって、この例では、プライマリ VLAN ID 200 が表に表示されます。

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/3      ip trk       active       40.1.1.23                           200
Fa0/3      ip trk       active       40.1.1.24                           200
Fa0/3      ip trk       active       40.1.1.20                           200
Fa0/3      ip trk       active       40.1.1.21                           200
Fa0/3      ip trk       active       40.1.1.22                           200
Fa0/3      ip trk       active       40.1.1.23                           201
Fa0/3      ip trk       active       40.1.1.24                           201
Fa0/3      ip trk       active       40.1.1.20                           201
Fa0/3      ip trk       active       40.1.1.21                           201
Fa0/30/3      ip trk       active       40.1.1.22                           201
```

この出力は、プライマリ VLAN とセカンダリ VLAN の両方に 5 つの有効な IP-MAC バインディングがあることを示しています。

IP ソース ガード情報の表示

表 26-3　IP ソース ガード情報を表示するためのコマンド

コマンド	目的
show ip device tracking	すべてのインターフェイスのアクティブな IP または MAC バインディング エントリを表示します。
show ip source binding	スイッチ上の IP 送信元バインディングを表示します。
show ip verify source	スイッチ上の IP ソース ガード設定を表示します。

DHCP サーバのポートベースのアドレス割り当ての概要

DHCP サーバのポートベースのアドレス割り当ては、接続されている装置のクライアント ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポート上で同じアドレスを保持できるようにする機能です。

イーサネット スイッチがネットワーク内に配置されている場合、それらのスイッチは、直接接続されている装置への接続を提供します。一部の環境（作業現場など）では、装置に障害が発生した場合、既存ネットワーク内の交換装置がただちに稼動する必要があります。現在の DHCP 実装では、DHCP が交換装置に同じ IP アドレスを提供する保証はありません。制御やモニタなどに使用されるソフトウェアでは、安定した IP アドレスが各装置に関連付けられていることが前提となります。装置を交換したときには、DHCP クライアントが変更された場合でも、安定したアドレスが割り当てられる必要があります。

DHCP サーバのポートベースのアドレス割り当て機能を設定すると、ポートで受信した DHCP メッセージのクライアント ID またはクライアント ハードウェア アドレスが変更された場合でも、常に同じ IP アドレスが同じ接続ポートに提供されることが保証されます。DHCP プロトコルでは、DHCP パケット内のクライアント ID オプションで DHCP クライアントが識別されます。クライアント ID オプションを挿入しないクライアントは、クライアント ハードウェア アドレスで識別されます。この機能を設定した場合は、インターフェイスのポート名がクライアント ID やハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

どの場合でも、イーサネット ケーブルを同じポートに接続することで、同じ IP アドレスが DHCP を介して接続装置に割り当てられます。

DHCP サーバのポートベースのアドレス割り当て機能は、Cisco IOS DHCP でだけサポートされ、サードパーティ製サーバではサポートされません。

DHCP サーバのポートベースのアドレス割り当ての設定

ここでは、次の設定情報について説明します。

- 「ポートベースのアドレス割り当てのデフォルト設定」（P.26-26）
- 「ポートベースのアドレス割り当て設定時の注意事項」（P.26-27）
- 「DHCP サーバのポートベースのアドレス割り当てのイネーブル化」（P.26-27）

ポートベースのアドレス割り当てのデフォルト設定

デフォルトでは、DHCP サーバのポートベースのアドレス割り当てはディセーブルに設定されています。

ポートベースのアドレス割り当て設定時の注意事項

ここでは、DHCP ポートベースのアドレス割り当ての設定時の注意事項を説明します。

- 1 つのポートに割り当てることができる IP アドレスは 1 つだけです。
- 予約済み（事前割り当て済み）のアドレスは、**clear ip dhcp binding** グローバル コンフィギュレーション コマンドで消去できません。
- 事前割り当て済みのアドレスは、通常のダイナミック IP アドレス割り当てから自動的に除外されます。事前割り当て済みのアドレスはホスト プールで使用できませんが、各 DHCP アドレス プールには複数のアドレスを事前に割り当てることができます。
- DHCP プールからの割り当てを、予約済みアドレスに制限する（予約されていないアドレスはクライアントに提供されず、他のクライアントにはプールのサービスが提供されない）には、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

DHCP サーバのポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブルにし、インターフェイス上で加入者 ID を自動的に生成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp use subscriber-id client-id**	DHCP サーバがすべての着信 DHCP メッセージで加入者 ID をクライアント ID としてグローバルに使用するように設定します。
ステップ 3	**ip dhcp subscriber-id interface-name**	インターフェイスの短い名前に基づいて加入者 ID を自動的に生成します。 特定のインターフェイス上で設定された加入者 ID は、このコマンドよりも優先されます。
ステップ 4	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip dhcp server use subscriber-id client-id**	DHCP サーバがインターフェイス上のすべての着信 DHCP メッセージで加入者 ID をクライアント ID として使用するように設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチで DHCP ポートベースのアドレス割り当てをイネーブルにしたあとに、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用し、IP アドレスの事前割り当てを行って、そのアドレスをクライアントに関連付けます。DHCP プールからの割り当てを、予約済みアドレスに制限するには、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。ネットワークに含まれているアドレスやプール範囲にあるアドレスでも、予約されていないアドレスはクライアントに提供されず、他のクライアントには DHCP プールのサービスが提供されません。ユーザはこのコマンドを使用して、DHCP プールを装備した 1 組のスイッチが共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視するように設定できます。

IP アドレスの事前割り当てを行って、そのアドレスをインターフェイス名で識別されるクライアントに関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *poolname*	DHCP プール コンフィギュレーション モードを開始し、DHCP プールの名前を定義します。プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 3	**network** *network-number* [*mask* | */prefix-length*]	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。
ステップ 4	**address** *ip-address* **client-id** *string* [**ascii**]	インターフェイス名で識別される DHCP クライアントの IP アドレスを予約します。 *string* : ASCII 値または 16 進数値を指定できます。
ステップ 5	**reserved-only**	（任意）DHCP アドレス プール内の予約済みアドレスだけを使用します。デフォルトでは、プール アドレスは制限されません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip dhcp pool**	DHCP プールの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

DHCP ポートベースのアドレス割り当てをディセーブルにするには、**no ip dhcp use subscriber-id client-id** グローバル コンフィギュレーション コマンドを使用します。加入者 ID の自動生成をディセーブルにするには、**no ip dhcp subscriber-id interface-name** グローバル コンフィギュレーション コマンドを使用します。インターフェイス上で加入者 ID をディセーブルにするには、**no ip dhcp server use subscriber-id client-id** インターフェイス コンフィギュレーション コマンドを使用します。

IP アドレスの予約を DHCP プールから削除するには、**no address** *ip-address* **client-id** *string* DHCP プール コンフィギュレーション コマンドを使用します。アドレス プールを制限なしに変更するには、**no reserved-only** DHCP プール コンフィギュレーション コマンドを使用します。

次の例では、加入者 ID が自動的に生成され、DHCP サーバは DHCP メッセージのクライアント ID フィールドを無視し、代わりに加入者 ID を使用します。加入者 ID は、インターフェイスの短い名前とクライアントの事前割り当て済み IP アドレス 10.1.1.7 に基づいています。

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
```

```
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id “Et1/0” ascii
<output truncated>
```

次の例は、事前割り当て済みのアドレスが DHCP プールで正しく予約されたことを示しています。

```
switch# show ip dhcp pool dhcppool
Pool dhcp pool:
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 0
 Excluded addresses : 4
 Pending event : none
 1 subnet is currently in the pool:
 Current index   IP address range         Leased/Excluded/Total
 10.1.1.1        10.1.1.1 - 10.1.1.254     0     / 4 / 254
 1 reserved address is currently in the pool
 Address         Client
 10.1.1.7 Et1/0
```

DHCP サーバのポートベースのアドレス割り当て機能の詳細については、Cisco.com ページで [Search] フィールドに *Cisco IOS IP Addressing Services* と入力して、Cisco IOS ソフトウェア マニュアルにアクセスしてください。マニュアルは次の URL からも入手できます。
http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

DHCP サーバのポートベースのアドレス割り当ての表示

DHCP サーバのポートベースのアドレス割り当て情報を表示するには、表 26-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 26-4　DHCP ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
show interface *interface id*	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバのアドレス バインディングを表示します。

CHAPTER 27

ダイナミック ARP 検査の設定

この章では、IE 3000 スイッチに Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（ダイナミック ARP 検査）を設定する方法について説明します。この機能は、スイッチに対する悪意ある攻撃を防ぐため、無効な ARP 要求および ARP 応答が、同じ VLAN 内の他のポートにリレーされないようにします。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

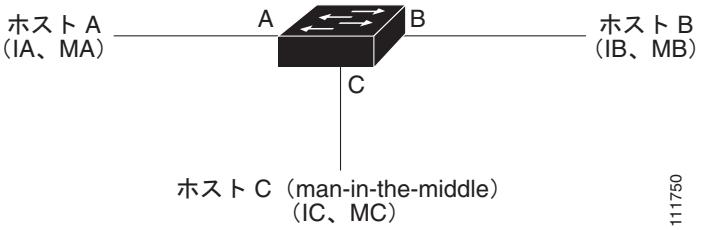
- 「ダイナミック ARP 検査の概要」（P.27-1）
- 「ダイナミック ARP 検査の設定」（P.27-5）
- 「ダイナミック ARP 検査情報の表示」（P.27-15）

ダイナミック ARP 検査の概要

ARP では、IP アドレスを MAC（メディア アクセス制御）アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B がホスト A に情報を送信しようとする場合、ホスト B の ARP キャッシュにホスト A の MAC アドレスが存在しないとします。ホスト B は、ホスト A の IP アドレスに関連付けられた MAC アドレスを取得するため、このブロードキャスト ドメイン内のすべてのホストに対してブロードキャスト メッセージを送信します。ブロードキャスト ドメイン内のすべてのホストがこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスを返します。ただし、ARP 要求を受信していない場合でも ARP によってホストが無償応答できるため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生する可能性があります。攻撃が開始されると、攻撃を受けた機器からのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意あるユーザは、サブネットに接続されたシステムの ARP キャッシュをポイズニング（汚染）し、このサブネット上の他のホスト宛てのトラフィックを代行受信することで、レイヤ 2 ネットワークに接続されたホスト、スイッチ、およびルータを攻撃できます。図 27-1 に、ARP キャッシュ ポイズニングの例を示します。

図 27-1　ARP キャッシュ ポイズニング



ホスト A、B、C は、それぞれインターフェイス A、B、C でスイッチに接続されています。すべてのホストは同一サブネットに属します。カッコ内は、各ホストの IP および MAC アドレスを示します。たとえば、ホスト A の IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤ上でホスト B と通信する必要がある場合、ホスト A は、IP アドレス IB に関連付けられた MAC アドレスに対する ARP 要求をブロードキャストします。スイッチとホスト B は ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングを、それぞれの ARP キャッシュ内に書き込みます。たとえば、IP アドレス IA が MAC アドレス MA にバインドされます。ホスト B が応答すると、スイッチとホスト A は、IP アドレス IB および MAC アドレス MB を持つホストのバインディングを、それぞれの ARP キャッシュ内に書き込みます。

ホスト C は、IP アドレス IA（または IB）および MAC アドレス MC を持つホストのバインディングによって偽装した ARP 応答をブロードキャストすることで、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングできます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は、ホスト A からホスト B へのトラフィック ストリーム内に自身を割り込ませています。これは、典型的な *man-in-the-middle* 攻撃です。

ダイナミック ARP 検査は、ネットワーク内の ARP パケットを検証するセキュリティ機能です。この機能は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、ログ記録、および廃棄します。この機能により、一部の man-in-the-middle 攻撃からネットワークを保護できます。

ダイナミック ARP 検査を使用することで、有効な ARP 要求および ARP 応答だけがリレーされるようにできます。スイッチの動作は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットは廃棄します。

ダイナミック ARP 検査は、信頼できるデータベースに保存された IP アドレスと MAC アドレスとの有効なバインディングに基づき、ARP パケットの有効性を判断します。このデータベースを、DHCP スヌーピング バインディング データベースと呼びます。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。信頼できるインターフェイス上で ARP パケットを受信した場合、スイッチはこのパケットを検査せずに転送します。信頼できないインターフェイスでは、スイッチは有効性を確認できたパケットだけを転送します。

ダイナミック ARP 検査を VLAN 単位でイネーブルにするには、**ip arp inspection vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「DHCP 環境におけるダイナミック ARP 検査の設定」（P.27-7）を参照してください。

非 DHCP 環境におけるダイナミック ARP 検査では、スタティックに設定した IP アドレスを持つホストに対し、ユーザ定義の ARP Access Control List（ACL; アクセス制御リスト）に照合することで ARP パケットを検証できます。ARP ACL を定義するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「非 DHCP 環境に対する ARP ACL の設定」（P.27-9）を参照してください。スイッチは、廃棄されたパケットをログ記録します。ログ バッファの詳細については、「廃棄パケットのロギング」（P.27-5）を参照してください。

ダイナミック ARP 検査では、パケット内の IP アドレスが無効な場合に ARP パケットを廃棄するのか、または ARP パケット本体の MAC アドレスがイーサネット ヘッダーに指定されたアドレスと一致しない場合に ARP パケットを廃棄するのかを設定できます。**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} グローバル コンフィギュレーション コマンドを使用してください。詳細については、「有効性検査の実行」（P.27-12）を参照してください。

インターフェイスの信頼状態とネットワーク セキュリティ

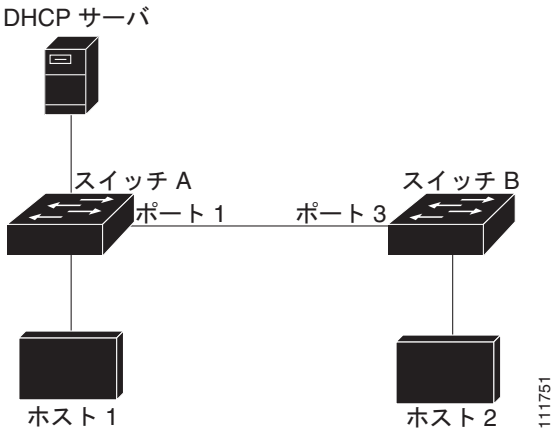
ダイナミック ARP 検査は、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、ダイナミック ARP 検査のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、ダイナミック ARP 検査の有効性検査が行われます。

一般的なネットワーク設定では、ホスト ポートに接続されているすべてのスイッチ ポートを信頼できないポートとして、スイッチに接続されているすべてのスイッチ ポートを信頼できるポートとして設定します。この設定では、指定のスイッチからネットワークに送信されるすべての ARP パケットは、セキュリティ検査をバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、**ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

注意　信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

図 27-2 では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 が属する VLAN 上でダイナミック ARP 検査を実行していると仮定します。ホスト 1 とホスト 2 がスイッチ A に接続されている DHCP サーバから IP アドレスを取得すると、スイッチ A だけがホスト 1 の IP アドレスと MAC アドレスをバインドします。したがって、スイッチ A とスイッチ B の間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B では廃棄されます。こうして、ホスト 1 とホスト 2 の間の接続が失われます。

図 27-2　ダイナミック ARP 検査をイネーブルにした VLAN での ARP パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A がダイナミック ARP 検査を実行していなければ、ホスト 1 は（スイッチ間のリンクが信頼可能として設定されている場合はホスト 2 も同様）、スイッチ B の ARP キャッシュを簡単にポイズニングできます。この状況は、スイッチ B がダイナミック ARP 検査を実行している場合でも起こりえます。

ダイナミック ARP 検査は、ダイナミック ARP 検査を実行するスイッチに接続された、信頼できないインターフェイス上のホストが、ネットワーク内の他のホストの ARP キャッシュをポイズニングしないように保証します。しかし、ネットワークのその他の場所にあるホストが、ダイナミック ARP 検査を実行するスイッチに接続されたホストのキャッシュをポイズニングする可能性は防止できません。

ダイナミック ARP 検査を実行するスイッチと実行しないスイッチが VLAN 内にある場合は、これらのスイッチに接続されたインターフェイスを信頼できないインターフェイスとして設定します。ただし、ダイナミック ARP 検査を実行していないスイッチからのパケットのバインディングを検証するには、ダイナミック ARP 検査を実行するスイッチに ARP ACL を設定します。こうしたバインディングを判断できない場合は、レイヤ 3 において、ダイナミック ARP 検査を実行するスイッチを実行しないスイッチから切り離します。設定の詳細については、「非 DHCP 環境に対する ARP ACL の設定」（P.27-9）を参照してください。

（注）　DHCP サーバとネットワークのセットアップ方法によっては、VLAN 内のすべてのスイッチで、指定の ARP パケットを検証できない場合もあります。

ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP 検査の有効性を確認することによって、着信 ARP パケット数をレート制限し、DoS 攻撃を防止します。デフォルトでは、信頼できないインターフェイスのレートは 15 pps（パケット/秒）です。信頼できるインターフェイスは、レート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが、設定したレート制限を超えると、スイッチはこのポートを errdisable ステートに設定します。ユーザが介入するまで、ポートはこの状態を維持します。errdisable ステート回復をイネーブルにするには、**errdisable recovery** グローバル コンフィギュレーション コマンドを使用します。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

設定の詳細については、「着信 ARP パケットのレート制限」（P.27-11）を参照してください。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP 検査では、DHCP スヌーピング バインディング データベースを使用して、IP アドレスと MAC アドレスとの有効なバインディングのリストを維持します。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL のほうが優先されます。ACL は、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して設定している場合に限り、スイッチに適用されます。スイッチはまず、ARP パケットを、ユーザが設定した ARP ACL と照合します。ARP パケットが ARP ACL によって拒否される場合は、DHCP スヌーピングによって書き込まれた有効なバインディングがデータベース内に存在する場合であっても、スイッチはこのパケットを拒否します。

廃棄パケットのロギング

スイッチはパケットを廃棄すると、ログ バッファ内にエントリを作成して、レート制限に基づくシステム メッセージを生成します。メッセージの生成後、スイッチはこのエントリをログ バッファから消去します。各ログ エントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定するには、**ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドを使用します。ログ記録されるパケットのタイプを指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「ログ バッファの設定」（P.27-13）を参照してください。

ダイナミック ARP 検査の設定

ここでは、次の設定情報について説明します。

ダイナミック ARP 検査のデフォルト設定

表 27-1 に、ダイナミック ARP 検査のデフォルト設定を示します。

表 27-1　ダイナミック ARP 検査のデフォルト設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブルです。
インターフェイスの信頼状態	すべてのインターフェイスは信頼できない状態です。

表 27-1　ダイナミック ARP 検査のデフォルト設定 （続き）

機能	デフォルト設定
着信 ARP パケットのレート制限	このレートは、信頼できないインターフェイス上で 15 pps に設定されています。ただし、1 台のホストが 1 秒間に 15 台の新規ホストに接続できるスイッチド ネットワークであると仮定しています。 信頼できるすべてのインターフェイスでは、レートは無制限です。 バースト インターバルは 1 秒に設定されています。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	どの検証も実行されません。
ログ バッファ	ダイナミック ARP 検査をイネーブルにした場合は、拒否または廃棄されたすべての ARP パケットがログ記録されます。 ログ内のエントリ数は 32 です。 システム メッセージの数は 1 秒あたり 5 つに制限されています。 ロギングレート インターバルは、1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットがログ記録されます。

ダイナミック ARP 検査設定時の注意事項

ダイナミック ARP 検査設定時の注意事項を次に示します。

- ダイナミック ARP 検査は入力セキュリティ機能であり、出力検査は行いません。
- ダイナミック ARP 検査は、ダイナミック ARP 検査をサポートしないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されたホストに対しては、効果がありません。man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、ダイナミック ARP 検査が有効なドメインを、ダイナミック ARP 検査の行われないドメインから切り離します。これにより、ダイナミック ARP 検査をイネーブルにしたドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- ダイナミック ARP 検査では、受信する ARP 要求および ARP 応答内の IP と MAC アドレス とのバインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。設定の詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。

  DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可および拒否を行います。
- ダイナミック ARP 検査は、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポート上でサポートされています。

（注）　RSPAN VLAN 上では、ダイナミック ARP 検査をイネーブルにしないでください。RSPAN VLAN 上でダイナミック ARP 検査をイネーブルにすると、ダイナミック ARP 検査パケットが RSPAN 宛先ポートに到達しないことがあります。

- 物理ポートを EtherChannel ポート チャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポート チャネル内で中断状態のままとなります。ポート チャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポート チャネルの信頼状態を変更すると、スイッチはチャネルを構成するすべての物理ポートに対し、新たにこの信頼状態を設定します。

- ポート チャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポートチャネルの設定に照合して検査されます。ポート チャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。

- 受信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートは、各ポートの集約値を考慮し、ダイナミック ARP 検査をイネーブルにした複数の VLAN でパケットを処理できるように、高い値に設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用すると、レートを無制限として設定できます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

- スイッチ上でダイナミック ARP 検査をイネーブルにすると、ARP トラフィックに対して設定されていたポリサーは効力を失います。その結果、すべての ARP トラフィックが CPU に送信されるようになります。

DHCP 環境におけるダイナミック ARP 検査の設定

この手順は、2 つのスイッチがダイナミック ARP 検査機能をサポートする場合の設定方法を示します。図 27-2（P.27-4）に示すように、ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。両方のスイッチは、各ホストが属する VLAN 1 上でダイナミック ARP 検査を実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同じ DHCP サーバから IP アドレスを取得します。したがって、スイッチ A はホスト 1 およびホスト 2 のバインディングを持ち、スイッチ B はホスト 2 のバインディングを持ちます。

（注）　ダイナミック ARP 検査では、受信する ARP 要求および ARP 応答内の IP と MAC アドレス とのバインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。設定の詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。

1 台のスイッチだけがダイナミック ARP 検査機能をサポートしている場合の設定方法については、「非 DHCP 環境に対する ARP ACL の設定」（P.27-9）を参照してください。

ダイナミック ARP 検査を設定するには、特権 EXEC モードで次の手順を実行します。両方のスイッチでこの手順を実行する必要があります。この手順は必須です。

	コマンド	目的
ステップ 1	**show cdp neighbors**	スイッチ間の接続を確認します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip arp inspection *vlan*** *vlan-range*	VLAN 単位でダイナミック ARP 検査をイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP 検査がディセーブルになっています。 *vlan-range* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 両方のスイッチに対して同じ VLAN ID を指定します。
ステップ 4	**interface** *interface-id*	別のスイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip arp inspection trust**	スイッチ間の接続を、信頼できる接続として設定します。 デフォルトでは、すべてのインターフェイスは信頼できない状態です。 スイッチは、信頼できるインターフェイス上の他のスイッチから受信した ARP パケットは検査しません。この場合、パケットはそのまま転送されます。 信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。スイッチは、無効なパケットを廃棄し、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。詳細については、「ログ バッファの設定」（P.27-13）を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip arp inspection interfaces** **show ip arp inspection vlan** *vlan-range*	ダイナミック ARP 検査の設定を確認します。
ステップ 8	**show ip dhcp snooping binding**	DHCP バインディングを確認します。
ステップ 9	**show ip arp inspection statistics vlan** *vlan-range*	ダイナミック ARP 検査の統計情報を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ダイナミック ARP 検査をディセーブルにするには、**no ip arp inspection vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。インターフェイスを信頼できない状態に戻すには、**no ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

次に、VLAN 1 内のスイッチ A にダイナミック ARP 検査を設定する例を示します。スイッチ B にも同様の手順を実行します。

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境に対する ARP ACL の設定

この手順では、図 27-2 (P.27-4) に示すスイッチ B がダイナミック ARP 検査および DHCP スヌーピングをサポートしていない場合の、ダイナミック ARP 検査の設定方法を示します。

スイッチ A のポート 1 を信頼できるポートとして設定すると、セキュリティ ホールが生じます。これは、スイッチ A およびホスト 1 が、スイッチ B またはホスト 2 によって攻撃される可能性があるためです。この可能性を排除するには、スイッチ A のポート 1 を信頼できないポートとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL を設定して VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない場合は、スイッチ A に ACL 設定を適用できなくなるため、レイヤ 3 でスイッチ B からスイッチ A を切り離す必要があります。これらのスイッチ間では、ルータを使用してパケットをルーティングします。

スイッチ A に ARP ACL を設定するには、特権 EXEC モードで次の手順を実行します。この手順は、非 DHCP 環境では必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**arp access-list** *acl-name*	ARP ACL を定義し、ARP アクセスリスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセスリストは定義されていません。 **（注）** ARP アクセス リストの末尾には、暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 3	**permit ip host** *sender-ip* **mac host** *sender-mac* [**log**]	指定したホスト（ホスト 2）からの ARP パケットを許可します。 • *sender-ip* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。 • （任意）Access Control Entry（ACE; アクセス制御エントリ）と一致したパケットをログ バッファに記録するには、**log** を指定します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで **matchlog** キーワードを設定している場合も、一致したパケットがログ記録されます。詳細については、「ログ バッファの設定」（P.27-13）を参照してください。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 5	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]	ARP ACL を VLAN に適用します。デフォルトでは、VLAN に適用される ARP ACL は定義されていません。 • *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。 • *vlan-range* には、スイッチとホストが属する VLAN を指定します。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットを廃棄するために、**static** を指定します。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、パケットを拒否する明示的な拒否が ACL 内にないことを意味し、パケットが ACL 内の句に一致しないと DHCP バインディングがパケットの許可または拒否を決定します。 IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセス リストで許可された場合にだけ許可されます。
ステップ 6	**interface** *interface-id*	スイッチ B に接続されているスイッチ A のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**no ip arp inspection trust**	スイッチ B に接続されているスイッチ A のインターフェイスを、信頼できないインターフェイスとして設定します。 デフォルトでは、すべてのインターフェイスは信頼できない状態です。 信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。スイッチは、無効なパケットを廃棄し、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。詳細については、「ログ バッファの設定」（P.27-13）を参照してください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show arp access-list** [*acl-name*] **show ip arp inspection vlan** *vlan-range* **show ip arp inspection interfaces**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ARP ACL を削除するには、**no arp access-list** グローバル コンフィギュレーション コマンドを使用します。VLAN に関連付けられた ARP ACL を削除するには、**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチ A に *host2* という ARP ACL を設定し、ホスト 2（IP アドレス 1.1.1.1、MAC アドレス 0001.0001.0001）からの ARP パケットを許可し、ACL を VLAN 1 に適用し、スイッチ A のポート 1 を信頼できないポートとして設定する例を示します。

```
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no ip arp inspection trust
```

着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP 検査の有効性を確認することによって、着信 ARP パケット数をレート制限し、DoS 攻撃を防止します。

着信 ARP パケットのレートが、設定したレート制限を超えると、スイッチはこのポートを errdisable ステートに設定します。ポートは、errdisable ステート回復がイネーブルにされるまで、errdisable ステートを維持します。errdisable ステート回復をイネーブルにすると、指定のタイムアウト時間が経過した時点で、ポートは自動的にこのステートから回復します。

（注） インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更すると、レート制限も信頼状態のデフォルト値に変更されます。レート制限を設定すると、インターフェイスはその信頼状態が変更された場合でも設定されたレート制限を維持します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

トランク ポートおよび EtherChannel ポートのレート制限設定時の注意事項については、「ダイナミック ARP 検査設定時の注意事項」（P.27-6）を参照してください。

着信 ARP パケットのレートを制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レート制限するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] | **none**}	インターフェイスに着信する ARP 要求および ARP 応答のレートを制限します。 デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒に設定されています。 キーワードの意味は次のとおりです。 • **rate** *pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。指定できる範囲は 0 ～ 2048 pps です。 • （任意）**burst interval** *seconds* には、レートの高い ARP パケットの有無についてインターフェイスをモニタする間隔（秒）を指定します。指定できる範囲は 1 ～ 15 です。 • **rate none** の場合は、処理できる着信 ARP パケットのレートの上限を指定しません。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**errdisable recovery cause arp-inspection interval** *interval*	（任意）ダイナミック ARP 検査の errdisable ステートからの回復をイネーブルにします。 デフォルトでは、回復はディセーブルに、回復間隔は 300 秒に設定されています。 **interval** *interval* には、errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。
ステップ 6	**exit**	特権 EXEC モードに戻ります。
ステップ 7	**show ip arp inspection interfaces** **show errdisable recovery**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのレート制限設定に戻すには、**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。ダイナミック ARP 検査のエラー回復をディセーブルにするには、**no errdisable recovery cause arp-inspection** グローバル コンフィギュレーション コマンドを使用します。

有効性検査の実行

ダイナミック ARP 検査は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、ログ記録、および廃棄します。宛先 MAC アドレス、送信元と宛先の IP アドレス、および送信元 MAC アドレスに対する追加の検査を実行するように、スイッチを設定できます。

着信 ARP パケットに特定の検査を実行するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}	着信 ARP パケットに特定の検査を実行します。デフォルトでは、どの検査も実行されません。 キーワードの意味は次のとおりです。 • **src-mac** の場合は、イーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信元 MAC アドレスと比較します。この検証は、ARP 要求と ARP 応答に両方に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、廃棄されます。 • **dst-mac** の場合は、イーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体の宛先 MAC アドレスと比較します。この検証は、ARP 応答に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、廃棄されます。 • **ip** の場合は、無効な IP アドレスや予期しない IP アドレスが ARP 本体にないかどうかを確認します。0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスがこれに該当します。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。 少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、あるコマンドで **src mac** および **dst mac** の検証をイネーブルにし、2 番めのコマンドで IP 検証だけをイネーブルにした場合は、2 番めのコマンドによって **src mac** および **dst mac** の検証がディセーブルになります。
ステップ 3	**exit**	特権 EXEC モードに戻ります。
ステップ 4	**show ip arp inspection vlan** *vlan-range*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

検査をディセーブルにするには、**no ip arp inspection validate** [**src-mac**] [**dst-mac**] [**ip**] グローバル コンフィギュレーション コマンドを使用します。転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、および IP 検証に失敗したパケットの統計情報を表示するには、**show ip arp inspection statistics** 特権 EXEC コマンドを使用します。

ログ バッファの設定

スイッチはパケットを廃棄すると、ログ バッファ内にエントリを作成して、レート制限に基づくシステム メッセージを生成します。メッセージの生成後、スイッチはこのエントリをログ バッファから消去します。各ログ エントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

1 つのログ バッファ エントリによって、複数のパケットを表現できます。たとえば、同じ ARP パラメータを持つ同一 VLAN 上で、1 つのインターフェイスが多数のパケットを受信した場合は、ログ バッファではこれらのパケットが 1 つのエントリとして結合され、このエントリに対して 1 つのシステム メッセージが生成されます。

ログ バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに [--] が表示されます。このエントリに関してそれ以外の統計情報は表示されません。このようなエントリが表示された場合は、ログ バッファ内のエントリ数を増やすか、またはログ レートを高くしてください。

ログ バッファを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip arp inspection log-buffer** {**entries** *number* | **logs** *number* **interval** *seconds*}	ダイナミック ARP 検査のログ バッファを設定します。 デフォルトでは、ダイナミック ARP 検査をイネーブルにした場合は、拒否または廃棄された ARP パケットがログ記録されます。ログ エントリ数は、32 です。システム メッセージの数は 1 秒あたり 5 つに制限されています。ロギングレート インターバルは、1 秒です。 キーワードの意味は次のとおりです。 • **entries** *number* には、バッファにログ記録するエントリの数を指定します。指定できる範囲は 0 ～ 1024 です。 • **logs** *number* **interval** *seconds* には、指定のインターバルでシステム メッセージを生成するエントリの数を指定します。 **logs** *number* に指定できる範囲は 0 ～ 1024 です。値を 0 に設定すると、エントリはログ バッファに配置されますが、システム メッセージが生成されません。 指定できる **interval** *seconds* の範囲は 0 ～ 86400 秒（1 日）です。値を 0 に設定すると、システム メッセージがただちに生成されます（ログ バッファは常に空になります）。 インターバル値を 0 に設定すると、ログ値 0 は上書きされます。 **logs** および **interval** の設定は、相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合は、X を Y で割って（X/Y）求められたシステム メッセージ数が 1 秒間に送信されます。それ以外の場合は、Y を X で割って（Y/X）求められた間隔（秒）で 1 つのシステム メッセージが送信されます。

	コマンド	目的
ステップ 3	**ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	VLAN 単位でログ記録するパケットのタイプを制御します。デフォルトでは、拒否または廃棄されたすべてのパケットがログ記録されます。*ログ記録される*という表現は、エントリがログ バッファに格納されることと、システム メッセージが生成されることを意味しています。 キーワードの意味は次のとおりです。 • *vlan-range* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • **acl-match matchlog** の場合は、ACE ロギング設定に基づいてパケットをログ記録します。このコマンドに **matchlog** キーワードを指定して、さらに **permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドに **log** キーワードを指定すると、ACL によって許可または拒否された ARP パケットがログ記録されます。 • **acl-match none** の場合は、ACL と一致したパケットをログ記録しません。 • **dhcp-bindings all** の場合は、DHCP バインディングと一致したすべてのパケットがログ記録されます。 • **dhcp-bindings none** の場合は、DHCP バインディングと一致したパケットをログ記録しません。 • **dhcp-bindings permit** の場合は、DHCP バインディングによって許可されたパケットがログ記録されます。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**show ip arp inspection log**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのログ バッファ設定に戻すには、**no ip arp inspection log-buffer** {**entries** | **logs**} グローバル コンフィギュレーション コマンドを使用します。デフォルトの VLAN ログ設定に戻すには、**no ip arp inspection vlan** *vlan-range* **logging** {**acl-match** | **dhcp-bindings**} グローバル コンフィギュレーション コマンドを使用します。ログ バッファを消去するには、**clear ip arp inspection log** 特権 EXEC コマンドを使用します。

ダイナミック ARP 検査情報の表示

ダイナミック ARP 検査情報を表示するには、表 27-2 に示す各特権 EXEC コマンドを使用します。

表 27-2　ダイナミック ARP 検査情報を表示するためのコマンド

コマンド	説明
show arp access-list [*acl-name*]	ARP ACL に関する詳細情報を表示します。
show ip arp inspection interfaces [*interface-id*]	指定されたインターフェイスまたはすべてのインターフェイスに関して、ARP パケットの信頼状態およびレート制限を表示します。
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、ダイナミック ARP 検査がイネーブル（アクティブ）にされている VLAN の情報だけが表示されます。

ダイナミック ARP 検査の統計情報を消去または表示するには、表 27-3 に示す各特権 EXEC コマンドを使用します。

表 27-3　ダイナミック ARP 検査の統計情報を消去または表示するためのコマンド

コマンド	説明
clear ip arp inspection statistics	ダイナミック ARP 検査の統計情報を消去します。
show ip arp inspection statistics [**vlan** *vlan-range*]	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可または拒否されたパケット、DHCP によって許可または拒否されたパケットの統計情報を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、ダイナミック ARP 検査がイネーブル（アクティブ）にされている VLAN の情報だけが表示されます。

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インスペクション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

ダイナミック ARP 検査のログ情報を消去または表示するには、表 27-4 に示す各特権 EXEC コマンドを使用します。

表 27-4　ダイナミック ARP 検査のログ情報を消去または表示するためのコマンド

コマンド	説明
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファを消去します。
show ip arp inspection log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

これらのコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 28

IGMP スヌーピングおよび MVR の設定

この章では、ローカルの IGMP スヌーピングの適用、Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）など、IE 3000 スイッチに Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングを設定する手順について説明します。また、IGMP フィルタリングを使用してマルチキャスト グループのメンバーシップを制御する手順と、IGMP スロットリング アクションを設定する手順についても説明します。

（注） IP バージョン 6（IPv6）トラフィックの場合、Multicast Listener Discovery（MLD）スヌーピングは、IPv4 トラフィックの IGMP スヌーピングと同じ機能を実行します。MLD スヌーピングの詳細については、第 43 章「IPv6 MLD スヌーピングの設定」を参照してください。

（注） この章で使用されるコマンドの構文と使用方法の詳細については、このリリースのスイッチ コマンド リファレンスと、『*Cisco IOS IP Command Reference, Volume 3 of 3:Multicast, Release 12.2*』の「IP Multicast Routing Commands」を参照してください。このリリースは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にあります。

この章で説明する内容は、次のとおりです。

（注） IGMP スヌーピングや MVR などの機能を使用して IP マルチキャスト グループ アドレスを管理するか、またはスタティック IP アドレスを使用することもできます。

IGMP スヌーピングの概要

レイヤ 2 スイッチは、IGMP スヌーピングを使用して、レイヤ 2 インターフェイスのダイナミックな設定によるマルチキャスト トラフィックのフラッディングを抑制します。これにより、マルチキャスト トラフィックが、IP マルチキャスト装置と関連付けられたインターフェイスだけに転送されるようにします。名前が暗示するように、IGMP スヌーピングに必要となる LAN スイッチは、ホストおよびルータ間の IGMP 伝送にスヌーピングを行い、マルチキャスト グループとメンバー ポートの追跡を続けます。このスイッチが、特定のマルチキャスト グループに関する IGMP レポートをホストから受信すると、スイッチは転送テーブル エントリにこのホスト番号を追加します。ホストから IGMP Leave Group メッセージを受信すると、そのホスト ポートをテーブル エントリから削除します。また、マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しない場合は、スイッチが定期的にエントリを削除します。

（注）　IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャスト ルータはすべての VLAN に一般的クエリーを定期的に送信します。このマルチキャスト トラフィックに関係し、Join 要求を送信するすべてのホストが、転送テーブル エントリに追加されます。スイッチは、IGMP Join 要求を受信すると、各グループの IGMP スヌーピング IP マルチキャストの転送テーブルに VLAN あたり 1 つのエントリを生成します。

スイッチは、MAC アドレス グループではなく、IP マルチキャスト グループに基づいてブリッジをサポートします。マルチキャスト MAC アドレスに基づくグループを使用すると、設定済みの IP アドレスが以前に設定した MAC アドレスや予約済みの任意のマルチキャスト MAC アドレス（224.0.0.xxx の範囲内）に変換されると（エイリアスが作成されると）、コマンドが失敗します。スイッチは IP マルチキャスト グループを使用しているため、アドレスのエイリアス作成の問題は発生しません。

IGMP スヌーピングによって学習される IP マルチキャスト グループは、ダイナミックです。ただし、**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用すると、マルチキャスト グループをスタティックに設定できます。グループ メンバーシップをマルチキャスト グループ アドレスにスタティックに指定すると、その設定は IGMP スヌーピングによる自動的な処理よりも優先されます。マルチキャスト グループ メンバーシップのリストは、ユーザ定義の設定と、IGMP スヌーピングによって学習された設定の両方で構成できます。

IGMP スヌーピング クエリアを設定すると、マルチキャスト インターフェイスを使用しないでサブネット内の IGMP スヌーピングをサポートできます。これは、マルチキャスト トラフィックがルーティングを必要としないためです。IGMP スヌーピング クエリアの詳細については、「IGMP スヌーピング クエリアの設定」（P.28-14）を参照してください。

ポート スパニング ツリー、ポート グループ、または VLAN ID に変更が発生すると、IGMP スヌーピングによって学習されたマルチキャスト グループは、VLAN 内のこのポートから削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

IGMP のバージョン

スイッチは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートします。これらのバージョンはスイッチ上で相互運用が可能です。たとえば、IGMP スヌーピングが IGMPv2 スイッチ上でイネーブルであり、このスイッチがホストから IGMPv3 レポートを受信する場合、スイッチは IGMPv3 レポートをマルチキャスト ルータに転送できます。

（注）　スイッチがサポートする IGMPv3 スヌーピングは、宛先マルチキャスト MAC アドレスだけに基づいています。送信元 MAC アドレスまたはプロキシ レポートに基づくスヌーピングはサポートされません。

IGMPv3 スイッチがサポートする Basic IGMPv3 Snooping Support（BISS）には、IGMPv1 スイッチおよび IGMPv2 スイッチ上のスヌーピング機能と IGMPv3 メンバーシップ レポート メッセージのサポートが含まれます。BISS は、ネットワークに IGMPv3 ホストが含まれる場合にマルチキャスト トラフィックのフラッディングを抑制します。IGMPv2 ホストまたは IGMPv1 ホスト上の IGMP スヌーピング機能と、ほぼ同等のポート セットへのトラフィックを抑制します。

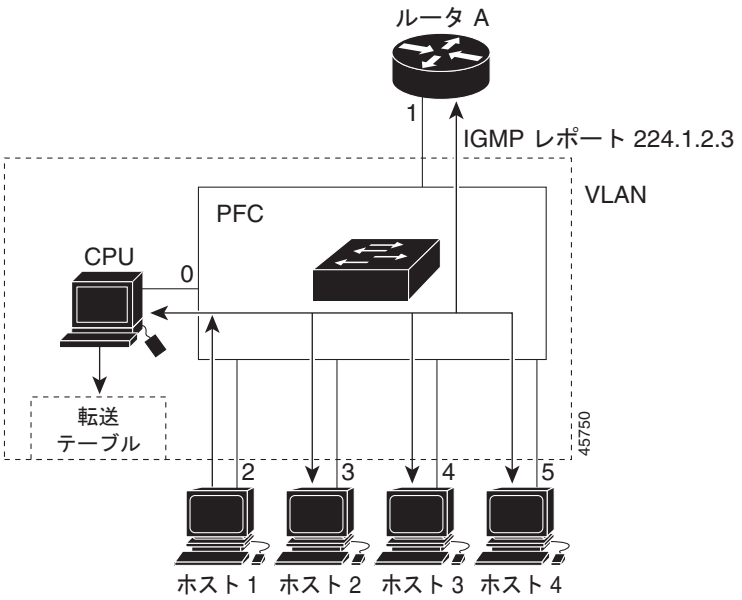
（注）　IGMPv3 の Join メッセージと Leave メッセージは、IGMP フィルタリングまたは MVR を実行中のスイッチにはサポートされません。

IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行中の装置とメッセージを送受信できます。IGMPv3 および IGMP の送信元固有のマルチキャストの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008008048a.html

マルチキャスト グループへの加入

スイッチに接続済みのホストを IP マルチキャスト グループに加入させ、そのグループが IGMP バージョン 2 のクライアントである場合、加入する IP マルチキャスト グループを指定して、非送信請求の IGMP Join メッセージを送信します。または、スイッチがルータから一般的クエリーを受信する場合、クエリーは VLAN 内のすべてのポートに転送されます。マルチキャスト グループに加入する IGMP バージョン 1 またはバージョン 2 のホストは、Join メッセージをスイッチに送信することで応答します。スイッチの CPU は、マルチキャスト転送テーブル エントリがまだ存在しない場合、グループ用にテーブル エントリを作成します。また、CPU は Join メッセージを受信したインターフェイスを、転送テーブル エントリに追加します。そのインターフェイスに関連付けられたホストは、マルチキャスト グループに対応するマルチキャスト トラフィックを受信します。図 28-1 を参照してください。

図 28-1　最初の IGMP Join メッセージ



ルータ A が一般的クエリーをスイッチに送信すると、スイッチがそのクエリーを同じ VLAN の全メンバーのポート 2 ～ 5 に転送します。ホスト 1 をマルチキャスト グループ 224.1.2.3 に加入させ、IGMP メンバーシップ レポート（IGMP Join メッセージ）をグループにマルチキャストします。スイッチの CPU は IGMP レポート内の情報を使用して、転送テーブル エントリ（表 28-1 を参照）を設定します。これにはホスト 1 とルータに接続済みのポート番号が含まれています。

表 28-1　IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2

スイッチのハードウェアは、IGMP 情報パケットをマルチキャスト グループ用の他のパケットと区別できます。テーブルに含まれる情報の指示により、スイッチング エンジンは、224.1.2.3 マルチキャスト IP アドレス宛てにフレームを送信します。このフレームは、グループに加入済みのルータおよびホスト宛ての IGMP パケットではありません。

別のホスト（たとえば、ホスト 4）が、同じグループに対して非送信請求 IGMP Join メッセージを送信する場合（図 28-2 を参照）、そのメッセージを受信した CPU は、ホスト 4 のポート番号を転送テーブルに追加します（表 28-2 を参照）。転送テーブルは CPU だけを IGMP メッセージの宛先に指示するため、メッセージがスイッチ上の他のポートへフラッディングされないことに注意してください。認識されているマルチキャスト トラフィックは、CPU 宛てではなくグループ宛てに転送されます。

図 28-2　2 番めのホストのマルチキャスト グループへの加入

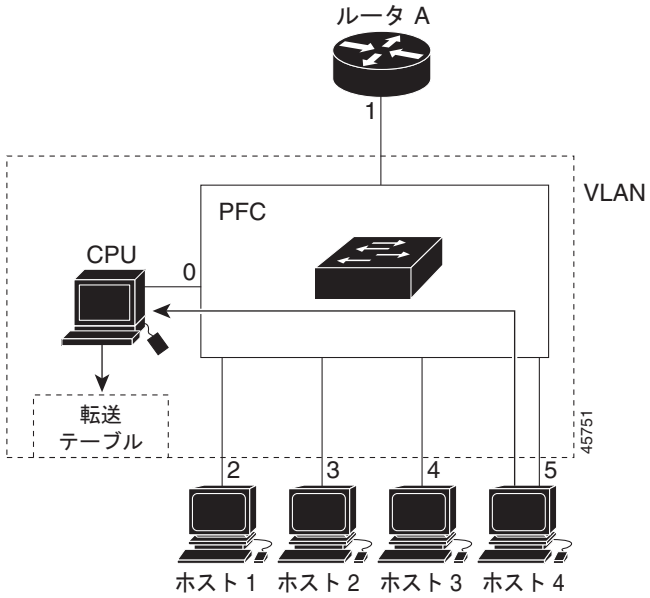


表 28-2　更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

マルチキャスト グループからの脱退

ルータは一般的なマルチキャスト クエリーを定期的に送信し、スイッチはこれらのクエリーを VLAN 内のすべてのポートを経由して転送します。対象ホストがクエリーに応答します。VLAN 内で少なくとも 1 つのホストがマルチキャスト トラフィックを受信する場合、ルータは VLAN へのマルチキャスト トラフィックの転送を続行します。スイッチがマルチキャスト グループ トラフィックを転送するのは、IGMP スヌーピングによって維持される IP マルチキャスト グループの転送テーブルにリストされたホストだけです。

ホストをマルチキャスト グループから脱退させる場合は、暗黙的に脱退するか、または Leave メッセージを送信することができます。スイッチがホストから Leave メッセージを受信すると、グループ固有のクエリーを送信して、そのインターフェイスに接続済みの他の装置が、特定のマルチキャスト グループのトラフィックに関係しているかどうかを学習します。次に、スイッチはその MAC グループの転送テーブルを更新し、グループに対応したマルチキャスト トラフィックの受信に関係するホストだけが転送テーブルにリストされるようになります。ルータが VLAN からレポートを受信しない場合、ルータはその VLAN のグループを IGMP キャッシュから削除します。

即時脱退

即時脱退は IGMP バージョン 2 のホストにだけサポートされます。

スイッチは IGMP スヌーピングの即時脱退を使用して、グループ固有のクエリーをインターフェイスに送信せずに、Leave メッセージを送信するインターフェイスを転送テーブルから削除します。VLAN のインターフェイスは、元の Leave メッセージに指定されたマルチキャスト グループに対するマルチキャスト ツリーからプルーニングされます。即時脱退により、複数のマルチキャスト グループが同時に使用中であっても、スイッチド ネットワーク上のすべてのホストに最適な帯域幅の管理を実現します。

（注）　即時脱退機能は、各ポートにシングル ホストが接続されている VLAN 上でしか使用できません。各ポートに複数のホストが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のホストが偶発的に廃棄される可能性があります。

設定の手順については、「IGMP 即時脱退のイネーブル化」（P.28-11）を参照してください。

IGMP の設定可能な Leave タイマー

ホストが特定のマルチキャスト グループにまだ関係しているかどうかを判断するために、グループ固有のクエリーを送信したあとにスイッチが待機する時間を設定できます。IGMP 脱退の応答時間は、100 ～ 5000 ミリ秒の範囲で設定できます。タイマーはグローバルまたは VLAN 単位のいずれかを設定できます。VLAN 単位で Leave タイムを設定すると、グローバル設定値が上書きされます。

設定の手順については、「IGMP Leave タイマーの設定」（P.28-11）を参照してください。

IGMP レポート抑制

（注）　IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは IGMP レポート抑制を使用して、マルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト装置に転送します。IGMP ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト装置にレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。

マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト装置に転送します。

IGMP レポート抑制をディセーブルにすると、IGMP レポートはすべてマルチキャスト ルータに転送されます。設定の手順については、「IGMP レポート抑制のディセーブル化」（P.28-16）を参照してください。

IGMP スヌーピングの設定

IGMP スヌーピングにより、スイッチは IGMP パケットを調べ、パケットの内容に基づいて転送先を決定できるようになります。ここでは、次の設定情報について説明します。

IGMP スヌーピングのデフォルト設定

表 28-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 28-3　IGMP スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位にイネーブル
マルチキャスト ルータ	設定なし
マルチキャスト ルータの学習（スヌーピング）方式	PIM-DVMRP
IGMP スヌーピングの即時脱退	ディセーブル
スタティック グループ	設定なし
TCN[1] フラッディング クエリー カウント	2
TCN クエリー送信請求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	イネーブル

1. TCN は、トポロジの変更通知のこと

IGMP スヌーピングのイネーブルまたはディセーブル

デフォルトで、スイッチ上の IGMP スヌーピングはグローバルにイネーブルになります。グローバルにイネーブルまたはディセーブルになっている場合、IGMP スヌーピングは既存のすべての VLAN インターフェイスでもイネーブルまたはディセーブルになります。デフォルトで、IGMP スヌーピングはすべての VLAN 上でイネーブルになりますが、VLAN 単位でイネーブルまたはディセーブルにすることができます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングを上書きします。グローバル スヌーピングがディセーブルの場合、VLAN のスヌーピングをイネーブルにできません。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルにすることができます。

スイッチ上で IGMP スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping**	既存のすべての VLAN インターフェイスで、IGMP スヌーピングをグローバルにイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

すべての VLAN インターフェイス上で IGMP スヌーピングをグローバルにディセーブルにするには、**no ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。

VLAN インターフェイス上で IGMP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id*	VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 **（注）** VLAN スヌーピングをイネーブルにするには、IGMP スヌーピングをグローバルにイネーブルにする必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、指定された VLAN 番号に対して **no ip igmp snooping vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

スヌーピング方式の設定

マルチキャスト対応ルータ ポートは、レイヤ 2 のマルチキャスト エントリの転送テーブルに追加されます。次の方式のいずれかにより、スイッチはこのようなポートを学習します。

- IGMP クエリー、Protocol Independent Multicast（PIM）パケット、および Distance Vector Multicast Routing Protocol（DVMRP）パケットのスヌーピング
- 他のルータからの Cisco Group Management Protocol（CGMP）のパケットの待ち受け
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによる、マルチキャスト ルータ ポートへのスタティックな接続

スイッチを設定して、IGMP クエリーおよび PIM/DVMRP パケットをスヌーピングするか、CGMP self-join パケットまたは proxy-join パケットを待ち受けすることができます。デフォルトで、スイッチはすべての VLAN 上の PIM/DVMRP パケットをスヌーピングします。マルチキャスト ルータ ポートを CGMP パケットだけで学習させるには、**ip igmp snooping vlan** *vlan-id* **mrouter learn cgmp** グローバル コンフィギュレーション コマンドを使用します。このコマンドを入力すると、ルータは CGMP self-join パケットおよび CGMP proxy-join パケットだけを待ち受け、他の CGMP パケットを無視します。マルチキャスト ルータ ポートを PIM-DVMRP パケットだけで学習させるには、**ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp** グローバル コンフィギュレーション コマンドを使用します。

（注） 学習方式として CGMP を使用し、VLAN に、CGMP proxy に対応した マルチキャスト ルータが存在しない場合、**ip cgmp router-only** コマンドを入力してルータにダイナミックにアクセスする必要があります。詳細については、第 49 章「IP マルチキャスト ルーティングの設定」を参照してください。

VLAN インターフェイスがマルチキャスト ルータにダイナミックにアクセスする方法を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **mrouter learn** {**cgmp** | **pim-dvmrp**}	VLAN 上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。 マルチキャスト ルータの学習方式を指定します。 • **cgmp**：CGMP パケットを待ち受けます。この方式は制御トラフィックの削減に役立ちます。 • **pim-dvmrp**：IGMP クエリーおよび PIM-DVMRP パケットをスヌーピングします。これはデフォルトです。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの学習方式に戻すには、**no ip igmp snooping vlan** *vlan-id* **mrouter learn cgmp** グローバル コンフィギュレーション コマンドを使用します。

次に、IGMP スヌーピングを設定して CGMP パケットを学習方式として使用する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
```

マルチキャスト ルータ ポートの設定

マルチキャスト ルータ ポートを追加するには（マルチキャスト ルータにスタティックな接続を追加する）、スイッチ上で **ip igmp snooping vlan mrouter** グローバル コンフィギュレーション コマンドを使用します。

（注） マルチキャスト ルータへのスタティックな接続は、スイッチ ポート上でだけサポートされます。

マルチキャスト ルータへのスタティックな接続をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	マルチキャスト ルータの VLAN ID と、マルチキャスト ルータへのインターフェイスを指定します。 • 指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 6 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping mrouter** [**vlan** *vlan-id*]	VLAN インターフェイスで IGMP スヌーピングがイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN からマルチキャスト ルータ ポートを削除するには、**no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト ルータへのスタティックな接続をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/2
Switch(config)# end
```

グループにスタティックに加入するホストの設定

ホストまたはレイヤ 2 ポートは、通常、ダイナミックにマルチキャスト グループに加入しますが、インターフェイス上にホストをスタティックに設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id*	レイヤ 2 ポートをマルチキャスト グループのメンバーとしてスタティックに設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *ip-address* はグループ IP アドレスです。 • *interface-id* は、メンバー ポートです。物理インターフェイスまたはポート チャネル（1 ～ 6）を指定できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping groups**	メンバー ポートおよび IP アドレスを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

マルチキャスト グループからレイヤ 2 ポートを削除するには、**no ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、ポート上でホストをスタティックに設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/1
Switch(config)# end
```

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルにして、ポート上に IGMP バージョン 2 の Leave メッセージが検出された場合、スイッチはすぐにそのポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバーが 1 つだけ存在する場合に限定してください。

（注）　即時脱退は、IGMP バージョン 2 のホストにだけサポートされます。

IGMP 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **immediate-leave**	VLAN インターフェイスで IGMP 即時脱退をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping vlan** *vlan-id*	VLAN インターフェイスで即時脱退がイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN で IGMP 即時脱退をディセーブルにするには、**no ip igmp snooping vlan** *vlan-id* **immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 で IGMP 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

IGMP Leave タイマーの設定

FIGMP Leave タイマーを設定する場合、次の注意事項に従ってください。

- Leave タイムは、グローバルまたは VLAN 単位で設定できます。
- VLAN 上に Leave タイムを設定すると、グローバル設定を上書きします。
- デフォルトの Leave タイムは 1000 ミリ秒です。
- IGMP の設定可能な Leave タイムは、IGMP バージョン 2 を実行しているホスト上だけにサポートされています。
- 通常は、ネットワークにおける脱退の実際の待ち時間が、Leave タイムに設定されます。ただし、Leave タイムは、リアルタイム の CPU 負荷の状態、ネットワークの遅延、およびインターフェイスを経由して送信されるトラフィックの量によって、設定時間の前後に変動する *可能性があります*。

IGMP の設定可能な Leave タイマーをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping last-member-query-interval** *time*	IGMP Leave タイマーをグローバルに設定します。指定できる範囲は 100 ～ 32768 ミリ秒です。デフォルト値は 1000 秒です。
ステップ 3	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time*	（任意）VLAN インターフェイス上に IGMP Leave タイムを設定します。指定できる範囲は 100 ～ 32768 ミリ秒です。 **（注）** VLAN 上に Leave タイムを設定すると、グローバル設定のタイマーを上書きします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping**	（任意）設定された IGMP Leave タイムを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IGMP Leave タイマーをグローバルにデフォルト設定にリセットするには、**no ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

設定済みの IGMP Leave タイム設定を、指定の VLAN から削除するには、**no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

TCN 関連コマンドの設定

ここでは、TCN イベント中にフラッディングされたマルチキャスト トラフィックを制御する方法を示します。

- 「TCN イベント後のマルチキャスト フラッディング時間の制御」（P.28-12）
- 「フラッド モードからの回復」（P.28-13）
- 「TCN イベント中のマルチキャスト フラッディングのディセーブル化」（P.28-14）

TCN イベント後のマルチキャスト フラッディング時間の制御

ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用して、TCN イベントのあとにマルチキャスト トラフィックがフラッディングされる時間を制御できます。このコマンドは、TCN イベント後にフラッディングされたマルチキャスト データ トラフィックに対する一般的クエリーの数を設定します。TCN イベントの例としては、クライアントが位置を変更したときに、レシーバーの存在する同じポートが、以前ブロックされていたが現在は転送中であったり、ポートが Leave メッセージを送信せずにダウンしたりする場合などです。

ip igmp snooping tcn flood query count コマンドを使用して TCN フラッド クエリー カウントを 1 に設定した場合、1 つの一般的クエリーの受信後にフラッディングが停止します。カウントを 7 に設定すると、一般的クエリーを 7 件受信するまでフラッディングが継続します。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

TCN フラッディング クエリー カウントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping tcn flood query count** *count*	マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ～ 10 です。デフォルトでは、フラッディング クエリー カウントは 2 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	TCN 設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フラッディング クエリー カウントをデフォルトに戻すには、**no ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します 。

フラッド モードからの回復

トポロジに変更が発生すると、スパニング ツリー ルートによって、グループ マルチキャスト アドレスを 0.0.0.0. に指定した、特定の IGMP Leave メッセージ（グローバル脱退）が送信されます。ただし、**ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドをイネーブルにすると、スパニング ツリー ルートであるかどうかに関係なく、スイッチがグローバル脱退メッセージを送信します。ルータがこの特定の Leave メッセージを受信すると、すぐに一般的クエリーが送信され、TCN イベント中のフラッド モードからの回復が速やかに処理されます。スイッチがスパニング ツリー ルートである場合、コンフィギュレーション コマンドに関係なく、常に Leave メッセージが送信されます。デフォルトでは、クエリー送信請求はディセーブルです。

スパニング ツリー ルートであるかどうかに関係なく、グローバル脱退メッセージを送信するようにスイッチをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping tcn query solicit**	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。デフォルトでは、クエリー送信請求はディセーブルです。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	TCN 設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

クエリー送信請求をデフォルトに戻すには、**no ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。

TCN イベント中のマルチキャスト フラッディングのディセーブル化

スイッチが TCN を受信すると、一般的クエリーが 2 件受信されるまで、マルチキャスト トラフィックはすべてのポートに対してフラッディングされます。スイッチ内の多数のポートが、異なるマルチキャスト グループに加入している接続ホストを持つ場合、フラッディングがリンクの容量を超過し、パケット損失を招くことがあります。**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用して、この動作を制御できます。

インターフェイス上でマルチキャスト フラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no ip igmp snooping tcn flood**	スパニング ツリーの TCN イベント中に、マルチキャスト トラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャスト フラッディングはイネーブルです。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping**	TCN 設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイス上でマルチキャスト フラッディングを再度イネーブルにするには、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP スヌーピング クエリアの設定

IGMP スヌーピング クエリアを設定する場合は、次の注意事項に従ってください。

- グローバル コンフィギュレーション モードで VLAN を設定します。
- VLAN インターフェイス上に IP アドレスを設定します。イネーブルにすると、IGMP スヌーピング クエリアは、この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上に IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは、IGMP クエリアに設定されたグローバル IP アドレスの使用を試みます。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）の IP アドレスの使用を試みます（存在する場合）。SVI の IP アドレスが存在しない場合、スイッチは、スイッチ上に設定された最初の利用可能な IP アドレスを使用します。最初に利用可能な IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。スイッチ上に利用可能な IP アドレスを検出できない場合、IGMP スヌーピング クエリアは、IGMP の一般的クエリーを生成しません。
- IGMP スヌーピング クエリアは、IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルになっている場合、IGMP スヌーピング クエリアは、ネットワークでマルチキャスト ルータの存在を検出すると、非クエリア ステートに移行します。
- 管理上イネーブルになっている場合、IGMP スヌーピング クエリアは、次の条件に一致すると、動作上のディセーブル ステートに移行します。
  - VLAN で IGMP スヌーピングがディセーブルになっている。
  - 対応する VLAN の SVI 上で PIM がイネーブルになっている。

VLAN の IGMP スヌーピング クエリア機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping querier**	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 3	**ip igmp snooping querier address** *ip_address*	（任意）IGMP スヌーピング クエリアに IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 **（注）** スイッチ上に IP アドレスを検出できない場合、IGMP スヌーピング クエリアは、IGMP の一般的クエリーを生成しません。
ステップ 4	**ip igmp snooping querier query-interval** *interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
ステップ 5	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*]	（任意）トポロジ変更通知（TCN）クエリーの間の時間を設定します。カウントの範囲は 1 ～ 10 です。間隔の範囲は 1 ～ 255 秒です。
ステップ 6	**ip igmp snooping querier timer expiry** *timeout*	（任意）IGMP クエリアが期限切れになるまでの時間の長さを設定します。指定できる範囲は 60 ～ 300 秒です。
ステップ 7	**ip igmp snooping querier version** *version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip igmp snooping vlan** *vlan-id*	（任意）IGMP スヌーピング クエリアが VLAN インターフェイス上でイネーブルになっていることを確認します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

IGMP レポート抑制のディセーブル化

（注）　IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

IGMP レポート抑制はデフォルトでイネーブルになっています。この機能がイネーブルの場合、マルチキャスト ルータ クエリーごとに IGMP レポートが 1 つだけ転送されます。レポート抑制をディセーブルにすると、IGMP レポートはすべてマルチキャスト ルータに転送されます。

IGMP レポート抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ip igmp snooping report-suppression**	IGMP レポート抑制をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	IGMP レポート抑制がディセーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IGMP レポート抑制を再度イネーブルにするには、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。

IGMP スヌーピング情報の表示

ダイナミックに学習された、またはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの IGMP スヌーピング情報を表示できます。IGMP スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

IGMP スヌーピング情報を表示するには、表 28-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 28-4　IGMP スヌーピング情報を表示するためのコマンド

コマンド	目的
show ip igmp snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定した 1 つの VLAN のスヌーピング設定情報を表示します。 （任意）1 つの VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ip igmp snooping groups [**count** |**dynamic** [**count**] | **user** [**count**]]	スイッチまたは特定のパラメータに関するマルチキャスト テーブル情報を表示します。 • **count**：実際のエントリの代わりに、指定のコマンド オプションに関するエントリの合計数を表示します。 • **dynamic**：IGMP スヌーピングによって学習されたエントリを表示します。 • **user**：ユーザ設定のマルチキャスト エントリだけを表示します。
show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user**[**count**]]	マルチキャスト VLAN または VLAN の特定パラメータに関するマルチキャスト テーブル情報を表示します。 • *vlan-id*：VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • **count**：実際のエントリの代わりに、指定のコマンド オプションに関するエントリの合計数を表示します。 • **dynamic**：IGMP スヌーピングによって学習されたエントリを表示します。 • *ip_address*：グループ IP アドレスを指定したマルチキャスト グループの特性を表示します。 • **user**：ユーザ設定のマルチキャスト エントリだけを表示します。
show ip igmp snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習された、または手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。 **（注）** IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスはダイナミックに学習されます。 （任意）1 つの VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。

表 28-4　IGMP スヌーピング情報を表示するためのコマンド （続き）

コマンド	目的
show ip igmp snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した IGMP クエリー メッセージの IP アドレスおよび受信ポートに関する情報を表示します。 （任意）1 つの VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。
show ip igmp snooping querier [**vlan** *vlan-id*] **detail**	VLAN 内で直前に受信した IGMP クエリー メッセージの IP アドレスおよび受信ポートに関する情報と、VLAN 内の IGMP スヌーピング クエリアの設定ステートおよび動作ステートに関する情報を表示します。

これらのコマンドのキーワードとオプションの詳細については、このリリースのコマンド リファレンスを参照してください。

マルチキャスト VLAN レジストレーションの概要

Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）は、イーサネット リングベースのサービス プロバイダー ネットワーク全体に、広範囲なマルチキャスト トラフィックを展開する（たとえば、サービス プロバイダー ネットワーク上で複数のテレビ チャネルをブロードキャストする）アプリケーション向けに設計されています。MVR を使用すると、ポート上の加入者は、ネットワーク全体のマルチキャスト VLAN 上でマルチキャスト ストリームへの加入およびそこからの脱退ができるようになります。また、加入者は個別の VLAN に残りながら、ネットワークで単一のマルチキャスト VLAN を共有することができます。MVR はマルチキャスト VLAN でマルチキャスト ストリームを連続送信する機能を持つと同時に、帯域幅やセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。

MVR は、加入者ポートが、IGMP の Join メッセージと Leave メッセージを送信することにより、これらのマルチキャスト ストリームに加入したりそこから脱退したりすると想定します。これらのメッセージは、IGMP バージョン 2 と互換性のあるホストからイーサネット接続によって送信できます。MVR は IGMP スヌーピングのメカニズムに基づいて動作しますが、2 つの機能は互いに独立して動作します。1 つの機能を、もう一方の動作に影響を与えずにイネーブルまたはディセーブルにすることができます。ただし、IGMP スヌーピングと MVR がどちらもイネーブルの場合、MVR は、MVR に基づいて設定されたマルチキャスト グループからの Join メッセージと Leave メッセージだけに反応します。他のすべてのマルチキャスト グループからの Join メッセージと Leave メッセージは、IGMP スヌーピングによって管理されます。

スイッチの CPU は、MVR IP マルチキャスト ストリームとそれに関連付けられた IP マルチキャスト グループを、スイッチ転送テーブル内で特定します。また、IGMP メッセージを代行受信し、レシーバーが送信元と異なる VLAN に属していても、マルチキャスト ストリームのレシーバーとして加入者を含めるか、または削除するために転送テーブルを変更します。この転送動作により、異なる VLAN 間へのトラフィックの通過が選択的に許可されます。

スイッチは、MVR 動作を互換モードまたはダイナミック モードに設定できます。

- 互換モードの場合、MVR ホストが受信したマルチキャスト データは、ポート上の MVR ホスト メンバーシップに関係なく、すべての MVR データ ポートに転送されます。マルチキャスト データは、IGMP レポートまたは MVR スタティック設定のいずれかにより、MVR ホストが加入しているレシーバー ポートにだけ転送されます。MVR ホストから受信した IGMP レポートは、スイッチで設定された MVR データ ポートから転送されることはありません。

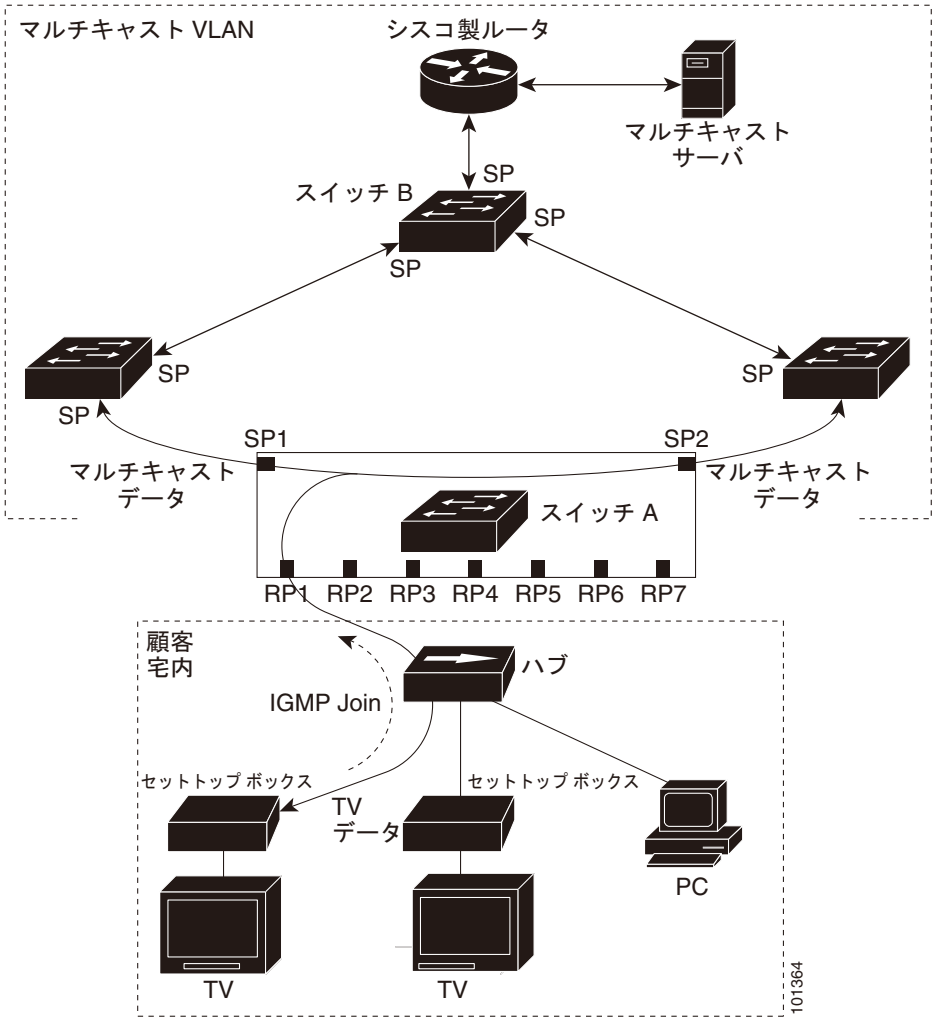
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは MVR スタティック設定のいずれかにより、MVR ホストが加入している MVR データ ポートとクライアント ポートだけから転送されます。MVR ホストから受信したすべての IGMP レポートも、スイッチのすべての MVR データ ポートから転送されます。これにより、MVR データ ポート リンクで不要な帯域幅が使用されなくなります。帯域幅の問題は、スイッチを互換モードで実行すると発生します。

レイヤ 2 ポートだけが MVR に属しています。ポートを MVR のレシーバー ポートとして設定する必要があります。スイッチごとに 1 つの MVR マルチキャスト VLAN だけがサポートされます。

マルチキャスト テレビ アプリケーションでの MVR の使用

マルチキャスト テレビ アプリケーションの場合、セットトップ ボックス搭載の PC またはテレビでマルチキャスト ストリームを受信することができます。複数のセットトップ ボックスまたは PC を、1 つの加入者ポートに接続できます。それには、MVR レシーバー ポートとしてスイッチ ポートを設定します。図 28-3 に設定の例を示します。DHCP は、セットトップ ボックスまたは PC に IP アドレスを割り当てます。加入者がチャネルを選択すると、セットトップ ボックスまたは PC が適切なマルチキャストに加入するように IGMP レポートをスイッチ A に送信します。IGMP レポートが、設定済みの IP マルチキャスト グループ アドレスのいずれかと一致すると、スイッチの CPU はハードウェアのアドレス テーブルを変更し、指定されたマルチキャスト ストリームをマルチキャスト VLAN から受信した場合の転送宛先として、このレシーバー ポートと VLAN をテーブルに含めます。マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートは、MVR 送信元ポートと呼ばれます。

図 28-3　マルチキャスト VLAN レジストレーションの例



加入者がチャネルを変更したり、テレビのスイッチを切ったりした場合、セットトップ ボックスはマルチキャスト ストリームに対する IGMP Leave メッセージを送信します。スイッチの CPU は、MAC ベースの一般的クエリーをレシーバー ポート VLAN を介して送信します。VLAN に別のセットトップ ボックスが存在し、まだこのグループに加入している場合、そのセットトップ ボックスは、クエリーに指定された最大応答時間内に応答する必要があります。CPU が応答を受信しないと、このグループの転送宛先としてそのレシーバー ポートが破棄されます。

即時脱退を使用しない場合、スイッチがレシーバー ポート上の加入者から IGMP Leave メッセージを受信すると、そのポート上で IGMP クエリーを送信し、IGMP グループ メンバーシップ レポートを待機します。設定された時間内にレポートが届かないと、レシーバー ポートがマルチキャスト グループ メンバシップから削除されます。即時脱退を使用すると、IGMP Leave メッセージを受信したレシーバー ポートから IGMP クエリーは送信されません。Leave メッセージの受信後ただちに、マルチキャスト グループ メンバシップからレシーバー ポートが削除されるので、脱退のための待ち時間が短縮されます。即時脱退機能をイネーブルにするのは、レシーバー装置が 1 つだけ接続されたレシーバー ポート上に限定してください。

MVR では、それぞれの VLAN の加入者に、テレビチャネルのマルチキャスト トラフィックを重複させる必要はありません。すべてのチャネルに対するマルチキャスト トラフィックは、マルチキャスト VLAN 上に限定して、VLAN トランクに一度だけ送信されます。IGMP Leave メッセージと Join メッセージは、加入者ポートの割り当て先の VLAN に含まれます。これらのメッセージは、レイヤ 3 装置（スイッチ B）上でマルチキャスト VLAN のマルチキャスト トラフィックのストリームにダイナミックに登録されます。アクセス レイヤ スイッチであるスイッチ A が、トラフィックがマルチキャスト VLAN から異なる VLAN の加入者ポートへ転送されるように転送動作を変更すると、2 つの VLAN 間でトラフィックの通過が選択的に許可されます。

IGMP レポートは、マルチキャスト データと同じ IP マルチキャスト グループのアドレスに送信されます。スイッチ A の CPU は、レシーバー ポートからのすべての IGMP Join メッセージと Leave メッセージをキャプチャし、MVR モードに基づき送信元（アップリンク）ポートのマルチキャスト VLAN に転送する必要があります。

MVR の設定

ここでは、次の設定情報について説明します。

- 「MVR のデフォルト設定」（P.28-21）
- 「MVR 設定時の注意事項および制約事項」（P.28-22）
- 「MVR グローバル パラメータの設定」（P.28-22）
- 「MVR インターフェイスの設定」（P.28-24）

MVR のデフォルト設定

表 28-5 に、MVR のデフォルト設定を示します。

表 28-5　MVR のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位にディセーブル
マルチキャスト アドレス	設定なし
クエリー応答時間	0.5 秒
マルチキャスト VLAN	VLAN 1
モード	互換
インターフェイス（ポート単位）デフォルト	レシーバー ポートと送信元ポートのどちらでもない
即時脱退	すべてのポート上でディセーブル

MVR 設定時の注意事項および制約事項

MVR を設定する場合、次の注意事項に従ってください。

- レシーバー ポートはアクセス ポートだけにしてください。トランク ポートにすることはできません。スイッチのレシーバー ポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。
- スイッチ上に設定できるマルチキャスト エントリ（MVR グループ アドレス）の最大数（つまり、受信可能なテレビ チャネルの最大数）は 256 です。
- 送信元 VLAN で受信された MVR マルチキャスト データがレシーバー ポートから脱退すると、スイッチの Time to Live（TTL）が 1 つ減少します。
- スイッチ上の MVR は、MAC マルチキャスト アドレスではなく IP マルチキャスト アドレスを使用するため、スイッチ上ではエイリアス IP マルチキャスト アドレスが許可されます。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス（224.0.0.xxx 範囲内）を設定する必要はありません。
- プライベート VLAN ポートには MVR を設定しないでください。
- スイッチ上でマルチキャスト ルーティングがイネーブルになっている場合、MVR はサポートされません。MVR がイネーブルになっている状態で、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにすると、MVR はディセーブルになり、警告メッセージが表示されます。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの状態で、MVR をイネーブルにしようとすると、MVR をイネーブルにする動作はキャンセルされ、エラー メッセージが表示されます。
- MVR はスイッチで IGMP スヌーピングと共存できます。
- MVR レシーバー ポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- MVR は IGMPv3 メッセージをサポートしません。

MVR グローバル パラメータの設定

デフォルト設定の使用を選択する場合、任意の MVR パラメータを設定する必要はありません。デフォルトのパラメータを変更する場合（MVR VLAN を除く）、最初に MVR をイネーブルにする必要があります。

（注）　この項で使用しているコマンドの構文と使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

MVR パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルにします。

	コマンド	目的
ステップ 3	**mvr group** *ip-address* [*count*]	スイッチ上に IP マルチキャスト アドレスを設定するか、*count* パラメータ（*count* の範囲は 1 ～ 256 で、デフォルト値は 1）を使用して、一連の連続 MVR グループ アドレスを設定します。このアドレスに送信されるすべてのマルチキャスト データは、スイッチ上のすべての送信元ポートと、そのマルチキャスト アドレスでデータを受信するように選択されたすべてのレシーバー ポートに送信されます。各マルチキャスト アドレスは、1 つのテレビ チャネルに対応します。
ステップ 4	**mvr querytime** *value*	（任意）マルチキャスト グループ メンバーシップからポートを削除する前に、レシーバー ポート上で IGMP レポート メンバーシップを待機する最大時間を定義します。この値は 10 分の 1 秒単位です。指定できる範囲は 1 ～ 100 です。デフォルトは 5/10 秒つまり 1/2 秒です。
ステップ 5	**mvr vlan** *vlan-id*	（任意）マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートがこの VLAN に属している必要があります。VLAN の範囲は 1 ～ 1001 および 1006 ～ 4094 です。デフォルトは VLAN 1 です。
ステップ 6	**mvr mode** {**dynamic** | **compatible**}	（任意）MVR の動作モードを指定します。 • **dynamic**：送信元ポート上でダイナミック MVR メンバーシップが使用できるようになります。 • **compatible**：Catalyst 3500 XL および Catalyst 2900 XL スイッチと互換性があり、送信元ポートで IGMP ダイナミック加入をサポートしません。 デフォルトは **compatible** モードです。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show mvr** or **show mvr members**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no mvr** [**mode** | **group** *ip-address* | **querytime** | **vlan**] グローバル コンフィギュレーション コマンドを使用します。

次に、MVR をイネーブルにし、グループ アドレスを設定し、クエリー時間を 1 秒（10/10 秒）に設定し、MVR マルチキャスト VLAN を VLAN 22 に指定し、MVR モードをダイナミックに設定する例を示します。

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(config)# end
```

show mvr members 特権 EXEC コマンドを使用して、スイッチ上の MVR マルチキャスト グループ アドレスを確認できます。

MVR インターフェイスの設定

レイヤ 2 MVR インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルにします。
ステップ 3	**interface** *interface-id*	設定するレイヤ 2 ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**mvr type** {**source** | **receiver**}	MVR ポートを次のいずれかに設定します。 • **source**：マルチキャスト データを送受信するアップリンク ポートを、送信元ポートとして設定します。加入者は、送信元ポートに直接接続できません。スイッチ上のすべての送信元ポートは、単一のマルチキャスト VLAN に属します。 • **receiver**：ポートが加入者ポートで、マルチキャスト データの受信だけを行う場合は、ポートをレシーバー ポートとして設定します。スタティックに、または IGMP の Leave メッセージまたは Join メッセージによってポートがマルチキャスト グループのメンバーにならない限り、データは受信されません。レシーバー ポートはマルチキャスト VLAN に属することはできません。 デフォルト設定は、非 MVR ポートです。MVR 特性を使用して非 MVR ポートの設定を試行すると、動作が失敗します。
ステップ 5	**mvr vlan** *vlan-id* **group** [*ip-address*]	（任意）マルチキャスト VLAN と IP マルチキャスト アドレスに送信されるマルチキャスト トラフィックを受信するように、ポートをスタティックに設定します。グループのメンバーとしてスタティックに設定されたポートは、スタティックに削除されるまではそのグループのメンバーのままです。 **（注）** 互換モードの場合、このコマンドはレシーバー ポートにだけ適用されます。ダイナミック モードの場合、このコマンドはレシーバー ポートと送信元ポートに適用されます。 レシーバー ポートは、IGMP の Join メッセージと Leave メッセージを使用して、ダイナミックにマルチキャスト グループに加入することもできます。
ステップ 6	**mvr immediate**	（任意）ポートの MVR の即時脱退機能をイネーブルにします。 **（注）** このコマンドはレシーバー ポートにだけ適用され、レシーバー装置が 1 つだけ接続されたレシーバー ポートに限定してイネーブルにしてください。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show mvr** **show mvr interface** または **show mvr members**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスをデフォルト設定に戻すには、**no mvr** [**type** | **immediate** | **vlan** *vlan-id* | **group**] インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをレシーバー ポートとして設定し、マルチキャスト グループ アドレスに送信されるマルチキャスト トラフィックを受信するようにポートをスタティックに設定し、ポート上で即時脱退を設定し、結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config)# end
Switch# show mvr interface
Port    Type        Status          Immediate Leave
----    ----        -------         ---------------
Gi1/2   RECEIVER    ACTIVE/DOWN     ENABLED
```

MVR 情報の表示

スイッチまたは指定されたインターフェイスの MVR 情報を表示できます。MVR 設定を表示するには、特権 EXEC モードで表 28-6 に示すコマンドを使用します。

表 28-6　MVR 情報を表示するためのコマンド

コマンド	目的
show mvr	スイッチの MVR ステータスと値を表示します。MVR がイネーブルかディセーブルであるかに関係なく、マルチキャスト VLAN、マルチキャスト グループの最大値（256）および現在値（0 ～ 256）、クエリー応答時間、および MVR モードを表示します。
show mvr interface [*interface-id*] [**members** [**vlan** *vlan-id*]]	すべての MVR インターフェイスとその MVR 設定を表示します。 特定のインターフェイスを入力すると、この情報が表示されます。 • タイプ：レシーバーまたは送信元 • ステータス：次のいずれかになります。 – ACTIVE は、ポートが VLAN に含まれていることを意味します。 – UP/DOWN は、ポートが転送中か転送中でないかを示します。 – INACTIVE は、ポートが VLAN に含まれていないことを意味します。 • 即時脱退：イネーブルまたはディセーブル **members** キーワードを入力すると、このポート上のすべてのマルチキャスト グループ メンバーが表示され、VLAN ID を入力すると、VLAN 上のすべてのマルチキャスト グループ メンバーが表示されます。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show mvr members [*ip-address*]	任意の IP マルチキャスト グループのメンバーであるすべてのレシーバー ポートと送信元ポート、または指定 IP マルチキャスト グループの IP アドレスを表示します。

IGMP フィルタリング/スロットリングの設定

たとえば、首都圏または Multiple-Dwelling Unit（MDU; 集合住宅）での設置など、環境によっては、スイッチ ポート上のユーザが所属できるマルチキャスト グループのセットを制御する場合があります。加入またはサービス プランのタイプに基づき、IP/TV など、マルチキャスト サービスの分散を制御できます。スイッチ ポート上のユーザが所属できるマルチキャスト グループの数を制限する場合もあります。

IGMP フィルタリング機能を使用すると、IP マルチキャスト プロファイルを設定して個別のスイッチ ポートに関連付けることで、ポート単位でマルチキャスト加入をフィルタリングできます。1 つの IGMP プロファイルには 1 つまたは複数のマルチキャスト グループを含めることができます。また、IGMP プロファイルは、グループへのアクセスを許可するか拒否するかを指定します。IGMP プロファイルのマルチキャスト グループへのアクセス拒否がスイッチ ポートに適用されると、IP マルチキャスト トラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループから IP マルチキャスト トラフィックを受信できなくなります。フィルタリング アクションによってマルチキャスト グループへのアクセスが許可されると、ポートからの IGMP レポートは転送されて通常に処理されます。レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定することもできます。

IGMP フィルタリングは、Join レポートや Leave レポートなど、グループ固有のクエリーとメンバーシップ レポートだけを制御します。一般的な IGMP クエリーは制御しません。IGMP フィルタリングは、IP マルチキャスト トラフィックの転送を指示する機能とは関連していません。フィルタリング機能は、マルチキャスト トラフィックの転送に CGMP または MVR が使用されていても同様に動作します。

IGMP フィルタリングが適用可能なのは、IP マルチキャスト グループ アドレスのダイナミックな学習だけで、スタティックな設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定されて、IGMP スヌーピング転送テーブルに最大数のエントリが含まれ、インターフェイスが IGMP Join レポートを受信した場合、IGMP ポートを廃棄するか、ランダムに選択したマルチキャスト エントリを受信済みの IGMP レポートで置き換えるように、インターフェイスを設定できます。

（注）　IGMPv3 の Join メッセージと Leave メッセージは、IGMP フィルタリングを実行中のスイッチにはサポートされません。

ここでは、次の設定情報について説明します。

- 「IGMP フィルタリング/スロットリングのデフォルト設定」（P.28-27）
- 「IGMP プロファイルの設定」（P.28-27）（任意）
- 「IGMP プロファイルの適用」（P.28-28）（任意）
- 「IGMP グループの最大数の設定」（P.28-29）（任意）
- 「IGMP スロットリング アクションの設定」（P.28-30）（任意）

IGMP フィルタリング/スロットリングのデフォルト設定

表 28-7 に、IGMP フィルタリングのデフォルト設定を示します。

表 28-7　IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用なし
IGMP グループの IGMP 最大数	最大値の設定なし
IGMP プロファイル	定義なし
IGMP プロファイル アクション	アドレス範囲の拒否

転送テーブル内に最大数のグループが含まれる場合、デフォルトの IGMP スロットリング アクションにより IGMP レポートが拒否されます。設定の注意事項については、「IGMP スロットリング アクションの設定」（P.28-30）を参照してください。

IGMP プロファイルの設定

IGMP プロファイルを設定するには、**ip igmp profile** グローバル コンフィギュレーション コマンドをプロファイル番号とともに使用して IGMP プロファイルを作成し、IGMP プロファイル コンフィギュレーション モードを開始します。このモードで、IGMP プロファイルのパラメータを指定し、ポートからの IGMP Join 要求をフィルタリングするために使用できます。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- **deny**：一致するアドレスを拒否します（デフォルト設定）。
- **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、デフォルト設定に戻します。
- **permit**：一致するアドレスを許可します。
- **range**：プロファイルに対する IP アドレスの範囲を指定します。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。

デフォルトでは、スイッチには IGMP プロファイルが設定されません。プロファイルの設定の際に、**permit** または **deny** キーワードのいずれも含まれない場合、デフォルトで IP アドレスの範囲へのアクセスが拒否されます。

IGMP プロファイルを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp profile** *profile number*	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。プロファイル番号の範囲は、1 ～ 4294967295 です。
ステップ 3	**permit** | **deny**	（任意）IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションが設定されない場合、プロファイルはデフォルトでアクセスを拒否します。

	コマンド	目的
ステップ 4	**range** *ip multicast address*	アクセスが制御される IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力する場合、低い方の IP マルチキャスト アドレスを入力してからスペースを入力し、次に高い方の IP マルチキャスト アドレスを入力します。 **range** コマンドを数回使用して、複数のアドレスまたはアドレスの範囲を入力できます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp profile** *profile number*	プロファイル設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

プロファイルを削除するには、**no ip igmp profile** *profile number* グローバル コンフィギュレーション コマンドを使用します。

IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を削除するには、**no range** *ip multicast address* IGMP プロファイル コンフィギュレーション コマンドを使用します。

次に、単一の IP マルチキャスト アドレスへのアクセスを許可する IGMP プロファイル 4 を作成し、設定を確認する例を示します。アクションがアクセス拒否（デフォルト）の場合、**show ip igmp profile** の出力に表示されません。

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

IGMP プロファイルの適用

IGMP プロファイルに定義されたアクセスを制御するには、**ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用してプロファイルを適切なインターフェイスに適用します。IGMP プロファイルはレイヤ 2 アクセス ポートにだけ適用できます。IGMP プロファイルをルーテッド ポートまたは SVI に適用することはできません。EtherChannel ポート グループに属するポートには、プロファイルを適用できません。プロファイルは複数のインターフェイスに適用できますが、各インターフェイスには 1 つのプロファイルしか適用できません。

IGMP プロファイルをスイッチ ポートに適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに属さないレイヤ 2 ポートにする必要があります。
ステップ 3	**ip igmp filter** *profile number*	指定した IGMP プロファイルをインターフェイスに適用します。指定できる範囲は 1 ～ 4294967295 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスからプロファイルを削除するには、**no ip igmp filter** *profile number* インターフェイス コンフィギュレーション コマンドを使用します。

次に、IGMP プロファイル 4 をポートに適用する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

IGMP グループの最大数の設定

ip igmp max-groups インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定できます。最大値をデフォルトの no limit に戻すには、このコマンドの **no** 形式を使用します。

この制限はレイヤ 2 ポートにだけ適用されます。ルーテッド ポートまたは SVI 上には IGMP グループの最大数を設定することはできません。このコマンドは論理 EtherChannel インターフェイス上でも使用できますが、EtherChannel ポート グループに属するポートには使用できません。

転送テーブル内の IGMP グループの最大数を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel グループに属さないレイヤ 2 ポート、または EtherChannel インターフェイスにすることができます。
ステップ 3	**ip igmp max-groups** *number*	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ～ 4294967294 です。デフォルトでは最大数は設定されていません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

最大グループ制限を削除して、最大数が指定されないデフォルトに戻すには、**no ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

IGMP スロットリング アクションの設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定したあとに、**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドを使用して、既存グループを IGMP レポートを受信した新しいグループに置き換えるようにインターフェイスを設定できます。IGMP Join レポートを廃棄するデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

IGMP スロットリング アクションを設定する場合には、次の注意事項に従ってください。

- この制約は、レイヤ 2 ポートにだけ適用できます。このコマンドは論理 EtherChannel インターフェイス上で使用できますが、EtherChannel ポート グループに属するポートには使用できません。
- 最大グループ制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action** {**deny** | **replace**} コマンドを入力しても無効です。
- インターフェイスがマルチキャスト エントリを転送テーブルに追加したあとに、スロットリング アクションを設定して最大グループ制限を設定する場合、スロットリング アクションに応じて、転送テーブルのエントリは期限切れになるか、削除されます。
  - スロットリング アクションを **deny** に設定すると、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れて、最大数のエントリが転送テーブルにある場合、スイッチは、インターフェイス上で受信された次の IGMP レポートを廃棄します。
  - スロットリング アクションを **replace** に設定すると、以前転送テーブルにあったエントリが削除されます。最大数のエントリが転送テーブルにある場合、スイッチはランダムに選択したエントリを、受信した IGMP レポートと置き換えます。

  スイッチによって転送テーブルのエントリが削除されないように、インターフェイスがエントリを転送テーブルに追加する前に、IGMP スロットリング アクションを設定できます。

転送テーブルに最大数のエントリが含まれる場合のスロットリング アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel グループに属さないレイヤ 2 ポート、または EtherChannel インターフェイスにすることができます。このインターフェイスはトランク ポートにはできません。
ステップ 3	**ip igmp max-groups action** {**deny** | **replace**}	インターフェイスが IGMP レポートを受信し、転送テーブルに最大数のエントリが含まれる場合、インターフェイスが行うアクションを指定します。 • **deny**：レポートを廃棄します。 • **replace**：既存グループを IGMP レポートを受信した新しいグループと置き換えます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

レポートを廃棄するデフォルト動作に戻すには、**no ip igmp max-groups action** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP フィルタリング/スロットリング設定の表示

IGMP プロファイルの特性を表示し、スイッチ上のすべてのインターフェイスまたは指定したインターフェイスの IGMP プロファイルと最大グループ設定を表示できます。また、スイッチ上のすべてのインターフェイスまたは指定したインターフェイスに対する IGMP スロットリング設定を表示できます。

IGMP フィルタリング/スロットリング設定を表示するには、表 28-8 に示す各特権 EXEC コマンドを使用します。

表 28-8　IGMP フィルタリング/スロットリング設定を表示するためのコマンド

コマンド	目的
show ip igmp profile [*profile number*]	指定した IGMP プロファイルまたはスイッチ上に定義されたすべての IGMP プロファイルを表示します。
show running-config [**interface** *interface-id*]	インターフェイスが所属できる IGMP グループの最大数やインターフェイスに適用される IGMP プロファイル（設定されている場合）など、指定したインターフェイスの設定またはスイッチ上のすべてのインターフェイスの設定を表示します。

CHAPTER 29

ポートベースのトラフィック制御の設定

この章では、IE 3000 スイッチにポートベースのトラフィック制御機能を設定する手順について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

ストーム制御の設定

ここでは、次の概要と設定情報について説明します。

ストーム制御の概要

ストーム制御は、LAN 上のトラフィックが、いずれかの物理インターフェイスのブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防ぎます。LAN ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。プロトコルスタック実装のエラー、ネットワーク設定の誤り、またはユーザによる DoS 攻撃（サービス拒絶攻撃）の開始がストームの原因になります。

ストーム制御（またはトラフィック抑制）は、インターフェイスからスイッチング バスに送信されるパケットをモニタし、パケットがユニキャスト、マルチキャスト、ブロードキャストのいずれであるかを判断します。スイッチは、1 秒間隔で受信される特定タイプのパケット数をカウントし、あらかじめ定義された抑制レベル スレッシュホールドと測定値を比較します。

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

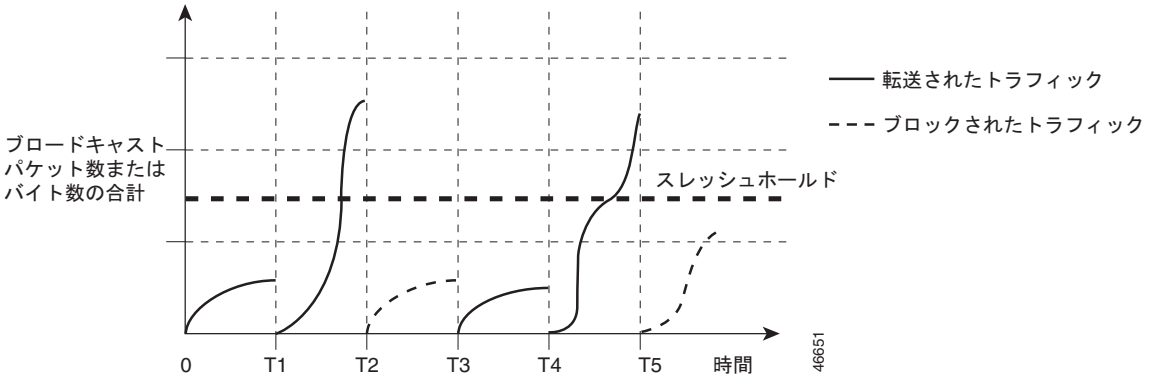
- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックで利用可能なポートの全帯域幅のパーセンテージ）。
- トラフィック レート（ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるときの 1 秒あたりのパケット数）。
- トラフィック レート（ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるときの 1 秒あたりのビット数）。
- トラフィック レート（1 秒あたりのパケット数、小さいフレームの場合）。この機能は、グローバルにイネーブルになっています。小さいフレームのスレッシュホールドは、それぞれのインターフェイスで設定されます。

いずれの方法も、上限のスレッシュホールドに到達するとポートがトラフィックをブロックします。トラフィック レートが下限のスレッシュホールド（指定されている場合）を下回るまでポートはブロックされたままになり、下回ると通常の転送が再開されます。下限抑制レベルが指定されていない場合、スイッチはトラフィック レートが上限抑制レベルを下回るまですべてのトラフィックをブロックします。一般的に、抑制レベルが高くなると、ブロードキャスト ストームに対する保護の効果が薄くなります。

（注） マルチキャスト トラフィックのストーム制御スレッシュホールドに達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどのコントロール トラフィック以外のマルチキャスト トラフィックすべてがブロックされます。ただし、スイッチは、Open Shortest Path First（OSPF）および通常のマルチキャスト データ トラフィック間のように、ルーティング アップデート間を区別しないため、両方のトラフィックがブロックされます。

図 29-1 のグラフは、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。この例は、マルチキャストおよびユニキャスト トラフィックにも適用できます。この例では、転送されているブロードキャスト トラフィックが、T1 ～ T2 間および T4 ～ T5 間の時間間隔で設定されたスレッシュホールドを上回っています。特定のトラフィックの量がスレッシュホールドを上回ると、そのタイプのすべてのトラフィックは、次の一定時間にわたり廃棄されます。したがって、ブロードキャスト トラフィックは T2 および T5 のあとの時間間隔ではブロックされています。次の時間間隔（たとえば T3）では、ブロードキャスト トラフィックがスレッシュホールドを上回らなければ、再度転送されます。

図 29-1　ブロードキャスト ストーム制御の例



ストーム制御抑制レベルと 1 秒の時間間隔の組み合わせにより、ストーム制御アルゴリズムの動作を制御します。スレッシュホールドが高くなると、より多くのパケットを通過させることができます。スレッシュホールドの値が 100% であれば、トラフィックに対する制限はありません。0.0 の値は、ポート上のすべてのブロードキャスト、マルチキャスト、ユニキャスト トラフィックをブロックします。

（注）　パケットは一定間隔で着信しないので、トラフィック アクティビティを 1 秒間隔で測定することは、トラフィック ストーム制御の動作に影響する可能性があります。

各トラフィック タイプのスレッシュホールドの値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御のデフォルト設定

デフォルトでは、スイッチ インターフェイスでユニキャスト、ブロードキャスト、およびマルチキャスト ストーム制御はディセーブルになっています（抑制レベルは 100% です）。

ストーム制御およびスレッシュホールド レベルの設定

ポートでストーム制御を設定し、特定タイプのトラフィックで使用するスレッシュホールド レベルを入力します。

ただし、ハードウェアの制約や、さまざまなサイズのパケットがカウントされる動作のため、スレッシュホールドのパーセンテージには誤差が生じます。着信トラフィックを構成するパケットのサイズにより、実際に適用されるスレッシュホールドは、設定レベルと数 % 程度異なる場合があります。

（注）　ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御およびスレッシュホールド レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}	ブロードキャスト、マルチキャスト、ユニキャストのいずれかのストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルです。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャストの上限スレッシュホールド レベルを帯域幅のパーセンテージ（小数点以下第 2 位まで）で指定します。上限スレッシュホールドに達すると、ポートではトラフィックがブロックされます。指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、下限スレッシュホールド レベルを帯域幅のパーセンテージ（小数点以下第 2 位まで）で指定します。この値は、上限抑制値より小さいまたは等しい必要があります。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ～ 100.00 です。 スレッシュホールドを最大値（100%）に設定すると、トラフィックは制限されません。スレッシュホールドを 0.0 に設定すると、ブロードキャスト、マルチキャスト、ユニキャストのすべてのトラフィックがそのポートでブロックされます。 • **bps** *bps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィック用に上限スレッシュホールド レベルを 1 秒あたりのビット数単位（小数点以下第 1 位まで）で指定します。上限スレッシュホールドに達すると、ポートではトラフィックがブロックされます。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限スレッシュホールド レベルを 1 秒あたりのビット数単位（小数点以下第 1 位まで）で指定します。上限スレッシュホールド レベル以下にしてください。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。指定できる範囲は 0.0 ～ 10000000000.0 です。 • **pps** *pps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィック用に上限スレッシュホールド レベルを 1 秒あたりのパケット数単位（小数点以下第 1 位まで）で指定します。上限スレッシュホールドに達すると、ポートではトラフィックがブロックされます。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限スレッシュホールド レベルを 1 秒あたりのパケット数単位（小数点以下第 1 位まで）で指定します。上限スレッシュホールド レベル以下にしてください。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。指定できる範囲は **0.0** ～ 10000000000.0 です。 BPS 設定および PPS 設定には、スレッシュホールド値が大きくなる場合、k、m、g などのメトリック サフィクスを使用できます。
ステップ 4	**storm-control action** {**shutdown** | **trap**}	ストームが検出されたときのアクションを指定します。デフォルトでは、トラフィックをフィルタリングし、トラップを送信しません。 • ストーム中にポートを errdisable にするには、**shutdown** キーワードを選択します。 • ストームが検出されたときに SNMP トラップを生成するには、**trap** キーワードを選択します。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]	指定したトラフィック タイプについてインターフェイスに設定したストーム制御抑制レベルを確認します。トラフィック タイプを指定しない場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ストーム制御をディセーブルにするには、**no storm-control** {**broadcast** | **multicast** | **unicast**} **level** インターフェイス コンフィギュレーション コマンドを使用します。

次に、87% の上限抑制レベルと 65% の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# storm-control unicast level 87 65
```

次に、ポートのブロードキャスト アドレス ストーム制御を 20% のレベルでイネーブルにする例を示します。トラフィック ストーム制御インターバルで、ブロードキャスト トラフィックがポートの利用可能な全帯域幅の 20% という設定レベルを超えると、トラフィックストーム制御インターバルが終了するまでスイッチはすべてのブロードキャスト トラフィックを廃棄します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# storm-control broadcast level 20
```

小さいフレームの着信レートの設定

着信 VLAN タグ付きパケットが 67 バイト以下のときは、*小さいフレーム*と見なされます。小さいフレームはスイッチによって転送されますが、スイッチのストーム制御カウンタは増分されません。Cisco IOS Release 12.2(44)SE 以降では、小さいフレームが指定のレート（スレッシュホールド）で着信する場合、ポートを errdisable にできます。

小さいフレームの着信機能をスイッチ上でグローバルにイネーブルにし、各インターフェイスで小さいフレームのスレッシュホールド（パケット数）を設定します。パケットが最小サイズよりも小さく、指定のレート（スレッシュホールド）で着信する場合、ポートが errdisable なので、パケットは廃棄されます。

errdisable recovery cause small-frame グローバル コンフィギュレーション コマンドを入力すると、指定の時間が経過した時点で、ポートが再びイネーブルになります（**errdisable recovery** グローバル コンフィギュレーション コマンドを使用して回復時間を指定します）。

各インターフェイスのスレッシュホールド レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause small-frame**	小さいフレームの着信レート機能をスイッチ上でイネーブルにします。
ステップ 3	**errdisable recovery interval** *interval*	（任意）指定された errdisable ステートから回復する時間を指定します。

	コマンド	目的
ステップ 4	**errdisable recovery cause small-frame**	（任意）小さいフレームの着信によりポートが errdisable になったあと、ポートが自動的に再びイネーブルになる回復時間を設定します。
ステップ 5	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 6	**small violation-rate** *pps*	インターフェイスが着信パケットを廃棄するスレッシュホールド レートを設定し、ポートを errdisable にします。指定できる範囲は 1 ～ 10,000 pps（パケット/秒）です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** *interface-id*	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、小さいフレームの着信レート機能をイネーブルにする例、ポート 回復時間を設定する例、およびポートが errdisable になるスレッシュホールドを設定する例を示します。

```
Switch# configure terminal
Switch# errdisable detect cause small-frame
Switch# errdisable recovery cause small-frame
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# small-frame violation rate 10000
Switch(config-if)# end
```

保護ポートの設定

一部のアプリケーションでは、同一スイッチ上のポート間でトラフィックがレイヤ 2 で転送されないようにすることにより、あるネイバーによって生成されたトラフィックを別のネイバーが認識しないようにする必要があります。このような環境では、保護ポートを使用すれば、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換は行われません。

保護ポートには次のような機能があります。

- 保護ポートは、他の保護ポートにユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、PIM パケットなどの制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックはレイヤ 3 装置を介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおり行われます。

ここでは、次の設定情報について説明します。

- 「保護ポートのデフォルト設定」（P.29-6）
- 「保護ポートの設定時の注意事項」（P.29-7）
- 「保護ポートの設定」（P.29-7）

保護ポートのデフォルト設定

デフォルトでは、保護ポートが定義されていません。

保護ポートの設定時の注意事項

保護ポートは、物理インターフェイス（ギガビット イーサネット ポート 1 など）または EtherChannel グループ（ポートチャネル 5 など）のいずれにも設定できます。特定のポート チャネルについて保護ポートをイネーブルにすると、ポートチャネル グループ内の全ポートで保護ポートがイネーブルになります。

プライベート VLAN ポートを保護ポートとして設定しないでください。保護ポートをプライベート VLAN ポートとして設定しないでください。プライベート VLAN の独立ポートは、他の独立ポートやコミュニティ ポートにトラフィックを転送しません。プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」を参照してください。

保護ポートの設定

ポートを保護ポートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport protected**	インターフェイスを保護ポートとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

保護ポートをディセーブルにするには、**no switchport protected** インターフェイス コンフィギュレーション コマンドを使用します。

次に、保護ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

ポート ブロッキングの設定

デフォルトでは、スイッチは、宛先 MAC アドレスが不明なパケットをすべてのポートからフラッディングします。不明なユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上の問題が発生することがあります。不明なユニキャストまたはマルチキャスト トラフィックがポート間で転送されないようにするため、不明なユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにポート（保護ポートまたは非保護ポート）をブロックできます。

（注）　ポート ブロッキング機能はピュア レイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 情報を持つマルチキャスト パケットは、ブロックされません。

ここでは、次の設定情報について説明します。

ポート ブロッキングのデフォルト設定

デフォルトでは、ポートから送信される不明なマルチキャストおよびユニキャスト トラフィックのフラッディングはブロックされませんが、これらのパケットは、すべてのポートにフラッディングされます。

インターフェイスでのフラッディング トラフィックのブロック

（注）　このインターフェイスには物理インターフェイスまたは EtherChannel グループを指定できます。特定のポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポートチャネル グループ内の全ポートでブロックされます。

インターフェイスから送信されるユニキャスト パケットおよびレイヤ 2 マルチキャスト パケットのフラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport block multicast**	ポートからの不明なマルチキャストの転送をブロックします。 （注）　ピュア レイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 情報を持つマルチキャスト パケットは、ブロックされません。
ステップ 4	**switchport block unicast**	ポートからの不明なユニキャストの転送をブロックします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

トラフィックがブロックされずに、ポート上で通常転送が行われるデフォルト状態にインターフェイスを戻すには、**no switchport block** {**multicast** | **unicast**} インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上でユニキャストおよびレイヤ 2 マルチキャスト フラッディングをブロックする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

ポート セキュリティの設定

ポート セキュリティ機能を使用すると、ポートへのアクセスが許可されたステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは、定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレスの数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されているワークステーションでは、ポートの全帯域幅が保証されます。

セキュア ポートとして設定されたポートのセキュア MAC アドレスが最大数に達した場合に、ポートにアクセスしようとするステーションの MAC アドレスが、識別されたどのセキュア MAC アドレスとも異なるときは、セキュリティ違反が発生します。また、あるセキュア ポートで設定または学習されたセキュア MAC アドレスを持つステーションが別のセキュア ポートにアクセスしようとすると、違反のフラグが立てられます。

ここでは、次の概要と設定情報について説明します。

ポート セキュリティの概要

ここでは、次の概念情報について説明します。

セキュア MAC アドレス

1 つのポートで許可されるセキュア アドレスの最大数を設定するには、**switchport port-security maximum** *value* インターフェイス コンフィギュレーション コマンドを使用します。

（注）　インターフェイスにすでに設定されているセキュア アドレス数よりも小さい値を最大値に設定しようとすると、コマンドは拒否されます。

スイッチは、次のタイプのセキュア MAC アドレスをサポートします。

- スタティック セキュア MAC アドレス：**switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して手動で設定されます。これらはアドレス テーブルに格納され、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス：ダイナミックに設定されます。これらはアドレス テーブルだけに格納され、スイッチが再起動したときに削除されます。
- スティッキ セキュア MAC アドレス：ダイナミックに学習されるか、または手動で設定されます。これらはアドレス テーブルに格納され、実行コンフィギュレーションに追加されます。これらのアドレスがコンフィギュレーション ファイルに保存されている場合は、スイッチが再起動するときに、インターフェイスはアドレスをダイナミックに再設定しなくてすみます。

*スティッキ ラーニング*をイネーブルにすると、ダイナミック MAC アドレスをスティッキ セキュア MAC アドレスに変換し、それらを実行コンフィギュレーションに追加するように、インターフェイスを設定できます。スティッキ ラーニングをイネーブルにするには、**switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、インターフェイスは、すべてのダイナミック セキュア MAC アドレス（スティッキ ラーニングがイネーブルになる前にダイナミックに学習されたアドレスを含む）をスティッキ セキュア MAC アドレスに変換します。すべてのスティッキ セキュア MAC アドレスが、実行コンフィギュレーションに追加されます。

スティッキ セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチの再起動時に使用されるスタートアップ コンフィギュレーション）に自動的に格納されません。スティッキ セキュア MAC アドレスがコンフィギュレーション ファイルに保存されている場合は、スイッチが再起動するときに、インターフェイスはこれらのアドレスを再学習しなくてすみます。スティッキ セキュア アドレスが保存されていない場合は、アドレスは失われます。

スティッキ ラーニングをディセーブルにした場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

スイッチに設定できるセキュア MAC アドレスの最大数は、システムで使用が許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management（SDM）テンプレートによって決められます。第 10 章「SDM テンプレートの設定」を参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数です。

セキュリティ違反

セキュリティ違反とは、次のいずれかの状況が発生したときです。

- セキュア MAC アドレスが最大数までアドレス テーブルに追加され、アドレス テーブルにない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同じ VLAN 内の別のセキュア インターフェイスで認識された場合。

違反発生時の対処方法に関して、次の 4 つの違反モードのいずれかにインターフェイスを設定できます。

- protect：セキュア MAC アドレス数がポートで許可されている最大制限に到達した場合、不明な送信元アドレスのパケットは廃棄されます。十分な数のセキュア MAC アドレスを削除して最大値以下にするか、許可するアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。

（注） トランク ポート上で protect 違反モードを設定することは推奨できません。protect モードでは、ポートが最大制限に達していなくても、VLAN が最大制限に達するとラーニングがディセーブルになります。

- restrict：セキュア MAC アドレス数がポートで許可されている最大制限に到達した場合、不明な送信元アドレスのパケットは廃棄されます。十分な数のセキュア MAC アドレスを削除して最大値以下にするか、許可するアドレスの最大数を増やさない限り、この状態が続きます。このモードでは、セキュリティ違反が起こった場合、ユーザに通知されます。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。
- shutdown：ポート セキュリティ違反が発生すると、インターフェイスは errdisable ステートになって、ただちにシャットダウンし、ポートの LED がオフになります。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが errdisable ステートの場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して、ポートを手動で再びイネーブルにできます（デフォルトのモードです）。
- shutdown vlan：VLAN 単位でセキュリティ違反モードを設定するときに使います。このモードでは、セキュリティ違反が起こった場合、ポート全体ではなく、VLAN が errdisable になります。

表 29-1 に、違反モード、およびポート セキュリティのインターフェイスを設定した場合のアクションを示します。

表 29-1　セキュリティ違反モードのアクション

違反モード	トラフィックの転送[1]	SNMP トラップの送信	Syslog メッセージの送信	エラー メッセージの表示[2]	違反カウンタの増加	ポートのシャットダウン
protect	なし	なし	なし	なし	なし	なし
restrict	なし	あり	あり	なし	あり	なし
shutdown	なし	あり	あり	なし	あり	あり
shutdown vlan	なし	あり	あり	なし	あり	なし[3]

1. 送信元アドレスが不明なパケットは、十分な数のセキュア MAC アドレスが削除されるまで、廃棄されます。
2. 手動で設定したアドレスがセキュリティ違反の原因となる場合、スイッチはエラー メッセージを返します。
3. 違反が発生した VLAN だけをシャットダウンします。

ポート セキュリティのデフォルト設定

表 29-2 に、インターフェイス用のデフォルトのポート セキュリティ設定を示します。

表 29-2　ポート セキュリティのデフォルト設定

機能	デフォルト設定
ポート セキュリティ	ポートでディセーブル。
スティッキ アドレス学習	ディセーブル。
ポート単位のセキュア MAC アドレスの最大数	1
違反モード	shutdown。セキュア MAC アドレスの最大数を超過すると、ポートはシャットダウンします。
ポート セキュリティのエージング	ディセーブル。エージング タイムは 0 です。 スタティック エージングはディセーブルです。 タイプは absolute です。

ポート セキュリティ設定時の注意事項

ポート セキュリティを設定する場合、次の注意事項に従ってください。

- ポート セキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートはダイナミック アクセス ポートにできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートを Fast EtherChannel または Gigabit EtherChannel ポート グループに含めることはできません。

（注）　音声 VLAN は、アクセス ポート上だけでサポートされます。設定で許可されている場合でも、トランク ポート上ではサポートされません。

- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定する必要があります。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つを許可する十分なセキュア アドレスを設定する必要があります。
- ポート セキュリティが設定されているトランク ポートが、データ トラフィック用のアクセス VLAN および音声トラフィック用の音声 VLAN に割り当てられている場合は、**switchport voice** および **switchport priority extend** インターフェイス コンフィギュレーション コマンドを入力しても無効です。

  接続先装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレスを要求し、次に、音声 VLAN の IP アドレスを要求する場合、アクセス VLAN だけに IP アドレスが割り当てられます。
- インターフェイスにセキュア アドレス最大値を入力した場合、新規の値が前回の値より大きいと、新規の値により、前回の設定値が上書きされます。新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングはサポートしていません。

表 29-3 は、ポート セキュリティとその他のポートベース機能の互換性をまとめたものです。

表 29-3　ポート セキュリティとその他のスイッチ機能との互換性

ポートのタイプまたは機能	ポート セキュリティとの互換性
DTP[1] ポート[2]	なし
トランク ポート	あり
ダイナミック アクセス ポート[3]	なし
ルーテッド ポート	なし
SPAN 送信元ポート	あり
SPAN 宛先ポート	なし
EtherChannel	なし
トンネリング ポート	あり
保護ポート	あり
IEEE 802.1x ポート	あり

表 29-3　ポート セキュリティとその他のスイッチ機能との互換性 （続き）

ポートのタイプまたは機能	ポート セキュリティとの互換性
音声 VLAN ポート[4]	あり
プライベート VLAN ポート	あり
IP ソース ガード	あり
ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査	あり
Flex Link	あり

1. DTP = Dynamic Trunking Protocol（ダイナミック トランキング プロトコル）。
2. **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート。
3. **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定された VLAN Query Protocol（VQP）ポート。
4. ポートの最大セキュア アドレス許容数を 2 に設定し、さらにアクセス VLAN に許可されているセキュア アドレスの最大数を加える必要があります。

ポート セキュリティのイネーブル化と設定

ポートへのアクセスが許可されたステーションの MAC アドレスを制限および識別することによって、インターフェイスへの入力を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode** {**access** | **trunk**}	インターフェイス スイッチポート モードを access または trunk に設定します。デフォルト モード（dynamic auto）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 4	**switchport voice vlan** *vlan-id*	ポートで音声 VLAN をイネーブルにします。 *vlan-id*：音声トラフィックに使用する VLAN を指定します。
ステップ 5	**switchport port-security**	インターフェイスでポート セキュリティをイネーブルにします。

	コマンド	目的
ステップ 6	**switchport port-security** [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]	（任意）インターフェイスのセキュア MAC アドレスの最大数を設定します。スイッチに設定できるセキュア MAC アドレスの最大数は、システムで使用が許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management（SDM）テンプレートによって設定されます。第 10 章「スイッチ SDM テンプレートの設定」を参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数です。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-list*：トランク ポートで、VLAN 範囲、または一連の VLAN 内の VLAN ごとに最大値を設定します。VLAN 範囲はハイフン、一連の VLAN はカンマで区切ります。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 • **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。 • **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、そのポートがアクセス VLAN でない場合に限り、利用可能です。インターフェイスが音声 VLAN 用に設定されている場合、最大 2 つのセキュア MAC アドレスを設定します。

	コマンド	目的
ステップ 7	**switchport port-security [violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}]	（任意）違反モード、およびセキュリティ違反が検出されたときの対処方法を次のいずれかで設定します。 • **protect**：ポートのセキュア MAC アドレス数がポートで許可されている最大制限に到達した場合、不明な送信元アドレスのパケットは廃棄されます。十分な数のセキュア MAC アドレスを削除して最大値以下にするか、許可するアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。 **（注）** トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大制限に達していなくても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。 • **restrict**：セキュア MAC アドレス数がポートで許可されている制限に到達した場合、不明な送信元アドレスのパケットは廃棄されます。十分な数のセキュア MAC アドレスを削除するか、許可するアドレスの最大数を増やさない限り、この状態が続きます。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown**：違反が発生し、ポートの LED がオフになると、インターフェイスが errdisable の状態になります。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown vlan**：VLAN 単位でセキュリティ違反モードを設定するときに使います。このモードでは、セキュリティ違反が起こった場合、ポート全体ではなく、VLAN が errdisable になります。 **（注）** セキュア ポートが errdisable ステートになっているときは、**errdisable recovery cause psecure-violatio** グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface vlan** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにできます。

	コマンド	目的
ステップ 8	**switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]	（任意）インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用してセキュア MAC アドレスの最大数を入力できます。最大数より少ないセキュア MAC アドレスを設定すると、残りの MAC アドレスはダイナミックに学習されます。 **（注）** このコマンドを入力したあとにスティッキ ラーニングをイネーブルにすると、ダイナミックに学習されたセキュア アドレスがスティッキ セキュア MAC アドレスに変換されて、実行コンフィギュレーションに追加されます。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポート上で、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しないと、ネイティブ VLAN が使用されます。 • **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。 • **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、そのポートがアクセス VLAN でない場合に限り、利用可能です。インターフェイスが音声 VLAN 用に設定されている場合、最大 2 つのセキュア MAC アドレスを設定します。
ステップ 9	**switchport port-security mac-address sticky**	（任意）インターフェイスでスティッキ ラーニングをイネーブルにします。
ステップ 10	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {**vlan-id** | {**access** | **voice**}}]	（任意）スティッキ セキュア MAC アドレスを入力します。必要に応じて、このコマンドを繰り返し入力します。最大数より少ないセキュア MAC アドレスを設定すると、残りの MAC アドレスはダイナミックに学習され、スティッキ セキュア MAC アドレスに変換されて、実行コンフィギュレーションに追加されます。 **（注）** このコマンドを入力する前にスティッキ ラーニングをイネーブルにしておかないと、エラー メッセージが表示され、スティッキ セキュア MAC アドレスを入力できません。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポート上で、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しないと、ネイティブ VLAN が使用されます。 • **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。 • **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、そのポートがアクセス VLAN でない場合に限り、利用可能です。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show port-security**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスをデフォルト状態の非セキュア ポートに戻すには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。スティッキ ラーニングがイネーブルのときにこのコマンドを入力すると、スティッキ セキュア アドレスの一部は実行コンフィギュレーションのままですが、アドレス テーブルから削除されます。ここで、すべてのアドレスがダイナミックに学習されます。

インターフェイスのセキュア MAC アドレス数をデフォルトに戻すには、**no switchport port-security maximum** *value* インターフェイス コンフィギュレーション コマンドを使用します。違反モードをデフォルト状態の shutdown に戻すには、**no switchport port-security violation** {**protocol** | **restrict**} インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスでスティッキ ラーニングをディセーブルにするには、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスは、スティッキ セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。ただし、スティッキ MAC アドレスを含む設定がすでに保存されている場合は、**no switchport port-security mac-address sticky** コマンドを入力したあとに再び設定を保存する必要があります。保存しない場合、スイッチを再起動するとスティッキ アドレスが復元されます。

MAC アドレス テーブルからすべてのセキュア アドレスを削除するか、スイッチまたはインターフェイス上の特定タイプ（設定済み、ダイナミック、スティッキ）のすべてのセキュア アドレスを削除するには、**clear port-security** {**all** | **configured | dynamic | sticky**} 特権 EXEC コマンドを使用します。

アドレス テーブルから特定のセキュア MAC アドレスを削除するには、**no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用します。アドレス テーブルから特定のインターフェイスのダイナミック セキュア アドレスをすべて削除するには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドのあとに、（インターフェイスでポート セキュリティを再びイネーブルにするために）**switchport port-security** コマンドを入力します。**no switchport port-security** コマンドを入力する前に、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキ セキュア MAC アドレスをダイナミック セキュア MAC アドレスに変換すると、手動で設定されたセキュア アドレスを除き、インターフェイス上のすべてのセキュア アドレスが削除されます。

no switchport port-security mac-address *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、アドレス テーブルから設定済みセキュア MAC アドレスを削除する必要があります。

次に、ポートでポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。違反モードはデフォルト設定、スタティック セキュア MAC アドレスは設定なし、スティッキ ラーニングはイネーブルにします。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 にスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、ポート上でスティッキ ポート セキュリティをイネーブルにして、データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの最大合計数を 20（データ VLAN に 10、音声 VLAN に 10）に設定する例を示します。

```
Switch(config)# interface FastEthernet1/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
```

```
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

ポート セキュリティ エージングのイネーブル化と設定

ポート セキュリティ エージングを使用すると、ポート上のすべてのセキュア アドレスにエージング タイムを設定できます。ポートごとに 2 種類のエージングがサポートされています。

- absolute：ポートのセキュア アドレスは、指定のエージング タイムの経過後、削除されます。
- inactivity：ポートのセキュア アドレスが削除されるのは、指定したエージング タイムの間、そのセキュア アドレスが非アクティブであった場合だけです。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュア ポートで装置の削除や追加を実行でき、ポートのセキュア アドレスの数を制限することもできます。セキュア アドレスのエージングはポート単位でイネーブルまたはディセーブルにできます。

ポート セキュリティ エージングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}	セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにするか、またはエージング タイムやタイプを設定します。 **（注）** スイッチは、スティッキ セキュア アドレスのポート セキュリティ エージングをサポートしていません。 このポートにスタティックに設定されたセキュア アドレスのエージングをイネーブルにする場合は、**static** を入力します。 *time* には、このポートのエージング タイムを指定します。指定できる範囲は 0 ～ 1440 分です。 **type** には、次に示すキーワードのいずれかを選択します。 • **absolute**：エージング タイプを absolute に設定します。このポートのすべてのセキュア アドレスは、指定された time（分）が経過したあとに期限切れとなり、セキュア アドレス リストから削除されます。 • **inactivity**：エージング タイプを inactivity に設定します。指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュア アドレスが期限切れになります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show port-security** [**interface** *interface-id*] [**address**]	設定を確認します。
ステップ 6	**copy running-config startup-config**	(任意) 設定をコンフィギュレーション ファイルに保存します。

ポート上のすべてのセキュア アドレスに対してポート セキュリティ エージングをディセーブルにするには、**no switchport port-security aging time** インターフェイス コンフィギュレーション コマンドを使用します。スタティックに設定されたセキュア アドレスに対してだけエージングをディセーブルにするには、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートのセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport port-security aging time 120
```

次に、インターフェイスに設定されたセキュア アドレスのエージングをイネーブルにし、エージング タイプを inactivity に、エージング タイムを 2 分に設定する例を示します。

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

設定したコマンドを確認するには、**show port-security interface** *interface-id* 特権 EXEC コマンドを入力します。

ポート セキュリティとプライベート VLAN

管理者はポート セキュリティを使用して、ポート上で学習される MAC アドレスの数を制限したり、ポート上で学習可能な MAC アドレス を定義したりできます。

PVLAN ホストおよびプロミスキャス ポートでポート セキュリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode private-vlan** {**host** | **promiscuous**}	インターフェイスでプライベート VLAN をイネーブルにします。
ステップ 4	**switchport port-security**	インターフェイスでポート セキュリティをイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show port-security** [**interface** *interface-id*] [**address**]	設定を確認します。
ステップ 7	**copy running-config startup-config**	(任意) 設定をコンフィギュレーション ファイルに保存します。

```
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```

（注）　ポート セキュリティとプライベート VLAN の両方が設定されているポートには、セキュア PVLAN ポートのラベル付けが可能です。セキュア アドレスがセキュア PVLAN ポートで学習されるとき、同じセキュア アドレスが、同じプライマリ VLAN に属する別のセキュア PVLAN ポートで学習されることはありません。ただし、非セキュア PVLAN ポートで学習されたアドレスは、同じプライマリ VLAN に属するセキュア PVLAN ポートでの学習が可能です。

ホスト ポートで学習されるセキュア アドレスは、関連プライマリ VLAN で自動的に複製されます。同様に、プロミスキャス ポートで学習されるセキュア アドレスは、すべての関連セカンダリ VLAN で自動的に複製されます。スタティック アドレスは、（mac-address-table static コマンドを使用して）セキュア ポートでユーザ設定できません。

ポートベースのトラフィック制御設定の表示

show interfaces *interface-id* **switchport** 特権 EXEC コマンドを使用すると、（各種の特性とともに）インターフェイスのトラフィック抑制および制御の設定が表示されます。**show storm-control** および **show port-security** 特権 EXEC コマンドを使用すると、それぞれストーム制御とポート セキュリティ設定が表示されます。

トラフィック制御情報を表示するには、表 29-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 29-4　トラフィック制御のステータスと設定の表示用コマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定したポートについて、管理ステータスおよび動作ステータスを表示します（ポート ブロッキング、ポート保護設定など）。
show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**]	すべてのインターフェイスまたは指定されたインターフェイスに設定されているストーム制御抑制レベルを、指定されたトラフィック タイプについて、またはブロードキャスト トラフィック（トラフィック タイプが入力されていない場合）について表示します。
show port-security [**interface** *interface-id*]	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を、各インターフェイスで許可されるセキュア MAC アドレスの最大数、インターフェイスに設定されたセキュア MAC アドレスの数、発生したセキュリティ違反の数、違反モードを含めて表示します。
show port-security [**interface** *interface-id*] **address**	すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
show port-security interface *interface-id* **vlan**	指定されたインターフェイスに VLAN 単位で設定されているセキュア MAC アドレスの数を表示します。

CHAPTER 30

SPAN および RSPAN の設定

この章では、IE 3000 スイッチに Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN; リモート SPAN）を設定する方法について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

SPAN および RSPAN の概要

ポートまたは VLAN（仮想 LAN）を通過するネットワーク トラフィックを分析するには、SPAN または RSPAN を使用して、そのスイッチの別のポート、またはネットワーク アナライザなどのモニタリング装置やセキュリティ装置に接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポートまたは送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、分析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングに影響を与えません。宛先ポートを SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外のトラフィックを、宛先ポートが受信または転送することはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN を出入りするトラフィックだけです。送信元 VLAN にルーティングされるトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

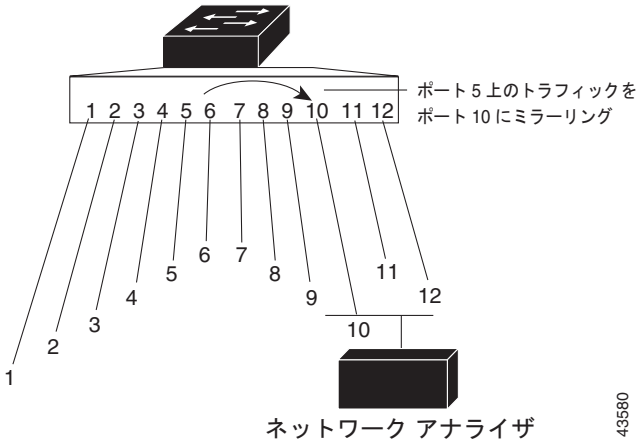
SPAN または RSPAN 宛先ポートを使用すると、ネットワーク セキュリティ装置からトラフィックを送信できます。たとえば、Cisco Intrusion Detection System（IDS; 侵入検知システム）センサー アプライアンスを宛先ポートに接続した場合、IDS 装置は TCP リセット パケットを送信して疑わしい攻撃者の TCP セッションを停止できます。

ここでは、次の概念情報について説明します。

ローカル SPAN

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートあるいは 1 つまたは複数の VLAN から宛先ポートに送信されるトラフィックをコピーして、分析します。たとえば、図 30-1 では、ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされています。ポート 10 のネットワーク アナライザは、ポート 5 に物理的に接続しなくても、ポート 5 からすべてのネットワーク トラフィックを受信します。

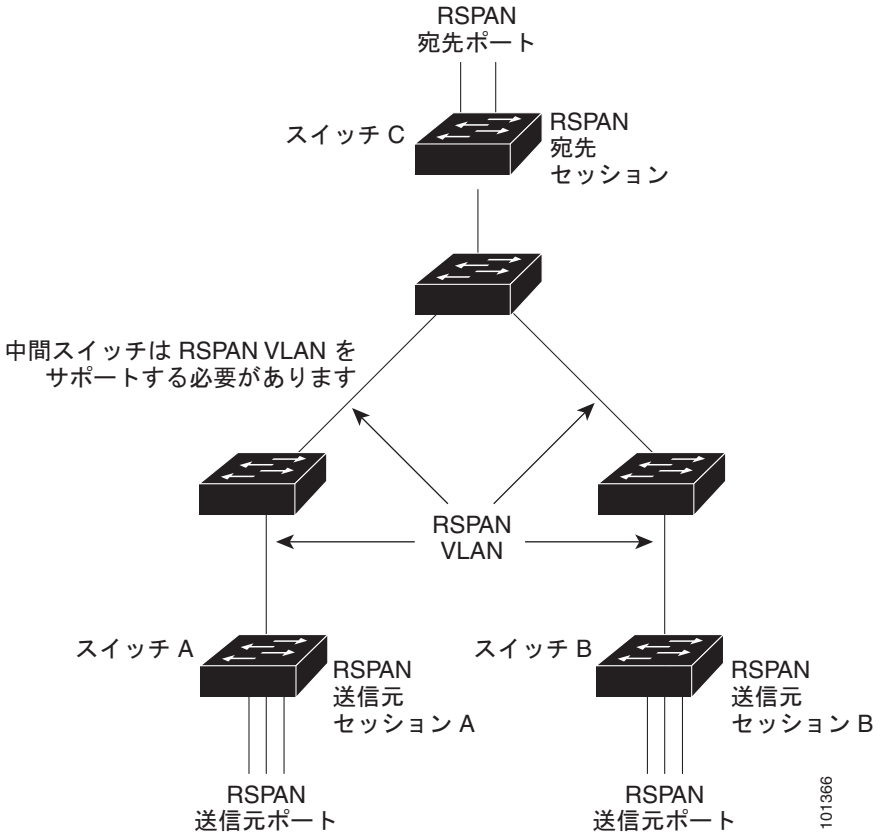
図 30-1　　単一スイッチでのローカル SPAN の設定例



リモート SPAN（RSPAN）

RSPAN は異なるスイッチ上の送信元ポート、送信元 VLAN、および宛先ポートをサポートし、ネットワーク上の複数のスイッチのリモート モニタリングを可能にします。図 30-2 に、スイッチ A およびスイッチ B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元スイッチでは、RSPAN 送信元としてポートまたは VLAN のいずれかを設定する必要があります。宛先は常に物理ポートになります（図のスイッチ C）。

図 30-2　RSPAN の設定例



SPAN および RSPAN の概念と用語

ここでは、SPAN および RSPAN の設定に関連する概念と用語について説明します。

SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1 つまたは複数のポート、あるいは 1 つまたは複数の VLAN 上でトラフィックをモニタし、モニタしたトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN（すべて単一のネットワーク装置上にある）を対応付けます。ローカル SPAN には、個別の送信元および宛先のセッションはありません。ローカル SPAN セッションはユーザが指定した入力および出力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は 1 つまたは複数の RSPAN 送信元セッション、1 つの RSPAN VLAN、および 1 つまたは複数の RSPAN 宛先セッションで構成されます。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク装置上に別々に設定します。装置に RSPAN 送信元セッションを設定するには、送信元ポートまたは送信元 VLAN のセットを RSPAN VLAN と関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別の装置に RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN と関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームの転送先を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを介して宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットから VLAN タギングを除去し、宛先ポートに送ります。RSPAN 宛先セッションの目的は、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットをユーザにコピーして、分析することです。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。RSPAN 送信元セッションと宛先セッションを分離する中間スイッチを配置することもできます。これらのスイッチには RSPAN の実行機能は不要ですが、RSPAN VLAN の要件を満たす必要があります（「RSPAN VLAN」（P.30-8）を参照）。

SPAN セッションでのトラフィックのモニタには、次のような制限があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- スイッチは 2 つまでの送信元セッション（ローカル SPAN と RSPAN の送信元セッション）をサポートします。同じスイッチ内でローカル SPAN と RSPAN の送信元セッションの両方を実行できます。スイッチは合計 66 個の送信元および RSPAN 宛先セッションをサポートします。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、設定できる宛先ポートは最大で 64 個です。
- 個別のまたは重複する SPAN 送信元ポートと VLAN の集合を使用して、2 つの独立した SPAN または RSPAN 送信元セッションを設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- SPAN セッションは、スイッチの正常な動作を妨げません。ただし、SPAN の宛先がオーバーサブスクライブ型ポートである場合（たとえば 100 Mbps ポートをモニタする 10 Mbps ポートなど）、パケットが廃棄されるか、または消失する可能性があります。
- RSPAN がイネーブルの場合、モニタ中の各パケットは 2 回送信されます。1 回は標準トラフィックとして、もう 1 回はモニタされたパケットとしてです。したがって、多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上でも SPAN セッションを設定できます。ただし、宛先ポートと、1 つまたは複数の送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- スイッチの単一セッション内では、ローカル SPAN と RSPAN を併用できません。つまり、RSPAN 送信元セッションにローカル宛先ポートを設定したり、RSPAN 宛先セッションにローカル送信元ポートを設定したり、同じスイッチ上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行したりできません。

モニタ対象トラフィック

SPAN セッションは、次のトラフィック タイプをモニタできます。

- 受信（RX）SPAN : 受信（または入力）SPAN の目的は、スイッチが変更または処理を行う前に送信元インターフェイスまたは VLAN が受信したすべてのパケットをできる限り多くモニタすることです。送信元が受信した各パケットのコピーが、その SPAN セッションの宛先ポートに送信されます。

  Differentiated Services Code Point（DSCP）の変更など、ルーティングまたは Quality of Service（QoS; サービス品質）が原因で変更されるパケットは、変更前にコピーされます。

受信処理中にパケットを廃棄する可能性のある機能は、入力 SPAN には無効です。宛先ポートは、実際の着信パケットが廃棄された場合でも、パケットのコピーを受信します。これらの機能には、標準および拡張 IP 入力 Access Control List（ACL; アクセス制御リスト）、入力 QoS ポリシング、VLAN ACL、出力 QoS ポリシングなどがあります。

- 送信（TX）SPAN：送信（または出力）SPAN の目的は、スイッチによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできる限り多くモニタすることです。送信元から送信された各パケットのコピーが、その SPAN セッションの宛先ポートに送信されます。コピーは、パケットの変更後送信されます。

  Time to Live（TTL; 存続可能時間）、MAC（メディア アクセス制御）アドレス、QoS 値の変更など、ルーティングが原因で変更されたパケットは、宛先ポートで（変更されて）コピーされます。

  送信処理中にパケットを廃棄する可能性のある機能は、SPAN 用のコピーにも影響を与えます。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングなどがあります。

- 双方向：1 つの SPAN セッションで、単一のポートまたは VLAN の送信パケットと受信パケットを両方モニタできます。これはデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてタグなしのパケットが送信されます。通常、SPAN は Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）、Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）などの Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）パケットおよびレイヤ 2 プロトコルをモニタしません。ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次のように変更されます。

- 送信元ポートの場合と同じカプセル化設定（タグなしまたは IEEE 802.1Q）を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットがモニタされます。

したがって、encapsulation replicate がイネーブル化されたローカル SPAN セッションでは、タグなしおよび IEEE 802.1Q タグ付きパケットが宛先ポートに混在する場合があります。

スイッチが輻輳すると、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットが廃棄されることがあります。一般に、これらの特性は相互に依存しません。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニタされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スイッチ輻輳が原因で廃棄された出力パケットは、出力 SPAN からも廃棄されます。

SPAN の設定によっては、同じ送信元パケットの複数のコピーが SPAN 宛先ポートに送信される場合があります。たとえば、ポート A では RX モニタ用に、ポート B では TX モニタ用に、双方向（RX と TX）SPAN セッションが設定されているとします。パケットがポート A を介してスイッチに着信し、ポート B にスイッチングされると、着信パケットと発信パケットの両方が宛先ポートに送信されます。このため、両方のパケットは同じものになります（レイヤ 3 書き換えが行われない場合。レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります）。

送信元ポート

送信元ポート（別名、*モニタ対象ポート*）は、ネットワーク トラフィック分析のためにモニタするスイッチド ポートまたはルーテッド ポートです。1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニタできます。スイッチは、任意の数の送信元ポート（スイッチで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートします。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数は最大 2 つ（ローカルまたは RSPAN）であるため、単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートには、次の特性があります。

- 複数の SPAN セッションでモニタできます。
- 各送信元ポートに、モニタする方向（入力、出力、両方）を設定できます。
- すべてのポート タイプ（EtherChannel、ファスト イーサネット、ギガビット イーサネットなど）が可能です。
- EtherChannel 送信元の場合は EtherChannel 全体で、または物理ポートがポート チャネルに含まれている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセス ポート、トランク ポート、ルーテッド ポート、または音声 VLAN ポートに指定できます。
- 宛先ポートには指定できません。
- 送信元ポートは同じ VLAN 内にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタできます。

送信元 VLAN

VLAN-based SPAN（VSPAN）では、1 つまたは複数の VLAN のネットワーク トラフィックをモニタできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスは VLAN ID で指定され、トラフィックはその VLAN のすべてのポートでモニタされます。

VSPAN には、次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象の VLAN 上のトラフィックだけが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内ではフィルタ VLAN を使用できません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニタされます。VLAN フィルタリングを使用すれば、トランクの送信元ポートでの SPAN トラフィックのモニタを特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートだけです。
- VLAN フィルタリングはポートベース セッションだけに適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の VLAN だけがモニタされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリングは、宛先 SPAN ポートに転送されたトラフィックにだけ作用し、通常のトラフィックのスイッチングには影響しません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートまたは VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名、*モニタリング ポート*）が必要です。

宛先ポートには、次の特性があります。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチに存在している必要があります。RSPAN セッションの場合、宛先ポートは RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションだけを実行するスイッチには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先ポートの設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。
- EtherChannel グループに含まれていたポートが宛先ポートとして設定されている場合、そのポートはグループから削除されます。削除されたポートがルーテッド ポートであった場合、このポートはルーテッド ポートではなくなります。
- 任意のイーサネット物理ポートに指定できます。
- セキュア ポートには指定できません。
- 送信元ポートには指定できません。
- EtherChannel グループまたは VLAN には指定できません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。このポートでは、SPAN セッションに必要なトラフィック以外の転送は行われません。宛先ポートでは着信トラフィックの学習または転送は行われません。
- 入力トラフィック転送がネットワーク セキュリティ装置でイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- スイッチの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートでは、VLAN タギングおよびカプセル化に関する動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなしまたは IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブル化されたローカル SPAN セッションの出力に、タグなしまたは IEEE 802.1Q タグ付きパケットが混在する場合があります。
- RSPAN の場合、元の VLAN ID は RSPAN VLAN ID で上書きされるため、失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN 送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には次の特殊な特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上だけです。
- RSPAN VLAN は、**remote-span** VLAN コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN はプライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VTP に認識される VLAN 1 ～ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲（1006 ～ 4094）内の RSPAN VLAN ID を割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、同時にそれぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションから RSPAN セッションにパケットを送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信することもできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN と他の機能との相互作用

SPAN は、次の機能と相互作用します。

- ルーティング：SPAN はルーテッド トラフィックをモニタしません。VSPAN がモニタするのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックはモニタしません。たとえば、VLAN が受信モニタされ、スイッチが別の VLAN からモニタ対象 VLAN にトラフィックをルーティングする場合、そのトラフィックはモニタされず、SPAN 宛先ポートで受信されません。
- STP：宛先ポートの SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は、RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP：SPAN 宛先ポートは、SPAN セッションがアクティブな間は CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP：VTP を使用して、スイッチ間で RSPAN VLAN をプルーニングできます。
- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定は、いつでも変更できます。ただし、宛先ポートの VLAN メンバーシップまたはトランクの設定に対する変更は、SPAN 宛先設定を削除しない限り有効になりません。送信元ポートの VLAN メンバーシップまたはトランク設定の変更はただちに有効になり、個々の SPAN セッションは、それに応じて自動的に調整されます。

- EtherChannel：EtherChannel グループを送信元ポートに設定できますが、SPAN 宛先ポートには設定できません。グループを SPAN 送信元として設定すると、グループ全体がモニタ対象となります。

  モニタ対象の EtherChannel グループに物理ポートを追加すると、新しいポートが SPAN 送信元ポート リストに追加されます。モニタ対象の EtherChannel グループからポートを削除すると、SPAN 送信元ポート リストから自動的に削除されます。

  EtherChannel グループに属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに属する物理ポートを SPAN 宛先ポートに設定した場合は、EtherChannel グループから削除されます。SPAN セッションからポートが削除されると、EtherChannel グループに復帰します。EtherChannel グループから削除されたポートはグループのメンバーに残りますが、*非アクティブ*または*中断*ステートになります。

  EtherChannel グループに属する物理ポートが宛先ポートであり、かつ、EtherChannel グループが送信元である場合、ポートは EtherChannel グループおよびモニタ対象ポートのリストから削除されます。

- マルチキャスト トラフィックをモニタできます。出力側および入力側ポート モニタの場合は、未編集パケットが 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト パケットが送信される回数は反映されません。
- プライベート VLAN ポートは、SPAN 宛先ポートにはなれません。
- セキュア ポートは SPAN 宛先ポートにはできません。

  SPAN セッションでは、宛先ポートで入力転送がイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているどのポートでもポート セキュリティをイネーブルにしないでください。

- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポートで IEEE 802.1x をイネーブルにできますが、SPAN 宛先として削除するまでは IEEE 802.1x はディセーブルに設定されます。

  SPAN セッションでは、宛先ポートで入力転送がイネーブルの場合、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているどのポートでも IEEE 802.1x をイネーブルにしないでください。

SPAN および RSPAN の設定

ここでは、次の設定情報について説明します。

SPAN および RSPAN のデフォルト設定

表 30-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 30-1　SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN ステート（SPAN および RSPAN）	ディセーブル。
モニタする送信元ポートのトラフィック	受信トラフィックと送信トラフィックの両方（**both**）。
カプセル化タイプ（宛先ポート）	ネイティブ形式（タグなしパケット）。
入力転送（宛先ポート）	ディセーブル。
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタされます。
RSPAN VLAN	設定なし。

ローカル SPAN の設定

ここでは、次の設定情報について説明します。

- 「SPAN 設定時の注意事項」（P.30-10）
- 「ローカル SPAN セッションの作成」（P.30-11）
- 「ローカル SPAN セッションの作成および着信トラフィックの設定」（P.30-14）
- 「フィルタリングする VLAN の指定」（P.30-16）

SPAN 設定時の注意事項

SPAN を設定する場合、次の注意事項に従ってください。

- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、または一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートは送信元ポートにできません。また、送信元ポートは宛先ポートにできません。
- 同じ宛先ポートでは 2 つの SPAN セッションを設定できません。
- スイッチ ポートを SPAN 宛先ポートに設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するのは、モニタ対象のトラフィックだけです。
- SPAN コンフィギュレーション コマンドを入力しても、設定済みの SPAN パラメータは削除されません。設定済みの SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットには元のカプセル化ヘッダー（タグなしまたは IEEE 802.1Q）が付加されます。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。RSPAN 宛先ポートの場合、発信パケットはタグなしです。
- ディセーブルに設定されているポートを送信元または宛先ポートにすることはできますが、SPAN 機能は、宛先ポートおよび 1 つまたは複数の送信元ポートまたは送信元 VLAN がイネーブルになるまでは起動しません。

- **filter vlan** キーワードを使用すると、特定の VLAN に対して SPAN トラフィックを制限できます。モニタ対象がトランク ポートの場合、このキーワードで指定された VLAN 上のトラフィックだけがモニタされます。デフォルトでは、トランク ポートのすべての VLAN がモニタされます。
- 1 つの SPAN セッション内で送信元 VLAN とフィルタ VLAN を混在させることはできません。

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元（モニタ対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* に指定できる範囲は、1 ～ 66 です。 すべての SPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべてのリモート SPAN セッションを削除するには **remote** を指定します。

	コマンド	目的
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number* に指定できる範囲は、1 ～ 66 です。 *interface-id* には、モニタする送信元ポートまたは送信元 VLAN を指定します。 • 送信元 *interface-id* には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスとポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）が含まれます。有効なポートチャネル番号は 1 ～ 6 です。 • *vlan-id* には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 **（注）** 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN は併用できません。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、SPAN は送受信両方のトラフィックをモニタします。 • **both**：送受信両方のトラフィックをモニタします。これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。 **（注）** **monitor session** *session_number* **source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**]}	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 *session_number* には、ステップ 3 で入力したセッション番号を指定します。 **（注）** ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するように指定するには、**encapsulation replicate** を入力します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 **（注）** **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SPAN セッションを削除するには、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除するには、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスに対してこのコマンドの **no** 形式を使用すると、カプセル化オプションは無視されます。

次に、SPAN セッション 1 を設定し、送信元ポートから宛先ポートへのトラフィックをモニタする例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、双方向トラフィックを送信元ギガビット イーサネット ポート 1 から宛先ギガビット イーサネット ポート 2 へミラーリングして、カプセル化方式を維持します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/2
encapsulation replicate
Switch(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元である、ポート 1 を削除する例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/1
Switch(config)# end
```

次に、双方向モニタ用に設定された、ポート 1 での受信トラフィック モニタをディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/1 rx
```

ポート 1 での受信トラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ～ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ギガビット イーサネット ポート 2 に送信する例を示します。さらに、VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするように、コンフィギュレーションが変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成して、送信元ポートまたは送信元 VLAN および宛先ポートを指定し、ネットワーク セキュリティ装置（Cisco IDS センサー アプライアンスなど）用の宛先ポート上の着信トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

着信トラフィックに関連しないキーワードの詳細については、「ローカル SPAN セッションの作成」（P.30-11）を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケット カプセル化、および入力 VLAN とカプセル化を指定します。 *session_number* には、ステップ 3 で入力したセッション番号を指定します。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマまたはハイフンの前後にスペースを入力します。 （任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するように指定するには、**encapsulation replicate** を入力します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 宛先ポートで着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** に次のキーワードを指定して入力します。 • **dot1q vlan** *vlan-id*：IEEE 802.1Q カプセル化を使用し、デフォルト VLAN として指定された VLAN を設定して、着信パケットを受け入れます。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id*：タグなしカプセル化タイプを使用し、デフォルト VLAN として指定された VLAN を設定して、着信パケットを受け入れます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SPAN セッションを削除するには、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除するには、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスに対してこのコマンドの **no** 形式を使用すると、カプセル化および入力オプションは無視されます。

次に、SPAN セッション 2 の既存の設定を削除し、ギガビット イーサネット送信元ポート 1 で受信トラフィックをモニタするように SPAN セッション 2 を設定し、このトラフィックを送信元ポートと同じ出力カプセル化タイプを使用して宛先ギガビット イーサネット ポート 2 に送信し、IEEE 802.1Q カプセル化およびデフォルト入力 VLAN として VLAN 6 を使用する入力転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation
replicate ingress dot1q vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* に指定できる範囲は、1 ～ 66 です。 すべての SPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべてのリモート SPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id*	送信元ポート（モニタ対象ポート）および SPAN セッションの特性を指定します。 *session_number* に指定できる範囲は、1 ～ 66 です。 *interface-id* には、モニタする送信元ポートを指定します。指定されたインターフェイスが、トランク ポートとして設定されている必要があります。
ステップ 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* には、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* では、指定できる範囲は 1 ～ 4094 です。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して一定範囲の VLAN を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]}	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 *session_number* には、ステップ 3 で入力したセッション番号を指定します。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （任意）[**,** | **-**]：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するように指定するには、**encapsulation replicate** を入力します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

トランク ポート上のすべての VLAN をモニタするには、**no monitor session** *session_number* **filter** グローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定を削除し、ギガビット イーサネット トランク ポート 2 での受信トラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および VLAN 9 のトラフィックだけを宛先ギガビット イーサネット ポート 1 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/1
Switch(config)# end
```

RSPAN の設定

ここでは、次の設定情報について説明します。

RSPAN 設定時の注意事項

RSPAN を設定する場合、次の注意事項に従ってください。

- RSPAN には、「SPAN 設定時の注意事項」（P.30-10）のすべての項目が当てはまります。
- RSPAN VLAN には特殊なプロパティがあるので、RSPAN VLAN として使用する VLAN をネットワーク上にいくつか確保しておき、これらの VLAN にはアクセス ポートを割り当てないでください。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択してフィルタリングまたはモニタできます。これらの ACL は、RSPAN 送信元スイッチ内の RSPAN VLAN 上で指定します。
- RSPAN の設定では、送信元ポートと宛先ポートをネットワーク内の複数のスイッチに分散できます。
- RSPAN は BPDU パケット モニタリングやその他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートだけに設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生するのを防ぐため、参加しているすべてのスイッチで VLAN remote-span 機能がサポートされていることを確認してください。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として組み込まれます。また、RSPAN VLAN を SPAN セッションの送信元にすることもできます。ただし、スイッチはセッション間にわたるトラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。
- 任意の VLAN を RSPAN VLAN として設定するには、次の条件を満たす必要があります。
  - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
  - 参加するすべてのスイッチが RSPAN をサポートしている。

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定してください。
- VTP および VTP プルーニングをイネーブルにすると、RSPAN トラフィックはトラックでプルーニングされ、VLAN ID が 1005 以下の RSPAN トラフィックがネットワーク上で不必要にフラッディングするのを防止できます。

RSPAN VLAN としての VLAN の設定

最初に、RSPAN セッション用の RSPAN VLAN に設定する VLAN を新規に作成します。RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲（1005 以下）であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するように設定できます。拡張範囲 VLAN（1006 以上）の場合、送信元と宛先の両方のスイッチ、およびすべての中間スイッチに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックのフローを効率化するか、または RSPAN トラフィックを伝達する必要のないすべてのトラックから、RSPAN VLAN を手動で削除してください。

RSPAN VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ～ 1001 および 1006 ～ 4094 です。 RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークン リングや FDDI VLAN 専用）にすることはできません。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN から RSPAN の特性を削除して、標準 VLAN に変換するには、**no remote-span** VLAN コンフィギュレーション コマンドを使用します。

次に、RSPAN VLAN 901 を作成する例を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の RSPAN 設定を削除します。 *session_number* に指定できる範囲は、1 ～ 66 です。 すべての RSPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべてのリモート SPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number* に指定できる範囲は、1 ～ 66 です。 RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 • *interface-id* には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスとポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）が含まれます。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN は併用できません。 （任意）[**,** | **-**]：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送受信両方のトラフィックを送信します。 • **both**：送受信両方のトラフィックをモニタします。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。
ステップ 4	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先 RSPAN VLAN を指定します。 *session_number* には、ステップ 3 で定義した番号を入力します。 *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SPAN セッションを削除するには、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session** *session_number* **destination remote vlan** *vlan-id* コマンドを使用します。

次に、セッション 1 の既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/2 rx

Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは別のスイッチ（送信元セッションが設定されていないスイッチ）に設定します。

スイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	送信元スイッチで作成された RSPAN VLAN の VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し､RSPAN VLAN ID が 2 ～ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 2 ～ 4 は不要です。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として識別します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の RSPAN 設定を削除します。 *session_number* に指定できる範囲は、1 ～ 66 です。 すべての RSPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべてのリモート SPAN セッションを削除するには **remote** を指定します。
ステップ 6	**monitor session** *session_number* **source remote vlan** *vlan-id*	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 *session_number* に指定できる範囲は、1 ～ 66 です。 *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。

	コマンド	目的
ステップ 7	**monitor session** *session_number* **destination interface** *interface-id*	RSPAN セッションおよび宛先インターフェイスを指定します。 *session_number* には、ステップ 6 で定義した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスには物理インターフェイスを指定する必要があります。 **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしとして表示されます。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SPAN セッションを削除するには、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから宛先ポートを削除するには、**no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session** *session_number* **source remote vlan** *vlan-id* コマンドを使用します。

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet1/1
Switch(config)# end
```

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成して、送信元 RSPAN VLAN および宛先ポートを指定し、ネットワーク セキュリティ装置（Cisco IDS センサー アプライアンスなど）用の宛先ポート上の着信トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

着信トラフィックに関連しないキーワードの詳細については、「RSPAN 宛先セッションの作成」（P.30-20）を参照してください。この手順では、RSPAN VLAN がすでに設定済みであると想定しています。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。
ステップ 3	**monitor session** *session_number* **source remote vlan** *vlan-id*	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 *session_number* に指定できる範囲は、1 ～ 66 です。 *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケット カプセル化、および着信 VLAN とカプセル化を指定します。 *session_number* には、ステップ 4 で定義した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスには物理インターフェイスを指定する必要があります。 **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしとして表示されます。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 宛先ポートで着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** と追加のキーワードを入力します。 • **dot1q vlan** *vlan-id*：IEEE 802.1Q カプセル化を使用し、デフォルト VLAN として指定された VLAN を設定して、着信パケットを転送します。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id*：タグなしカプセル化タイプを使用し、デフォルト VLAN として指定された VLAN を設定して、着信パケットを転送します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

RSPAN セッションを削除する場合は、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。RSPAN セッションから宛先ポートを削除するには、**no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。このコマンドの **no** 形式を使用すると、入力オプションは無視されます。

次に、VLAN 901 を RSPAN セッション 2 の送信元リモート VLAN として設定し、ギガビット イーサネット送信元ポート 2 を宛先インターフェイスとして設定し、VLAN 6 がデフォルトの受信側 VLAN として設定されたインターフェイス上で着信トラフィックの転送をイネーブルにする例を示します。

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/2 ingress vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* に指定できる範囲は、1 ～ 66 です。 すべての SPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべてのリモート SPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id*	送信元ポート（モニタ対象ポート）および SPAN セッションの特性を指定します。 *session_number* に指定できる範囲は、1 ～ 66 です。 *interface-id* には、モニタする送信元ポートを指定します。指定されたインターフェイスが、トランク ポートとして設定されている必要があります。
ステップ 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* には、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* では、指定できる範囲は 1 ～ 4094 です。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して一定範囲の VLAN を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 *session_number* には、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* には、モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

トランク ポート上のすべての VLAN をモニタするには、**no monitor session** *session_number* **filter vlan** グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 での受信トラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 のトラフィックだけを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Switch(config)# no monitor session 2
(config)# monitor session 2 source interface gigabitethernet1/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

SPAN および RSPAN ステータスの表示

現在の SPAN または RSPAN 設定を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。**show running-config** 特権 EXEC コマンドを使用すれば、設定された SPAN セッションまたは RSPAN セッションを表示することもできます。

CHAPTER 31

LLDP、LLDP-MED、および有線のロケーション サービスの設定

この章では、IE 3000 スイッチ上で Link Layer Discovery Protocol（LLDP）、LLDP Media Endpoint Discovery（LLDP-MED）、および有線のロケーション サービスを設定する手順について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスと、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「System Management Commands」を参照してください。

LLDP、LLDP-MED、および有線のロケーション サービスの概要

LLDP

Cisco Discovery Protocol（CDP; シスコ検出プロトコル）は、シスコ製のすべての装置（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）上のレイヤ 2（データ リンク層）で動作する装置検出プロトコルです。CDP を使用すると、ネットワーク管理アプリケーションによってネットワークに接続された シスコ デバイスが自動的に検出および学習されます。

非シスコ デバイスをサポートし、他の装置との相互運用性を確保するために、スイッチは IEEE 802.1AB Link Layer Discovery Protocol（LLDP）をサポートします。LLDP は、ネットワーク上の他の装置に対してその装置自身の情報をアドバタイズするために、ネットワーク装置に使用されているネイバー探索プロトコルです。このプロトコルはデータリンク層で動作するので、異なるネットワーク層のプロトコルで動作している 2 台のシステムでも相互認識が可能です。

LLDP は、ネイバー装置を検出するために使用する一連の属性をサポートします。これらの属性には、タイプ、長さ、および値の説明が含まれ、TLV と呼ばれます。LLDP をサポートしている装置は、TLV を使用してネイバー装置の情報を受信、およびネイバー装置への情報の送信を行うことができます。このプロトコルは、設定情報、装置の機能、および装置の ID などの詳細をアドバタイズできます。

スイッチは次の基本的な管理 TLV をサポートします。次は必須 LLDP TLV です。

- ポートの説明 TLV
- システム名 TLV
- システムの説明 TLV
- システムの機能 TLV
- 管理アドレス TLV

次の組織的に特定された LLDP TLV も LLDP-MED をサポートするようにアドバタイズされます。

- ポート VLAN ID TLV（IEEE 802.1 の組織的に特定された TLV）
- MAC/PHY コンフィギュレーション/ステータス TLV（IEEE 802.3 の組織的に特定された TLV）

（注）　スイッチ スタックがネットワーク内の単一のスイッチとして表示されます。このため、LLDP は個別のスタック メンバーではなくスイッチ スタックを検出します。

LLDP または CDP ロケーション情報をポート単位に設定すると、リモート デバイスが Cisco Medianet ロケーション情報をスイッチに送信できるようになります。詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html

LLDP-MED

LLDP for Media Endpoint Devices（LLDP-MED）は、IP Phone などのエンドポイント装置とスイッチなどのネットワーク装置の間で動作する LLDP に対する拡張です。特に、Voice over IP（VoIP）アプリケーションに対するサポートを提供すると同時に、機能検出、ネットワーク ポリシー、Power over Ethernet（PoE; イーサネット経由の電源供給）、コンポーネント管理、およびロケーション情報に追加の TLV も提供します。デフォルトでは、すべての LLDP-MED TLV がイネーブルになっています。

LLDP-MED は、次の TLV をサポートします。

- LLDP-MED 機能 TLV

  接続されている装置がサポートし、イネーブルになっている機能を LLDP-MED エンドポイントが判別できるようにします。

- ネットワーク ポリシー TLV

  ネットワーク接続している装置とエンドポイントの両方が、そのポート上の特定のアプリケーションに対する VLAN 設定および関連付けられたレイヤ 2 およびレイヤ 3 の属性をアドバタイズできるようにします。たとえば、スイッチは使用すべき VLAN 番号を電話機に通知できます。電話機は、任意のスイッチに接続し、その VLAN 番号を取得してから、コール制御との通信を開始できます。

  ネットワーク ポリシー プロファイル TLV を定義することによって、VLAN、class of service（CoS; サービス クラス）、Differentiated Services Code Point（DSCP）、およびタギング モードに対する値を指定し、音声と音声シグナリングのプロファイルを作成できます。これらのプロファイル属性は、その後、スイッチ上で集中してメンテナンスされ、電話機に伝播されます。

- 電源管理 TLV

  LLDP-MED エンドポイントとネットワーク接続している装置間の高度な電源管理をイネーブルにします。スイッチと電話機が、装置への電源供給方法、電源のプライオリティ、装置に必要な電力量などの電源情報を伝達できるようにします。

- コンポーネント管理 TLV

  エンドポイントが、ハードウェア リビジョン、ファームウェア バージョン、ソフトウェア バージョン、シリアル番号、メーカー名、モデル名、およびアセット ID TLV 情報を含むエンドポイント自身についての詳細なコンポーネント情報をスイッチに送信できるようにします。

- ロケーション TLV

  スイッチからエンドポイント装置にロケーション情報を提供します。ロケーション TLV は次の情報を送信できます。

  - 都市ロケーション情報

    都市のアドレス情報と郵便情報を提供します。都市ロケーション情報の例としては、住所、道路名、および郵便区名の情報があります。

  - ELIN ロケーション情報

    発信者のロケーション情報を提供します。ロケーションは、Emergency location identifier number（ELIN; 緊急ロケーション情報）によって決定されます。これは地域の public safety answering point（PSAP）への緊急コールをルーティングし、緊急コールの発信者にコールバックするために PSAP が使用できる電話番号です。

有線のロケーション サービス

スイッチは、有線のロケーション サービスを使用して、Cisco Mobility Services Engine（MSE）に、そのスイッチに接続された装置に関するロケーションと接続の追跡情報を送信します。追跡する装置は、無線エンドポイント、有線エンドポイント、または有線スイッチまたはコントローラになります。スイッチは、Network Mobility Services Protocol（NMSP; ネットワーク モビリティ サービス プロトコル）ロケーションと接続通知を使用して、MSE に装置のリンクアップ イベントとリンクダウン イベントを通知します。

MSE はスイッチに対する NMSP 接続を開始し、サーバ ポートを開きます。MSE がスイッチに接続すると、バージョン互換性、サービス交換情報、およびその後にロケーション情報の同期を確立するため、一連のメッセージ交換を行います。接続後、スイッチは定期的にロケーションと接続通知を MSE に送信します。インターバルの間に検出されたリンクアップ イベントまたはリンクダウン イベントは、集約されインターバルの最後に送信されます。

スイッチが、リンクアップ イベントまたはリンク ダウン イベント上で装置の有無を判断すると、MAC アドレス、IP アドレス、ユーザ名などのクライアント固有の情報を取得します。クライアントが LLDP-MED 対応または CDP 対応である場合、スイッチは LLDP-MED ロケーション TLV または CDP を通してシリアル番号と UDI を取得します。

装置の機能に応じて、スイッチはリンクアップの時点で次のクライアント情報を取得します。

- ポート接続で指定されたスロットとポート。
- クライアント MAC アドレスで指定された MAC アドレス。
- ポート接続で指定された IP アドレス。
- 802.1X ユーザ名（該当する場合）。
- 装置カテゴリが *有線ステーション*として指定されているか。
- ステートが *new* として指定されているか。
- シリアル番号、UDI。
- モデル番号。
- スイッチが関連付けを検出してからの時間（秒単位）。

装置の機能に応じて、スイッチはリンクダウン時に次のクライアント情報を取得します。

- 切断されたスロットとポート。
- MAC アドレス。
- IP アドレス。
- 802.1X ユーザ名（該当する場合）。
- 装置カテゴリが *有線ステーション*として指定されているか。
- ステートが *delete* として指定されているか。
- シリアル番号、UDI。
- スイッチが関連付けの解除を検出してからの時間（秒単位）。

スイッチがシャットダウンされると、MSE への NMSP 接続を閉じる前に *delete* ステートの接続通知および IP アドレスが送信されます。MSE は、この通知をスイッチに関連付けられている有線クライアントのすべてに対する関連付けの解除として解釈します。

スイッチ上でロケーション アドレスを変更する場合は、スイッチは影響を受けるポートと変更されたアドレス情報を識別する NMSP ロケーション通知メッセージを送信します。

LLDP、LLDP-MED、および有線のロケーション サービスの設定

LLDP のデフォルト設定

表 31-1　LLDP のデフォルト設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv の選択	すべての TLV を送受信するようにディセーブル
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	ディセーブル

表 31-1　LLDP のデフォルト設定 （続き）

機能	デフォルト設定
LLDP 転送	ディセーブル
LLDP med-tlv の選択	すべての LLDP-MED TLV を送信するようにディセーブル（LLDP がグローバルにイネーブルの場合、LLDP-MED-TLV もイネーブル）

設定時の注意事項

- インターフェイスがトンネル ポートとして設定されている場合は、LLDP は自動的にディセーブルになります。
- ネットワーク ポリシー プロファイルを初めて設定したインターフェイスには、**switchport voice vlan** コマンドを適用できません。**switchport voice vlan** *vlan-id* がすでに設定されているインターフェイスには、ネットワーク ポリシー プロファイルを適用できます。このようにして、そのインターフェイスには、音声または音声シグナリング VLAN ネットワーク ポリシー プロファイルが適用されます。
- ネットワーク ポリシー プロファイルを持っているインターフェイス上では、スタティック セキュア MAC アドレスを設定できません。
- プライベート VLAN ポート上ではネットワーク ポリシー プロファイルを設定できません。
- 有線のロケーションが機能するには、最初に **ip device tracking** グローバル コンフィギュレーション コマンドを入力する必要があります。

LLDP のイネーブル化

LLDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lldp run**	スイッチ上で LLDP をグローバルにイネーブルにします。
ステップ 3	**interface** *interface-id*	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lldp transmit**	インターフェイスが LLDP パケットを送信できるようにします。
ステップ 5	**lldp receive**	インターフェイスが LLDP パケットを受信できるようにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show lldp**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

LLDP をディセーブルにするには、**no lldp run** グローバル コンフィギュレーション コマンドを使用します。インターフェイス上で LLDP をディセーブルにするには、**no lldp transmit** および **no lldp receive** インターフェイス コンフィギュレーション コマンドを使用します。

次に、LLDP をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

次に、インターフェイス上で LLDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```

LLDP の特性の設定

LLDP 更新の頻度、情報を廃棄する前に保持する時間、および初期化遅延時間を設定できます。LLDP および LLDP-MED TLV を選択して送受信ができます。

LLDP の特性を設定するには、特権 EXEC モードで次の手順を実行します。

（注）　ステップ 2 ～ 5 は任意であり、どの順序で実行してもかまいません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lldp holdtime** *seconds*	（任意）装置からの情報を受信側装置が廃棄する前まで保持する時間を指定します。 指定できる範囲は 0 ～ 65535 秒です。デフォルトは 120 秒です。
ステップ 3	**lldp reinit** *delay*	（任意）LLDP がインターフェイス上で初期化するための遅延時間を秒単位で指定します。 指定できる範囲は 2 ～ 5 秒です。デフォルトは 2 秒です。
ステップ 4	**lldp timer** *rate*	（任意）LLDP 更新の送信頻度を秒単位で設定します。 指定できる範囲は 5 ～ 65534 秒です。デフォルトは 30 秒です。
ステップ 5	**lldp tlv-select**	（任意）送信または受信する LLDP TLV を指定します。
ステップ 6	**interface** *interface-id*	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**lldp med-tlv-select**	（任意）送信または受信する LLDP-MED TLV を指定します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show lldp**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、各 LLDP コマンドの **no** 形式を使用します。

次に、LLDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config)# lldp timer 30
Switch(config)# end
```

LLDP-MED TLV の設定

デフォルトでは、スイッチはエンド装置から LLDP-MED パケットを受信するまで LLDP パケットだけを送信します。その後で、MED TLV を持つ LLDP パケットも送信します。LLDP-MED エントリが期限切れになった場合は、再度 LLDP パケットだけを送信します。

lldp インターフェイス コンフィギュレーション コマンドを使用することによって、表 31-2 に示す TLV を送信しないようにインターフェイスを設定できます。

表 31-2　LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED コンポーネント管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

インターフェイス上で TLV をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	LLDP-MED TLV を設定しているインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**lldp med-tlv-select** *tlv*	イネーブルにする TLV を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、インターフェイス上で TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```

ネットワーク ポリシーの設定

ネットワーク ポリシー プロファイルを作成し、ポリシー属性を設定し、インターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**network-policy profile** *profile number*	ネットワーク ポリシー プロファイル番号を指定し、ネットワーク ポリシー コンフィギュレーション モードを開始します。指定できる範囲は 1 ～ 4294967295 です。

	コマンド	目的
ステップ 3	{**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos** *cvalue* | **dscp** *dvalue*}] | [[**dot1p** {**cos** *cvalue* | **dscp** *dvalue*}] | **none** | **untagged**]	ポリシー属性を設定します。 **voice**：音声アプリケーション タイプを指定します。 **voice-signaling**：音声シグナリング アプリケーション タイプを指定します。 **vlan**：音声トラフィックのネイティブ VLAN を指定します。 *vlan-id*：（任意）音声トラフィックの VLAN を指定します。指定できる範囲は 1 ～ 4094 です。 **cos** *cvalue*：（任意）設定された VLAN のレイヤ 2 プライオリティ サービス クラス（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルトは 5 です。 **dscp** *dvalue*：（任意）設定された VLAN の Differentiated Services Code Point（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルトは 46 です。 **dot1p**：（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように IP Phone を設定します。 **none**：（任意）音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。 **untagged**：（任意）タグなしの音声トラフィックを送信するように IP Phone を設定します。これが IP Phone のデフォルト設定になります。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	ネットワーク ポリシー プロファイルを設定しているインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**network-policy** *profile number*	ネットワーク ポリシー プロファイル番号を指定します。
ステップ 7	**lldp med-tlv-select network-policy**	ネットワーク ポリシー TLV を指定します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show network-policy profile**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

次に、CoS を使用して音声アプリケーションに対する VLAN 100 を設定して、インターフェイス上でネットワーク ポリシー プロファイルとネットワーク ポリシー TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# network-policy 1
Switch(config-network-policy)# voice vlan 100 cos 4
Switch(config-network-policy)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# network-policy profile 1
Switch(config-if)# lldp med-tlv-select network-policy
```

次の例では、プライオリティ タギングを使用したネイティブ VLAN に音声アプリケーション タイプを設定する方法を示します。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
Switch(config-network-policy)# voice vlan dot1p dscp 34
```

ロケーション TLV および有線のロケーション サービスの設定

エンドポイントのロケーション情報を設定し、それをインターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location** {**admin-tag** *string* | **civic-location identifier** *id* | **elin-location** *string* **identifier** *id*}	エンドポイントにロケーション情報を指定します。 • **admin-tag**：管理タグまたはサイト情報を指定します。 • **civic-location**：都市ロケーション情報を指定します。 • **elin-location**：緊急ロケーション情報（ELIN）を指定します。 • **identifier** *id* *:* 都市ロケーションの ID を指定します。 • *string*：サイト情報またはロケーション情報を英数字形式で指定します。
ステップ 3	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id*	ロケーション情報を設定しているインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**location** {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}	インターフェイスに対するロケーション情報を入力します。 **additional-location-information**：ロケーションまたは場所に関する追加情報を設定します。 **civic-location-id**：インターフェイスにグローバル都市ロケーション情報を指定します。 **elin-location-id**：インターフェイスに緊急ロケーション情報を指定します。 *id :*都市ロケーションまたは ELIN ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。 *word*:追加のロケーション情報を持つ語またはフレーズを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show location**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

スイッチ上の有線のロケーション サービスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

（注）　スイッチは、暗号化ソフトウェア イメージを実行して **nmsp** グローバル コンフィギュレーション コマンドをイネーブルにする必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**nmsp enable**	スイッチで NMSP 機能をイネーブルにします。
ステップ 3	**nmsp notification interval** {**attachment** | **location**} *interval-seconds*	NMSP 通知間隔を指定します。 **attachment**：接続通知間隔を指定します。 **location**：位置通知間隔を指定します。 *interval-seconds*：スイッチから MSE に位置更新または接続更新が送信されるまでの時間（秒単位）。指定できる範囲は 1 ～ 30 です。デフォルト値は 30 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show network-policy profile**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、スイッチ上で NMSP をイネーブルにして、位置通知間隔を 10 秒に設定する例を示します。

```
Switch(config)# nmsp enable
Switch(config)# nmsp notification interval location 10
```

LLDP、LLDP-MED および有線ロケーション サービスのモニタおよびメンテナンス

装置上の LLDP、LLDP-MED、および有線のロケーション サービスをモニタおよびメンテナンスするには、特権 EXEC モードで次の手順を実行します。

コマンド	説明
clear lldp counters	トラフィック カウンタをゼロにリセットします。
clear lldp table	LLDP ネイバー情報テーブルを削除します。
clear nmsp statistics	NMSP 統計情報カウンタを消去します。
show lldp	送信の頻度、送信されたパケットのホールドタイム、インターフェイス上で LLDP が初期化されるまでの遅延時間など、グローバルな情報を表示します。
show lldp entry *entry-name*	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力してすべてのネイバーを表示したり、ネイバー名を入力したりできます。
show lldp interface [*interface-id*]	LLDP がイネーブルになった状態のインターフェイスについての情報を表示します。 特定のインターフェイスに表示を制限できます。

コマンド	説明
show lldp neighbors [*interface-id*] [**detail**]	装置のタイプ、インターフェイスのタイプと番号、ホールドタイム設定、機能、およびポート ID を含むネイバーに関する情報を表示します。 特定のインターフェイスのネイバーだけを表示することも、さらに詳細な情報を表示することもできます。
show lldp traffic	送受信されたパケットの数、廃棄されたパケットの数、および認識不能な TLV の数を含む LLDP カウンタを表示します。
show location	エンドポイントにロケーション情報を表示します。
show network-policy profile	設定されたネットワーク ポリシー プロファイルを表示します。
show nmsp	NMSP 統計情報を表示します。

CHAPTER 32

CDP の設定

この章では、IE 3000 スイッチに Cisco Discovery Protocol（CDP; シスコ検出プロトコル）を設定する手順について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスと、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「System Management Commands」を参照してください。

この章で説明する内容は、次のとおりです。

CDP の概要

CDP は、シスコ製のすべての装置（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データ リンク層）で動作する装置検出プロトコルです。CDP を使用することにより、ネットワーク管理アプリケーションで、既知装置のネイバーであるシスコ デバイスを検索することができます。ネットワーク管理アプリケーションは CDP によって、下位レイヤのトランスペアレント プロトコルを実行しているネイバー装置の、装置タイプおよび Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）エージェント アドレスを確認できます。この機能によって、アプリケーションからネイバー装置に SNMP クエリーを送信できます。

CDP は、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）をサポートしているすべてのメディアで動作します。CDP はデータリンク層だけで動作するため、ネットワーク層のプロトコルが異なる 2 台のシステムでも相互認識が可能です。

CDP を設定した各装置は、マルチキャスト アドレスに対して定期的にメッセージを送信し、SNMP メッセージを受信できる 1 つまたは複数のアドレスをアドバタイズします。このアドバタイズには、受信側装置で CDP 情報を廃棄する前に保持しておく時間を表す Time to Live（TTL; 存続可能時間）またはホールドタイム情報も含まれます。各装置は、他の装置から送信されるメッセージを待ち受けて、ネイバー装置を確認します。

スイッチ上で CDP を使用すると、Network Assistant でネットワークを視覚的に表示できます。スイッチは CDP を使用してクラスタ候補を検出し、クラスタ メンバーと、コマンド スイッチから最大 3 台（デフォルト）先にあるクラスタ対応のその他の装置について、情報を維持します。

スイッチと、それに接続されている Cisco Medianet を実行しているエンドポイント デバイスの場合、次のようになります。

- CDP が、スイッチと直接通信している接続されたエンドポイントを識別します。
- ネイバー デバイスのレポートが重複しないように、有線で接続された 1 台のスイッチだけがロケーション情報をレポートします。
- 有線で接続されたスイッチとエンドポイントの両方が、ロケーション情報の送受信を行います。

  詳細については、次の URL を参照してください。
  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html

スイッチは CDP バージョン 2 をサポートします。

CDP の設定

ここでは、次の設定情報について説明します。

CDP のデフォルト設定

表 32-1 に、CDP のデフォルト設定を示します。

表 32-1　CDP のデフォルト設定

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー（パケット更新頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

CDP の特性の設定

CDP 更新の頻度、廃棄するまで情報を保持する時間、およびバージョン 2 アドバタイズを送信するかどうかを設定できます。

CDP タイマー、ホールドタイム、およびアドバタイズ タイプを設定するには、特権 EXEC モードで次の手順を実行します。

（注）　ステップ 2 ～ 4 はすべて任意であり、どの順序で実行してもかまいません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp timer** *seconds*	（任意）CDP 更新の送信頻度（秒）を設定します。 指定できる範囲は 5 ～ 254 です。デフォルトは 60 秒です。
ステップ 3	**cdp holdtime** *seconds*	（任意）装置から送信された情報を受信側装置が廃棄するまで保持する時間を指定します。 指定できる範囲は 10 ～ 255 です。デフォルトは 180 秒です。
ステップ 4	**cdp advertise-v2**	（任意）バージョン 2 アドバタイズを送信するように CDP を設定します。 これがデフォルトの状態になります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show cdp**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

次に、CDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

その他の CDP の **show** コマンドについては、「CDP のモニタおよびメンテナンス」（P.32-5）を参照してください。

CDP のディセーブル化およびイネーブル化

CDP はデフォルトでイネーブルになっています。

（注）　スイッチ クラスタとその他のシスコ デバイス（Cisco IP Phone など）は、定期的に CDP メッセージを交換しています。CDP をディセーブルにすると、クラスタの検出と装置の接続が中断される可能性があります。詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com の『*Getting Started with Cisco Network Assistant*』を参照してください。

CDP 装置検出機能をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no cdp run**	CDP をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

ディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp run**	ディセーブル化されている CDP をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

次に、ディセーブル化されている CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```

インターフェイスでの CDP のディセーブル化およびイネーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

ポート上で CDP をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no cdp enable**	インターフェイスで CDP をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポート上でディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	CDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**cdp enable**	インターフェイス上でディセーブル化されている CDP をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ポート上でディセーブル化されている CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# cdp enable
Switch(config-if)# end
```

CDP のモニタおよびメンテナンス

装置上の CDP をモニタおよびメンテナンスするには、特権 EXEC モードで次の作業を 1 つまたは複数実行します。

コマンド	説明
clear cdp counters	トラフィック カウンタをゼロにリセットします。
clear cdp table	ネイバーに関する情報を格納する CDP テーブルを削除します。
show cdp	送信の頻度、送信されたパケットのホールドタイムなど、グローバルな情報を表示します。
show cdp entry *entry-name* [**protocol** | **version**]	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力してすべての CDP ネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定したネイバーでイネーブルになっているプロトコルの情報や、装置上で実行されているソフトウェアのバージョン情報だけを表示することもできます。
show cdp interface [*interface-id*]	CDP がイネーブルになっているインターフェイスに関する情報を表示します。 情報が必要なインターフェイスだけを表示することもできます。
show cdp neighbors [*interface-id*] [**detail**]	装置タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、プラットフォーム、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスのネイバーだけを表示することも、さらに詳細な情報を表示することもできます。
show cdp traffic	CDP カウンタ（送受信されたパケット数、チェックサム エラーを含む）を表示します。

CHAPTER 33

UDLD の設定

この章では、IE 3000 スイッチに Unidirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルを設定する方法について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

UDLD の概要

UDLD は、光ファイバまたはツイストペア イーサネット ケーブルを通じて接続された装置がケーブルの物理設定をモニタしたり、単一方向リンクの存在を検出できるようにしたりするレイヤ 2 プロトコルです。このプロトコルで単一方向リンクを正しく識別してディセーブルにするためには、接続されたすべての装置で UDLD をサポートしている必要があります。UDLD は、単一方向リンクを検出すると、影響のあるポートをディセーブルにし、警告を発します。単一方向リンクは、スパニング ツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、2 つの動作モードをサポートしています。ノーマル モード（デフォルト）とアグレッシブ モードです。通常モードでは、UDLD は、光ファイバ接続において誤って接続されたポートによる単一方向リンクを検出できます。アグレッシブ モードでは、UDLD は、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたポートによる単一方向リンクも検出できます。

通常モードとアグレッシブ モードで、UDLD はレイヤ 1 のメカニズムとともに動作し、リンクの物理ステータスを学習します。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバーの ID の検知、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検知機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

単一方向リンクは、ローカルの装置が送信したトラフィックをネイバーが受信し、そのネイバーからのトラフィックをローカルの装置が受信していない場合に発生します。

通常モードでは、UDLD は光ファイバ ポートのファイバ ケーブルが正しく接続されていない場合や、レイヤ 1 のメカニズムによってこの誤接続が検出されない場合に単一方向リンクを検出します。ポートは正しく接続されているにもかかわらずトラフィックが単方向である場合、この状況を検出することになっているリンク 1 メカニズムが単一方向リンクを検出しないため、UDLD は単一方向リンクを検出しません。この場合、論理リンクは不定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、対になっているファイバ ケーブルのどちらかの接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクは存続できません。これは、レイヤ 1 メカニズムがリンクにおける物理的な問題を検出するからです。この場合、UDLD は何も実行せず、論理リンクは不定と見なされます。

アグレッシブ モードでは、UDLD は前記の検出方法を使用して単一方向リンクを検出します。アグレッシブ モードの UDLD は、2 つの装置間の障害発生が許容されないポイントツーポイント リンクの単一方向リンクも検出することができます。また、次のいずれかの問題が発生した場合にも単一方向リンクを検出できます。

- 光ファイバまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバまたはツイストペア リンクで、ポートの 1 つがダウンし、残りのポートがアップ状態になっている。
- ファイバ ケーブルの 1 本が切れている。

このような場合、UDLD は影響のあるポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD hello パケットをハート ビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハート ビートがないことは、双方向リンクを再確立できない限り、リンクはシャットダウンする必要があることを意味しています。

レイヤ 1 の観点から両方のファイバ ケーブルが正常な状態であれば、アグレッシブ モードの UDLD はそれらのファイバ ケーブルが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で行われるので、このチェックは自動ネゴシエーションでは実行されません。

単一方向リンクを検出する方法

UDLD は次の 2 つのメカニズムを使用して動作します。

- ネイバー データベースのメンテナンス

  UDLD は、アクティブなすべてのポートで hello パケット（アドバタイズまたはプローブとも呼ばれる）を定期的に送信して他の UDLD 対応ネイバーについて学習し、各装置がそのネイバーに関する情報を常に維持できるようにします。

  スイッチは hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、その情報をキャッシュします。古いキャッシュ エントリの時間が経過する前に、スイッチが新しい hello メッセージを受信すると、古いエントリは新しいエントリで置き換えられます。

  UDLD 実行中にポートがディセーブルになったり、UDLD がポートでディセーブになったり、またはスイッチがリセットされたりする場合は、UDLD は設定変更の影響を受けるポートの既存のキャッシュ エントリをすべて消去します。UDLD は、少なくとも 1 つのメッセージを送信して、ステータスの変更によって影響を受けるキャッシュの一部を消去するようにネイバーに伝えます。このメッセージはキャッシュの同期を維持するために使用されます。

- イベントドリブン検出とエコー

  UDLD は、検出メカニズムとしてエコーを使用します。UDLD 装置が新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD 装置側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作はすべての UDLD ネイバーで同じであるため、エコーの送信側はエコーの返信を受信するよう待機します。

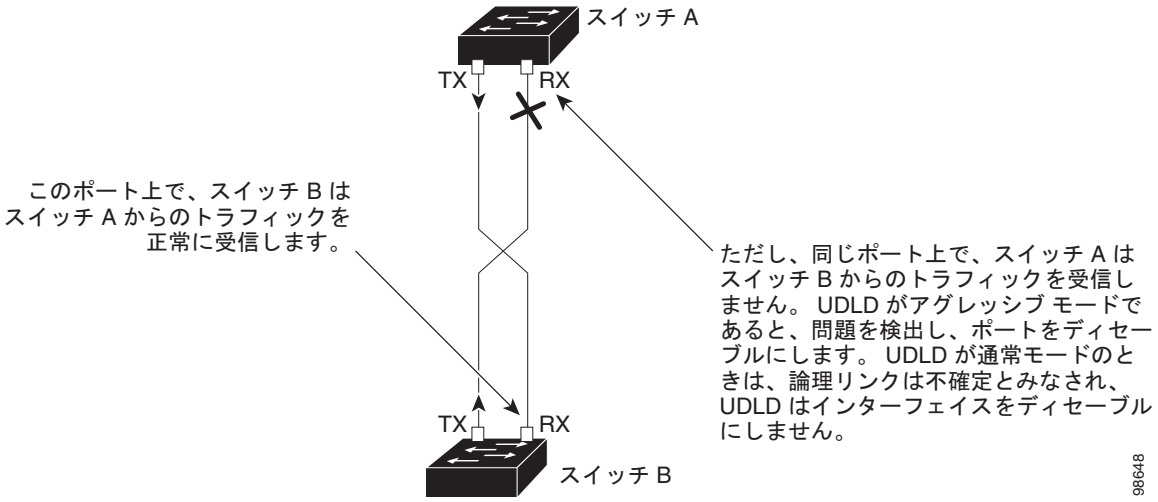
  検出ウィンドウが終了し、有効な返信メッセージを受信しない場合、UDLD モードに応じてリンクがシャットダウンする場合があります。UDLD が通常モードの場合、リンクは不定と見なされて、シャットダウンされない場合があります。UDLD がアグレッシブ モードの場合、リンクは単一方向と見なされて、ポートはディセーブルになります。

通常モードの UDLD がアドバタイズまたは検出フェーズにあり、すべてのネイバーのキャッシュ エントリが期限切れになると、UDLD はリンクアップ シーケンスを再開して、同期されていない可能性のあるネイバーと再同期します。

アグレッシブ モードをイネーブルにしている場合に、ポートのすべてのネイバーがアドバタイズまたは検出フェーズで期限切れになると、UDLD はリンクアップ シーケンスを再開して、同期されていない可能性のあるネイバーと再同期します。メッセージを高速で送受信した後も、リンク ステータスが不定である場合、UDLD はポートをシャットダウンします。

図 33-1 に、単一方向リンク条件の例を示します。

図 33-1　　単一方向リンクの UDLD 検出



UDLD の設定

ここでは、次の設定情報について説明します。

- 「UDLD のデフォルト設定」（P.33-4）
- 「設定時の注意事項」（P.33-4）
- 「UDLD のグローバルなイネーブル化」（P.33-5）
- 「インターフェイスでの UDLD のイネーブル化」（P.33-5）
- 「UDLD でディセーブルにされたインターフェイスのリセット」（P.33-6）

UDLD のデフォルト設定

表 33-1 に、UDLD のデフォルト設定を示します。

表 33-1　UDLD のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ ポートでディセーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX ポートでディセーブル
UDLD アグレッシブ モード	ディセーブル

設定時の注意事項

UDLD 設定時の注意事項を次に示します。

- UDLD は Asynchronous Transfer Mode（ATM; 非同期転送モード）ポートでサポートされません。
- UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合は、このポートは単一方向リンクを検出できません。
- モード（ノーマルまたはアグレッシブ）を設定する場合は、リンクの両端に同じモードが設定されていることを確認してください。

注意　ループ ガードは、ポイントツーポイント リンクでだけ機能します。リンクの両端に、STP を実行している装置を直接接続することを推奨します。

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは通常モードで UDLD をイネーブルにして、スイッチのすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*}	UDLD の動作モードを指定します。 • **aggressive**：すべての光ファイバ ポートで、アグレッシブ モードで UDLD をイネーブルにします。 • **enable**：スイッチのすべての光ファイバ ポートで、通常モードで UDLD をイネーブルにします。UDLD はデフォルトでディセーブルです。 個々のインターフェイス設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定よりも優先されます。 アグレッシブ モードと通常モードの詳細については、「動作モード」（P.33-1）を参照してください。 • **message time** *message-timer-interval*：アドバタイズ フェーズにあり、双方向として検出されたポートでの UDLD プローブ メッセージ間の時間間隔を設定します。指定できる範囲は 1 ～ 90 秒です。デフォルト値は 15 です。 （注）　このコマンドが作用するのは、光ファイバ ポートだけです。他のポート タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。詳細については、「インターフェイスでの UDLD のイネーブル化」（P.33-5）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show udld**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

UDLD をグローバルにディセーブルにするには、**no udld enable** グローバル コンフィギュレーション コマンドを使用して、すべての光ファイバ ポートで通常モードの UDLD をディセーブルにします。すべての光ファイバ ポートでアグレッシブ モードの UDLD をディセーブルにするには、**no udld aggressive** グローバル コンフィギュレーション コマンドを使用します。

インターフェイスでの UDLD のイネーブル化

UDLD をアグレッシブ モードまたは通常モードでイネーブルにするか、ポートで UDLD をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	UDLD をイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**udld port** [**aggressive**]	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポートで、UDLD を通常モードで イネーブルにします。 • **udld port aggressive**：指定されたポートで、UDLD をアグレッシブ モードでイネーブルにします。 **（注）** 指定された光ファイバ ポートで UDLD をディセーブルにするには、**no udld port** インターフェイス コンフィギュレーション コマンドを使用します。 アグレッシブ モードと通常モードの詳細については、「動作モード」（P.33-1）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show udld** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

UDLD でディセーブルにされたインターフェイスのリセット

UDLD でディセーブルにされたすべてのポートをリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**udld reset**	UDLD でディセーブルにされたすべてのポートをリセットします。
ステップ 2	**show udld**	設定を確認します。

また、次のコマンドを使用してポートを復旧できます。

- **shutdown** インターフェイス コンフィギュレーション コマンドの後に **no shutdown** インターフェイス コンフィギュレーション コマンドを指定すると、ディセーブルになったポートが再起動します。
- **no udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを指定すると、ディセーブルになったポートが再度イネーブルになります。
- The **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** [**aggressive**] インターフェイス コンフィギュレーション コマンドを指定すると、ディセーブルになった光ファイバ ポートが再度イネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを指定すると、タイマーが UDLD errdisable ステートから自動的に回復できます。また、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドでは、UDLD errdisable ステートから回復する時間を指定します。

UDLD ステータスの表示

指定したポートまたはすべてのポートの UDLD ステータスを表示するには、**show udld** [*interface-id*] 特権 EXEC コマンドを使用します。

コマンド出力のフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 34

RMON の設定

この章では、IE 3000 スイッチに Remote Network Monitoring（RMON; リモート ネットワーク モニタリング）を設定する手順について説明します。

RMON は RMON 準拠コンソール システムとネットワーク プローブの間で交換できる統計と機能のセットを定義する標準のモニタリング仕様です。RMON は、総合的なネットワーク障害の診断、準備、およびパフォーマンス調整についての情報を提供します。

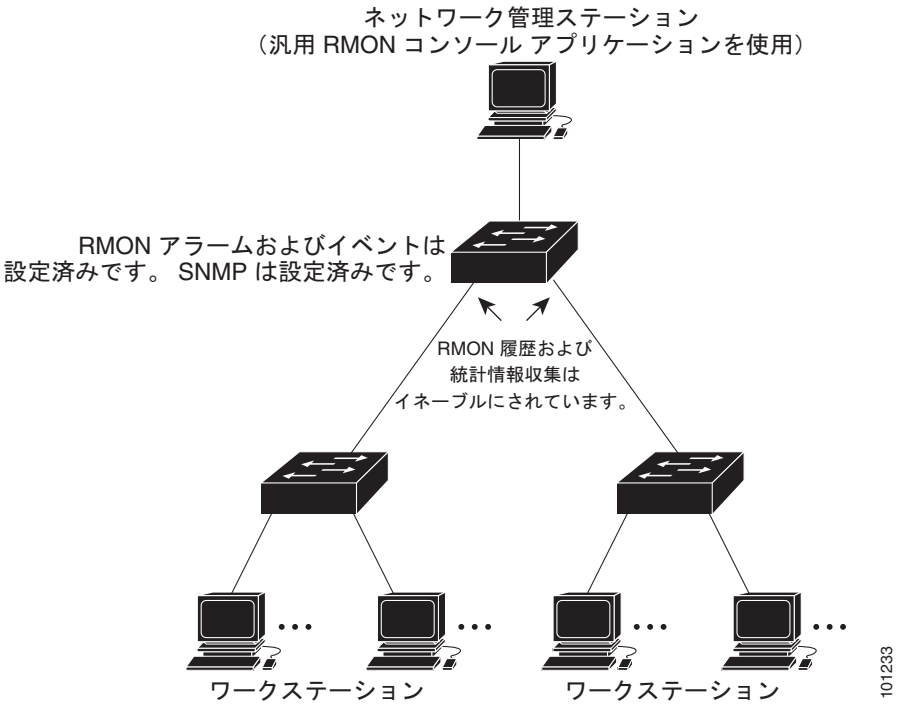
（注） この項で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「System Management Commands」を参照してください。

この章で説明する内容は、次のとおりです。

RMON の概要

RMON は、さまざまなネットワーク エージェントとコンソール システムがネットワーク モニタリング データを交換できるようにする Internet Engineering Task Force（IETF）標準モニタリング仕様です。RMON 機能をスイッチの Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）エージェントとともに使用して、すべての接続されている LAN セグメント上のスイッチ間のトラフィック フローをモニタできます（図 34-1 を参照）。

図 34-1　リモート モニタリングの例



スイッチは次の RMON グループ（RFC 1757 で定義）をサポートします。

- 統計情報（RMON グループ 1）：インターフェイス上でイーサネット統計情報（スイッチ タイプとサポートされているインターフェイスに応じて、ファスト イーサネット統計情報とギガビット イーサネット統計情報）を収集します。
- 履歴（RMON グループ 2）：指定されたポーリング インターバルの間に、イーサネット ポート上の統計情報（スイッチ タイプとサポートされているインターフェイスに応じて、ファスト イーサネット統計情報とギガビット イーサネット統計情報）の履歴グループを収集します。
- アラーム（RMON グループ 3）：指定されたインターバルの間の特定の Management Information Base（MIB; 管理情報ベース）オブジェクトをモニタし、指定の値（上限スレッシュホールド）でアラームをトリガーし、別の値（下限スレッシュホールド）でアラームをリセットします。アラームは、イベントとともに使用できます。アラームは、ログ エントリまたは SNMP トラップを生成できるイベントをトリガーします。
- イベント（RMON グループ 9）：イベントがアラームによってトリガーされる場合に実行するアクションを指定します。アクションによってログ エントリまたは SNMP トラップを生成できます。

このソフトウェア リリースによってサポートされているスイッチは RMON データ処理にハードウェア カウンタを使用するため、モニタリングの効率が向上し、処理のための力はほとんど必要とされません。

（注）　64 ビット カウンタは RMON アラームに対してはサポートされません。

RMON の設定

ここでは、次の設定情報について説明します。

- 「RMON のデフォルト設定」（P.34-3）
- 「RMON アラームとイベントの設定」（P.34-3）（必須）
- 「インターフェイスでのグループ履歴統計情報の収集」（P.34-5）（任意）
- 「インターフェイスでのグループ イーサネット統計情報の収集」（P.34-6）（任意）

RMON のデフォルト設定

RMON はデフォルトではディセーブルになっています。アラームやイベントは設定されません。

RMON アラームとイベントの設定

CLI（コマンドライン インターフェイス）または SNMP 互換のネットワーク管理ステーションを使用して、RMON に対するスイッチを設定できます。汎用 RMON コンソール アプリケーションを使用して、Network Management Station（NMS; ネットワーク管理ステーション）上で RMON ネットワーク管理機能を利用することを推奨します。RMON MIB オブジェクトにアクセスするには、スイッチで SNMP を設定する必要もあります。詳細については、第 36 章「SNMP の設定」を参照してください。

（注）　64 ビット カウンタは RMON アラームに対してはサポートされません。

RMON アラームとイベントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rmon alarm** *number variable interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]	MIB オブジェクトに対するアラームを設定します。 • *number* には、アラーム番号を指定します。指定できる範囲は 1 ～ 65535 です。 • *variable* には、モニタする MIB オブジェクトを指定します。 • *interval* には、アラームが MIB 変数をモニタする時間を秒単位で指定します。指定できる範囲は 1 ～ 4294967295 秒です。 • 各 MIB 変数を直接テストするには、**absolute** キーワードを指定します。MIB 変数のサンプル間での変更をテストするには、**delta** キーワードを指定します。 • *value* には、アラームがトリガーされる数、およびアラームがリセットされるときの数を指定します。上限スレッシュホールドと下限スレッシュホールドの範囲は -2147483648 ～ 2147483647 です。 • （任意）*event-number* には、上限スレッシュホールドまた下限スレッシュホールドがそれぞれの制限を超える場合にトリガーするイベント番号を指定します。 • （任意）**owner** *string* には、アラームのオーナーを指定します。
ステップ 3	**rmon event** *number* [**description** *string*] [**log**] [**owner** *string*] [**trap** *community*]	RMON イベント番号に関連付けられる RMON イベント テーブル内のイベントを追加します。 • *number* には、イベント番号を割り当てます。指定できる範囲は 1 ～ 65535 です。 • （任意）**description** *string* には、イベントの説明を指定します。 • （任意）イベントがトリガーされるときに RMON ログ エントリを生成するには、**log** キーワードを使用します。 • （任意）**owner** *string* には、このイベントのオーナーを指定します。 • （任意）**trap** *community* には、このトラップに使用される SNMP コミュニティ ストリングを入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アラームをディセーブルにするには、設定した各アラームに **no rmon alarm** *number* グローバル コンフィギュレーション コマンドを使用します。設定したすべてのアラームを一度にディセーブルにできません。イベントをディセーブルにするには、**no rmon event** *number* グローバル コンフィギュレーション コマンドを使用します。アラームとイベント、およびそれらがどのように相互作用するかの詳細については、RFC 1757 を参照してください。

任意の MIB オブジェクトに対してアラームを設定できます。次に、**rmon alarm** コマンドを使用して RMON アラーム番号を 10 に設定する例を示します。アラームは、アラームがディセーブルにされるまで MIB 変数 *ifEntry.20.1* を 20 秒ごとに 1 回ずつモニタし、この変数の上昇または下降における変化を確認します。*ifEntry.20.1* 値によって MIB カウンタが、100000 から 100015 に増えるなど、15 以上の幅で増加していることを示す場合は、アラームがトリガーされます。アラームは次に **rmon event** コマンドで設定されているイベント番号 1 をトリガーします。使用できるイベントには、ログ エントリまたは SNMP トラップが含めることができます。*ifEntry.20.1* 値の変更が 0 である場合、アラームはリセットされ、再びトリガーできます。

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0 owner jjohnson
```

次に、**rmon event** コマンドを使用して RMON イベント番号 1 を作成する例を示します。イベントは *High ifOutErrors* として定義され、イベントがアラームによってトリガーされるときにログ エントリを生成します。ユーザ *jjones* は、このコマンドによってイベント テーブル内に作成される行を所有しています。この例は、イベントがトリガーされるときに SNMP トラップも生成します。

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones
```

インターフェイスでのグループ履歴統計情報の収集

収集情報を表示するには、まず RMON アラームとイベントを設定する必要があります。

インターフェイス上のグループ履歴統計情報を収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	履歴を収集するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**rmon collection history** *index* [**buckets** *bucket-number*] [**interval** *seconds*] [**owner** *ownername*]	指定されたバケット数と期間に対する履歴収集をイネーブルにします。 • *index* には、統計情報の RMON グループを指定します。指定できる範囲は 1 ～ 65535 です。 • （任意）**buckets** *bucket-number* には、統計情報の RMON 収集履歴グループに対して必要なバケットの最大数を指定します。指定できる範囲は 1 ～ 65535 です。デフォルトは 50 バケットです。 • （任意）**interval** *seconds* には、各ポーリング サイクルの秒数を指定します。指定できる範囲は 1 ～ 3600 です。デフォルト値は 1800 秒です。 • （任意）**owner** *ownername* には、統計情報の RMON グループのオーナーの名前を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**show rmon history**	スイッチ履歴テーブルの内容を表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

履歴収集をディセーブルにするには、**no rmon collection history** *index* インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスでのグループ イーサネット統計情報の収集

インターフェイス上のグループ イーサネット統計情報を収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	統計情報を収集するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**rmon collection stats** *index* [**owner** *ownername*]	インターフェイス上で RMON 統計情報収集をイネーブルにします。 • *index* には、統計情報の RMON グループを指定します。指定できる範囲は 1 ～ 65535 です。 • （任意）**owner** *ownername* には、統計情報の RMON グループのオーナーの名前を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**show rmon statistics**	スイッチ統計情報テーブルの内容を表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

グループ イーサネット統計情報の収集をディセーブルにするには、**no rmon collection stats** *index* インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、所有者 *root* の RMON 統計情報を収集する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# rmon collection stats 2 owner root
```

RMON ステーテスの表示

RMON ステータスを表示するには、表 34-1 の 1 つまたは複数の特権 EXEC コマンドを使用します。

表 34-1　RMON ステータスを表示するコマンド

コマンド	目的
show rmon	一般的な RMON 統計情報を表示します。
show rmon alarms	RMON アラーム テーブルを表示します。
show rmon events	RMON イベント テーブルを表示します。
show rmon history	RMON 履歴テーブルを表示します。
show rmon statistics	RMON 統計情報テーブルを表示します。

この出力に表示されるフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「System Management Commands」を参照してください。

CHAPTER 35

システム メッセージ ロギングの設定

この章では、IE 3000 スイッチにシステム メッセージ ロギングを設定する方法について説明します。

（注） この章で使用しているコマンドの構文と使用法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。

この章で説明する内容は、次のとおりです。

注意 高レートでコンソールへのメッセージを記録すると、CPU の使用率が高くなり、スイッチの動作に悪影響を与える可能性があります。

システム メッセージ ロギングの概要

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をロギング プロセスに送信します。ロギング プロセスは設定に応じて、ロギング メッセージを各宛先（ログ バッファ、端末回線、UNIX Syslog サーバなど）に配信する処理を制御します。ロギング プロセスは、コンソールにもメッセージを送信します。

（注） Syslog フォーマットは、4.3 BSD UNIX と互換性があります。

ロギング プロセスがディセーブルの場合、メッセージはコンソールだけに送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリース用のシステム メッセージ ガイドを参照してください。

ロギングされたシステム メッセージにアクセスするには、スイッチの CLI（コマンドライン インターフェイス）を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチ ソフトウェアは Syslog メッセージを内部バッファに保存します。

Syslog サーバ上でログを表示したり、Telnet またはコンソール ポート経由でスイッチにアクセスしたりすることによって、システム メッセージをリモートでモニタできます。

システム メッセージ ロギングの設定

ここでは、次の設定情報について説明します。

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字と 1 つのパーセント記号（%）で構成され、設定されている場合にはその前に、オプションのシーケンス番号またはタイムスタンプ情報が付加されます。メッセージは、次のフォーマットで表示されます。

seq no:timestamp: %facility-severity-MNEMONIC:description

パーセント記号の前のメッセージ部分は、**service sequence-numbers**、**service timestamps log datetime**、**service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]、または **service timestamps log uptime** グローバル コンフィギュレーション コマンドの設定によって変わります。

表 35-1 に、Syslog メッセージの要素を示します。

表 35-1　システム ログ メッセージの要素

要素	説明
seq no:	**service sequence-numbers** グローバル コンフィギュレーション コマンドが設定されている場合にだけ、ログ メッセージにシーケンス番号をスタンプします。 詳細については、「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」（P.35-8）を参照してください。
timestamp のフォーマット： *mm/dd hh:mm:ss* または *hh:mm:ss*（短時間） または *d h*（長時間）	メッセージまたはイベントの日時です。**service timestamps log [datetime | log]** グローバル コンフィギュレーション コマンドが設定されている場合にだけ、この情報が表示されます。 詳細については、「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」（P.35-8）を参照してください。
facility	メッセージが参照するファシリティ（SNMP、SYS など）です。サポートされるファシリティのリストについては、表 35-4（P.35-14）を参照してください。
severity	メッセージの重大度を示す 0 ～ 7 の 1 桁のコードです。重大度の詳細については、表 35-3（P.35-10）を参照してください。
MNEMONIC	メッセージを一意に示すテキスト ストリングです。
description	レポートされているイベントの詳細を示すテキスト ストリングです。

次に、スイッチ システム メッセージの一部の例を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

システム メッセージ ロギングのデフォルト設定

表 35-2 に、システム メッセージ ロギングのデフォルト設定を示します。

表 35-2　システム メッセージ ロギングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル
コンソールの重大度	debugging（および数値的により低い重大度。表 35-3（P.35-10）を参照）
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ

表 35-2　システム メッセージ ロギングのデフォルト設定 （続き）

機能	デフォルト設定
タイム スタンプ	ディセーブル
同期ロギング	ディセーブル
ロギング サーバ	ディセーブル
Syslog サーバの IP アドレス	設定なし
設定変更ロガー	ディセーブル
サーバ ファシリティ	local7（表 35-4（P.35-14）を参照）
サーバの重大度	informational（および数値的により低い重大度。表 35-3（P.35-10）を参照）

メッセージ ロギングのディセーブル化

メッセージ ロギングはデフォルトでイネーブルになっています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ロギングをイネーブルにする必要があります。メッセージ ロギングがイネーブルの場合、ログ メッセージはロギング プロセスに送信されます。ロギング プロセスは、メッセージを生成元プロセスとは非同期で指定場所に記録します。

メッセージ ロギングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no logging console**	メッセージ ロギングをディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** または **show logging**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ロギング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ロギング プロセスがディセーブルの場合、メッセージは生成後すぐに（しばしばコマンド出力に割り込む形で）コンソールに表示されます。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、Return を押すまではメッセージが表示されません。詳細については、「ログ メッセージの同期化」（P.35-6）を参照してください。

メッセージ ロギングをディセーブルにしたあとに再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

メッセージ表示宛先装置の設定

メッセージ ロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。メッセージの受信場所を指定するには、特権 EXEC モードで次のコマンドを 1 つまたは複数使用します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging buffered** [*size*]	スイッチの内部バッファにメッセージをロギングします。指定できる範囲は 4096 ～ 2147483647 バイトです。デフォルトのバッファ サイズは 4096 バイトです。 スイッチに障害が発生すると、フラッシュ メモリに保存されていないログ ファイルは失われます。ステップ 4 を参照してください。 **（注）** バッファ サイズを大きすぎる値に設定しないでください。スイッチで他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、**show memory** 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定 *しない* でください。
ステップ 3	**logging** *host*	UNIX Syslog サーバ ホストにメッセージを記録します。 *host* には、Syslog サーバとして使用するホストの名前または IP アドレスを指定します。 ロギング メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。 Syslog サーバの詳細な設定手順については、「UNIX Syslog サーバの設定」（P.35-12）を参照してください。
ステップ 4	**logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]	フラッシュ メモリ内のファイルにログ メッセージを保存します。 • *filename* には、ログ メッセージのファイル名を入力します。 • （任意）*max-file-size* には、ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。デフォルト値は 4096 バイトです。 • （任意）*min-file-size* には、ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。デフォルト値は 2048 バイトです。 • （任意）*severity-level-number* | *type* には、ロギングの重大度またはロギング タイプを指定します。指定できる重大度の範囲は 0 ～ 7 です。ロギング タイプ キーワードのリストについては、表 35-3（P.35-10）を参照してください。デフォルトでは、デバッグ メッセージ、および数値的により低い重大度のメッセージがログ ファイルに送信されます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**terminal monitor**	現在のセッション中に、コンソール以外の端末にメッセージを記録します。 端末パラメータ設定コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。

	コマンド	目的
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

logging buffered グローバル コンフィギュレーション コマンドを実行すると、ロギング メッセージが内部バッファにコピーされます。循環バッファなので、バッファがいっぱいになると、古いメッセージが新しいメッセージで置き換えられます。バッファに記録されたメッセージを表示するには、**show logging** 特権 EXEC コマンドを使用します。バッファ内の最も古いメッセージが最初に表示されます。バッファの内容をクリアするには、**clear logging** 特権 EXEC コマンドを使用します。

特定の Power over Ethernet（PoE）対応ポートで PoE イベントのロギングをイネーブルまたはディセーブルにするには、**logging event power-inline-status** インターフェイス コンフィギュレーション コマンドを使用します。これらのポートでのロギングは、デフォルトでイネーブルです。

コンソールへのロギングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。ファイルへのロギングをディセーブルにするには、**no logging file** [*severity-level-number* | *type*] グローバル コンフィギュレーション コマンドを使用します。

ログ メッセージの同期化

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求装置の出力およびプロンプトと同期させることができます。重大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージが廃棄されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ロギングがイネーブルの場合、送信請求装置出力がコンソールに表示されるか印刷されたあとに、非送信請求装置からの出力が表示または印刷されます。非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力用プロンプトが返されたあとに、コンソールに表示されます。したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求装置出力およびプロンプトに割り込まれることはありません。非送信請求メッセージが表示されたあとに、コンソールはユーザ プロンプトを再表示します。

同期ロギングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number* [*ending-line-number*]	メッセージの同期ロギングを設定する回線を指定します。 • スイッチのコンソール ポートを介して行われる設定には、**console** キーワードを使用します。 • 同期ロギングをイネーブルにする vty 回線を指定するには、**line vty** *line-number* コマンドを使用します。Telnet セッションを介して行われる設定には、vty 接続を使用します。指定できる回線番号の範囲は 0 ～ 15 です。 16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。 **line vty 0 15** また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。 **line vty 2** このコマンドを入力すると、ライン コンフィギュレーション モードになります。
ステップ 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*]	メッセージの同期ロギングをイネーブルにします。 • （任意）**level** *severity-level* には、メッセージの重大度を指定します。重大度がこの値以上であるメッセージは、非同期に出力されます。値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。デフォルト値は 2 です。 • （任意）**level all** を指定すると、重大度に関係なく、すべてのメッセージが非同期に出力されます。 • （任意）**limit** *number-of-buffers* には、キューイングされる端末のバッファ数を指定します。これ以降の新しいメッセージは廃棄されます。指定できる範囲は 0 ～ 2147483647 です。デフォルト値は 20 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

非送信請求メッセージおよびデバッグ出力の同期をディセーブルにするには、**no logging synchronous** [**level** *severity-level* | **all**] [**limit** *number-of-buffers*] ライン コンフィギュレーション コマンドを使用します。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにはタイム スタンプが適用されません。

ログ メッセージのタイム スタンプをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service timestamps log uptime** または **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	ログのタイム スタンプをイネーブルにします。 最初のコマンドを実行するとログ メッセージのタイム スタンプがイネーブルになり、システムを再起動したあとの経過時間を示します。 2 番めのコマンドを実行すると、ログ メッセージのタイム スタンプがイネーブルになります。選択したオプションに応じて、現地の時間帯を基準とした日付、時間（ミリ秒）、時間帯の名前をタイム スタンプに含めることができます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	(任意)設定をコンフィギュレーション ファイルに保存します。

デバッグ メッセージとログ メッセージの両方のタイム スタンプをディセーブルにするには、**no service timestamps** グローバル コンフィギュレーション コマンドを使用します。

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージのタイム スタンプが同じになることがあるため、1 つのメッセージを正確に識別できるように、メッセージにシーケンス番号を表示できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

ログ メッセージのシーケンス番号をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service sequence-numbers**	シーケンス番号をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

シーケンス番号をディセーブルにするには、**no service sequence-numbers** グローバル コンフィギュレーション コマンドを使用します。

次に、シーケンス番号をイネーブルにした場合のロギング表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

メッセージ重大度の定義

メッセージの重大度を指定することにより、選択した装置に表示されるメッセージを制限できます（メッセージの重大度については、表 35-3 を参照してください）。

メッセージの重大度を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging console** *level*	コンソールに記録されるメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低い重大度のメッセージを受信します（表 35-3（P.35-10）を参照）。
ステップ 3	**logging monitor** *level*	端末回線に記録されるメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低い重大度のメッセージを受信します（表 35-3（P.35-10）を参照）。
ステップ 4	**logging trap** *level*	Syslog サーバに記録されるメッセージを制限します。 デフォルトで、Syslog サーバは情報メッセージ、および数値的により低い重大度のメッセージを受信します（表 35-3（P.35-10）を参照）。 Syslog サーバの詳細な設定手順については、「UNIX Syslog サーバの設定」（P.35-12）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** または **show logging**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　*level* を指定すると、その重大度のメッセージおよび数値的により低い重大度のメッセージが宛先に表示されます。

コンソールへのロギングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのロギングをディセーブルにするには、**no logging monitor** グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのロギングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを使用します。

表 35-3 に、*level* キーワードについて説明します。また、対応する UNIX Syslog 定義を、重大度の最も高いものから順に示します。

表 35-3　メッセージ ロギング level キーワード

level キーワード	重大度	説明	Syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	ただちに対処が必要	LOG_ALERT
critical	2	クリティカル	LOG_CRIT
errors	3	エラー	LOG_ERR
warnings	4	警告	LOG_WARNING
notifications	5	正常だが重大な状態	LOG_NOTICE
informational	6	情報メッセージのみ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアは、これ以外に 4 つのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージが、**warnings** から **emergencies** までの重大度で表示されます。これらのタイプのメッセージは、スイッチの機能に影響があることを示します。この誤動作からの回復手順については、このリリースに対応するシステム メッセージ ガイドを参照してください。
- **debug** コマンドの出力が、**debugging** の重大度で表示されます。通常、デバッグ コマンドは Technical Assistance Center（TAC）だけで使用されます。
- インターフェイスのアップまたはダウン移行メッセージおよびシステム再起動メッセージが、**notifications** の重大度で表示されます。このメッセージは単なる情報であり、スイッチの機能には影響がありません。

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

Syslog メッセージ トラップの SNMP ネットワーク管理ステーションへの送信が、**snmp-server enable trap** グローバル コンフィギュレーション コマンドを使用してイネーブルに設定されている場合は、スイッチ履歴テーブルに送信および格納されるメッセージの重大度を変更できます。また、履歴テーブルに格納されるメッセージの数を変更することもできます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、Syslog トラップがイネーブルでない場合も、重大度が **warning** のメッセージ、および数値的により低いメッセージ（表 35-3（P.35-10）を参照）が、履歴テーブルに 1 つ格納されます。

重大度および履歴テーブル サイズのデフォルト値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging history** *level*[1]	履歴ファイルに格納され、SNMP サーバに送信される Syslog メッセージのデフォルトの重大度を変更します。 *level* キーワードのリストについては、表 35-3（P.35-10）を参照してください。 デフォルトでは、**warnings**、**errors**、**critical**、**alerts**、および **emergencies** のメッセージが送信されます。
ステップ 3	**logging history size** *number*	履歴テーブルに格納できる Syslog メッセージ数を指定します。 デフォルトでは 1 つのメッセージが格納されます。指定できる範囲は 0 ～ 500 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

1. 表 35-3 に、level キーワードおよび重大度を示します。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、*emergencies* は 0 ではなく 1 に、*critical* は 2 ではなく 3 になります。

履歴テーブルがいっぱいの場合（**logging history size** グローバル コンフィギュレーション コマンドで指定した最大メッセージ エントリ数が格納されている場合）は、新しいメッセージ エントリを格納できるように、最も古いエントリがテーブルから削除されます。

Syslog メッセージのロギングをデフォルトの重大度に戻すには、**no logging history** グローバル コンフィギュレーション コマンドを使用します。履歴テーブル内のメッセージ数をデフォルト値に戻すには、**no logging history size** グローバル コンフィギュレーション コマンドを使用します。

設定変更ロガーのイネーブル化

CLI（コマンドライン インターフェイス）で行った設定変更を追跡するために設定ロガーをイネーブルにすることができます。**logging enable** 設定変更ロガー コンフィギュレーション コマンドを入力すると、セッション、ユーザ、および設定変更のために入力されたコマンドがログに記録されます。設定ログのサイズは 1 ～ 1000 エントリの間で設定できます（デフォルトは 100）。**no logging enable** コマンドに続けて **logging enable** コマンドを入力して、ロギングをディセーブルにしてから再びイネーブルにすることで、いつでもログをクリアできます。

show archive log config {**all** | *number* [*end-number*] | **user** *username* [**session** *number*] *number* [*end-number*] | **statistics**} [**provisioning**] 特権 EXEC コマンドを使用して、設定ログ全体または指定したパラメータのログを表示します。

デフォルトで設定ロギングはディセーブルになっています。

このコマンドの詳細については、次の URL の『*Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a8086.html#wp1114989

設定ロギングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	archive	アーカイブ コンフィギュレーション モードを開始します。
ステップ 3	**log config**	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ 4	**logging enable**	設定変更ロギングをイネーブルにします。
ステップ 5	**logging size** *entries*	（任意）設定ログに保持するエントリ数を設定します。範囲は 1 ～ 1000 です。デフォルト値は 100 です。 **（注）** 設定ログがいっぱいになると、新規エントリが入力されるたびに最も古いログ エントリが削除されます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show archive log config**	設定ログを表示して設定を確認します。

次に、設定変更ロガーをイネーブルにして、ログのエントリ数を 500 に設定する例を示します。

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

設定ログの出力例は次のとおりです。

```
Switch# show archive log config all
 idx   sess           user@line      Logged command
   38    11   unknown user@vty3     |no aaa authorization config-commands
   39    12   unknown user@vty3     |no aaa authorization network default group radius
   40    12   unknown user@vty3     |no aaa accounting dot1x default start-stop group
radius
   41    13   unknown user@vty3     |no aaa accounting system default
   42    14           temi@vty4     |interface GigabitEthernet4/0/1
   43    14           temi@vty4     | switchport mode trunk
   44    14           temi@vty4     | exit
   45    16           temi@vty5     |interface FastEthernet5/0/1
   46    16           temi@vty5     | switchport mode trunk
   47    16           temi@vty5     | exit
```

UNIX Syslog サーバの設定

次に、UNIX サーバの Syslog デーモンを設定し、UNIX システム ロギング ファシリティを定義する方法を説明します。

UNIX Syslog デーモンへのメッセージ ロギング

システム ログ メッセージを UNIX Syslog サーバに送信するには、事前に UNIX サーバ上で Syslog デーモンを設定しておく必要があります。この手順は任意です。

root としてログインし、次の手順を実行します。

（注）　最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。このようなシステムの場合は、Syslog メッセージのリモート ロギングをイネーブルにするために Syslog コマンドラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

ステップ 1　/etc/syslog.conf ファイルに次のような 1 行を追加します。

```
local7.debug /usr/adm/logs/cisco.log
```

local7 キーワードは、使用するロギング ファシリティを指定します。ファシリティの詳細については、表 35-4（P.35-14）を参照してください。**debug** キーワードは、Syslog の重大度を指定します。重大度の詳細については、表 35-3（P.35-10）を参照してください。Syslog デーモンは、これ以上の重大度の場合に、次のフィールドで指定されたファイルにメッセージを送信します。このファイルは、Syslog デーモンに書き込み権限がある既存ファイルでなければなりません。

ステップ 2　UNIX シェル プロンプトに次のコマンドを入力して、ログ ファイルを作成します。

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

ステップ 3　Syslog デーモンに新しい設定を認識させます。

```
$ kill -HUP `cat /etc/syslog.pid`
```

詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

UNIX システム ロギング ファシリティの設定

システム ログ メッセージを外部装置に送信する場合は、メッセージを UNIX Syslog ファシリティから送信されたメッセージとして特定するようにスイッチを設定できます。

UNIX システム ファシリティ メッセージ ロギングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging** *host*	IP アドレスを入力して、UNIX Syslog サーバ ホストにメッセージを記録します。 ロギング メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。

	コマンド	目的
ステップ 3	**logging trap** *level*	Syslog サーバに記録されるメッセージを制限します。 デフォルトでは、Syslog サーバは情報メッセージおよびそれ以下のメッセージを受信します。*level* キーワードについては、表 35-3（P.35-10）を参照してください。
ステップ 4	**logging facility** *facility-type*	Syslog ファシリティを設定します。*facility-type* キーワードについては、表 35-4（P.35-14）を参照してください。 デフォルトは **local7** です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

Syslog サーバを削除するには、**no logging** *host* グローバル コンフィギュレーション コマンドを使用して、Syslog サーバの IP アドレスを指定します。Syslog サーバへのロギングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを入力します。

表 35-4 に、ソフトウェアでサポートされている UNIX システム ファシリティを示します。これらのファシリティの詳細については、ご使用の UNIX オペレーティング システムの操作マニュアルを参照してください。

表 35-4　ロギング facility-type キーワード

facility-type キーワード	説明
auth	許可システム
cron	cron ファシリティ
daemon	システム デーモン
kern	カーネル
local0 ～ local7	ローカルに定義されたメッセージ
lpr	ライン プリンタ システム
mail	メール システム
news	USENET ニュース
sys9 ～ sys14	システムで使用
syslog	システム ログ
user	ユーザ プロセス
uucp	UNIX-to-UNIX コピー システム

ロギング設定の表示

ロギング設定およびログ バッファの内容を表示するには、**show logging** 特権 EXEC コマンドを使用します。この場合に表示されるフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。

CHAPTER 36

SNMP の設定

この章では、IE 3000 スイッチに Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を設定する方法について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスおよび『*Cisco IOS Network Management Command Reference, Release 12.4*』を参照してください。
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

SNMP の概要

SNMP は、マネージャとエージェントの間の通信のメッセージのフォーマットを提供する、アプリケーション層のプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および Management Information Base（MIB; 管理情報ベース）で構成されます。SNMP マネージャは、CiscoWorks などの Network Management System（NMS; ネットワーク管理システム）に統合できます。エージェントと MIB はスイッチ上に存在します。スイッチで SNMP を設定するには、マネージャとエージェントの関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、装置パラメータやネットワーク データに関する情報のリポジトリである MIB から値を収集します。エージェントは、マネージャからのデータの取得要求または設定要求に応答することもできます。

また、非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上の特定の状態を SNMP マネージャに通知するメッセージです。トラップは、不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントを意味する場合があります。

ここでは、次の概念情報について説明します。

SNMP のバージョン

このソフトウェア リリースでは、SNMP の次のバージョンをサポートしています。

- SNMPv1：RFC 1157 に規定されている簡易ネットワーク管理プロトコル（完全インターネット標準）。
- SNMPv2C は、SNMPv2Classic のバルク取得機能を引き継ぎ、エラー処理を改善したうえで、SNMPv2Classic のパーティベースの管理およびセキュリティ フレームワークをコミュニティストリングベースの管理フレームワークに置き換えたものです。SNMPv2C には次の機能があります。
  - SNMPv2：RFC 1902 ～ 1907 に規定されている簡易ネットワーク管理プロトコルのバージョン 2（ドラフト版インターネット標準）。
  - SNMPv2C：RFC 1901 に規定されている SNMPv2 のコミュニティストリングベースの管理フレームワーク（試験版インターネット プロトコル）。
- SNMPv3：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に規定されている相互運用可能な標準ベース プロトコルです。SNMPv3 は、ネットワーク上のパケットを認証および暗号化することで装置へのセキュアなアクセスを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
  - メッセージの完全性：パケットが送信中に改ざんされないようにします。
  - 認証：メッセージの送信元が有効かどうかを判別します。
  - 暗号化：パッケージの内容を混合して、許可されていない送信元が読み取ることができないようにします。

（注）　暗号化を選択するには、**priv** キーワードを入力します。このキーワードは、暗号化ソフトウェア イメージがインストールされている場合にだけ使用できます。

SNMPv1 と SNMPv2C は、どちらもコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレスの Access Control List（ACL; アクセス制御リスト）およびパスワードによって定義されます。

SNMPv2C は、バルク取得メカニズムと、より詳細なエラー メッセージを管理ステーションに報告する機能を備えています。バルク取得メカニズムは、テーブルや大量の情報を取得し、必要な往復回数を最小限に抑えます。SNMPv2C では、エラー処理機能が改善され、さまざまな種類のエラー状態を区別する拡張エラー コードが使用されています。これらの状態は、SNMPv1 では単一のエラー コードで報告されます。SNMPv2 では、エラー リターン コードでエラー タイプが報告されます。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティ レベルは、セキュリティ モデル内で許可されたセキュリティのレベルです。セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを処理するときに使用されるセキュリティ メカニズムが決まります。使用可能なセキュリティ モデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

表 36-1 に、セキュリティ モデルとセキュリティ レベルのさまざまな組み合わせについて、その特性を示します。

表 36-1　SNMP のセキュリティ モデルとセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	不可	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	不可	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	ユーザ名	不可	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	不可	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。
SNMPv3	authPriv（暗号化ソフトウェア イメージが必要）	MD5 または SHA	データ暗号化規格（DES）または高度暗号化規格（AES）	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。次の暗号化アルゴリズムを使用する User-based Security Model（USM）を指定できます。 • CBC-DES（DES-56）規格に基づく認証および DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット、192 ビット、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるので、SNMPv1、SNMPv2C、および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP マネージャ機能

SNMP マネージャは、MIB の情報を使用して、表 36-2 に示す動作を実行します。

表 36-2　SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[1]
get-bulk-request[2]	テーブルの複数の行など、大きいデータ ブロックを取得します。通常、このようなデータは、小さい多数のデータ ブロックに分割して送信する必要があります。
get-response	NMS から送信される get-request、get-next-request、および set-request に応答します。
set-request	特定の変数に値を格納します。
trap	イベントの発生時に SNMP エージェントから SNMP マネージャに送信される非送信請求メッセージです。

1. この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
2. **get-bulk** コマンドを使用できるのは、SNMPv2 以降だけです。

SNMP エージェント機能

SNMP エージェントは、次のように SNMP マネージャの要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、その値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

また、エージェントで重要なイベントが発生したことを NMS に通知するために、非送信請求トラップ メッセージを送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニング ツリー トポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするためには、NMS のコミュニティ ストリング定義が、スイッチ上の 3 つのコミュニティ ストリング定義の少なくとも 1 つに一致する必要があります。

コミュニティ ストリングには、次の 3 つの属性のいずれかを指定できます。

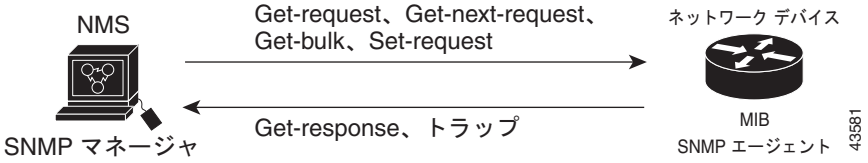
- 読み取り専用（RO）：許可された管理ステーションに対して、コミュニティ ストリングを除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- 読み書き（RW）：許可された管理ステーションに対して、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ ストリングへのアクセスは許可しません。
- クラスタを作成すると、メンバー スイッチと SNMP アプリケーション間のメッセージ交換がコマンド スイッチによって管理されます。Network Assistant ソフトウェアは、コマンド スイッチ上で最初に設定された RW コミュニティ ストリングと RO コミュニティ ストリングにメンバー スイッチ番号（*@esN*、*N* はスイッチ番号）を追加し、これらのストリングをメンバー スイッチに伝播します。詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com の『*Getting Started with Cisco Network Assistant*』を参照してください。

SNMP による MIB 変数へのアクセス

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、スイッチの MIB 変数を使用して装置変数を設定し、ネットワーク上の装置をポーリングして特定の情報を取得します。ポーリングの結果は、グラフで表示できます。この結果を解析して、インターネットワーキングに関する問題のトラブルシューティング、ネットワーク パフォーマンスの向上、装置の設定確認、トラフィック負荷のモニタなどを行うことができます。

図 36-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャにトラップ（特定のイベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス追跡など、ネットワーク上の状況を SNMP マネージャに通知します。また、SNMP エージェントは、*get-request*、*get-next-request*、および *set-request* の形式で SNMP マネージャから送信される MIB 関連のクエリーに応答します。

図 36-1　SNMP ネットワーク



サポートされる MIB の詳細、および MIB へのアクセス方法については、付録 A「サポートされる MIB」を参照してください。

SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない場合、キーワード *traps* はトラップか情報、またはその両方を表します。SNMP 通知をトラップとして送信するか情報として送信するかを指定するには、**snmp-server host** コマンドを使用します。

（注）　SNMPv1 は情報をサポートしません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうか送信側にはわからないためです。情報要求の場合、受信した SNMP マネージャは SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）でメッセージに確認応答します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップよりも意図した宛先に届く可能性が高くなります。

ただし、この特性によって、情報の方がトラップよりも信頼性が高くなる一方で、スイッチおよびネットワークで消費されるリソースが多くなります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなります。したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信する必要がある場合は、情報要求を使用してください。ネットワーク上またはスイッチのメモリ上のトラフィックが問題になる場合で、通知が不要なときは、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

NMS では、IF-MIB によって、インターフェイス インデックス（ifIndex）オブジェクト値の生成および割り当てを行います。このオブジェクト値は、物理インターフェイスまたは論理インターフェイスを識別するゼロより大きい一意の値です。スイッチの再起動またはスイッチのソフトウェアのアップグレード時、インターフェイスに対してこれと同じ値が使用されます。たとえば、スイッチのポート 2 に 10003 という ifIndex 値が割り当てられている場合、スイッチの再起動後も同じ値が使用されます。

スイッチでは、表 36-3 のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

表 36-3　ifIndex 値

インターフェイス タイプ	ifIndex の範囲
SVI[1]	1 ～ 4999
EtherChannel	5000 ～ 5012
ループバック	5013 ～ 5077
トンネル	5078 ～ 5142
物理（ギガビット イーサネットまたは SFP[2] モジュール インターフェイス）	10000 ～ 14500
ヌル	14501

1. SVI = Switch Virtual Interface（スイッチ仮想インターフェイス）
2. SFP = Small Form-Factor Pluggable（着脱可能小型フォーム ファクタ）

（注）　範囲内の連続した値が使用されるとは限りません。

SNMP の設定

SNMP のデフォルト設定

表 36-4 に、SNMP のデフォルト設定を示します。

表 36-4　SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル[1]。
SNMP トラップ レシーバー	設定なし。
SNMP トラップ	TCP 接続のトラップ（**tty**）以外は、イネーブルではありません。
SNMP バージョン	**version** キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで **noauth**（noAuthNoPriv）になります。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

1. スイッチを起動したときにスタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

スイッチを起動したときに、スイッチのスタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが少なくとも 1 つ設定されていると、SNMP エージェントはイネーブルになります。

SNMP *グループ*は、SNMP ユーザを SNMP ビューにマッピングするテーブルです。SNMP *ユーザ*は、SNMP グループのメンバーです。SNMP *ホスト*は、SNMP トラップ動作の受信側です。SNMP *エンジン ID* は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP の設定時は、次の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しないでください。**snmp-server host** グローバル コンフィギュレーション コマンドによって、ユーザの通知ビューが自動生成され、そのユーザに関連付けられているグループに追加されます。グループの通知ビューを変更すると、そのグループに関連付けられているすべてのユーザが影響を受けます。通知ビューを設定する必要がある場合の詳細については、『*Cisco IOS Network Management Command Reference*』を参照してください。
- リモート ユーザを設定する場合は、ユーザが存在する装置のリモート SNMP エージェントに対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。リモート エージェントの SNMP エンジン ID とユーザ パスワードを使用して、認証およびプライバシ ダイジェストが算出されます。あらかじめリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときは、プロキシ要求または情報の送信先となるリモート エージェントの SNMP エンジン ID を SNMP データベースに設定する必要があります。
- ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）認証レベルの情報を送信しません。

- SNMP エンジン ID の値を変更すると、重大な影響が生じます。コマンドラインで入力されたユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 または SHA のセキュリティ ダイジェストに変換されます。コマンドラインのパスワードは、RFC 2274 の規定に従って破棄されます。この破棄により、エンジン ID の値を変更した場合は、SNMPv3 ユーザのセキュリティ ダイジェストが無効となるので、**snmp-server user** *username* グローバル コンフィギュレーション コマンドを使用して SNMP ユーザを再設定する必要があります。同様の理由から、エンジン ID を変更した場合は、コミュニティ ストリングも再設定する必要があります。

SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no snmp-server**	SNMP エージェントの動作をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

no snmp-server グローバル コンフィギュレーション コマンドを使用すると、装置上で稼動しているすべてのバージョン（バージョン 1、バージョン 2C、およびバージョン 3）がディセーブルになります。SNMP をイネーブルにする特定の Cisco IOS コマンドはありません。最初に入力する **snmp-server** グローバル コンフィギュレーション コマンドによって、SNMP のすべてのバージョンがイネーブルになります。

コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、スイッチ上のエージェントへのアクセスを許可するパスワードと同様に機能します。任意で、ストリングに関連付けられる次の特性を 1 つまたは複数指定できます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティがアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティがアクセスできる MIB オブジェクトに対する読み書き権限または読み取り専用権限

スイッチでコミュニティ ストリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*]	コミュニティ ストリングを設定します。 **（注）** @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定するとき、@ 記号を SNMP コミュニティ ストリングの一部として使用しないでください。 • *string* には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 • （任意）**view** には、コミュニティがアクセスできるビュー レコードを指定します。 • （任意）許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用（**ro**）を指定し、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き（**rw**）を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 • （任意）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 までの標準 IP アクセス リスト番号を入力します。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	（任意）ステップ 2 で標準 IP アクセス リスト番号を指定し、そのあとにリストを作成する場合は、必要に応じてコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注） SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します（コミュニティ ストリングに値を入力しないでください）。

特定のコミュニティ ストリングを削除するには、**no snmp-server community** *string* グローバル コンフィギュレーション コマンドを使用します。

次に、ストリング *comaccess* を SNMP に割り当て、読み取り専用アクセスを許可して、IP アクセス リスト 4 がこのコミュニティ ストリングを使用してスイッチの SNMP エージェントにアクセスできるように指定する例を示します。

```
Switch(config)# snmp-server community comaccess ro 4
```

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモートの SNMP サーバ エンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする SNMP サーバ グループを設定し、その SNMP グループに新しいユーザを追加することができます。

スイッチで SNMP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}	SNMP のローカル コピーまたはリモート コピーの名前を設定します。 • *engineid-string* は、SNMP のコピーの名前を指定する 24 文字の ID ストリングです。後続ゼロがある場合は、24 文字のエンジン ID 全体を指定する必要はありません。指定するのは、エンジン ID のうち、末尾までゼロだけが続く箇所を除いた部分だけです。たとえば、123400000000000000000000 というエンジン ID を設定する場合、次のように入力できます。 **snmp-server engineID local 1234** • **remote** を指定した場合は、SNMP のリモート コピーが置かれている装置の *ip-address* を指定し、任意でリモート装置の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポートを指定します。デフォルト値は 162 です。

	コマンド	目的
ステップ 3	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	リモート装置に新しい SNMP グループを設定します。 • *groupname* には、グループの名前を指定します。 • セキュリティ モデルを指定します。 – **v1** は、最も安全性の低いセキュリティ モデルです。 – **v2c** は、2 番めに安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を伝送できます。 – **v3** は最も安全なセキュリティ モデルで、認証レベルを選択する必要があります。 **auth**：Message Digest 5（MD5）および Secure Hash Algorithm（SHA）によるパケット認証をイネーブルにします。 **noauth**：noAuthNoPriv というセキュリティ レベルをイネーブルにします。キーワードを指定しなかった場合、この値がデフォルトになります。 **priv**：Data Encryption Standard（DES; データ暗号化規格）によるパケット暗号化（別名、*プライバシ*）をイネーブルにします。 **（注）** **priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合にだけ使用できます。 • （任意）**read** *readview* とともに、エージェントの内容の表示だけ可能なビューの名前を表すストリング（64 文字以下）を入力します。 • （任意）**write** *writeview* とともに、データの入力とエージェントの内容の設定を行うビューの名前を表すストリング（64 文字以下）を入力します。 • （任意）**notify** *notifyview* とともに、通知、情報、またはトラップを指定するビューの名前を表すストリング（64 文字以下）を入力します。 • （任意）**access** *access-list* とともに、アクセス リストの名前を表すストリング（64 文字以下）を入力します。

	コマンド	目的
ステップ 4	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]} [*priv* {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]	SNMP グループの新しいユーザを追加します。 • *username* は、エージェントに接続するホスト上のユーザの名前です。 • *groupname* は、ユーザを関連付けるグループの名前です。 • **remote** を入力して、ユーザが属するリモート SNMP エンティティ、そのエンティティのホスト名または IP アドレス、さらに任意で UDP ポート番号を指定します。デフォルト値は 162 です。 • SNMP バージョン番号（**v1**、**v2c**、または **v3**）を入力します。**v3** を入力する場合は、次のオプションを追加します。 – **encrypted** は、パスワードを暗号化形式で表示することを指定します。このキーワードは、**v3** キーワードが指定されている場合にだけ使用できます。 – **auth** は認証レベル設定セッションで、HMAC-MD5-96（**md5**）または HMAC-SHA-96（**sha**）認証レベルを指定できます。このオプションにはパスワード ストリング *auth-password*（64 文字以下）が必要です。 • **v3** を入力する場合、スイッチで暗号化ソフトウェア イメージが実行されているときは、プライベート（**priv**）暗号化アルゴリズムおよびパスワード ストリング *priv-password*（64 文字以下）を設定することもできます。 – **priv** は、User-based Security Model（USM）を指定します。 – **des** は、56 ビット DES アルゴリズムの使用を指定します。 – **3des** は、168 ビット DES アルゴリズムの使用を指定します。 – **aes** は、DES アルゴリズムの使用を指定します。128 ビット、192 ビット、または 256 ビットの暗号化を選択する必要があります。 • （任意）**access** *access-list* とともに、アクセス リストの名前を表すストリング（64 文字以下）を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。 **（注）** **auth** | **noauth** | **priv** のモード設定に関する SNMPv3 情報を表示するには、**show snmp user** 特権 EXEC コマンドを入力する必要があります。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにスイッチで生成されるシステム アラートです。デフォルトでは、トラップ マネージャは定義されておらず、トラップは送信されません。この Cisco IOS リリースが稼動しているスイッチでは、設定できるトラップ マネージャの数に制限はありません。

（注）　コマンド構文で *traps* という単語を使用するコマンドは多数あります。トラップまたは情報を選択するオプションがコマンドにない場合、キーワード **traps** はトラップか情報、またはその両方を表します。SNMP 通知をトラップとして送信するか情報として送信するかを指定するには、**snmp-server host** グローバル コンフィギュレーション コマンドを使用します。

表 36-5 に、サポートされているスイッチ トラップ（通知タイプ）を示します。これらのトラップのいずれかまたはすべてをイネーブルにして、そのトラップを受信するようにトラップ マネージャを設定できます。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr* **informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

表 36-5　スイッチの通知タイプ

通知タイプのキーワード	説明
bgp	Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ステート変更トラップを生成します。このオプションは、Enhanced Multilayer Image（EMI）がインストールされている場合にだけ使用できます。
bridge	Spanning Tree Protocol（STP; スパニング ツリー プロトコル）ブリッジ MIB トラップを生成します。
cluster	クラスタ設定が変更されたときに、トラップを生成します。
config	SNMP 設定が変更されたときに、トラップを生成します。
copy-config	SNMP コピー設定が変更されたときに、トラップを生成します。
entity	SNMP エンティティが変更されたときに、トラップを生成します。
cpu threshold	CPU に関連したトラップを許可します。
envmon	環境モニタ トラップを生成します。ファン、シャットダウン、ステータス、電源、温度の環境トラップのいずれかまたはすべてをイネーブルにすることができます。
errdisable	ポート VLAN が errdisable ステートになったときに、トラップを生成します。1 分あたりの最大トラップ レートも設定できます。指定できる範囲は 0 ～ 10000 です。デフォルト値は 0 で、レート制限がないことを意味します。
flash	SNMP FLASH 通知を生成します。
hsrp	Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）が変更されたときに、トラップを生成します。
ipmulticast	IP マルチキャスト ルーティングが変更されたときに、トラップを生成します。
mac-notification	MAC アドレス通知トラップを生成します。
msdp	Multicast Source Discovery Protocol（MSDP）が変更されたときに、トラップを生成します。
ospf	Open Shortest Path First（OSPF）が変更されたときに、トラップを生成します。シスコ固有、エラー、リンクステート アドバタイズ、レート制限、再送信、ステート変更のトラップのいずれかまたはすべてをイネーブルにすることができます。
pim	Protocol-Independent Multicast（PIM）が変更されたときに、トラップを生成します。無効な PIM メッセージ、ネイバー変更、Rendezvous Point（RP; ランデブー ポイント）マッピング変更のトラップのいずれかまたはすべてをイネーブルにすることができます。

表 36-5　スイッチの通知タイプ （続き）

通知タイプのキーワード	説明
port-security	SNMP ポート セキュリティ トラップを生成します。1 秒あたりの最大トラップ レートも設定できます。指定できる範囲は 0 ～ 1000 です。デフォルト値は 0 で、レート制限がないことを意味します。 （注）　通知タイプ **port-security** を使用してトラップを設定する場合は、まずポート セキュリティ トラップを設定し、次に以下のポート セキュリティ トラップ レートを設定します。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate** *rate*
rtr	SNMP Response Time Reporter（RTR）トラップを生成します。
snmp	認証、コールド スタート、ウォーム スタート、リンクアップ、リンクダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 分あたりの最大トラップ レートも設定できます。指定できる範囲は 0 ～ 1000 です。デフォルト値は 0 です（制限はなく、トラップは発生するたびに送信されます）。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP Syslog トラップを生成します。
tty	TCP 接続のトラップを生成します。このトラップはデフォルトでイネーブルになっています。
vlan-membership	SNMP VLAN メンバーシップが変更されたときに、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）が変更されたときに、トラップを生成します。

（注）　**fru-ctrl**、**insertion**、および **removal** の各キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

表 36-5 に示す通知タイプを受信する場合は、特定のホストに対して **snmp-server host** グローバル コンフィギュレーション コマンドを使用できます。

ホストにトラップまたは情報を送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server engineID remote** *ip-address engineid-string*	リモート ホストのエンジン ID を指定します。
ステップ 3	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]}	ステップ 2 で作成したリモート ホストに関連付ける SNMP ユーザを設定します。 （注）　アドレスに対応するリモート ユーザを設定するには、あらかじめリモート ホストのエンジン ID を設定しておく必要があります。設定していない場合、エラー メッセージが表示され、コマンドが実行されません。

	コマンド	目的
ステップ 4	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	SNMP グループを設定します。
ステップ 5	**snmp-server host** *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [*notification-type*]	SNMP トラップ動作の受信側を指定します。 • *host-addr* には、ホスト（対象となる受信側）の名前またはインターネット アドレスを指定します。 • （任意）SNMP 情報をホストに送信するには、**informs** を入力します。 • （任意）SNMP トラップをホストに送信するには、**traps**（デフォルト）を入力します。 • （任意）SNMP **version**（**1**、**2c**、または **3**）を指定します。SNMPv1 は情報をサポートしません。 • （任意）バージョン 3 の場合、認証レベルとして **auth**、**noauth**、または **priv** を選択します。 **（注）** **priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合にだけ使用できます。 • *community-string* には、**version 1** または **version 2c** を指定した場合は、通知処理で送信されるパスワードと類似したコミュニティ ストリングを入力します。**version 3** を指定した場合は、SNMPv3 ユーザ名を入力します。 **（注）** @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定するとき、@ 記号を SNMP コミュニティ ストリングの一部として使用しないでください。 • （任意）*notification-type* には、表 36-5（P.36-13）に示されているキーワードを使用します。タイプが指定されていない場合、すべての通知が送信されます。
ステップ 6	**snmp-server enable traps** *notification-types*	トラップまたは情報を送信するようにスイッチでイネーブルにし、送信する通知タイプを指定します。通知タイプの一覧については、表 36-5（P.36-13）を参照するか、**snmp-server enable traps ?** と入力してください。 複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。 **（注）** 通知タイプ **port-security** を使用してトラップを設定する場合は、まずポート セキュリティ トラップを設定し、次に以下のポート セキュリティ トラップ レートを設定します。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate** *rate*
ステップ 7	**snmp-server trap-source** *interface-id*	（任意）送信元インターフェイスを指定します。そのインターフェイスから、トラップ メッセージに対応する IP アドレスが取得されます。情報の送信元 IP アドレスも、このコマンドで設定します。
ステップ 8	**snmp-server queue-length** *length*	（任意）各トラップ ホストのメッセージ キューの長さを設定します。指定できる範囲は 1 ～ 1000 です。デフォルト値は 10 です。
ステップ 9	**snmp-server trap-timeout** *seconds*	（任意）トラップ メッセージを再送信する頻度を設定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 30 秒です。

	コマンド	目的
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	設定を確認します。 （注）　**auth** | **noauth** | **priv** のモード設定に関する SNMPv3 情報を表示するには、**show snmp user** 特権 EXEC コマンドを入力する必要があります。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

snmp-server host コマンドは、通知を受信するホストを指定します。**snmp-server enable trap** コマンドは、指定された通知（トラップおよび情報）のメカニズムをグローバルにイネーブルにします。ホストが情報を受信できるようにするには、そのホストについて **snmp-server host informs** コマンドを設定し、**snmp-server enable traps** コマンドを使用して情報をグローバルにイネーブルにする必要があります。

指定したホストがトラップを受信しないようにするには、**no snmp-server host** *host* グローバル コンフィギュレーション コマンドを使用します。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** グローバル コンフィギュレーション コマンドを使用します。特定のトラップ タイプをディセーブルにするには、**no snmp-server enable traps** *notification-types* グローバル コンフィギュレーション コマンドを使用します。

CPU スレッシュホールドの通知タイプと値の設定

CPU スレッシュホールドの通知タイプと値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**process cpu threshold type** {**total** | **process** | **interrupt**} **rising** *percentage* **interval** *seconds* [**falling** *fall-percentage* **interval** *seconds*]	CPU スレッシュホールドの通知タイプと値を設定します。 • **total**：CPU 総使用率に対する通知タイプを設定します。 • **process**：CPU プロセス使用率に対する通知タイプを設定します。 • **interrupt**：CPU 割り込み率に対する通知タイプを設定します。 • **rising** *percentage*：CPU リソースのパーセント値（1 ～ 100）を指定します。設定した期間この値を上回ると、CPU スレッシュホールドの通知が送信されます。 • **interval** *seconds*：CPU スレッシュホールド超過の期間を秒単位（5 ～ 86400）で指定します。超過期間がこの値に達すると、CPU スレッシュホールドの通知が送信されます。 • **falling** *fall-percentage*：CPU リソースのパーセント値（1 ～ 100）を指定します。設定した期間使用率がこの値を下回ると、CPU スレッシュホールドの通知が送信されます。 この値は、**rising** *percentage* 値以下にする必要があります。**falling** *fall-percentage* 値は、指定しない場合、**rising** *percentage* 値と同じになります。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

エージェント コンタクトおよびロケーションに関する情報の設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server contact** *text*	システム コンタクトを表すストリングを設定します。 次に例を示します。 `snmp-server contact Dial System Operator at beeper 21555.`
ステップ 3	**snmp-server location** *text*	システム ロケーションを表すストリングを設定します。 次に例を示します。 `snmp-server location Building 3/Room 222`
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SNMP を介して使用する TFTP サーバの制限

SNMP を介してコンフィギュレーション ファイルを保存およびロードするために使用する Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバを、アクセス リストに指定されているサーバに限定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server tftp-server-list** *access-list-number*	SNMP を介してコンフィギュレーション ファイルをコピーするために使用する TFTP サーバを、アクセス リスト内のサーバに限定します。 *access-list-number* には、1 ～ 99 および 1300 ～ 1999 までの標準 IP アクセス リスト番号を入力します。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルド カード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用してすべてのオブジェクトに読み取り専用権限でアクセスできます。また、スイッチはトラップを送信しません。

```
Switch(config)# snmp-server community public
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用してすべてのオブジェクトに読み取り専用権限でアクセスする例を示します。スイッチは、SNMPv1 を使用してホスト 192.180.1.111 とホスト 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に VTP トラップを送信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバーに対して、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証失敗トラップは、コミュニティ ストリング *public* を使用して SNMPv2C からホスト *cisco.com* に送信されます。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されます。1 行目は、すでにイネーブルに設定されているトラップに加えて、エンティティ MIB トラップを送信するようにスイッチをイネーブルにします。2 行目は、これらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の **snmp-server host** コマンドを上書きします。

```
Switch(config)# snmp-server enable traps entity
```

```
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザをリモート ホストに関連付け、ユーザがグローバル コンフィギュレーション モードになったときに **auth**（authNoPriv）認証レベルの情報を送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

SNMP ステータスの表示

不正なコミュニティ ストリング エントリ、エラー、要求された変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。また、表 36-6 に示すその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。表示されるフィールドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

表 36-6　SNMP 情報を表示するためのコマンド

機能	デフォルト設定
show snmp	SNMP 統計情報を表示します。
show snmp engineID [**local** | **remote**]	装置に設定されているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求に関する情報を表示します。
show snmp sessions	現在の SNMP セッションに関する情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 （注）　**auth** | **noauth** | **priv** のモードについて SNMPv3 設定情報を表示するには、このコマンドを使用する必要があります。この情報は、**show running-config** の出力には表示されません。

CHAPTER 37

Embedded Event Manager の設定

Embedded Event Manager（EEM）は、Cisco IOS 装置内でイベントの検出と回復を行うための分散型のカスタマイズされた方法です。EEM には、イベントをモニタし、モニタ対象のイベントが発生するかスレッシュホールドに達した場合に通知や修正などの EEM アクションを実行できる機能が備わっています。イベントおよびイベントが発生した場合に行うアクションは、EEM ポリシーで定義します。

この章では、EEM の使用方法と IE3000 スイッチで EEM を設定する方法について説明します。この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスおよび『*Cisco IOS Network Management Command Reference*』を参照してください。EEM の完全なドキュメント セットについては、『*Cisco IOS Network Management Configuration Guide*』の次のドキュメントを参照してください。

- 『*Embedded Event Manager Overview*』
  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html
- 『*Writing Embedded Event Manager Policies Using the Cisco IOS CLI*』
  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_cli.html
- 『*Writing Embedded Event Manager Policies Using Tcl*』
  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html

（注） Cisco IOS Release 12.2(55)SE 以降、この機能は、IP ベース イメージが稼動しているスイッチでサポートされます。

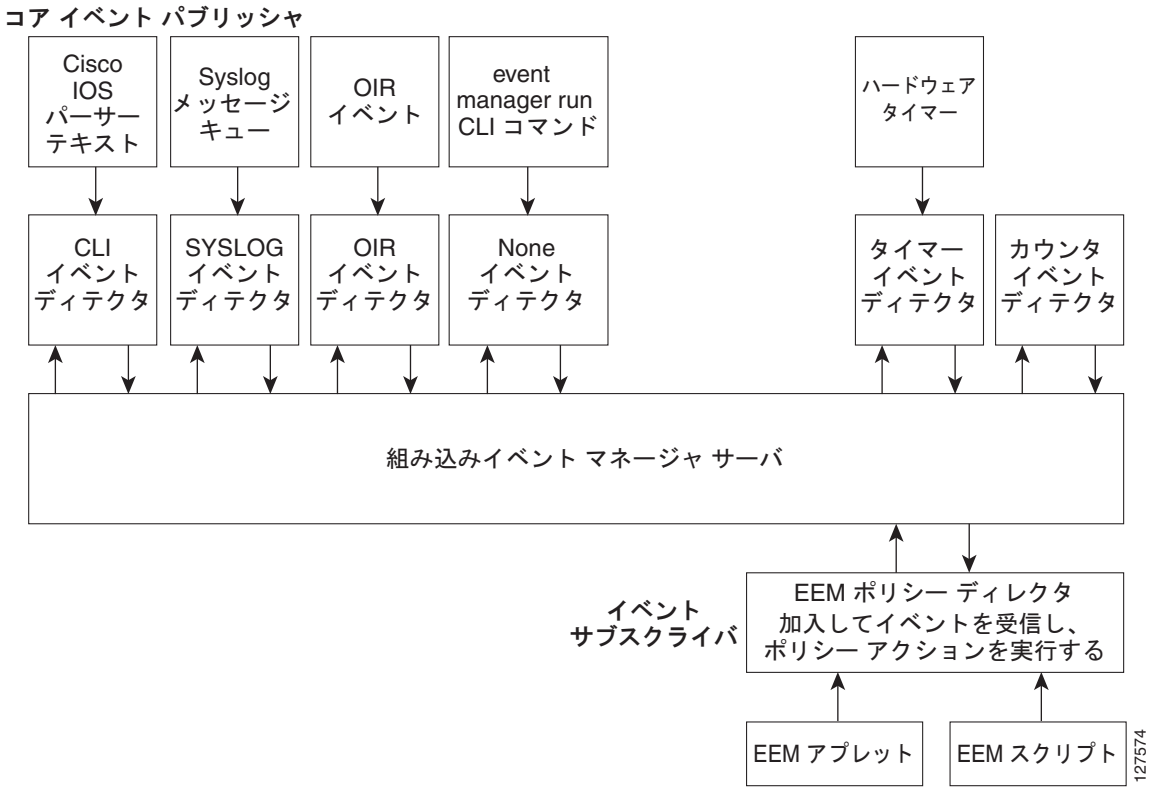
この章の内容は次のとおりです。

Embedded Event Manager の概要

EEM は主要なシステム イベントをモニタし、セット ポリシーを通してイベントに作用します。このポリシーはプログラムされたスクリプトで、これを使用して、発生した特定の一連のイベントに基づいてアクションを呼び出すように、スクリプトをカスタマイズできます。このスクリプトは、カスタム Syslog または Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップの生成、CLI（コマンドライン インターフェイス）コマンドの呼び出し、フェールオーバーの強制などのアクションを生成します。スイッチからすべてのイベント管理を行うことはできず、問題の発生により、スイッチと外部ネットワーク管理装置間の通信に支障をきたすので、EEM のイベント管理機能は有益です。スイッチを再起動することなく自動回復アクションが行われる場合、ネットワークのアベイラビリティは向上します。

図 37-1 に、EEM サーバ、コア イベント パブリッシャ（イベント検出器）、およびイベント サブスクライバ（ポリシー）の関係を示します。イベント パブリッシャはイベントを選別し、イベント サブスクライバによって提供されたイベント仕様と一致するとそれらのイベントをパブリッシュします。イベントが発生すると、イベント検出器が EEM サーバに通知します。次に、システムの現在の状態と特定のイベントに対してポリシーで指定されたアクションに基づいて、EEM ポリシーが回復を実行します。

図 37-1　Embedded Event Manager のコア イベント検出器



EEM の配置の例については、『*EEM Configuration for Cisco Integrated Services Router Platforms Guide*』を参照してください。

- 「イベント検出器」（P.37-2）
- 「Embedded Event Manager のアクション」（P.37-4）
- 「Embedded Event Manager ポリシー」（P.37-4）
- 「Embedded Event Manager の環境変数」（P.37-4）

イベント検出器

イベント検出器と呼ばれる EEM ソフトウェア プログラムは、EEM イベントがいつ発生するかを決定します。イベント検出器は、モニタ対象のエージェント（SNMP など）とアクションを実行できる EEM ポリシーの間のインターフェイスを提供する別個のシステムです。

- アプリケーション固有のイベント検出器：任意の EEM ポリシーがイベントをパブリッシュできます。
- IOS CLI イベント検出器：CLI によって入力されたコマンドに基づいてポリシーを生成します。

- カウンタ イベント検出器：名前付きカウンタが指定されたスレッシュホールドを超えたときにイベントをパブリッシュします。
- インターフェイス カウンタ イベント検出器：指定されたインターフェイスの汎用 Cisco IOS インターフェイス カウンタが定義されたスレッシュホールドを超えたときにイベントをパブリッシュします。スレッシュホールドは絶対値または増分値として指定できます。たとえば、増分値が 50 に設定されている場合、インターフェイス カウンタが 50 増加したときにイベントがパブリッシュされます。

  この検出器はさらに、開始時と終了時の値の変化の度合いに基づいてインターフェイスに関するイベントをパブリッシュします。
- None イベント検出器：**event manager run** CLI コマンドで EEM ポリシーを実行するときにイベントをパブリッシュします。EEM は、ポリシー内のイベント仕様に基づいて、ポリシーをスケジューリングして実行します。EEM ポリシーは、**event manager run** コマンドの実行前に手動で識別して登録する必要があります。
- Online Insertion and Removal（OIR; ホットスワップ）イベント検出器：ハードウェアの取り付けまたは取り外し（OIR）イベントが発生したときにイベントをパブリッシュします。
- リソース スレッシュホールド イベント検出器：グローバル プラットフォームの値およびスレッシュホールドに基づいてポリシーを生成します。CPU の使用率および残りのバッファ容量などのリソースを含みます。
- Remote Procedure Call（RPC; リモート プロシージャ コール）イベント検出器：Secure Shell（SSH; セキュア シェル）を使用して暗号化された接続でスイッチの外部から EEM ポリシーを呼び出し、Simple Object Access Protocol（SOAP）データ符号化を使用して XML ベースのメッセージを交換します。また、EEM ポリシーを実行し、SOAP XML 形式の応答の出力を取得します。
- SNMP イベント検出器：標準 SNMP MIB オブジェクトをモニタし、次の場合にイベントを生成することができます。
  - オブジェクトが指定された値と一致するか指定されたスレッシュホールドを超えた場合
  - SNMP のデルタ値（モニタ期間の開始時の Object Identifier（OID; オブジェクト ID）値とイベントのパブリッシュ時の実際の OID 値の差）が指定された値と一致する場合
- SNMP 通知イベント検出器：スイッチで受信される SNMP トラップと inform メッセージを代行受信します。着信メッセージが指定された値と一致するか定義されたスレッシュホールドを超えたときにイベントが生成されます。
- Syslog イベント検出器：正規表現パターン マッチを持つ Syslog メッセージを選別できます。選別されたメッセージをさらに限定し、指定された時間内に特定の回数の発生を記録するように要求できます。指定されたイベント基準での一致により、設定されたポリシー アクションがトリガーされます。
- タイマー イベント検出器：次のイベントをパブリッシュします。
  - absolute-time-of-day タイマーは、指定された絶対的な日時になったときにイベントをパブリッシュします。
  - カウントダウン タイマーは、タイマーがゼロまでカウントダウンされたときにイベントをパブリッシュします。
  - ウォッチドッグ タイマーは、タイマーがゼロまでカウントダウンされたときにイベントをパブリッシュします。タイマーは初期値に自動的にリセットされ、再びカウントダウンを開始します。
  - CRON タイマーは、UNIX 標準 CRON 仕様を使用して、イベントをパブリッシュする時期を定義することによって、イベントをパブリッシュします。CRON タイマーは、1 分間にイベントを複数回パブリッシュすることはありません。

- ウォッチドッグ イベント検出器（IOSWDSysMon）：次の場合にイベントをパブリッシュします。
  - Cisco IOS プロセスでの CPU の使用率がスレッシュホールドを超えた場合
  - Cisco IOS プロセスでのメモリの使用率がスレッシュホールドを超えた場合

  同時に 2 つのイベントをモニタすることができ、イベントがパブリッシュされる基準は、1 つまたは両方のイベントが指定されたスレッシュホールドを超えた場合です。

Embedded Event Manager のアクション

イベントに応じて次のようなアクションが実行されます。

- 名前付きカウンタの修正
- アプリケーション固有のイベントのパブリッシュ
- SNMP トラップの生成
- 優先される Syslog メッセージの生成
- Cisco IOS ソフトウェアのリロード

Embedded Event Manager ポリシー

EEM はイベントをモニタして情報を提供するか、またはモニタ対象のイベントが発生するかスレッシュホールドに達した場合に修正措置を行うことができます。EEM ポリシーは、イベントおよびイベントが発生した場合に行うアクションを定義するエンティティです。

EEM ポリシーにはアプレットとスクリプトの 2 つのタイプがあります。アプレットは、CLI 設定内で定義される簡易なポリシーです。イベントの選別基準とイベントが発生した場合に行うアクションを定義する簡易な方法です。スクリプトは、ASCII エディタを使用して、ネットワーキング装置上で定義されます。バイトコード（.tbc）およびテキスト（.tcl）のスクリプトとして定義され、ネットワーキング装置にコピーされて EEM に登録されます。.tcl ファイルの複数のイベントを登録することもできます。

EEM を使用して、EEM ポリシー Tool Command Language（TCL; ツール コマンド言語）スクリプトを使用する独自のポリシーを記述して実行します。

キーワード拡張という形式のシスコの TCL 拡張機能は、EEM ポリシーの開発を容易にします。これらのキーワードは、検出されたイベント、その後のアクション、ユーティリティ情報、カウンタ値、およびシステム情報を識別します。

EEM のポリシーおよびスクリプトの設定の詳細については、『*Cisco IOS Network Management Configuration Guide, Release 12.4T*』を参照してください。

Embedded Event Manager の環境変数

EEM は EEM ポリシーで環境変数を使用します。これらの変数は、CLI コマンドと **event manager environment** コマンドを実行することにより、EEM ポリシー TCL スクリプトで定義されます。

- ユーザ定義の変数

  ユーザ定義のポリシーに対して、ユーザにより定義されます。

- シスコ定義の変数

  特定のサンプル ポリシーに対して、シスコにより定義されます。

- シスコ組み込み変数（EEM アプレットで使用可能）

  シスコにより定義され、読み取り専用または読み書きに設定できます。読み取り専用変数は、アプレットが実行を開始する前に、システムによって設定されます。1 つの読み書き変数 _exit_status により、同期イベントからトリガーされるポリシーの終了ステータスを設定できます。

シスコ定義の環境変数とシスコ システム定義の環境変数には、特定の イベント検出器だけに適用されるものとすべてのイベント検出器に適用されるものがあります。ユーザ定義の環境変数またはサンプル ポリシーでシスコにより定義される環境変数は、**event manager environment** グローバル コンフィギュレーション コマンドを使用して設定されます。ポリシーを登録する前に、変数を EEM ポリシーに定義する必要があります。

EEM がサポートする環境変数の詳細については、『*Cisco IOS Network Management Configuration Guide, Release 12.4T*』を参照してください。

Embedded Event Manager の設定

Embedded Event Manager の設定の詳細については、『*Cisco IOS Network Management Configuration Guide, Release 12.4T*』を参照してください。

Embedded Event Manager アプレットの登録と定義

EEM にアプレットを登録し、**event applet** および **action applet** コンフィギュレーション コマンドを使用して EEM アプレットを定義するには、特権 EXEC モードで、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**event manager applet** *applet-name*	EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。
ステップ 3	**event snmp oid** *oid-value* **get-type** {**exact** | **next**} **entry-op** {**gt** | **ge** | **eq** | **ne** | **lt** | **le**} **entry-val** *entry-val* [**exit-comb** {**or** | **and**}] [**exit-op** {**gt** | **ge** | **eq** | **ne** | **lt** | **le**}] [**exit-val** *exit-val*] [**exit-time** *exit-time-val*] **poll-interval** *poll-int-val*	EEM アプレットを稼動させるイベント基準を指定します。 （任意）終了基準。終了基準を指定しない場合、イベントのモニタがすぐに再びイネーブルになります。
ステップ 4	**action label syslog** [**priority** *priority-level*] **msg** *msg-text*	EEM アプレットがトリガーされたときのアクションを指定します。このアクションを繰り返して、アプレットに他の CLI コマンドを追加します。 • （任意）priority キーワードは、Syslog メッセージのプライオリティ レベルを指定します。選択した場合、priority-level 引数を定義する必要があります。 • *msg-text* 引数には、文字テキスト、環境変数、またはこの 2 つを組み合わせたものを指定できます。
ステップ 5	**end**	アプレット コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次に、SNMP オブジェクト ID によって指定されたフィールドの 1 つが定義されたスレッシュホールドを超えた場合の EEM での出力例を示します。

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
```

次に、EEM イベントに応じて行われるアクションの例を示します。

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current
available memory is $_snmp_oid_val bytes"
Switch (config-applet)# action 2.0 force-switchover
```

Embedded Event Manager TCL スクリプトの登録と定義

EEM に TCL スクリプトを登録し、TCL スクリプトとポリシー コマンドを定義するには、特権 EXEC モードで、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 1	**show event manager environment** [**all** | *variable-name*]	（任意）**show event manager environment** コマンドは、EEM 環境変数の名前と値を表示します。 （任意）**all** キーワードは、EEM 環境変数を表示します。 （任意）*variable-name* 引数は、指定された環境変数に関する情報を表示します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**event manager environment variable-name string**	指定された EEM 環境変数の値を設定します。必要なすべての環境変数でこのステップを繰り返します。
ステップ 4	**event manager policy** *policy-file-name* [**type system**] [**trap**]	EEM ポリシーを登録し、ポリシー内で定義された特定のイベントが発生した場合に実行されるようにします。
ステップ 5	**exit**	グローバル コンフィギュレーション モードを終了し、特権 EXECE モードに戻ります。

次に、show event manager environment コマンドの出力例を示します。

```
Switch# show event manager environment all
No.  Name                           Value
1    _cron_entry                    0-59/2 0-23/1 * * 0-6
2    _show_cmd                      show ver
3    _syslog_pattern                .*UPDOWN.*Ethernet1/0.*
4    _config_cmd1                   interface Ethernet1/0
5    _config_cmd2                   no shut
```

次に、ソフトウェアによって割り当てられた CRON タイマー環境変数を毎日の毎時間、毎分、毎秒に設定する方法を示します。

```
Switch (config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

次に、システム ポリシーとして登録された *tm_cli_cmd.tcl* という名前の EEM ポリシーの例を示します。システム ポリシーは Cisco IOS イメージの一部です。ユーザ定義の TCL スクリプトは、最初にフラッシュ メモリにコピーする必要があります。

```
Switch (config)# event manager policy tm_cli_cmd.tcl type system
```

Embedded Event Manager 情報の表示

EEM に関する情報（EEM の登録されたポリシーや EEM の履歴データを含む）を表示するには、『*Cisco IOS Network Management Command Reference*』を参照してください。

CHAPTER 38

ACL によるネットワーク セキュリティの設定

この章では、Access Control List（ACL; アクセス制御リスト）（アクセス リストとも呼ばれる）を使用して、IE 3000 スイッチにネットワーク セキュリティを設定する手順について説明します。この章で言及される IP ACL は、IP バージョン 4（IPv4）ACL を指しています。IPv6 ACL の詳細については、第 44 章「IPv6 ACL の設定」を参照してください。

この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2* 』を参照してください。Cisco IOS のマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックの制限や、特定のユーザまたは装置によるネットワーク利用の制限に役立ちます。ACL は、ルータまたはスイッチを通過するトラフィックをフィルタリングし、指定したインターフェイスまたは VLAN を通るパケットを許可または拒否します。ACL とは、パケットに適用される許可条件と拒否条件を列挙したものです。インターフェイス上でパケットが受信されると、スイッチはパケット内の各フィールドと適用されているすべての ACL を比較し、アクセス リストで指定された基準に基づいて、そのパケットを転送するのに必要な許可があることを確認します。スイッチは、パケットをアクセス リスト内の各条件と 1 つずつ照合してテストします。最初の条件一致で、スイッチがパケットを受け入れるか拒否するかが決まります。最初の条件一致後にスイッチはテストを停止するため、リスト内の条件の順序が重要となります。どの条件も一致しない場合、スイッチはパケットを拒否します。制限がない場合はスイッチがパケットを転送しますが、そうでない場合はスイッチがパケットを廃棄します。スイッチは、VLAN 内でブリッジされるパケットを含め、転送するすべてのパケットに対して ACL を使用できます。

ルータまたはレイヤ 3 スイッチ上でアクセス リストを設定すると、ネットワークの基本的なセキュリティが実現されます。ACL を設定しないと、スイッチを通過するすべてのパケットがネットワークのどの部分に対しても許可される可能性があります。ACL を使用すると、ネットワークのさまざまな部分にアクセスできるホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラ

フィックのタイプを決定したりすることができます。たとえば、E メール トラフィックは転送を許可し、Telnet トラフィックは禁止するといった設定が可能です。ACL の設定により、インバウンド トラフィック、アウトバウンド トラフィック、またはその両方をブロックできます。

ACL には、Access Control Entry（ACE; アクセス制御エントリ）の順序指定リストが含まれています。各 ACE には、*許可*または*拒否*と、パケットがその ACE と一致するために満たす必要のある条件のセットが指定されます。*許可*または*拒否*の意味は、その ACL が使用されているコンテキストによって決まります。

このスイッチでは、IP ACL およびイーサネット（MAC）ACL がサポートされています。

- IP ACL は、Transmission Control Protocol（TCP; 伝送制御プロトコル）、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）を含む IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は、非 IP トラフィックをフィルタリングします。

このスイッチでは、Quality Of Service（QoS; サービス品質）分類の ACL もサポートされています。詳細については、「QoS ACL に基づく分類」（P.39-8）を参照してください。

ここでは、次の概念情報について説明します。

- 「サポートされる ACL」（P.38-2）
- 「フラグメント化およびフラグメント解除されたトラフィックの処理」（P.38-5）

サポートされる ACL

（注）　ルータ ACL および VLAN マップは、IP サービス イメージが稼動しているスイッチ上でだけサポートされます。

- ポート ACL は、レイヤ 2 インターフェイスに着信するトラフィックをアクセス制御します。発信方向のポート ACL は、このスイッチではサポートされていません。レイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。詳細については、「ポート ACL」（P.38-3）を参照してください。
- ルータ ACL は、VLAN 間のルーテッド トラフィックをアクセス制御し、特定の方向（着信または発信）のレイヤ 3 インターフェイスに適用されます。詳細については、「ルータ ACL」（P.38-4）を参照してください。
- VLAN ACL または VLAN マップは、すべてのパケット（ブリッジドおよびルーテッド）をアクセス制御します。VLAN マップを使用すると、同じ VLAN 内の装置間のトラフィックをフィルタリングできます。VLAN マップを設定すると、IPv4 のレイヤ 3 アドレスに基づいたアクセス制御を行います。サポートされていないプロトコルは、イーサネット ACE を使用する MAC アドレスを通じてアクセス制御されます。VLAN マップが VLAN に適用されると、VLAN に着信するすべてのパケット（ルーテッドまたはブリッジド）が VLAN マップと照合されます。パケットは、スイッチ ポートまたはルーティングされたあとのルーテッド ポートのいずれかを通して VLAN に入ることができます。詳細については、「VLAN マップ」（P.38-5）を参照してください。

ユーザは同一のスイッチ上で、入力ポート ACL、ルータ ACL、VLAN マップを使用できます。ただし、ポート ACL はルータ ACL や VLAN マップよりも優先されます。

- 入力ポート ACL と VLAN マップの両方が適用されている場合、ポート ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。その他のパケットには、VLAN マップのフィルタが適用されます。

- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- 出力ルータ ACL および入力ポート ACL が SVI に存在している場合、ポート ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- VLAN マップ、入力ルータ ACL、および入力ポート ACL が SVI に存在している場合、ポート ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけ適用されます。
- VLAN マップ、出力ルータ ACL、および入力ポート ACL が SVI に存在している場合、ポート ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけ適用されます。

IEEE 802.1Q トンネリングがインターフェイス上で設定されている場合、トンネル ポートで受信された IEEE 802.1Q カプセル化 IP パケットには MAC ACL のフィルタを適用できますが、IP ACL のフィルタは適用できません。これは、スイッチが IEEE 802.1Q ヘッダー内部のプロトコルを認識しないためです。ルータ ACL、ポート ACL、および VLAN マップに、この制限が適用されます。IEEE 802.1Q トンネリングの詳細については、第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

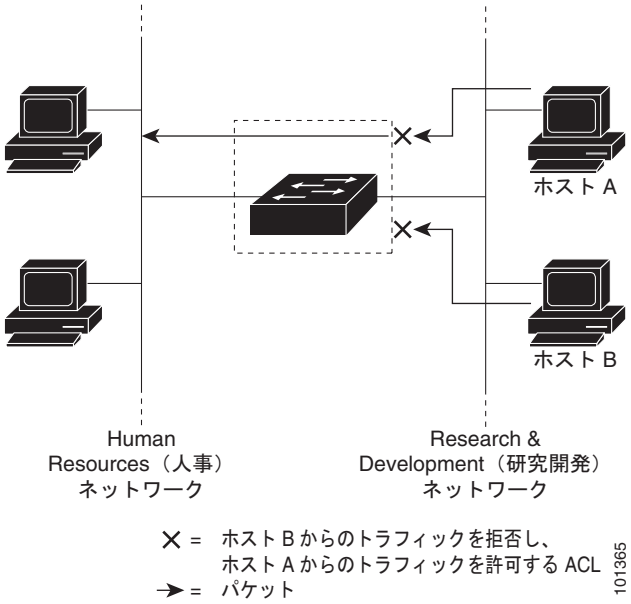
ポート ACL

ポート ACL は、スイッチ上のレイヤ 2 インターフェイスに適用される ACL です。ポート ACL は EtherChannel インターフェイス上ではなく物理インターフェイス上でだけサポートされ、着信方向のインターフェイスにだけ適用できます。次のアクセス リストがサポートされています。

- 送信元アドレスを使用する標準 IP アクセス リスト
- 送信元アドレスおよび宛先アドレスと、任意のプロトコル タイプ情報を使用する拡張 IP アクセス リスト
- 送信元 MAC アドレスおよび宛先 MAC アドレスと、任意のプロトコル タイプ情報を使用する MAC 拡張アクセス リスト

スイッチは、指定したインターフェイス上で設定されたすべての着信機能と関連付けられた ACL を検証し、パケットが ACL 内のエントリとどのように一致するかに基づいてパケット転送を許可または拒否します。このようにして、ACL はネットワーク全体またはネットワークの一部に対するアクセスを制御します。図 38-1 に、すべてのワークステーションが同一 VLAN 内にある場合に、ポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 入力に適用された ACL は、ホスト A から人事部のネットワークへのアクセスは許可しますが、ホスト B から同じネットワークへのアクセスは禁止します。ポート ACL は、着信方向のレイヤ 2 インターフェイスにしか適用できません。

図 38-1　ACL によるネットワークへのトラフィックの制御



ポート ACL をトランク ポートに適用すると、ACL によってトランク ポート上に存在するすべての VLAN のトラフィックがフィルタリングされます。ポート ACL を音声 VLAN のポートに適用すると、ACL によってデータと音声の両方の VLAN のトラフィックがフィルタリングされます。

ポート ACL を使用すると、IP トラフィックは IP アクセス リストでフィルタリングし、非 IP トラフィックは MAC アドレスでフィルタリングすることができます。インターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用すると、同じレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックの両方をフィルタリングできます。

（注）　1 つのレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストまたは MAC アクセス リストがレイヤ 2 インターフェイス上ですでに設定されている場合に、新しい IP アクセス リストまたは MAC アクセス リストをこのインターフェイスに適用すると、以前に設定されていた ACL は新しい ACL で置換されます。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスである SVI、物理レイヤ 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイス上で特定の方向（着信または発信）に対して適用します。インターフェイス上の各方向で、1 つのルータ ACL を適用できます。

1 つの ACL をある特定インターフェイスの複数の機能に使用できます。また、1 つの機能に複数の ACL を使用することもできます。複数の機能で 1 つのルータ ACL が使用されている場合は、その ACL が複数回検証されます。

IPv4 トラフィックに対して次のアクセス リストがサポートされています。

- 標準 IP アクセス リストでは、照合処理に送信元アドレスが使用されます。
- 拡張 IP アクセス リストでは、照合処理に送信元アドレスおよび宛先アドレスと、任意のプロトコル情報が使用されます。

ポート ACL と同様に、スイッチは指定のインターフェイス上で設定された機能と関連付けられた ACL を検証します。ただし、ルータ ACL は双方向で使用できますが、適用できるのは着信ポート ACL だけです。パケットがインターフェイス上でスイッチに入ってくると、そのインターフェイス上で設定されたすべての着信機能と関連付けられた ACL が検証されます。パケットがルーティングされたあと、ネクストホップに転送される前に、出力インターフェイス上で設定された発信機能と関連付けられた ACL がすべて検証されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス制御が行えます。図 38-1 では、ルータ入力に適用された ACL は、ホスト A から人事部のネットワークへのアクセスは許可しますが、ホスト B から同じネットワークへのアクセスは禁止します。

VLAN マップ

*すべて*のトラフィックをアクセス制御するには、VLAN ACL または VLAN マップを使用します。VLAN マップは、VLAN に（または VLAN から）ルーティングされる、あるいはスイッチの VLAN 内でブリッジされるすべてのパケットに適用できます。

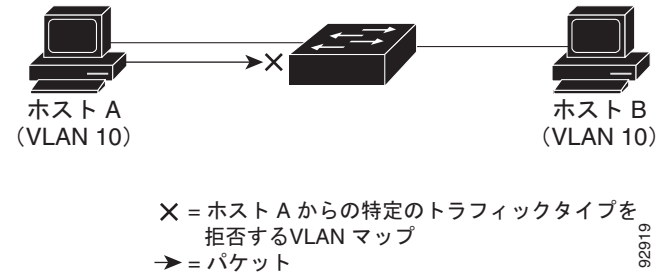
VLAN マップは、セキュリティ パケット フィルタリングに使用します。VLAN マップは方向（入力または出力）別では定義されません。

IPv4 トラフィックのレイヤ 3 アドレスと照合する VLAN マップを設定できます。

非 IP プロトコルはすべて、MAC VLAN マップを使用する MAC アドレスおよび Ethertype を通してアクセス制御されます（IP トラフィックは MAC VLAN マップではアクセス制御*されません*）。スイッチを通過するパケットに対してだけ VLAN マップを適用できますが、ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックに対しては VLAN マップを適用できません。

VLAN マップを使用すると、マップ内で指定されたアクションに基づいて、パケット転送が許可または拒否されます。図 38-2 に、VLAN マップを適用して、VLAN 10 内のホスト A からの特定タイプのトラフィックが転送されないようにする方法を示します。VLAN に適用できる VLAN マップは 1 つだけです。

図 38-2　VLAN マップによるトラフィック制御



フラグメント化およびフラグメント解除されたトラフィックの処理

IP パケットは、ネットワークを通過するときにフラグメント化できます。フラグメント化が行われた場合、TCP または UDP ポート番号、ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの先頭が格納されたフラグメントにだけ含まれます。他のすべてのフラグメントには、この情報はありません。

ACE の中には、レイヤ 4 情報を確認しないため、すべてのパケット フラグメントに適用できるものもあります。レイヤ 4 情報をテストする ACE は、標準の方法では、フラグメント化された IP パケット内の大半のフラグメントに適用できません。フラグメントにレイヤ 4 情報がなく、ACE が何らかのレイヤ 4 情報をテストする場合は、照合ルールが変更されます。

- フラグメント内のレイヤ 3 情報（TCP、UDP などのプロトコル タイプを含む）を確認する許可 ACE は、欠落しているレイヤ 4 情報の内容にかかわらず、フラグメントと一致するものと見なされます。
- レイヤ 4 情報を確認する拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、そのフラグメントとは一致しません。

次のコマンドで設定されたアクセス リスト 102 が、フラグメント化された 3 つのパケットに適用されるとします。

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

（注） この例の最初および 2 番めの ACE で、宛先アドレスのあとの *eq* キーワードは、TCP 宛先ポートの既知の番号がそれぞれ Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）および Telnet と一致しているかどうかをテストすることを意味します。

- パケット A は、ホスト 10.2.2.2、ポート 65000 から SMTP ポート上のホスト 10.1.1.1 に転送される TCP パケットです。すべてのレイヤ 4 情報が存在するため、このパケットがフラグメント化されている場合は、最初のフラグメントが完全なパケットであるかのように最初の ACE（許可）と一致します。最初の ACE はフラグメントに適用された際のレイヤ 3 情報をチェックするだけなので、SMTP ポート情報が含まれていなくても、残りのフラグメントも最初の ACE と一致します。この例の情報では、パケットは TCP、宛先は 10.1.1.1 になっています。
- パケット B は、ホスト 10.2.2.2、ポート 65001 から Telnet ポート上のホスト 10.1.1.2 に転送されます。すべてのレイヤ 3 およびレイヤ 4 情報が存在するため、このパケットがフラグメント化されている場合は、最初のフラグメントが 2 番めの ACE（拒否）と一致します。パケット内の残りのフラグメントにはレイヤ 4 情報がないため、2 番めの ACE とは一致しません。代わりに、残りのフラグメントは 3 番めの ACE（許可）と一致します。

  最初のフラグメントは拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できません。このため、パケット B は事実上拒否されます。ただし、許可されたあとのフラグメントは、パケットの再構成を試みる際に、ネットワーク上の帯域幅とホスト 10.1.1.2 のリソースを消費します。
- フラグメント化されたパケット C は、ホスト 10.2.2.2、ポート 65001 からホスト 10.1.1.3、ポート ftp に転送されます。このパケットがフラグメント化されている場合は、最初のフラグメントが 4 番めの ACE（拒否）と一致します。4 番めの ACE はレイヤ 4 情報をチェックせず、全フラグメント内のレイヤ 3 情報は全フラグメントがホスト 10.1.1.3 に送信されることを示しており、前の許可 ACE は別のホストをチェックしていたため、他のフラグメントもすべて 4 番めの ACE と一致します。

IPv4 ACL の設定

このスイッチで IP v4ACL を設定する方法は、他の Cisco スイッチおよびルータで IPv4 ACL を設定する方法と同じです。次に、このプロセスについて簡単に説明します。ACL の設定の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」を参照してください。コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2* 』を参照してください。Cisco IOS のマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

このスイッチでは、次の Cisco IOS ルータ ACL 関連機能はサポートされていません。

- 非 IP プロトコル ACL（表 38-1（P.38-8）を参照）またはブリッジグループ ACL
- IP アカウンティング
- 着信および発信レート制限（QoS ACL を使用した場合を除く）
- 再帰 ACL またはダイナミック ACL（スイッチ クラスタリング機能で使用される、一部の特殊なダイナミック ACL を除く）
- ポート ACL および VLAN マップに関する ACL ロギング

次に、このスイッチで IP ACL を使用するための手順を示します。

ステップ 1　アクセス リストの番号または名前、およびアクセス条件を指定して、ACL を作成します。

ステップ 2　ACL をインターフェイスまたは端末回線に適用します。また、標準および拡張 IP ACL を VLAN マップに適用することもできます。

ここでは、次の設定情報について説明します。

- 「標準および拡張 IPv4 ACL の作成」（P.38-7）
- 「端末回線への IPv4 ACL の適用」（P.38-20）
- 「インターフェイスへの IPv4 ACL の適用」（P.38-20）
- 「IP ACL のハードウェアおよびソフトウェアの処理」（P.38-22）
- 「ACL のトラブルシューティング」（P.38-23）
- 「IPv4 ACL の設定例」（P.38-24）

標準および拡張 IPv4 ACL の作成

ここでは、IP ACL について説明します。ACL とは、許可条件と拒否条件を列挙したものです。スイッチは、パケットをアクセス リスト内の各条件と 1 つずつ照合してテストします。最初の条件一致で、スイッチがパケットを受け入れるか拒否するかが決まります。最初の一致後にスイッチはテストを停止するため、条件の順序が重要となります。どの条件も一致しない場合、スイッチはパケットを拒否します。

ソフトウェアでは、次のタイプの ACL または IPv4 対応アクセス リストがサポートされています。

- 標準 IP アクセス リストでは、照合処理に送信元アドレスが使用されます。
- 拡張 IP アクセス リストでは、照合処理に送信元アドレスと宛先アドレスが使用され、さらに細かい制御を行う場合は任意でプロトコル タイプ情報も使用されます。

ここでは、アクセス リストとその作成手順について説明します。

- 「アクセス リスト番号」（P.38-8）

アクセス リスト番号

ACL を表すために使用する番号は、作成するアクセス リストのタイプを示します。表 38-1 に、アクセス リスト番号とそれに対応するアクセス リスト タイプを示し、それらがスイッチでサポートされているかどうかを示します。このスイッチでは、IPv4 の標準および拡張アクセス リスト、番号 1 ～ 199 および 1300 ～ 2699 がサポートされています。

表 38-1　　アクセス リスト番号

アクセス リスト番号	タイプ	サポート
1 ～ 99	IP 標準アクセス リスト	あり
100 ～ 199	IP 拡張アクセス リスト	あり
200 ～ 299	プロトコル タイプコード アクセス リスト	なし
300 ～ 399	DECnet アクセス リスト	なし
400 ～ 499	XNS 標準アクセス リスト	なし
500 ～ 599	XNS 拡張アクセス リスト	なし
600 ～ 699	AppleTalk アクセス リスト	なし
700 ～ 799	48 ビット MAC アドレス アクセス リスト	なし
800 ～ 899	IPX 標準アクセス リスト	なし
900 ～ 999	IPX 拡張アクセス リスト	なし
1000 ～ 1099	IPX SAP アクセス リスト	なし
1100 ～ 1199	拡張 48 ビット MAC アドレス アクセス リスト	なし
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	なし
1300 ～ 1999	IP 標準アクセス リスト（拡張範囲）	あり
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	あり

（注） 番号付きの標準および拡張 ACL に加えて、サポート対象の番号を使用して名前付きの標準および拡張 IP ACL を作成することもできます。つまり、標準 IP ACL の名前には 1 ～ 99、拡張 IP ACL の名前には 100 ～ 199 を使用できます。番号付きリストではなく名前付き ACL を使用することの利点は、名前付きリストから個別のエントリを削除できることです。

ACL ロギング

スイッチ ソフトウェアでは、標準の IP アクセス リストによって許可または拒否されたパケットに関するロギング メッセージを提供できます。つまり、パケットが ACL と一致すると、そのパケットの詳細を示すロギング メッセージがコンソールに送信されます。コンソールに記録されるメッセージのレベルは、syslog メッセージを制御する logging console コマンドで制御します。

（注）　ルーティングはハードウェアで行われ、ロギングはソフトウェアで行われるため、多数のパケットが **log** キーワードを含む*許可*または*拒否* ACE と一致する場合は、ソフトウェアがハードウェアの処理速度に対応できず、一部のパケットが記録されない可能性があります。

ACL をトリガーする最初のパケットによって、ロギング メッセージが直ちに表示され、後続のパケットは 5 分間隔で収集されたあと、表示または記録されます。ロギング メッセージには、アクセス リスト番号、パケットが許可されたか拒否されたか、パケットの送信元 IP アドレス、直前の 5 分間隔でこの送信元から許可または拒否されたパケットの数が含まれます。

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	送信元アドレスとワイルドカードを使用して、標準 IPv4 アクセス リストを定義します。 *access-list-number* 値は、1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にアクセスを拒否するのか許可するのかを指定します。 *source* 値は、パケットの送信元となるネットワークまたはホストのアドレスであり、次の形式で指定されます。 • ドット付き 10 進表記による 32 ビット長の値。 • *source* および *source-wildcard* 値 0.0.0.0 255.255.255.255 の略を意味するキーワード **any**。source-wildcard を入力する必要はありません。 • source および source-wildcard 値 *source* 0.0.0.0 の略を意味するキーワード **host**。 （任意）*source-wildcard* を使用して、ワイルドカード ビットを送信元に適用します。 （任意）**log** を入力すると、エントリと一致するパケットの詳細を示すロギング メッセージがコンソールに送信されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** [*number* | *name*]	アクセス リスト コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ACL 全体を削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストから個別の ACE は削除できません。

（注）　ACL を作成する場合は、ACL の最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否暗黙の拒否文が、デフォルトで ACL の最後尾に含まれることに注意してください。標準アクセス リストで、関連 IP ホスト アドレス ACL の指定からマスクを省略した場合は、0.0.0.0 がマスクと見なされます。

次に、IP ホスト 171.69.198.102 へのアクセスを拒否し、それ以外へのアクセスを許可し、結果を表示する標準 ACL を作成する例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
    10 deny   171.69.198.102
    20 permit any
```

スイッチは常に、標準アクセス リストの順序を上書きします。これにより、**host** が一致するエントリ、および *don't care* マスクが 0.0.0.0 に一致するエントリがリストの先頭に移動され、*don't care* マスクが 0 以外のどのエントリよりも上になります。このため、**show** コマンド出力とコンフィギュレーション ファイルでは、ACE は必ずしも入力順どおりには表示されません。

作成した番号付き標準 IPv4 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.38-20）を参照）、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.38-20）を参照）、または VLAN（「VLAN マップの設定」（P.38-31）を参照）に適用できます。

番号付き拡張 ACL の作成

標準 ACL では送信元アドレスだけを照合に使用しますが、照合処理に拡張 ACL の送信元アドレスと宛先アドレスを使用でき、さらに細かい制御を行う場合は任意でプロトコル タイプ情報も使用できます。番号付き拡張アクセス リストで ACE を作成する場合は、ACL の作成後の追加はすべてリストの末尾に置かれることに注意してください。リストの順序の変更や、番号付きリストでの ACE の選択的な追加または削除を行うことはできません。

プロトコルの中には、特定のパラメータやキーワードをそのプロトコルに適用するものもあります。

次の IP プロトコルがサポートされています（カッコ内の太字がプロトコル キーワードです）。

認証ヘッダー プロトコル（**ahp**）、Enhanced Interior Gateway Routing Protocol（**eigrp**）、カプセル化セキュリティ ペイロード（**esp**）、総称ルーティング カプセル化（**gre**）、インターネット制御メッセージ プロトコル（**icmp**）、インターネット グループ管理プロトコル（**igmp**）、任意の内部プロトコル（**ip**）、IP in IP トンネリング（**ipinip**）、KA9Q NOS 互換 IP over IP トンネリング（**nos**）、Open Shortest Path First ルーティング（**ospf**）、ペイロード圧縮プロトコル（**pcp**）、Protocol Independent Multicast（**pim**）、伝送制御プロトコル（**tcp**）、ユーザ データグラム プロトコル（**udp**）

（注）　ICMP エコー応答はフィルタリングできません。他のすべての ICMP コードまたはタイプはすべてフィルタリングできます。

各プロトコルの特定のキーワードの詳細については、次のコマンド リファレンスを参照してください。

- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』
- 『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』

- 『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』

これらのマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] から入手できます。

（注）　このスイッチでは、ダイナミックまたは再帰アクセス リストはサポートされていません。また、Type of Service（ToS; サービス タイプ）の minimize-monetary-cost ビットに基づいたフィルタリングもサポートされていません。

サポート対象パラメータは、TCP、UDP、ICMP、IGMP、その他の IP の各カテゴリに分類できます。

拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2a	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] （注）　**dscp** 値を入力した場合は、**tos** と **precedence** は入力できません。**dscp** がない場合は、**tos** と **precedence** の両方の値を入力できます。	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* 値は、100 ～ 199 または 2000 ～ 2699 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にパケットを拒否するのか許可するのかを指定します。 *protocol* には、IP プロトコルの名前（**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、または **udp**）、または番号（IP プロトコル番号を示す 0 ～ 255 の範囲の整数）を入力します。任意のインターネット プロトコル（ICMP、TCP、および UDP を含む）を照合するには、キーワード **ip** を使用します。 （注）　この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の具体的なパラメータについては、ステップ 2b ～ 2e を参照してください。 *source* 値は、パケットの送信元となるネットワークまたはホストの番号です。 *source-wildcard* を使用して、ワイルドカード ビットを送信元に適用します。 *destination* 値は、パケットの送信先となるネットワークまたはホストの番号です。 *destination-wildcard* を使用して、ワイルドカード ビットを宛先に適用します。 source、source-wildcard、destination、および destination-wildcard は、次の形式で指定できます。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。 • シングル ホスト 0.0.0.0 を表すキーワード **host**。 その他のキーワードは任意です。各キーワードの意味は次のとおりです。 • **precedence**：0 ～ 7 の数値または名前で指定された優先レベルを使用してパケットを照合します。指定可能な値は、**routine**（**0**）、***priority***（**1**）、**immediate**（**2**）、**flash**（**3**）、**flash-override**（**4**）、**critical**（**5**）、**internet**（6）、**network**（**7**）です。 • **fragments**：非初期フラグメントを確認します。 • **tos**：0 ～ 15 の数値または名前で指定されたサービス タイプ レベルを使用して照合する場合に入力します。指定可能な値は、**normal**（**0**）、**max-reliability**（**2**）、**max-throughput**（**4**）、**min-delay**（**8**）です。 • **log**：エントリと一致するパケットの詳細を示すロギング メッセージを作成してコンソールに送信します。または、**log-input** を入力して、ログ エントリに入力インターフェイスを含めます。 • **time-range**：このキーワードの詳細については、「ACL での時間範囲の使用」（P.38-17）を参照してください。 • **dscp**：0 ～ 63 の数値で指定された DSCP 値を使用してパケットを照合します。使用可能な値のリストを表示する場合は、疑問符（?）を使用します。

	コマンド	目的
または	**access-list** *access-list-number* {**deny** | permit} *protocol* any any [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	アクセス リスト コンフィギュレーション モードで、source および source wildcard 値 0.0.0.0 255.255.255.255 の略と、destination および destination wildcard 値 0.0.0.0 255.255.255.255 の略を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のアドレスおよびワイルドカードの代わりに **any** キーワードを使用できます。
または	**access-list** *access-list-number* {**deny** | **permit**} *protocol* **host** *source* **host** *destination* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	source および source wildcard 値 *source* 0.0.0.0 の略と、destination および destination wildcard 値 *destination* 0.0.0.0 の略を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のワイルドカードまたはマスクの代わりに **host** キーワードを使用できます。
ステップ 2b	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*]	（任意）拡張 TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。 パラメータはステップ 2a で説明されているパラメータと同じです。ただし、次の例外があります。 （任意）送信元ポート（*source source-wildcard* の後ろに置かれた場合）または宛先ポート（*destination destination-wildcard* の後ろに置かれた場合）を比較する場合は、*operator* および *port* を入力します。使用できる演算子には、**eq**（equal：一致）、**gt**（greater than：より大きい）、**lt**（less than：未満）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）があります。演算子にはポート番号が必要です（**range** にはスペースで区切った 2 つのポート番号が必要です）。 10 進数値（0 ～ 65535）の *port* または TCP ポート名を入力します。TCP ポート名を表示するには、? を使用するか、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」を参照してください。TCP をフィルタリングする場合は、TCP ポート番号またはポート名だけを使用します。 その他の任意のキーワードの意味は次のとおりです。 • **established**：確立された接続を照合します。これには、**ack** または **rst** フラグの照合と同じ機能があります。 • *flag*：指定された TCP ヘッダー ビットによって照合する場合は、次のいずれかのフラグを入力します。**ack**（acknowledge：確認応答）、**fin**（finish：終了）、**psh**（push：プッシュ）、**rst**（reset：リセット）、**syn**（synchronize：同期）、**urg**（urgent：緊急）
ステップ 2c	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP の場合は、**udp** を入力します。 UDP パラメータは TCP に関して説明されているパラメータと同じですが、[*operator* [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP の場合、**flag** および **established** パラメータは無効です。

	コマンド	目的
ステップ 2d	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP の場合は、**icmp** を入力します。 ICMP パラメータはステップ 2a の IP プロトコルに関して説明されているパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。任意のキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプを基準にしてフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-code*：ICMP メッセージ コード タイプを基準にしてフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-message*：ICMP メッセージ タイプ名、または ICMP メッセージのタイプおよびコード名を基準にして、ICMP パケットをフィルタリングします。ICMP メッセージのタイプ名およびコード名のリストについては、? を使用するか、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「Configuring IP Services」を参照してください。
ステップ 2e	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。 IGMP の場合は、**igmp** を入力します。 IGMP パラメータはステップ 2a の IP プロトコルに関して説明されているパラメータとほとんど同じですが、次に示す任意のパラメータが追加されています。 *igmp-type*：IGMP メッセージ タイプを照合するには、0 ～ 15 の数値、またはメッセージ名（**dvmrp**、**host-query**、**host-report**、**pim**、または **trace**）を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** [*number* | *name*]	アクセス リスト コンフィギュレーションを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アクセス リスト全体を削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストから個別の ACE は削除できません。

次に、拡張アクセス リストを作成および表示して、ネットワーク 171.69.198.0 内の任意のホストからネットワーク 172.20.52.0 内の任意のホストへの Telnet アクセスを拒否し、それ以外はすべて許可する例を示します（宛先アドレスのあとの **eq** キーワードは、TCP 宛先ポート番号が Telnet と一致しているかどうかをテストすることを意味します）。

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq
telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
    10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
    20 permit tcp any any
```

ACL の作成後の追加（端末から入力される可能性がある）は、すべてリストの末尾に置かれます。番号付きアクセス リストでアクセス リスト エントリを選択的に追加または削除できません。

（注）　ACL を作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。

作成した番号付き拡張 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.38-20）を参照）、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.38-20）を参照）、または VLAN（「VLAN マップの設定」（P.38-31）を参照）に適用できます。

ACL 内の ACE の順序変更

アクセス リスト内のエントリのシーケンス番号は、新しい ACL の作成時に自動的に生成されます。**ip access-list resequence** グローバル コンフィギュレーション コマンドを使用すると、ACL 内のシーケンス番号を編集して、ACE の適用順序を変更することができます。たとえば、新しい ACE を ACL に追加すると、その ACE はリストの末尾に置かれます。シーケンス番号を変更すると、この ACE を ACL 内の別の位置に移動できます。

ip access-list resequence コマンドの詳細については、次の URL を参照してください。
http://preview.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a60.html

名前付き標準および拡張 ACL の作成

IPv4 ACL を番号ではなく英数字のストリング（名前）で識別することができます。名前付き ACL を使用して、番号付きアクセス リストを使用した場合よりも多くの IPv4 アクセス リストをルータに設定できます。番号ではなく名前でアクセス リストを識別する場合は、モードとコマンド構文が若干異なります。ただし、IP アクセス リストを使用するすべてのコマンドが名前付きアクセス リストを受け入れるとは限りません。

（注）　標準または拡張 ACL に付ける名前は、サポート対象のアクセス リスト番号範囲の数値でも構いません。つまり、標準 IP ACL の名前には 1 ～ 99、拡張 IP ACL の名前には 100 ～ 199 を使用できます。番号付きリストではなく名前付き ACL を使用することの利点は、名前付きリストから個別のエントリを削除できることです。

名前付き ACL を設定する場合は、次の注意事項および制限事項を考慮してください。

- 番号付き ACL を受け入れるすべてのコマンドが、名前付き ACL を受け入れるとは限りません。インターフェイス上のパケット フィルタとルート フィルタに関する ACL には名前を使用できます。VLAN マップも名前を受け入れます。
- 標準 ACL と拡張 ACL は同じ名前にできません。
- 番号付き ACL も使用可能です（「標準および拡張 IPv4 ACL の作成」（P.38-7）を参照）。
- VLAN マップでは、標準および拡張 ACL（名前付きまたは番号付き）を使用できます。

名前を使用して標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list standard** *name*	名前を使用して標準 IPv4 アクセス リストを定義し、アクセスリスト コンフィギュレーション モードを開始します。 名前には 1 ～ 99 の範囲の数値を使用できます。
ステップ 3	**deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**] または **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]	アクセスリスト コンフィギュレーション モードで、パケットを転送するか廃棄するかを決定する拒否条件または許可条件を 1 つまたは複数指定します。 • **host** *source*：source および source wildcard 値 *source* 0.0.0.0。 • **any**：source および source wildcard 値 0.0.0.0 255.255.255.255。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	アクセス リスト コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

名前付き標準 ACL を削除するには、**no ip access-list standard** *name* グローバル コンフィギュレーション コマンドを使用します。

名前を使用して拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list extended** *name*	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセスリスト コンフィギュレーション モードを開始します。 名前には 100 ～ 199 の範囲の数値を使用できます。
ステップ 3	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**] [**time-range** *time-range-name*]	アクセスリスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。違反を含むアクセス リスト ロギング メッセージを取得するには、**log** キーワードを使用します。 プロトコルおよびその他のキーワードの定義については、「番号付き拡張 ACL の作成」（P.38-10）を参照してください。 • **host** *source*：source および source wildcard 値 *source* 0.0.0.0。 • ***host destination***：destination および destination wildcard 値 *destination* 0.0.0.0。 • **any**：source および source wildcard、または destination および destination wildcard 値 0.0.0.0 255.255.255.255。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	アクセス リスト コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

名前付き拡張 ACL を削除するには、**no ip access-list extended** *name* グローバル コンフィギュレーション コマンドを使用します。

標準および拡張 ACL を作成する場合は、ACL の最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトで ACL の最後尾に含まれることに注意してください。標準 ACL で、関連 IP ホスト アドレス アクセス リストの指定からマスクを省略した場合は、0.0.0.0 がマスクと見なされます。

ACL の作成後の追加は、すべてリストの末尾に置かれます。特定の ACL に ACL エントリを選択的に追加できません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。次に、名前付きアクセス リスト *border-list* から個別の ACE を削除する例を示します。

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つは、名前付き ACL から行を選択的に削除できることです。

作成した名前付き ACL は、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.38-20）を参照）、または VLAN（「VLAN マップの設定」（P.38-31）を参照）に適用できます。

ACL での時間範囲の使用

time-range グローバル コンフィギュレーション コマンドを使用すると、時刻や週に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲名を定義し、その時間範囲内の日時や曜日を設定します。次に、ACL を適用してアクセス リストへの制限を設定する際に、定義した時間範囲名を入力します。時間範囲を使用すると、ACL 内の permit または deny ステートメントが有効な時期（指定された時間帯や指定された曜日など）を定義できます。**time-range** キーワードおよび引数については、前述の「標準および拡張 IPv4 ACL の作成」（P.38-7）および「名前付き標準および拡張 ACL の作成」（P.38-15）の名前付き拡張 ACL および番号付き拡張 ACL の作業表を参照してください。

時間範囲を使用すると、次のような利点があります。

- （IP アドレス/マスクのペアとポート番号で識別される）アプリケーションなどのリソースへのユーザ アクセスの許可または拒否をより細かく制御できます。
- ロギング メッセージを制御できます。特定の時刻のトラフィックだけを記録するように ACL エントリを設定できます。このため、ピーク時に生成される多数のログを分析しなくても、単にアクセスを拒否することができます。

時間ベースのアクセス リストは CPU のアクティビティをトリガーします。これは、このアクセス リストの新しい設定を他の機能や、TCAM にロードされた結合済みの設定と統合する必要があるためです。このため、複数のアクセス リストを短時間に連続で（互いに数分以内で）有効化する設定は行わないよう注意してください。

（注） 時間範囲はスイッチのシステム クロックに依存するため、信頼できるクロック ソースが必要です。スイッチ クロックの同期には、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用することを推奨します。詳細については、「システム日時の管理」（P.7-1）を参照してください。

ACL の時間範囲パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**time-range** *time-range-name*	作成する時間範囲にわかりやすい名前（たとえば *workhours*）を割り当てて、time-range コンフィギュレーション モードを開始します。名前にはスペースまたは引用符を含めることはできません。また、名前の先頭は文字にする必要があります。
ステップ 3	**absolute** [**start** *time date*] [**end** *time date*] または **periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm* または **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*	適用対象の機能の動作可能時期を指定します。 • 時間範囲で使用できる **absolute** ステートメントは 1 つだけです。absolute ステートメントを複数設定した場合は、最後に設定したステートメントだけが実行されます。 • **periodic** ステートメントは複数入力できます。たとえば、平日と週末に異なる時間を設定することができます。 設定例を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show time-range**	時間範囲の設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

異なる時間に有効化する項目が複数ある場合は、これらの手順を繰り返します。

設定された時間範囲の制限を削除するには、**no time-range** *time-range-name* グローバル コンフィギュレーション コマンドを使用します。

次に、*workhours* の時間範囲を設定し、会社の休日を 2006 年 1 月 1 日に設定して、設定内容を確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL に時間範囲名を入力します。次に、定義された休日の時間中は任意の送信元から任意の宛先への TCP トラフィックを拒否し、業務時間中はすべての TCP トラフィックを許可する拡張アクセス リスト 188 を作成および確認する例を示します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

ACL でのコメント付け

remark キーワードを使用すると、任意の IP 標準 ACL または IP 拡張 ACL 内のエントリに関するコメント（備考）を付けることができます。remark を使用すると、ACL がわかりやすく、またスキャンしやすくなります。各 remark 行は 100 文字以内に制限されています。

remark は、permit または deny ステートメントの前後どちらにでも設定できます。どの remark ステートメントがどの permit または deny ステートメントを説明しているかが明確になるように、remark の位置は一貫性を保ってください。たとえば、関連付けられている permit または deny ステートメントの前に付く remark と後ろに付く remark が混在していると、わかりにくくなってしまいます。

IP 番号付き標準 ACL または IP 番号付き拡張 ACL にコメントを付けるには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。remark を削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションのアクセスは許可され、Smith のワークステーションのアクセスは許可されません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL 内のエントリには、**remark** アクセスリスト コンフィギュレーション コマンドを使用します。remark を削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットによる発信 Telnet の使用が許可されません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

端末回線への IPv4 ACL の適用

番号付き ACL を使用すると、1 つまたは複数の端末回線へのアクセスを制御できます。名前付き ACL は回線に適用できません。ユーザはどの仮想端末回線にも接続を試行できるため、すべての仮想端末回線に同一の制限を設定する必要があります。

ACL をインターフェイスに適用する手順については、「インターフェイスへの IPv4 ACL の適用」（P.38-20）を参照してください。ACL を VLAN に適用する方法については、「VLAN マップの設定」（P.38-31）を参照してください。

仮想端末回線と ACL 内のアドレス間の着信および発信接続を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number*	設定する特定の回線を指定し、インライン コンフィギュレーション モードを開始します。 • **console**：コンソール端末回線を指定します。コンソール ポートは DCE です。 • **vty**：リモート コンソール アクセス用の仮想端末を指定します。 *line-number* には、回線タイプの指定時に設定する連続グループ内で最初の回線番号が入ります。指定できる範囲は 0 ～ 16 です。
ステップ 3	**access-class** *access-list-number* {**in** | **out**}	特定の（装置に対する）仮想端末回線とアクセス リスト内のアドレス間の着信および発信接続を制限します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	アクセス リスト コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

端末回線から ACL を削除するには、**no access-class** *access-list-number* {**in** | **out**} ライン コンフィギュレーション コマンドを使用します。

インターフェイスへの IPv4 ACL の適用

次の注意事項を確認してください。

- レイヤ 2 ポートには、着信方向にだけ ACL を適用してください。
- レイヤ 3 インターフェイスでは、発信側または着信側のいずれかに ACL を適用してください。
- インターフェイスへのアクセスを制御する場合は、名前付きまたは番号付き ACL を使用できます。
- ACL を VLAN のメンバーであるポートに適用した場合、ポート ACL の方が VLAN インターフェイスに適用された ACL より優先されます。
- VLAN のメンバーになっているレイヤ 2 インターフェイスに ACL を適用すると、レイヤ 2（ポート）ACL は、VLAN インターフェイスに適用された入力レイヤ 3 ACL や VLAN に適用された VLAN マップよりも優先されます。ポート ACL は、レイヤ 2 ポートで受信した着信パケットを常にフィルタリングします。

- ルーティングがイネーブルでない状態で、レイヤ 3 インターフェイスに ACL を適用すると、CPU 宛てのパケット（SNMP、Telnet、Web トラフィックなど）だけがこの ACL によってフィルタリングされます。ACL をレイヤ 2 インターフェイスに適用する場合、ルーティングをイネーブルにする必要はありません。
- プライベート VLAN が設定されている場合は、ルータ ACL はプライマリ VLAN SVI にだけ適用できます。ACL はプライマリ VLAN およびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。

（注）　パケットがアクセス グループによって拒否された場合、デフォルトでルータがインターネット制御メッセージ プロトコル（ICMP）到達不能メッセージを送信します。アクセス グループによって拒否されたパケットはハードウェアで廃棄されるのではなく、ICMP 到達不能メッセージを生成できるようにスイッチの CPU にブリッジされます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定対象となる特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ 3 インターフェイス（ルータ ACL）を指定できます。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**}	指定のインターフェイス宛てのアクセスを制御します。 **out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	アクセス リスト コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定のアクセス グループを削除するには、**no ip access-group** {*access-list-number* | *name*} {**in** | **out**} インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートにアクセス リスト 2 を適用して、このポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 2 in
```

（注）　**ip access-group** インターフェイス コンフィギュレーション コマンドをレイヤ 3 インターフェイス（SVI、レイヤ 3 EtherChannel、またはルーテッド ポート）に適用する場合は、インターフェイスが IP アドレスで設定されている必要があります。レイヤ 3 アクセス グループは、CPU 上のレイヤ 3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。VLAN 内でブリッジされるパケットには影響しません。

着信 ACL では、スイッチは、パケットを受信すると、ACL と照合することでそのパケットを確認します。ACL がパケットを許可する場合、スイッチはパケットの処理を続行します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 ACL では、スイッチは、パケットを受信してそれを制御されたインターフェイスへ送信したあと、ACL と照合することでそのパケットを確認します。ACL がパケットを許可する場合、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

パケットが入力インターフェイス上の ACL によって廃棄されたか出力インターフェイス上の ACL によって廃棄されたかに関係なく、パケットが廃棄されるたびに、デフォルトで入力インターフェイスが ICMP 到達不能メッセージを送信します。ICMP 到達不能メッセージは通常、入力インターフェイスあたり 1/2 秒につき 1 つまでに制限されていますが、**ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用すると、これを変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチはその ACL がインターフェイスに適用されていないかのように動作し、すべてのパケットを許可します。ネットワーク セキュリティ用に未定義の ACL を使用する場合は、この動作に注意してください。

IP ACL のハードウェアおよびソフトウェアの処理

ACL 処理は主にハードウェアで行われますが、ソフトウェア処理のために一部のトラフィック フローを CPU に転送する必要があります。ハードウェアが ACL 設定の格納容量に達すると、パケットが転送のために CPU に送信されます。ソフトウェア転送トラフィックの転送レートは、ハードウェア転送トラフィックに比べると、大幅に小さくなります。

（注） スイッチがリソース不足状態になっているためにハードウェアで ACL 設定を実装できない場合は、そのスイッチに到着する対象 VLAN 内のトラフィックだけが影響を受けます（ソフトウェアで転送されます）。パケットのソフトウェア転送で消費される CPU サイクル数によっては、スイッチのパフォーマンスが低下する可能性があります。

ルータ ACL の場合は、次のような他の要因によってパケットが CPU に送信される可能性があります。

- **log** キーワードの使用
- ICMP 到達不能メッセージの生成

トラフィック フローの記録と転送の両方が行われる場合、転送はハードウェアによって行われますが、記録はソフトウェアによって行う必要があります。ハードウェアとソフトウェアのパケット処理能力は異なるため、記録される全フロー（許可フローと拒否フローの両方）の合計の帯域幅がかなり大きい場合は、転送されるパケットの一部を記録できない可能性があります。

ルータ ACL の設定をハードウェアで適用できない場合、ルーティングする必要のある VLAN に着信するパケットはソフトウェアではルーティングされますが、ハードウェアではブリッジされます。ACL によって大量のパケットが CPU に送信される場合は、スイッチ パフォーマンスが低下する可能性があります。

show ip access-lists 特権 EXEC コマンドの出力に表示されるマッチ カウントは、ハードウェアでアクセス制御されるパケットに対応しません。スイッチド パケットおよびルーテッド パケットの基本的なハードウェア ACL 統計情報を取得するには、**show access-lists hardware counters** 特権 EXEC コマンドを使用します。

ACL のトラブルシューティング

次の ACL マネージャ メッセージが表示され、[chars] がアクセスリスト名の場合、

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

スイッチには ACL のハードウェア表現を作成するためのリソースが不足していることになります。リソースにはハードウェア メモリやラベル スペースが含まれますが、CPU メモリは含まれません。この問題は、使用可能な論理演算ユニットまたは専用のハードウェア リソースの不足が原因と考えられます。論理演算ユニットは、TCP フラグの一致、または TCP、UDP、SCTP ポート番号での **eq** 以外（**ne**、**gt**、**lt**、**range**）のテストで必要です。

次のいずれかの回避策を実行してください。

- ACL 設定を変更して使用するリソースを減らします。
- ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します。

特殊なハードウェア リソースを判別するには、**show platform layer4 acl map** 特権 EXEC コマンドをを入力します。スイッチに使用可能なリソースがない場合の出力には、インデックス 0 ～ インデックス 15 が使用可能でないことが示されます。

リソースが不十分な状態での ACL の設定の詳細については、Bug Toolkit の CSCsq63926 を参照してください。

たとえば、次の ACL をインターフェイスに適用した場合で、

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

なおかつ次のメッセージが表示された場合は、

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

フラグ関連の演算子が使用できないことになります。この問題を回避するには、次のようにします。

- **ip access-list resequence** グローバル コンフィギュレーション コマンドを使用して､4 番めの ACE を最初の ACE の前に移動します。

  ```
  permit tcp source source-wildcard destination destination-wildcard
  permit tcp source source-wildcard destination destination-wildcard range 5 60
  permit tcp source source-wildcard destination destination-wildcard range 15 160
  permit tcp source source-wildcard destination destination-wildcard range 115 1660
  ```

  または

- 他の ACL よりも英数字順で先に表示される名前または番号に ACL の名前を変更します（たとえば、ACL *79* から ACL *1* に変更します）。

これで、ACL 内の最初の ACE をインターフェイスに適用できます。スイッチはこの ACE を Opselect インデックス内の使用可能なマッピング ビットに割り当てたあと、フラグ関連の演算子を割り当てて Ternary Content Addressable Memory（TCAM; 三値連想メモリ）内の同じビットを使用します。

ルータ ACL は次のように機能します。

- ハードウェアは標準および拡張 ACL（入力および出力）の許可アクションと拒否アクションを制御して、セキュリティ アクセス制御を実現します。
- **log** が指定されていない場合、セキュリティ ACL 内の *deny* ステートメントに一致するフローはハードウェアによって廃棄されます（*ip unreachables* がディセーブルに設定されている場合）。*permit* ステートメントと一致するフローは、ハードウェアでスイッチングされます。

- ルータ ACL 内の ACE に **log** キーワードを追加すると、ロギングだけの目的でパケットのコピーが CPU に送信されます。ACE が *permit* ステートメントの場合でも、パケットはハードウェアでスイッチングおよびルーティングされます。

IPv4 ACL の設定例

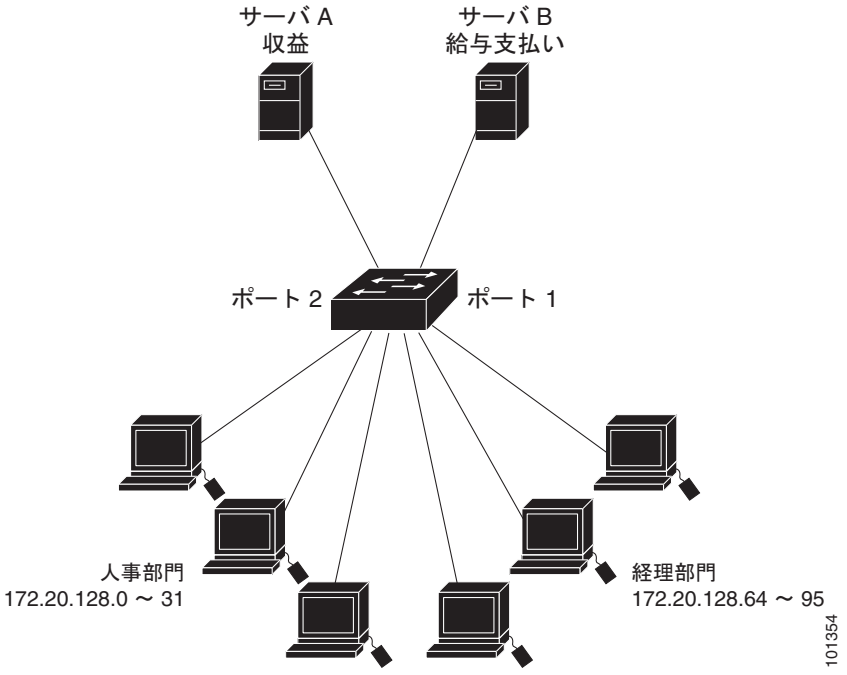
ここでは、IPv4 ACL の設定例と適用例を示します。ACL のコンパイルの詳細については、『*Cisco IOS Security Configuration Guide, Release 12.2*』および『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」を参照してください。

図 38-3 に、サーバ A に接続されたルーテッド ポート 2 と、サーバ B に接続されたルーテッド ポート 1 を使用した小規模なネットワーク オフィス環境を示します。サーバ A には全従業員がアクセスできる収益などの情報が格納されており、サーバ B には機密の給与支払いデータが格納されています。サーバ A にはユーザ全員がアクセスできますが、サーバ B のアクセスは制限されます。

ルータ ACL を使用してこれを実現するには、次のいずれかの方法を用います。

- 標準 ACL を作成して、ポート 1 からサーバに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成して、サーバからポート 1 に着信するトラフィックをフィルタリングします。

図 38-3　　ルータ ACL によるトラフィックの制御



次に、標準 ACL を使用して、ポートからサーバ B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 からのトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスのルーテッド ポート 1 からのトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch #show access-lists
Standard IP access list 6
 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 6 out
```

次に、拡張 ACL を使用して、サーバ B からポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 へのトラフィックだけを許可する例を示します。この ACL はルーテッド ポート 1 へのトラフィックに適用され、指定した宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前にプロトコル（IP）を入力する必要があります。

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch #show access-lists
Extended IP access list 106
 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 106 in
```

番号付き ACL

次の例のネットワーク 36.0.0.0 は、2 番めのオクテットはサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク 36.0.0.0 のアドレスの 3 番めと 4 番めのオクテットは、特定のホストを指定します。スイッチは、アクセス リスト 2 を使用してサブネット 48 上のアドレスを 1 つ受け入れ、このサブネット上の他のアドレスはすべて拒否します。リストの最後の行は、スイッチがネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスを受け入れることを示しています。この ACL はポートに着信するパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL

次の例の最初の行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番めの行は、ホスト 128.88.1.2 のシンプル メール転送プロトコル（SMTP）ポートへの着信 TCP 接続を許可します。3 番めの行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 102 in
```

この例で、ネットワークがインターネットに接続されている状態で、ネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を形成できるようにするとします。ただし、IP ホストは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストへの TCP 接続を形成できないようにします。

SMTP は、接続の一端では TCP ポート 25 を使用し、他端ではランダムなポート番号を使用します。接続の間は、同じポート番号が使用されます。インターネットからの着信メール パケットの宛先ポートは 25 です。発信パケットでは、ポート番号が逆になります。ネットワークのセキュア システムはポート 25 上のメール接続を常に受け入れるため、着信サービスと発信サービスは個別に制御されます。ACL は、発信インターフェイス上では入力 ACL として設定し、着信インターフェイス上では出力 ACL として設定する必要があります。

次の例のネットワークはアドレス 128.88.0.0 のクラス B ネットワークであり、メール ホスト アドレスは 128.88.1.2 です。**established** キーワードは TCP だけに使用され、確立された接続を示します。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われ、パケットが既存の接続に属していることを示します。ギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 102 in
```

名前付き ACL

次に、*internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*internet_filter* ACL は、送信元アドレス 1.2.3.4 からのトラフィックをすべて許可します。

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

marketing_group ACL は、宛先のアドレスおよびワイルドカード 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、それ以外の TCP トラフィックをすべて拒否します。この ACL は、ICMP トラフィックを許可し、任意の送信元から 1024 より小さい宛先ポートの 171.69.0.0 ～ 179.69.255.255 の宛先アドレス範囲への UDP トラフィックを拒否し、それ以外の IP トラフィックをすべて拒否して、結果のログを表示します。

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポート上の着信トラフィックに適用されます。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

IP ACL に適用される時間範囲

次の例では、月曜日から金曜日の午前 8 時～午後 6 時（18 時）の間、IP 上の HTTP トラフィックを拒否します。この例では、土曜日と日曜日の正午～午後 8 時（20 時）の間だけ UDP トラフィックを許可します。

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
```

```
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group strict in
```

コメント付き IP ACL エントリ

次の例の番号付き ACL では、Jones のワークステーションのアクセスは許可され、Smith のワークステーションのアクセスは許可されません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

次の例の番号付き ACL では、Winter および Smith のワークステーションでの Web 閲覧が許可されません。

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次の例の名前付き ACL では、Jones のサブネットのアクセスが許可されます。

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次の例の名前付き ACL では、Jones のサブネットによる発信 Telnet の使用が許可されません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

ACL ロギング

ルータ ACL では、2 種類のロギングがサポートされています。**log** キーワードは、エントリと一致するパケットの詳細を示すロギング メッセージをコンソールに送信します。**log-input** キーワードは、ログ エントリに入力インターフェイスを含めます。

次の例の名前付き標準アクセス リスト *stan1* は、10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックは許可し、**log** キーワードを含めます。

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems
```

```
<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次の例の名前付き拡張アクセス リスト *ext1* は、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、UDP パケットはすべて拒否します。

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8
packets
```

IP ACL のロギング エントリはすべて `%SEC-6-IPACCESSLOG` で始まりますが、ACL の種類および一致するアクセス エントリによっては、形式が若干異なります。

次に、**log-input** キーワードを入力した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1
0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet
```

log キーワードを使用した同じ種類のパケットのログ メッセージには、入力インターフェイス情報が含まれません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1
packet
```

名前付き MAC 拡張 ACL の作成

VLAN 上またはレイヤ 2 インターフェイス上の非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。この手順は、他の名前付き拡張 ACL の設定手順と同様です。

（注） 名前付き MAC 拡張 ACL を、レイヤ 3 インターフェイスに適用できません。

mac access-list extended コマンドでサポートされる非 IP プロトコルの詳細については、このリリースのコマンド リファレンスを参照してください。

（注） **appletalk** は、コマンドラインのヘルプ ストリングには表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてはサポートされていません。

名前付き MAC 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name*	名前を使用して、拡張 MAC アクセス リストを定義します。
ステップ 3	{**deny** | **permit**} {**any** | **host** *source MAC address* | *source MAC address mask*} {**any** | **host** *destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap** *lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp** | *0-65535*] [**cos** *cos*]	拡張 MAC アクセスリスト コンフィギュレーション モードで、**permit** または **deny** を、すべての（**any**）送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定の **host** 送信元 MAC アドレス、およびすべての（**any**）宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに指定します。 （任意）次のオプションも入力できます。 • *type mask* : Ethernet II または Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）でカプセル化されたパケットの任意の EtherType 番号（10 進数、16 進数、または 8 進数）。一致をテストする前に *don't care* ビットのマスクが EtherType に任意で適用されます。 • **lsap** *lsap mask* : IEEE 802.2 カプセル化を使用したパケットの LSAP 番号（10 進数、16 進数、または 8 進数）。*don't care* ビットのマスクが任意で付加されます。 • **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp** : 非 IP プロトコル。 • **cos** *cos* : プライオリティの設定に使用する 0 ～ 7 の IEEE 802.1Q CoS 番号。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	アクセス リスト コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ACL 全体を削除するには、**no mac access-list extended** *name* グローバル コンフィギュレーション コマンドを使用します。名前付き MAC 拡張 ACL から個別の ACE を削除することもできます。

次に、*mac1* という名前のアクセス リストを作成および表示して、EtherType DECnet Phase IV トラフィックだけを拒否し、それ以外のタイプのトラフィックはすべて許可する例を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    10 deny   any any decnet-iv
    20 permit any any
```

レイヤ 2 インターフェイスへの MAC ACL の適用

MAC ACL を作成したら、それをレイヤ 2 インターフェイスに適用して、このインターフェイスへの非 IP トラフィックをフィルタリングできます。MAC ACL の適用時は、次の注意事項を考慮してください。

- VLAN のメンバーになっているレイヤ 2 インターフェイスに ACL を適用すると、レイヤ 2（ポート）ACL は、VLAN インターフェイスに適用された入力レイヤ 3 ACL や VLAN に適用された VLAN マップよりも優先されます。レイヤ 2 ポート上で受信した着信パケットは常に、そのポート ACL でフィルタリングされます。
- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アクセス リストは 1 つだけです。MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、以前に設定されていた ACL は新しい ACL で置換されます。

MAC アクセス リストを適用してレイヤ 2 インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。このインターフェイスは、物理レイヤ 2 インターフェイス（ポート ACL）を指定する必要があります。
ステップ 3	**mac access-group** {*name*} {**in**}	MAC アクセス リストを使用して、指定のインターフェイス宛てのアクセスを制御します。 ポート ACL は、着信方向でだけサポートされます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mac access-group** [**interface** *interface-id*]	このインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用される MAC アクセス リストを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定のアクセス グループを削除するには、**no mac access-group** {*name*} インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに MAC アクセス リスト *mac1* を適用して、このポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mac access-group mac1 in
```

（注）　**mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用される場合だけ有効です。EtherChannel ポート チャネルにはこのコマンドを使用できません。

スイッチはパケットを受信すると、着信 ACL と照合することでそのパケットを確認します。ACL がパケットを許可する場合、スイッチはパケットの処理を続行します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチはその ACL が適用されていないかのように動作し、すべてのパケットを許可します。ネットワーク セキュリティ用に未定義の ACL を使用する場合は、この動作に注意してください。

VLAN マップの設定

ここでは、VLAN マップの設定する方法を説明します。これは、VLAN 内のフィルタリングを制御する唯一の方法です。VLAN マップには方向の指定がありません。VLAN マップを使用して特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスの ACL を含める必要があります。VLAN マップにそのパケット タイプ（IP または MAC）に対する match コマンドがある場合、デフォルトのアクションでは、マップ内のどのエントリとも一致しないパケットは廃棄されます。そのパケット タイプに対する match コマンドがない場合、デフォルトではパケットが転送されます。

この項で使用しているコマンドの構文と使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

VLAN マップを作成し、それを 1 つまたは複数の VLAN に適用するには、次の手順を実行します。

ステップ 1　VLAN に適用する標準または拡張 IPv4 ACL または名前付き MAC 拡張 ACL を作成します。「標準および拡張 IPv4 ACL の作成」（P.38-7）および「VLAN マップの作成」（P.38-33）を参照してください。

ステップ 2　**vlan access-map** グローバル コンフィギュレーション コマンドを入力して、VLAN ACL マップ エントリを作成します。

ステップ 3　アクセスマップ コンフィギュレーション モードでは、任意で、**action**（**forward**（デフォルト）または **drop**）を入力します。また、**match** コマンドを入力して、（既知の MAC アドレスだけを格納した）IP パケットまたは非 IP パケットを指定し、このパケットを 1 つまたは複数の ACL（標準または拡張）と照合します。

（注）　VLAN マップが特定のパケット タイプ（IP または MAC）に対する match コマンドで設定されていて、マップ アクションが drop の場合は、このタイプと一致するパケットがすべて廃棄されます。VLAN マップに match コマンドがなく、設定されたアクションが drop の場合は、IP パケットとレイヤ 2 パケットがすべて廃棄されます。

ステップ 4　**vlan filter** グローバル コンフィギュレーション コマンドは、VLAN マップを 1 つまたは複数の VLAN に適用します。

ここでは、次の設定情報について説明します。

- 「VLAN マップ設定時の注意事項」（P.38-32）
- 「VLAN マップの作成」（P.38-33）
- 「VLAN への VLAN マップの適用」（P.38-35）
- 「ネットワークでの VLAN マップの使用」（P.38-36）

VLAN マップ設定時の注意事項

VLAN マップを設定する場合、次の注意事項に従ってください。

- インターフェイス上のトラフィックを拒否するよう設定された ACL がなく、VLAN マップが*設定されていない*場合は、すべてのトラフィックが許可されます。
- 各 VLAN マップは、一連のエントリで構成されます。VLAN マップ内のエントリの順序は重要です。スイッチに着信したパケットは、VLAN マップ内の最初のエントリと照合してテストされます。パケットが一致する場合は、VLAN マップのその部分に対して指定されたアクションが実行されます。一致しない場合は、パケットはマップ内の次のエントリと照合してテストされます。
- VLAN マップに特定のパケット タイプ（IP または MAC）に対する match コマンドが少なくとも 1 つあり、パケットがこれらの match コマンドのいずれとも一致しない場合、デフォルトではそのパケットが廃棄されます。VLAN マップ内にそのパケット タイプに対する match コマンドがない場合、デフォルトではパケットが転送されます。
- ACL が多数設定されていると、システムの起動に時間が掛かる可能性があります。
- ロギングは VLAN マップではサポートされません。
- スイッチが IP アクセス リストまたは MAC アクセス リストをレイヤ 2 インターフェイスに適用させている状態で、ポートが属する VLAN に VLAN マップを適用した場合、ポート ACL は VLAN マップよりも優先されます。
- VLAN マップの設定をハードウェアで適用できない場合、この VLAN 内のすべてのパケットをソフトウェアによってブリッジおよびルーティングする必要があります。
- プライマリ VLAN およびセカンダリ VLAN では VLAN マップを設定できます。ただし、プライベート VLAN のプライマリ VLAN とセカンダリ VLAN には、同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内でレイヤ 2 転送される場合、入力側と出力側で同じ VLAN マップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップは入力側で適用されます。
  - ホスト ポートからプロミスキャス ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN で設定された VLAN マップが適用されます。
  - プロミスキャス ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN で設定された VLAN マップが適用されます。

  プライベート VLAN の特定の IP トラフィックをフィルタリングするには、プライマリ VLAN とセカンダリ VLAN の両方に VLAN マップを適用する必要があります。プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」を参照してください。

設定例については、「ネットワークでの VLAN マップの使用」（P.38-36）を参照してください。

ルータ ACL と VLAN マップの両方の使用については、「VLAN マップおよびルータ ACL 設定時の注意事項」（P.38-38）を参照してください。

VLAN マップの作成

各 VLAN マップは、順序指定された一連のエントリで構成されます。VLAN マップ エントリの作成、追加、削除を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan access-map** *name* [*number*]	VLAN マップを作成し、マップに名前と（任意で）番号を付けます。この番号は、マップ内のエントリのシーケンス番号になります。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップの修正または削除時には、修正または削除するマップ エントリの番号を入力できます。 このコマンドを入力すると、アクセスマップ コンフィギュレーション モードになります。
ステップ 3	**action** {**drop** | **forward**}	（任意）マップ エントリのアクションを設定します。デフォルトは forward です。
ステップ 4	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]	（IP アドレスまたは MAC アドレスを使用している）パケットを 1 つまたは複数の標準または拡張アクセス リストと照合します。パケットは正しいプロトコル タイプのアクセス リストだけと照合されます。IP パケットは標準または拡張 IP アクセス リストと照合されます。非 IP パケットは名前付き MAC 拡張アクセス リストだけと照合されます。
ステップ 5	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**show running-config**	アクセス リスト コンフィギュレーションを表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

マップを削除するには、**no vlan access-map** *name* グローバル コンフィギュレーション コマンドを使用します。マップ内から 1 つのシーケンス エントリを削除するには、**no vlan access-map** *name number* グローバル コンフィギュレーション コマンドを使用します。

デフォルトのアクション（forward）を適用するには、**no action** アクセス マップ コンフィギュレーション コマンドを使用します。

VLAN マップでは、特定の permit キーワードや deny キーワードは使用しません。VLAN マップを使用してパケットを拒否するには、そのパケットと一致する ACL を作成し、アクションを drop に設定します。ACL 内の permit は一致と見なされます。ACL 内の deny は不一致と見なされます。

ACL および VLAN マップの例

次に、特定の目的のための ACL および VLAN マップを作成する例を示します。

例 1

次に、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、*ip1* ACL（TCP パケット）と一致するパケットがすべて廃棄されます。最初に、任意の TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1*ACL を作成します。VLAN マップには IP パケットに対する match コマンドがあるため、デフォルトのアクションでは、どの match コマンドとも一致しない IP パケットは廃棄されます。

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
```

```
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これまでのどの ACL とも一致しなかった IP パケット（つまり、TCP パケットでも UDP パケットでもないパケット）がすべて廃棄されます。

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

例 2

次の例の VLAN マップには、IP パケットに対してデフォルトのアクション drop と、MAC パケットに対してデフォルトのアクション forward が設定されています。このマップを標準 ACL 101 と、名前付き拡張アクセス リスト **igmp-match** および **tcp-match** とともに使用すると、次のような結果になります。

- UDP パケットはすべて転送されます。
- IGMP パケットはすべて廃棄されます。
- TCP パケットはすべて転送されます。
- その他の IP パケットはすべて廃棄されます。
- 非 IP パケットはすべて転送されます。

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

例 3

次の例の VLAN マップには、MAC パケットに対してデフォルトのアクション drop と、IP パケットに対してデフォルトのアクション forward が設定されています。このマップを MAC 拡張アクセス リスト **good-hosts** および **good-protocols** とともに使用すると、次のような結果になります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットは転送されます。
- decnet-iv または vines-ip プロトコルを使用した MAC パケットは転送されます。
- その他の非 IP パケットはすべて廃棄されます。
- IP パケットはすべて転送されます。

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any decnet-ip
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

例 4

次の例の VLAN マップには、すべてのパケット（IP および非 IP）に対してデフォルトのアクション drop が設定されています。このマップを例 2 および 3 のアクセス リスト **tcp-match** および **good-hosts** とともに使用すると、次のような結果になります。

- TCP パケットはすべて転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットは転送されます。
- その他の IP パケットはすべて廃棄されます。
- その他の MAC パケットはすべて廃棄されます。

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

VLAN への VLAN マップの適用

VLAN マップを 1 つまたは複数の VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan filter** *mapname* **vlan-list** *list*	VLAN マップを 1 つまたは複数の VLAN ID に適用します。 list には、単一の VLAN ID（22）、連続する範囲（10-22）、または VLAN ID のストリング（12, 22, 30）を指定できます。カンマやハイフンの前後のスペースは任意です。
ステップ 3	**show running-config**	アクセス リスト コンフィギュレーションを表示します。
ステップ 4	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN マップを削除するには、**no vlan filter** *mapname* **vlan-list** *list* グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN マップ 1 を VLAN 20 ～ 22 に適用する例を示します。

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

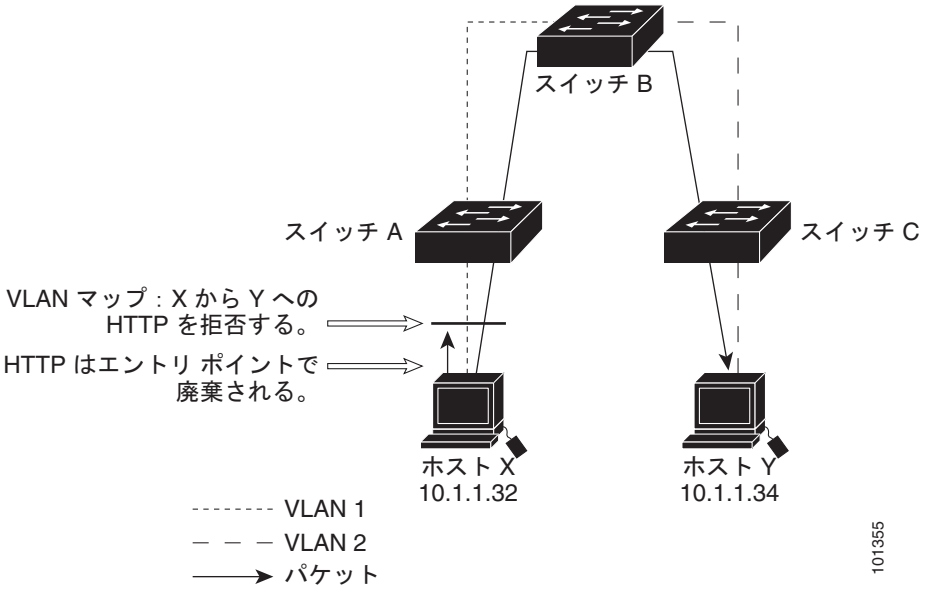
ネットワークでの VLAN マップの使用

ここでは、VLAN マップの一般的な使用法について説明します。

配線クローゼットの設定

配線クローゼットの設定では、スイッチ上でルーティングがイネーブルでない可能性があります。この設定でも、スイッチは VLAN マップと QoS 分類 ACL をサポートできます。図 38-4 では、ホスト X とホスト Y が異なる VLAN 内にあり、配線クローゼットのスイッチ A と C にそれぞれ接続されていると仮定します。ホスト X からホスト Y へのトラフィックは最終的にスイッチ B（ルーティングがイネーブルになっているレイヤ 3 スイッチ）によってルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィック エントリ ポイントであるスイッチ A でアクセス制御できます。

図 38-4　　配線クローゼットの設定



HTTP トラフィックがホスト X からホスト Y にスイッチングされないようにするには、ホスト X（IP アドレス 10.1.1.32）からホスト Y（IP アドレス 10.1.1.34）への HTTP トラフィックをスイッチ A ですべて廃棄し、トラフィックをスイッチ B にブリッジしないように、スイッチ A 上の VLAN マップを設定できます。

まず、HTTP ポート上で任意の TCP トラフィックを許可（一致）する IP アクセス リスト *http* を定義します。

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

次に、VLAN アクセス マップ *map2* を作成して、*http* アクセス リストと一致するトラフィックが廃棄され、その他の IP トラフィックはすべて転送されるようにします。

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
```

```
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

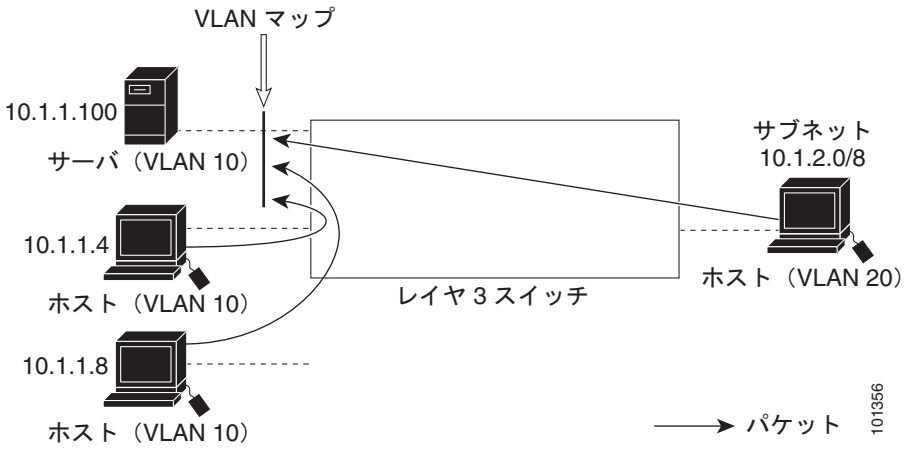
```
Switch(config)# vlan filter map2 vlan 1
```

別の VLAN 上のサーバへのアクセスの拒否

別の VLAN 上のサーバへのアクセスを制限できます。たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります（図 38-5 を参照）。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストがアクセスできないようにします。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 がアクセスできないようにします。

図 38-5　別の VLAN 上のサーバへのアクセスの拒否



次に、サブネット 10.1.2.0.8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 へのアクセスを拒否し、その他の IP トラフィックは許可する VLAN マップ SERVER 1 を作成して、別の VLAN 上のサーバへのアクセスを拒否する例を示します。最後に、マップ SERVER1 を VLAN 10 に適用します。

ステップ 1　正しいパケットと一致する IP ACL を定義します。

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl))# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl))# exit
```

ステップ 2　この ACL を使用して、SERVER1_ACL と一致する IP パケットを廃棄し、ACL と一致しない IP パケットを転送する VLAN マップを定義します。

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
```

```
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

ステップ 3　この VLAN マップを VLAN 10 に適用します。

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

VLAN マップとルータ ACL の併用

ブリッジド トラフィックとルーテッド トラフィックの両方をアクセス制御する場合、VLAN マップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせて使用します。入力と出力の両方のルーテッド VLAN インターフェイスでルータ ACL を定義し、ブリッジド トラフィックをアクセス制御する VLAN マップを定義できます。

パケット フローが ACL 内の VLAN マップの deny コマンドと一致する場合は、ルータ ACL の設定に関係なく、パケット フローが拒否されます。

（注）　ルータ ACL と VLAN マップを併用する際には、ルータ ACL でのロギングの必要があるパケットは、VLAN マップで拒否された場合、記録されません。

VLAN マップにパケット タイプ（IP または MAC）に対する match コマンドがあり、パケットがそのタイプと一致しない場合、デフォルトではそのパケットが廃棄されます。VLAN マップに match コマンドがなく、アクションが指定されていない状態で、パケットがどの VLAN マップ エントリとも一致しない場合は、そのパケットが転送されます。

ここでは、VLAN マップとルータ ACL の併用について説明します。

- 「VLAN マップおよびルータ ACL 設定時の注意事項」（P.38-38）
- 「VLAN に適用されたルータ ACL および VLAN マップの例」（P.38-39）

VLAN マップおよびルータ ACL 設定時の注意事項

次の注意事項は、同じ VLAN 上でルータ ACL *および* VLAN マップを使用する必要がある設定に適用されます。これらの注意事項は、ルータ ACL と VLAN マップを異なる VLAN 上にマッピングする設定には適用されません。

スイッチのハードウェアには、方向（入力および出力）ごとにセキュリティ ACL を 1 回検索します。このため、ルータ ACL と VLAN マップが同じ VLAN 上で設定されている場合は、これらを結合する必要があります。ルータ ACL と VLAN マップを結合すると、ACE の数が大幅に増える可能性があります。

ルータ ACL と VLAN マップを同じ VLAN 上に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定について次の注意事項があります。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつだけ設定できます。
- タイプが異なる場合の末尾のデフォルト アクションを除き、すべてのエントリのアクションを可能な限り単一にして ACL を記述するようにします。つまり、次のいずれかの形式を使用して ACL を記述します。

permit...
permit...
permit...
deny ip any any

または

deny...
deny...
deny...
permit ip any any

- ACL で複数のアクション（permit、deny）を定義する場合は、エントリ数を減らすために、アクション タイプごとにグループ化します。
- レイヤ 4 情報を ACL に含めないようにします。この情報を加えると、結合処理が複雑になります。完全なフロー（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）ではなく IP アドレス（送信元および宛先）に基づいて ACL をフィルタリングすると、最適な結合結果が得られます。可能な限り、IP アドレス内に *don't care* ビットを使用するのも効果的です。

  full-flow モードを指定する必要があり、ACL に IP ACE とレイヤ 4 情報を持つ TCP/UDP/ICMP ACE の両方が含まれている場合は、レイヤ 4 ACE をリストの末尾に置きます。これにより、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

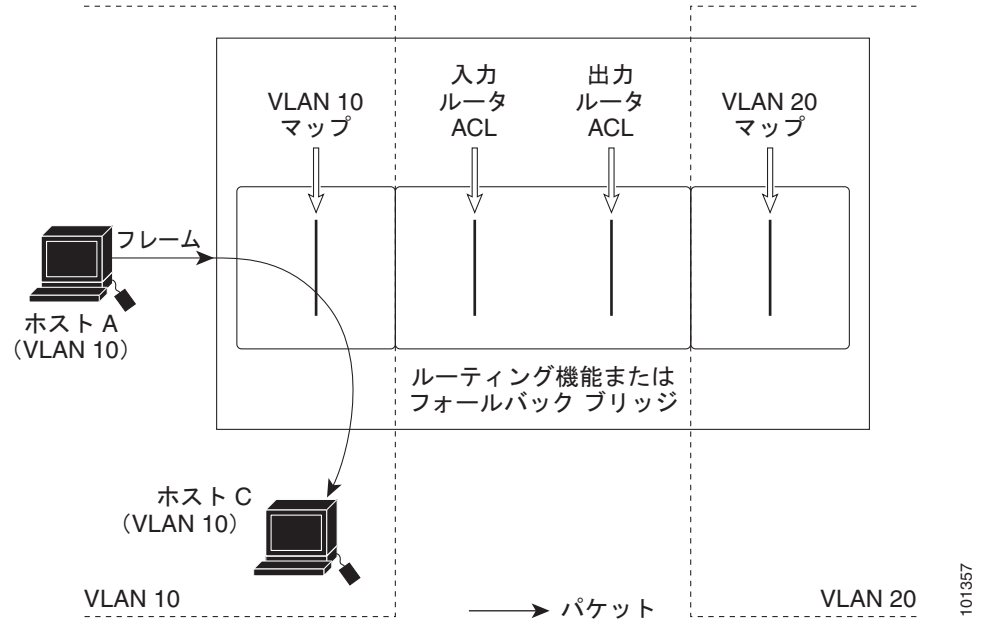
VLAN に適用されたルータ ACL および VLAN マップの例

ここでは、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを対象に、ルータ ACL と VLAN マップを VLAN に適用する例を示します。次の各図はパケットが宛先に転送される様子を示していますが、パケットのパスが VLAN マップまたは ACL を示す線を通過するたびに、パケットが転送されずに廃棄される可能性もあります。

ACL およびスイッチド パケット

図 38-6 に、VLAN 内でスイッチングされるパケットに ACL を適用する方法を示します。フォールバック ブリッジングによってルーティングまたは転送されずに VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップだけが適用されます。

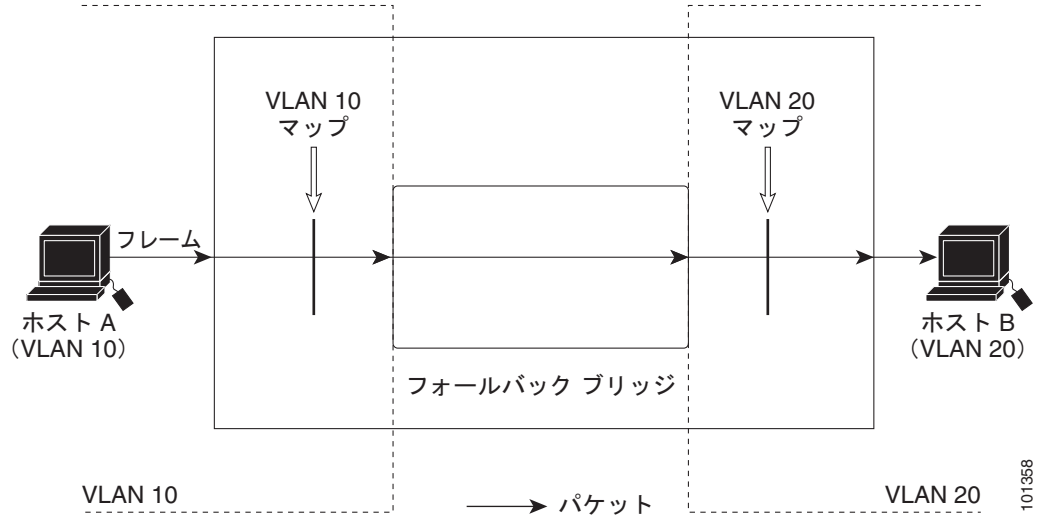
図 38-6　スイッチド パケットへの ACL の適用



ACL およびブリッジド パケット

図 38-7 に、フォールバック ブリッジド パケットに ACL を適用する方法を示します。ブリッジド パケットの場合は、レイヤ 2 ACL だけが入力 VLAN に適用されます。フォールバック ブリッジングが可能なのは、非 IP の非 ARP パケットだけです。

図 38-7　ブリッジド パケットへの ACL の適用

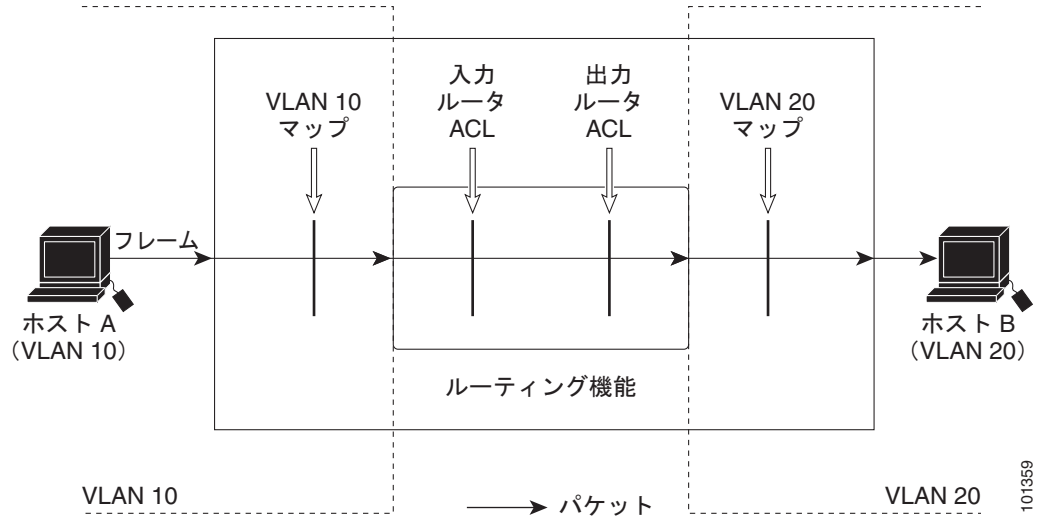


ACL およびルーテッド パケット

図 38-8 に、ルーテッド パケットに ACL を適用する方法を示します。ルーテッド パケットの場合は、次の順序で ACL が適用されます。

1. 入力 VLAN 用 VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN 用 VLAN マップ

図 38-8　　ルーテッド パケットへの ACL の適用

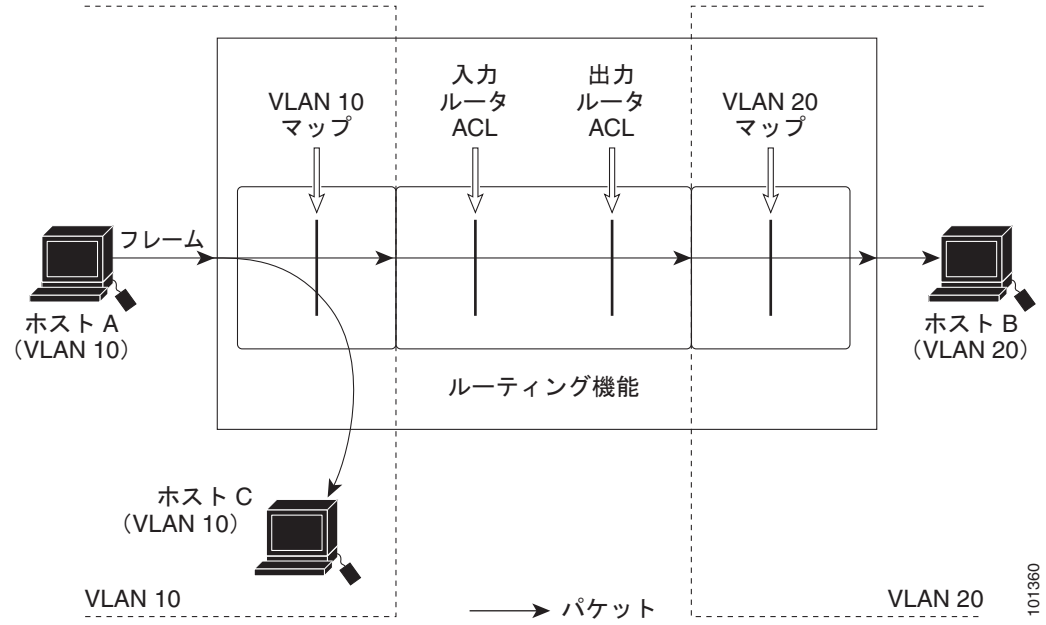


ACL およびマルチキャスト パケット

図 38-9 に、IP マルチキャスト用に複製されるパケットに ACL を適用する方法を示します。ルーティングされるマルチキャスト パケットには、2 つの異なる種類のフィルタが適用されます。1 つは入力 VLAN 内の他のポートである宛先用のフィルタで、もう 1 つはパケットのルーティング先となった他の VLAN 内の宛先用のフィルタです。このパケットは複数の出力 VLAN にルーティングされる可能性があります。この場合、それぞれの宛先 VLAN に異なるルータ出力 ACL と VLAN マップが適用されます。

最終的な結果としては、一部の出力 VLAN ではパケットが許可され、他の VLAN では拒否される場合もあります。許可された宛先には、パケットのコピーが転送されます。ただし、入力 VLAN マップ（図 38-9 の VLAN 10）がパケットを廃棄した場合は、どの宛先もパケットのコピーを受信しません。

図 38-9　マルチキャスト パケットへの ACL の適用



IPv4 ACL 設定の表示

スイッチ上で設定された ACL や、インターフェイスおよび VLAN に適用されている ACL を表示することができます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して ACL をレイヤ 2 またはレイヤ 3 インターフェイスに適用した場合は、インターフェイス上のアクセス グループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL を表示することもできます。この情報を表示するには 、表 38-2 に示す各特権 EXEC コマンドを使用します。

表 38-2　アクセス リストおよびアクセス グループを表示するためのコマンド

コマンド	目的
show access-lists [*number* | *name*]	現在の IP および MAC アドレス アクセス リスト（1 つまたはすべて）、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	現在のすべての IP アクセス リスト、または特定の IP アクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip interface *interface-id*	インターフェイスの詳細な設定およびステータスを表示します。インターフェイス上で IP がイネーブルになっていて、ACL が **ip access-group** インターフェイス コンフィギュレーション コマンドによって適用されている場合は、アクセス グループも表示されます。
show running-config [**interface** *interface-id*]	スイッチまたは指定したインターフェイスのコンフィギュレーション ファイルの内容を表示します。設定されたすべての MAC および IP アクセス リストや、インターフェイスに適用されているアクセス グループなどが表示されます。
show mac access-group [**interface** ***interface-i***d]	すべてのレイヤ 2 インターフェイスまたは指定したレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。

また、VLAN アクセス マップまたは VLAN フィルタ に関する情報も表示できます。VLAN マップ情報を表示するには、表 38-3 に示す各特権 EXEC コマンドを使用します。

表 38-3　VLAN マップ情報を表示するためのコマンド

コマンド	目的
show vlan access-map [*mapname*]	すべての VLAN アクセス マップまたは指定されたアクセス マップに関する情報を表示します。
show vlan filter [**access-map** *name* | **vlan** *vlan-id*]	すべての VLAN フィルタに関する情報や、指定された VLAN または VLAN アクセス マップに関する情報を表示します。

CHAPTER 39

QoS の設定

この章では、IE 3000 スイッチで Automatic QoS（auto-QoS）コマンドを使用して、または標準 QoS コマンドを使用して Quality of Service（QoS; サービス品質）を設定する手順について説明します。QoS を使用すると、特定のタイプのトラフィックを他のトラフィックよりも優先的に処理することができます。QoS を使用しないと、パケットの内容やサイズにかかわらず、スイッチは各パケットにベストエフォートサービスを提供します。パケットは、信頼性、遅延限界、またはスループットが保証されない状態で送信されます。QoS は、物理ポートおよび Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）で設定できます。ポリシー マップを適用するだけではなく、分類、キューイング、スケジューリングなどの QoS 設定を、物理ポートと SVI で同様に設定します。物理ポートで QoS を設定する場合は、非階層ポリシー マップをポートに適用します。SVI で QoS を設定する場合は、非階層または階層ポリシー マップを適用します。Catalyst 3750 Metro スイッチのドキュメンテーションでは、非階層ポリシー マップは非階層シングルレベル ポリシー マップと呼ばれ、階層ポリシー マップは階層デュアルレベル ポリシー マップと呼ばれます。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

このスイッチは、一部の Modular QoS CLI（MQC; モジュラー QoS コマンドライン インターフェイス）コマンドをサポートしています。MQC コマンドの詳細については、次の URL の「Modular Quality of Service Command-Line Interface Overview」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd908.html

QoS の概要

ネットワークは通常、ベスト エフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、適度なタイミングで配信される可能性はどのトラフィックでも同等です。輻輳が発生した場合に廃棄される可能性についても、すべてのトラフィックで同等です。

QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、その相対的な重要度に基づいてプライオリティを設定し、輻輳管理および輻輳回避技術を使用して優先的に処理することができます。QoS をネットワークに実装することで、ネットワーク パフォーマンスが予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS の実装は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）の新しい標準である Differentiated Service（Diff-Serv; ディファレンシエーテッド サービス）アーキテクチャに基づいて行われます。このアーキテクチャは、各パケットがネットワークに入るときに分類されることを既定してします。

この分類は IP パケット ヘッダー内で、非推奨の IP Type of Service（ToS; サービス タイプ）フィールドの 6 ビットを使用して、分類（クラス）情報として伝送されます。分類はレイヤ 2 フレームでも伝送できます。レイヤ 2 フレームまたはレイヤ 3 パケットのこれらの特別なビットについてここで説明し、図 39-1 に示します。

- レイヤ 2 フレームのプライオリティ ビット：

  レイヤ 2 Inter-Switch Link（ISL; スイッチ間リンク）フレーム ヘッダーには、Class of Service（CoS; サービス クラス）値の IEEE 802.1p クラスを最下位 3 ビットで 伝送する、1 バイトの User フィールドがあります。レイヤ 2 ISL トランクとして設定されたポートでは、すべてのトラフィックは ISL フレームに含まれます。

  レイヤ 2 IEEE 802.1Q フレーム ヘッダーには、ユーザ プライオリティ ビットと呼ばれる最上位 3 ビットで CoS 値を伝送する 2 バイトの Tag Control Information フィールドがあります。レイヤ 2 IEEE 802.1Q トランクとして設定されたポートでは、ネイティブ VLAN のトラフィックを除き、全てのトラフィックは IEEE 802.1Q フレームに含まれます。

  その他のフレーム タイプはレイヤ 2 CoS 値を伝送できません。

  レイヤ 2 CoS 値は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）の範囲で指定できます。

- レイヤ 3 パケットのプライオリティ ビット：

  レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point（DSCP）値を伝送できます。DSCP 値には IP precedence 値との下位互換性があるため、QoS はいずれの値の使用もサポートします。

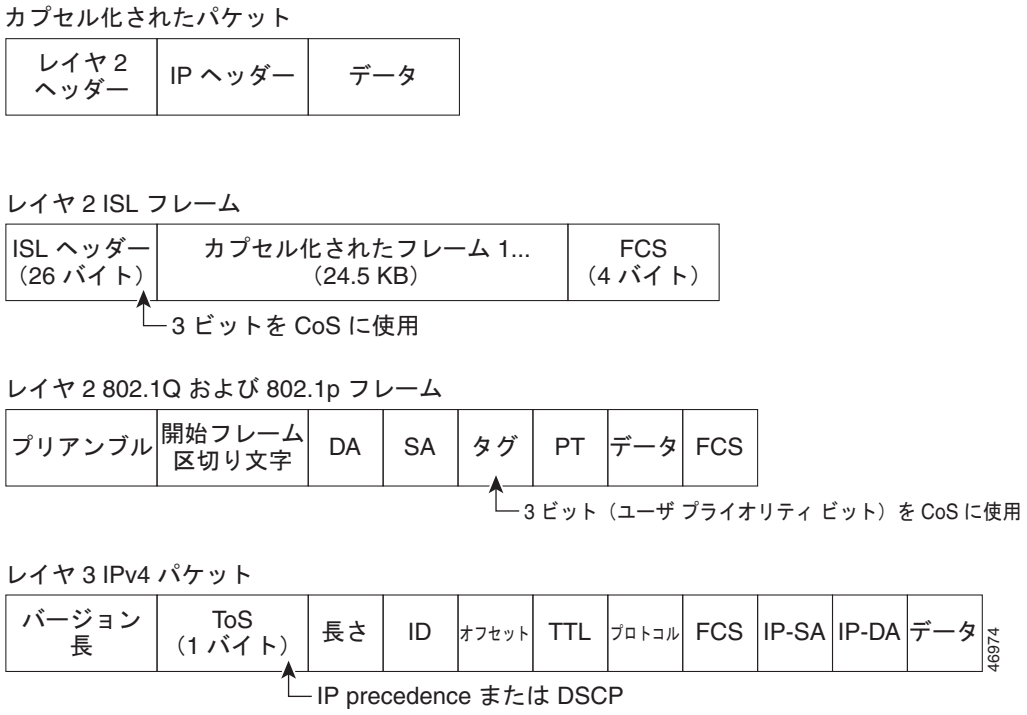
  IP precedence 値の範囲は 0 ～ 7 です。

  DSCP 値の範囲は 0 ～ 63 です。

（注） Cisco IOS Release 12.2(52)SE 以降は、デュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを使用した、IPv6 ポートベースの信頼をサポートします。IPv6 を実行しているスイッチでは、デュアル IPv4/IPv6 テンプレートを使用してスイッチをリロードしなければなりません。詳細については、第 10 章「SDM テンプレートの設定」を参照してください。

（注） IPv6 QoS はこのリリースではサポートされていません。

図 39-1　フレームおよびパケットの QoS 分類レイヤ



インターネットにアクセスするすべてのスイッチとルータは、クラス情報に基づいて、同じクラス情報を持つパケットは同じ方法で転送処理し、異なるクラス情報を持つパケットは異なる処理をします。パケットのクラス情報は、設定済みのポリシー、パケットの詳細な確認、またはその両方に基づいて、エンド ホストにより、または転送中にスイッチやルータにより、割り当てることができます。パケットの詳細な確認は、コア スイッチやルータがこの作業で過負荷にならないように、ネットワークのエッジの近くで行われます。

パス上のスイッチとルータは、クラス情報を使用して、トラフィック クラスごとに割り当てるリソースの量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの個々の装置の動作は、Per-Hop Behavior（PHB）と呼ばれます。パス上のすべての装置が一貫した PHB を提供することにより、エンドツーエンドの QoS ソリューションを構築できます。

ネットワークに QoS を実装する作業は、インターネットワーキング装置により提供される QoS 機能、ネットワークのトラフィック タイプおよびパターン、また、着信および発信トラフィックに必要な制御の細かさのレベルによって、単純にも複雑にもなります。

基本的な QoS モデル

QoS を実装するには、スイッチが個々のパケットまたはフローを区別（分類）し、パケットがスイッチを通過するときに特定のサービス品質を示すためのラベルを割り当て、設定済みのリソースの使用限界にパケットが準拠するようにし（ポリシングおよびマーキング）、リソースの競合が発生するすべての状況でさまざまな処理を提供する（キューイングおよびスケジューリング）必要があります。また、スイッチから送信されたトラフィックが特定のトラフィック プロファイルを満たすようにする（シェイピング）必要もあります。

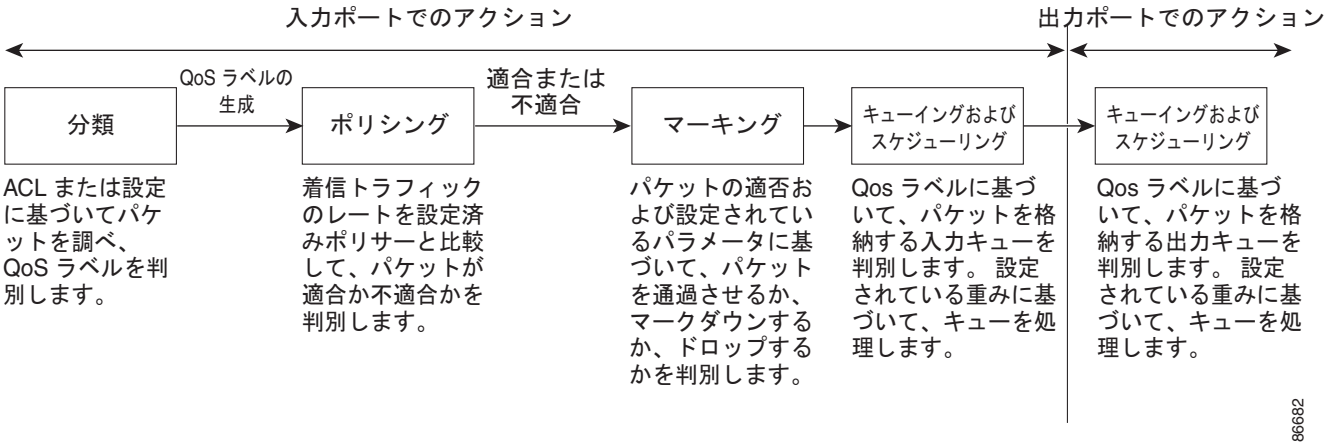
図 39-2 に、基本的な QoS モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、キューイング、スケジューリングが含まれます。

- パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。スイッチは、パケット内の CoS または DSCP を QoS ラベルにマッピングし、トラフィックの種類を区別します。生成される QoS ラベルは、このパケットで今後実行されるすべての QoS アクションを識別します。詳細については、「分類」（P.39-5）を参照してください。
- ポリシングでは、着信トラフィックのレートを設定済みのポリサーと比較することにより、パケットがプロファイル内かプロファイル外かを判別します。ポリサーは、トラフィック フローにより消費される帯域幅を制限します。その結果はマーカに渡されます。詳細については、「ポリシングおよびマーキング」（P.39-9）を参照してください。
- マーキングでは、パケットがプロファイル外のときに実行するアクションのポリサーおよび設定情報を評価し、パケットの処理（無修正でのパケットの通過、パケット内の QoS ラベルのマークダウン、またはパケットの廃棄）を決定します。詳細については、「ポリシングおよびマーキング」（P.39-9）を参照してください。
- キューイングでは、QoS ラベルとそれに対応する DSCP または CoS 値を評価し、2 つの入力キューのどちらにパケットを格納するかを選択します。キューイングは、輻輳回避メカニズムである Weighted Tail-Drop（WTD）アルゴリズムにより拡張されています。スレッシュホールドを超えると、パケットは廃棄されます。詳細については、「キューイングとスケジューリングの概要」（P.39-14）を参照してください。
- スケジュールでは、設定された Shaped Round Robin（SRR; シェイプド ラウンド ロビン）の重みに基づいてキューを処理します。入力キューの 1 つはプライオリティ キューであり、SRR は他のキューを処理する前に、設定済みの共有に従いプライオリティ キューを処理します。詳細については、「SRR のシェーピングおよび共有」（P.39-15）を参照してください。

出力ポートでのアクションには、キューイングとスケジューリングがあります。

- キューイングでは、4 つの出力キューのどれを使用するかを選択する前に、QoS パケット ラベルとそれに対応する DSCP または CoS 値を評価します。複数の入力ポートが 1 つの出力ポートにデータを同時に送信すると輻輳が発生するため、WTD でトラフィック クラスを区別し、QoS ラベルに基づいてパケットに異なるスレッシュホールドを適用します。スレッシュホールドを超えると、パケットは廃棄されます。詳細については、「キューイングとスケジューリングの概要」（P.39-14）を参照してください。
- スケジューリングでは、設定済みの SRR の共有された、またはシェーピングされた重みに基づいて 4 つの出力キューを処理します。キューの 1 つ（キュー 1）を緊急キューにできます。緊急キューは、他のキューを処理する前に、空になるまで処理されます。

図 39-2　基本的な QoS モデル



分類

分類は、パケットのフィールドを確認することで、トラフィックの種類を区別するプロセスです。分類は、スイッチで QoS がグローバルにイネーブルになっている場合に限りイネーブルになります。デフォルトでは、QoS はグローバルにディセーブルになるため、分類は行われません。

分類中にスイッチは検索を行い、QoS ラベルをパケットに割り当てます。QoS ラベルは、パケットに対して実行されるすべての QoS アクションと、パケットの送信元のキューを識別します。

QoS ラベルは、パケットの DSCP または CoS 値に基づいており、そのパケットに対して実行されるキューイング アクションとスケジューリング アクションを決定します。図 39-3（P.39-7）に示すように、ラベルは信頼設定とパケット タイプに応じてマッピングされます。

着信トラフィックの分類に使用するフレームまたはパケットのフィールドは、ユーザが指定します。非 IP トラフィックでは、図 39-3 に示す分類オプションがあります。

- 着信フレームの CoS 値を信頼します（CoS を信頼するようにポートを設定する）。次に、設定可能な CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。レイヤ 2 ISL フレーム ヘッダーは、1 バイトの User フィールドの最下位 3 ビットで CoS 値を伝送します。レイヤ 2 IEEE 802.1Q フレーム ヘッダーは、Tag Control Information フィールドの最上位 3 ビットで CoS 値を伝送します。CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。
- 着信フレームの DSCP または IP precedence 値を信頼します。これらの設定は、非 IP トラフィックでは意味がありません。これらのいずれかのオプションを使用してポートを設定したときに非 IP トラフィックを受信すると、スイッチは CoS 値を割り当て、CoS/DSCP マップから内部 DSCP 値を生成します。スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表す CoS 値を生成します。
- 設定されたレイヤ 2 MAC Access Control List（ACL; アクセス制御リスト）に基づいて分類を行います。この場合、MAC 送信元アドレス、MAC 宛先アドレス、その他のフィールドを確認できます。ACL が設定されていない場合は、DSCP および CoS 値としてパケットに 0 が割り当てられます。これはベストエフォート トラフィックを意味します。ACL が設定されている場合は、ポリシーマップ アクションが DSCP または CoS 値を指定し、着信フレームに割り当てます。

IP トラフィックでは、図 39-3 に示す分類オプションがあります。

- 着信パケットの DSCP 値を信頼（DSCP を信頼するようにポートを設定）し、同じ DSCP 値をパケットに割り当てます。IETF は、1 バイトの ToS フィールドの最上位 6 ビットを DSCP として定義します。特定の DSCP 値によって表されるプライオリティは設定が可能です。DSCP 値の範囲は 0 ～ 63 です。

  2 つの QoS 管理ドメイン間の境界にあるポートでは、設定可能な DSCP/DSCP 変換マップを使用して、DSCP を別の値に修正できます。

- 着信パケットの IP precedence 値を信頼（IP precedence を信頼するようにポートを設定）し、設定可能な IP precedence/DSCP マップを使用して、パケットの DSCP 値を生成します。IP Version 4 の仕様では、1 バイトの ToS フィールドの最上位 3 ビットを IP precedence として定義しています。IP precedence 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

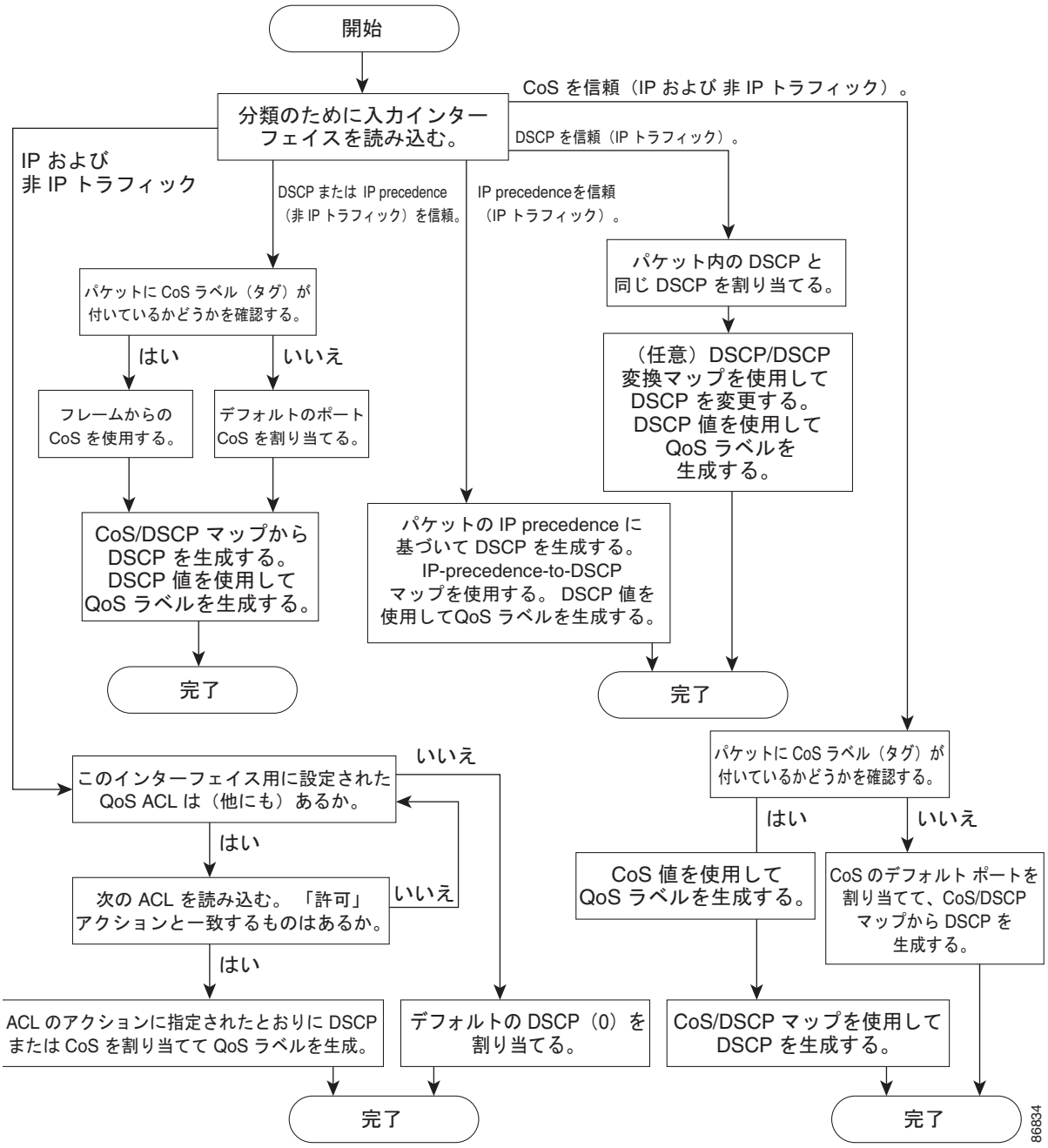
- 着信パケットの CoS 値（ある場合）を信頼し、CoS/DSCP マップを使用することで、パケットの DSCP 値を生成します。CoS 値がない場合は、デフォルトのポート CoS 値を使用します。

- 設定された IP 標準 ACL または拡張された ACL に基づいて分類を行います。この場合、IP ヘッダーのさまざまなフィールドを確認します。ACL が設定されていない場合は、DSCP および CoS 値としてパケットに 0 が割り当てられます。これはベストエフォート トラフィックを意味します。ACL が設定されている場合は、ポリシーマップ アクションが DSCP または CoS 値を指定し、着信フレームに割り当てます。

このセッションで説明したマップについては、「マッピング テーブル」（P.39-13）を参照してください。ポートの信頼状態の設定については、「ポートの信頼状態を使用した分類の設定」（P.39-38）を参照してください。

分類後、パケットはポリシング、マーキング、入力キューイングおよびスケジューリングの各段階に送信されます。

図 39-3　分類のフローチャート



QoS ACL に基づく分類

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用して、同じ特性を持つパケットのグループ（クラス）を定義できます。QoS のコンテキストでは、Access Control Entry（ACE; アクセス制御エントリ）の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が発生すると（最初の一致の原則）、指定された QoS に関連するアクションが実行されます。
- 拒否アクションとの一致が発生すると、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が発生しないまま、すべての ACE の確認が終了すると、パケットでは QoS の処理は行われず、スイッチはパケットにベストエフォートサービスを提供します。
- 複数の ACL がポートで設定されている場合は、許可アクションを使用する最初の ACL にパケットが一致した後に検索が停止し、QoS 処理が開始されます。

（注）　アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。

トラフィック クラスが ACL を使用して定義された後、このクラスにポリシーを付加できます。ポリシーには、それぞれ指定されたアクションを持つ複数のクラスを含めることができます。ポリシーには、特定の集約としてクラスを分類する（DSCP を割り当てるなど）、またはクラスをレート制限するコマンドが含まれることがあります。次に、このポリシーを特定のポートに付加すると、そのポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類するには、**access-list** グローバル コンフィギュレーション コマンドを使用してします。レイヤ 2 MAC ACL を実装して 非 IP トラフィックを分類するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します、設定の詳細については、「QoS ポリシーの設定」（P.39-44）を参照してください。

クラス マップとポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）を指定し、これを他のすべてのトラフィックから分離するために使用するメカニズムです。クラス マップでは、さらに詳細に分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL によって定義されるアクセス グループとの照合や、DSCP または IP precedence 値の特定のリストとの照合を含めることができます。分類するトラフィックのタイプが 2 つ以上ある場合は、別のクラス マップを作成して別の名前を使用できます。パケットをクラスマップ条件と照合した後で、ポリシー マップを使用してさらに分類します。

ポリシー マップは、対象のトラフィック クラスを指定します。アクションには、トラフィック クラスの CoS、DSCP、または IP precedence 値の信頼、トラフィック クラスの特定への DSCP または IP precedence 値の設定、またはトラフィック帯域幅の制限と、トラフィックがプロファイル外のときに実行するアクションの指定などが含まれます。ポリシー マップを有効にするには、あらかじめこれをポートに付加する必要があります。

class-map グローバル コンフィギュレーション コマンドまたは **class** ポリシーマップ コンフィギュレーション コマンドを作成します。多くのポートでマップを共有する場合は、**class-map** コマンドを使用する必要があります。**class-map** コマンドを入力すると、スイッチはクラスマップ コンフィギュレーション モードに入ります。このモードでは、**match** クラスマップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

class class-default ポリシー マップ コンフィギュレーション コマンドを使用して、デフォルト クラスを設定できます。分類されないトラフィック（トラフィック クラスで指定されている一致基準に適合しないトラフィック）は、デフォルト トラフィックとして処理されます。

policy-map グローバル コンフィギュレーション コマンドを使用して、ポリシー マップを作成し、名前を指定します。このコマンドを入力すると、スイッチはポリシーマップ コンフィギュレーション モードに入ります。このモードでは、**class**、**trust**、または **set** ポリシーマップ コンフィギュレーション コマンドおよびポリシーマップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシー マップには、ポリサー、トラフィックの帯域幅の制限、制限を超えたときに実行するアクションを定義する **police** および **police aggregate** ポリシーマップ クラス コンフィギュレーション コマンドを含めることができます。

ポリシー マップをイネーブルにするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートにマップを付加します。

非階層ポリシー マップは物理ポートまたは SVI に適用できます。ただし、階層ポリシー マップは SVI だけに適用できます。階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。2 つ目はインターフェイス レベルで、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。インターフェイスレベルのアクションは、インターフェイスレベルのポリシー マップで指定されます。

詳細については、「ポリシングおよびマーキング」（P.39-9）を参照してください。設定の詳細については、「QoS ポリシーの設定」（P.39-44）を参照してください。

ポリシングおよびマーキング

パケットを分類し、DSCP または CoS ベースの QoS ラベルを割り当てた後、図 39-4 に示すように、ポリシングおよびマーキング プロセスを開始できます。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が含まれます。限度を超えたパケットは、*プロファイル外*または*不適合*と見なされます。各ポリサーは、パケットがプロファイル内かプロファイル外かをパケットごとに確認し、パケットに対するアクションを指定します。マーカによって実行されるこれらのアクションには、無修正でのパケットの通過、パケットの廃棄、またはパケットに割り当てられた DSCP を修正（マークダウン）した上でのパケットの通過の許可などが含まれます。設定可能なポリシングされた DSCP マップは、新しい DSCP ベースの QoS ラベルをパケットに提供します。ポリシングされた DSCP マップについては、「マッピング テーブル」（P.39-13）を参照してください。マークダウンされたパケットは、元の QoS ラベルと同じキューを使用して、フローのパケットの順番が乱れないようにします。

（注） ブリッジドであるか、ルーテッドであるかにかかわらず、すべてのトラフィックにはポリサーが適用されます（ポリサーが設定されている場合）。その結果、ブリッジド パケットは、ポリシングおよびマーキングされるときに廃棄されたり、DSCP または CoS フィールドが修正されたりすることがあります。

ポリシング（individual または aggregate ポリサー）は、物理ポートまたは SVI で設定できます。物理ポートでは、信頼状態の設定、パケットの新しい DSCP または IP pecedence 値の設定、individual または aggregate ポリサーの定義ができます。物理ポートでのポリシングの設定の詳細については、「物理ポートでのポリシング」（P.39-10）を参照してください。SVI でポリシー マップを設定する場合は、セカンダリ インターフェイスレベル ポリシー マップだけで、階層ポリシー マップを作成して、individual ポリサーを定義できます。詳細については、「SVI でのポリシング」（P.39-11）を参照してください。

ポリシー マップとポリシング アクションを設定した後、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、ポリシーを入力ポートまたは SVI に付加します。設定情報については、「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）、「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）、および「aggregate ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング」（P.39-62）を参照してください。

物理ポートでのポリシング

物理ポートのポリシー マップでは、次のタイプのポリサーを作成できます。

- individual：QoS は、ポリサーで指定された帯域幅限度を、一致する各トラフィック クラスに個別に適用します。このタイプのポリサーは、**police** ポリシーマップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップ内部で設定します。
- aggregate：QoS はポリサーで指定された帯域幅限度を、一致するすべてのトラフィック フローに累積的に適用します。このタイプのポリサーは、**police aggregate** ポリシーマップ クラス コンフィギュレーション コマンドを使用し、ポリシー マップ内部で aggregate ポリサー名を指定することで設定します。ポリサーの帯域幅限度は、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用して指定します。このように、aggregate ポリサーは、ポリシー マップ内の複数のトラフィック クラスにより共有されます。

（注）　SVI には individual ポリサーだけを設定できます。

ポリシングはトークンバケット アルゴリズムを使用します。各フレームがスイッチにより受信されると、トークンがバケットに追加されます。バケットには穴があり、平均トラフィック レート（ビット/秒）として指定したレートでリークが発生します。トークンがバケットに追加されるたびに、スイッチはバケットに十分な空間があることを確認します。十分な空間がない場合は、パケットに不適合のマークが付き、指定されたポリサー アクションが実行されます（廃棄またはマークダウン）。

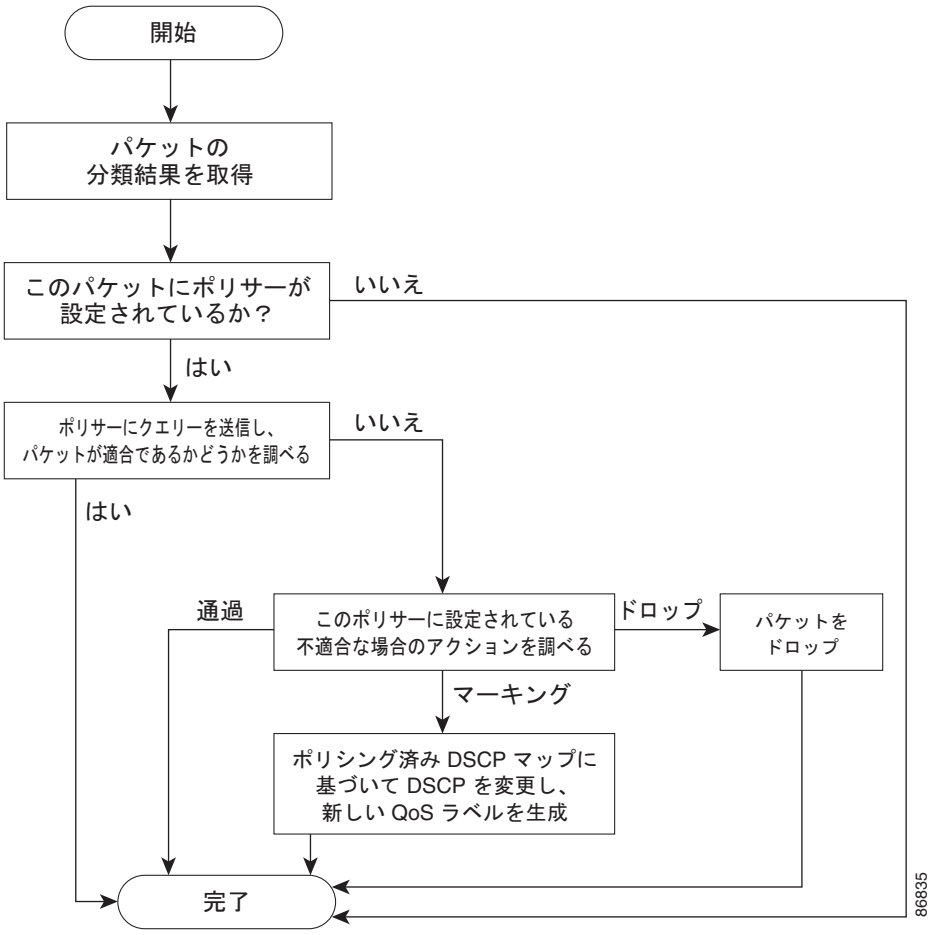
バケットが満杯になるまでの速度は、バケットの深さ（burst-byte）、トークンの削除レート（rate-b/s）、および平均レートを超えているバーストの継続時間によって決まります。バケットのサイズによりバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バーストが短い場合は、バケットがオーバーフローすることはなく、トラフィック フローに対してアクションは実行されません。しかし、バーストが長く、レートが高い場合は、バケットがオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *rate-bps* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。

図 39-4 に、ポリシングおよびマーキング プロセスを示します。次のタイプのポリシー マップが設定されます。

- 物理ポートの非階層ポリシー マップ。
- SVI に付加されたインターフェイス レベルの階層ポリシー マップ。物理ポートは、このセカンダリ ポリシー マップで指定されます。

図 39-4　物理ポートでのポリシングおよびマーキングのフローチャート



SVI でのポリシング

（注）　SVI で individual ポリサーを使用して階層ポリシー マップを設定する前に、その SVI に属する物理ポートで、VLAN ベースの QoS をイネーブルにする必要があります。ポリシー マップは SVI に付加されますが、individual ポリサーは、階層ポリシー マップのセカンダリ インターフェイス レベルで指定された物理ポート上のトラフィックだけに影響を与えます。

階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。もう 1 つはインターフェイス レベルで、インターフェイス レベルのポリシー マップに指定されていて、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。

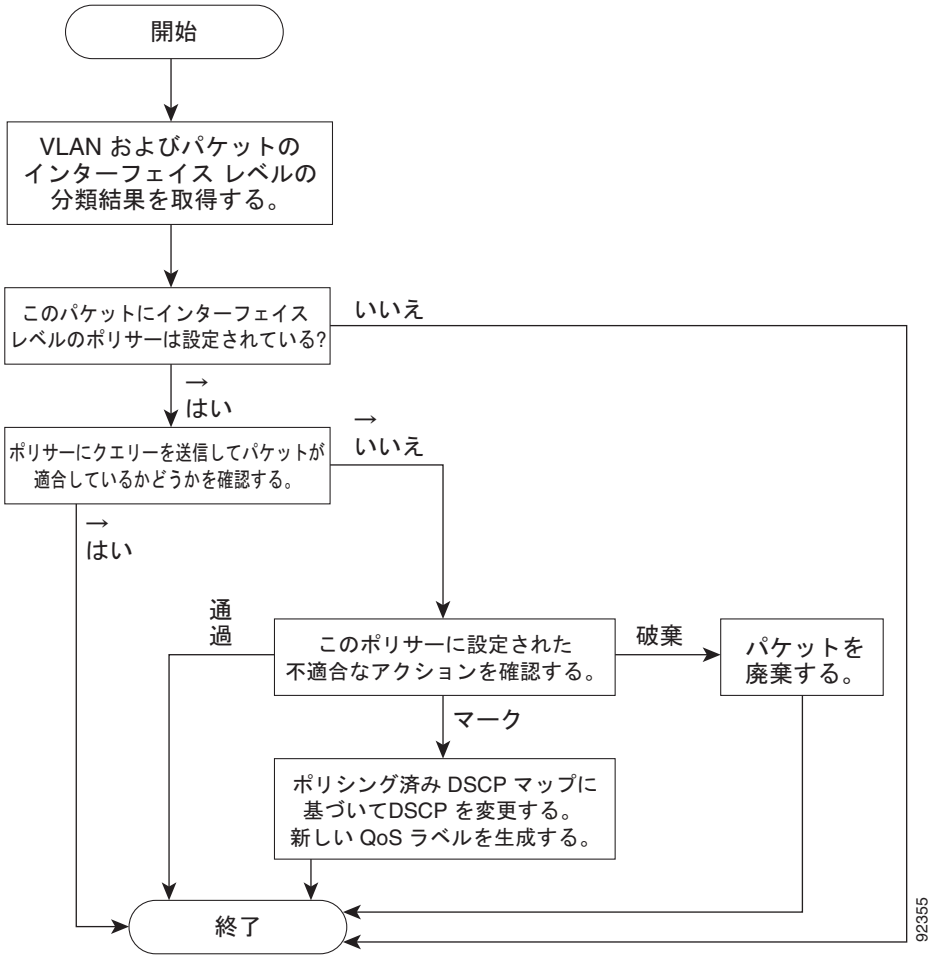
SVI にポリシングを設定する場合は、次の 2 つのレベルを持つ階層ポリシー マップを作成および設定できます。

- VLAN レベル：ポートの信頼状態を指定する、またはパケットの新しい DSCP または IP precedence 値を設定するクラス マップおよびクラスを設定することにより、このプライマリ レベルを作成します。VLAN レベルのポリシー マップは、SVI の VLAN だけに適用され、ポリサーはサポートしません。
- インターフェイス レベル：SVI に属する物理ポートの individual ポリサーを指定するクラス マップとクラスを設定することにより、このセカンダリ レベルを作成します。インターフェイスレベルのポリシー マップは individual ポリサーだけをサポートし、aggregate ポリサーはサポートしません。VLAN レベルのポリシー マップで定義されたクラスごとに、異なるインターフェイス レベル ポリシー マップを設定できます。

階層ポリシー マップの例は、「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）を参照してください。

図 39-5 に、SVI に階層ポリシーがマップされている場合のポリシングおよびマーキングのプロセスを示します。

図 39-5　SVI でのポリシングとマーキングのフローチャート



マッピング テーブル

QoS 処理の実行時に、スイッチでは、分類段階の DSCP または CoS 値に基づく QoS ラベルを使用して、全てのトラフィック（非 IP トラフィックも含む）のプライオリティが表されます。

- 分類中に、QoS は設定可能なマッピング テーブルを使用して、受信した CoS、DSCP、または IP precedence 値から対応する DSCP または CoS 値を取得します。これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどが含まれます。これらのマップは、**mls qos map cos-dscp** および **mls qos map ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用して設定します。

  DSCP 信頼状態で設定された入力ポートで、DSCP 値が QoS ドメイン間で異なる場合は、設定可能な DSCP/DSCP 変換マップを、2 つの QoS ドメイン間の境界上のポートに適用できます。このマップは、**mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドを使用して設定します。

- ポリシングの実行中に、QoS は別の DSCP 値を IP または非 IP パケットに割り当てることができます（パケットがプロファイル外で、ポリサーがマークダウン値を指定している場合）。この設定可能なマップは、ポリシングされた DSCP マップと呼ばれます。このマップは、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用して設定します。

- トラフィックがスケジューリング段階に入る前に、QoS は、QoS ラベルに従ってパケットを入力および出力キューに格納します。QoS ラベルは、パケットの DSCP または CoS 値に基づいており、DSCP 入力および出力キュー スレッシュホールド マップによって、または CoS 入力および出力キュー スレッシュホールド マップによってキューを選択します。入力または出力キューに加えて、QOS ラベルは WTD スレッシュホールド値も識別します。これらのマップは、**mls qos srr-queue** {**input** | **output**} **dscp-map** および **mls qos srr-queue** {**input** | **output**} **cos-map** グローバル コンフィギュレーション コマンドを使用して設定します。

CoS/DSCP、DSCP/CoS、および IP precedence/DSCP マップのデフォルト値は、ネットワークに適している場合と、適していない場合があります。

デフォルトの DSCP/DSCP 変換マップとデフォルトのポリシングされた DSCP マップはヌル マップであり、着信 DSCP 値を同じ DSCP 値にマッピングします。DSCP/DSCP 変換マップは、特定のポートに適用する唯一のマップです。その他のすべてのマップは、スイッチ全体に適用されます。

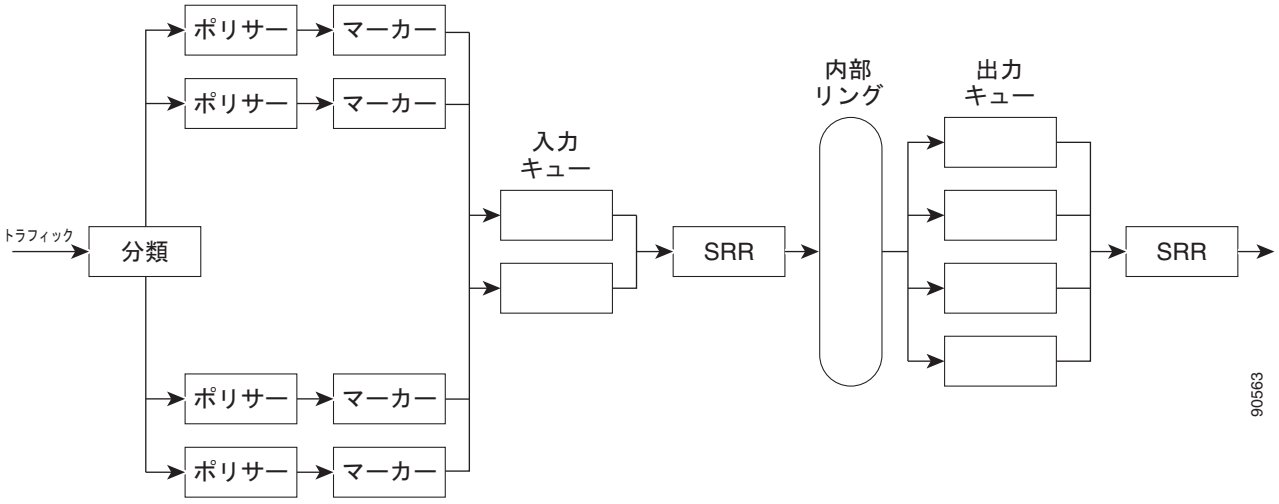
設定の詳細については、「DSCP マップの設定」（P.39-65）を参照してください。

DSCP および CoS 入力キューのスレッシュホールド マップについては、「入力キューでのキューイングおよびスケジューリング」（P.39-16）を参照してください。DSCP および CoS 出力キューのスレッシュホールド マップについては、「出力キューでのキューイングおよびスケジューリング」（P.39-18）を参照してください。

キューイングとスケジューリングの概要

図 39-6 に示すように、スイッチには、輻輳の防止に役立つキューが特定のポイントにあります。

図 39-6　入力および出力キューの場所



すべてのポートの入力帯域幅の合計が内部リングの帯域幅を超えることがあるため、入力キューは、パケットの分類、ポリシング、およびマーキングの後、かつスイッチ ファブリックへのパケットの転送前に配置されます。複数の入力ポートが出力ポートにパケットを同時に送信し、輻輳の原因になることがあるため、出力キューは内部リングの後に配置されます。

WTD

入力キューと出力キューのいずれも、weighted tail drop（WTD）と呼ばれるテール廃棄輻輳回避メカニズムの拡張バージョンを使用しています。WTD は、キューの長さを管理し、トラフィック分類別の廃棄優先度を設定する目的で、キューに実装されます。

フレームが特定のキューに入れられると、WTD は、そのフレームに割り当てられた QoS ラベルを使用して別のスレッショルドを適用します。その QoS ラベルのスレッショルドを超えると（宛先キューで使用可能な領域がフレームのサイズを下回ると）、スイッチはフレームを廃棄します。

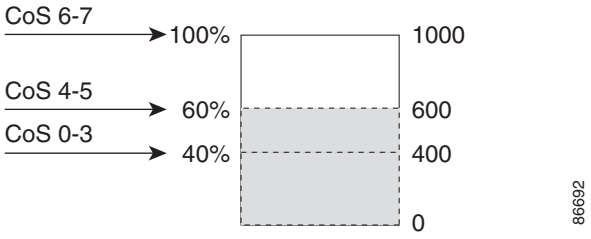
各キューには 3 つのスレッショルド値があります。QOS ラベルは、3 つのスレッショルド値からフレームに適用する値を決定します。3 つのスレッショルドのうち、2 つは設定可能で（明示的）、1 つは設定変更ができません（暗黙）。

図 39-7 に、サイズが 1000 フレームのキューに対して機能する WTD の例を示します。3 つの廃棄パーセンテージ、40%（400 フレーム）、60%（600 フレーム）、100%（1000 フレーム）が設定されています。これらのパーセンテージは、40% のスレッショルドでは最大 400 のフレームを、60% のスレッショルドでは最大 600 のフレームを 、100% のスレッショルドでは最大 1000 のフレームをキューに入れられることを意味します。

この例では、CoS 値 6 および 7 は他の CoS 値よりも重要であり、100% の廃棄スレッショルドに割り当てられます（キューが満杯の状態）。CoS 値 4 および 5 は 60% のスレッショルドに、CoS 値 0 ～ 3 は 40% のスレッショルドに割り当てられます。

すでに 600 のフレームでキューが満杯になっているときに、新しいフレームが到着したとします。このフレームには、CoS 値 4 および 5 が含まれ、60% のスレッシュホールドが適用されます。このフレームがキューに追加されると、スレッシュホールドを超えるため、スイッチはそのフレームを廃棄します。

図 39-7　　WTD およびキューの動作



詳細については、「DSCP または CoS 値の入力キューへのマッピングと、WTD スレッシュホールドの設定」（P.39-71）、「出力キューセットのバッファ領域の割り当てと WTD スレッシュホールドの設定」（P.39-75）、および「DSCP または CoS 値の出力キューとスレッシュホールド ID へのマッピング」（P.39-78）を参照してください。

SRR のシェーピングおよび共有

入力キューと出力キューは、いずれもパケットの送信レートを制御する SRR によって処理されます。入力キューでは、SRR はパケットを内部リングに送信します。出力キューでは、SRR はパケットを出力ポートに送信します。

出力キューでは、SRR を共有またはシェーピング用に設定できます。ただし、入力キューでは、共有がデフォルトのモードであり、サポートされる唯一のモードです。

シェーピング モードでは、出力キューは帯域幅のパーセンテージが保証され、この値にレートが制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を越えて使用できません。シェーピングによって、トラフィック フローの時間的変動がより均一になり、バースト性の高いトラフィックによるピークや谷が軽減されます。シェーピングでは、各重みの絶対値を使用して、そのキューで使用可能な帯域幅を計算します。

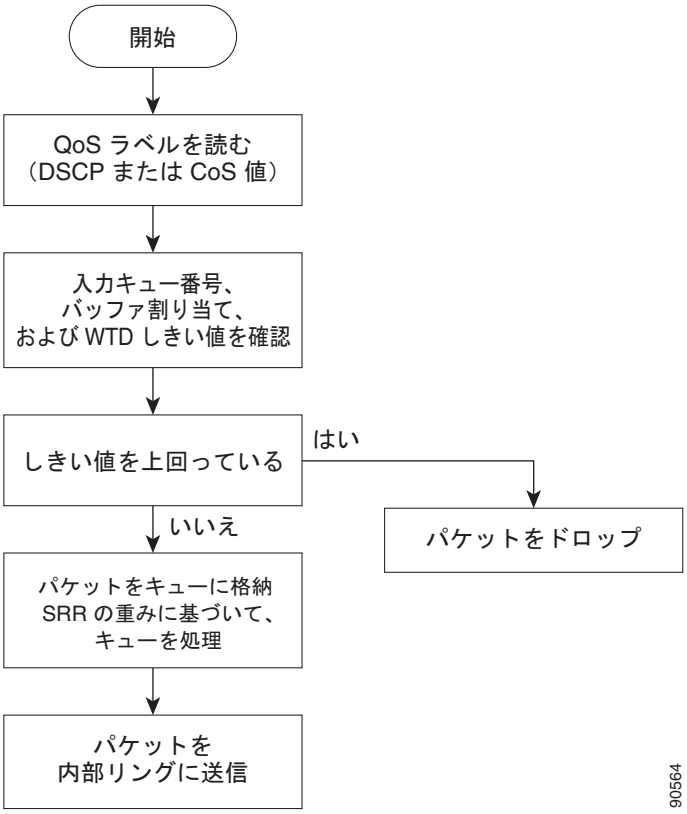
共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、キューが空でそれ以上リンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。共有では、デキューイングの頻度は重みの比によって制御され、絶対値には意味はありません。シェーピングと共有は、インターフェイスごとに設定されます。各インターフェイスには固有の設定が可能です。

詳細については、「入力キュー間での帯域幅の割り当て」（P.39-73）、「出力キューでの SRR のシェーピングされた重みの設定」（P.39-79）、および「出力キューでの SRR の共有された重みの設定」（P.39-80）を参照してください。

入力キューでのキューイングおよびスケジューリング

図 39-8 に、入力ポートのキューイングとスケジューリングのフローチャートを示します。

図 39-8　入力ポートのキューイングおよびスケジューリングのフローチャート



（注）　SRR は、他のキューを処理する前に、その設定済みの共有に従いプライオリティ キューを処理します。

スイッチは 2 つの設定可能な入力キューをサポートしています。これらのキューは、共有モードの SRR だけで処理されます。表 39-1 でキューについて説明します。

表 39-1　入力キューのタイプ

キューのタイプ[1]	機能
標準	標準のプライオリティと見なされるユーザ トラフィック。フローを区別するために 3 つの異なるスレッシュホールドを設定できます。**mls qos srr-queue input threshold**、**mls qos srr-queue input dscp-map**、および **mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用できます。
緊急	Differentiated Service（DF; ディファレンシエーテッド サービス）緊急転送または音声トラフィックなどのプライオリティの高いユーザ トラフィック。このトラフィックに必要な帯域幅を、**mls qos srr-queue input priority-queue** グローバル コンフィギュレーション コマンドを使用して、総トラフィックのパーセンテージとして設定できます。緊急キューには保証された帯域幅があります。

1. スイッチは、適切なネットワーク動作に不可欠なトラフィック用に、設定変更ができない 2 つのキューを使用します。

スイッチを通過する各パケットを、キューとスレッシュホールドに割り当てます。具体的には、DSCP または CoS 値を入力キューに割り当て、DSCP または CoS 値をスレッシュホールド ID に割り当てます。**mls qos srr-queue input dscp-map** queue *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*} または **mls qos srr-queue input cos-map queue** *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*} グローバル コンフィギュレーション コマンドを使用します。DSCP 入力キュー スレッシュホールド マップおよび CoS 入力キュー スレッシュホールド マップは、**show mls qos maps** 特権 EXEC コマンドを使用して表示できます。

WTD スレッシュホールド

キューは WTD を使用して、トラフィック クラスごとに異なる廃棄パーセンテージをサポートします。各キューには 3 つの廃棄スレッシュホールドがあります。そのうちの 2 つは設定可能な（*明示的な*）WTD スレッシュホールドで、1 つは、キューが満杯の状態に事前設定されていて設定変更ができない（*暗黙の*）スレッシュホールドです。スレッシュホールド ID 1 および ID 2 用に、2 つの明示的な WTD スレッシュホールド パーセンテージを入力キューに割り当てるには、**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2* グローバル コンフィギュレーション コマンドを使用します。各スレッシュホールドは、キューに割り当てられたバッファの総数に対する割合です。スレッシュホールド ID 3 の廃棄スレッシュホールドは、キューが満杯の状態に事前設定されており、修正はできません。WTD の動作の詳細については、「WTD」（P.39-14）を参照してください。

バッファと帯域幅の割り当て

2 つのキューの間で入力バッファを分割する（領域の大きさを割り当てる）比率を定義するには、**mls qos srr-queue input buffers** *percentage1 percentage2* グローバル コンフィギュレーション コマンドを使用します。バッファ割り当てと帯域幅割り当てを組み合わせることにより、パケットの廃棄前にバッファリングし、送信できるデータの大きさを制御します。帯域幅をパーセンテージとして割り当てるには、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドを使用します。重みの比率は、SRR スケジューラがパケットを各キューから送信する頻度の比率です。

プライオリティ キューイング

mls qos srr-queue input priority-queue *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドを使用して、1 つの入力キューをプライオリティ キューとして設定できます。プライオリティ キューは、内部リングの負荷にかかわらず帯域幅が保証されたキューの一部であるため、確実な配信を必要とするトラフィック（音声など）に使用します。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に SRR は、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定された重みに従い、両方の入力キューで残りの帯域幅を共有し、キューを処理します。

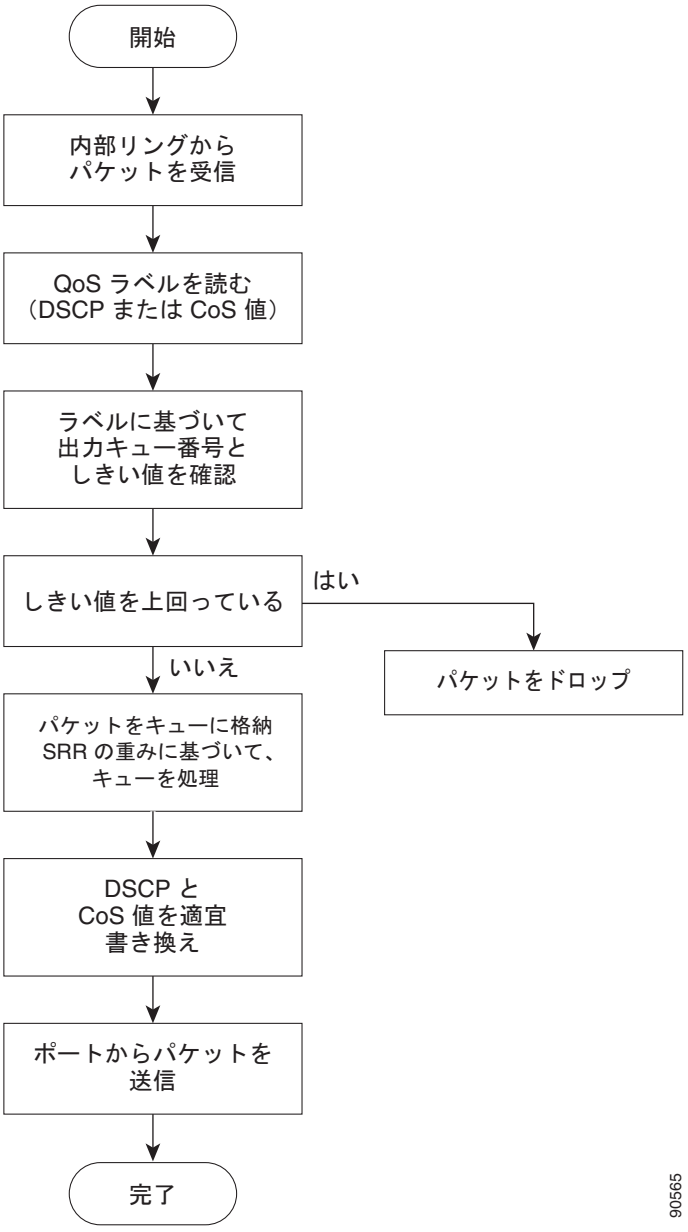
この項で説明するコマンドを組み合わせて、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティの低いパケットが廃棄されるようにキューのスレッシュホールドを調整したりして、トラフィックのプライオリティを設定できます。設定の詳細については、「入力キューの特性の設定」（P.39-70）を参照してください。

出力キューでのキューイングおよびスケジューリング

図 39-9 に、出力ポートのキューイングとスケジューリングのフローチャートを示します。

（注）　緊急キューがイネーブルになっている場合、SRR は、他の 3 つのキューを処理する前に、そのキューが空になるまで処理します。

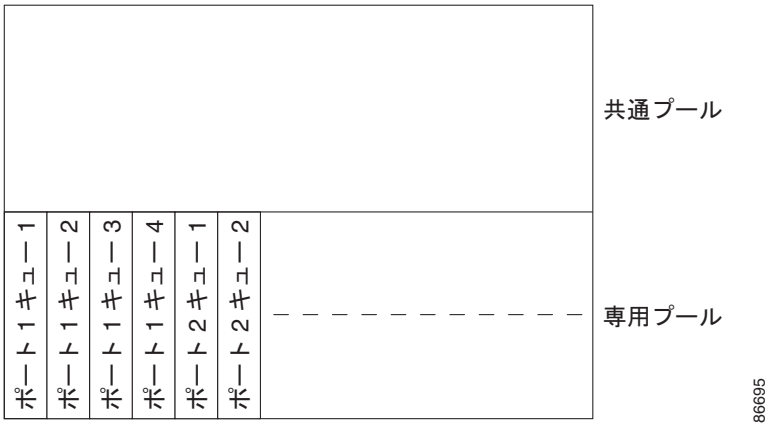
図 39-9　出力ポートのキューイングおよびスケジューリングのフローチャート



各ポートは 4 つの出力キューをサポートしており、そのうちの 1 つ（キュー 1）を出力緊急キューにできます。これらのキューはキューセットにより設定されます。出力ポートからのすべてのトラフィックは、これらの 4 つのキューの 1 つを通過し、パケットに割り当てられた QoS ラベルに基づいてスレッショルドが適用されます。

図 39-10 に出力キュー バッファを示します。バッファ領域は、共通のプールと予約済みプールとにわかれます。スイッチは、バッファ割り当て方式を使用して、出力キューごとに最小バッファ量を予約し、いずれかのキューまたはポートがすべてのバッファを消費してその他のキューがバッファを使用できなくなるのを防ぎ、バッファ スペースを要求元のキューに許可するかどうかを制御します。スイッチは、ターゲット キューが予約量を超えるバッファを消費していないかどうか（アンダーリミット）、その最大バッファをすべて消費したかどうか（オーバーリミット）、共通のプールが空（空きバッファがない）か、または空でない（空きバッファ）かを検出します。キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファ スペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームを廃棄します。

図 39-10　出力キュー バッファの割り当て



バッファおよびメモリの割り当て

mls qos queue-set output *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンドを使用して、バッファのアベイラビリティを保証し、廃棄スレッショルドを設定し、キューセットの最大メモリ割り当てを設定します。各スレッショルド値は、キューに割り当てられたメモリのパーセンテージであり、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* グローバル コンフィギュレーション コマンドを使用して指定します。割り当てられたすべてのバッファの合計が予約済みプールになり、残りのバッファは共通のプールの一部になります。

バッファ割り当てによって、ハイ プライオリティ トラフィックを確実にバッファリングできます。たとえば、バッファ領域が 400 の場合は、その 70% をキュー 1 に割り当て、10% をキュー 2 ～ 4 に割り当てることができます。この結果、キュー 1 には 280 のバッファが割り当てられ、キュー 2 ～ 4 には、それぞれ 40 のバッファが割り当てられます。

割り当てられたバッファがキューセットの特定のキュー用に予約されていることを保証できます。たとえば、キューに 100 のバッファがある場合は、50%（50 のバッファ）を予約できます。スイッチは、残りの 50 のバッファを共通のプールに返します。また、最大スレッショルドを設定することにより、フル状態のキューが予約済みのバッファを超える大きさのバッファを取得できるようにすることもできます。スイッチは、共通のプールが空でない場合に、必要なバッファを共通のプールから割り当てることができます。

WTD スレッシュホールド

スイッチを通過する各パケットを、キューとスレッシュホールドに割り当てできます。具体的には、DSCP または CoS 値を出力キューに割り当て、DSCP または CoS 値をスレッシュホールド ID に割り当てます。**mls qos srr-queue output dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*} または **mls qos srr-queue output cos-map queue** *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*} グローバル コンフィギュレーション コマンドを使用します。DSCP 出力キュー スレッシュホールド マップおよび CoS 出力キュー スレッシュホールド マップは、**show mls qos maps** 特権 EXEC コマンドを使用して表示できます。

キューは WTD を使用して、トラフィック クラスごとに異なる廃棄パーセンテージをサポートします。各キューには 3 つの廃棄スレッシュホールドがあります。そのうちの 2 つは設定可能な（*明示的な*）WTD スレッシュホールドで、1 つは、キューが満杯の状態に事前設定されていて設定変更ができない（*暗黙の*）スレッシュホールドです。スレッシュホールド ID 1 および ID 2 用の 2 つの WTD スレッシュホールド パーセンテージを割り当てます。スレッシュホールド ID 3 の廃棄スレッシュホールドは、キューが満杯の状態に事前設定されており、修正はできません。**queue-set qset-id** インターフェイス コンフィギュレーション コマンドを使用して、ポートをキューセットにマッピングします。WTD スレッシュホールドのパーセンテージを変更するには、キューセットの設定を修正します。WTD の動作の詳細については、「WTD」（P.39-14）を参照してください。

シェーピング モードまたは共有モード

SRR は、共有モードまたはシェーピング モードでキューセットを処理します。**srr-queue bandwidth share** *weight1 weight2 weight3 weight4* または **srr-queue bandwidth shape** *weight1 weight2 weight3 weight4* インターフェイス コンフィギュレーション コマンドを使用して、共有重みまたはシェーピングされた重みをポートに割り当てます。シェーピングと共有の違いについては、「SRR のシェーピングおよび共有」（P.39-15）を参照してください。

バッファ割り当てと SRR の重み比率を組み合わせることにより、パケットの廃棄前にバッファリングし、送信できるデータの大きさを制御します。重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。

緊急キューがイネーブルでない限り、4 つのキューすべてが SRR に関与します。この場合、1 番めの帯域幅の重みは無視されて、比率の計算には使用されません。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。緊急キューは、**priority-queue out** インターフェイス コンフィギュレーション コマンドを使用してイネーブルにします。

この項で説明するコマンドを組み合わせて、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティの低いパケットが廃棄されるようにキューのスレッシュホールドを調整したりして、トラフィックのプライオリティを設定できます。設定の詳細については、「出力キューの特性の設定」（P.39-75）を参照してください。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合だけ、設定を変更してください。

パケットの変更

QoS を提供するために、パケットは、分類され、ポリシングされ、キューイングされます。このプロセス中に、次のようにパケットが変更されることがあります。

- IP および非 IP パケットの分類では、受信したパケットの DSCP または CoS に基づいて、QoS ラベルがパケットに割り当てられます。ただし、パケットはこの段階では変更されず、割り当てられた DSCP または CoS 値の指定だけが伝送されます。これは、QoS の分類と転送の検索が並行して行われるためです。パケットを元の DSCP のまま CPU に転送し、そこでソフトウェアによって再度処理することもできます。
- ポリシングの実行中に、IP および非 IP パケットに別の DSCP を割り当てることができます（パケットがプロファイル外で、ポリサーがマークダウン DSCP を指定している場合）。この場合もパケットの DSCP は変更されず、マークダウンされた値の指定が伝送されます。IP パケットでは、パケットの変更は後の段階で行われます。非 IP パケットでは、DSCP が CoS に変換され、キューイングやスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベルと選択した変換に応じて、フレームの DSCP 値と CoS 値が書き換えられます。変換マップを設定していないときに、着信フレームの DSCP を信頼するようにポートを設定すると、フレームの DSCP 値は変更されませんが、CoS は DSCP/CoS マップに従って書き換えられます。着信フレームの CoS を信頼するようにポートを設定し、これが IP パケットの場合は、フレームの CoS 値は変更されませんが、DSCP は CoS/DSCP マップに従って変更されることがあります。

  入力変換により、DSCP は、選択した DSCP の新しい値に応じて書き換えられます。ポリシーマップの設定されたアクションによっても、DSCP の書き換えが発生します。

auto-QoS の設定

auto-QoS 機能を使用して、QoS 機能の導入を簡易化できます。auto-QoS はネットワーク設計を判断し、スイッチで異なるトラフィック フローの優先順位付けができるように、QoS 設定をイネーブルにします。デフォルトの（ディセーブルにされた）QoS 動作を使用する代わりに、入力キューと出力キューを使用します。スイッチは、パケットの内容やサイズにかかわらずベストエフォート サービスを各パケットに提供し、単一のキューからパケットを送信します。

auto-QoS をイネーブルにすると、トラフィックのタイプと入力パケットのラベルに従ってトラフィックが自動的に分類されます。スイッチは分類結果を使用して、適切な出力キューを選択します。

auto-QoS コマンドを使用して、次のシスコ デバイスに接続されているポートを識別します。

- Cisco IP Phones
- Cisco SoftPhone アプリケーションが動作しているデバイス

また、アップリンクを介して信頼されたトラフィックを受信するポートを識別するためにも、これらのコマンドを使用します。auto-QoS は次の機能を実行します。

- 条件付きの信頼できるインターフェイスによる auto-QoS 装置の有無の検出
- QoS の分類の設定
- 出力キューの設定

ここでは、次の設定情報について説明します。

- 「生成される auto-QoS の設定」（P.39-22）
- 「設定に与える auto-QoS の影響」（P.39-29）
- 「auto-QoS 設定時の注意事項」（P.39-30）
- 「Auto-QoS のイネーブル化」（P.39-30）

生成される auto-QoS の設定

デフォルトでは、auto-QoS はすべてのポートでディセーブルになっています。パケットは変更されません。つまり、パケットの CoS、DSCP、および IP precedence の値は変更されません。

インターフェイスの最初のポートで auto-QoS 機能をイネーブルにすると、次のようになります。

- 入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力キューと出力キューの設定が行われます。
- QoS はグローバルにイネーブル化され（**mls qos** グローバル コンフィギュレーション コマンド）、その他のグローバル コンフィギュレーション コマンドが自動的に生成されます（表 39-6 を参照）。
- スイッチが信頼境界機能をイネーブルにし、サポート対象の装置があるかどうかを Cisco Discovery Protocol（CDP; シスコ検出プロトコル）を使用して検出します。
- ポリシングを使用してパケットがプロファイル内にあるのかプロファイル外にあるのかを確認し、そのパケットに対するアクションを指定します。

VOIP 装置固有

- Cisco IP Phone に接続されたネットワーク エッジにあるポートで **auto qos voip cisco-phone** コマンドを入力すると、スイッチは信頼境界機能をイネーブルにします。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。Cisco IP Phone がない場合、入力ポートでの分類は、パケットの QoS ラベルを信頼しないように設定されます。ポリシングは、スイッチが信頼境界機能をイネーブルにする前に、ポリシーマップの分類に一致するトラフィックに適用されます。
- Cisco SoftPhone が動作する装置に接続されたネットワーク エッジにあるポートで **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチはポリシングを使用してパケットがプロファイル内にあるのかプロファイル外にあるのかを確認し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。
- ネットワーク内部に接続されたポートで **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは、入力パケット内の非ルーテッド ポートの CoS 値、またはルーテッド ポートの DSCP 値を信頼します（トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります）。

スイッチは、ポートの入力キューと出力キューを、表 39-2 および表 39-3 の設定値に従って設定します。

表 39-2　トラフィック タイプ、パケット ラベル、およびキュー

	VoIP[1] データ トラフィック	VoIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP BPDU トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP	46	24、26	48	56	34	–	
CoS	5	3	6	7	3	–	
CoS から入力キューへのマッピング	4、5（キュー 2）					0、1、2、3、6、7（キュー 1）	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

1. VoIP = Voice over IP

表 39-3　入力キューに対する auto-QoS の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	キュー（バッファ）サイズ
SRR 共有	1	0、1、2、3、6、7	70%	90%
プライオリティ	2	4、5	30%	10%

表 39-4　出力キューに対する auto-QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

信頼境界機能の詳細については、「ポート セキュリティを保証するための信頼境界の設定」（P.39-41）を参照してください。

auto qos voip cisco-phone、**auto qos voip cisco-softphone** 、または **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを使用して auto-QoS をイネーブルにする場合、スイッチは、トラフィックのタイプと入力パケットのラベルに基づいて QoS の設定を自動的に生成し、表 39-6 に示すコマンドをポートに適用します。

グローバル auto-QoS の設定

表 39-5　生成される auto-QoS の設定

説明	自動生成されるコマンド {voip}	自動生成される拡張コマンド {Video|Trust|Classify}
スイッチは、標準の QoS を自動的にイネーブルにし、CoS/DSCP マップを設定します（着信パケットの CoS 値を DSCP 値にマッピングする）。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 24 32 46 48 56**
スイッチは、入力キューとスレッシュホールド ID に CoS 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 1** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 0** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 3 3 5**	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 3** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 4**

表 39-5　生成される auto-QoS の設定 （続き）

説明	自動生成されるコマンド {voip}	自動生成される拡張コマンド {Video|Trust|Classify}
スイッチは、出力キューとスレッシュホールド ID に CoS 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 4 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 2 3** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 0** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 1**
スイッチは、入力キューとスレッシュホールド ID に DSCP 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 32** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47**	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 24** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41 42 43 44 45** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 46 47**

表 39-5　生成される auto-QoS の設定 （続き）

説明	自動生成されるコマンド {voip}	自動生成される拡張コマンド {Video|Trust|Classify}
スイッチは、出力キューとスレッシュホールド ID に DSCP 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 2 24** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14**

表 39-5　生成される auto-QoS の設定 （続き）

説明	自動生成されるコマンド {voip}	自動生成される拡張コマンド {Video|Trust|Classify}
スイッチは入力キューを自動的に設定します。キュー 2 がプライオリティ キューで、キュー 1 が共有モードです。スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 90 10** Switch(config)# **mls qos srr-queue input threshold 1 8 16** Switch(config)# **mls qos srr-queue input threshold 2 34 66** Switch(config)# **mls qos srr-queue input buffers 67 33**	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 70 30** Switch(config)# **mls qos srr-queue input threshold 1 80 90** Switch(config)# **mls qos srr-queue input priority-queue 2 bandwidth 30**
スイッチは、出力キューのバッファ サイズを自動的に設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード（シェーピングまたは共有）を設定します。	Switch(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Switch(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Switch(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Switch(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Switch(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Switch(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Switch(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Switch(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Switch(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Switch(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Switch(config-if)# **priority-queue out** Switch(config-if)# **srr-queue bandwidth share 10 10 60 20**	Switch(config)# **mls qos queue-set output 1 threshold 2 100 100 50 200** Switch(config)# **mls qos queue-set output 1 threshold 2 125 125 100 400** Switch(config)# **mls qos queue-set output 1 threshold 3 100 100 100 400** Switch(config)# **mls qos queue-set output 1 threshold 4 60 150 50 200** Switch(config)# **mls qos queue-set output 1 buffers 15 25 40 20**

VoIP 装置に対して生成される auto-QoS の設定

表 39-6　生成される auto-QoS の設定

説明	自動生成されるコマンド {voip}
スイッチは、標準の QoS を自動的にイネーブルにし、CoS/DSCP マップを設定します（着信パケットの CoS 値を DSCP 値にマッピングする）。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**
スイッチは入力キューを自動的に設定します。キュー 2 がプライオリティ キューで、キュー 1 が共有モードです。スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 1** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 0** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 3 3 5**
スイッチは、出力キューとスレッショルド ID に CoS 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**
スイッチは、入力キューとスレッショルド ID に DSCP 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 32** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47**

表 39-6　生成される auto-QoS の設定 （続き）

説明	自動生成されるコマンド {voip}
スイッチは、出力キューとスレッシュホールド ID に DSCP 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**
スイッチは入力キューを自動的に設定します。キュー 2 がプライオリティ キューで、キュー 1 が共有モードです。スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 90 10** Switch(config)# **mls qos srr-queue input threshold 1 8 16** Switch(config)# **mls qos srr-queue input threshold 2 34 66** Switch(config)# **mls qos srr-queue input buffers 67 33**
スイッチは、出力キューのバッファ サイズを自動的に設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード（シェーピングまたは共有）を設定します。	Switch(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Switch(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Switch(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Switch(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Switch(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Switch(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Switch(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Switch(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Switch(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Switch(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Switch(config-if)# **priority-que out** Switch(config-if)# **srr-queue bandwidth share 10 10 60 20**

auto qos voip cisco-phone コマンドを入力すると、スイッチは、CDP を使用して Cisco IP Phone の存在を検出する信頼境界機能を自動的にイネーブルにします。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチはクラス マップとポリシー マップを自動的に作成します。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-SoftPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成した後、スイッチは、*AutoQoS-Police-SoftPhone* と呼ばれるポリシー マップを、Cisco SoftPhone 機能を持つ auto-QoS がイネーブルにされている入力インターフェイスに自動的に適用します。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

auto qos voip cisco-phone コマンドを入力すると、スイッチはクラス マップとポリシー マップを自動的に作成します。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチはクラス マップとポリシー マップを自動的に作成します。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-CiscoPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成した後、スイッチは、*AutoQoS-Police-SoftPhone* と呼ばれるポリシー マップを、Cisco SoftPhone 機能を持つ auto-QoS がイネーブルにされている入力インターフェイスに自動的に適用します。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

設定に与える auto-QoS の影響

auto-QoS がイネーブルになっていると、**auto qos** インターフェイス コンフィギュレーション コマンドと生成されたグローバル設定が、実行コンフィギュレーションに追加されます。

スイッチは、CLI からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドが適用されない場合は、以前の実行コンフィギュレーションが復元されます。

auto-QoS 設定時の注意事項

auto-QoS を設定する前に、次の点に注意してください。

- auto-QoS では、非ルーテッド ポートとルーテッドポート上に Cisco IP Phone がある VoIP 用にスイッチが設定されます。auto-QoS はまた、Cisco SoftPhone アプリケーションを実行している装置を使用する VoIP 用にスイッチを設定します。
- Cisco SoftPhone が動作する装置が、非ルーテッド ポートまたはルーテッド ポートに接続されている場合、スイッチはポートごとに 1 つの Cisco SoftPhone アプリケーションだけをサポートします。
- auto-Qos VoIP では、**priority-queue** インターフェイス コンフィギュレーション コマンドを出力インターフェイスに使用します。Cisco IP phone の同一インターフェイス上でポリシーマップと信頼する装置を設定することもできます。
- auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。必要に応じて QoS 設定を微調整できますが、これは、auto-QoS の設定が完了した後に限り実行することを推奨します。詳細については、「設定に与える auto-QoS の影響」（P.39-29）を参照してください。
- auto-QoS をイネーブルにしたあと、名前に *AutoQoS* を含むポリシー マップや aggregate ポリサーを変更しないでください。ポリシー マップや aggregate ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成したポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップをインターフェイスに適用します。
- スタティック ポート、ダイナミック アクセス ポート、音声 VLAN アクセス ポート、およびトランク ポートで auto-QoS をイネーブルにできます。
- デフォルトでは、auto-CDP はすべてのポートでイネーブルになっています。auto-QoS が正しく動作するように、CDP はディセーブルにしないでください。
- ルーテッド ポートにある Cisco IP Phone で auto-QoS をイネーブルにする場合は、スタティック IP アドレスを IP Phone に割り当てる必要があります。
- このリリースでは、Cisco IP SoftPhone バージョン 1.3(3) 以降だけがサポートされます。
- 接続される装置は Cisco CallManager バージョン 4 以降を使用する必要があります。

Auto-QoS のイネーブル化

QoS パフォーマンスを最適にするには、ネットワーク内部のすべての装置で自動 QoS をイネーブルにします。

特権 EXEC モードで開始し、次の手順に従って、QoS ドメイン内部で auto-QoS 装置をイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	ビデオ装置に接続されているポート、またはネットワーク内部の別の信頼できるスイッチまたはルータに接続されているアップリンク ポートを指定し、インターフェイス コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 3	**auto qos voip** {**cisco-phone** | **cisco-softphone** | **trust**} または	auto-QoS をイネーブルにします。 キーワードの意味は次のとおりです。 • **cisco-phone**：ポートが Cisco IP Phone に接続されている場合は、電話が検出されたときに限り、着信パケットの QoS ラベルが信頼されます。 • **cisco-softphone**：ポートは、Cisco SoftPhone 機能を実行している装置に接続されています。 • **trust**：アップリンク ポートは信頼できるスイッチまたはルータに接続されており、VoIP トラフィックの分類が
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	信頼できるスイッチまたはルータに接続されていると識別されるスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 6	**auto qos trust**	ポートで auto-QoS をイネーブルにし、そのポートを信頼できるルータまたはスイッチに接続することを指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show auto qos interface** *interface-id*	設定を確認します。 このコマンドは、auto-QoS がイネーブルにされていたインターフェイスの auto-QoS コマンドを表示します。auto-QoS 設定とユーザによる変更を表示するには、**show running-config** 特権 EXEC コマンドを使用できます。

auto-QoS コマンドのトラブルシューティング

auto-QoS をイネーブルまたはディセーブルにしたときに自動的に生成される QoS コマンドを表示するには、auto-QoS をイネーブルにする*前に* **debug auto qos** 特権 EXEC コマンドを入力します。詳細については、このリリースのコマンド リファレンスの **debug autoqos** コマンドを参照してください。

ポート上で auto-QoS をディセーブルにするには、auto qos コマンド インターフェイス コンフィギュレーション コマンドの **no** 形式（**no auto qos voip** など）を使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

no mls qos グローバル コンフィギュレーション コマンドを使用して、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合、パケットが修正されなくなるため（パケットの CoS、DSCP、IP precedence の値は変更されない）、ポートの信頼性に関する概念はなくなります。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

auto-QoS 情報の表示

auto-QoS の初期設定を表示するには、**show auto qos** [**interface** [*interface-id*]] 特権 EXEC コマンドを使用します。その設定に対するユーザの変更を表示するには、**show running-config** 特権 EXEC コマンドを使用します。**show auto qos** コマンドと **show running-config** コマンドの出力を比較して、ユーザ定義の QoS 設定を識別できます。

auto-QoS の影響を受ける可能性のある現在の QoS の設定情報を表示するには、次のいずれかのコマンドを使用します。

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface** [*interface-id*] [**buffers** | **queueing**]
- **show mls qos maps** [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-output-q**]
- **show mls qos input-queue**
- **show running-config**

標準の QoS の設定

次の項目について十分に理解したうえで、標準の QoS を設定してください。

- 使用するアプリケーションのタイプと、ネットワーク上のトラフィック パターン。
- トラフィックの特性と、ネットワークのニーズ。トラフィックのバースト性が高いかどうか。音声およびビデオ ストリーム用に帯域幅を予約する必要があるかどうか。
- ネットワークの帯域幅要件と速度。
- ネットワーク内の輻輳ポイントの位置。

ここでは、次の設定情報について説明します。

- 「標準の QoS のデフォルト設定」（P.39-33）
- 「標準の QoS 設定の注意事項」（P.39-35）
- 「QoS をグローバルにイネーブルにする方法」（P.39-37）（必須）
- 「物理ポートでの VLAN ベースの QoS のイネーブル化」（P.39-38）（任意）
- 「ポートの信頼状態を使用した分類の設定」（P.39-38）（必須）
- 「QoS ポリシーの設定」（P.39-44）（必須）
- 「DSCP マップの設定」（P.39-65）（任意、DSCP/DSCP 変換マップまたはポリシングされた DSCP マップを使用する必要がある場合を除く）
- 「入力キューの特性の設定」（P.39-70）（任意）
- 「出力キューの特性の設定」（P.39-75）（任意）

標準の QoS のデフォルト設定

QoS はディセーブルです。パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念は存在しません。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

mls qos グローバル コンフィギュレーション コマンドによって QoS がイネーブルにされ、その他のすべての QoS 設定値がデフォルト値に設定されている場合、トラフィックはポリシングされず、ベスト エフォート（DSCP 値と CoS 値は 0 に設定される）として分類されます。ポリシー マップは設定されません。すべてのポート上のデフォルト ポートの信頼性は、信頼性なし（untrusted）の状態です。入力および出力キューのデフォルト設定については、「入力キューのデフォルト設定」（P.39-33）および「出力キューのデフォルト設定」（P.39-34）で説明します。

入力キューのデフォルト設定

表 39-7 に、QoS がイネーブルになっているときの入力キューのデフォルト設定を示します。

表 39-7　入力キューのデフォルト設定

機能	キュー 1	キュー 2
バッファ割り当て	90%	10%
帯域幅割り当て [1]	4	4
プライオリティ キューの帯域幅 [2]	0	10
WTD 廃棄スレッシュホールド 1	100%	100%
WTD 廃棄スレッシュホールド 2	100%	100%

1. 帯域幅はキューの間で均等に分配されます。SRR は、共有モードだけでパケットを送信します。
2. キュー 2 はプライオリティ キューです。SRR は、他のキューを処理する前に、その設定済みの共有に従いプライオリティ キューを処理します。

表 39-8 に、QoS をイネーブルにしたときのデフォルトの CoS 入力キュー スレッシュホールド マップを示します。

表 39-8　デフォルトの CoS 入力キュー スレッシュホールド マップ

CoS 値	キュー ID - スレッシュホールド ID
0 ～ 4	1–1
5	2–1
6、7	1–1

表 39-9 に、QoS をイネーブルにしたときのデフォルトの DSCP 入力キュー スレッシュホールド マップを示します。

表 39-9　デフォルトの DSCP 入力キュー スレッシュホールド マップ

DSCP 値	キュー ID - スレッシュホールド ID
0 ～ 39	1–1

表 39-9　デフォルトの DSCP 入力キュー スレッシュホールド マップ （続き）

DSCP 値	キュー ID - スレッシュホールド ID
40 ～ 47	2–1
48 ～ 63	1–1

出力キューのデフォルト設定

表 39-10 に、QoS をイネーブルにしたときの各キュー セットの出力キューのデフォルト設定を示します。すべてのポートがキューセット 1 にマッピングされます。ポートの帯域幅限度は 100% に、レートは無制限に設定されます。

表 39-10　出力キューのデフォルト設定

機能	キュー 1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD 廃棄スレッシュホールド 1	100%	200%	100%	100%
WTD 廃棄スレッシュホールド 2	100%	200%	100%	100%
予約済みスレッシュホールド	50%	50%	50%	50%
最大スレッシュホールド	400%	400%	400%	400%
SRR のシェーピングされた重み（絶対値）[1]	25	0	0	0
SRR の共有された重み [2]	25	25	25	25

1. シェーピングされた重み 0 は、このキューが共有モードで動作していることを示します。
2. 帯域幅の 4 分の 1 が各キューに割り当てられます。

表 39-11 に、QoS をイネーブルにしたときのデフォルトの CoS 出力キュー スレッシュホールド マップを示します。

表 39-11　デフォルトの CoS 出力キュー スレッシュホールド マップ

CoS 値	キュー ID - スレッシュホールド ID
0、1	2–1
2、3	3–1
4	4–1
5	1–1
6、7	4–1

表 39-12 に、QoS をイネーブルにしたときのデフォルトの DSCP 出力キュー スレッシュホールド マップを示します。

表 39-12　デフォルトの DSCP 出力キュー スレッシュホールド マップ

DSCP 値	キュー ID - スレッシュホールド ID
0 ～ 15	2–1
16 ～ 31	3–1

表 39-12　デフォルトの DSCP 出力キュー スレッシュホールド マップ （続き）

DSCP 値	キュー ID - スレッシュホールド ID
32 ～ 39	4–1
40 ～ 47	1–1
48 ～ 63	4–1

デフォルトのマッピング テーブルの設定

デフォルトの CoS/DSCP マップを表 39-13（P.39-65）に示します。

デフォルトの IP precedence/DSCP マップを表 39-14（P.39-66）に示します。

デフォルトの DSCP/CoS マップを表 39-15（P.39-68）に示します。

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです（マークダウンなし）。

標準の QoS 設定の注意事項

QoS 設定を開始する前に、次の項の情報に注意してください。

- 「QoS ACL の注意事項」（P.39-35）
- 「インターフェイスへの QoS の適用」（P.39-35）
- 「ポリシングの注意事項」（P.39-36）
- 「QoS の一般的な注意事項」（P.39-37）

QoS ACL の注意事項

- IP フラグメントと設定済みの IP 拡張 ACL を照合することによって、QoS は適用できません。IP フラグメントはベストエフォートとして送信されます。IP フラグメントは、IP ヘッダーのフィールドで表されます。
- クラス マップごとに 1 つの ACL と、1 つの **match** クラスマップ コンフィギュレーション コマンドだけがサポートされます。ACL は、フィールドをパケットの内容と照合する ACE を複数持つことができます。
- ポリシー マップの信頼文には、ACL 行ごとに複数の TCAM エントリが必要です。入力サービス ポリシー マップで ACL に信頼文が含まれる場合は、アクセスリストが大きすぎるために使用可能な QoS TCAM に収まらず、ポリシー マップをポートに適用したときにエラーが発生することがあります。可能な限り、QoS ACL の行数を最小限に抑えてください。

インターフェイスへの QoS の適用

次のガイドラインが、物理ポートおよび SVI（レイヤ 3 インターフェイス）での QoS の設定に適用されます。

- QoS は、物理ポートと SVI に設定できます。QoS を物理ポートで設定する場合は、非階層ポリシー マップを作成し、適用します。QoS を SVI に設定する場合は、非階層ポリシー マップおよび階層ポリシー マップを適用できます。
- 着信トラフィックは、トラフィックがブリッジングされるか、ルーティングされるか、CPU に送信されるかにかかわらず、分類され、ポリシングされ、マークダウンされます（設定されている場合）。ブリジッド フレームが廃棄されたり、その DSCP および CoS 値が修正されたりすることもあります。
- 物理ポートまたは SVI にポリシー マップを設定する場合は、次の注意事項に従ってください。
  - 物理ポートと SVI に同じポリシー マップを適用できません。
  - VLAN ベースの QoS を物理ポートで設定すると、スイッチは、そのポート上のポートベースのポリシー マップをすべて削除します。それによって、この物理ポート上のトラフィックは、物理ポートが属する SVI に付加されたポリシー マップの適用を受けるようになります。
  - SVI に付加された階層ポリシー マップでは、ポート上のトラフィックの帯域幅限度を指定するために、物理ポート上のインターフェイス レベルで individual ポリサーを設定することだけができます。入力ポートは、トランクとして、またはスタティック アクセス ポートとして設定する必要があります。階層ポリシー マップの VLAN レベルではポリサーを設定できません。
  - スイッチは、仮想ポリシー マップで aggregate ポリサーをサポートしません。
  - 階層ポリシー マップを SVI に適用した後は、インターフェイス レベルのポリシー マップを変更したり、階層ポリシー マップから削除したりできません。階層ポリシー マップに、新しいインターフェイス レベル ポリシー マップを追加することもできません。このような変更を行いたい場合は、まず階層ポリシー マップを SVI から削除する必要があります。また、階層ポリシー マップで指定されたクラス マップは、追加することも削除することもできません。

ポリシングの注意事項

- 2 つ以上の物理ポートを制御するポート ASIC 装置は、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個のシステム内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。たとえば、32 個のポリサーをギガビット イーサネット ポート上で、8 個のポリサーをファスト イーサネット ポート上で設定できます。または、64 個のポリサーをギガビット イーサネット ポート上で、5 個のポリサーをファスト イーサネット ポート上で設定できます。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとのポリサーの予約はできません（特定のポートがいずれかのポリサーに割り当てられるという保証はありません）。
- 入力ポートでは、1 つのパケットに 1 つのポリサーだけが適用されます。設定できるパラメータは、平均レートと認定バーストだけです。
- 同じ非階層ポリシー マップ内部の複数のトラフィック クラスによって共有される aggregate ポリサーを作成できます。ただし、aggregate ポリサーを異なるポリシー マップにわたって使用することはできません。
- QoS 用に設定されたポートでは、そのポートを通じて受信されるすべてのトラフィックが、ポートに付加されたポリシー マップに従って分類され、ポリシングされ、マーキングされます。QoS 用に設定されたトランク ポートでは、そのポートを通じて受信されるすべての VLAN のトラフィックが、ポートに付加されたポリシー マップに従って分類され、ポリシングされ、マーキングされます。
- スイッチで EtherChannel ポートを設定している場合は、QoS の分類、ポリシング、マッピング、およびキューイングを、EtherChannel を構成している個々の物理ポートで設定する必要があります。EtherChannel のすべてのポートで QoS 設定が一致していなければならないかどうかを決定する必要があります。

- 既存の QoS ポリシーのポリシー マップを変更する必要がある場合は、まずポリシー マップをすべてのインターフェイスから削除し、それからポリシー マップを変更またはコピーします。変更が終了したら、変更したポリシー マップをインターフェイスに適用します。最初にポリシー マップをすべてのインターフェイスから削除しなかった場合、CPU 使用率が高くなり、その結果、コンソールが長時間停止することがあります。

QoS の一般的な注意事項

QoS の一般的な注意事項を次に示します。

- スイッチによって受信される制御トラフィック（スパニング ツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）やルーティング アップデート パケットなど）は、すべて入力 QoS 処理の対象となります。
- キューの設定を変更するとデータが失われることがあるため、トラフィックが最小のときに変更を行うようにしてください。

IP サービス イメージを実行しているスイッチは、Policy-Based Routing（PBR; ポリシーベース ルーティング）ルート マップでの QoS DSCP および IP precedence の照合をサポートしていて、次の制限があります。

- QoS DSCP 変換マップと PBR ルート マップを同じインターフェイスに適用することはできません。
- DSCP の透過性と PBR DSCP ルート マップを同じスイッチに設定することはできません。

QoS をグローバルにイネーブルにする方法

デフォルトでは、QoS はスイッチ上でディセーブルになっています。

特権 EXEC モードで開始し、次の手順に従って QoS をイネーブルにします。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	QoS をグローバルにイネーブルにします。 QoS は、「標準の QoS のデフォルト設定」（P.39-33）、「入力キューでのキューイングおよびスケジューリング」（P.39-16）、および「出力キューでのキューイングおよびスケジューリング」（P.39-18）で説明したデフォルトの設定で実行されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

QoS をディセーブルにするには、**no mls qos** グローバル コンフィギュレーション コマンドを使用します。

物理ポートでの VLAN ベースの QoS のイネーブル化

デフォルトでは、VLAN ベースの QoS はすべての物理スイッチ ポートでディセーブルになっています。スイッチは、クラス マップとポリシー マップを含む QoS を、物理ポート ベースだけに適用できます。VLAN ベースの QoS は、スイッチ ポートでイネーブルにできます。

特権 EXEC モードで開始し、次の手順に従って VLAN ベースの QoS をイネーブルにします。この手順は、SVI 上の階層ポリシー マップのインターフェイス レベルで指定された物理ポートで必要となります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 3	**mls qos vlan-based**	ポートで VLAN ベースの QoS をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id*	物理ポートで VLAN ベースの QoS がイネーブルになっているかどうかを確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

物理ポートで VLAN ベースの QoS をディセーブルにするには、**no mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用します。

ポートの信頼状態を使用した分類の設定

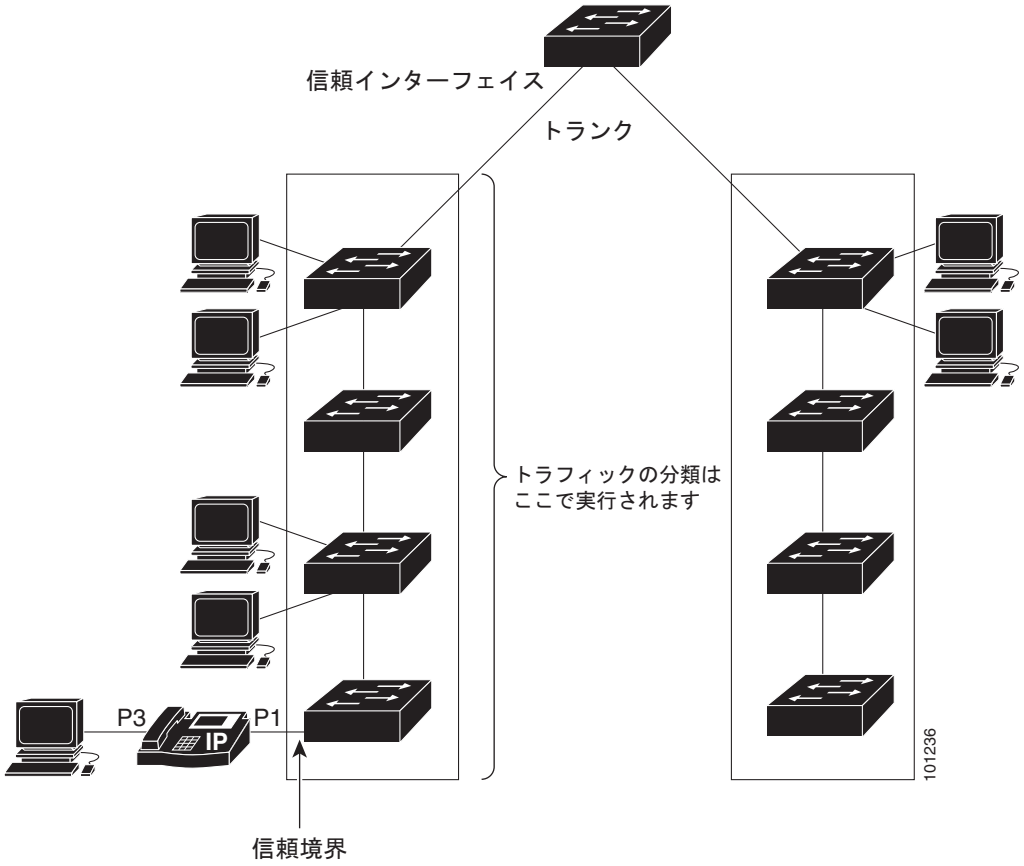
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネットワークの設定に応じて、次の 1 つ以上の作業、または「QoS ポリシーの設定」（P.39-44）の 1 つ以上の作業を実行する必要があります。

- 「QoS ドメイン内部のポートでの信頼状態の設定」（P.39-38）
- 「インターフェイスの CoS 値の設定」（P.39-40）
- 「ポート セキュリティを保証するための信頼境界の設定」（P.39-41）
- 「DSCP 透過性モードのイネーブル化」（P.39-42）
- 「別の QoS ドメインと境界を接しているポート上での DSCP 信頼状態の設定」（P.39-43）

QoS ドメイン内部のポートでの信頼状態の設定

QoS ドメインに着信するパケットは、QoS ドメインのエッジで分類されます。パケットがエッジで分類される場合は、QoS ドメイン内の各スイッチでパケットを分類する必要がないため、QoS ドメイン内のスイッチ ポートをいずれか 1 つの信頼状態に設定できます。図 39-11 に、ネットワーク トポロジの例を示します。

図 39-11　QoS ドメイン内部でのポートの信頼状態



特権 EXEC モードで開始し、次の手順に従って、受信するトラフィックの分類を信頼するようにポートを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	信頼するポートを指定し、インターフェイス コンフィギュレーション モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 3	**mls qos trust** [**cos** | **dscp** | **ip-precedence**]	ポートの信頼状態を設定します。 デフォルトでは、ポートは信頼されません。キーワードを指定しないと、デフォルトの **dscp** が使用されます。 キーワードの意味は次のとおりです。 • **cos**：パケットの CoS 値を使用して、入力パケットを分類します。タグのない非 IP パケットの場合、デフォルト ポートの CoS 値が使用されます。デフォルトのポート CoS 値は 0 です。 • **dscp**：パケットの DSCP 値を使用して、入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合はパケット CoS 値が使用されます。タグがないパケットでは、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 • **ip-precedence**：パケットの IP-precedence 値を使用して、入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合はパケット CoS 値が使用されます。タグがないパケットでは、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートを信頼されない状態に戻すには、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。

デフォルトの CoS 値の変更方法については、「インターフェイスの CoS 値の設定」（P.39-40）を参照してください。CoS/DSCP マップの設定方法については、「CoS/DSCP マップの設定」（P.39-65）を参照してください。

インターフェイスの CoS 値の設定

QoS は、**mls qos cos** インターフェイス コンフィギュレーション コマンドを使用して指定された CoS 値を、信頼できるポートと信頼できないポートで受信したタグなしフレームに割り当てます。

特権 EXEC モードで開始し、次の手順に従って、ポートのデフォルトの CoS 値を定義するか、デフォルトの CoS 値をそのポートのすべての着信パケットに割り当てます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 3	**mls qos cos** {*default-cos* | **override**}	ポートのデフォルトの CoS 値を設定します。 • *default-cos* には、ポートに割り当てるデフォルトの CoS 値を指定します。パケットがタグなしの場合は、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ～ 7 です。デフォルト値は 0 です。 • 着信パケットにあらかじめ設定されている信頼状態を上書きし、すべての着信パケットのポートにデフォルトのポート CoS 値を適用するには、**override** キーワードを使用します。デフォルトでは、CoS の上書きはディセーブルになっています。 特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合は、**override** キーワードを使用します。ポートが、すでに DSCP、CoS、または IP precedence を信頼するように設定されていても、このコマンドはそれまでに設定済みの信頼状態を上書きし、すべての着信 CoS 値にこの コマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、パケットの CoS 値は、入力ポートで、ポートのデフォルト CoS を使用して変更されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no mls qos cos** {*default-cos* | **override**} インターフェイス コンフィギュレーション コマンドを使用します。

ポート セキュリティを保証するための信頼境界の設定

一般的なネットワークでは、図 39-11（P.39-39）に示すように、Cisco IP Phone をスイッチ ポートに接続し、データ パケットを生成する装置を電話機の背面からカスケード接続します。Cisco IP Phone は、音声パケットの CoS レベルをハイ プライオリティ（CoS = 5）にし、データ パケットをロー プライオリティ（CoS = 0）にすることで、共有データ リンクの音声品質を保証します。電話機からスイッチに送信されるトラフィックには、通常は、IEEE 802.1Q ヘッダーを使用するタグのマークが付きます。このヘッダーには VLAN 情報と、パケットのプライオリティを示す CoS の 3 ビット フィールドが含まれます。

ほとんどの Cisco IP Phone の設定では、音声トラフィックのプライオリティが、ネットワークの他のタイプのトラフィックよりも高く設定されるように、電話機からスイッチに送信されるトラフィックが信頼されています。**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを使用して、電話機を接続するスイッチ ポートが、そのポートで受信するすべてのトラフィックの CoS ラベルを信頼するように設定します。**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを使用して、電話機を接続するルーテッド ポートが、そのポートで受信するすべてのトラフィックの DSCP ラベルを信頼するように設定します。

信頼設定では、信頼境界機能を使用して、ユーザが電話機をバイパスし、PC をスイッチに直接接続したときに、ハイ プライオリティ キューが誤って使用されるのを防ぐこともできます。信頼境界を使用しないと、PC によって生成された CoS ラベルがスイッチにより信頼されてしまいます（CoS 設定が信頼されるため）。これに対し、信頼境界機能は CDP を使用して、スイッチ ポート上の Cisco IP Phone（Cisco IP Phone 7910、7935、7940、7960 など）の存在を検出します。電話が検出されなかった場合、信頼境界機能はスイッチ ポートの信頼設定をディセーブルにし、ハイ プライオリティ キューが誤って使用されないようにします。スイッチに接続されたハブに PC と Cisco IP Phone が接続されている場合は、信頼境界機能が機能しないことに注意してください。

Cisco IP Phone に接続された PC がハイ プライオリティ データ キューを使用するのを防ぐことができる場合もあります。スイッチ CLI から **switchport priority extend cos** インターフェイス コンフィギュレーション コマンドを使用して、PC から受信したトラフィックのプライオリティを上書するように電話機を設定することができます。

特権 EXEC モードで開始し、次の手順に従ってポートの信頼境界をイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp run**	CDP をグローバルにイネーブルにします。デフォルトでは、CDP はイネーブルになっています。
ステップ 3	**interface** *interface-id*	Cisco IP Phone に接続されたポートを指定し、インターフェイス コンフィギュレーション モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**cdp enable**	ポートで CDP をイネーブルにします。デフォルトでは、CDP はイネーブルになっています。
ステップ 5	**mls qos trust cos** または **mls qos trust dscp**	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するようにスイッチ ポートを設定します。 Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するようにルーテッド ポートを設定します。 デフォルトでは、ポートは信頼されません。
ステップ 6	**mls qos trust device cisco-phone**	Cisco IP Phone が信頼できる装置であることを指定します。 信頼境界と auto-QoS（**auto qos voip** インターフェイス コンフィギュレーション コマンド）は同時にイネーブルにできません。これらは互いに排他的です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show mls qos interface**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

信頼境界機能をディセーブルにするには、**no mls qos trust device** インターフェイス コンフィギュレーション コマンドを使用します。

DSCP 透過性モードのイネーブル化

スイッチは、DSCP 透過性機能をサポートしています。この機能は、出力におけるパケットの DSCP フィールドだけに影響を与えます。デフォルトでは、DSCP 透過性はディセーブルです。スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて QoS（Quality of Service）に基づきます。

no mls qos rewrite ip dscp コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

（注）　DSCP 透過性をイネーブルにしても、IEEE 802.1Q トンネリング ポート上のポート信頼性の設定には影響しません。

DSCP 透過性の設定にかかわらず、スイッチは、トラフィックのプライオリティを表すサービス クラス（CoS）値の生成に使用するパケットの内部 DSCP 値を変更します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびスレッシュホールドを選択します。

特権 EXEC モードで開始し、次の手順に従ってスイッチの DSCP 透過性をイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	QoS をグローバルにイネーブルにします。
ステップ 3	**no mls qos rewrite ip dscp**	DSCP 透過性をイネーブルにします。スイッチは、IP パケットの DSCP フィールドを修正しないように設定されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

信頼設定に基づいて、または（DSCP 透過性をディセーブルにすることにより）ACL に基づいて DSCP 値を修正するようにスイッチを設定するには、**mls qos rewrite ip dscp** グローバル コンフィギュレーション コマンドを使用します。

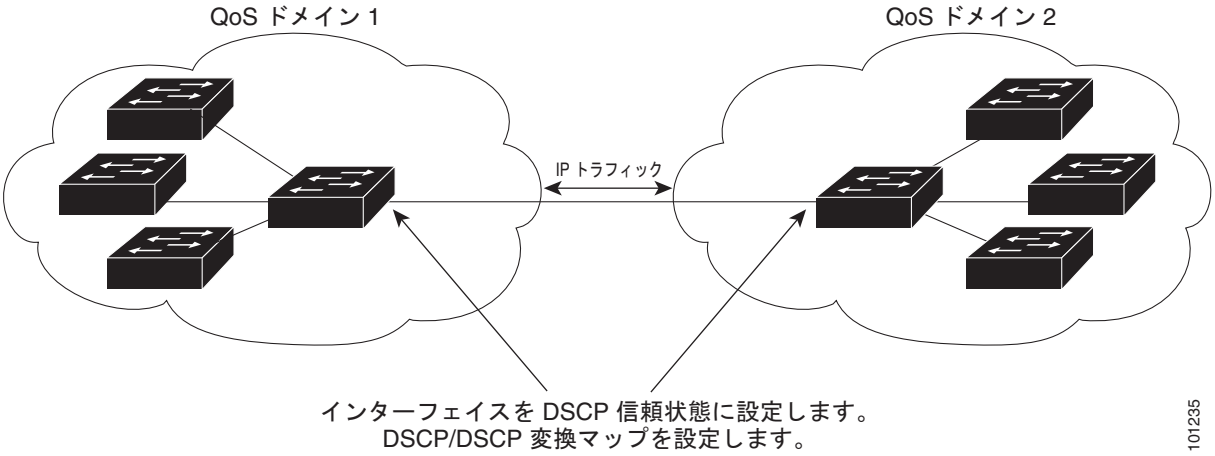
no mls qos グローバル コンフィギュレーション コマンドを使用して QoS をディセーブルにした場合は、CoS および DSCP 値は変更されません（デフォルトの QoS 設定）。

no mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを入力して DSCP 透過性をイネーブルにしてから、**mls qos trust** [**cos** | **dscp**] インターフェイス コンフィギュレーション コマンドを入力しても、DSCP 透過性はイネーブルのままです。

別の QoS ドメインと境界を接しているポート上での DSCP 信頼状態の設定

管理している 2 つの個別の QoS ドメイン間に、IP トラフィックの QoS 機能を実装する場合は、図 39-12 に示すように、それらのドメインの境界に位置するスイッチ ポートを DSCP 信頼状態に設定できます。これで、受信ポートが DSCP 信頼値を受け入れ、QoS の分類段階を省略できるようになります。2 つのドメインが異なる DSCP 値を使用している場合は、DSCP/DSCP 変換マップを設定して、DSCP 値のセットをもう一方のドメインの定義に一致するように変換できます。

図 39-12　別の QoS ドメインと境界を接するポート上での DSCP 信頼状態



特権 EXEC モードで開始し、次の手順に従ってポートで DSCP 信頼状態を設定し、DSCP/DSCP 変換マップを修正します。両方の QoS ドメインでマッピングの方法に一貫性を持たせるには、両方のドメインのポートで次の手順を実行する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを修正します。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。 • *dscp-mutation-name* には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp* には、最大で 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *out-dscp* には、1 つの DSCP 値を入力します。 指定できる DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id*	信頼するポートを指定し、インターフェイス コンフィギュレーション モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**mls qos trust dscp**	入力ポートを DSCP の信頼できるポートとして設定します。デフォルトでは、ポートは信頼されません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された入力 DSCP の信頼できるポートにマップを適用します。 *dscp-mutation-name* には、ステップ 2 で作成した変換マップ名を指定します。 1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos maps dscp-mutation**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートを信頼されない状態に戻すには、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの DSCP/DSCP 変換マップ値に戻すには、**no mls qos map dscp-mutation** *dscp-mutation-name* グローバル コンフィギュレーション コマンドを使用します。

次に、ポートを DSCP 信頼状態に設定し、10 ～ 13 の着信 DSCP 値を DSCP 30 にマッピングするように DSCP/DSCP 変換マップ（*gi0/2-mutation*）を修正する例を示します。

```
Switch(config)# mls qos map dscp-mutation gi1/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi1/2-mutation
Switch(config-if)# end
```

QoS ポリシーの設定

QoS ポリシーを設定するには、通常は、トラフィックのクラスへの分類、これらのトラフィック クラスに適用するポリシーの設定、ポートへのポリシーの付加が必要です。

基本的な情報については、「分類」（P.39-5）および「ポリシングおよびマーキング」（P.39-9）を参照してください。設定の注意事項については、「標準の QoS 設定の注意事項」（P.39-35）を参照してください。

ここでは、トラフィックを分類し、ポリシングし、マーキングする方法について説明します。ネットワークの設定に応じて、次の 1 つまたは複数の作業を実行する必要があります。

- 「ACL を使用したトラフィックの分類」（P.39-45）
- 「クラス マップを使用したトラフィックの分類」（P.39-48）
- 「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）
- 「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）
- 「aggregate ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング」（P.39-62）

ACL を使用したトラフィックの分類

IP トラフィックは、IP 標準 ACL または IP 拡張 ACL を使用して分類できます。非 IP トラフィックは、レイヤ 2 MAC ACL を使用して分類できます。

特権 EXEC モードで開始し、次の手順に従って、IP トラフィックの IP 標準 ACL を作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* にはアクセス リスト番号を入力します。指定できる範囲は 1 ～ 99 および 1300 ～ 1999 です。 • 条件が一致したときに特定のタイプのトラフィックを許可するには、**permit** キーワードを使用します。条件が一致したときに特定のタイプのトラフィックを拒否するには、**deny** キーワードを使用します。 • *source* には、パケットの送信元のネットワークまたはホストを入力します。**any** キーワードは、0.0.0.0 255.255.255.255 の略として使用できます。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。ワイルドカード ビットが、ネットワーク アドレスのホスト部分に適用されます。アクセス リスト ステートメントに一致しない発信元アドレスを持つホストは拒否されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```

特権 EXEC モードで開始し、次の手順に従って、IP トラフィックの IP 拡張 ACL を作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* にはアクセス リスト番号を入力します。指定できる範囲は 100 ～ 199 および 2000 ～ 2699 です。 • 条件が一致したときに特定のタイプのトラフィックを許可するには、**permit** キーワードを使用します。条件が一致したときに特定のタイプのトラフィックを拒否するには、**deny** キーワードを使用します。 • *protocol* には、IP プロトコルの名前または番号を入力します。疑問符（?）を使用すると、使用可能なプロトコルのキーワードのリストが表示されます。 • *source* には、パケットの送信元のネットワークまたはホストを入力します。これを指定するには、ドット付き 10 進表記を使用したり、*source* 0.0.0.0 *source-wildcard* 255.255.255.255 の略として **any** キーワードを使用したり、*source* 0.0.0.0 を表す **host** キーワードを使用します。 • *source-wildcard* では、無視するビット位置に 1 を入れて、ワイルドカード ビットを指定します。ワイルドカードを指定するには、ドット付き 10 進を使用したり、*source* 0.0.0.0 *source-wildcard* 255.255.255.255 の略として **any** キーワードを使用したり、*source* 0.0.0.0 を表す **host** キーワードを使用します。 • *destination* には、パケットの送信先のネットワークまたはホストを入力します。*destination* と *destination-wildcard* の指定には、*source* と *source-wildcard* で説明したものと同じオプションを使用できます。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。

次に、任意の送信元から、DSCP 値が 32 に設定された着信先への IP トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから、precedence 値が 5 に設定された 10.1.1.2 の着信先ホストまでの IP トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

次に、任意のソースから、DSCP が 32 に設定された着信先グループ アドレス 224.0.0.2 への PIM トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

特権 EXEC モードで開始し、次の手順に従って、非 IP トラフィックのレイヤ 2 MAC ACL を作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name*	リストの名前を指定して、レイヤ 2 MAC ACL を作成します。 このコマンドを入力すると、拡張 MAC ACL コンフィギュレーション モードに変わります。
ステップ 3	{**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	条件が一致したときに許可または拒否するトラフィックのタイプを指定し、必要な回数だけコマンドを入力します。 • *src-MAC-addr* には、パケットの送信元ホストの MAC アドレスを入力します。これを指定するには、16 進フォーマット（H.H.H）を使用したり、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff の略として **any** キーワードを使用したり、*source* 0.0.0 を表す **host** キーワードを使用します。 • *mask* では、無視するビット位置に 1 を入れて、ワイルドカード ビットを指定します。 • *dst-MAC-addr* には、パケットの送信先ホストの MAC アドレスを入力します。これを指定するには、16 進フォーマット（H.H.H）を使用したり、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff の略として **any** キーワードを使用したり、*source* 0.0.0 を表す **host** キーワードを使用します。 • （任意）*type mask* には、Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロトコルを識別します。*type* の指定できる範囲は 0 ～ 65535 です。通常は 16 進数で指定します。*mask* には、一致をテストする前に Ethertype に適用する *don't care* ビットを入力します。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*access-list-number* | *access-list-name*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アクセス リストを削除するには、**no mac access-list extended** *access-list-name* グローバル コンフィギュレーション コマンドを使用します。

次に、2 つの許可ステートメントを持つレイヤ 2 MAC ACL を作成する例を示します。最初のステートメントにより、MAC アドレスが 0001.0000.0001 のホストから MAC アドレスが 0002.0000.0001 のホストへのトラフィックが許可されます。次のステートメントでは、MAC アドレスが 0001.0000.0002 のホストから MAC アドレスが 0002.0000.0002 のホストへの、Ethertype が XNS-IDP のトラフィックだけが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

クラス マップを使用したトラフィックの分類

class-map グローバル コンフィギュレーション コマンドを使用して、特定のトラフィック フロー（またはクラス）の名前を指定し、他のすべてのトラフィックから分離します。クラス マップは、さらに詳細に分類するために、特定のトラフィック フローと照合する基準を定義します。一致ステートメントには、ACL、IP precedence 値、DSCP 値などの基準を入れることができます。一致基準は、クラスマップ コンフィギュレーション モードで 1 つの一致ステートメントを入力することにより定義されます。

（注）　**class** ポリシーマップ コンフィギュレーション コマンドを使用して、ポリシー マップの作成時にクラス マップを作成することもできます。詳細については、「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）および「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）を参照してください。

特権 EXEC モードで開始し、次の手順に従ってクラス マップを作成し、トラフィックを分類するための一致基準を定義します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] または **access-list** *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] または **mac access-list extended** *name* {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	IP トラフィック用の IP 標準 ACL または IP 拡張 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「ACL を使用したトラフィックの分類」（P.39-45）を参照してください。 （注）　アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。

	コマンド	目的
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラスマップ コンフィギュレーション モードに入ります。 デフォルトでは、クラス マップは定義されません。 • （任意）このクラス マップのすべての一致ステートメントで論理 AND を実行するには、**match-all** キーワードを使用します。クラス マップ内のすべての一致基準が一致する必要があります。 • （任意）このクラス マップのすべての一致ステートメントで論理 OR を実行するには、**match-any** キーワードを使用します。1 つまたは複数の一致基準が一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとに 1 つの **match** コマンドだけがサポートされるため、**match-all** キーワードと **match-any** キーワードの機能は同じです。
ステップ 4	**match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致基準を定義します。 デフォルトでは、一致基準は定義されません。 クラス マップごとに 1 つの一致基準だけがサポートされます。また、クラス マップごとに 1 つの ACL だけがサポートされます。 • **access-group** *acl-index-or-name* には、ステップ 2 で作成した ACL の番号または名前を指定します。 • **ip dscp** *dscp-list* には、着信パケットと照合する最大で 8 つの IP DSCP 値のリストを入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する最大で 8 つの IP-precedence 値のリストを入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show class-map**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class-map** [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用します。一致基準を削除するには、**no match** {**access-group** *acl-index-or-name* | **ip dscp** | **ip precedence**} クラスマップ コンフィギュレーション コマンドを使用します。

次に、*class1* という名前のクラス マップを設定する例を示します。*class1* には 1 つの一致基準（アクセス リスト 103）があります。この基準は、任意のホストから、DSCP 値 10 に一致する着信先へのトラフィックを許可します。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
Switch#
```

次に、DSCP 値 10、11、および 12 を持つ着信トラフィックと照合する、*class2* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#
```

次に、IP precedence 値 5、6、および 7 を持つ着信トラフィックと照合する、*class3* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```

ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング

アクションの対象とするトラフィック クラスを指定する非階層ポリシー マップを物理ポートで設定できます。アクションには、トラフィック クラスの CoS、DSCP、または IP precedence 値の信頼、トラフィック クラスへの特定の DSCP または IP precedence 値の設定、また一致する各トラフィック クラスのトラフィック帯域幅の制限（ポリサー）と、トラフィックがプロファイル外のときに実行するアクションの指定（マーキング）が含まれます。

ポリシー マップには次の特性もあります。

- 1 つのポリシー マップに、それぞれが異なる一致基準とポリサーを持つ複数のクラス ステートメントを含めることができます。
- ポリシー マップには、あらかじめ定義されたデフォルト トラフィック クラスを含めることができます。これはマップの末尾に明示的に配置されます。
- 1 つのポートを通じて受信されるトラフィックのタイプごとに、個別のポリシーマップ クラスを持つことができます。
- ポリシーマップの信頼状態とポートの信頼状態は互いに排他的で、後で設定した方が優先されます。

物理ポートでポリシー マップを設定する場合は、次の注意事項に従ってください。

- 入力ポートごとに 1 つのポリシー マップだけを付加できます。
- **mls qos map ip-prec-dscp** *dscp1...dscp8* グローバル コンフィギュレーション コマンドを使用して IP precedence/DSCP マップを設定すると、この設定は、IP precedence 値を信頼するように設定された入力インターフェイス上のパケットだけに影響を与えます。ポリシー マップで、**set ip precedence** *new-precedence* ポリシーマップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定すると、出力 DSCP 値は IP precedence/DSCP マップの影響を受けません。出力 DSCP 値を入力値とは異なる値にする場合は、**set dscp** *new-dscp* ポリシーマップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力するか、またはすでに使用していると、このコマンドはスイッチの設定で **set dscp** に変更されます。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用して、パケットの IP precedence 値を変更できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- ポートについて定義されたクラスごとに、第 2 レベルのポリシー マップを個別に設定できます。第 2 レベルのポリシー マップは、各トラフィック クラスで実行するポリシング アクションを指定します。階層ポリシー マップの設定については、「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）を参照してください。

- ポリシーマップとポートの信頼状態の両方を、1 つの物理インターフェイス上で実行できます。ポリシーマップは、ポートの信頼状態の前に適用します。
- **class class-default** ポリシー マップ コンフィギュレーション コマンドを使用してデフォルト トラフィック クラスを設定すると、分類されないトラフィック（トラフィック クラスで指定されている一致基準に適合しないトラフィック）は、デフォルト トラフィック クラス（**class-default**）として処理されます。

特権 EXEC モードで開始し、次の手順に従って非階層ポリシー マップを作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラスマップ コンフィギュレーション モードに入ります。 デフォルトでは、クラス マップは定義されません。 • （任意）このクラス マップのすべての一致ステートメントで論理 AND を実行するには、**match-all** キーワードを使用します。クラス マップ内のすべての一致基準が一致する必要があります。 • （任意）このクラス マップのすべての一致ステートメントで論理 OR を実行するには、**match-any** キーワードを使用します。1 つまたは複数の一致基準が一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとに 1 つの **match** コマンドだけがサポートされるため、**match-all** キーワードと **match-any** キーワードの機能は同じです。
ステップ 3	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードに入ります。 デフォルトでは、ポリシー マップは定義されません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合に DSCP が 0 に、パケットがタグ付きの場合に CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 4	**class** [*class-map-name* | **class-default**]	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードに入ります。 デフォルトでは、ポリシー マップ クラスマップは定義されません。 **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスがすでに定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスはあらかじめ定義されていて、任意のポリシーに追加できます。これは常に、ポリシー マップの末尾に配置されます。**class-default** クラスには **match any** が暗黙的に含まれているため、他のトラフィック クラスに一致しなかったパケットはすべて、**class-default** に一致します。

	コマンド	目的
ステップ 5	**trust** [**cos** | **dscp** | **ip-precedence**]	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼状態を設定します。 **（注）** このコマンドは、同じポリシー マップ内では **set** コマンドと互いに排他的です。**trust** コマンドを入力する場合は、ステップ 6 に進みます。 デフォルトでは、ポートは信頼されません。キーワードが指定されず、コマンドが入力されている場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：QoS は、受信した CoS 値またはデフォルトのポート CoS 値と、CoS/DSCP マップを使用して DSCP 値を導出します。 • **dscp**：QoS は、入力パケットの DSCP 値を使用して DSCP 値を導出します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用して DSCP 値を導出します。タグなしの非 IP パケットでは､QoS はデフォルトのポート CoS 値を使用して DSCP 値を導出します。いずれの場合でも、DSCP 値は CoS/DSCP マップから導出されます。 • **ip-precedence**：QoS は、入力パケットの IP precedence 値と IP precedence/DSCP マップを使用して DSCP 値を導出します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用して DSCP 値を導出します。タグなしの非 IP パケットでは、QoS はデフォルトのポート CoS 値を使用して DSCP 値を導出します。いずれの場合でも、DSCP 値は CoS/DSCP マップから導出されます。 詳細については、「CoS/DSCP マップの設定」（P.39-65）を参照してください。
ステップ 6	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットで新しい値を設定することにより IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類したトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *new-precedence* には、分類したトラフィックに割り当てる新しい IP-precedence 値を入力します。指定できる範囲は 0 ～ 7 です。

	コマンド	目的
ステップ 7	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類したトラフィックのポリサーを定義します。 デフォルトでは、ポリサーは定義されません。サポートされているポリサーの数については、「標準の QoS 設定の注意事項」（P.39-35）を参照してください。 • *rate-bps* には、平均トラフィック レートをビット/秒（b/s）単位で指定します。指定できる範囲は 8000 ～ 10000000000 です。 *burst-byte* には、通常のバースト サイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超えたときに実行するアクションを指定します。パケットを廃棄するには、**exceed-action drop** キーワードを使用します。（ポリシング設定 DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。詳細については、「ポリシング設定 DSCP マップの設定」（P.39-67）を参照してください。
ステップ 8	**exit**	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *interface-id*	ポリシー マップを付加するポートを指定し、インターフェイス コンフィギュレーション モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 11	**service-policy input** *policy-map-name*	ポリシー マップ名を指定し、これを入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class** *class-map-name* ポリシーマップ コンフィギュレーション コマンドを使用します。信頼されない状態に戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、**no set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*} ポリシーマップ コンフィギュレーション コマンドを使用します。既存のポリサーを削除するには、**no police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] ポリシーマップ コンフィギュレーション コマンドを使用します。ポリシー マップとポートの関連付けを削除するには、**no service-policy input** *policy-map-name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポリシー マップを作成し、入力ポートに適用する例を示します。この設定では、IP 標準 ACL は、ネットワーク 10.1.0.0 からのトラフィックを許可します。この分類に一致するトラフィックでは、着信パケットの DSCP 値は信頼されます。一致するトラフィックが、平均トラフィック レートの 48000 b/s と通常のバースト サイズの 8000 バイトを超える場合は、（ポリシング設定 DSCP マップに基づいて）その DSCP がマークダウンされ、送信されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map flow1t
```

```
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input flow1t
```

次に、2 つの許可ステートメントを使用してレイヤ 2 MAC ACL を作成し、入力ポートに付加する例を示します。最初の許可ステートメントにより、MAC アドレスが 0001.0000.0001 のホストから MAC アドレスが 0002.0000.0001 のホストまでのトラフィックが許可されます。次の許可ステートメントでは、MAC アドレスが 0001.0000.0002 のホストから MAC アドレスが 0002.0000.0002 のホストまでの Ethertype XNS-IDP トラフィックだけが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

次の例では、IPv4 トラフィックと IPv6 トラフィックの両方に適用されるとともに、分類されないトラフィックに適用されるデフォルト クラスを含むクラス マップの作成方法を示します。

```
Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list ipv6-any permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
```

階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング

階層ポリシー マップは SVI では設定できますが、他のタイプのインターフェイスでは設定できません。階層ポリシングでは、VLAN レベルとインターフェイスレベルのポリシー マップを組み合わせて 1 つのポリシー マップを作成します。

SVI では、VLAN レベルのポリシー マップは、アクションの対象となるトラフィック クラスを指定します。アクションには、CoS、DSCP、または IP precedence 値の信頼設定や、トラフィック クラスの特定の DSCP または IP precedence 値の設定などが含まれます。individual ポリサーの影響を受ける物理ポートを指定するには、インターフェイスレベルのポリシー マップを使用します。

階層ポリシー マップを設定する場合は、次の注意事項に従ってください。

- 階層ポリシー マップを設定する前に、ポリシー マップのインターフェイス レベルで指定する物理ポートで VLAN ベースの QoS をイネーブルにする必要があります。
- 入力ポートまたは SVI ごとに 1 つのポリシー マップだけを付加できます。
- ポリシー マップには、それぞれ異なる一致基準とアクションを持つ複数のクラス ステートメントを含めることができます。
- SVI で受信されるトラフィックのタイプごとに、個別のポリシーマップ クラスを持つことができます。
- ポリシーマップとポートの信頼状態の両方を、1 つの物理インターフェイス上で実行できます。ポリシーマップは、ポートの信頼状態の前に適用します。
- **mls qos map ip-prec-dscp** *dscp1...dscp8* グローバル コンフィギュレーション コマンドを使用して IP precedence/DSCP マップを設定すると、この設定は、IP precedence 値を信頼するように設定された入力インターフェイス上のパケットだけに影響を与えます。ポリシー マップで、**set ip precedence** *new-precedence* ポリシーマップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定すると、出力 DSCP 値は IP precedence/DSCP マップの影響を受けません。出力 DSCP 値を入力値とは異なる値にする場合は、**set dscp** *new-dscp* ポリシーマップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力するか、またはすでに使用していると、このコマンドはスイッチの設定で **set dscp** に変更されます。**set ip dscp** コマンドを入力すると、スイッチ コンフィギュレーションではこの設定は **set dscp** として表示されます。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用して、パケットの IP precedence 値を変更できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- VLAN ベースの QoS をイネーブルにすると、階層ポリシー マップは、それまでに設定されているポートベースのポリシー マップよりも優先されます。
- 階層ポリシー マップは SVI に付加され、VLAN に属するすべてのトラフィックに影響を与えます。VLAN レベルのポリシー マップで指定されたアクションは、SVI に属するトラフィックに影響を与えます。ポートレベルのポリシー マップでのポリシング アクションは、関連する物理インターフェイス上の入力トラフィックに影響を与えます。
- トランク ポートで階層ポリシー マップを設定する場合は、VLAN の範囲が重なってはなりません。範囲が重なると、ポリシー マップで指定されたアクションが、重なった VLAN の入力トラフィックと出力トラフィックに影響を与えます。
- 階層ポリシー マップでは aggregate ポリサーはサポートされていません。
- VLAN ベースの QoS を有効にすると、スイッチは、VLAN マップなどの VLAN ベースの機能をサポートします。
- 階層ポリシー マップは、プライベート VLAN のプライマリ VLAN だけで設定できます。

- **class class-default** ポリシー マップ コンフィギュレーション コマンドを使用してデフォルト トラフィック クラスを設定すると、分類されないトラフィック（トラフィック クラスで指定されている一致基準に適合しないトラフィック）は、デフォルト トラフィック クラス（**class-default**）として処理されます。

特権 EXEC モードで開始し、次の手順に従って階層ポリシー マップを作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	VLAN レベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードに入ります。クラス マップの作成については、「クラス マップを使用したトラフィックの分類」（P.39-48）を参照してください。 デフォルトでは、クラス マップは定義されません。 • （任意）このクラス マップのすべての一致ステートメントで論理 AND を実行するには、**match-all** キーワードを使用します。クラス マップ内のすべての一致基準が一致する必要があります。 • （任意）このクラス マップのすべての一致ステートメントで論理 OR を実行するには、**match-any** キーワードを使用します。1 つまたは複数の一致基準が一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとに 1 つの **match** コマンドだけがサポートされるため、**match-all** キーワードと **match-any** キーワードの機能は同じです。
ステップ 3	**match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致基準を定義します。 デフォルトでは、一致基準は定義されません。 クラス マップごとに 1 つの一致基準だけがサポートされます。また、クラス マップごとに 1 つの ACL だけがサポートされます。 • **access-group** *acl-index-or-name* には、ACL の番号または名前を指定します。 • **ip dscp** *dscp-list* には、着信パケットと照合する最大で 8 つの IP DSCP 値のリストを入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する最大で 8 つの IP-precedence 値のリストを入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 4	**exit**	クラスマップ コンフィギュレーション モードに戻ります。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**class-map** [**match-all** | **match-any**] *class-map-name*	インターフェイスレベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードに入ります。 デフォルトでは、クラス マップは定義されません。 • （任意）このクラス マップのすべての一致ステートメントで論理 AND を実行するには、**match-all** キーワードを使用します。クラス マップ内のすべての一致基準が一致する必要があります。 • （任意）このクラス マップのすべての一致ステートメントで論理 OR を実行するには、**match-any** キーワードを使用します。1 つまたは複数の一致基準が一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとに 1 つの **match** コマンドだけがサポートされるため、**match-all** キーワードと **match-any** キーワードの機能は同じです。
ステップ 7	**match input-interface** *interface-id-list*	インターフェイスレベルのクラス マップの対象となる物理ポートを指定します。最大で 6 つのポートを次のように指定できます。 • 単一のポート（1 つのエントリとしてカウントされる） • スペースで区切られたポートのリスト（各ポートが 1 つのエントリとしてカウントされる） • ハイフンで区切られたポートの範囲（2 つのエントリとしてカウントされる） このコマンドは、子レベルのポリシー マップでだけ使用でき、子レベルのポリシー マップ内での唯一の一致条件である必要があります。
ステップ 8	**exit**	クラスマップ コンフィギュレーション モードに戻ります。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**policy-map** *policy-map-name*	ポリシーマップ名を入力してインターフェイスレベルのポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードに入ります。 デフォルトでは、ポリシー マップは定義されず、ポリシングは実行されません。
ステップ 11	**class-map** *class-map-name*	インターフェイスレベルのトラフィックの分類を定義し、ポリシーマップ コンフィギュレーション モードに入ります。 デフォルトでは、ポリシーマップ クラスマップは定義されません。 **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスがすでに定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。

	コマンド	目的
ステップ 12	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類されたトラフィックに individual ポリサーを定義します。 デフォルトでは、ポリサーは定義されません。サポートされているポリサーの数については、「標準の QoS 設定の注意事項」（P.39-35）を参照してください。 *rate-bps* には、平均トラフィック レートをビット/秒（b/s）単位で指定します。指定できる範囲は 8000 ～ 10000000000 です。 • *burst-byte* には、通常のバースト サイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超えたときに実行するアクションを指定します。パケットを廃棄するには、**exceed-action drop** キーワードを使用します。（ポリシング設定 DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。詳細については、「ポリシング設定 DSCP マップの設定」（P.39-67）を参照してください。
ステップ 13	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 14	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**policy-map** *policy-map-name*	ポリシーマップ名を入力して VLAN レベルのポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードに入ります。 デフォルトでは、ポリシー マップは定義されません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合に DSCP が 0 に、パケットがタグ付きの場合に CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 16	**class** [*class-map-name* | **class-default**]	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードに入ります。 デフォルトでは、ポリシー マップ クラスマップは定義されません。 **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスがすでに定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスはあらかじめ定義されていて、任意のポリシーに追加できます。これは常に、ポリシー マップの末尾に配置されます。**class-default** クラスには **match any** が暗黙的に含まれているため、他のトラフィック クラスに一致しなかったパケットはすべて、**class-default** に一致します。

	コマンド	目的
ステップ 17	**trust** [**cos** | **dscp** | **ip-precedence**]	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼状態を設定します。 **（注）** このコマンドは、同じポリシー マップ内では **set** コマンドと互いに排他的です。**trust** コマンドを入力する場合は、ステップ 18 を飛ばします。 デフォルトでは、ポートは信頼されません。キーワードが指定されず、コマンドが入力されている場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：QoS は、受信した CoS 値またはデフォルトのポート CoS 値と、CoS/DSCP マップを使用して DSCP 値を導出します。 • **dscp**：QoS は、入力パケットの DSCP 値を使用して DSCP 値を導出します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用して DSCP 値を導出します。タグなしの非 IP パケットでは、QoS はデフォルトのポート CoS 値を使用して DSCP 値を導出します。いずれの場合でも、DSCP 値は CoS/DSCP マップから導出されます。 • **ip-precedence**：QoS は、入力パケットの IP precedence 値と IP precedence/DSCP マップを使用して DSCP 値を導出します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用して DSCP 値を導出します。タグなしの非 IP パケットでは、QoS はデフォルトのポート CoS 値を使用して DSCP 値を導出します。いずれの場合でも、DSCP 値は CoS/DSCP マップから導出されます。 詳細については、「CoS/DSCP マップの設定」（P.39-65）を参照してください。
ステップ 18	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットで新しい値を設定することにより IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類したトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *new-precedence* には、分類したトラフィックに割り当てる新しい IP-precedence 値を入力します。指定できる範囲は 0 ～ 7 です。
ステップ 19	**service-policy** *policy-map-name*	インターフェイスレベルのポリシーマップ名を指定し（ステップ 10 より）、これを VLAN レベルのポリシー マップと関連付けます。 VLAN レベルのポリシー マップが複数のクラスを指定する場合は、Cisco IOS Release 12.2(25)SED 以降、各クラスに異なる **service-policy** *policy-map-name* コマンドを使用できます。
ステップ 20	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 21	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 22	**interface** *interface-id*	階層ポリシー マップを付加する SVI を指定し、インターフェイス コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 23	**service-policy input** *policy-map-name*	VLAN レベルのポリシーマップ名を指定し、SVI に適用します。前のステップとこのコマンドを繰り返し、ポリシー マップを他の SVI に適用します。 階層 VLAN レベルのポリシー マップに複数のインターフェイスレベルのポリシー マップがある場合は、すべてのクラス マップを、**service-policy** *policy-map-name* コマンドで指定された同じ VLAN レベルのポリシー マップに設定しなければなりません。
ステップ 24	**end**	特権 EXEC モードに戻ります。
ステップ 25	**show policy-map** [*policy-map-name* [**class** *class-map-name*]] または **show mls qos vlan-based**	設定を確認します。
ステップ 26	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class** *class-map-name* ポリシーマップ コンフィギュレーション コマンドを使用します。

ポリシー マップで信頼されない状態に戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、**no set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*} ポリシーマップ コンフィギュレーション コマンドを使用します。

（注）　インターフェイスレベルのポリシー マップで既存のポリサーを削除するには、**no police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] ポリシーマップ コンフィギュレーション コマンドを使用します。階層ポリシー マップとポートの関連付けを削除するには、**no service-policy input** *policy-map-name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、階層ポリシー マップを作成する例を示します。

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
Switch#
```

次に、新しいマップを SVI に付加する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input g3/0/1 - g3/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcmap
```

```
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

次の例では、ポリシー マップにデフォルト トラフィック クラスを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c) set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust cos
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

次の例では、class-default が先に設定されていても、ポリシー マップ pm3 の末尾にデフォルト トラフィック クラスが自動的に配置される様子を示します。

```
Switch# show policy-map pm3
  Policy Map pm3
    Class cm-3
      set dscp 4
    Class cm-4
      trust cos
    Class class-default
      police 8000 80000 exceed-action drop
Switch#
```

aggregate ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング

aggregate ポリサーを使用することで、同じポリシー マップ内の複数のトラフィック クラスで共有されるポリサーを作成できます。ただし、aggregate ポリサーは、異なるポリシー マップ間やポート間では使用できません。

aggregate ポリサーは、物理ポートの非階層ポリシー マップだけで設定できます。

特権 EXEC モードで開始し、次の手順に従って aggregate ポリサーを作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos aggregate-policer** *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**}	同じポリシー マップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。 デフォルトでは、aggregate ポリサーは定義されません。サポートされているポリサーの数については、「標準の QoS 設定の注意事項」（P.39-35）を参照してください。 • *aggregate-policer-name* には、aggregate ポリサーの名前を指定します。 *rate-bps* には、平均トラフィック レートをビット/秒（b/s）単位で指定します。指定できる範囲は 8000 ～ 10000000000 です。 • *burst-byte* には、通常のバースト サイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • レートを超えたときに実行するアクションを指定します。パケットを廃棄するには、**exceed-action drop** キーワードを使用します。（ポリシング設定 DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。詳細については、「ポリシング設定 DSCP マップの設定」（P.39-67）を参照してください。
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name*	必要に応じてトラフィックを分類するクラス マップを作成します。詳細については、「クラス マップを使用したトラフィックの分類」（P.39-48）を参照してください。
ステップ 4	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードに入ります。 詳細については、「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）を参照してください。
ステップ 5	**class** [*class-map-name* | **class-default**]	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードに入ります。 詳細については、「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）を参照してください。
ステップ 6	**police aggregate** *aggregate-policer-name*	同じポリシー マップ内の複数のクラスに aggregate ポリサーを適用します。 *aggregate-policer-name* には、ステップ 2 で指定した名前を入力します。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ポリシー マップを付加するポートを指定し、インターフェイス コンフィギュレーション モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 9	**service-policy input** *policy-map-name*	ポリシー マップ名を指定し、これを入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show mls qos aggregate-policer** [*aggregate-policer-name*]	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定された aggregate ポリサーをポリシー マップから削除するには、**no police aggregate** *aggregate-policer-name* ポリシー マップ コンフィギュレーション モードを使用します。aggregate ポリサーとそのパラメータを削除するには、**no mls qos aggregate-policer** *aggregate-policer-name* グローバル コンフィギュレーション コマンドを使用します。

次に、aggregate ポリサーを作成し、これをポリシー マップ内の複数のクラスに付加する例を示します。この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。ネットワーク 10.1.0.0 から着信するトラフィックでは、着信パケットの DSCP が信頼されます。ホスト 11.3.1.1 から着信するトラフィックでは、パケットの DSCP が 56 に変更されます。ネットワーク 10.1.0.0 とホスト 11.3.1.1 からのトラフィック レートがポリシングされます。トラフィックの平均レートが 48000 b/s を超え、通常のバースト サイズが 8000 バイトを超える場合は、（ポリシング設定 DSCP マップに基づいて）その DSCP がマークダウンされ、送信されます。ポリシー マップは入力ポートに付加されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

DSCP マップの設定

ここでは、次の設定情報について説明します。

- 「CoS/DSCP マップの設定」（P.39-65）（任意）
- 「IP precedence/DSCP マップの設定」（P.39-66）（任意）
- 「ポリシング設定 DSCP マップの設定」（P.39-67）（任意、マップのヌル設定が適切でない場合を除く）
- 「DSCP/CoS マップの設定」（P.39-68）（任意）
- 「DSCP/DSCP 変換マップの設定」（P.39-69）（任意、マップのヌル設定が適切でない場合を除く）

DSCP/DSCP 変換マップを除くすべてのマップはグローバルに定義されており、すべてのポートに適用されます。

CoS/DSCP マップの設定

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表すために内部で使用する DSCP 値にマッピングします。

表 39-13 に、デフォルトの CoS/DSCP マップを示します。

表 39-13　デフォルトの CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

これらの値がネットワークに適していない場合は、値を修正する必要があります。

特権 EXEC モードで開始し、次の手順に従って CoS/DSCP マップを修正します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map cos-dscp** *dscp1...dscp8*	CoS/DSCP マップを修正します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 指定できる DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps cos-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのマップに戻すには、**no mls qos cos-dscp** グローバル コンフィギュレーション コマンドを使用します。

次に、CoS/DSCP マップを修正し、表示する例を示します。

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

IP precedence/DSCP マップの設定

IP precedence/DSCP マップを使用して、着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部で使用する DSCP 値にマッピングします。

表 39-14 に、デフォルトの IP precedence/DSCP マップを示します。

表 39-14　デフォルトの IP Precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

これらの値がネットワークに適していない場合は、値を修正する必要があります。

特権 EXEC モードで開始し、次の手順に従って IP precedence/DSCP マップを修正します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map ip-prec-dscp** *dscp1...dscp8*	IP precedence/DSCP マップを修正します。 *dscp1...dscp8* には、IP precedence 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 指定できる DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps ip-prec-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのマップに戻すには、**no mls qos ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

次の例に、IP precedence/DSCP マップを修正し、表示する方法を示します。

```
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

ポリシング設定 DSCP マップの設定

ポリシング設定 DSCP マップを使用し、ポリシングおよびマーキング アクションの結果として、DSCP 値を新しい値にマークダウンします。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

特権 EXEC モードで開始し、次の手順に従ってポリシング設定 DSCP マップを修正します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map policed-dscp** *dscp-list* **to** *mark-down-dscp*	ポリシング設定 DSCP マップを修正します。 • *dscp-list* には、最大で 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *mark-down-dscp* には、対応するポリシング設定（マークダウンされた）DSCP 値を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps policed-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのマップに戻すには、**no mls qos policed-dscp** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 50 を 57 にマッピングし、DSCP 値 0 をマークダウンする例を示します。

```
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    00 00 00 00 00 00 00 00 58 59
      6 :    60 61 62 63
```

（注）　このポリシング設定 DSCP マップでは、マークダウンされた DSCP 値はマトリクスの本体に表示されます。d1 列は元の DSCP の最上位桁を指定し、d2 行は元の DSCP の最下位桁を指定します。d1 値と d2 値の交点がマークダウン値を示します。たとえば、元の DSCP 値 53 は、マークダウンされた DSCP 値 0 に対応します。

DSCP/CoS マップの設定

DSCP/CoS マップを使用して、4 つの出力キューの 1 つを選択するために使用する CoS 値を生成します。

表 39-15 に、デフォルトの DSCP/CoS マップを示します。

表 39-15　デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

これらの値がネットワークに適していない場合は、値を修正する必要があります。

特権 EXEC モードで開始し、次の手順に従って DSCP/CoS マップを修正します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-cos** *dscp-list* **to** *cos*	DSCP/CoS マップを修正します。 • *dscp-list* には、最大で 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *cos* には、DSCP 値が対応する 1 つの CoS 値を入力します。 指定できる DSCP の範囲は 0 ～ 63 で、CoS の範囲は 0 ～ 7 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps dscp-to-cos**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのマップに戻すには、**no mls qos dscp-cos** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 0、8、16、24、32、40、48、50 を CoS 値 0 にマッピングし、このマップを表示する例を示します。

```
Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
```

```
Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 00 01
      1 :    01 01 01 01 01 01 00 02 02 02
      2 :    02 02 02 02 00 03 03 03 03 03
      3 :    03 03 00 04 04 04 04 04 04 04
      4 :    00 05 05 05 05 05 05 05 00 06
      5 :    00 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

（注）　この DSCP/CoS マップでは、CoS 値がマトリクスの本体に表示されています。d1 列は DSCP の最上位桁を指定し、d2 行は DSCP の最下位桁を指定します。d1 値と d2 値の交点が CoS 値を示します。たとえば、この DSCP/CoS マップでは、DSCP 値 08 は CoS 値 0 に対応します。

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインが異なる DSCP 定義を持つ場合は、DSCP/DSCP 変換マップを使用して、一方の DSCP 値のセットをもう一方のドメインの定義に適合するように変換します。DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します（入力変換）。

入力変換では、新しい DSCP 値がパケット内の値を上書きし、QoS はこの新しい値を使用してパケットを処理します。スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

特権 EXEC モードで開始し、次の手順に従って DSCP/DSCP 変換マップを修正します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを修正します。 • *dscp-mutation-name* には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp* には、最大で 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *out-dscp* には、1 つの DSCP 値を入力します。 指定できる DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id*	マップを付加するポートを指定し、インターフェイス コンフィギュレーション モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**mls qos trust dscp**	入力ポートを DSCP の信頼できるポートとして設定します。デフォルトでは、ポートは信頼されません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された入力 DSCP の信頼できるポートにマップを適用します。 *dscp-mutation-name* には、ステップ 2 で指定した変換マップ名を入力します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show mls qos maps dscp-mutation**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのマップに戻すには、**no mls qos dscp-mutation** *dscp-mutation-name* グローバル コンフィギュレーション コマンドを使用します。

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。明示的に設定されていないエントリはすべて変更されません（ヌル マップ内の指定のままです）。

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
   mutation1:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 00 00 00 00 00 00 00 10 10
      1 :    10 10 10 10 14 15 16 17 18 19
      2 :    20 20 20 23 24 25 26 27 28 29
      3 :    30 30 30 30 30 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

（注） この DSCP/DSCP 変換マップでは、変換される値がマトリクスの本体に表示されています。d1 列は元の DSCP の最上位桁を指定し、d2 行は元の DSCP の最下位桁を指定します。d1 値と d2 値の交点が変換される値を示します。たとえば、DSCP 値 12 が変換される値 10 に対応します。

入力キューの特性の設定

ネットワークと QoS ソリューションの複雑さによっては、次の項の作業をすべて実行しなければならないことがあります。次の特性を決定する必要があります。

- （DSCP または CoS 値によって）各キューに割り当てるパケット
- 各キューに適用する廃棄スレッシュホールド（%）と、各スレッシュホールドにマッピングする CoS または DSCP 値
- 各キューに割り当てる使用可能なバッファ領域の大きさ
- 各キューに割り当てる使用可能な帯域幅の大きさ
- 高いプライオリティを割り当てる必要があるトラフィック（音声など）があるかどうか

ここでは、次の設定情報について説明します。

- 「DSCP または CoS 値の入力キューへのマッピングと、WTD スレッショルドの設定」（P.39-71）（任意）
- 「入力キュー間でのバッファ領域の割り当て」（P.39-72）（任意）
- 「入力キュー間での帯域幅の割り当て」（P.39-73）（任意）
- 「入力プライオリティ キューの設定」（P.39-74）（任意）

DSCP または CoS 値の入力キューへのマッピングと、WTD スレッショルドの設定

特定の DSCP または CoS を持つパケットを特定のキューに置き、低いプライオリティを持つパケットが廃棄されるように、キューのスレッショルドを調整することで、トラフィックのプライオリティを設定できます。

特権 EXEC モードで開始し、次の手順に従って、DSCP または CoS 値を入力キューにマッピングし、WTD スレッショルドを設定します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* または **mls qos srr-queue input cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を、入力キューとスレッショルド ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 39 および 48 ～ 63 は、キュー 1 およびスレッショルド 1 にマッピングされます。DSCP 値 40 ～ 47 は、キュー 2 およびスレッショルド 1 にマッピングされます。 デフォルトでは、CoS 値 0 ～ 4、6、7 は、キュー 1 およびスレッショルド 1 にマッピングされます。CoS 値 5 は、キュー 2 およびスレッショルド 1 にマッピングされます。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • *threshold-id* で指定できる範囲は 1 ～ 3 です。スレッショルド 3 の廃棄スレッショルド（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。 • *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
ステップ 3	**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2*	スレッショルド 1 および 2 の 2 つの WTD スレッショルド（%）を入力キューに割り当てます。デフォルトでは、両方のスレッショルドが 100% に設定されます。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • *threshold-percentage1 threshold-percentage2* では、指定できる範囲は 1 ～ 100 です。各値はスペースで区切ります。 各スレッショルドは、キューに割り当てられたキュー記述子の総数に対する割合です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show mls qos maps**	設定を確認します。 DSCP 入力キュー スレッショルド マップがマトリクスとして表示されます。d1 列は DSCP 番号の最上位桁を指定し、d2 行は DSCP 番号の最下位桁を指定します。d1 値と d2 値の交点がキュー ID とスレッショルド ID です。たとえば、キュー 2 とスレッショルド 1（02-01）のようになります。 CoS 入力キュー スレッショルド マップは、一番上の行に CoS 値を、2 番めの行に対応するキュー ID とスレッショルド ID を示します。たとえば、キュー 2 とスレッショルド 2（2-2）のようになります。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの CoS 入力キュー スレッショルド マップまたはデフォルトの DSCP 入力キュー スレッショルド マップに戻すには、**no mls qos srr-queue input cos-map** または **no mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD スレッショルド（%）に戻すには、**no mls qos srr-queue input threshold** *queue-id* グローバル コンフィギュレーション コマンドを使用します。

次の例では、DSCP 値 0 ～ 6 を、入力キュー 1 と廃棄スレッショルド 50% のスレッショルド 1 にマッピングする方法を示します。DSCP 値 20 と 26 は、入力キュー 1 とスレッショルド 70% のスレッショルド 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

次の例では、DSCP 値（0 ～ 6）が WTD スレッショルド 50% に割り当てられ、WTD スレッショルド 70% に割り当てられた DSCP 値（20 ～ 26）よりも早く廃棄されます。

入力キュー間でのバッファ領域の割り当て

2 つのキューの間で入力バッファを分割する（領域の大きさを割り当てる）比率を定義します。バッファおよび帯域幅割り当ては、パケットを廃棄する前にバッファリングできるデータの量を制御します。

特権 EXEC モードで開始し、次の手順に従って入力キューの間でバッファを割り当てます。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input buffers** *percentage1 percentage2*	入力キュー間にバッファを割り当てます。 デフォルトでは、90% のバッファをキュー 1 に割り当て、10% のバッファをキュー 2 に割り当てます。 *percentage1 percentage2* では、指定できる範囲は 0 ～ 100 です。各値はスペースで区切ります。 キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show mls qos interface buffer** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no mls qos srr-queue input buffers** グローバル コンフィギュレーション コマンドを使用します。

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

入力キュー間での帯域幅の割り当て

入力キューの間に割り当てる使用可能な帯域幅の大きさを指定する必要があります。重みの比率は、SRR スケジューラがパケットを各キューから送信する頻度の比率です。帯域幅割り当てとバッファ割り当ては、パケットを廃棄する前にバッファリングできるデータの大きさを制御します。入力キューでは、SRR は共有モードだけで動作します。

特権 EXEC モードで開始し、次の手順に従って入力キュー間で帯域幅を割り当てます。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input bandwidth** *weight1 weight2*	共有ラウンド ロビンの重みを入力キューに割り当てます。 *weight1* と *weight2* のデフォルト設定は 4 です（帯域幅の 1/2 が 2 つのキューの間で均等に共有されます）。 *weight1* および *weight2* では、指定可能な範囲は 1 ～ 100 です。各値はスペースで区切ります。 SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に SRR は、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定された重みに従い、両方の入力キューで残りの帯域幅を共有し、キューを処理します。詳細については、「入力プライオリティ キューの設定」（P.39-74）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos interface queueing** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no mls qos srr-queue input bandwidth** グローバル コンフィギュレーション コマンドを使用します。

次に、キューに入力帯域幅を割り当てる例を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/（25+75）、キュー 2 が 75/（25+75）です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

入力プライオリティ キューの設定

プライオリティ キューは、優先して進める必要があるトラフィックにだけ使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューは帯域幅の一部が保証されており、オーバーサブスクライブ型のリング上でネットワーク トラフィックが多い場合（バックプレーンが送達できる量よりもトラフィックが多い場合、およびキューが満杯でフレームを廃棄している場合）に、遅延とジッタを軽減します。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に SRR は、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定された重みに従い、両方の入力キューで残りの帯域幅を共有し、キューを処理します。

特権 EXEC モードで開始し、次の手順に従ってプライオリティ キューを設定します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight*	キューをプライオリティ キューとして割り当て、リングが輻輳している場合に内部リングの帯域幅を保証します。 デフォルトのプライオリティ キューはキュー 2 で、帯域幅の 10% が割り当てられています。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • **bandwidth** *weight* には、内部リングの帯域幅のパーセンテージを割り当てます。指定できる範囲は 0 ～ 40 です。大きい値はリング全体に影響を与え、パフォーマンスを低下させることがあるため、保証可能な帯域幅の大きさには制限があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos interface queueing** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no mls qos srr-queue input priority-queue** *queue-id* グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth 0** と入力します。

次に、キューに入力帯域幅を割り当てる例を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/（4+4）です。SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。そのあと、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

出力キューの特性の設定

ネットワークと QoS ソリューションの複雑さによっては、次の項の作業をすべて実行しなければならないことがあります。次の特性を決定する必要があります。

- DSCP または CoS 値によって各キューおよびスレッショルド ID にマッピングされるパケット
- キューセットに適用する廃棄スレッショルド（%）（ポート 1 つあたり 4 つの出力キュー）と、そのトラフィック タイプに予約するメモリと最大メモリの大きさ
- キューセットに割り当てる固定バッファ領域の大きさ
- ポートの帯域幅をレート制限する必要があるかどうか
- 出力キューを処理する頻度と、使用する方法（シェーピング、共有、またはその両方）

ここでは、次の設定情報について説明します。

- 「設定時の注意事項」（P.39-75）
- 「出力キューセットのバッファ領域の割り当てと WTD スレッショルドの設定」（P.39-75）（任意）
- 「DSCP または CoS 値の出力キューとスレッショルド ID へのマッピング」（P.39-78）（任意）
- 「出力キューでの SRR のシェーピングされた重みの設定」（P.39-79）（任意）
- 「出力キューでの SRR の共有された重みの設定」（P.39-80）（任意）
- 「出力緊急キューの設定」（P.39-81）（任意）
- 「出力インターフェイスでの帯域幅の制限」（P.39-82）（任意）

設定時の注意事項

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングされた重みが設定されていない場合は、SRR は共有モードでこのキューを処理します。

出力キューセットのバッファ領域の割り当てと WTD スレッショルドの設定

mls qos queue-set output *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンドを使用して、バッファの可用性を保証し、WTD スレッショルドを設定し、キューセットの最大割り当てを設定できます。

各スレッシュホールドは、キューに割り当てられたメモリのパーセンテージであり、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* グローバル コンフィギュレーション コマンドを使用して指定します。キューは WTD を使用して、トラフィック クラスごとに異なる廃棄パーセンテージをサポートします。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合だけ、設定を変更してください。

特権 EXEC モードで開始し、次の手順に従って、キューセットのメモリ割り当てと廃棄スレッシュホールドを設定します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4*	バッファをキューセットに割り当てます。 デフォルトでは、すべての割り当て値は、4 つのキューに均等にマッピングされます（25、25、25、25）。各キューがバッファ スペースの 1/4 を持ちます。 • *qset-id* には、キューセットの ID を入力します。指定できる範囲は 1 ～ 2 です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。 • *allocation1 ... allocation4* には、キューセットのキューごとに 1 つずつ、4 つのパーセンテージを指定します。*allocation1*、*allocation3*、および *allocation4* に指定できる範囲は 0 ～ 99 です。*allocation2* の場合、指定できる範囲は 1 ～ 100 です（CPU バッファを含む）。 トラフィックの重要度に応じてバッファを割り当てます。たとえば、ベストエフォート トラフィックを含むキューには大きな割合のバッファを与えます。

	コマンド	目的
ステップ 3	**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*	WTD スレッシュホールドを設定し、バッファの可用性を保証し、キューセットの最大メモリ割り当てを設定します（ポート 1 つあたり 4 つの出力キュー）。 デフォルトでは、キュー 1、3、4 の WTD スレッシュホールドは 100% に設定されます。キュー 2 のスレッシュホールドは 200% に設定されます。キュー 1、2、3、4 の予約済みスレッシュホールドは 50% に設定されます。すべてのキューの最大スレッシュホールドは 400% に設定されます。 • *qset-id* には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ～ 2 です。 • *queue-id* には、コマンドを実行するキューセットの特定のキューを入力します。指定できる範囲は 1 ～ 4 です。 • *drop-threshold1 drop-threshold2* には、キューに割り当てられたメモリのパーセンテージとして表される 2 つの WTD スレッシュホールドを指定します。指定できる範囲は 1 ～ 3200% です。 • *reserved-threshold* には、キューに保証（予約）するメモリの大きさを、割り当てられるメモリのパーセンテージとして入力します。指定できる範囲は 1 ～ 100% です。 • *maximum-threshold* では、フル状態のキューが予約量を超えるバッファを取得できるようにします。これは、共通のプールが空ではない場合に、キューがパケットを廃棄せずに保持できる最大メモリです。指定できる範囲は 1 ～ 3200% です。
ステップ 4	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 5	**queue-set** *qset-id*	ポートをキューセットにマッピングします。 *qset-id* には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ～ 2 です。デフォルトは 1 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos interface** [*interface-id*] **buffers**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no mls qos queue-set output** *qset-id* **buffers** グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD スレッシュホールド（%）に戻すには、**no mls qos queue-set output** *qset-id* **threshold** [*queue-id*] グローバル コンフィギュレーション コマンドを使用します。

次の例では、ポートをキューセット 2 にマッピングする方法を示します。出力キュー 1 にバッファ スペースの 40 % を、出力キュー 2、3、4 にそれぞれ 20 % を割り当てます。キュー 2 の廃棄スレッシュホールドを、割り当てられたメモリの 40% と 60% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットを廃棄せずに保持可能な最大メモリを 200% に設定します。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# queue-set 2
```

DSCP または CoS 値の出力キューとスレッシュホールド ID へのマッピング

特定の DSCP または CoS を持つパケットを特定のキューに置き、低いプライオリティを持つパケットが廃棄されるようにキューのスレッシュホールドを調整することで、トラフィックのプライオリティを設定できます。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合だけ、設定を変更してください。

特権 EXEC モードで開始し、次の手順に従って DSCP または CoS 値を出力キューにマッピングし、スレッシュホールド ID を設定します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue output dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* または **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を、出力キューとスレッシュホールド ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 15 は、キュー 2 およびスレッシュホールド 1 にマッピングされます。DSCP 値 16 ～ 31 は、キュー 3 およびスレッシュホールド 1 にマッピングされます。DSCP 値 32 ～ 39 および 48 ～ 63 は、キュー 4 およびスレッシュホールド 1 にマッピングされます。DSCP 値 40 ～ 47 は、キュー 1 およびスレッシュホールド 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 は、キュー 2 およびスレッシュホールド 1 にマッピングされます。CoS 値 2 および 3 は、キュー 3 およびスレッシュホールド 1 にマッピングされます。CoS 値 4、6、7 は、キュー 4 およびスレッシュホールド 1 にマッピングされます。CoS 値 5 は、キュー 1 およびスレッシュホールド 1 にマッピングされます。 • *queue-id* で指定できる範囲は 1 ～ 4 です。 • *threshold-id* で指定できる範囲は 1 ～ 3 です。スレッシュホールド 3 の廃棄スレッシュホールド（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。 • *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show mls qos maps**	設定を確認します。 DSCP 出力キュースレッシュホールド マップがマトリクスとして表示されます。d1 列は DSCP 番号の最上位桁を指定し、d2 行は DSCP 番号の最下位桁を指定します。d1 値と d2 値の交点がキュー ID とスレッシュホールド ID です。たとえば、キュー 2 とスレッシュホールド 1（02-01）のようになります。 CoS 出力キュースレッシュホールド マップは、一番上の行に CoS 値を、2 番めの行に対応するキュー ID とスレッシュホールド ID を示します。たとえば、キュー 2 とスレッシュホールド 2（2-2）のようになります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの DSCP 出力キュースレッシュホールド マップまたはデフォルトの CoS 出力キュー スレッシュホールド マップに戻すには、**no mls qos srr-queue output dscp-map** または **no mls qos srr-queue output cos-map** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 10 および 11 を出力キュー 1 およびスレッシュホールド 2 にマッピングする例を示します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

出力キューでの SRR のシェーピングされた重みの設定

各キューに割り当てる使用可能な帯域幅を指定できます。重みの比率は、SRR スケジューラがパケットを各キューから送出する頻度の比率です。

出力キューでは、シェーピングされた重みか共有された重み、またはその両方を設定できます。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。シェーピングされた重みについては、「SRR のシェーピングおよび共有」（P.39-15）を参照してください。共有された重みについては、「出力キューでの SRR の共有された重みの設定」（P.39-80）を参照してください。

特権 EXEC モードで開始し、次の手順に従ってシェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キューで帯域幅のシェーピングをイネーブルにします。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 3	**srr-queue bandwidth shape** *weight1 weight2 weight3 weight4*	SRR の重みを出力キューに割り当てます。 デフォルトでは、weight1 は 25 に設定され、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。 *weight1 weight2 weight3 weight4* には、シェーピングするポートのパーセンテージを制御する重みを入力します。このキューのシェーピング帯域幅は、インバース比（1/*weight*）によって制御されます。各値はスペースで区切ります。指定できる範囲は 0 ～ 65535 です。 重み 0 を設定すると、対応するキューは共有モードで動作します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。同じキューセットのキューにシェーピングと共有を混在させて設定する場合、最小番号のキューにシェーピングを設定します。 シェーピング モードは、共有モードを無効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用します。

次に、キュー 1 で帯域幅のシェーピングを設定する例を示します。キュー 2、3、4 の重み比が 0 に設定されているので、キューは共有モードで動作します。キュー 1 の帯域幅の重みは 1/8（12.5%）です。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

出力キューでの SRR の共有された重みの設定

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、1 つのキューが空になってリンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。共有では、デキューイングの頻度は重みの比によって制御され、絶対値には意味はありません。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合だけ、設定を変更してください。

特権 EXEC モードで開始し、次の手順に従って共有された重みを割り当て、ポートにマッピングされた 4 つの出力キューでの帯域幅の共有をイネーブルにします。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 3	**srr-queue bandwidth share** *weight1 weight2 weight3 weight4*	SRR の重みを出力キューに割り当てます。 デフォルトでは、4 つの重みはすべて 25 です（帯域幅の 1/4 が各キューに割り当てられます）。 *weight1 weight2 weight3 weight4* には、SRR スケジューラがパケットを送出する頻度の比率を制御する重みを入力します。各値はスペースで区切ります。指定できる範囲は 1 ～ 255 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、出力ポートで稼動する SRR スケジューラの重みの比を設定する方法を示します。4 つのキューが使用され、共有モードで 1、2、3、4 の各キューに割り当てられる帯域幅はそれぞれ 1/（1+2+3+4）、2/（1+2+3+4）、3/（1+2+3+4）、および 4/（1+2+3+4）です（それぞれ 10%、20%、30%、および 40%）。キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

出力緊急キューの設定

特定のパケットを出力緊急キューに入れることで、そのパケットのプライオリティを他のパケットよりも高く設定できます。SRR は、このキューが空になるまで処理してから他のキューを処理します。

特権 EXEC モードで開始し、次の手順に従って出力緊急キューをイネーブルにします。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	スイッチで QoS をイネーブルにします。
ステップ 3	**interface** *interface-id*	出力ポートを指定し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 4	**priority-queue out**	出力緊急キューをイネーブルにします。このキューは、デフォルトではディセーブルです。 このコマンドを設定すると、SRR に参加するキューの数が 1 つ少なくなるため、SRR の重みとキュー サイズの比に影響を与えます。これは、**srr-queue bandwidth shape** または **srr-queue bandwidth share** コマンドの *weight1* が無視されることを意味します（比率の計算に使用されません）。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

出力緊急キューをディセーブルにするには、**no priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

出力インターフェイスでの帯域幅の制限

出力ポートでは帯域幅を制限できます。たとえば、ある顧客が、高速リンクの一部しか費用を負担しない場合は、帯域幅をそのパーセンテージまで制限できます。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合だけ、設定を変更してください。

特権 EXEC モードで開始し、次の手順に従って出力ポートで帯域幅を制限します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レートを制限するポートを指定し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 3	**srr-queue bandwidth limit** *weight1*	制限するポート速度のパーセンテージを指定します。指定できる範囲は 10 ～ 90 です。 デフォルトでは、ポートはレート制限されず、100% に設定されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*] **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no srr-queue bandwidth limit** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの帯域幅を 80% に制限する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth limit 80
```

このコマンドを 80% に設定した場合、ポートは 20% の時間はアイドル状態になります。ラインレートは接続速度の 80% まで下がります（800 Mb/s）。ただし、ハードウェアはラインレートが 6 つずつ増加するよう調整しているので、この値は厳密ではありません。

標準の QoS 情報の表示

標準の QoS 情報を表示するには、表 39-16 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 39-16　標準の QoS 情報を表示するためのコマンド

コマンド	目的
show class-map [*class-map-name*]	トラフィックを分類するための一致基準を定義する QoS クラスマップを表示します。
show mls qos	グローバルな QoS 設定情報を表示します。
show mls qos aggregate-policer [*aggregate-policer-name*]	aggregate ポリサーの設定を表示します。
show mls qos input-queue	入力キューの QoS 設定を表示します。
show mls qos interface [*interface-id*] [**buffers** | **policers** | **queueing** | **statistics**]	バッファ割り当て、ポリサーを設定したポート、キューイング方法、入力および出力の統計情報など、ポート レベルの QoS 情報を表示します。
show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	QoS マッピング情報を表示します。
show mls qos queue-set [*qset-id*]	出力キューの QoS 設定を表示します。
show mls qos vlan *vlan-id*	指定された SVI に付加されたポリシー マップを表示します。
show policy-map [*policy-map-name* [**class** *class-map-name*]]	着信トラフィックの分類基準を定義する QoS ポリシー マップを表示します。 **（注）** 着信トラフィックの分類情報を表示する目的で **show policy-map interface** 特権 EXEC コマンドは使用しないでください。**control-plane** および **interface** キーワードはサポートされていません。表示される統計情報は無視してください。
show running-config | include rewrite	DSCP 透過性設定を表示します。

CHAPTER 40

EtherChannel およびリンクステート トラッキングの設定

この章では、IE 3000 スイッチに EtherChannel を設定する手順について説明します。EtherChannel は、スイッチ、ルータ、サーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用して配線クローゼットとデータセンター間の帯域幅を拡張でき、ボトルネックが発生しやすいネットワーク内の任意の場所に EtherChannel を配備できます。EtherChannel には、残りのリンク間で負荷を再分配し、リンク切断から自動的に回復する機能があります。リンクに障害が発生した場合、EtherChannel は仲介なしに、障害のあるリンクからチャネル内の残りのリンクにトラフィックをリダイレクトします。またこの章では、リンクステート トラッキングの設定方法についても説明します。

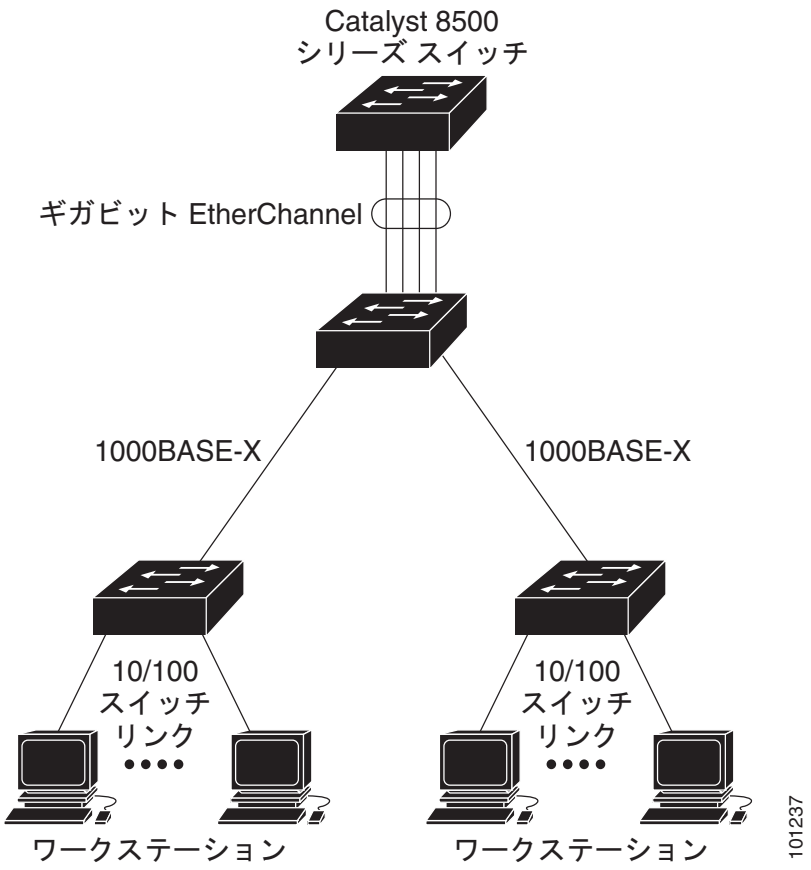
（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

EtherChannel の概要

EtherChannel の概要

EtherChannel は、単一の論理リンクにバンドルされた個々のファスト イーサネットまたはギガビット イーサネット リンクで構成されます（図 40-1 を参照）。

図 40-1　一般的な EtherChannel の設定



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 800 Mbps（ファスト EtherChannel）または 8 Gbps（ギガビット EtherChannel）の全二重帯域幅を提供します。各 EtherChannel には、最大 8 個の（設定に互換性のある）イーサネット ポートを含めることができます。

各 EtherChannel 内のすべてのポートは、レイヤ 2 またはレイヤ 3 ポートのいずれかとして設定する必要があります。EtherChannel の数は、6 に制限されています。EtherChannel レイヤ 3 ポートは、ルーテッド ポートで構成されます。ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。

（注）　レイヤ 3 EtherChannel は、IP サービス イメージが稼動しているスイッチでだけサポートされます。

詳細については、「EtherChannel 設定時の注意事項」（P.40-10）を参照してください。

EtherChannel には、Port Aggregation Protocol（PAgP）、Link Aggregation Control Protocol（LACP）、または on のいずれかのモードを設定できます。EtherChannel の両端は同じモードで設定します。

- EtherChannel の一端を PAgP または LACP モードのいずれかで設定すると、システムはチャネルのもう一端とネゴシエートして、アクティブになるポートを決定します。互換性のないポートは独立ステートになり、他の単一リンクと同様にデータ トラフィックを継続して伝送します。ポート設定は変更されませんが、ポートは EtherChannel には参加しません。
- **on** モードで EtherChannel を設定した場合、ネゴシエーションは実行されません。スイッチは EtherChannel の互換性のあるポートすべてを強制的にアクティブにします。チャネルのもう一端（他のスイッチ上の）も **on** モードで設定する必要があります。そうしないと、パケット損失が発生します。

EtherChannel 内のリンクで障害が発生すると、障害リンク上でそれまで伝送されていたトラフィックがその EtherChannel 内の残りのリンクに切り替えられます。スイッチでトラップがイネーブルになっている場合は、障害が発生すると、スイッチ、EtherChannel、および障害リンクを識別するトラップが送信されます。EtherChannel の 1 つのリンクに着信したブロードキャストおよびマルチキャスト パケットが、EtherChannel の別のリンクに戻されることはありません。

ポートチャネル インターフェイス

EtherChannel を作成すると、ポートチャネル論理インターフェイスも作成されます。

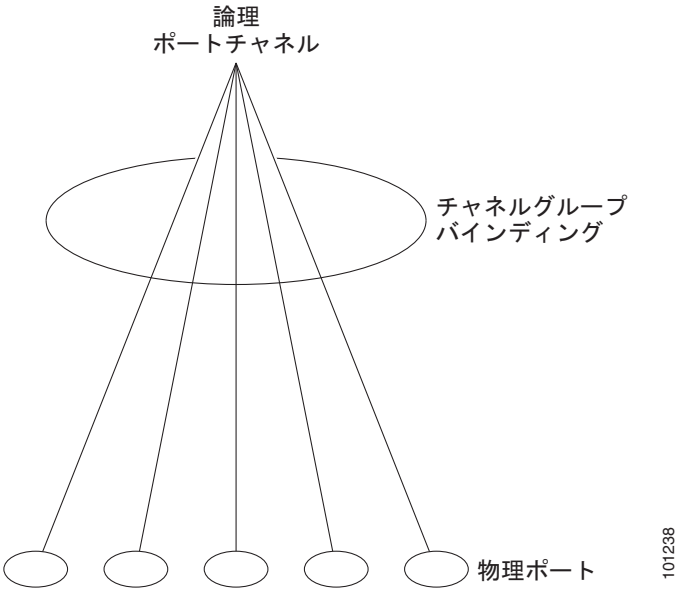
- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスをダイナミックに作成します。

  また、**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。*channel-group-number* は、*port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは新しいポート チャネルをダイナミックに作成します。
- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。次に、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを手動で EtherChannel に割り当てます。

レイヤ 2 およびレイヤ 3 ポートのいずれの場合も、**channel-group** コマンドを実行すると、物理ポートと論理インターフェイスがバインドされます（図 40-2 を参照）。

各 EtherChannel には、1 ～ 6 まで番号付けされたポートチャネル論理インターフェイスがあります。このポートチャネル インターフェイスの番号は、**channel-group** インターフェイス コンフィギュレーション コマンドにより指定された番号に対応します。

図 40-2　物理ポート、論理ポート チャネル、およびチャネル グループの関係



EtherChannel を設定したあと、ポートチャネル インターフェイスに適用された設定の変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャネル インターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、spanning-tree コマンドを使用して、レイヤ 2 EtherChannel をトランクとして設定します。

Port Aggregation Protocol

Port Aggregation Protocol（PAgP）はシスコ独自のプロトコルで、Cisco スイッチと、PAgP に対応するためにライセンスを得たベンダーのスイッチでだけ動作します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク（チャネルまたは集約ポート）にダイナミックにグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータスおよびタイプが同じであるポートが PAgP によってグループ化されます。リンクが EtherChannel にグループ化されたあと、グループは PAgP によって単一のスイッチ ポートとしてスパニング ツリーに追加されます。

PAgP モード

表 40-1 に、**channel-group** インターフェイス コンフィギュレーション コマンドにユーザが設定できる EtherChannel PAgP モードを示します。

表 40-1　EtherChannel PAgP モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。この設定では、PAgP パケットの伝送が最小化されます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。

スイッチ ポートは、**auto** または **desirable** モードに設定されたパートナー ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto および **desirable** モードでは、どちらの場合も、ポートはパートナー ポートとネゴシエートし、一定の基準に従って EtherChannel を形成します。その基準とは、ポート速度、およびレイヤ 2 EtherChannel の場合、トランキング ステートと VLAN 番号などです。

ポート間で PAgP モードが異なっていても、モードが矛盾しない限り EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートと EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートと EtherChannel を形成できます。

auto モードのポートは、どちらのポートも PAgP ネゴシエーションを開始しないので、**auto** モードの別のポートとは EtherChannel を形成できません。

PAgP 対応のパートナーにスイッチが接続されている場合は、**non-silent** キーワードを使用して、非サイレント動作を行うようにスイッチ ポートを設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されているものと見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しない装置にスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼動させると、このスイッチ ポートが動作しなくなります。ただし、サイレント設定を使用すると、PAgP が動作するようになり、チャネル グループにポートを接続したり、ポートを伝送に使用したりできます。

PAgP と仮想スイッチとの相互作用とデュアル アクティブ検出

1 つの仮想スイッチは、複数の Catalyst 6500 コア スイッチとなることができます。これらのコア スイッチ間は、制御トラフィックとデータ トラフィックを伝送する Virtual Switch Link（VSL; 仮想スイッチ リンク）により接続されます。これらのスイッチのうち 1 台がアクティブ モードとなり、その他はスタンバイ モードとなります。冗長性を確保するため、IE3000 スイッチなどのリモート スイッチは、Remote Satellite Link（RSL）により仮想スイッチに接続されます。

2 つのスイッチ間の VSL に障害が発生した場合、一方のスイッチはもう一方のスイッチのステータスを認識しません。両方のスイッチがアクティブ モードに変わり、ネットワーク内で設定の重複（IP アドレスやブリッジ ID の重複など）を伴う *デュアル アクティブ状態*が発生する可能性があります。ネットワークがダウンする可能性があります。

デュアル アクティブ状態を回避するため、コア スイッチは RSL 経由でリモート スイッチに PAgP Protocol Data Unit（PDU; プロトコル データ ユニット）を送信します。PAgP PDU はアクティブなスイッチを識別し、リモート スイッチはコア スイッチとの同期が取れるようコア スイッチに PDU を転送します。アクティブ スイッチで障害が発生した、またはアクティブ スイッチをリセットした場合は、スタンバイ スイッチがアクティブ スイッチを引き継ぎます。VSL がダウンした場合でも、一方のコア スイッチはもう一方のスイッチのステータスを認識し、ステートを変更しません。

PAgP と他の機能との相互作用

Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）および Cisco Discovery Protocol（CDP; シスコ検出プロトコル）は、EtherChannel の物理ポートを経由してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP プロトコル データ ユニット（PDU）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼動状態のポート上だけです。

Link Aggregation Control Protocol

LACP は IEEE 802.3ad で定義されており、Cisco スイッチが IEEE 802.3ad プロトコルに準拠したスイッチ間のイーサネット チャネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク（チャネルまたは集約ポート）にダイナミックにグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータスおよびタイプが同じであるポートが LACP によってグループ化されます。リンクが EtherChannel にグループ化されたあと、グループは LACP によって単一のスイッチ ポートとしてスパニング ツリーに追加されます。

LACP モード

表 40-2 に、**channel-group** インターフェイス コンフィギュレーション コマンドにユーザが設定できる EtherChannel LACP モードを示します。

表 40-2　EtherChannel LACP モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。
passive	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。この設定では、LACP パケットの伝送が最小化されます。

LACP の **active** モードおよび **passive** モードでは、どちらの場合も、ポートはパートナー ポートとネゴシエートし、一定の基準に従って EtherChannel を形成します。その基準とは、ポート速度、およびレイヤ 2 EtherChannel の場合、トランキング ステートと VLAN 番号などです。

ポート間で LACP モードが異なっていても、モードが矛盾しない限り EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートと EtherChannel を形成できます。
- **passive** モードのポートは、どちらのポートも LACP ネゴシエーションを開始しないので、**passive** モードの別のポートとは EtherChannel を形成できません。

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを経由してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている、稼動状態のポート上だけです。

EtherChannel の on モード

EtherChannel の **on** モードを使用すると、手動で EherChannel を設定できます。**on** モードにすると、ポートはネゴシエーションせずに強制的に EtherChannel に加入されます。リモート装置で PAgP または LACP がサポートされていない場合に、**on** モードは便利な機能です。**on** モードでは、リンクの両端のスイッチが **on** モードで設定されている場合に限り、EtherChannel を使用できます。

on モードで設定された同一チャネル グループ内のポートには、速度およびデュプレックスなどのポート特性に互換性がある必要があります。**on** モードで設定されていても、互換性のないポートは停止します。

注意　**on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端にあるポートで同じ設定になっている必要があります。グループの設定を誤ると、パケット損失またはスパニング ツリーのループが発生することがあります。

ロード バランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に変換することによって、チャネル内のリンク間でトラフィックの負荷を分散させます。EtherChannel ロード バランシングには、MAC アドレスや IP アドレス、送信元アドレスや宛先アドレス、または送信元と宛先の両方のアドレスを使用できます。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。ロード バランシングおよび転送方式を設定するには、**port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャネルポートを使用しますが、送信元ホストが同じパケットは同じチャネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットに指定されている宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

送信元/宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。この転送方式は、送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式の負荷分散を組み合わせたものです。特定のスイッチに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元/宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

送信元 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、IP アドレスが異なるパケットはそれぞれ異なるチャネルポートを使用しますが、IP アドレスが同じパケットは同じチャネル ポートを使用します。

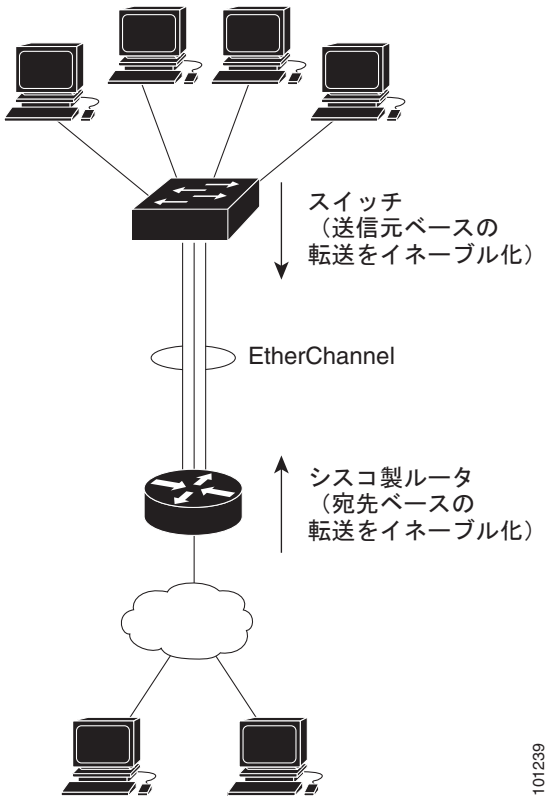
宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、異なるチャネル ポートに送信できます。ただし、異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常に同じチャネル ポートで送信されます。

送信元/宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたものです。特定のスイッチに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるかが不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

ロードバランシング方式ごとに利点が異なります。ロードバランシング方式は、ネットワーク内のスイッチの位置、および負荷分散が必要なトラフィックの種類に基づいて選択する必要があります。図 40-3 では、4 台のワークステーションのデータを集約するスイッチの EtherChannel がルータと通信しています。ルータは単一の MAC アドレスを持つ装置であるため、スイッチの EtherChannel で送信元ベース転送を行うことにより、スイッチがルータで有効な帯域幅をすべて使用するようになります。ルータは、宛先ベース転送を行うように設定されます。このように設定すると、多数のワークステーションで、ルータの EtherChannel からのトラフィックが均等に分散されることが保証されるためです。

設定には最も柔軟なオプションを使用してください。たとえば、チャネル上のトラフィックが単一 MAC アドレスを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンクが常に選択されます。送信元アドレスまたは IP アドレスを使用した方が、ロード バランシングの効率がよくなることがあります。

図 40-3　負荷分散および転送方式



EtherChannel の設定

ここでは、次の設定情報について説明します。

- 「EtherChannel のデフォルト設定」（P.40-10）
- 「EtherChannel 設定時の注意事項」（P.40-10）
- 「レイヤ 2 EtherChannel の設定」（P.40-12）（必須）
- 「レイヤ 3 EtherChannel の設定」（P.40-14）（必須）
- 「EtherChannel ロード バランシングの設定」（P.40-17）（任意）
- 「PAgP 学習方式およびプライオリティの設定」（P.40-18）（任意）
- 「LACP ホットスタンバイ ポートの設定」（P.40-19）（任意）

（注）　ポートが正しく設定されていることを確認してください。詳細については、「EtherChannel 設定時の注意事項」（P.40-10）を参照してください。

（注）　EtherChannel を設定したあと、ポートチャネル インターフェイスに適用された設定の変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートに限り有効です。

EtherChannel のデフォルト設定

表 40-3 に、EtherChannel のデフォルト設定を示します。

表 40-3　EtherChannel のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし。
ポートチャネル論理インターフェイス	定義なし。
PAgP モード	デフォルトなし。
PAgP 学習方式	すべてのポートで集約ポート ラーニング。
PAgP プライオリティ	すべてのポートで 128。
LACP モード	デフォルトなし。
LACP 学習方式	すべてのポートで集約ポート ラーニング。
LACP ポート プライオリティ	すべてのポートで 32768。
LACP システム プライオリティ	32768。
LACP システム ID	LACP システム プライオリティおよびスイッチの MAC アドレス。
ロード バランシング	着信パケットの送信元 MAC アドレスに基づいてスイッチ上で負荷を分散。

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定しないと、ネットワーク ループなどの問題を回避するために、一部の EtherChannel ポートが自動的にディセーブルになることがあります。設定上の問題を回避するために、次の注意事項に従ってください。

- 6 を超える数の EtherChannel をスイッチで設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを最大 8 個使用して設定してください。
- LACP EtherChannel は、同じタイプのイーサネット ポートを最大 16 個使用して設定してください。最大 8 個のポートをアクティブにして、最大 8 個のポートをスタンバイ モードにすることができます。
- EtherChannel 内のすべてのポートが、同じ速度および同じデュプレックス モードで動作するように設定してください。
- EtherChannel のすべてのポートをイネーブルにしてください。**shutdown** インターフェイス コンフィギュレーション コマンドを使用してディセーブル化された EtherChannel のポートは、リンク障害として扱われ、そのポートのトラフィックが EtherChannel 内の残りのポートの 1 つに転送されます。
- グループを初めて作成したときは、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次に示すパラメータのいずれかの設定を変更する場合は、グループ内のすべてのポートに関する設定も変更する必要があります。
  - 許可 VLAN リスト
  - 各 VLAN のスパニング ツリー パス コスト
  - 各 VLAN のスパニング ツリー ポート プライオリティ
  - スパニング ツリーの PortFast 設定

- ポートが複数の EtherChannel グループのメンバーにならないように設定してください。
- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP と LACP が稼動している EtherChannel グループは同じスイッチ上に共存できます。個々の EtherChannel グループは PAgP または LACP のどちらかを実行できますが、相互運用することはできません。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポートを EtherChannel の一部として設定しないでください。
- セキュア ポートを EtherChannel の一部として、またはその逆として設定しないでください。
- プライベート VLAN ポートを EtherChannel の一部として設定しないでください。
- アクティブまたはアクティブでない EtherChannel メンバーを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がスイッチ インターフェイスに設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用してスイッチの IEEE 802.1x をグローバルにイネーブルにする前に、インターフェイスから EtherChannel の設定を削除します。
- ダウンストリーム Etherchannel インターフェイスの一部になる個別のインターフェイスでリンクステート トラッキングをイネーブルにしないでください。
- レイヤ 2 EtherChannel の場合
  - EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されているポートは、EtherChannel を形成できません。
  - トランク ポートから EtherChannel を設定する場合は、すべてのトランクでトランキング モード（Inter-Switch Link（ISL; スイッチ間リンク）または IEEE 802.1Q）が同じであることを確認してください。EtherChannel ポートでトランク モードが統一されていない場合は、予想外の結果が生じる可能性があります。
  - EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポートで同じ許容範囲の VLAN をサポートします。VLAN の許容範囲が異なる場合、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
  - スパニング ツリー パス コストが異なるポートは、設定に互換性があれば、EtherChannel を形成できます。異なるスパニング ツリー パス コストを設定しても、それ自体は、EtherChannel を形成でポートに矛盾をもたらしません。
- レイヤ 3 EtherChannel の場合は、チャネル内の物理ポートに対してではなく、ポートチャネル論理インターフェイスに対してレイヤ 3 アドレスを割り当ててください。

レイヤ 2 EtherChannel の設定

レイヤ 2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネル グループにポートを割り当てます。このコマンドにより、ポートチャネル論理インターフェイスが自動的に作成されます。

レイヤ 2 EtherChannel にレイヤ 2 イーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。 PAgP EtherChannel の場合、同じタイプおよび同じ速度のポートを 8 個まで同じグループに設定できます。 LACP EtherChannel の場合は、同じタイプのイーサネット ポートを 16 個まで設定できます。最大 8 個のポートをアクティブにして、最大 8 個のポートをスタンバイ モードにすることができます。
ステップ 3	**switchport mode** {**access** | **trunk**} **switchport access vlan** *vlan-id*	すべてのポートをスタティック アクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティック アクセス ポートとして設定する場合は、ポートを 1 つの VLAN にだけ割り当ててください。指定できる範囲は 1 ～ 4094 です。

	コマンド	目的
ステップ 4	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}	ポートをチャネル グループに割り当て、PAgP または LACP モードを指定します。 *channel-group-number* に指定できる範囲は、1 ～ 6 です。 **mode** には、次に示すキーワードのいずれかを選択します。 • **auto**：PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 • **desirable**：PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。 • **on**：PAgP や LACP を使用せずに、ポートを強制的にチャネル化します。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）PAgP 対応のパートナーに接続されたスイッチのポートが **auto** または **desirable** モードの場合に、非サイレント動作を行うようにスイッチ ポートを設定します。**non-silent** を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザに接続する場合に使用します。この設定を使用すると、PAgP が動作するようになり、チャネル グループにポートを接続したり、ポートを伝送に使用したりできます。 • **active**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。 • **passive**：ポートで LACP をイネーブルにしてパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 スイッチおよびパートナーのモードの互換性については、「PAgP モード」（P.40-5）および「LACP モード」（P.40-6）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

EtherChannel グループからポートを削除するには、**no channel-group** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチ上で EtherChannel を設定する例を示します。2 つのポートを、VLAN 10 のスタティック アクセス ポートとして、PAgP モード **desirable** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

次に、スイッチ上で EtherChannel を設定する例を示します。2 つのポートを、VLAN 10 のスタティック アクセス ポートとして、LACP モード **active** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

レイヤ 3 EtherChannel の設定

レイヤ 3 EtherChannel を設定するには、ポートチャネル論理インターフェイスを作成し、そのポートチャネルにイーサネット ポートを組み込みます。次に設定方法を説明します。

ポートチャネル論理インターフェイスの作成

レイヤ 3 EtherChannel を設定する場合、まず **interface port-channel** グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成する必要があります。次に、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスをチャネル グループに配置します。

（注）　物理ポートから EtherChannel に IP アドレスを移動するには、物理ポートから IP アドレスを削除したあとで、その IP アドレスをポートチャネル インターフェイス上で設定する必要があります。

レイヤ 3 EtherChannel 用のポートチャネル インターフェイスを作成するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *port-channel-number*	ポートチャネル論理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 *port-channel-number* に指定できる範囲は、1 ～ 6 です。
ステップ 3	**no switchport**	インターフェイスをレイヤ 3 モードにします。
ステップ 4	**ip address** *ip-address mask*	EtherChannel に IP アドレスおよびサブネット マスクを割り当てます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show etherchannel** *channel-group-number* **detail**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。
ステップ 8		レイヤ 3 EtherChannel にイーサネット ポートを割り当てます。詳細については、「物理インターフェイスの設定」（P.40-15）を参照してください。

ポートチャネルを削除するには、**no interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用します。

次に、論理ポート チャネル 5 を作成し、IP アドレスとして 172.10.20.10 を割り当てる例を示します。

```
Switch# configure terminal
```

```
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

物理インターフェイスの設定

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。 PAgP EtherChannel の場合、同じタイプおよび同じ速度のポートを 8 個まで同じグループに設定できます。 LACP EtherChannel の場合は、同じタイプのイーサネット ポートを 16 個まで設定できます。最大 8 個のポートをアクティブにして、最大 8 個のポートをスタンバイ モードにすることができます。
ステップ 3	**no ip address**	この物理ポートに IP アドレスが割り当てられていないことを確認します。
ステップ 4	**no switchport**	ポートをレイヤ 3 モードにします。

	コマンド	目的
ステップ 5	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}	ポートをチャネル グループに割り当て、PAgP または LACP モードを指定します。 *channel-group-number* に指定できる範囲は、1 ～ 6 です。この番号は、「ポートチャネル論理インターフェイスの作成」（P.40-14）で設定された *port-channel-number*（論理ポート）と同じである必要があります。 **mode** には、次に示すキーワードのいずれかを選択します。 • **auto**：PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 • **desirable**：PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。 • **on**：PAgP や LACP を使用せずに、ポートを強制的にチャネル化します。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）PAgP 対応のパートナーに接続されたスイッチのポートが **auto** または **desirable** モードの場合に、非サイレント動作を行うようにスイッチ ポートを設定します。**non-silent** を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザに接続する場合に使用します。この設定を使用すると、PAgP が動作するようになり、チャネル グループにポートを接続したり、ポートを伝送に使用したりできます。 • **active**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。 • **passive**：ポートで LACP をイネーブルにしてパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 スイッチおよびパートナーのモードの互換性については、「PAgP モード」（P.40-5）および「LACP モード」（P.40-6）を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次の例では、EtherChannel を設定する方法を示します。2 つのポートを、LACP モード **active** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

EtherChannel ロード バランシングの設定

ここでは、送信元ベースまたは宛先ベースの転送方式を使用して、EtherChannel ロード バランシングを設定する方法について説明します。詳細については、「ロード バランシングおよび転送方式」（P.40-7）を参照してください。

EtherChannel ロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}	EtherChannel ロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次に示す負荷分散方式のいずれかを選択します。 • **dst-ip**：宛先ホストの IP アドレスに基づいた負荷分散。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスに基づいた負荷分散。 • **src-dst-ip**：送信元および宛先ホストの IP アドレスに基づいた負荷分散。 • **src-dst-mac**：送信元および宛先ホストの MAC アドレスに基づいた負荷分散。 • **src-ip**：送信元ホストの IP アドレスに基づいた負荷分散。 • **src-mac**：着信パケットの送信元の MAC アドレスに基づいた負荷分散。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show etherchannel load-balance**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

EtherChannel ロード バランシングをデフォルト設定に戻すには、**no port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

PAgP 学習方式およびプライオリティの設定

ネットワーク装置は PAgP の物理ラーナーまたは集約ポート ラーナーとして分類されます。物理ポートでアドレスを学習し、その知識に基づいて伝送を指示する装置が物理ラーナーです。集約（論理）ポートでアドレスを学習する装置は、集約ポート ラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

装置とそのパートナーが両方とも集約ポート ラーナーである場合、これらは論理ポートチャネルのアドレスを学習します。装置は、EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。集約ポート ラーニングの場合、どの物理ポートにパケットが届くかは重要でありません。

PAgP は、パートナー装置が物理ラーナーであるときと、ローカル装置が集約ポート ラーナーであるときを自動的に検出できません。したがって、物理ポートを使用してアドレスを学習する場合は、ローカル装置に手動で学習方式を設定する必要があります。負荷分散方式を送信元ベースに設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内にグループ内の未使用のポートに切り替えて動作させることができます。あるポートが常にパケット伝送に選択されるように設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注） CLI を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレス学習だけです。スイッチ ハードウェアでは、**pagp learn-method** コマンドおよび **pagp port-priority** コマンドは無効ですが、物理ポートによるアドレス学習だけをサポートする装置との PAgP の相互運用にはこれらのコマンドが必要です。

スイッチのリンク パートナーが物理ラーナー（Catalyst 1900 シリーズ スイッチなど）である場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して、IE 3000 スイッチを物理ポート ラーナーとして設定することを推奨します。送信元 MAC アドレスに基づく負荷分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。この設定により、スイッチは、送信元アドレスを学習したものと同じ EtherChannel 内のポートを使用して Catalyst 1900 へパケットを送信します。この状況に限り、**pagp learn-method** コマンドを使用します。

スイッチを PAgP 物理ポート ラーナーとして設定し、バンドル内の同じポートがパケット送信用として選択されるようにプライオリティを調整するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	伝送用のポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**pagp learn-method** physical-port	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port learning** が選択されています。つまり、スイッチは、EtherChannel 内のいずれかのポートを使用することによって、送信元にパケットを送信します。集約ポート ラーニングの場合、どの物理ポートにパケットが届くかは重要でありません。 物理ラーナーである別のスイッチに接続するには、**physical-port** を選択します。**port-channel load-balance** グローバル コンフィギュレーション コマンドは、必ず **src-mac** に設定してください（「EtherChannel ロード バランシングの設定」（P.40-17）を参照）。 学習方式は、リンクの両端で同一の設定にする必要があります。
ステップ 4	**pagp port-priority** *priority*	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* に指定できる範囲は 0 ～ 255 です。デフォルト値は 128 です。プライオリティが高いほど、そのポートが PAgP 伝送に使用される可能性が高まります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** または **show pagp** *channel-group-number* **internal**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

プライオリティをデフォルト設定に戻すには、**no pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。学習方式をデフォルト設定に戻すには、**no pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

LACP ホットスタンバイ ポートの設定

LACP がイネーブルの場合、チャネル内に最大数の LACP 対応ポートを設定しようとします（最大 16 ポート）。同時にアクティブにできる LACP リンクは 8 つだけです。それ以上のリンクはソフトウェアによってホットスタンバイ モードになります。アクティブ リンクの 1 つが非アクティブになると、代わりにホットスタンバイ モードになっているリンクがアクティブになります。

EtherChannel グループに 8 リンクより多く設定されている場合、LACP プライオリティに基づいてアクティブにするホットスタンバイ ポートがソフトウェアによって自動的に決定されます。ソフトウェアは LACP が動作するシステム間のリンクごとに、次の要素（プライオリティ順）からなる一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID（スイッチの MAC アドレス）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。ハードウェアの制限により互換性のあるすべてのポートを集約できない場合、プライオリティによって、スタンバイ モードにする必要があるポートが決定されます。

アクティブ ポートかホットスタンバイ ポートかを判別するには、次の（2 つの）手順を使用します。はじめに、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホットスタンバイ ポートを決定します。他のシステムのポートプライオリティとポート番号の値は使用されません。

LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更して、ソフトウェアによるアクティブおよびスタンバイ リンクの選択方法を変更できます。詳細については、「LACP システム プライオリティの設定」（P.40-20）および「LACP ポート プライオリティの設定」（P.40-20）を参照してください。

LACP システム プライオリティの設定

lacp system-priority グローバル コンフィギュレーション コマンドを使用して、LACP でイネーブルになっているすべての EtherChannel にシステム プライオリティを設定できます。各 LACP 設定チャネルにはシステム プライオリティを設定できません。この値をデフォルトから変更すると、ソフトウェアによるアクティブおよびスタンバイ リンクの選択方法を変更できます。

ホットスタンバイ モードにあるポート（H ポートステート フラグで表されます）を確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

LACP システム プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lacp system-priority** *priority*	LACP システム プライオリティを設定します。 *priority* に指定できる範囲は 1 ～ 65535 です。デフォルト値は 32768 です。 値が小さいほど、システム プライオリティは高くなります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** または **show lacp sys-id**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

LACP システム プライオリティをデフォルト値に戻すには、**no lacp system-priority** グローバル コンフィギュレーション コマンドを使用します。

LACP ポート プライオリティの設定

デフォルトでは、すべてのポートは同じポート プライオリティに設定されています。ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。ポート番号が小さなホットスタンバイ ポートほど、先にチャネル内でアクティブになります。ホットスタンバイ モードにあるポート（*H* ポートステート フラグで表されます）を確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

（注）　互換性のあるすべてのポートを LACP が集約できない場合（たとえば、リモート システムのハードウェア制限が厳しい場合）、EtherChannel にアクティブに追加できないすべてのポートはホットスタンバイ ステートになり、チャネル ポートのいずれかに障害が発生した場合に限り使用されます。

LACP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**lacp port-priority** ***priority***	LACP ポート プライオリティを設定します。 *priority* に指定できる範囲は 1 ～ 65535 です。デフォルト値は 32768 です。値が小さいほど、そのポートが LACP 伝送に使用される可能性が高まります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show lacp** [*channel-group-number*] **internal**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

LACP ポート プライオリティをデフォルト値に戻すには、**no lacp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel、PAgP、および LACP ステータスの表示

表 40-4　EtherChannel、PAgP、および LACP ステータスを表示するためのコマンド

コマンド	説明
show etherchannel [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}	EtherChannel 情報を簡潔、詳細に、1 行のサマリー形式で表示します。さらに、負荷分散方式またはフレーム配布方式、ポート、ポートチャネル、およびプロトコル情報も表示します。
show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 PAgP 設定、ネイバー情報などの PAgP 情報を表示します。
show pagp [*channel-group-number*] **dual-active**	デュアル アクティブ検出ステータスを表示します。
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報を表示します。

PAgP チャネルグループ情報およびトラフィック カウンタを消去するには、**clear pagp** {*channel-group-number* **counters** | **counters**} イネーブル EXEC コマンドを使用します。

LACP チャネルグループ情報およびトラフィック カウンタを消去するには、**clear lacp** {*channel-group-number* **counters** | **counters**} 特権 EXEC コマンドを使用します。

出力に表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

リンクステート トラッキングの概要

リンクステート トラッキングは、トランク フェールオーバーとも呼ばれ、複数のインターフェイスのリンク ステートをバインドする機能です。たとえば、リンクステート トラッキングをサーバ Network Interface Card（NIC; ネットワーク インターフェイス カード）アダプタ チーミング機能とともに使用すると、ネットワークの冗長性が実現されます。サーバ ネットワーク アダプタがチーミングと呼ばれるプライマリまたはセカンダリ関係で設定され、プライマリ インターフェイスでリンクが切断された場合、接続はセカンダリ インターフェイスにトランスペアレントに切り替えられます。

（注） ポートの集合（EtherChannel）、アクセス モードまたはトランク モードの単一の物理ポート、またはルーテッド ポートをインターフェイスに指定できます。

図 40-4（P.40-24）に、リンクステート トラッキングが設定されたネットワークを示します。リンクステート トラッキングをイネーブルにするには、*link-state group* を作成し、リンクステート グループに割り当てるインターフェイスを指定します。リンクステート グループでは、これらのインターフェイスはまとめてバンドルされます。*ダウンストリーム インターフェイス*は、*アップストリーム インターフェイス*にバインドされます。サーバに接続されたインターフェイスはダウンストリーム インターフェイスと呼ばれ、ディストリビューション スイッチおよびネットワーク装置に接続されたインターフェイスはアップストリーム インターフェイスと呼ばれます。

図 40-4 に示された設定では、ネットワーク トラフィック フローが次のようにバランシングされていることが確認できます。

- スイッチおよびその他のネットワーク装置へのリンク
  - サーバ 1 とサーバ 2 は、プライマリ リンクにスイッチ A を使用し、セカンダリ リンクにスイッチ B を使用しています。
  - サーバ 3 とサーバ 4 は、プライマリ リンクにスイッチ B を使用し、セカンダリ リンクにスイッチ A を使用しています。
- スイッチ A 上のリンクステート グループ 1
  - スイッチ A は、リンクステート グループ 1 を介してサーバ 1 とサーバ 2 にプライマリ リンクを提供します。ポート 1 はサーバ 1 に、ポート 2 はサーバ 2 に接続されます。ポート 1 およびポート 2 は、リンクステート グループ 1 のダウンストリーム インターフェイスです。
  - ポート 5 およびポート 6 は、リンクステート グループ 1 を介してディストリビューション スイッチ 1 に接続されます。ポート 5 およびポート 6 は、リンクステート グループ 1 のアップストリーム インターフェイスです。
- スイッチ A 上のリンクステート グループ 2
  - スイッチ A は、リンクステート グループ 2 を介してサーバ 3 とサーバ 4 にセカンダリ リンクを提供します。ポート 3 はサーバ 3 に、ポート 4 はサーバ 4 に接続されます。ポート 3 およびポート 4 は、リンクステート グループ 2 のダウンストリーム インターフェイスです。
  - ポート 7 およびポート 8 は、リンクステート グループ 2 を介してディストリビューション スイッチ 2 に接続されます。ポート 7 およびポート 8 は、リンクステート グループ 2 のアップストリーム インターフェイスです。

- スイッチ B 上のリンクステート グループ 2
  - スイッチ B は、リンクステート グループ 2 を介してサーバ 3 とサーバ 4 にプライマリ リンクを提供します。ポート 3 はサーバ 3 に、ポート 4 はサーバ 4 に接続されます。ポート 3 およびポート 4 は、リンクステート グループ 2 のダウンストリーム インターフェイスです。
  - ポート 5 およびポート 6 は、リンクステート グループ 2 を介してディストリビューション スイッチ 2 に接続されます。ポート 5 およびポート 6 は、リンクステート グループ 2 のアップストリーム インターフェイスです。
- スイッチ B 上のリンクステート グループ 1
  - スイッチ B は、リンクステート グループ 1 を介してサーバ 1 とサーバ 2 にセカンダリ リンクを提供します。ポート 1 はサーバ 1 に、ポート 2 はサーバ 2 に接続されます。ポート 1 およびポート 2 は、リンクステート グループ 1 のダウンストリーム インターフェイスです。
  - ポート 7 およびポート 8 は、リンクステート グループ 1 を介してディストリビューション スイッチ 1 に接続されます。ポート 7 およびポート 8 は、リンクステート グループ 1 のアップストリーム インターフェイスです。

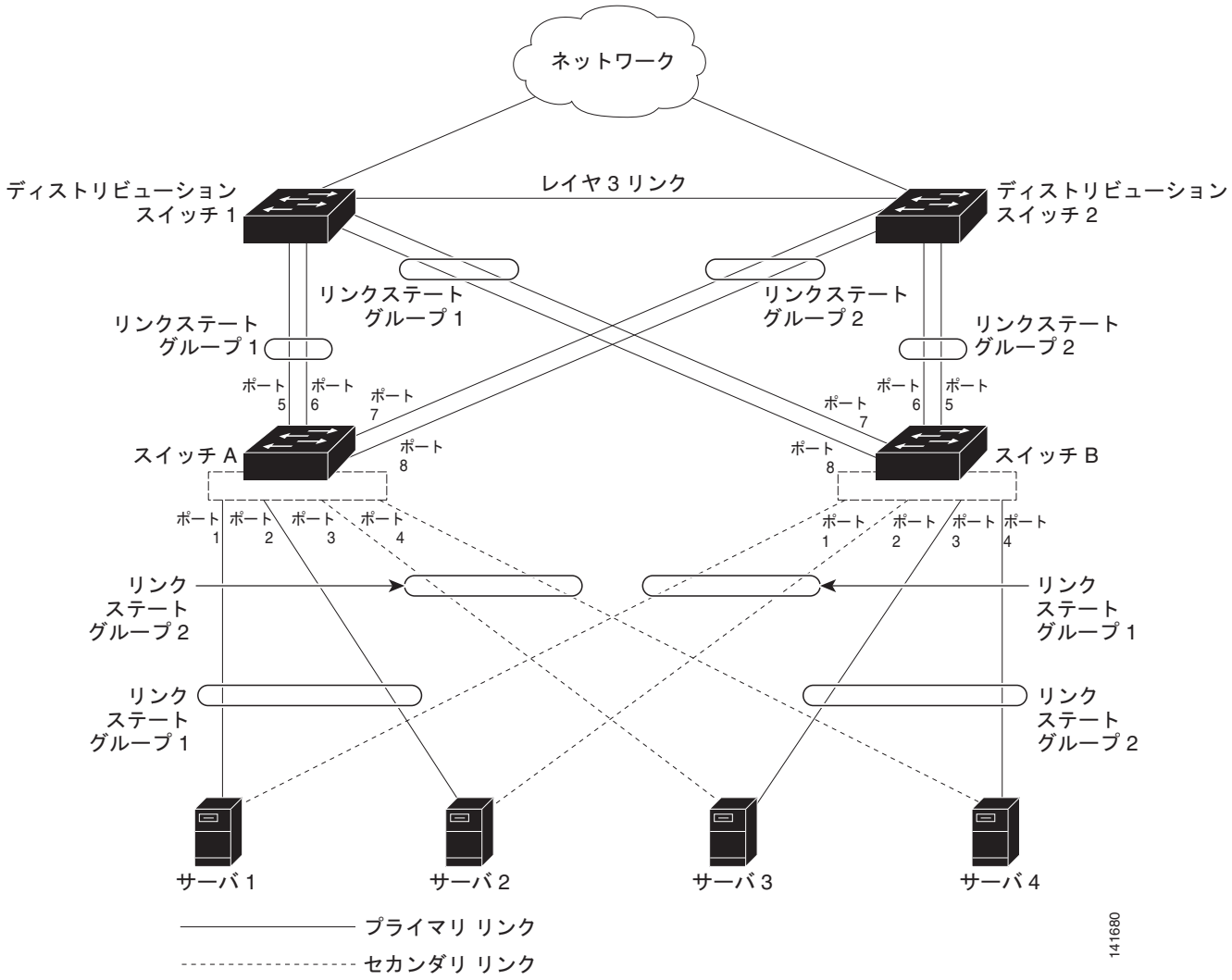
リンクステート グループでは、ディストリビューション スイッチまたはルータの障害、ケーブル切断、またはリンク損失のため、アップストリーム ポートが使用不可能になったり、接続が切断されたりする場合があります。リンクステート トラッキングがイネーブルである場合、ダウンストリーム インターフェイスとアップストリーム インターフェイス間は相互作用します。

- 任意のアップストリーム インターフェイスがリンクアップ ステートになった場合、ダウンストリーム インターフェイスもリンクアップ ステートに変更するか、またはリンクアップ ステートのまま維持されます。
- すべてのアップストリーム インターフェイスが使用不可能になると、ダウンストリーム インターフェイスは、リンクステート トラッキングにより自動的に errdisable ステートとなります。サーバとの間の接続は、プライマリ サーバ インターフェイスからセカンダリ サーバ インターフェイスに自動的に変更されます。

  スイッチ A でリンクステート グループ 1 からリンクステート グループ 2 への接続変更の例について、図 40-4（P.40-24）を参照してください。ポート 6 のアップストリーム リンクが切断されても、ダウンストリーム ポート 1 および 2 のリンク ステートは変わりません。ただし、アップストリーム ポート 5 のリンクも切断された場合、ダウンストリーム ポートのリンク ステートはリンクダウン ステートに変わります。次に、サーバ 1 およびサーバ 2 への接続が、リンクステート グループ 1 からリンクステート グループ 2 に変わります。ダウンストリーム ポート 3 および 4 は、リンク グループ 2 に存在するため、ステートの変更はありません。
- リンクステート グループが設定済みで、リンクステート トラッキングがディセーブルである場合は、アップストリーム インターフェイスで接続が切断されても、ダウンストリーム インターフェイスのリンク ステートは変わりません。サーバはアップストリームの接続が切断されたことを認識しないため、セカンダリ インターフェイスにフェールオーバーしません。

リンクステート グループから障害のあるダウンストリーム ポートを削除することにより、ダウンストリーム インターフェイスのリンクダウン状態から回復できます。複数のダウンストリーム インターフェイスを回復するには、リンクステート グループをディセーブルにします。

図 40-4　一般的なリンクステート トラッキングの設定



リンクステート トラッキングの設定

リンクステート トラッキングのデフォルト設定

リンクステート グループは定義されていません。また、リンクステート トラッキングはどのグループに対してもイネーブルではありません。

リンクステート トラッキング設定時の注意事項

設定上の問題を回避するために、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。
- ダウンストリーム Etherchannel インターフェイスの一部になる個別のインターフェイスでリンクステート トラッキングをイネーブルにしないでください。
- インターフェイスは、複数のリンクステート グループのメンバーにはなれません。
- スイッチごとに設定できるのは、2 個のリンクステート グループだけです。

リンクステート トラッキングの設定

リンクステート グループを設定し、そのグループにインターフェイスを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**link state track** *number*	リンクステート グループを作成し、リンクステート トラッキングをイネーブルにします。グループ番号は、1 ～ 2 です。デフォルトは 1 です。
ステップ 3	**interface** *interface-id*	設定する物理インターフェイスまたはインターフェイスの範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、アクセス モードまたはトランク モード（IEEE 802.1Q）のスイッチ ポート、ルーテッド ポート、アップストリーム EtherChannel インターフェイス（スタティック、PAgP、または LACP）にバンドルされている複数のポート（トランク モード）が含まれます。 **（注）** ダウンストリーム Etherchannel インターフェイスの一部になる個別のインターフェイスでリンクステート トラッキングをイネーブルにしないでください。
ステップ 4	**link state group** [*number*] {**upstream** | **downstream**}	リンクステート グループを指定し、グループ内の**アップストリーム**または**ダウンストリーム** インターフェイスとしてインターフェイスを設定します。グループ番号は、1 ～ 2 です。デフォルトは 1 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、リンクステート グループを作成し、インターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet1/1
```

```
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/2
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

リンクステート グループをディセーブルにするには、**no link state track** *number* グローバル コンフィギュレーション コマンドを使用します。

リンクステート トラッキング ステータスの表示

リンクステート グループ情報を表示するには、**show link state group** コマンドを使用します。キーワードを指定しないでこのコマンドを使用すると、すべてのリンクステート グループの情報が表示されます。特定のグループの情報を表示するには、グループ番号を入力します。グループの詳細情報を表示するには、detail キーワードを使用します。

次の例では、**show link state group 1** コマンドの出力を示します。

```
Switch> show link state group 1

Link State Group: 1      Status: Enabled, Down
```

次の例では、**show link state group detail** コマンドの出力を示します。

```
Switch> show link state group detail

(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Fa1/7(Dwn) Fa1/8(Dwn)
Downstream Interfaces : Fa1/3(Dis) Fa1/4(Dis) Fa1/5(Dis) Fa1/6(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Fa1/6(Dwn) Fa1/7(Dwn) Fa1/8(Dwn)
Downstream Interfaces : Fa1/2(Dis) Fa1/3(Dis) Fa1/4(Dis) Fa1/5(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

出力に表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 41

IP ユニキャスト ルーティングの設定

この章では、IE 3000 スイッチに IP バージョン 4（IPv4）ユニキャスト ルーティングを設定する方法について説明します。ルーティングをイネーブルにするには、スイッチが IP サービス イメージを実行している必要があります。

（注） スイッチが IP サービス イメージを実行している場合、IP バージョン 6（IPv6）ユニキャスト ルーティングもイネーブルにして、IPv4 トラフィックに加えて IPv6 トラフィックを転送するようにインターフェイスを設定できます。スイッチの IPv6 の設定の詳細については、第 42 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

IP ユニキャスト設定情報の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。この章で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] で、次のコマンド リファレンスを参照してください。

- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』
- 『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』
- 『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』

この章で説明する内容は、次のとおりです。

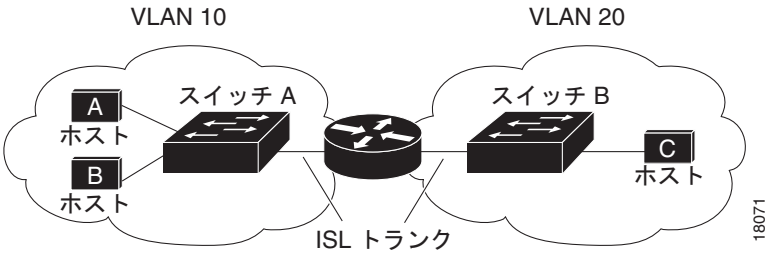
（注）　スイッチにルーティング パラメータを設定する場合、使用できるユニキャスト ルート数が最大となるようにシステム リソースを割り当てるには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用すると、Switch Database Management（SDM）機能をルーティング テンプレートに設定できます。SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」またはこのリリースのコマンド リファレンスで **sdm prefer** コマンドを参照してください。

IP ルーティングの概要

一部のネットワーク環境では、VLAN は個別のネットワークまたはサブネットワークに関連付けられています。IP ネットワークでは、各サブネットワークは個々の VLAN にマッピングされます。VLAN を設定すると、ブロードキャスト ドメインのサイズを制御し、ローカル トラフィックをローカルのまま維持できます。ただし、異なる VLAN でのネットワーク装置が相互に通信するには、VLAN 間のトラフィックをルーティング（VLAN 間ルーティング）するためにレイヤ 3 装置（ルータ）を使用する必要があります。トラフィックを該当する宛先 VLAN にルーティングするように、1 つまたは複数のルータを設定します。

図 41-1 に、基本的なルーティング トポロジを示します。スイッチ A は VLAN 10 内に、スイッチ B は VLAN 20 内にあります。ルータには、各 VLAN のインターフェイスが備わっています。

図 41-1　　ルーティング トポロジの例



VLAN 10 内のホスト A が VLAN 10 内 のホスト B と通信する必要がある場合、ホスト A はホスト B を宛先とするパケットを送信します。スイッチ A は、パケットをルータに送信せずに、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでトラフィックを受信します。ルータはルーティング テーブルをチェックし、適切な発信インターフェイスを検索し、VLAN 20 インターフェイスのパケットをスイッチ B に転送します。スイッチ B はパケットを受信し、ホスト C に転送します。

ルーティングのタイプ

ルータおよびレイヤ 3 スイッチは、次の 3 つの方法でパケットをルーティングできます。

- デフォルト ルーティング
- 事前にプログラムされているトラフィックのスタティック ルート
- ルーティング プロトコルによるルートのダイナミックな計算

デフォルト ルーティングとは、宛先がルータにとって不明であるトラフィックをデフォルトの出口または宛先に送信することです。

スタティック ユニキャスト ルーティングでは、パケットは事前に設定されたポートから単一のパスを通り、ネットワークの内部および外部に転送されます。スタティック ルーティングは、安全であり、帯域幅もほとんど使用しませんが、リンク障害などのネットワークの変更には自動的に対応しないため、パケットが宛先に到達しないことがあります。ネットワークが拡大するにつれ、スタティック ルーティングの設定は煩雑になります。

ルータでは、トラフィックを転送する最適ルートをダイナミックに計算するために、ダイナミック ルーティング プロトコルが使用されます。ダイナミック ルーティング プロトコルには、次の 2 種類があります。

- ディスタンスベクトル プロトコルを使用するルータでは、ネットワーク リソースの距離の値を使用してルーティング テーブルを維持し、これらのテーブルをネイバーに定期的に渡します。ディスタンスベクトル プロトコルは、1 つまたは複数のメトリックを使用し、最適ルートを計算します。これらのプロトコルは簡単に設定および使用できます。
- リンクステート プロトコルを使用するルータでは、ルータ間の Link-State Advertisement（LSA; リンクステート アドバタイズ）の交換に基づいて、ネットワーク トポロジの複雑なデータベースを維持します。LSA はネットワークのイベントがきっかけで発生し、コンバージェンスに要する時間やこれらの変更への対応に必要な時間を短縮します。リンクステート プロトコルは、トポロジの変更にすばやく対応しますが、ディスタンスベクトル プロトコルよりも多くの帯域幅とリソースが必要になります。

スイッチでサポートされるディスタンスベクトル プロトコルは、Routing Information Protocol（RIP）と Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）です。RIP は単一の距離メトリック（コスト）を使用して最適なパスを決定し、BGP はパス ベクトル メカニズムを追加します。また、Open Shortest Path First（OSPF）リンクステート プロトコル、および従来の Interior Gateway Routing Protocol（IGRP）にリンクステート ルーティング機能の一部を追加して効率化を図った拡張 IGRP（EIGRP）もサポートされます。

ルーティングを設定する手順

デフォルトでは、スイッチ上で IP ルーティングがディセーブルになっています。ルーティングを行う前に IP ルーティングをイネーブルにする必要があります。IP ルーティングの設定情報の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。

次の手順では、次のいずれかのレイヤ 3 インターフェイスを指定する必要があります。

- ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 3 ポートとして設定された物理ポートです。
- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）：**interface vlan** *vlan_id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。デフォルトでは、レイヤ 3 インターフェイスです。
- レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイスです。詳細については、「レイヤ 3 EtherChannel の設定」（P.40-14）を参照してください。

（注）　スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。

ルーティングが発生するすべてのレイヤ 3 インターフェイスに、IP アドレスを割り当てる必要があります。「ネットワーク インターフェイスへの IP アドレスの割り当て」（P.41-5）を参照してください。

（注）　レイヤ 3 スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。ユーザが設定可能なルーテッド ポートおよび SVI の数は、ソフトウェアによって制限されません。ただし、ハードウェアの制限により、この数と、実装された機能の組み合わせとの関係が、CPU 使用率に影響を与える可能性があります。システム メモリをルーティング用に最適化するには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用します。

ルーティングを設定するための主な手順は次のとおりです。

- VLAN インターフェイスをサポートするには、スイッチで VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てます。詳細については、第 16 章「VLAN の設定」を参照してください。
- レイヤ 3 インターフェイスを設定します。
- スイッチ上で IP ルーティングをイネーブルにします。
- レイヤ 3 インターフェイスに IP アドレスを割り当てます。
- 選択したルーティング プロトコルをスイッチ上でイネーブルにします。
- ルーティング プロトコル パラメータを設定します（任意）。

IP アドレッシングの設定

IP ルーティングを設定するには、レイヤ 3 インターフェイスに IP アドレスを割り当ててインターフェイスをイネーブルにし、IP を使用するインターフェイスを経由してホストとの通信を許可する必要があります。ここでは、さまざまな IP アドレッシング機能の設定手順について説明します。IP アドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

アドレッシングのデフォルト設定

表 41-1 に、アドレッシングのデフォルト設定を示します。

表 41-1　アドレッシングのデフォルト設定

機能	デフォルト設定
IP アドレス	定義なし。
ARP（アドレス解決プロトコル）	Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュに相手先固定エントリはありません。 カプセル化：標準のイーサネット形式の ARP。 タイムアウト：14400 秒（4 時間）。

表 41-1　アドレッシングのデフォルト設定 （続き）

機能	デフォルト設定
IP ブロードキャスト アドレス	255.255.255.255（すべて 1）。
IP クラスレス ルーティング	イネーブル。
IP デフォルト ゲートウェイ	ディセーブル。
IP ダイレクト ブロードキャスト	ディセーブル(すべての IP ダイレクト ブロードキャストは廃棄されます)。
IP ドメイン	ドメイン リスト：ドメイン名は定義されていません。 ドメイン検索：イネーブル。 ドメイン名：イネーブル。
IP 転送プロトコル	ヘルパー アドレスが定義されているか、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）フラッディングが設定されている場合、デフォルト ポートでは UDP 転送がイネーブルになります。 ローカル ブロードキャスト：ディセーブル Spanning Tree Protocol（STP; スパニング ツリー プロトコル）：ディセーブル ターボフラッディング：ディセーブル
IP ヘルパー アドレス	ディセーブル。
IP ホスト	ディセーブル。
IRDP	ディセーブル。 イネーブルの場合のデフォルト： • ブロードキャスト IRDP アドバタイズ • アドバタイズ間の最大インターバル：600 秒 • アドバタイズ間の最小インターバル：最大インターバルの 0.75 倍 • プリファレンス：0
IP プロキシ ARP	イネーブル。
IP ルーティング	ディセーブル。
IP サブネットゼロ	ディセーブル。

ネットワーク インターフェイスへの IP アドレスの割り当て

IP アドレスは、IP パケットの送信先を特定します。一部の IP アドレスは、特殊な用途のために予約されていて、ホスト、サブネット、またはネットワーク アドレスには使用できません。RFC 1166「Internet Numbers」に、IP アドレスに関する公式な説明が掲載されています。

インターフェイスには、1 つのプライマリ IP アドレスを指定できます。マスクは、IP アドレスのネットワーク番号を表すビットを特定します。マスクを使用してネットワークをサブネット化する場合、そのマスクをサブネット マスクと呼びます。割り当てられているネットワーク番号については、インターネット サービス プロバイダーにお問い合わせください。

IP アドレスおよびネットワーク マスクをレイヤ 3 インターフェイスに割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 5	**no shutdown**	インターフェイスをイネーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **show ip interface** [*interface-id*] **show running-config interface** [*interface-id*]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

サブネット ゼロの使用

サブネット アドレスがゼロであるサブネットを作成しないでください。同じアドレスを持つネットワークおよびサブネットがある場合に問題が発生することがあります。たとえば、ネットワーク 131.108.0.0 のサブネットが 255.255.255.0 の場合、サブネット ゼロは 131.108.0.0 と記述され、ネットワーク アドレスと同じとなってしまいます。

すべてが 1 のサブネット（131.108.255.0）を使用できます。また、IP アドレス用にサブネット スペース全体が必要な場合は、サブネット ゼロの使用をイネーブルにできます（ただし、推奨しません）。

サブネット ゼロをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip subnet-zero**	インターフェイス アドレスおよびルーティング アップデートにサブネット ゼロの使用をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトに戻して、サブネット ゼロの使用をディセーブルにするには、**no ip subnet-zero** グローバル コンフィギュレーション コマンドを使用します。

クラスレス ルーティング

デフォルトでは、ルーティングするように設定されたスイッチで、クラスレス ルーティング動作はイネーブルになっています。クラスレス ルーティングがイネーブルの場合、デフォルト ルートがないネットワークのサブネット宛てパケットをルータが受信すると、ルータは最適なスーパーネット ルートにパケットを転送します。*スーパーネット*は、単一の大規模アドレス スペースをシミュレートするために使用されるクラス C アドレス空間の連続ブロックで構成されています。スーパーネットは、クラス B アドレス空間の急速な枯渇を回避するように設計されています。

図 41-2 では、クラスレス ルーティングがイネーブルになっています。ホストがパケットを 128.20.4.1 に送信すると、ルータはパケットを廃棄せずに、最適なスーパーネット ルートに転送します。クラスレス ルーティングがディセーブルの場合、デフォルト ルートがないネットワークのサブネット宛てパケットをルータが受信すると、ルータはパケットを廃棄します。

図 41-2　IP クラスレス ルーティングがイネーブルの場合

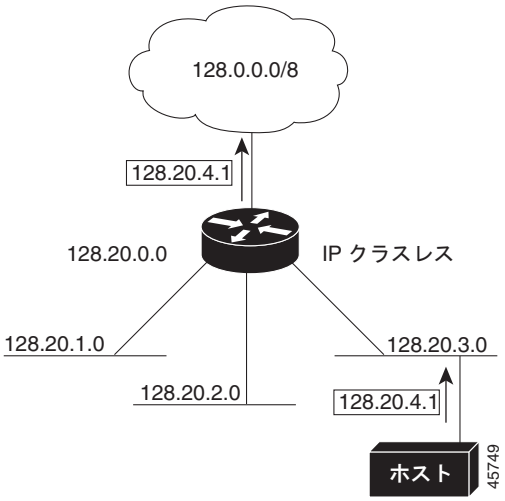
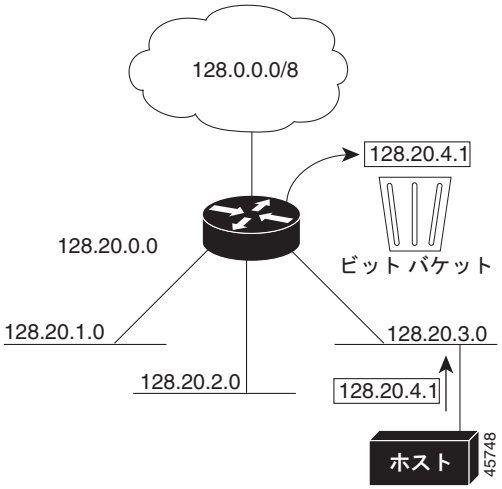


図 41-3 では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、および 128.20.3.0 に接続されています。ホストがパケットを 128.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 41-3　IP クラスレス ルーティングがディセーブルの場合



認識不能なサブネット宛てのパケットが最適なスーパーネット ルートに転送されないようにするには、クラスレス ルーティング動作をディセーブルにします。

クラスレス ルーティングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ip classless**	クラスレス ルーティング動作をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトに戻して、デフォルト ルートがないネットワークのサブネット宛てのパケットが最適なスーパーネット ルートに転送されるようにするには、**ip classless** グローバル コンフィギュレーション コマンドを使用します。

アドレス解決方法の設定

インターフェイス固有の IP 処理方法を制御するには、アドレス解決を使用します。IP を使用する装置は、ローカル セグメントまたは LAN 上の装置を一意に定義するローカル アドレス（MAC アドレス）と、装置が属するネットワークを特定するネットワーク アドレスがあります。

ローカル アドレス（MAC アドレス）は、パケット ヘッダーのデータ リンク層（レイヤ 2）セクションに格納されて、データ リンク（レイヤ 2）装置によって読み取られるため、データ リンク アドレスと呼ばれます。ソフトウェアがイーサネット上の装置と通信するために、装置の MAC アドレスを学習する必要があります。IP アドレスから MAC アドレスを判別するプロセスを、*アドレス解決*と呼びます。MAC アドレスから IP アドレスを学習するプロセスは、*逆アドレス解決*と呼ばれます。

スイッチでは、次の形式のアドレス解決を行うことができます。

- アドレス解決プロトコル（ARP）は、IP アドレスを MAC アドレスと関連付けるために使用されます。ARP は IP アドレスを入力と解釈し、関連付けられた MAC アドレスを学習します。次に、IP アドレスと MAC アドレスの関連付けを ARP キャッシュに保存され、すぐに取得できます。次に、IP データグラムがリンクレイヤ フレームにカプセル化され、ネットワーク上で送信されます。イーサネット以外の IEEE 802 ネットワークでの IP データグラムまたは ARP 要求および応答のカプセル化は、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）で指定されます。
- プロキシ ARP は、ルーティング テーブルを持たないホストで、他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにします。スイッチ（ルータ）が送信元と異なるインターフェイス上のホストに宛てた ARP 要求を受信した場合、そのルータに他のインターフェイスを経由してそのホストに至るすべてのルートが格納されていれば、ルータは自身のローカル データリンク アドレスを示すプロキシ ARP パケットを生成します。ARP 要求を送信したホストはルータにパケットを送信し、ルータはパケットを目的のホストに転送します。

スイッチでは、ARP と同様の機能である Reverse Address Resolution Protocol（RARP; 逆アドレス解決プロトコル）も使用できます（RARP パケットがローカル MAC アドレスでなく IP アドレスを要求する点を除く）。RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメントに RARP サーバを設置する必要があります。サーバを識別するには、**ip rarp-server** *address* インターフェイス コンフィギュレーション コマンドを使用します。

RARP の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*』を参照してください。

アドレス解決を設定するには、次の作業を実行します。

- 「スタティック ARP キャッシュの定義」（P.41-9）
- 「ARP カプセル化の設定」（P.41-10）
- 「プロキシ ARP のイネーブル化」（P.41-10）

スタティック ARP キャッシュの定義

ARP および他のアドレス解決プロトコルを使用すると、IP アドレスと MAC アドレス間をダイナミックにマッピングできます。ほとんどのホストではダイナミック アドレス解決がサポートされているため、通常はスタティック ARP キャッシュ エントリを指定する必要はありません。スタティック ARP キャッシュ エントリを定義する必要がある場合は、グローバルに定義できます。グローバルに定義すると、IP アドレスを MAC アドレスに変換するために使用される相手先固定エントリを、ARP キャッシュに確保できます。任意で、指定の IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定することもできます。ARP エントリを相手先固定エントリにしない場合は、ARP エントリのタイムアウト時間を指定できます。

IP アドレスと MAC アドレス間をスタティックにマッピングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**arp** *ip-address hardware-address type*	ARP キャッシュ内で IP アドレスを MAC（ハードウェア）アドレスにグローバルに関連付け、次に示すカプセル化タイプのいずれかを指定します。 • **arpa**：ARP カプセル化（イーサネット インターフェイス用） • **snap**：Subnetwork Address Protocol カプセル化（トークン リングおよび Fiber Distributed Data Interface（FDDI; ファイバ分散データ インターフェイス）用） • **sap**：HP の ARP タイプ
ステップ 3	**arp** *ip-address hardware-address type* [*alias*]	（任意）指定の IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定します。
ステップ 4	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 5	**arp timeout** *seconds*	（任意）ARP キャッシュ エントリがキャッシュに保持される時間を設定します。デフォルト値は 14400 秒（4 時間）です。指定できる範囲は 0 ～ 2147483 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*]	すべてのインターフェイスまたは特定のインターフェイスで使用される ARP のタイプおよびタイムアウト値を確認します。
ステップ 8	**show arp** または **show ip arp**	ARP キャッシュの内容を表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ARP キャッシュからエントリを削除するには、**no arp** *ip-address hardware-address type* グローバル コンフィギュレーション コマンドを使用します。ARP キャッシュからすべての非スタティック エントリを削除するには、**clear arp-cache** 特権 EXEC コマンドを使用します。

ARP カプセル化の設定

デフォルトでは、IP インターフェイスでイーサネット ARP 形式の ARP カプセル化（**arpa** キーワードで表される）はイネーブルになっています。ネットワークの必要性に応じて、カプセル化方式を SNAP に変更できます。

ARP カプセル化タイプを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**arp** {**arpa** | **snap**}	ARP カプセル化方式を指定します。 • **arpa**：アドレス解決プロトコル • **snap**：Subnetwork Address Protocol
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスの ARP カプセル化設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

カプセル化タイプをディセーブルにするには、**no arp arpa** または **no arp snap** インターフェイス コンフィギュレーション コマンドを使用します。

プロキシ ARP のイネーブル化

デフォルトでは、スイッチはプロキシ ARP を使用します。ホストが他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにするためです。

ディセーブル化されているプロキシ ARP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip proxy-arp**	インターフェイスでプロキシ ARP をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip interface** [*interface-id*]	特定のインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスでプロキシ ARP をディセーブルにするには、**no ip proxy-arp** インターフェイス コンフィギュレーション コマンドを使用します。

IP ルーティングがディセーブルの場合のルーティング支援機能

次のメカニズムを使用することで、スイッチは IP ルーティングがイネーブルでない場合、別のネットワークへのルートを学習できます。

- 「プロキシ ARP」（P.41-11）
- 「デフォルト ゲートウェイ」（P.41-11）
- 「ICMP Router Discovery Protocol（IRDP）」（P.41-12）

プロキシ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネット ホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。このホストでは、すべてのホストが同じローカル イーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定しています。スイッチが送信元と異なるネットワーク上のホストに宛てた ARP 要求を受信した場合、そのホストへの最適ルートがあるかどうかを調べます。最適ルートがある場合、スイッチはスイッチ自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信します。要求を送信したホストはスイッチにパケットを送信し、スイッチはパケットを目的のホストに転送します。プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 要求を実行します。

プロキシ ARP はデフォルトでイネーブルになっています。プロキシ ARP をディセーブルにしたあとにイネーブルにするには、「プロキシ ARP のイネーブル化」（P.41-10）を参照してください。プロキシ ARP は、他のルータでサポートされている限り有効です。

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法は、デフォルト ルータ、つまりデフォルト ゲートウェイを定義する方法です。ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行う、または Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）リダイレクト メッセージを返信するという方法で、ホストが使用するローカル ルータを定義します。スイッチはリダイレクト メッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送します。この方法には、デフォルト ルータがダウンした場合、または使用できなくなった場合に、検出が不可能となる制限があります。

IP ルーティングがディセーブルの場合にデフォルト ゲートウェイ（ルータ）を定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip default-gateway** *ip-address*	デフォルト ゲートウェイ（ルータ）を設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip redirects**	設定を確認するため、デフォルト ゲートウェイ ルータのアドレスを表示します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

この機能をディセーブルにするには、**no ip default-gateway** グローバル コンフィギュレーション コマンドを使用します。

ICMP Router Discovery Protocol（IRDP）

ルータ検出を使用すると、スイッチは IRDP を使用し、他のネットワークへのルートをダイナミックに学習します。ホストは IRDP を使用し、ルータを特定します。クライアントとして動作しているスイッチは、ルータ検出パケットを生成します。ホストとして動作しているスイッチは、ルータ検出パケットを受信します。スイッチは RIP ルーティングのアップデートを受信し、この情報からルータの場所を推測することもできます。実際には、ルーティング装置によって送信されたルーティング テーブルは、スイッチに格納されません。どのシステムがデータを送信しているのかが追跡されるだけです。IRDP を使用することの利点は、プライオリティと、パケットが受信されなくなってから装置がダウンしていると見なされるまでの時間を、ルータごとに両方指定できることです。

検出された各装置は、デフォルト ルータの候補となります。現在のデフォルト ルータがダウンしたと宣言された場合、または再送信が多すぎて Transmission Control Protocol（TCP; 伝送制御プロトコル）接続がタイムアウトになりつつある場合、プライオリティが上位のルータが検出されると、最も高いプライオリティを持つ新しいルータが選択されます。

インターフェイスで IRDP ルーティングを行う場合は、インターフェイスで IRDP 処理をイネーブルにしてください。IRDP 処理をイネーブルにすると、デフォルトのパラメータが適用されます。必要に応じて、これらのパラメータを変更できます。

インターフェイス上で IRDP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip irdp**	インターフェイスで IRDP 処理をイネーブルにします。
ステップ 4	**ip irdp multicast**	（任意）IP ブロードキャストの代わりとして、IRDP アドバタイズをマルチキャスト アドレス（224.0.0.1）に送信します。 **（注）** このコマンドを使用すると、IRDP パケットをマルチキャストとして送信するサン・マイクロシステムズ社の Solaris との互換性が維持できます。実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。
ステップ 5	**ip irdp holdtime** *seconds*	（任意）アドバタイズが有効である IRDP 期間を設定します。デフォルトは、**maxadvertinterval** 値の 3 倍です。**maxadvertinterval** 値よりも大きな値（9000 秒以下）を指定する必要があります。**maxadvertinterval** 値を変更すると、この値も変更されます。
ステップ 6	**ip irdp maxadvertinterval** *seconds*	（任意）アドバタイズ間の IRDP の最大インターバルを設定します。デフォルト値は 600 秒です。
ステップ 7	**ip irdp minadvertinterval** *seconds*	（任意）アドバタイズ間の IRDP の最小インターバルを設定します。デフォルトは、**maxadvertinterval** 値の 0.75 倍です。**maxadvertinterval** を変更すると、この値も新しいデフォルト値（**maxadvertinterval** の 0.75 倍）に変更されます。

	コマンド	目的
ステップ 8	**ip irdp preference** *number*	（任意）装置にプリファレンス レベルを設定します。指定できる範囲は -2^{31} ～ 2^{31} です。デフォルト値は 0 です。大きな値を設定すると、ルータのプリファレンス レベルも高くなります。
ステップ 9	**ip irdp address** *address* [*number*]	（任意）プロキシアドバタイズを行うために必要な IRDP アドレスとプリファレンスを指定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip irdp**	IRDP 値を表示し、設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

maxadvertinterval 値を変更すると、**holdtime** 値および **minadvertinterval** 値も変更されます。最初に **maxadvertinterval** 値を変更し、次に **holdtime** 値または **minadvertinterval** 値のいずれかを手動で変更することが重要です。

IRDP ルーティングをディセーブルにするには、**no ip irdp** インターフェイス コンフィギュレーション コマンドを使用します。

ブロードキャスト パケットの処理の設定

IP インターフェイス アドレスを設定したあとに、ルーティングをイネーブルにしたり、1 つまたは複数のルーティング プロトコルを設定したり、ネットワーク ブロードキャストへのスイッチの応答方法を設定できます。ブロードキャストは、物理ネットワーク上のすべてのホスト宛てのデータ パケットです。スイッチは次の 2 種類のブロードキャストをサポートします。

- ダイレクト ブロードキャスト パケット。特定のネットワークまたは一連のネットワークに送信されます。ダイレクト ブロードキャスト アドレスには、ネットワークまたはサブネット フィールドが含まれます。
- フラッディング ブロードキャスト パケット。すべてのネットワークに送信されます。

（注）　**storm-control** インターフェイス コンフィギュレーション コマンドを使用してトラフィック抑制レベルを設定し、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、およびマルチキャスト トラフィックを制限することもできます。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。

ルータはローカル ケーブル長を制限して、ブロードキャスト ストームを防ぎます。ブリッジ（インテリジェントなブリッジを含む）はレイヤ 2 装置であるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームが伝播します。ブロードキャスト ストームの問題を解決する最善の方法は、ネットワーク上で単一のブロードキャスト アドレス方式を使用することです。最新の IP 実装機能ではほとんどの場合、アドレスをブロードキャスト アドレスとして使用するように設定できます。スイッチ内の機能をはじめ、多数の実装機能では、ブロードキャスト メッセージを転送するためのアドレッシング方式が複数サポートされています。

ここでは、これらの方式をイネーブルにするために行う作業について説明します。

- 「ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化」（P.41-14）
- 「UDP ブロードキャスト パケットおよびプロトコルの転送」（P.41-15）
- 「IP ブロードキャスト アドレスの確立」（P.41-16）
- 「IP ブロードキャストのフラッディング」（P.41-16）

ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化

デフォルトでは、IP ダイレクト ブロードキャストは廃棄されるため、転送されることはありません。IP ダイレクト ブロードキャストが廃棄されると、ルータが DoS 攻撃にさらされる危険が少なくなります。

ブロードキャストが物理（MAC レイヤ）ブロードキャストになるインターフェイスでは、IP ダイレクト ブロードキャストの転送をイネーブルにできます。**ip forward-protocol** グローバル コンフィギュレーション コマンドを使用して設定されたプロトコルだけを転送できます。

転送するブロードキャストを制御するアクセス リストを指定できます。アクセス リストを指定すると、アクセス リストで許可された IP パケットだけをダイレクト ブロードキャストから物理ブロードキャストに変換できるようになります。アクセス リストの詳細については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。

インターフェイス上で IP ダイレクト ブロードキャストの転送をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ip directed-broadcast** [*access-list-number*]	インターフェイスでダイレクト ブロードキャストから物理ブロードキャストへの変換をイネーブルにします。転送するブロードキャストを制御するアクセス リストを指定できます。アクセス リストを指定すると、アクセス リストで許可された IP パケットだけを変換できます。 **（注）** **ip directed-broadcast** インターフェイス コンフィギュレーション コマンドは Virtual Private Network（VPN; 仮想私設網）Routing/Forwarding（VRF; VPN ルーティング / 転送）で設定でき、こうすると VRF 認識になります。ダイレクト ブロードキャスト トラフィックが VRF 内だけでルーティングされます。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルとポートを指定します。 • **udp**：User Datagram Protocol（UDP; ユーザ データグラム プロトコル）データグラムを転送します。 *port*：（任意）転送される UDP サービスを制御する宛先ポートです。 • **nd**：Network Disk（ND）データグラムを転送します。 • **sdns**：SDNS データグラムを転送します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip interface** [*interface-id*] または **show running-config**	特定のインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ダイレクト ブロードキャストから物理ブロードキャストへの変換をディセーブルにするには、**no ip directed-broadcast** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

UDP ブロードキャスト パケットおよびプロトコルの転送

ユーザ データグラム プロトコル（UDP）は、IP のホスト間レイヤ プロトコルで、TCP と同様です。UDP はオーバーヘッドが少ない、コネクションレス型セッションを 2 つのエンド システム間に提供しますが、受信されたデータグラムの確認応答は行いません。場合に応じてネットワーク ホストは UDP ブロードキャストを使用し、アドレス、コンフィギュレーション、および名前に関する情報を判別します。このようなホストが、サーバを含まないネットワーク セグメント上にある場合、通常 UDP ブロードキャストは転送されません。このような状況を修復するには、特定のクラスのブロードキャストをヘルパー アドレスに転送するように、ルータのインターフェイスを設定します。インターフェイスごとに、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定して、転送される UDP サービスを制御できます。複数の UDP プロトコルを指定することもできます。旧式のディスクレス Sun ワークステーションおよびネットワーク セキュリティ プロトコル SDNS で使用される Network Disk（ND）プロトコルも指定できます。

デフォルトでは、ヘルパー アドレスがインターフェイスに定義されている場合、UDP と ND の両方の転送がイネーブルになっています。『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』に記載されている **ip forward-protocol** インターフェイス コンフィギュレーション コマンドの説明には、UDP ポートを指定しない場合のデフォルトで転送されるポートの一覧があります。

UDP ブロードキャストの転送を設定するときに UDP ポートを指定しないと、ルータは Bootstrap Protocol（BOOTP）転送エージェントとして動作するように設定されます。BOOTP パケットは Dynamic Host Configuration Protocol（DHCP）情報を伝送します。

インターフェイス上で UDP ブロードキャスト パケットの転送をイネーブルにし、宛先アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip helper-address** *address*	転送をイネーブルにし、BOOTP などの UDP ブロードキャスト パケットを転送するための宛先アドレスを指定します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip interface** [*interface-id*] または **show running-config**	特定のインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

特定のアドレスへのブロードキャスト パケットの転送をディセーブルにするには、**no ip helper-address** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

IP ブロードキャスト アドレスの確立

最も一般的な（デフォルトの）IP ブロードキャスト アドレスは、すべて 1 で構成されているアドレスです（255.255.255.255）。ただし、任意の形式の IP ブロードキャスト アドレスを生成するようにスイッチを設定することもできます。

インターフェイス上で IP ブロードキャスト アドレスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ip broadcast-address** *ip-address*	デフォルト値とは異なるブロードキャスト アドレス（128.1.255.255 など）を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip interface** [*interface-id*]	特定のインターフェイスまたはすべてのインターフェイスのブロードキャスト アドレスを確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの IP ブロードキャスト アドレスに戻すには、**no ip broadcast-address** インターフェイス コンフィギュレーション コマンドを使用します。

IP ブロードキャストのフラッディング

IP ブロードキャストをインターネットワーク全体に制御可能な方式でフラッディングできるようにするには、ブリッジング STP で作成されたデータベースを使用します。この機能を使用すると、ループも防止できます。この機能を使用できるようにするには、フラッディングが行われるインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイス上でも、ブロードキャストを受信できます。ただし、ブリッジングが設定されていないインターフェイスでは、受信したブロードキャストが転送されません。また、異なるインターフェイスで受信されたブロードキャストをルータで送信する場合、このインターフェイスは使用されません。

IP ヘルパーアドレスのメカニズムを使用して単一のネットワーク アドレスに転送されるパケットをフラッディングできます。各ネットワーク セグメントには、パケットのコピーが 1 つだけ送信されます。

フラッディングを行う場合、パケットは次の基準を満たす必要があります（これらの基準は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです）。

- パケットは MAC レベル ブロードキャストである必要があります。
- パケットは IP レベル ブロードキャストである必要があります。
- パケットは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、Domain Name System（DNS; ドメイン ネーム システム）、Time、Network Basic Input/Output System（NetBIOS）、ND、または BOOTP パケットであるか、**ip forward-protocol udp** グローバル コンフィギュレーション コマンドで指定された UDP である必要があります。

- パケットの Time To Live（TTL; 存続可能時間）値が 2 以上である必要があります。

フラッディングされた UDP データグラムには、出力インターフェイスで **ip broadcast-address** インターフェイス コンフィギュレーション コマンドによって指定された宛先アドレスを設定します。宛先アドレスは任意のアドレスに設定できます。このため、データグラムがネットワークを介して伝播するにつれ、宛先アドレスが変更される場合があります。送信元アドレスは変更されません。TTL 値は減少します。

フラッディングされた UDP データグラムがインターフェイスから送信されると（場合によっては宛先アドレスが変更される）、データグラムは通常の IP 出力ルーチンに渡されます。このため、出力インターフェイスにアクセス リストがある場合、データグラムはその影響を受けます。

ブリッジング スパニング ツリー データベースを使用して UDP データグラムをフラッディングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip forward-protocol spanning-tree**	ブリッジング スパニング ツリー データベースを使用して UDP データグラムをフラッディングします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IP ブロードキャストのフラッディングをディセーブルにするには、**no ip forward-protocol spanning-tree** グローバル コンフィギュレーション コマンドを使用します。

スイッチでは、パケットの大部分がハードウェアで転送され、スイッチの CPU を経由しません。CPU に送信されるパケットの場合は、ターボフラッディングを使用し、スパニング ツリーベースの UDP フラッディングを約 4 ～ 5 倍高速化します。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされます。

スパニング ツリーベースのフラッディングを向上させるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip forward-protocol turbo-flood**	スパニング ツリー データベースを使用して UDP データグラムのフラッディングを高速化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

この機能をディセーブルにするには、**no ip forward-protocol turbo-flood** グローバル コンフィギュレーション コマンドを使用します。

IP アドレッシングのモニタおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になる場合、または無効である疑いがある場合は、**clear** 特権 EXEC コマンドを使用してすべての内容を削除できます。表 41-2 に、内容を消去するコマンドを示します。

表 41-2　キャッシュ、テーブル、データベースの消去を行うコマンド

コマンド	目的
clear arp-cache	IP ARP キャッシュおよび高速スイッチング キャッシュを消去します。
clear host {*name* | *}}	ホスト名およびアドレス キャッシュから特定のエントリまたはすべてのエントリを削除します。
clear ip route {*network* [*mask*] |*}	IP ルーティング テーブルから 1 つまたは複数のルートを削除します。

IP ルーティング テーブル、キャッシュ、データベースの内容、ノードへの到達可能性、パケットがネットワーク上で通過するルーティング パスなど、特定の統計情報を表示できます。表 41-3 に、IP 統計情報を表示するために使用する特権 EXEC コマンドを示します。

表 41-3　キャッシュ、テーブル、データベースの表示を行うコマンド

コマンド	目的
show arp	ARP テーブルのエントリを表示します。
show hosts	デフォルトのドメイン名、検索サービスの方式、ネーム サーバ ホスト、およびキャッシュされたホスト名とアドレスのリストを表示します。
show ip aliases	TCP ポートにマッピングされた IP アドレスを表示します（エイリアス）。
show ip arp	IP ARP キャッシュを表示します。
show ip interface [*interface-id*]	インターフェイスの IP ステータスを表示します。
show ip irdp	IRDP 値を表示します。
show ip masks *address*	ネットワーク アドレスに対して使用されるマスク、および各マスクを使用するサブネット番号を表示します。
show ip redirects	デフォルト ゲートウェイのアドレスを表示します。
show ip route [*address* [*mask*]] | [*protocol*]	ルーティング テーブルの現在のステートを表示します。
show ip route summary	ルーティング テーブルの現在のステートをサマリー形式で表示します。

IP ユニキャスト ルーティングのイネーブル化

デフォルトでは、スイッチはレイヤ 2 スイッチング モード、IP ルーティングがディセーブルになっています。スイッチのレイヤ 3 機能を使用するには、IP ルーティングをイネーブルにする必要があります。

IP ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします。

	コマンド	目的
ステップ 3	**router** *ip_routing_protocol*	**（注）** IP ルーティング プロトコルを指定します。このステップでは、他のコマンド（ルーティングするネットワークを指定する **network**（RIP）ルータ コンフィギュレーション コマンドなど）を使用する場合があります。特定のプロトコルの詳細については、この章の後半および『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。

次に、ルーティング プロトコルとして RIP を使用し、IP ルーティングをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end
```

次の項で説明するように、ここで、選択したルーティング プロトコルのパラメータを設定できます。

- 「RIP の設定」（P.41-19）
- 「OSPF の設定」（P.41-25）
- 「EIGRP の設定」（P.41-34）
- 「BGP の設定」（P.41-42）
- 「プロトコル独立機能の設定」（P.41-89）（任意）

RIP の設定

Routing Information Protocol（RIP）は、小規模な同種ネットワークで使用するために作成された Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）です。RIP は、ブロードキャスト User Datagram Protocol（UDP）データ パケットを使用してルーティング情報を交換するディスタンス ベクトル ルーティング プロトコルです。このプロトコルについては、RFC 1058 で説明されています。RIP の詳細については、『*IP Routing Fundamentals*』（Cisco Press 刊）を参照してください。

スイッチは RIP を使用し、30 秒ごとにルーティング情報アップデート（アドバタイズ）を送信します。180 秒以上を経過しても別のルータからアップデートがルータに届かない場合、該当するルータから送られたルートは使用不能としてマーキングされます。240 秒が経過してもアップデートが届かない場合、アップデートを行わないルータに関するすべてのルーティング テーブル エントリは削除されます。

RIP では、各ルートの値を評価するためにホップ カウントが使用されます。ホップ カウントは、ルート内で経由されるルータの数です。直接接続されたネットワークのホップ カウントは 0 です。ホップ カウントが 16 のネットワークに到達することはできません。このように範囲（0 ～ 15）が狭いため、RIP は大規模なネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP はルータを疑似ネットワーク 0.0.0.0 にリンクするルートをアドバタイズします。0.0.0.0 ネットワークは存在しません。RIP はデフォルトのルーティング機能を実装するためのネットワークとして、このネットワークを処理します。

デフォルト ネットワークが RIP によって学習された場合、またはルータがラスト リゾート ゲートウェイで、RIP がデフォルト メトリックによって設定されている場合、スイッチはデフォルト ネットワークをアドバタイズします。RIP は、指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイスのネットワークを指定しないと、RIP アップデート中にアドバタイズされません。

ここでは、次の設定情報について説明します。

- 「RIP のデフォルト設定」（P.41-20）
- 「基本的な RIP パラメータの設定」（P.41-21）
- 「RIP 認証の設定」（P.41-22）
- 「サマリー アドレスおよびスプリット ホライズンの設定」（P.41-23）

RIP のデフォルト設定

表 41-4 に、RIP のデフォルト設定を示します。

表 41-4　RIP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。
デフォルト情報送信元	ディセーブル。
デフォルト メトリック	自動メトリック変換（組み込み）。
IP RIP 認証キー チェーン	認証なし。 認証モード：クリア テキスト。
IP RIP 受信バージョン	**version** ルータ コンフィギュレーション コマンドに準拠。
IP RIP 送信バージョン	**version** ルータ コンフィギュレーション コマンドに準拠。
IP RIP のトリガー	**version** ルータ コンフィギュレーション コマンドに準拠。
IP スプリット ホライズン	メディアにより異なる。
ネイバー	定義なし。
ネットワーク	指定なし。
オフセット リスト	ディセーブル。
出力遅延	0 ミリ秒。
タイマー基準	• update：30 秒。 • invalid：180 秒。 • holdown：180 秒。 • flush：240 秒。
アップデート送信元の検証	イネーブル。
バージョン	RIP バージョン 1 およびバージョン 2 のパケットを受信し、バージョン 1 のパケットを送信。

基本的な RIP パラメータの設定

RIP を設定するには、ネットワークに対して RIP ルーティングをイネーブルにします。他のパラメータを設定することもできます。IE 3000 スイッチでは、ネットワーク番号を設定するまで RIP コンフィギュレーション コマンドは無視されます。

RIP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします（IP ルーティングがディセーブルになっている場合だけ必須）。
ステップ 3	**router rip**	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**network** *network number*	ネットワークを RIP ルーティング プロセスに関連付けます。複数の **network** コマンドを指定できます。RIP ルーティング アップデートの送受信は、これらのネットワークのインターフェイスを経由する場合だけ可能です。 **（注）** RIP コマンドを有効にするには、ネットワーク番号を設定する必要があります。
ステップ 5	**neighbor** *ip-address*	（任意）ルーティング情報を交換するネイバー ルータを定義します。このステップを使用すると、RIP（通常はブロードキャスト プロトコル）からのルーティング アップデートが非ブロードキャスト ネットワークに到達するようになります。
ステップ 6	**offset list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*]	（任意）オフセット リストをルーティング メトリックに適用して、RIP によって学習したルートへの着信および発信メトリックを増加させます。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 7	**timers basic** *update invalid holddown flush*	（任意）ルーティング プロトコル タイマーを調整します。すべてのタイマーの有効範囲は 0 ～ 4294967295 秒です。 • *update*：ルーティング アップデートの送信間隔。デフォルト値は 30 秒です。 • *invalid*：ルートが無効と宣言されたあとの時間。デフォルト値は 180 秒です。 • *holddown*：ルートがルーティング テーブルから削除されるまでの時間。デフォルト値は 180 秒です。 • *flush*：ルーティング アップデートが延期される時間。デフォルト値は 240 秒です。
ステップ 8	**version** {**1** | **2**}	（任意）RIP バージョン 1 または バージョン 2 のパケットだけを送受信するようにスイッチを設定します。デフォルトでは、スイッチはバージョン 1 およびバージョン 2 を受信しますが、送信するのはバージョン 1 だけです。 インターフェイス コマンド **ip rip** {**send** | **receive**} **version 1** | **2** | **1 2**} を使用して、インターフェイスでの送受信に使用するバージョンを制御することもできます。

	コマンド	目的
ステップ 9	**no auto summary**	（任意）自動サマライズをディセーブルにします。デフォルトでは、クラスフル ネットワーク境界を通過するときにサブプレフィクスがサマライズされます。サマライズをディセーブルにして（RIP バージョン 2 だけ）、クラスフル ネットワーク境界にサブネットおよびホスト ルーティング情報をアドバタイズします。
ステップ 10	**no validate-update-source**	（任意）着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチは着信 RIP ルーティング アップデートの送信元 IP アドレスを検証し、送信元 IP アドレスが有効でない場合はアップデートを廃棄します。通常の環境では、この機能をディセーブルにすることは推奨しません。ただし、ネットワークに接続されていないルータがあり、そのルータのアップデートを受信する場合は、このコマンドを使用できます。
ステップ 11	**output-delay** *delay*	（任意）送信される RIP アップデートのインターパケット遅延を追加します。 デフォルトでは、複数のパケットからなる RIP アップデートのパケットに、インターパケット遅延を追加することはできません。パケットを低速な装置に送信する場合は、8 ～ 50 ミリ秒のインターパケット遅延を追加できます。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip protocols**	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

RIP ルーティング プロセスをオフにするには、**no router rip** グローバル コンフィギュレーション コマンドを使用します。

アクティブなルーティング プロトコル プロセスのパラメータおよび現在のステートを表示するには、**show ip protocols** 特権 EXEC コマンドを使用します。RIP データベースのサマリー アドレス エントリを表示するには、**show ip rip database** 特権 EXEC コマンドを使用します。

RIP 認証の設定

RIP バージョン 1 は認証をサポートしません。RIP バージョン 2 のパケットを送受信する場合は、インターフェイスでの RIP 認証をイネーブルにできます。インターフェイスで使用できる一連のキーは、キー チェーンによって指定されます。キー チェーンが設定されていないと、デフォルトの場合でも認証は実行されません。このため、「認証キーの管理」（P.41-104）に記載されている作業も実行してください。

RIP 認証がイネーブルであるインターフェイスでは、プレーン テキストと MD5 という 2 つの認証モードがスイッチでサポートされます。デフォルトはプレーン テキストです。

インターフェイス上で RIP 認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ip rip authentication key-chain** *name-of-chain*	RIP 認証をイネーブルにします。

	コマンド	目的
ステップ 4	**ip rip authentication mode** [**text** | **md5**}	プレーン テキスト認証（デフォルト）または MD5 ダイジェスト認証を使用するようにインターフェイスを設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

クリア テキスト認証に戻すには、**no ip rip authentication mode** インターフェイス コンフィギュレーション コマンドを使用します。認証を禁止するには、**no ip rip authentication key-chain** インターフェイス コンフィギュレーション コマンドを使用します。

サマリー アドレスおよびスプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるためにスプリットホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報がその情報の送信元のインターフェイスで、ルータによってアドバタイズされないようにします。この機能を使用すると、複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

（注）　ルートを適切にアドバタイズするために、スプリット ホライズンをディセーブルにすることがアプリケーションに必要である場合を除き、一般的にこの機能をディセーブルにすることは推奨しません。

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカル IP アドレス プールをアドバタイズするように、RIP が動作しているインターフェイスを設定する場合は、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドを使用します。

（注）　スプリット ホライズンがイネーブルの場合、自動サマリーとインターフェイス IP サマリーはともにアドバタイズされません。

サマライズされたローカル IP アドレスをアドバタイズし、インターフェイスでスプリット ホライズンをディセーブルにするようにインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネットを設定します。
ステップ 4	**ip summary-address rip** *ip address ip-network mask*	サマライズする IP アドレスおよび IP ネットワーク マスクを設定します。
ステップ 5	**no ip split horizon**	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show ip interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IP サマライズをディセーブルにするには、**no ip summary-address rip** ルータ コンフィギュレーション コマンドを使用します。

次の例では、主要ネットは 10.0.0.0 です。自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイス ギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。この例で、インターフェイスがまだレイヤ 2 モード（デフォルト）の場合、**no switchport** インターフェイス コンフィギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

（注）　スプリット ホライズンがイネーブルの場合、（**ip summary-address rip** ルータ コンフィギュレーション コマンドによって設定される）自動サマリーとインターフェイス サマリー アドレスはともにアドバタイズされません。

```
Switch(config)# router rip
Switch(config-router)# interface gigabitethernet1/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

スプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるためにスプリットホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報がその情報の送信元のインターフェイスで、ルータによってアドバタイズされないようにします。この機能を使用すると、複数のルータ間通信を最適化できます（特にリンクが壊れている場合）。

（注）　ルートを適切にアドバタイズするために、スプリット ホライズンをディセーブルにすることがアプリケーションに必要である場合を除き、一般的にこの機能をディセーブルにすることは推奨しません。

インターフェイス上でスプリット ホライズンをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネットを設定します。

	コマンド	目的
ステップ 4	**no ip split-horizon**	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スプリット ホライズン メカニズムをイネーブルにするには、**ip split-horizon** インターフェイス コンフィギュレーション コマンドを使用します。

OSPF の設定

ここでは、Open Shortest Path First（OSPF）の設定方法について簡単に説明します。OSPF コマンドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「OSPF Commands」を参照してください。

（注）　OSPF では、各メディアがブロードキャスト、非ブロードキャスト、ポイントツーポイント ネットワークに分類されます。スイッチはブロードキャスト（イーサネット、トークン リング、FDDI）とポイントツーポイント ネットワーク（ポイントツーポイント リンクとして設定されたイーサネット インターフェイス）をサポートします。

OSPF は、IP ネットワーク専用の内部ゲートウェイ プロトコル（IGP）で、IP サブネット化、および外部から取得したルーティング情報のタグ付けをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。シスコ実装は RFC 1253 の OSPF Management Information Base（MIB; 管理情報ベース）をサポートします。

シスコ実装は、次の主な機能を含む OSPF バージョン 2 仕様に準拠します。

- スタブ エリアの定義がサポートされます。
- 任意の IP ルーティング プロトコルによって学習されたルートは、別の IP ルーティング プロトコルに再配信できます。つまり、ドメイン内レベルで、OSPF は EIGRP および RIP によって学習されたルートをインポートできます。OSPF ルートを RIP にエクスポートすることもできます。
- エリア内のネイバー ルータ間でのプレーン テキスト認証および MD5 認証がサポートされます。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信間隔、インターフェイス送信遅延、ルータ プライオリティ、ルータの dead と hello 間隔、認証キーなどがあります。
- 仮想リンクがサポートされます。
- RFC 1587 に基づく Not-So-Stubby-Area（NSSA）がサポートされます。

通常、OSPF を使用するには、多くの内部ルータ、複数のエリアに接続された *Area Border Router*（ABR; エリア境界ルータ）、および *Autonomous System Boundary Router*（ASBR; 自律システム境界ルータ）間で調整する必要があります。最小限の設定では、すべてのデフォルト パラメータ値、エリアに割り当てられたインターフェイスが使用され、認証は行われません。使用環境をカスタマイズする場合は、すべてのルータの設定を調整する必要があります。

ここでは、次の設定情報について説明します。

- 「OSPF のデフォルト設定」（P.41-26）
- 「基本的な OSPF パラメータの設定」（P.41-27）

- 「OSPF インターフェイスの設定」（P.41-28）
- 「OSPF エリア パラメータの設定」（P.41-30）
- 「その他の OSPF パラメータの設定」（P.41-31）
- 「LSA グループ ペーシングの変更」（P.41-33）
- 「ループバック インターフェイスの設定」（P.41-33）
- 「OSPF のモニタ」（P.41-34）

OSPF のデフォルト設定

表 41-5 に、OSPF のデフォルト設定を示します。

表 41-5　OSPF のデフォルト設定

機能	デフォルト設定
インターフェイス パラメータ	コスト：デフォルト コストは未定義。 再送信間隔：5 秒。 送信遅延：1 秒。 プライオリティ：1。 hello 間隔：10 秒。 dead 間隔：hello 間隔の 4 倍。 認証なし。 パスワードの指定なし。 MD5 認証はディセーブル。
エリア	認証タイプ：0（認証なし）。 デフォルト コスト：1。 範囲：ディセーブル。 スタブ：スタブ エリアは未定義。 NSSA：NSSA エリアは未定義。
自動コスト	100 Mbps。
デフォルト情報送信元	ディセーブル。イネーブルの場合、デフォルトのメトリック設定は 10、外部ルート タイプのデフォルトはタイプ 2 です。
デフォルト メトリック	各ルーティング プロトコルに適切な、組み込みの自動メトリック変換。
距離 OSPF	dist1（エリア内のすべてのルート）：110。 dist2（エリア間のすべてのルート）：110。 dist3（他のルーティング ドメインからのルート）：110。
OSPF データベース フィルタ	ディセーブル。すべての発信リンクステート アドバタイズ（LSA）がインターフェイスにフラッディングされます。
IP OSPF 名前検索	ディセーブル。
隣接関係変更ログ	イネーブル。
ネイバー	指定なし。

表 41-5　OSPF のデフォルト設定 （続き）

機能	デフォルト設定
ネイバー データベース フィルタ	ディセーブル。すべての発信 LSA がネイバーにフラッディングされます。
ネットワーク エリア	ディセーブル。
NSF[1] 認識	イネーブル ハードウェアまたはソフトウェアの変更中に、NSF 対応のネイバー ルータからのパケット転送をレイヤ 3 スイッチで継続できます。
ルータ ID	OSPF ルーティング プロセスは未定義。
サマリー アドレス	ディセーブル。
タイマー LSA グループ ペーシング	240 秒。
タイマー Shortest Path First（SPF）	spf-delay：5 秒。 spf-holdtime：10 秒。
仮想リンク	エリア ID または ルータ ID は未定義。 hello 間隔：10 秒。 再送信間隔：5 秒。 送信遅延：1 秒。 dead 間隔：40 秒。 認証キー：キーは未定義。 メッセージダイジェスト キー（MD5）：キーは未定義。

1. NSF = ノンストップ フォワーディング

OSPF NSF 認識

IP サービス イメージは IPv4 の OSPF NSF 認識をサポートします。ネイバー ルータが NSF 対応である場合、レイヤ 3 スイッチでは、プライマリ Route Processor（RP; ルート プロセッサ）に障害が発生してルータのバックアップ RP によって処理が引き継がれる前、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、ルータからパケットを転送し続けます。

この機能をディセーブルにはできません。この機能の詳細については、次の URL の『*OSPF Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a0080153edd.shtml

基本的な OSPF パラメータの設定

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、ルーティング プロセスに関連付ける IP アドレスの範囲を指定して、この範囲に関連付けるエリア ID を割り当てる必要があります。

OSPF をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID はローカルに割り当てられ、内部的に使用されている識別パラメータで、任意の正の整数を指定できます。各 OSPF ルーティング プロセスには一意の値があります。
ステップ 3	**network** *address wildcard-mask* **area** *area-id*	OSPF が動作するインターフェイス、およびそのインターフェイスのエリア ID を定義します。1 つのコマンドにワイルドカード マスクを指定して、特定の OSPF エリアに関連付けるインターフェイスを 1 つまたは複数定義できます。エリア ID には 10 進値または IP アドレスを指定できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

OSPF ルーティング プロセスを終了するには、**no router ospf** *process-id* グローバル コンフィギュレーション コマンドを使用します。

次に、OSPF ルーティング プロセスを設定し、プロセス番号 109 を割り当てる例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

OSPF インターフェイスの設定

ip ospf インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイス固有の OSPF パラメータを変更できます。これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータ（hello 間隔、dead 間隔、認証キー）については、接続されたネットワーク内のすべてのルータ間で一貫している必要があります。これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。

（注）　**ip ospf** インターフェイス コンフィギュレーション コマンドはすべて任意です。

OSPF インターフェイス パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip ospf** *cost*	（任意）インターフェイスでパケットを送信するコストを明示的に指定します。
ステップ 4	**ip ospf retransmit-interval** *seconds*	（任意）リンクステート アドバタイズの送信間隔の秒数を指定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 5 秒です。

	コマンド	目的
ステップ 5	**ip ospf transmit-delay** *seconds*	（任意）リンク ステート アップデート パケットを送信するまでの予測待機時間の秒数を設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 1 秒です。
ステップ 6	**ip ospf priority** *number*	（任意）ネットワークに対して、OSPF 指定ルータを検索するときに役立つプライオリティを設定します。指定できる範囲は 0 ～ 255 です。デフォルトは 1 です。
ステップ 7	**ip ospf hello-interval** *seconds*	（任意）OSPF インターフェイスで hello パケットの送信間隔の秒数を設定します。値はネットワークのすべてのノードで同じである必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 10 秒です。
ステップ 8	**ip ospf dead-interval** *seconds*	（任意）最後の装置で hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間の秒数を設定します。値はネットワークのすべてのノードで同じである必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は hello 間隔の 4 倍です。
ステップ 9	**ip ospf authentication-key** *key*	（任意）ネイバー OSPF ルータで使用されるパスワードを割り当てます。パスワードには、キーボードから入力した任意の文字列（最大 8 バイト長）を指定できます。同じネットワーク上のすべてのネイバー ルータには、OSPF 情報を交換するため、同じパスワードを設定する必要があります。
ステップ 10	**ip ospf message digest-key** *keyid* **md5** *key*	（任意）MD5 認証をイネーブルにします。 • *keyid*：1 ～ 255 の ID • *key*：最大 16 バイトの英数字パスワード
ステップ 11	**ip ospf database-filter all out**	（任意）インターフェイスへの OSPF LSA パケットのフラッディングをブロックします。デフォルトでは、LSA が着信するインターフェイスを除き、同じエリア内のすべてのインターフェイスに OSPF は新しい LSA をフラッディングします。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip ospf interface** [*interface-name*]	OSPF 関連のインターフェイス情報を表示します。
ステップ 14	**show ip ospf neighbor detail**	ネイバー スイッチの NSF 認識ステータスを表示します。出力は、次のいずれかに一致します。 • *Options is 0x52* *LLS Options is 0x1 (LR)* これらの両方の行が表示される場合、ネイバー スイッチが NSF 認識です。 • *Options is 0x42*：ネイバー スイッチが NSF 認識でないことを示します。
ステップ 15	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

設定されたパラメータ値を削除するか、またはデフォルト値に戻すには、これらのコマンドの **no** 形式を使用します。

OSPF エリア パラメータの設定

複数の OSPF エリア パラメータを設定することもできます。設定できるパラメータには、エリア、スタブ エリア、および Not-So-Stubby-Area（NSSA）への不正アクセスをパスワードに基づいて阻止する認証用パラメータがあります。*スタブ エリア*に外部ルートに関する情報は送信されません。代わりに、Autonomous System（AS; 自律システム）外の宛先に対するデフォルトの外部ルートが、エリア境界ルータ（ABR）によってスタブ エリアに生成されます。NSSA ではコアからそのエリアへ向かう LSA の一部がフラッディングされませんが、再配信することによって、エリア内の AS 外部ルートをインポートできます。

ルート サマライズとは、アドバタイズされたアドレスを、他のエリアでアドバタイズされる単一のサマリー ルートに統合することです。ネットワーク番号が連続する場合は、**area range** ルータ コンフィギュレーション コマンドを使用して、範囲内のすべてのネットワークを対象とするサマリー ルートをアドバタイズするように ABR を設定できます。

（注） OSPF **area** ルータ コンフィギュレーション コマンドはすべて任意です。

エリア パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**area** *area-id* **authentication**	（任意）特定のエリアへの不正アクセスのパスワードに基づいた阻止を可能にします。ID には 10 進値または IP アドレスのいずれかを指定できます。
ステップ 4	**area** *area-id* **authentication message-digest**	（任意）エリアで MD5 認証をイネーブルにします。
ステップ 5	**area** *area-id* **stub** [**no-summary**]	（任意）エリアをスタブ エリアとして定義します。**no-summary** キーワードを指定すると、ABR はサマリー リンク アドバタイズをスタブ エリアに送信できなくなります。
ステップ 6	**area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**]	（任意）エリアを Not-So-Stubby-Area として定義します。同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。次のいずれかのキーワードを選択します。 • **no-redistribution** : ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA ではなく通常のエリアにインポートする場合に選択します。 • **default-information-originate** : タイプ 7 LSA を NSSA にインポートする場合に、ABR で選択します。 • **no-summary** : サマリー LSA を NSSA に送信しない場合に選択します。
ステップ 7	**area** *area-id* **range** *address mask*	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、エリア境界ルータに対してだけ使用します。
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**show ip ospf** [*process-id*]	一般的な OSPF ルーティング プロセスまたは特定のプロセス ID に関する情報を表示して、設定を確認します。
	show ip ospf [*process-id* [*area-id*]] **database**	特定のルータの OSPF データベースに関連する情報のリストを表示します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

設定されたパラメータ値を削除するか、またはデフォルト値に戻すには、これらのコマンドの **no** 形式を使用します。

その他の OSPF パラメータの設定

ルータ コンフィギュレーション モードで、その他の OSPF パラメータを設定することもできます。

- ルート サマライズ：他のプロトコルからのルートを再配信すると（「ルート マップによるルーティング情報の再配信」（P.41-94）を参照）、各ルートは外部 LSA 内で個別にアドバタイズされます。OSPF リンク ステート データベースのサイズを小さくするには、**summary-address** ルータ コンフィギュレーション コマンドを使用して、指定されたネットワーク アドレスおよびマスクに含まれる再配信されたすべてのルートを単一のルータにアドバタイズします。
- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続的である場合に仮想リンクを確立するには、2 つのエリア境界ルータを仮想リンクのエンドポイントとして設定します。設定情報には、他の仮想エンドポイント（他の ABR）の ID、および 2 つのルータに共通する非バックボーン リンク（通過エリア）などがあります。仮想リンクをスタブ エリアから設定することはできません。
- デフォルト ルート：OSPF ルーティング ドメイン内へのルートの再配信を設定すると、ルートは自動的に自律システム境界ルータ（ASBR）になります。ASBR を設定し、強制的に OSPF ルーティング ドメイン内にデフォルト ルートを生成できます。
- すべての OSPF **show** 特権 EXEC コマンドで使用される Domain Name Server（DNS; ドメイン ネーム サーバ）名を使用すると、ルータ ID やネイバー ID を指定して表示する場合に比べ、ルータを簡単に識別できます。
- デフォルト メトリック：OSPF は、インターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックを計算します。メトリックは、帯域幅で分割された *ref-bw* として計算されます。ここでの *ref* のデフォルト値は 10 で、帯域幅（*bw*）は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。高帯域幅を持つ複数のリンクの場合は、大きな数値を指定してこれらのリンクのコストを区別できます。
- 管理ディスタンスは、ルーティング情報の送信元の信頼性を示す値です。0 ～ 255 の整数を指定でき、値が大きいほど信頼性は低下します。管理ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。OSPF では、エリア内のルート（エリア間）、別のエリアへのルート（エリア間）、および再配信によって学習された別のルーティング ドメインからのルート（外部）の 3 つの管理ディスタンスが使用されます。どの管理ディスタンスの値でも変更できます。
- 受動インターフェイス：イーサネット上の 2 つの装置間のインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信元インターフェイスに hello パケットを送信しないようにするには、送信元の装置を受動インターフェイスに設定する必要があります。両方の装置は、受信インターフェイス宛ての hello パケットを使用することで、相互の識別を可能にします。
- ルート計算タイマー：OSPF がトポロジの変更を受信してから Shortest Path First（SPF）計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールドタイムを設定できます。

- ネイバー変更ログ：OSPF ネイバー ステートが変更されたときに Syslog メッセージを送信するようにルータを設定し、ルータの変更を詳細に表示できます。

上記の OSPF パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**summary-address** *address mask*	（任意）1 つのサマリー ルートだけがアドバタイズされるように、再配信されたルートのアドレスおよび IP サブネット マスクを指定します。
ステップ 4	**area** *area-id* **virtual-link** router-id [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**trans**] [[**authentication-key** *key*] | **message-digest-key** *keyid* **md5** *key*]]	（任意）仮想リンクを確立し、パラメータを設定します。パラメータ定義については「OSPF インターフェイスの設定」（P.41-28）、仮想リンクのデフォルト設定については表 41-5（P.41-26）を参照してください。
ステップ 5	**default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]	（任意）強制的に OSPF ルーティング ドメイン内にデフォルト ルートを生成するように ASBR を設定します。パラメータはすべて任意です。
ステップ 6	**ip ospf name-lookup**	（任意）DNS 名前検索を設定します。デフォルトはディセーブルです。
ステップ 7	**ip auto-cost reference-bandwidth** *ref-bw*	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、エリア境界ルータに対してだけ使用します。
ステップ 8	**distance ospf** {[**inter-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}	（任意）OSPF のディスタンスの値を変更します。各タイプのルートのデフォルトのディスタンスは 110 です。指定できる範囲は 1 ～ 255 です。
ステップ 9	**passive-interface** *type number*	（任意）指定されたインターフェイス経由の hello パケットの送信を抑制します。
ステップ 10	**timers throttle spf** *spf-delay spf-holdtime spf-wait*	（任意）ルート計算タイマーを設定します。 • *spf-delay*：SPF 計算の変更を受信する間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-holdtime*：最初と 2 番めの SPF 計算間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-wait*：SPF 計算の最大待機時間（ミリ秒単位）。指定できる範囲は 1 ～ 600000 ミリ秒です。
ステップ 11	**ospf log-adj-changes**	（任意）ネイバー ステートが変更されたときに Syslog メッセージを送信します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip ospf** [*process-id* [*area-id*]] **database**	特定のルータの OSPF データベースに関連する情報のリストを表示します。キーワード オプションの一部については、「OSPF のモニタ」（P.41-34）を参照してください。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

LSA グループ ペーシングの変更

OSPF LSA グループ ペーシング機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、およびエージング機能をペーシングして、ルータをより効率的に使用することが可能になります。この機能はデフォルトでイネーブルになっています。デフォルトのペーシング間隔は 4 分間です。通常は、このパラメータを変更する必要はありません。最適なグループ ペーシング間隔は、ルータがリフレッシュ、チェックサム、およびエージングを行う LSA 数に反比例します。たとえば、データベースに約 10,000 個の LSA が格納されている場合、ペーシング間隔を短くすると便利です。小さなデータベース（40 ～ 100 LSA）を使用する場合は、ペーシング間隔を長くし、10 ～ 20 分に設定してください。

OSPF LSA ペーシングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**timers lsa-group-pacing** *seconds*	LSA グループ ペーシングを変更します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト値に戻すには、**no timers lsa-group-pacing** ルータ コンフィギュレーション コマンドを使用します。

ループバック インターフェイスの設定

OSPF は、インターフェイスに設定されている最大の IP アドレスをルータ ID として使用します。このインターフェイスがダウンした場合、または削除された場合、OSPF プロセスは新しいルータ ID を再計算し、すべてのルーティング情報をそのルータのインターフェイスから再送信する必要があります。ループバック インターフェイスが IP アドレスで設定されている場合、他のインターフェイスにより大きな IP アドレスがある場合でも、OSPF はこの IP アドレスをルータ ID として使用します。ループバック インターフェイスに障害は発生しないため、安定性は増大します。OSPF は他のインターフェイスよりもループバック インターフェイスを自動的に優先し、すべてのループバック インターフェイスの中で最大の IP アドレスを選択します。

ループバック インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface loopback 0**	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** *address mask*	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ループバック インターフェイスをディセーブルにするには、**no interface loopback 0** グローバル コンフィギュレーション コマンドを使用します。

OSPF のモニタ

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

表 41-6 に、統計情報を表示するために使用する特権 EXEC コマンドの一部を示します。**show ip ospf database** 特権 EXEC コマンド オプションおよび表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。

表 41-6　IP OSPF 統計情報の表示コマンド

コマンド	目的
show ip ospf [*process-id*]	OSPF ルーティング プロセスに関する一般情報を表示します。
show ip ospf [*process-id*] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id*] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id*] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**database-summary**]	OSPF データベースに関連する情報のリストを表示します。
show ip ospf border-routes	内部 OSPF ルーティング ABR および ASBR テーブル エントリを表示します。
show ip ospf interface [*interface-name*]	OSPF 関連のインターフェイス情報を表示します。
show ip ospf neighbor [*interface-name*] [*neighbor-id*] **detail**	OSPF インターフェイス ネイバー情報を表示します。
show ip ospf virtual-links	OSPF 関連の仮想リンク情報を表示します。

EIGRP の設定

拡張 IGRP（EIGRP）は、IGRP のシスコ独自の拡張バージョンです。EIGRP は IGRP と同じディスタンス ベクトル アルゴリズムおよびディスタンス情報を使用しますが、EIGRP ではコンバージェンス プロパティと動作効率が大幅に改善されています。

コンバージェンス テクノロジーには、Diffusing Update Algorithm（DUAL）と呼ばれるアルゴリズムが採用されています。DUAL を使用すると、ルート計算の各段階でループが発生しなくなり、トポロジの変更に関連するすべての装置を同時に同期できます。トポロジの変更の影響を受けないルータは、再計算から除外されます。

IP EIGRP を導入すると、ネットワークの幅が広がります。RIP の場合、ネットワークの最大幅は 15 ホップです。EIGRP メトリックは数千ホップをサポートするほど大きいため、ネットワークを拡張するときに問題となるのは、トランスポートレイヤのホップ カウンタだけです。IP パケットが 15 台のルータを経由し、宛先方向のネクストホップが EIGRP によって学習されている場合だけ、EIGRP は転送制御フィールドの値を増やします。RIP ルートを宛先方向のネクストホップとして使用する場合、転送制御フィールドでは、通常どおり値が増加します。

EIGRP には次の機能があります。

- 高速コンバージェンス。
- 差分更新。宛先のステートが変更された場合、ルーティング テーブルの内容全体を送信する代わりに差分更新を行い、EIGRP パケットに必要な帯域幅を最小化します。
- 低い CPU 使用率。受信ごとに完全更新パケットを処理する必要がないため、CPU 使用率が低下します。
- プロトコル独立型ネイバー探索メカニズム。このメカニズムを使用して、ネイバー ルータを確認します。
- Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）。
- 任意のルート サマライズ。
- 大規模ネットワークへの対応。

EIGRP には、次に示す 4 つの基本コンポーネントがあります。

- *ネイバー探索および回復*。直接接続されたネットワーク上の他のルータに関する情報をダイナミックに学習するために、ルータで使用されるプロセスです。ネイバーが到達不能になった場合、または操作不能になった場合、ルータもこの情報を検出する必要があります。ネイバー探索および回復は、サイズの小さな hello パケットを定期的に送信することにより、わずかなオーバーヘッドで実現されます。hello パケットが受信されている限り、Cisco IOS ソフトウェアは、ネイバーが有効に機能していると学習します。このように判別された場合、ネイバー ルータはルーティング情報を交換できます。
- *信頼性のあるトランスポート プロトコル*。EIGRP パケットをすべてのネイバーに確実に、順序どおりに配信します。マルチキャスト パケットとユニキャスト パケットが混在する送信もサポートされます。EIGRP パケットには、確実に送信する必要があるものと、そうでないものがあります。効率を高めるために、必要な場合だけ信頼性が確保されます。たとえば、マルチキャスト機能があるマルチアクセス ネットワーク（イーサネットなど）では、すべてのネイバーにそれぞれ hello パケットを確実に送信する必要はありません。したがって、EIGRP はパケットへの確認応答が不要であることを通知する、レシーバー宛ての情報をパケットに格納して、単一のマルチキャスト hello を送信します。他のタイプのパケット（アップデートなど）では、確認応答（ACK パケット）を要求します。信頼性のあるトランスポートであれば、保留中の未確認応答がある場合、マルチキャスト パケットを迅速に送信できます。このため、リンク速度が変化する場合でも、コンバージェンスに要する時間を短く保つことができます。
- *DUAL 有限ステート マシン*。すべてのルート計算に関する決定プロセスを統合します。すべてのネイバーによってアドバタイズされたすべてのルートを追跡します。DUAL は、ディスタンス情報（メトリック）を使用して効率的なループフリー パスを選択します。さらに、DUAL は適切な後継ルータに基づいて、ルーティング テーブルに挿入するルートを選択します。後継ルータは、宛先への最小コスト パス（ルーティング ループに関連しないことが保証されている）を持つ、パケット転送に使用されるネイバー ルータです。適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は、再計算を行う必要があります。この結果、新しい後継ルータが決定されます。ルートの再計算にかかる時間によって、コンバージェンスに要する時間が変わります。再計算はプロセッサを集中的に使用するため、必要でない場合は、再計算を行わないようにしてください。トポロジに変更が発生すると、DUAL は適切な後継ルータの有無を調べます。適切な後継ルータが存在する場合は、それらを探して使用し、不要な再計算を回避します。
- *プロトコル依存モジュール*。ネットワーク レイヤ プロトコルに特有の作業を行います。たとえば IP EIGRP モジュールは、IP でカプセル化された EIGRP パケットを送受信します。このモジュールは、EIGRP パケットを解析し、受信した新しい情報を DUAL に通知する作業も行います。EIGRP は DUAL にルーティング判断を行うように要求しますが、結果は IP ルーティング テーブルに格納されます。EIGRP は、他の IP ルーティング プロトコルによって学習されたルートの再配信も行います。

ここでは、次の設定情報について説明します。

EIGRP のデフォルト設定

表 41-7 に、EIGRP のデフォルト設定を示します。

表 41-7　EIGRP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。クラスフル ネットワーク境界を通過するときに、この境界にサブプレフィクスがサマライズされます。
デフォルト情報	再配信中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報が渡されます。
デフォルト メトリック	デフォルト メトリックなしで再配信できるのは、接続ルートおよびインターフェイスのスタティック ルートだけです。メトリックは次のとおりです。 • 帯域幅：0 kbps 以上 • 遅延（10 マイクロ秒単位）：0 または 39.1 ナノ秒の倍数である任意の正の数値 • 信頼性：0 ～ 255 の任意の数値（255 は信頼性が 100%） • 負荷：0 ～ 255 の数値で表される有効帯域幅（255 は 100% の負荷） • Maximum Transmission Unit（MTU; 最大伝送ユニット）：バイトで表された最大伝送ユニットのサイズ（0 または任意の正の整数）
ディスタンス	内部ディスタンス：90 外部ディスタンス：170
EIGRP ネイバー変更ログ	ディセーブル。隣接の変更はログに記録されません。
IP 認証キー チェーン	認証なし。
IP 認証モード	認証なし。
IP 帯域幅比率	50%
IP hello 間隔	低速の Nonbroadcast Multiaccess（NBMA; 非ブロードキャスト マルチアクセス）ネットワークの場合：60 秒、それ以外のネットワークの場合：5 秒
IP ホールドタイム	低速の NBMA ネットワークの場合：180 秒、それ以外のネットワークの場合：15 秒
IP スプリットホライズン	イネーブル。

表 41-7　EIGRP のデフォルト設定 （続き）

機能	デフォルト設定
IP サマリー アドレス	サマリー集約アドレスは未定義。
メトリックの重み	tos：0。k1 および k3：1。k2、k4、および k5：0。
ネットワーク	指定なし。
NSF[1] 認識	イネーブル。 ハードウェアまたはソフトウェアの変更中に、NSF 対応のネイバー ルータからのパケット転送をレイヤ 3 スイッチで継続できます。
オフセット リスト	ディセーブル。
ルータ EIGRP	ディセーブル。
メトリック設定	ルート マップにはメトリック設定なし。
トラフィック共有	メトリックの比率に応じて分散。
差異	1（等価コスト ロード バランシング）

1. NSF = ノンストップ フォワーディング

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにし、ネットワークを関連付ける必要があります。EIGRP は、指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイス ネットワークを指定しないと、どの EIGRP アップデート中にアドバタイズされません。

（注）　ネットワーク上に IGRP 用に設定されているルータがあり、この設定を EIGRP に変更する場合は、IGRP と EIGRP の両方が設定された移行ルータを指定する必要があります。この場合は、次の項に記載されているステップ 1 ～ 3 を実行してください（「スプリット ホライズンの設定」（P.41-24）も参照）。ルートを自動的に再配信するには、同じ AS 番号を使用する必要があります。

EIGRP NSF 認識

EIGRP NSF 認識機能は IP サービス イメージの IPv4 でサポートされています。ネイバー ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータのプライマリ ルート プロセッサ（RP）に障害が発生してバックアップ RP によって処理が引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、ネイバー ルータからパケットを転送し続けます。

この機能をディセーブルにはできません。この機能の詳細については、次の URL の『*EIGRP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080160010.html

基本的な EIGRP パラメータの設定

EIGRP を設定するには、特権 EXEC モードで次の手順を実行します。ルーティング プロセスの設定は必須ですが、それ以外のステップは任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *autonomous-system number*	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号によって他の EIGRP ルータへのルートを特定し、ルーティング情報をタグ付けします。
ステップ 3	**network** *network-number*	ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP は、指定されたネットワーク内のインターフェイスにアップデートを送信します。
ステップ 4	**eigrp log-neighbor-changes**	（任意）EIGRP ネイバー変更ログをイネーブルにして、ルーティング システムの安定性をモニタします。
ステップ 5	**metric weights** *tos k1 k2 k3 k4 k5*	（任意）EIGRP メトリックを調整します。デフォルト値はほとんどのネットワークで適切に動作するように入念に設定されていますが、調整することも可能です。 ⚠ **注意** メトリックを設定する作業は複雑です。熟練したネットワーク設計者の指導がない場合は、行わないでください。
ステップ 6	**offset list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*]	（任意）オフセット リストをルーティング メトリックに適用して、EIGRP によって学習したルートへの着信および発信メトリックを増加させます。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 7	**no auto-summary**	（任意）ネットワーク レベル ルートへのサブネット ルートの自動サマライズをディセーブルにします。
ステップ 8	**ip summary-address eigrp** *autonomous-system-number address mask*	（任意）サマリー集約を設定します。
ステップ 9	**end**	特権 EXEC モードに戻ります。

ステップ 10	**show ip protocols**	設定を確認します。
		NSF 認識の場合、出力に次のように表示されます。
		`*** IP Routing is NSF aware ***`
		`EIGRP NSF enabled`

ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。

EIGRP インターフェイスの設定

インターフェイスごとに、他の EIGRP パラメータを任意で設定できます。

EIGRP インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip bandwidth-percent eigrp** *percent*	（任意）インターフェイスで EIGRP が使用できる帯域幅のパーセンテージを設定します。デフォルト値は 50% です。
ステップ 4	**ip summary-address eigrp** *autonomous-system-number address mask*	（任意）指定されたインターフェイスのサマリー集約アドレスを設定します（自動サマリーがイネーブルの場合は、通常設定する必要はありません）。
ステップ 5	**ip hello-interval eigrp** *autonomous-system-number seconds*	（任意）EIGRP ルーティング プロセスの hello タイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は、低速の NBMA ネットワークの場合は 60 秒、それ以外のネットワークの場合は 5 秒です。
ステップ 6	**ip hold-time eigrp** *autonomous-system-number seconds*	（任意）EIGRP ルーティング プロセスのホールドタイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は、低速の NBMA ネットワークの場合は 180 秒、それ以外のネットワークの場合は 15 秒です。 **注意**　ホールドタイムを調整する前に、シスコのテクニカル サポートにお問い合わせください。
ステップ 7	**no ip split-horizon eigrp** *autonomous-system-number*	（任意）スプリット ホライズンをディセーブルにして、ルート情報がその情報の送信元のインターフェイスからルータによってアドバタイズされるようにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip eigrp interface**	EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。

EIGRP ルート認証の設定

EIGRP ルート認証を使用すると、EIGRP ルーティング プロトコルからのルーティング アップデートに関する MD5 認証が可能になり、承認されていない送信元から無許可または問題のあるルーティング メッセージを受け取ることがなくなります。

認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip authentication mode eigrp** *autonomous-system* **md5**	IP EIGRP パケットの MD5 認証をイネーブルにします。
ステップ 4	**ip authentication key-chain eigrp** *autonomous-system key-chain*	IP EIGRP パケットの認証をイネーブルにします。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**key chain** *name-of-chain*	キー チェーンを指定して、キー チェーン コンフィギュレーション モードを開始します。ステップ 4 で設定した名前を指定します。
ステップ 7	**key** *number*	キー チェーン コンフィギュレーション モードで、キー番号を指定します。
ステップ 8	**key-string** *text*	キー チェーン コンフィギュレーション モードで、キー文字列を指定します。
ステップ 9	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）キーの受信可能期間を指定します。 *start-time* および *end-time* 構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 10	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）キーの送信可能期間を指定します。 *start-time* および *end-time* 構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show key chain**	認証キーの情報を表示します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。

EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティング機能は、ルーテッド トラフィックをエンド ユーザにより近い場所に移動することでリソースの利用率を低減させます。

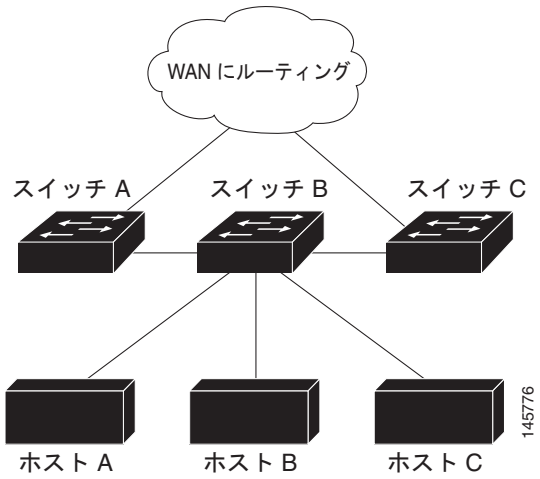
EIGRP スタブ ルーティングを使用するネットワークでは、ユーザに対して許容される IP トラフィックのルートは、EIGRP スタブ ルーティングで設定されたスイッチを介したルートだけです。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他の装置に接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングを使用する場合、EIGRP を使用してスイッチだけをスタブとして設定するようにディストリビューション ルータとリモート ルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ステータスを通知するパケットを受信するネイバーは、スタブ ルータに対してルートのクエリーを実行せず、スタブ ピアを持つルータはそのピアに対するクエリーを実行しません。スタブ ルータは、ディストリビューション ルータに依存してすべてのピアに適切なアップデートを送信します。

図 41-4 では、スイッチ B が EIGRP スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配信ルート、サマリー ルートをスイッチ A および C にアドバタイズします。スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 41-4　　EIGRP スタブ ルータ設定



（注） **eigrp stub** ルータ コンフィギュレーション コマンドを入力すると、**eigrp stub connected summary** コマンドだけが有効になります。CLI ヘルプでは **receive-only** および **static** キーワードが表示されることがありますが、IP ベース イメージを実行するスイッチは、常に **connected** および **summary** キーワードが設定されている場合と同様に動作します。

EIGRP スタブ ルーティングの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.2*』の「Configuring EIGRP Stub Routing」を参照してください。

EIGRP のモニタおよびメンテナンス

ネイバー テーブルからネイバーを削除できます。さらに、各種 EIGRP ルーティング統計情報を表示することもできます。表 41-8 に、ネイバーの削除および統計情報の表示に使用する特権 EXEC コマンドを示します。表示されるフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。

表 41-8　IP EIGRP の clear および show コマンド

コマンド	目的
clear ip eigrp neighbors [*if-address* | *interface*]	ネイバー テーブルからネイバーを削除します。
show ip eigrp interface [*interface*] [*as number*]	EIGRP 用に設定されたインターフェイスの情報を表示します。
show ip eigrp neighbors [*type-number*]	EIGRP によって検出されたネイバーを表示します。
show ip eigrp topology [*autonomous-system-number*] | [[*ip-address*] *mask*]]	指定されたプロセスの EIGRP トポロジ テーブルを表示します。
show ip eigrp traffic [*autonomous-system-number*]	すべてまたは特定の EIGRP プロセスの送受信されたパケット数を表示します。

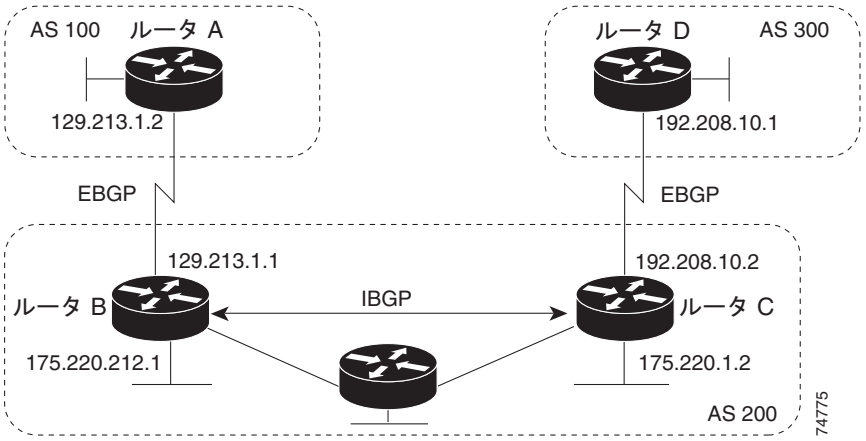
BGP の設定

Border Gateway Protocol（BGP）は Exterior Gateway Protocol（EGP; エクステリア ゲートウェイ プロトコル）です。自律システム間で、ループの発生しないルーティング情報の交換を保証するドメイン間ルーティング システムを設定するために使用されます。自律システムは、同じ管理下で動作して、RIP や OSPF などの Interior Gateway Protocol（IGP）を境界内で実行し、Exterior Gateway Protocol（EGP）を使用して相互接続するルータで構成されます。BGP Version 4 は、インターネットでドメイン間ルーティングを行うための標準 EGP です。このプロトコルは、RFC 1163、1267、および 1771 で定義されています。BGP の詳細については、『*Internet Routing Architectures*』（Cisco Press 刊）、および Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IP and IP Routing Configuration Guide*』の「Configuring BGP」の章を参照してください。

BGP コマンドおよびキーワードの詳細については、[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「IP Routing Protocols」を参照してください。表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 C「Cisco IOS Release 12.2(55)SE でサポートされていないコマンド」を参照してください。

BGP アップデートを交換する場合、同じ自律システム（AS）に属するルータは *Internal BGP*（IBGP; 内部 BGP）を実行し、異なる自律システムに属するルータは *External BGP*（EBGP; 外部 BGP）を実行します。大部分のコンフィギュレーション コマンドは、EBGP と IBGP で同じです。違いは、ルーティング アップデートが AS 間で交換されるか（EBGP）、または AS 内で交換されるか（IBGP）という点です。図 41-5 に、EBGP と IBGP の両方が稼動するネットワークを示します。

図 41-5　EBGP、IBGP、および複数の自律システム



外部 AS と情報を交換する前に、BGP は AS 内のルータ間で内部 BGP ピアリングを定義し、IGRP や OSPF などの AS 内で稼動する IGP に BGP ルーティング情報を再配信して、AS 内のネットワークに到達できることを確認します。

BGP ルーティング プロセスを実行するルータは、通常 BGP *スピーカー*と呼ばれます。BGP はトランスポート プロトコルとして Transmission Control Protocol（TCP; 伝送制御プロトコル）を使用します（特にポート 179）。ルーティング情報を交換するために相互に TCP 接続された 2 つの BGP スピーカーを、*ピア*または*ネイバー*と呼びます。図 41-5 では、ルータ A と B、ルータ B と C、およびルータ C と D がそれぞれ BGP ピアです。ルーティング情報は、宛先ネットワークへのフル パスを示す一連の AS 番号です。BGP はこの情報を使用して、ループのない自律システム マップを作成します。

このネットワークには、次の特性があります。

- ルータ A および B では EBGP が稼動し、ルータ B および C では IBGP が稼動しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。IGP が稼動し、2 つのネイバーが相互に到達する限り、IBGP ピアを直接接続する必要はありません。
- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。つまり、AS 内の BGP スピーカーは論理的にフル メッシュ構造である必要があります。BGP4 は、論理フル メッシュに関する要件を軽減する 2 つの技術（*連合*と*ルート リフレクタ*）を提供します。
- AS 200 は、AS 100 および AS 300 の*中継 AS* です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティング テーブルを最初に交換し、差分更新だけを送信します。BGP ピアは、キープアライブ メッセージ（接続がアップ状態であることを確認）、および通知メッセージ（エラーや特殊条件に応答）も交換します。

BGP の場合、各ルートはネットワーク番号、情報が通過した自律システムのリスト（*自律システム パス*）、および他の*パス属性*のリストで構成されます。BGP システムの主な機能は、AS パスのリストに関する情報など、ネットワーク到達可能性情報を他の BGP システムと交換することです。この情報は、AS が接続されているかどうかを判別したり、ルーティング ループをプルーニングしたり、AS レベル ポリシーの判断を行うために使用できます。

Cisco IOS が稼動しているルータまたはスイッチが IBGP ルートを選択または使用するのは、ネクストホップ ルータで使用可能なルートがあり、IGP から同期信号を受信している（IGP 同期がディセーブルである場合を除く）場合です。複数のルートが使用可能な場合、BGP は*属性*値に基づいてパスを選択します。BGP 属性の詳細については、「BGP 判断属性の設定」（P.41-51）を参照してください。

BGP Version 4 では Classless Interdomain Routing（CIDR; クラスレス ドメイン間ルーティング）がサポートされているため、集約ルートを作成して*スーパーネット*を構築することで、ルーティング テーブルのサイズを削減できます。CIDR では BGP 内部のネットワーク クラスの概念が排除され、IP プレフィクスのアドバタイズがサポートされています。

ここでは、次の設定情報について説明します。

- 「BGP のデフォルト設定」（P.41-44）
- 「BGP ルーティングのイネーブル化」（P.41-47）
- 「ルーティング ポリシーの変更の管理」（P.41-50）
- 「BGP 判断属性の設定」（P.41-51）
- 「ルート マップによる BGP フィルタリングの設定」（P.41-53）
- 「ネイバーによる BGP フィルタリングの設定」（P.41-54）
- 「BGP フィルタリング用のプレフィクス リストの設定」（P.41-55）
- 「BGP コミュニティ フィルタリングの設定」（P.41-56）
- 「BGP ネイバーおよびピア グループの設定」（P.41-58）
- 「集約アドレスの設定」（P.41-60）
- 「ルーティング ドメイン連合の設定」（P.41-61）
- 「BGP ルート リフレクタの設定」（P.41-61）
- 「ルート ダンプニングの設定」（P.41-62）
- 「BGP のモニタおよびメンテナンス」（P.41-63）

BGP 設定の詳細については、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Routing Protocols」にある「Configuring BGP」の章を参照してください。特定のコマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。これらのマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 C「Cisco IOS Release 12.2(55)SE でサポートされていないコマンド」を参照してください。

BGP のデフォルト設定

表 41-9 に、BGP の基本的なデフォルト設定を示します。すべての特性のデフォルトについては、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing ProtocolsRelease 12.2*』で特定のコマンドを参照してください。

表 41-9　BGP のデフォルト設定

機能	デフォルト設定
集約アドレス	ディセーブル：定義なし
AS パス アクセス リスト	定義なし。
自動サマリー	イネーブル。
最適パス	• ルータはルートを選択する場合に *as-path* を考慮し、外部 BGP ピアからの類似ルートは比較されません。 • ルータ ID の比較：ディセーブル

表 41-9　BGP のデフォルト設定 （続き）

機能	デフォルト設定
BGP コミュニティ リスト	• 番号：定義なし。コミュニティ番号を示す特定の値を許可すると、許可されていないその他すべてのコミュニティ番号は、暗黙の拒否にデフォルト設定されます。 • 形式：シスコのデフォルト形式（32 ビットの番号）
BGP 連合 ID/ ピア	• ID：設定なし • ピア：識別なし
BGP 高速外部フォールオーバー	イネーブル。
BGP ローカル プリファレンス	100. 指定できる範囲は 0 ～ 4294967295 です（大きな値を推奨）。
BGP ネットワーク	指定なし。バックドア ルートのアドバタイズなし。
BGP ルート ダンプニング	デフォルトではディセーブル。イネーブルの場合は次のようになります。 • 半減期は 15 分 • 再利用値は 750（10 秒増分） • 抑制値は 2000（10 秒増分） • 最大抑制時間は半減期の 4 倍（60 分）
BGP ルータ ID	ループバック インターフェイスに IP アドレスが設定されている場合はループバック インターフェイスの IP アドレス、またはルータの物理インターフェイスに対して設定された最大の IP アドレス。
デフォルト情報送信元（プロトコルまたはネットワーク再配信）	ディセーブル。
デフォルト メトリック	自動メトリック変換（組み込み）。
ディスタンス	• 外部ルート管理ディスタンス：20（指定できる値は 1 ～ 255） • 内部ルート管理ディスタンス：200（指定できる値は 1 ～ 255） • ローカル ルート管理ディスタンス：200（指定できる値は 1 ～ 255）
配信リスト	• 入力（アップデート中に受信されたネットワークをフィルタリング）：ディセーブル • 出力（アップデート中のネットワークのアドバタイズを抑制）：ディセーブル
内部ルート再配信	ディセーブル。
IP プレフィクス リスト	定義なし。
Multi Exit Discriminator（MED）	• 常に比較：ディセーブル。異なる自律システム内のネイバーからのパスに対して MED を比較しません。 • 最適パスの比較：ディセーブル。 • 最も条件の悪いパスである MED の除外：ディセーブル。 • 決定的な MED 比較：ディセーブル。

表 41-9　BGP のデフォルト設定 （続き）

機能	デフォルト設定
ネイバー	• アドバタイズの間隔：外部ピアの場合は 30 秒、内部ピアの場合は 5 秒 • ロギング変更：イネーブル • 条件付きアドバタイズ：ディセーブル • デフォルト送信元：ネイバーに送信されるデフォルト ルートはなし • 説明：なし • 配信リスト：定義なし • 外部 BGP マルチホップ：直接接続されたネイバーだけを許可 • フィルタ リスト：使用しない • 受信したプレフィクスの最大数：制限なし • ネクストホップ（BGP ネイバーのネクストホップとなるルータ）：ディセーブル • パスワード：ディセーブル • ピア グループ：定義なし。割り当てメンバーなし • プレフィクス リスト：指定なし • リモート AS（ネイバー BGP テーブルへのエントリ追加）：ピア定義なし • プライベート AS 番号の削除：ディセーブル • ルート マップ：ピアへの適用なし • コミュニティ属性送信：ネイバーへの送信なし • シャットダウンまたはソフト再設定：ディセーブル • タイマー：キープアライブは 60 秒、ホールドタイムは 180 秒 • アップデート送信元：最適ローカル アドレス • バージョン：BGP Version 4 • 重み：BGP ピアによって学習されたルートは 0、ローカル ルータから取得されたルートは 32768
NSF[1] 認識	ディセーブル。ハードウェアまたはソフトウェアの変更中に、NSF 対応のネイバー ルータからのパケット転送をレイヤ 3 スイッチで継続できます。 **（注）** NSF 認識は、グレースフル リスタートをイネーブルにすることで、IPv4 でイネーブルにできます。
ルート リフレクタ	設定なし。
同期化（BGP および IGP）	イネーブル。
テーブル マップ アップデート	ディセーブル。
タイマー	キープアライブ：60 秒、ホールドタイム：180 秒

1. NSF = ノンストップ フォワーディング

ノンストップ フォワーディング認識

BGP NSF 認識機能は IP サービス イメージの IPv4 でサポートされています。BGP ルーティングでこの機能をイネーブルにするには、グレースフル リスタートをイネーブルにする必要があります。ネイバー ルータが NSF 対応で、この機能がイネーブルである場合、レイヤ 3 スイッチでは、ルータのプライマリ ルート プロセッサ（RP）に障害が発生してバックアップ RP によって処理が引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、ネイバー ルータからパケットを転送し続けます。

詳細については、次の URL の『*BGP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008015fede.html

BGP ルーティングのイネーブル化

BGP ルーティングをイネーブルにするには、BGP ルーティング プロセスを確立し、ローカル ネットワークを定義します。BGP はネイバーとの関係を完全に認識する必要があるため、BGP ネイバーも指定する必要があります。

BGP は、内部および外部の 2 種類のネイバーをサポートします。*内部ネイバー*は同じ AS 内に、*外部ネイバー*は異なる自律システム内にあります。通常の場合、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダーによって割り当てられ、ルートが外部ネイバーにアドバタイズされないシステムに設定されます。プライベート AS 番号の範囲は 64512 ～ 65535 です。AS パスからプライベート AS 番号を削除するように外部ネイバーを設定するには、**neighbor remove-private-as** ルータ コンフィギュレーション コマンドを使用します。この結果、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号は廃棄されます。

AS が別の AS からさらに別の AS にトラフィックを渡す場合は、アドバタイズ対象のルートに矛盾が存在しないことが重要です。BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかったトラフィックを受信することがあります。このような事態を避けるため、BGP は IGP が AS に情報を伝播し、BGP が IGP と*同期化*されるまで、待機する必要があります。同期化はデフォルトでイネーブルになっています。AS が特定の AS から別の AS にトラフィックを渡さない場合、または自律システム内のすべてのルータで BGP が稼動している場合は、同期化をディセーブルにし、IGP 内で伝送されるルートを少なくして、BGP がより短時間で収束するようにします。

BGP ルーティングをイネーブルにして BGP ルーティング プロセスを確立し、ネイバーを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします（IP ルーティングがディセーブルになっている場合に限り必要）。
ステップ 3	**router bgp** *autonomous-system*	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。指定できる AS 番号は 1 ～ 65535 です。64512 ～ 65535 はプライベート自律システム番号専用です。
ステップ 4	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]	この AS に対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。

	コマンド	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	BGP ネイバー テーブルに設定を追加し、IP アドレスによって識別されるネイバーが、指定された AS に属することを示します。 EBGP の場合、通常ネイバーは直接接続されており、IP アドレスは接続のもう一方の端におけるインターフェイスのアドレスです。 IBGP の場合、IP アドレスに任意のルータ インターフェイスのアドレスを指定できます。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remove-private-as**	（任意）発信ルーティング アップデート内の AS パスからプライベート AS 番号を削除します。
ステップ 7	**no synchronization**	（任意）BGP と IGP の間の同期をディセーブルにします。
ステップ 8	**no auto-summary**	（任意）自動ネットワーク サマライズをディセーブルにします。デフォルトでは、IGP から BGP にサブネットが再配信された場合、ネットワーク ルートだけが BGP テーブルに挿入されます。
ステップ 9	**bgp fast-external-fallover**	（任意）外部ネイバー間のリンクがダウンした場合に、BGP セッションを自動的にリセットします。デフォルトでは、セッションがただちにリセットされることはありません。
ステップ 10	**bgp graceful-restart**	（任意）スイッチでの NSF 認識をイネーブルにします。デフォルトでは、NSF 認識はディセーブルになっています。
ステップ 11	**end**	特権 EXEC モードに戻ります。

ステップ 12	**show ip bgp network** *network-number*
	または
	show ip bgp neighbor
		設定を確認します。
		NSF 認識（グレースフル リスタート）がネイバーでイネーブルになっていることを確認します。
		スイッチおよびネイバーで NSF 認識がイネーブルになっている場合は、次のメッセージが表示されます。
		`Graceful Restart Capability: advertised and received`
		NSF 認識がスイッチではイネーブルになっているが、ネイバーではディセーブルになっている場合は、次のメッセージが表示されます。
		`Graceful Restart Capability: advertised`

ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BGP AS を削除するには、**no router bgp** *autonomous-system* グローバル コンフィギュレーション コマンドを使用します。BGP テーブルからネットワークを削除するには、**no network** *network-number* ルータ コンフィギュレーション コマンドを使用します。ネイバーを削除するには、**no neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number* ルータ コンフィギュレーション コマンドを使用します。ネイバーにアップデート内のプライベート AS 番号を追加するには、**no neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** ルータ コンフィギュレーション コマンドを使用します。同期を再度イネーブルにするには、**synchronization** ルータ コンフィギュレーション コマンドを使用します。

次に、図 41-5 に示されたルータ上で BGP を設定する例を示します。

ルータ A：

```
Switch(config)# router bgp 100
Switch(config-router)# neighbor 129.213.1.1 remote-as 200
```

ルータ B：

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 129.213.1.2 remote-as 100
Switch(config-router)# neighbor 175.220.1.2 remote-as 200
```

ルータ C：

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 175.220.212.1 remote-as 200
Switch(config-router)# neighbor 192.208.10.1 remote-as 300
```

ルータ D：

```
Switch(config)# router bgp 300
Switch(config-router)# neighbor 192.208.10.2 remote-as 200
```

BGP ピアが稼動していることを確認するには、**show ip bgp neighbors** 特権 EXEC コマンドを使用します。次に、ルータ A に対してこのコマンドを実行した場合の出力を示します。

```
Switch# show ip bgp neighbors

BGP neighbor is 129.213.1.1, remote AS 200, external link
 BGP version 4, remote router ID 175.220.212.1
 BGP state = established, table version = 3, up for 0:10:59
 Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
 Minimum time between advertisement runs is 30 seconds
 Received 2828 messages, 0 notifications, 0 in queue
 Sent 2826 messages, 0 notifications, 0 in queue
 Connections established 11; dropped 10
```

state = *established* 以外の情報が出力された場合、ピアは稼動していません。リモート ルータ ID は、ルータ（または最大のループバック インターフェイス）上の最大の IP アドレスです。テーブルが新しい情報で更新されるたびに、テーブルのバージョン番号が増加します。テーブルのバージョン番号が継続的に増加している場合は、ルートがフラッピングし、ルーティング アップデートが絶えず発生しています。

外部プロトコルの場合、**network** ルータ コンフィギュレーション コマンドによる IP ネットワークへの参照で制御されるのは、アドバタイズされるネットワークだけです。これは、Interior Gateway Protocol（IGP）とは対照的です。EIGRP などの IGP でも、**network** コマンドを使用してアップデートの送信先を指定します。

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Routing Protocols」を参照してください。特定のコマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。スイッチ プロンプトで疑問符を入力した場合に表示されるにもかかわらず、このスイッチでサポートされない BGP コマンドのリストについては、付録 C「Cisco IOS Release 12.2(55)SE でサポートされていないコマンド」を参照してください。

ルーティング ポリシーの変更の管理

ピアのルーティング ポリシーには、着信または発信ルーティング テーブルのアップデートに影響する可能性があるすべての設定が含まれます。BGP ネイバーとして定義された 2 台のルータは、BGP 接続を形成し、ルーティング情報を交換します。あとで BGP のフィルタ、重み、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行う場合は、BGP セッションをリセットし、設定の変更を有効にする必要があります。

リセットには、ハード リセットとソフト リセットの 2 種類があります。このスイッチでは、事前に設定を行わなくても、ソフト リセットを使用できます。事前設定を行わずにソフト リセットを使用するには、両方の BGP ピアでソフト ルート リフレッシュ機能がサポートされている必要があります。この機能は、ピアによって TCP セッションが確立されたときに送信される OPEN メッセージでアドバタイズされます。ソフト リセットを使用すると、BGP ルータ間でルート リフレッシュ要求やルーティング情報をダイナミックに交換したり、それぞれの発信ルーティング テーブルをあとで再アドバタイズしたりすることができます。

- ソフト リセットによってネイバーから着信アップデートが生成される場合のリセットを、*ダイナミック着信ソフト リセット*といいます。
- ソフト リセットによってネイバーに一連のアップデートが送信される場合のリセットを、*発信ソフト リセット*といいます。

ソフト着信リセットが発生すると、新しい着信ポリシーが有効になります。ソフト発信リセットが発生すると、BGP セッションがリセットされずに、新しいローカル発信ポリシーが有効になります。発信ポリシーのリセット中に一連の新しいアップデートが送信されると、新しい着信ポリシーも有効になる場合があります。

表 41-10 に、ハード リセットとソフト リセットの利点と欠点を示します。

表 41-10　ハード リセットとソフト リセットの利点と欠点

リセットのタイプ	利点	欠点
ハード リセット	メモリ オーバーヘッドが発生しません。	ネイバーから提供された BGP、IP、および Forwarding Information Base（FIB; 転送情報ベース）テーブルのプレフィクスが失われます。ハード リセットの使用は推奨しません。
発信ソフト リセット	ルーティング テーブルのアップデートが設定されず、保管もされません。	着信ルーティング テーブルのアップデートがリセットされません。
ダイナミック着信ソフト リセット	BGP セッションおよびキャッシュがクリアされません。 ルーティング テーブルのアップデートを保管する必要がなく、メモリ オーバーヘッドが発生しません。	両方の BGP ルータでルート リフレッシュ機能をサポートする必要があります。

BGP ピアがルート リフレッシュ機能をサポートしているかどうかの確認や、BGP セッションのリセットを行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**show ip bgp neighbors**	ネイバーがルート リフレッシュ機能をサポートしているかどうかを表示します。サポートされている場合は、ルータに関する次のメッセージが表示されます。 *Received route refresh capability from peer.*
ステップ 2	**clear ip bgp** {***** | *address* | *peer-group-name*}	指定された接続のルーティング テーブルをリセットします。 • すべての接続をリセットする場合は、アスタリスク（*）を入力します。 • 特定の接続をリセットする場合は、IP *アドレス*を入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 3	**clear ip bgp** {***** | *address* | *peer-group-name*} **soft out**	（任意）指定された接続の着信ルーティング テーブルをリセットするには、発信ソフト リセットを実行します。このコマンドは、ルート リフレッシュがサポートされている場合に使用してください。 • すべての接続をリセットする場合は、アスタリスク（*）を入力します。 • 特定の接続をリセットする場合は、IP *アドレス*を入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 4	**show ip bgp** **show ip bgp neighbors**	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断属性の設定

BGP スピーカーが複数の自律システムから受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達するための最適パスを 1 つ選択する必要があります。選択されたパスは BGP ルーティング テーブルに格納され、ネイバーに伝播されます。この判断は、アップデートに格納されている属性値、および BGP で設定可能な他の要素に基づいて行われます。

BGP ピアは、1 つのプレフィクスに対して 2 つの EBGP パスをネイバー AS から学習する場合、最適パスを選択して IP ルーティング テーブルに挿入します。BGP マルチパス サポートがイネーブルで、同じネイバー AS から複数の EBGP パスを学習する場合、単一の最適パスではなく、複数のパスが IP ルーティング テーブルに格納されます。そのあと、パケット スイッチング中に、複数のパス間でパケット単位または宛先単位のロード バランシングが実行されます。**maximum-paths** ルータ コンフィギュレーション コマンドは、許可されるパス数を制御します。

BGP が最適パスを選択する際に属性を評価する順序を次に示します。

1. パスで指定されているネクストホップにアクセス不能な場合、アップデートが削除されます。BGP のネクストホップ属性（ソフトウェアによって自動判別される）は、宛先に到達するために使用されるネクストホップの IP アドレスです。EBGP の場合、このアドレスは通常、**neighbor remote-as** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクストホップ処理をディセーブルにするには、ルート マップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。
2. 重みが最大のパスが優先されます（シスコ独自のパラメータ）。重み属性はルータにローカルであるため、ルーティング アップデートでは伝播されません。デフォルトでは、ルータ送信元のパスに対する重み属性は 32768 で、その他のパスに対する重み属性は 0 です。重みが最大のルートが優先されます。重みを設定するには、アクセス リスト、ルート マップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。

3. ローカル プリファレンスが最大のルートが優先されます。ローカル プリファレンスはルーティング アップデートに含まれ、同じ AS 内のルータ間で交換されます。ローカル プリファレンス属性のデフォルト値は 100 です。ローカル プリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルート マップを使用します。
4. ローカル ルータで実行されている BGP から送信されたルートが優先されます。
5. AS パスが最短のルートが優先されます。
6. 送信元のタイプが最小のルートが優先されます。内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP によって学習されたルートは、不明な送信元のルートや別の方法で学習されたルートよりも小さくなります。
7. 想定されるすべてのルートのネイバー AS が同じである場合は、Multi Exit Discriminator（MED）メトリック属性が最小のルートが優先されます。MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。
8. 内部（IBGP）パスより外部（EBGP）パスが優先されます。
9. 最も近い IGP ネイバー（最小の IGP メトリック）を経由して到達できるルートが優先されます。つまり、ルータは、宛先に到達するための AS 内の最短の内部パス（BGP のネクストホップへの最短パス）を優先します。
10. 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入してください。
    - 最適ルートと対象のルートがともに外部ルートである。
    - 最適ルートと対象のルートの両方が、同じネイバー AS（自律システム）からのルートである。
    - maximum-paths がイネーブルである。
11. マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレス値が最小のルートが優先されます。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック（仮想）アドレスですが、実装に依存する場合があります。

判断属性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp best-path as-path ignore**	（任意）ルートの選択中に AS パスの長さを無視するようにルータを設定します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	（任意）ネクストホップ アドレスの代わりに使用する特定の IP アドレスを入力し、ネイバーへの BGP アップデートに対するネクストホップ処理をディセーブルにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **weight** *weight*	（任意）ネイバー接続に重みを割り当てます。指定できる値は 0 ～ 65535 です。重みが最大のルートが優先されます。別の BGP ピアから学習したルートのデフォルトの重みは 0、ローカル ルータから送信されたルートのデフォルトの重みは 32768 です。
ステップ 6	**default-metric** *number*	（任意）優先パスを外部ネイバーに設定するように MED メトリックを設定します。MED が設定されていないルートも、すべてこの値に設定されます。指定できる範囲は 1 ～ 4294967295 です。最小値のルートが最優先されます。

	コマンド	目的
ステップ 7	**bgp bestpath med missing-as-worst**	（任意）MED が設定されていないパスは無限の値が設定されていると見なし、そのパスの優先順位が最も低くなるようにスイッチを設定します。
ステップ 8	**bgp always-compare med**	（任意）自律システムが異なるネイバーからのパスの MED を比較するようにスイッチを設定します。デフォルトでは、MED の比較は同じ AS 内のパス間でだけ行われます。
ステップ 9	**bgp bestpath med confed**	（任意）連合内の異なるサブ自律システムによってアドバタイズされたパスから特定のパスを選択する場合に、MED を考慮するようにスイッチを設定します。
ステップ 10	**bgp deterministic med**	（任意）同じ AS 内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。
ステップ 11	**bgp default local-preference** *value*	（任意）デフォルトのローカル プリファレンス値を変更します。指定できる範囲は 0 ～ 4294967295 です。デフォルト値は 100 です。最大のローカル プリファレンス値が優先されます。
ステップ 12	**maximum-paths** *number*	（任意）IP ルーティング テーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティング テーブルに格納されます。指定できる範囲は 1 ～ 16 です。パスの数を複数に設定すると、パス間のロード バランシングが可能になります（スイッチ ソフトウェアでは最大 32 の等価コスト ルートを使用できますが、スイッチ ハードウェアでは 1 ルートあたり 17 以上のパスは使用しません）。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show ip bgp** **show ip bgp neighbors**	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 15	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト ステートに戻すには、各コマンドの **no** 形式を使用します。

ルート マップによる BGP フィルタリングの設定

BGP 内でルート マップを使用すると、ルーティング情報の制御や変更を行ったり、ルーティング ドメイン間でルートを再配信する条件を定義したりすることができます。ルート マップの詳細については、「ルート マップによるルーティング情報の再配信」（P.41-94）を参照してください。各ルート マップには、ルート マップを識別する名前（*マップ タグ*）とオプションのシーケンス番号が付いています。

ルート マップを使用してネクストホップ処理をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [[**permit** | **deny**] | *sequence-number*]]	ルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**set ip next-hop** *ip-address* [*...ip-address*] [**peer-address**]	（任意）ネクストホップ処理をディセーブルにするようにルート マップを設定します。 • 着信ルート マップの場合は、一致するルートのネクストホップをネイバー ピアリング アドレスに設定し、サードパーティのネクストホップを上書きします。 • BGP ピアの発信ルート マップの場合は、ネクストホップをローカル ルータのピアリング アドレスに設定し、ネクストホップ計算をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show route-map** [*map-name*]	設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示して、設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルート マップを削除するには、**no route-map** *map-tag* コマンドを使用します。ネクストホップ処理を再びイネーブルにするには、**no set ip next-hop** *ip-address* コマンドを使用します。

ネイバーによる BGP フィルタリングの設定

BGP アドバタイズをフィルタリングするには、**as-path access-list** グローバル コンフィギュレーション コマンドや **neighbor filter-list** ルータ コンフィギュレーション コマンドなどの AS パス フィルタを使用します。**neighbor distribute-list** ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。distribute-list フィルタはネットワーク番号に適用されます。**distribute-list** コマンドの詳細については、「ルーティング アップデートのアドバタイズおよび処理の制御」（P.41-102）を参照してください。

ネイバー単位でルート マップを使用すると、アップデートのフィルタリングや、各属性の変更を行うことができます。ルート マップは、着信アップデートまたは発信アップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデート内で送受信されます。着信および発信の両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。AS パスのマッチングには **match as-path access-list** ルート マップ コマンドが、コミュニティに基づくマッチングには **match community-list** ルート マップ コマンドが、ネットワークに基づくマッチングには **ip access-list** グローバル コンフィギュレーション コマンドがそれぞれ必要です。

ネイバー単位のルート マップを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** {*ip-address* | *peer-group name*} **distribute-list** {*access-list-number* | *name*} {**in** | **out**}	（任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。 **（注）** **neighbor prefix-list** ルータ コンフィギュレーション コマンドを使用してアップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定することはできません。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **route-map** *map-tag* {**in** | **out**}	（任意）ルート マップを適用し、着信または発信ルートをフィルタリングします。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ネイバーからアクセス リストを削除するには、**no neighbor distribute-list** コマンドを使用します。ネイバーからルート マップを削除するには、**no neighbor route-map** *map-tag* ルータ コンフィギュレーション コマンドを使用します。

BGP AS パスに基づいて着信および発信の両方のアップデートにアクセス リスト フィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現に基づくアクセス リストです（正規表現の作成方法の詳細については、『*Cisco IOS Dial Technologies Command Reference, Release 12.2*』の付録「Regular Expressions」を参照してください。この方法を使用するには、AS パスのアクセス リストを定義し、特定のネイバーに対して送受信されるアップデートに適用します）。

BGP パス フィルタリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip as-path access-list** *access-list-number* {**permit** | **deny**} *as-regular-expressions*	BGP 関連アクセス リストを定義します。
ステップ 3	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **filter-list** {*access-list-number* | *name*} {**in** | **out** | **weight** *weight*}	アクセス リストに基づいて、BGP フィルタを確立します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** [**paths** *regular-expression*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BGP フィルタリング用のプレフィクス リストの設定

neighbor distribute-list ルータ コンフィギュレーション コマンドを含む多数の BGP ルート フィルタリング コマンドでは、アクセス リストの代わりにプレフィクス リストを使用できます。プレフィクス リストを使用すると、大規模なリストのロードや検索のパフォーマンスが改善する、差分更新がサポートされる、CLI（コマンドライン インターフェイス）設定が簡素化される、柔軟性が増すなどの利点が生じます。

プレフィクス リストによるフィルタリングでは、アクセス リストを照合する場合と同様に、プレフィクス リストに記載されたプレフィクスとルートのプレフィクスが照合されます。一致が存在する場合は、一致したルートが使用されます。プレフィクスが許可されるか拒否されるかは、次に示すルールに基づいて決定されます。

- 空のプレフィクス リストはすべてのプレフィクスを許可する。
- 指定されたプレフィクスがプレフィクス リスト内のどのエントリとも一致しない場合は、暗黙拒否が使用される。
- プレフィクス リストの複数のエントリが指定されたプレフィクスと一致する場合は、シーケンス番号が最小のプレフィクス リスト エントリが特定される。

デフォルトでは、シーケンス番号が自動生成されます。デフォルトの増分単位は 5 です。シーケンス番号の自動生成をディセーブルにした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号の増分単位には任意の値を指定できます。増分単位に 1 を指定すると、リストに追加エントリを挿入できなくなります。増分単位に非常に大きい値を指定すると、値が足りなくなることがあります。

コンフィギュレーション エントリを削除する場合は、シーケンス番号を指定する必要はありません。**show** コマンドの出力には、シーケンス番号が含まれます。

コマンド内でプレフィクス リストを使用する場合は、あらかじめプレフィクス リストを設定しておく必要があります。プレフィクス リストの作成や、プレフィクス リストへのエントリの追加を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip prefix-list** *list-name* [**seq** *seq-value*] **deny** | **permit** *network*/*len* [**ge** *ge-value*] [**le** *le-value*]	シーケンス番号（任意）を指定してプレフィクス リストを作成し、条件が一致する場合のアクセスを拒否（**deny**）または許可（**permit**）します。**permit** コマンド**deny** コマンドを少なくとも 1 つ入力する必要があります。 • *network*/*len* は、ネットワーク番号およびネットワーク マスクの長さ（ビット単位）です。 • （任意）**ge** および **le** の値は、照合するプレフィクス長の範囲を指定します。*ge-value* および *le-value* に指定する値は、次の条件を満たす必要があります。*len* < *ge-value* < *le-value* < 32
ステップ 3	**ip prefix-list** *list-name* **seq** *seq-value* **deny** | **permit** *network*/*len* [**ge** *ge-value*] [**le** *le-value*]	（任意）プレフィクス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip prefix list** [**detail** | **summary**] *name* [*network*/*len*] [**seq** *seq-num*] [**longer**] [**first-match**]	プレフィクス リストまたはプレフィクス リスト エントリに関する情報を表示して、設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

プレフィクス リストとそのエントリをすべて削除するには、**no ip prefix-list** *list-name* グローバル コンフィギュレーション コマンドを使用します。プレフィクス リストからエントリを削除するには、**no ip prefix-list seq** *seq-value* グローバル コンフィギュレーション コマンドを使用します。シーケンス番号の自動生成をディセーブルにするには **no ip prefix-list sequence number** コマンドを、自動生成を再びイネーブルにするには **ip prefix-list sequence number** コマンドを使用します。プレフィクス リスト エントリのヒット数テーブルをクリアするには、**clear ip prefix-list** 特権 EXEC コマンドを使用します。

BGP コミュニティ フィルタリングの設定

BGP コミュニティ フィルタリングは、COMMUNITIES 属性の値に基づいて、BGP でルーティング情報の配信を制御する方法の 1 つです。この属性によって、宛先がコミュニティにグループ化され、コミュニティに基づいてルーティング判断が適用されます。この方法を使用すると、ルーティング情報の配信制御を目的とする BGP スピーカーの設定が簡単になります。

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。各宛先は複数のコミュニティに属することができます。AS 管理者は、宛先が属するコミュニティを定義できます。デフォルトでは、すべての宛先が一般的なインターネット コミュニティに属します。コミュニティは、COMMUNITIES 属性（任意）によって識別されます。この属性は推移的かつグローバルで、その範囲は 1 ～ 4294967200 です。事前に定義されている既知のコミュニティの一部を次に示します。

- **internet**：対象のルートをインターネット コミュニティにアドバタイズします。すべてのルータがこのコミュニティに属します。
- **no-export**：EBGP ピアに対象のルートをアドバタイズしません。
- **no-advertise**：ピア（内部または外部）に対象のルートをアドバタイズしません。
- **local-as**：ローカル自律システムの外部のピアに対象のルートをアドバタイズしません。

許可するルーティング情報、他のネイバーよりも優先するルーティング情報、または他のネイバーに配信するルーティング情報は、コミュニティに基づいて制御できます。BGP スピーカーは、ルートの学習、アドバタイズ、または再配信を行うときに、ルートのコミュニティの設定、追加、または変更を行う場合があります。ルートを集約すると、その集約の COMMUNITIES 属性に、すべての初期ルートの全コミュニティが含まれるようになります。

コミュニティ リストを使用すると、ルート マップの match コマンドで使用するコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成することもできます。一致が見つかるまでステートメントがチェックされ、いずれかのステートメントで一致が見つかり次第、テストが終了します。

COMMUNITIES 属性および match コマンドをコミュニティに基づいて設定する場合は、「ルート マップによるルーティング情報の再配信」（P.41-94）に記載されている **match community-list** および **set community** ルート マップ コンフィギュレーション コマンドを参照してください。

デフォルトでは、COMMUNITIES 属性はネイバーに送信されません。COMMUNITIES 属性が特定の IP アドレスのネイバーに送信されるように指定するには、**neighbor send-community** ルータ コンフィギュレーション コマンドを使用します。

コミュニティ リストの作成および適用を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip community-list** *community-list-number* {**permit** | **deny**} *community-number*	コミュニティ リストを作成し、番号を割り当てます。 • *community-list-number* は 1 ～ 99 の整数です。この値によって、コミュニティの許可グループまたは拒否グループが 1 つまたは複数識別されます。 • *community-number* は、**set community** ルート マップ コンフィギュレーション コマンドで設定される番号です。
ステップ 3	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **send-community**	この IP アドレスのネイバーに COMMUNITIES 属性を送信することを指定します。
ステップ 5	**set comm-list** *list-num* **delete**	（任意）ルート マップで指定された標準または拡張コミュニティ リストと一致する着信または発信アップデートのコミュニティ属性から、コミュニティを削除します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 7	**ip bgp-community new-format**	（任意）AA:NN の形式で、BGP コミュニティを表示および解析します。 BGP コミュニティは、2 つの部分からなる 2 バイト長の形式で表示されます。シスコのデフォルトのコミュニティの形式は NNAA です。BGP に関する最新の RFC では、コミュニティは AA:NN の形式をとります。最初の部分は AS 番号で、その次の部分は 2 バイトの数値です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp community**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BGP ネイバーおよびピア グループの設定

通常、BGP ネイバーの多くは同じアップデート ポリシー（同じ発信ルート マップ、配信リスト、フィルタ リスト、アップデート送信元など）を使用して設定されます。アップデート ポリシーが同じネイバーをピア グループにまとめると設定が簡単になり、アップデートの効率が高まります。多数のピアを設定した場合は、この方法を推奨します。

BGP ピア グループを設定するには、ピア グループを作成してオプションを割り当て、ピア グループ メンバーとしてネイバーを追加します。ピア グループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。デフォルトでは、ピア グループ メンバーは remote-as（設定されている場合）、version、update-source、out-route-map、out-filter-list、out-dist-list、minimum-advertisement-interval、next-hop-self など、ピア グループの設定オプションをすべて継承します。すべてのピア グループ メンバーは、ピア グループに対して行われた変更も継承します。また、発信アップデートに影響しないオプションを無効にするように、メンバーを設定することもできます。

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用し、次に示すルータ コンフィギュレーション コマンドのいずれかを指定します。ピア グループにオプションを割り当てるには、ピア グループ名を使用し、いずれかのコマンドを指定します。**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用すると、すべての設定情報を削除せずに、BGP ピアまたはピア グループをディセーブルにできます。

BGP ピアを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** *peer-group-name* **peer-group**	BGP ピア グループを作成します。
ステップ 4	**neighbor** *ip-address* **peer-group** *peer-group-name*	BGP ネイバーをピア グループのメンバーにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	BGP ネイバーを指定します。ピア グループが **remote-as** *number* を使用して設定されていない場合は、このコマンドを使用して、EBGP ネイバーを含むピア グループを作成します。指定できる範囲は 1 ～ 65535 です。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **description** *text*	（任意）ネイバーに説明を関連付けます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]	（任意）BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

	コマンド	目的
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに COMMUNITIES 属性を送信することを指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface*	（任意）内部 BGP セッションで、TCP 接続用の操作インターフェイスをすべて使用できるようにします。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop**	（任意）ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを許可します。マルチホップ ピアのアドレスへの唯一のルートがデフォルト ルート（0.0.0.0）の場合、マルチホップ セッションは確立されません。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **local-as** *number*	（任意）ローカル AS として使用する AS 番号を指定します。指定できる範囲は 1 ～ 65535 です。
ステップ 12	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*	（任意）BGP ルーティング アップデートを送信する最小間隔を設定します。
ステップ 13	**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*]	（任意）ネイバーから受信できるプレフィクス数を制御します。指定できる範囲は 1 ～ 4294967295 です。*threshold*（任意）は最大割合を表します。この値に達すると警告メッセージが生成されます。デフォルト値は 75% です。
ステップ 14	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	（任意）ネイバーに対する BGP アップデートでのネクストホップ処理をディセーブルにします。
ステップ 15	**neighbor** {*ip-address* | *peer-group-name*} **password** *string*	（任意）TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間の接続が作成されません。
ステップ 16	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}	（任意）着信または発信ルートにルート マップを適用します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに COMMUNITIES 属性を送信することを指定します。
ステップ 18	**neighbor** {*ip-address* | *peer-group-name*} **timers** *keepalive holdtime*	（任意）ネイバーまたはピア グループ用のタイマーを設定します。 • *keepalive* インターバルで指定した時間内に、キープアライブ メッセージがピアに送信されます。指定できる範囲は 1 ～ 4294967295 です。デフォルトは 60 秒です。 • *holdtime* は、ピアからのキープアライブ メッセージを受信しなかった場合に、そのピアを非アクティブと宣言するまでの間隔です。指定できる範囲は 1 ～ 4294967295 です。デフォルトは 180 秒です。
ステップ 19	**neighbor** {*ip-address* | *peer-group-name*} **weight** *weight*	（任意）ネイバーからのすべてのルートに対する重みを指定します。
ステップ 20	**neighbor** {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *name*} {**in** | **out**}	（任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。
ステップ 21	**neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out** | **weight** *weight*}	（任意）BGP フィルタを確立します。
ステップ 22	**neighbor** {*ip-address* | *peer-group-name*} **version** *value*	（任意）ネイバーと通信するときに使用する BGP バージョンを指定します。
ステップ 23	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**	（任意）受信したアップデートの保管を開始するようにソフトウェアを設定します。

	コマンド	目的
ステップ 24	**end**	特権 EXEC モードに戻ります。
ステップ 25	**show ip bgp neighbors**	設定を確認します。
ステップ 26	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

既存の BGP ネイバーまたはネイバー ピア グループをディセーブルにするには、**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。ディセーブルになっている既存のネイバーまたはネイバー ピア グループをイネーブルにするには、**no neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。

集約アドレスの設定

クラスレス ドメイン間ルーティング（CIDR）を使用すると、集約ルート（またはスーパーネット）を作成して、ルーティング テーブルのサイズを最小にすることができます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配信するか、BGP ルーティング テーブル内に集約エントリを作成します。BGP テーブル内に特定のエントリがさらに 1 つ以上存在する場合は、BGP テーブルに集約アドレスが追加されます。

ルーティング テーブル内に集約アドレスを作成するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**aggregate-address** *address mask*	BGP ルーティング テーブル内に集約エントリを作成します。集約ルートは、AS からのルートとしてアドバタイズされます。情報が失われた可能性があることを示すために、アトミック集約属性が設定されます。
ステップ 4	**aggregate-address** *address mask* **as-set**	（任意）AS 設定パス情報を生成します。このコマンドは、前のコマンドと同じルールに従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET になります。このルートは絶えず取り消しや更新を行う必要があるため、多数のパスを集約する場合は、このキーワードを使用しないでください。
ステップ 5	**aggregate-address** *address-mask* **summary-only**	（任意）サマリー アドレスだけをアドバタイズします。
ステップ 6	**aggregate-address** *address mask* **suppress-map** *map-name*	（任意）選択された、より具体的なルートを抑制します。
ステップ 7	**aggregate-address** *address mask* **advertise-map** *map-name*	（任意）ルート マップによって指定された条件に基づいて、集約を生成します。
ステップ 8	**aggregate-address** *address mask* **attribute-map** *map-name*	（任意）ルート マップで指定された属性を持つ集約を生成します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp neighbors** [**advertised-routes**]	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

集約エントリを削除するには、**no aggregate-address** *address mask* ルータ コンフィギュレーション コマンドを使用します。オプションをデフォルト値に戻すには、キーワードを指定してコマンドを使用します。

ルーティング ドメイン連合の設定

IBGP メッシュを減らす方法の 1 つは、自律システムを複数のサブ自律システムに分割し、単一の自律システムとして認識される単一の連合にグループ化することです。各自律システムの内部はフル メッシュ構造になっており、同じ連合内の他の自律システムへの接続がいくつか確立されます。異なる自律システム内のピアでは EBGP セッションが使用されますが、ルーティング情報は IBGP ピアと同様の方法で交換されます。特に、ネクストホップ、MED、およびローカル プリファレンス情報が維持されるため、すべての自律システムで単一の IGP を使用できます。

BGP 連合を設定するには、自律システム グループの自律システム番号として機能する連合 ID を指定する必要があります。

BGP 連合を設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp confederation identifier** *autonomous-system*	BGP 連合 ID を設定します。
ステップ 4	**bgp confederation peers** *autonomous-system* [*autonomous-system ...*]	連合に属する自律システムと、特殊な EBGP ピアとして処理する自律システムを指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbor** **show ip bgp network**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BGP ルート リフレクタの設定

BGP では、すべての IBGP スピーカーをフル メッシュ構造にする必要があります。外部ネイバーからルートを受信したルータは、そのルートをすべての内部ネイバーにアドバタイズする必要があります。ルーティング情報のループを防止するには、すべての IBGP スピーカーを接続する必要があります。内部ネイバーは、内部ネイバーから学習したルートを他の内部ネイバーに送信しません。

ルート リフレクタを使用する場合は、すべての IBGP スピーカーをフル メッシュ構造にする必要がありません。学習したルートをネイバーに渡す場合に別の方法が使用されるためです。*ルート リフレクタ*に設定された内部 BGP ピアは、IBGP によって学習されたルートを一連の IBGP ネイバーに送信します。ルート リフレクタの内部ピアは、*クライアント ピア*と*非クライアント ピア*（自律システム内の他のすべてのルータ）の 2 つのグループに分類されます。ルート リフレクタは、これらの 2 つのグループ間でルートを反映します。ルート リフレクタとそのクライアント ピアは、*クラスタ*を形成します。非クライアント ピアは相互にフル メッシュ構造にする必要がありますが、クライアント ピアはその必要はありません。クラスタ内のクライアントは、そのクラスタ外の IBGP スピーカーと通信しません。

アドバタイズされたルートを受信したルート リフレクタでは、ネイバーに応じて、次のいずれかの処理が実行されます。

- 外部 BGP スピーカーからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズする。
- 非クライアント ピアからのルートをすべてのクライアントにアドバタイズする。
- クライアントからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズする（したがって、クライアントをフル メッシュ構造にする必要はありません）。

通常、クライアントのクラスタにはルート リフレクタが 1 つあり、クラスタはルート リフレクタのルータ ID で識別されます。冗長性を高めて、シングル ポイント障害を回避するために、複数のルート リフレクタをクラスタに設定する場合があります。このように設定した場合は、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるように、クラスタ内のすべてのルート リフレクタに同じクラスタ ID（4 バイト）を設定する必要があります。クラスタとして機能するルート リフレクタは、すべてフル メッシュ構造にする必要があります。また、一連の同一なクライアント ピアと非クライアント ピアを設定する必要があります。

ルート リフレクタおよびクライアントを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** *ip-address* | *peer-group-name* **route-reflector-client**	ローカル ルータを BGP ルート リフレクタに、指定されたネイバーをクライアントに設定します。
ステップ 4	**bgp cluster-id** *cluster-id*	（任意）クラスタに複数のルート リフレクタが存在する場合、クラスタ ID を設定します。
ステップ 5	**no bgp client-to-client reflection**	（任意）クライアント間のルート リフレクションをディセーブルにします。デフォルトでは、ルート リフレクタ クライアントからのルートが他のクライアントに反映されます。ただし、クライアントがフル メッシュ構造の場合、ルート リフレクタはクライアントにルートを反映する必要がありません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp**	設定を確認します。送信元 ID とクラスタ リスト属性を表示します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルート ダンプニングの設定

ルート フラップ ダンプニングは、インターネットワーク全体にフラッピング ルートが伝播するのを最小限に抑えるための BGP 機能です。ルートを使用できる状態と使用できない状態が交互に繰り返される場合、そのルートはフラッピングしていると見なされます。ルート ダンプニングがイネーブルになっている場合は、フラッピングしているルートに*ペナルティ*値が割り当てられます。ルートの累積ペナルティが制限値（設定可能）に達すると、そのルートが稼動している場合でも、BGP によってルートのアドバタイズが抑制されます。*再利用制限値*は、ペナルティと比較される設定可能な値です。ペナルティが再利用制限値よりも小さくなると、抑制されたルートが稼動中であれば、アドバタイズが再開されます。

ダンプニングは、IBGP によって学習されたルートには適用されません。このポリシーにより、IBGP ピアのペナルティが AS 外部のルートよりも大きくなることはありません。

BGP ルート ダンプニングを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp dampening**	BGP ルート ダンプニングをイネーブルにします。
ステップ 4	**bgp dampening** *half-life reuse suppress max-suppress* [**route-map** *map*]	（任意）ルート ダンプニングの各要素のデフォルト値を変更します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp flap-statistics** [{**regexp** *regexp*} | {**filter-list** *list*} | {*address mask* [**longer-prefix**]}]	（任意）フラッピングしているすべてのパスのフラップをモニタします。ルートの抑制が終了し、安定状態になると、統計情報が削除されます。
ステップ 7	**show ip bgp dampened-paths**	（任意）ダンプニングされたルートを表示します（抑制されるまでの時間も表示されます）。
ステップ 8	**clear ip bgp flap-statistics** [{**regexp** *regexp*} | {**filter-list** *list*} | {*address mask* [**longer-prefix**]}	（任意）BGP フラップ統計情報を消去して、ルートがダンプニングされる可能性を小さくします。
ステップ 9	**clear ip bgp dampening**	（任意）ルート ダンプニング情報を消去して、ルートの抑制を解除します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フラップ ダンプニングをディセーブルにするには、キーワードを指定せずに **no bgp dampening** ルータ コンフィギュレーション コマンドを使用します。ダンプニングの各要素をデフォルト値に戻すには、値を指定して **no bgp dampening** ルータ コンフィギュレーション コマンドを使用します。

BGP のモニタおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。この作業は、特定の構造の内容が無効になる場合、または無効である疑いがある場合に必要となります。

BGP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。リソースの利用率を取得したり、ネットワークの問題を解決するための情報を使用することもできます。さらに、ノードの到達可能性に関する情報を表示し、装置のパケットがネットワーク上で通過するルーティング パスを検出することもできます。

表 41-8 に、BGP を消去および表示するために使用する特権 EXEC コマンドを示します。表示フィールドの詳細については、Cisco.com のホーム ページにアクセスして、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）。

表 41-11　IP BGP の clear および show コマンド

コマンド	目的
clear ip bgp *address*	特定の BGP 接続をリセットします。
clear ip bgp *	すべての BGP 接続をリセットします。
clear ip bgp peer-group *tag*	BGP ピア グループのすべてのメンバーを削除します。

表 41-11　IP BGP の clear および show コマンド （続き）

コマンド	目的
show ip bgp *prefix*	プレフィクスがアドバタイズされている、ピア グループおよびピア グループに含まれないピアを表示します。ネクストホップやローカル プレフィクスなどのプレフィクス属性も表示されます。
show ip bgp cidr-only	サブネットおよびスーパーネットのネットワーク マスクを含むすべての BGP ルートを表示します。
show ip bgp community [*community-number*] [**exact**]	指定されたコミュニティに属するルートを表示します。
show ip bgp community-list *community-list-number* [**exact-match**]	コミュニティ リストで許可されたルートを表示します。
show ip bgp filter-list *access-list-number*	指定された AS パス アクセス リストによって照合されたルートを表示します。
show ip bgp inconsistent-as	送信元の自律システムと矛盾するルートを表示します。
show ip bgp regexp *regular-expression*	コマンドラインで入力された特定の正規表現と一致する AS パスを持つルートを表示します。
show ip bgp	BGP ルーティング テーブルの内容を表示します。
show ip bgp neighbors [*address*]	各ネイバーとの BGP 接続および TCP 接続に関する詳細情報を表示します。
show ip bgp neighbors [*address*] [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** *regular-expression* | **received-routes** | **routes**]	特定の BGP ネイバーから学習したルートを表示します。
show ip bgp paths	データベース内のすべての BGP パスを表示します。
show ip bgp peer-group [*tag*] [**summary**]	BGP ピア グループに関する情報を表示します。
show ip bgp summary	すべての BGP 接続のステータスを表示します。

また、**bgp log-neighbor changes** ルータ コンフィギュレーション コマンドを使用して、BGP ネイバーのリセット、起動、またはダウン時に生成されるメッセージのロギングをイネーブルにすることもできます。

ISO CLNS ルーティングの設定

International Organization for Standardization（ISO; 国際標準化機構）Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）プロトコルは、Open System Interconnection（OSI; 開放型システム間相互接続）モデルのネットワーク レイヤに関する標準です。ISO ネットワーク アーキテクチャでは、アドレスを Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）および Network Entity Title（NET）と呼びます。OSI ネットワーク内の各ノードには、1 つまたは複数の NET が 設定されます。また、NSAP アドレスも多数設定されます。

clns routing グローバル コンフィギュレーション コマンドを使用して、スイッチでのコネクションレス型ルーティングをイネーブルにした場合、スイッチはルーティング関連機能を実行せず、転送の判断だけを行います。ダイナミック ルーティングの場合は、ルーティング プロトコルもイネーブルにする必要があります。このスイッチは、ISO CLNS ネットワークの OSI ルーティング プロトコルに基づく Intermediate System-to-Intermediate System（IS-IS）ダイナミック ルーティング プロトコルをサポートしています。

ダイナミックにルーティングを行う場合は、IS-IS を使用します。このルーティング プロトコルは、*エリア*の概念をサポートしています。エリア内のすべてのルータは、すべてのシステム ID への到達方法を認識します。エリア間のルータは、適切なエリアへの到達方法を認識します。IS-IS は、*ステーション ルーティング*（エリア内）および*エリア ルーティング*（エリア間）の 2 つのレベルのルーティングをサポートしています。

ISO IGRP と IS-IS NSAP アドレッシング方式の主な違いは、エリア アドレスの定義です。どちらもレベル 1 ルーティング（エリア内ルーティング）にはシステム ID を使用しますが、エリア ルーティングにおけるアドレスの指定方法が異なります。ISO IGRP NSAP アドレスには、3 つの個別のルーティング用フィールド（*ドメイン*、*エリア*、*システム ID*）が含まれています。IS-IS アドレスには、2 つのフィールド（単一の連続した*エリア*フィールド（ドメイン フィールドとエリア フィールドで構成）、*システム ID*）が含まれています。

（注）　ISO CLNS の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide, Release 12.2*』を参照してください。この章で使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2*』を参照するか、IOS コマンド リファレンス マスター インデックスを使用するか、またはオンラインで検索してください。

IS-IS ダイナミック ルーティングの設定

IS-IS は ISO ダイナミック ルーティング プロトコルです（ISO 10589 を参照）。他のルーティング プロトコルとは異なり、IS-IS をイネーブルにするには、IS-IS ルーティング プロセスを作成し、ネットワークではなく、特定のインターフェイスに割り当てる必要があります。各レイヤ 3 スイッチまたはルータに複数の IS-IS ルーティング プロセスを指定するには、マルチエリア IS-IS 設定構文を使用します。次に、IS-IS ルーティング プロセスのインスタンスごとにパラメータを設定します。

小規模な IS-IS ネットワークは、ネットワーク内のすべてのルータを含む単一エリアとして作成されます。大規模になったネットワークは、通常、すべてのエリアから接続されているすべてのレベル 2 ルータで構成されるバックボーン エリアに再編成され、このバックボーン エリアからローカル エリアに接続されます。ローカル エリア内のルータは、すべてのシステム ID への到達方法を認識します。エリア間のルータはバックボーンへの到達方法を、バックボーン ルータは他のエリアへの到達方法を認識します。

ルータは、ローカル エリア内のルーティング（ステーション ルーティング）を実行する場合、レベル 1 隣接を確立します。レベル 1 エリア間のルーティング（エリア ルーティング）を実行する場合は、レベル 2 隣接を確立します。

単一の Cisco ルータは、最大 29 個のエリア内のルーティングに参加できます。また、バックボーンでは、レベル 2 ルーティングを実行できます。一般に、各ルーティング プロセスは 1 つのエリアに対応します。デフォルトでは、設定されたルーティング プロセスの最初のインスタンスによって、レベル 1 とレベル 2 の両方のルーティングが実行されます。追加のルータ インスタンスを設定することもでき、追加されたインスタンスはレベル 1 エリアとして自動的に処理されます。IS-IS ルーティング プロセスの各インスタンスのパラメータは、個別に設定する必要があります。

IS-IS マルチエリア ルーティングの場合、レベル 2 ルーティングを実行するように設定できるプロセスは 1 つだけです。ただし、各シスコ製装置にはレベル 1 エリアを 29 個まで定義できます。どのプロセスにもレベル 2 ルーティングが設定されている場合、すべての追加プロセスは自動的にレベル 1 として設定されます。このプロセスは、レベル 1 ルーティングを同時に実行するように設定できます。レベル 2 ルーティングがルータ インスタンスに対して適切でない場合は、**is-type** グローバル コンフィギュレーション コマンドを使用して、レベル 2 機能を削除します。レベル 2 ルータとして別のルータ インスタンスを設定する場合も、**is-type** コマンドを使用します。

（注）　IS-IS の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Routing Protocols」を参照してください。この項で使用しているコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference, Release 12.2*』を参照してください。

ここでは、IS-IS ルーティングの設定方法について簡単に説明します。内容は次のとおりです。

- 「IS-IS のデフォルト設定」（P.41-66）
- 「IS-IS ルーティングのイネーブル化」（P.41-67）
- 「IS-IS グローバル パラメータの設定」（P.41-69）
- 「IS-IS インターフェイス パラメータの設定」（P.41-72）

IS-IS のデフォルト設定

表 41-12 に、IS-IS のデフォルト設定を示します。

表 41-12　IS-IS のデフォルト設定

機能	デフォルト設定
リンクステート PDU（LSP）エラーの無視	イネーブル。
IS-IS タイプ	従来の IS-IS：ルータはレベル 1（ステーション）およびレベル 2（エリア）のルータとして機能します。 マルチエリア IS-IS：IS-IS ルーティング プロセスの最初のインスタンスはレベル 1-2 ルータです。残りのインスタンスはレベル 1 ルータです。
デフォルト情報送信元	ディセーブル。
IS-IS 隣接ステート変更ログ	ディセーブル。
LSP 生成スロットリング タイマー	2 つの連続する LSP 生成間の最大インターバル：5 秒。 最初の LSP 生成遅延：50 ミリ秒。 最初と 2 番めの LSP 生成間のホールドタイム：5000 ミリ秒。
LSP 最大存続時間（リフレッシュなし）	LSP パケットが削除されるまで 1200 秒（20 分）。
LSP リフレッシュ インターバル	LSP リフレッシュを 900 秒（15 分）ごとに送信。
最大 LSP パケット サイズ	1497 バイト。
NSF 認識[1]	イネーブル。ハードウェアまたはソフトウェアの変更中に、NSF 対応のネイバー ルータからのパケット転送をレイヤ 3 スイッチで継続できます。
Partial Route Computation（PRC）スロットリング タイマー	最大 PRC 待機インターバル：5 秒。 トポロジ変更後の最初の PRC 計算遅延：2000 ミリ秒。 最初と 2 番めの PRC 計算間のホールドタイム：5000 ミリ秒。
パーティション回避	ディセーブル。
パスワード	エリアまたはドメインのパスワードは定義されていません。認証はディセーブルになっています。
set-overload-bit	ディセーブル。引数を入力せずにイネーブルにすると、過負荷ビットがただちに設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになります。

表 41-12　IS-IS のデフォルト設定 （続き）

機能	デフォルト設定
Shortest Path First（SPF）スロットリング タイマー	連続する SPF 間の最大インターバル：10 秒。 トポロジ変更後の最初の SPF 計算：5500 ミリ秒。 最初と 2 番めの SPF 計算間のホールドタイム：5500 ミリ秒。
サマリー アドレス	ディセーブル。

1. NSF = ノンストップ フォワーディング。

ノンストップ フォワーディング認識

統合 IS-IS NSF 認識機能は、IPv4 に対してサポートされています。この機能により、NSF を認識する Customer Premises Equipment（CPE; 宅内装置）ルータが、NSF 対応ルータによるパケットのノンストップ フォワーディングの実行を支援できます。ローカル ルータが NSF を実行しているとは限りませんが、その NSF 認識により、NSF 対応のネイバー ルータにあるルーティング データベースとリンクステート データベースの完全性と正確性が、スイッチオーバー プロセスの間も維持されます。

この機能は自動的にイネーブルになるため、設定する必要がありません。この機能の詳細については、次の URL の『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a00801541c7.shtml

IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにするには、ルーティング プロセスごとに名前と NET を指定します。次に、インターフェイス上で IS-IS ルーティングをイネーブルにし、ルーティング プロセスのインスタンスごとにエリアを指定します。

IS-IS をイネーブルにし、IS-IS ルーティング プロセスのインスタンスごとにエリアを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clns routing**	スイッチ上で ISO コネクションレス型ルーティングをイネーブルにします。
ステップ 3	**router isis** [*area tag*]	指定されたルーティング プロセスの IS-IS ルーティングをイネーブルにして、IS-IS ルーティング コンフィギュレーション モードを開始します。 （任意）IS-IS ルータを割り当てるエリアを指定するには、*area tag* 引数を使用します。複数の IS-IS エリアを設定する場合は、値を入力する必要があります。 最初に設定した IS-IS インスタンスは、デフォルトではレベル 1-2 です。それ以降に設定したインスタンスは、自動的にレベル 1 になります。ルーティングのレベルを変更するには、**is-type** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**net** *network-entity-title*	ルーティング プロセスの NET を設定します。マルチエリア IS-IS を設定する場合は、ルーティング プロセスごとに NET を指定します。NET およびアドレスには、名前を指定できます。

	コマンド	目的
ステップ 5	**is-type** {**level-1** | **level-1-2** | **level-2-only**}	（任意）レベル 1（ステーション）ルータ、マルチエリア ルーティング用のレベル 2（エリア）ルータ、またはその両方（デフォルト）として機能するように、ルータを設定できます。 • **level-1**：ステーション ルータとしてだけ機能します。 • **level-1-2**：ステーション ルータおよびエリア ルータとして機能します。 • **level 2**：エリア ルータとしてだけ機能します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *interface-id*	IS-IS をルーティングするインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力して、レイヤ 3 モードにします。
ステップ 8	**ip router isis** [*area tag*]	インターフェイスに ISO CLNS 用の IS-IS ルーティング プロセスを設定し、ルーティング プロセスにエリア デジグネータを付加します。
ステップ 9	**clns router isis** [*area tag*]	インターフェイスで ISO CLNS をイネーブルにします。
ステップ 10	**ip address** *ip-address-mask*	インターフェイスの IP アドレスを定義します。いずれか 1 つのインターフェイスが IS-IS ルーティング用に設定されている場合は、IS-IS に対応しているエリア内のすべてのインターフェイスに IP アドレスを設定する必要があります。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show isis** [*area tag*] **database detail**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IS-IS ルーティングをディセーブルにするには、**no router isis** *area-tag* ルータ コンフィギュレーション コマンドを使用します。

次に、IP ルーティング プロトコルとして従来の IS-IS を実行するように、3 つのルータを設定する例を示します。従来の IS-IS では、すべてのルータがレベル 1 およびレベル 2 のルータとして機能します（デフォルト）。

ルータ A

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000a.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ B

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000b.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
```

```
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ C

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000c.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

IS-IS グローバル パラメータの設定

次に、設定可能な任意の IS-IS グローバル パラメータの一部を示します。

- ルート マップで制御されるデフォルト ルートを設定すると、デフォルト ルートを IS-IS ルーティング ドメインに強制的に設定することができます。また、ルート マップで設定可能なその他のフィルタリング オプションを指定することもできます。
- 内部チェックサム エラーとともに受信した IS-IS LSP を無視したり、壊れた LSP を消去して、LSP の発信側で LSP を再生成するように、ルータを設定することができます。
- エリアおよびドメインにパスワードを割り当てることができます。
- ルーティング テーブル内でサマリー アドレスによって表される集約アドレスを作成できます（ルート サマライズ）。他のルーティング プロトコルから学習したルートも集約できます。サマリーのアドバタイズに使用されるメトリックは、すべてのルートの中で最小のメトリックです。
- 過負荷ビットを設定できます。
- LSP リフレッシュ インターバル、およびリフレッシュを行わずに LSP がルータ データベース内に存続できる最大時間を設定できます。
- LSP 生成、Shortest Path First 計算、および Partial Route Computation のスロットリング タイマーを設定できます。
- IS-IS 隣接のステートが変更（アップまたはダウン）された場合に、ログ メッセージを生成するようにスイッチを設定できます。
- ネットワーク内のリンクの最大伝送ユニット（MTU）サイズが 1500 バイト未満である場合は、LSP MTU の値を小さくして、ルーティングを引き続き実行することができます。
- partition avoidance ルータ コンフィギュレーション コマンドを使用すると、レベル 1-2 境界ルータ、隣接レベル 1 ルータ、およびエンド ホスト間でフル接続が切断された場合に、エリアの分割を防止することができます。

IS-IS パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clns routing**	スイッチ上で ISO コネクションレス型ルーティングをイネーブルにします。
ステップ 3	**router isis**	IS-IS ルーティング プロトコルを指定して、ルータ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**default-information originate** [**route-map** *map-name*]	（任意）デフォルト ルートを IS-IS ルーティング ドメインに強制的に設定します。ルート マップが設定されている場合に **route-map** *map-name* を入力すると、ルーティング プロセスによってデフォルト ルートが生成されます。
ステップ 5	**ignore-lsp-errors**	（任意）内部チェックサム エラーを含む LSP を消去せず、無視するように、ルータを設定します。デフォルトでは、このコマンドはイネーブルになっています（壊れた LSP は廃棄されます）。壊れた LSP を消去するには、**no ignore-lsp-errors** ルータ コンフィギュレーション コマンドを入力します。
ステップ 6	**area-password** *password*	（任意）エリア認証パスワードを設定します。このパスワードはレベル 1（ステーション ルータ レベル）の LSP に挿入されます。
ステップ 7	**domain-password** *password*	（任意）ルーティング ドメイン認証パスワードを設定します。このパスワードはレベル 2（エリア ルータ レベル）の LSP に挿入されます。
ステップ 8	**summary-address** *address mask* [**level-1** | **level-1-2** | **level-2**]	（任意）指定されたレベルのアドレスのサマリーを作成します。
ステップ 9	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}]	（任意）ルータに問題がある場合に、他のルータが Shortest Path First（SPF）計算でそのルータを無視できるように、過負荷ビット（hippity ビット）を設定します。 • （任意）**on-startup**：起動時にだけ過負荷ビットを設定します。**on-startup** を指定しない場合は、過負荷ビットがただちに設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになります。**on-startup** を指定する場合は、秒数または **wait-for-bgp** を入力する必要があります。 • *seconds*：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定され、この秒数の間、設定されたままになります。指定できる範囲は 5 ～ 86400 秒です。 • **wait-for-bgp**：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定され、BGP が収束するまで設定されたままになります。BGP が収束したことが IS-IS に通知されない場合、IS-IS は 10 分後に過負荷ビットをオフにします。
ステップ 10	**lsp-refresh-interval** *seconds*	（任意）LSP リフレッシュ インターバルを秒単位で設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルトでは、LSP リフレッシュを 900 秒（15 分）ごとに送信します。
ステップ 11	**max-lsp-lifetime** *seconds*	（任意）リフレッシュを実行しない場合に、LSP パケットがルータ データベース内に存続する最大時間を設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 1200 秒（20 分）です。指定された時間が経過すると、LSP パケットは削除されます。
ステップ 12	**lsp-gen-interval** [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*]	（任意）IS-IS LSP 生成スロットリング タイマーを設定します。 • *lsp-max-wait*：2 つの連続する LSP 生成間の最大インターバル（秒単位）。指定できる範囲は 1 ～ 120 です。デフォルト値は 5 です。 • *lsp-initial-wait*：最初の LSP 生成遅延（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 50 です。 • *lsp-second-wait*：最初と 2 番めの LSP 生成間のホールドタイム（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 5000 です。

	コマンド	目的
ステップ 13	**spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]	（任意）IS-IS Shortest Path First（SPF）スロットリング タイマーを設定します。 • *spf-max-wait*：連続する SPF 間の最大インターバル（秒単位）。指定できる範囲は 1 ～ 120 です。デフォルト値は 10 です。 • *spf-initial-wait*：トポロジ変更後の最初の SPF 計算（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 5500 です。 • *spf-second-wait*：最初と 2 番めの SPF 計算間のホールドタイム（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 5500 です。
ステップ 14	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*]	（任意）IS-IS Partial Route Computation（PRC）スロットリング タイマーを設定します。 • *prc-max-wait*：2 つの連続する PRC 計算間の最大インターバル（秒単位）。指定できる範囲は 1 ～ 120 です。デフォルト値は 5 です。 • *prc-initial-wait*：トポロジ変更後の最初の PRC 計算遅延（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 2000 です。 • *prc-second-wait*：最初と 2 番めの PRC 計算間のホールドタイム（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 5000 です。
ステップ 15	**log-adjacency-changes** [**all**]	（任意）IS-IS 隣接のステート変更をログ記録するようにルータを設定します。End System-to-Intermediate System PDU や Link State Packet（LSP）など、Intermediate System-to-Intermediate System Hello に関連しないイベントによって生成されたすべての変更をログに含める場合は、**all** を入力します。
ステップ 16	**lsp-mtu** *size*	（任意）最大 LSP パケット サイズをバイト単位で指定します。指定できる範囲は 128 ～ 4352 です。デフォルト値は 1497 バイトです。 **（注）** ネットワーク内のあるリンクで MTU サイズが小さくなった場合は、ネットワーク内のすべてのルータで LSP MTU サイズを変更する必要があります。
ステップ 17	**partition avoidance**	（任意）境界ルータ、すべてのレベル 1 隣接ルータ、およびエンド ホスト間でフル接続が切断された場合、レベル 1 エリア プレフィクスのレベル 2 バックボーンへのアドバタイズを停止するように IS-IS レベル 1-2 境界ルータを設定します。
ステップ 18	**end**	特権 EXEC モードに戻ります。
ステップ 19	**show clns**	設定を確認します。
ステップ 20	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト ルートの生成をディセーブルにするには、**no default-information originate** ルータ コンフィギュレーション コマンドを使用します。パスワードをディセーブルにするには、**no area-password** または **no domain-password** ルータ コンフィギュレーション コマンドを使用します。LSP MTU 設定をディセーブルにするには、**no lsp mtu** ルータ コンフィギュレーション コマンドを使用します。サマリー アドレッシング、LSP リフレッシュ インターバル、LSP 存続時間、LSP タイマー、SPF タイマー、および PRC タイマーをデフォルト状態に戻すには、各コマンドの **no** 形式を使用します。出力形式をディセーブルにするには、**no partition avoidance** ルータ コンフィギュレーション コマンドを使用します。

IS-IS インターフェイス パラメータの設定

特定のインターフェイス固有の IS-IS パラメータは、接続された他のルータとは関係なく、任意に設定することができます。ただし、一部の値（乗数や間隔など）をデフォルトから変更する場合は、複数のルータおよびインターフェイスでもこれらを変更する必要があります。インターフェイス パラメータのほとんどは、レベル 1、レベル 2、またはその両方で設定できます。

次に、設定可能なインターフェイス レベルのパラメータの一部を示します。

- インターフェイスのデフォルト メトリック。Quality of Service（QoS; サービス品質）ルーティングが実行されない場合に、IS-IS メトリックの値として使用され、割り当てられます。
- hello 間隔（インターフェイスから送信される hello パケットの間隔）またはデフォルトの hello パケット乗数。IS-IS hello パケットで送信されるホールドタイムを判別するためにインターフェイスで使用されます。このホールドタイムによって、ネイバーがダウンしていると宣言されるまで、そのネイバが別の hello パケットを待機する時間が決定されます。また、ルートを再計算できるように、障害リンクまたはネイバーを検出する速度も決定されます。hello パケットが頻繁に失われ、IS-IS 隣接に無用な障害が発生する場合は、環境内の hello 乗数を変更してください。hello 乗数を大きくし、その分 hello 間隔を小さくすると、リンク障害を検出するための所要時間を増加させることなく、hello プロトコルの信頼性を高めることができます。
- その他の間隔：
  - Complete Sequence Number PDU（CSNP）間隔。CSNP は、データベースの同期を維持するために指定ルータから送信されます。
  - 再送信間隔。ポイントツーポイント リンクの IS-IS LSP の再送信間隔です。
  - IS-IS LSP 再送信スロットル間隔。IS-IS LSP をポイントツーポイント リンクで再送信する最大レート（パケット間のミリ秒数）です。この間隔は、*同じ* LSP の連続する再送信間隔である再送信間隔とは異なります。
- 指定ルータの選定優先度。このパラメータを使用すると、マルチアクセス ネットワークに必要な隣接数を削減できるため、ルーティング プロトコル トラフィック数やトポロジ データベースのサイズが削減されます。
- インターフェイス回路タイプ。指定されたインターフェイスのネイバーに必要な隣接タイプです。
- インターフェイスのパスワード認証。

IS-IS インターフェイス パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力して、レイヤ 3 モードにします。
ステップ 3	**isis metric** *default-metric* [**level-1** | **level-2**]	（任意）指定されたインターフェイスのメトリック（コスト）を設定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 10 です。レベルを入力しない場合は、デフォルト値がレベル 1 とレベル 2 の両方のルータに適用されます。

	コマンド	目的
ステップ 4	**isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**]	（任意）スイッチから送信される hello パケットの間隔を指定します。デフォルトでは、hello 間隔 *seconds* の 3 倍の値が、送信される hello パケットの *holdtime* としてアドバタイズされます。hello 間隔が小さいほどトポロジ変更が短時間で検出されますが、ルーティング トラフィックは増大します。 • **minimal**：ホールドタイムが 1 秒になるように、hello 乗数に基づいて hello 間隔が計算されます。 • *seconds*：指定できる範囲は 1 ～ 65535 です。デフォルト値は 10 秒です。
ステップ 5	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**]	（任意）隣接装置がダウンしているとルータによって宣言されるまでに、ネイバーが失う IS-IS hello パケットの数を指定します。指定できる範囲は 3 ～ 1000 です。デフォルト値は 3 です。小さい hello 乗数を使用すると高速コンバージェンスとなりますが、ルーティングが不安定になることがあります。
ステップ 6	**isis csnp-interval** *seconds* [**level-1** | **level-2**]	（任意）インターフェイスの IS-IS Complete Sequence Number PDU（CSNP）間隔を設定します。指定できる範囲は 0 ～ 65535 です。デフォルト値は 10 秒です。
ステップ 7	**isis retransmit-interval** *seconds*	（任意）ポイントツーポイント リンクの IS-IS LSP の再送信間隔を秒単位で設定します。ネットワーク上の任意の 2 つのルータ間の予測ラウンドトリップ遅延よりも大きい整数値を指定する必要があります。指定できる範囲は 0 ～ 65535 です。デフォルト値は 5 秒です。
ステップ 8	**isis retransmit-throttle-interval** *milliseconds*	（任意）IS-IS LSP 再送信スロットル間隔を設定します。この間隔は、ポイントツーポイント リンクで IS-IS LSP を再送信する最大レート（パケット間のミリ秒数）です。指定できる範囲は 0 ～ 65535 です。デフォルト値は **isis lsp-interval** コマンドによって決まります。
ステップ 9	**isis priority** *value* [**level-1** | **level-2**]	（任意）指定ルータの選定に使用する優先度を設定します。指定できる範囲は 0 ～ 127 です。デフォルト値は 64 です。
ステップ 10	**isis circuit-type** {**level-1** | **level-1-2** | **level-2-only**}	（任意）指定されたインターフェイスのネイバーに必要な隣接タイプを設定します（インターフェイス回路タイプを指定します）。 • **level-1**：現在のノードとそのネイバーに共通のエリア アドレスが少なくとも 1 つ存在する場合に、レベル 1 隣接を確立します。 • **level-1-2**：ネイバーがレベル 1 およびレベル 2 の両方として設定されていて、共通のエリアが少なくとも 1 つ存在する場合に、レベル 1-2 隣接を確立します。共通のエリアが存在しない場合は、レベル 2 隣接が確立されます。これはデフォルトです。 • **level 2**：レベル 2 隣接を確立します。ネイバー ルータがレベル 1 ルータの場合は、隣接が確立されません。
ステップ 11	**isis password** *password* [**level-1** | **level-2**]	（任意）インターフェイス用の認証パスワードを設定します。デフォルトでは、認証はディセーブルになっています。レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 またはレベル 2 のルーティング用のパスワードだけがイネーブルになります。レベルを指定しない場合のデフォルトは、レベル 1 およびレベル 2 です。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show clns interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ISO IGRP および IS-IS のモニタおよびメンテナンス

CLNS キャッシュの内容をすべて削除したり、特定のネイバーまたはルートの情報を削除したりすることができます。ルーティング テーブル、キャッシュ、データベースの内容など、特定の CLNS または IS-IS 統計情報を表示することができます。特定のインターフェイス、フィルタ、またはネイバーに関する情報も表示できます。

表 41-13 に、ISO CLNS および IS-IS ルーティングを消去および表示するための特権 EXEC コマンドを示します。表示フィールドの詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2*』を参照するか、Cisco IOS コマンド リファレンス マスター インデックスを使用するか、またはオンラインで検索してください。

表 41-13　ISO CLNS および IS-IS の clear および show コマンド

コマンド	目的
clear clns cache	CLNS ルーティング キャッシュを消去して、再初期化します。
clear clns es-neighbors	隣接データベースからエンド システム（ES）ネイバー情報を削除します。
clear clns is-neighbors	隣接データベースから中継システム（IS）ネイバー情報を削除します。
clear clns neighbors	隣接データベースから CLNS ネイバー情報を削除します。
clear clns route	ダイナミックに取得された CLNS ルーティング情報を削除します。
show clns	CLNS ネットワークに関する情報を表示します。
show clns cache	CLNS ルーティング キャッシュのエントリを表示します。
show clns es-neighbors	ES ネイバー エントリを、関連付けられたエリアを含めて表示します。
show clns filter-expr	フィルタ式を表示します。
show clns filter-set	フィルタ セットを表示します。
show clns interface [*interface-id*]	各インターフェイスに関する CLNS 固有の情報または ES-IS 情報を表示します。
show clns neighbor	IS-IS ネイバーに関する情報を表示します。
show clns protocol	現在のルータの IS-IS または ISO IGRP ルーティング プロセスごとに、プロトコル固有の情報を表示します。
show clns route	現在のルータが認識している CLNS パケットのルーティング方法での宛先をすべて表示します。
show clns traffic	現在のルータが確認した CLNS パケットに関する情報を表示します。
show ip route isis	IS-IS IP ルーティング テーブルの現在のステートを表示します。
show isis database	IS-IS リンク ステート データベースを表示します。
show isis routes	IS-IS レベル 1 ルーティング テーブルを表示します。
show isis spf-log	IS-IS の Shortest Path First（SPF）計算の履歴を表示します。
show isis topology	すべてのエリア内の接続されている全ルータのリストを表示します。
show route-map	設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示します。
trace clns *destination*	ネットワーク内の指定された宛先までパケットがたどるパスを検出します。
which-route {*nsap-address* | *clns-name*}	指定された CLNS 宛先が検出されたルーティング テーブルを表示します。

multi-VRF CE の設定

Virtual Private Network（VPN; 仮想私設網）を使用すると、カスタマーは ISP バックボーン ネットワーク上で帯域幅を安全に共有することができます。VPN は共通のルーティング テーブルを共有するサイトの集まりです。カスタマー サイトは、1 つまたは複数のインターフェイスによってサービス プロバイダー ネットワークに接続されます。サービス プロバイダーは、各インターフェイスを、VPN ルーティング/フォワーディング（VRF）テーブルと呼ばれる VPN ルーティング テーブルに関連付けます。

IE 3000 スイッチは、IP サービス イメージを稼動している場合、Customer Edge（CE; カスタマー エッジ）装置の複数の VPN ルーティング/フォワーディング（multi-VRF）インスタンスをサポートします（multi-VRF CE）。サービス プロバイダーは、multi-VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。

（注）　スイッチでは、VPN をサポートするための Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）は使用されません。MPLS VRF の詳細については、Cisco.com のホーム ページにアクセスして、『*Cisco IOS Switching Services Configuration Guide, Release 12.2*』を参照してください（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）。

multi-VRF CE の概要

multi-VRF CE は、サービス プロバイダーが複数の VPN をサポートして、VPN 間で IP アドレスを重複使用できるようにするための機能です。multi-VRF CE は、入力インターフェイスを使用してさまざまな VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスを各 VRF に関連付けることによって仮想パケット転送テーブルを形成します。VRF 内のインターフェイスは、物理インターフェイス（イーサネット ポートなど）と論理インターフェイス（VLAN SVI など）のどちらにもすることができますが、複数の VRF に属することはできません。

（注）　multi-VRF CE インターフェイスは、レイヤ 3 インターフェイスである必要があります。

multi-VRF CE には、次の装置が含まれます。

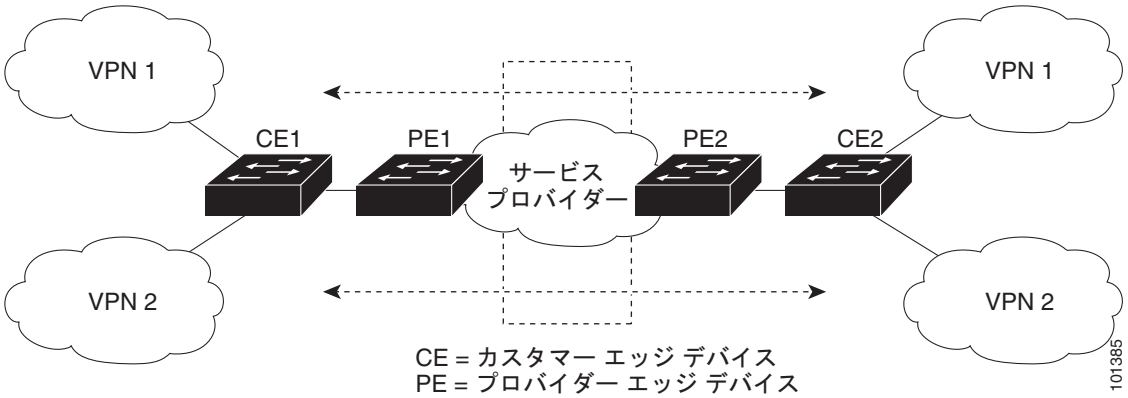
- カスタマー エッジ（CE）装置。この装置を使用すると、カスタマーは、1 つまたは複数のプロバイダー エッジ ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE 装置は、サイトのローカル ルートをルータにアドバタイズして、そこからリモート VPN ルートを学習します。IE 3000 スイッチは、CE に設定することができます。

- プロバイダー エッジ（PE）ルータ。このルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE 装置とルーティング情報を交換します。PE では、直接接続している VPN の VPN ルートを維持するだけでよいため、サービス プロバイダーのすべての VPN ルートを維持する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN 内に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、内部 BGP（IBGP）を使用して別の PE ルータと VPN ルーティング情報を交換します。
- プロバイダー ルータまたはコア ルータ。これらは、CE 装置に接続していないサービス プロバイダー ネットワーク内の任意のルータです。

multi-VRF CE では、複数のカスタマーが 1 つの CE を共有でき、CE と PE の間で物理リンクが 1 つだけ使用されます。CE を共有すると、各カスタマー用の個別の VRF テーブルが維持されます。パケットのスイッチングやルーティングは、独自のルーティング テーブルに基づいて、カスタマーごとに行われます。multi-VRF CE では、制限付きの PE 機能が CE 装置に拡張されます。これにより、VRF テーブルを個別に維持する機能が CE 装置に与えられるため、VPN のプライバシおよびセキュリティが支店にまで拡張されます。

図 41-6 に、IE3000 スイッチを複数の仮想 CE として使用した構成例を示します。このシナリオは、小規模な企業など、VPN サービスの帯域幅要件が低いカスタマーに適しています。この場合、IE3000 スイッチには multi-VRF CE のサポートが必要です。multi-VRF CE はレイヤ 3 機能であるため、VRF の各インターフェイスはレイヤ 3 インターフェイスにする必要があります。

図 41-6　　複数の仮想 CE として機能するスイッチ



CE スイッチは、レイヤ 3 インターフェイスを VRF に追加するコマンドを受信すると、multi-VRF CE 関連のデータ構造内の VLAN ID と Policy Label（PL; ポリシー ラベル）の間に適切なマッピングを設定し、VLAN ID と PL を VLAN データベースに追加します。

multi-VRF CE が設定されている場合、レイヤ 3 転送テーブルは次の 2 つのセクションに概念的に分割されます。

- multi-VRF CE ルーティング セクション。このセクションには、各 VPN からのルートが格納されます。
- グローバル ルーティング セクション。このセクションには、インターネットなど、非 VPN ネットワークへのルートが格納されます。

各 VRF の VLAN ID は別々のポリシー ラベルにマッピングされ、処理中に VRF を区別するために使用されます。レイヤ 3 設定機能は、学習した新しい VPN ルートごとに、入力ポートの VLAN ID を使用してポリシー ラベルを取得し、multi-VRF CE ルーティング セクションにポリシー ラベルおよび新しいルートを挿入します。ルーテッド ポートからパケットを受信した場合は、ポートの内部 VLAN ID 番号が使用されます。SVI からパケットを受信した場合は、VLAN 番号が使用されます。

multi-VRF CE 対応ネットワークでのパケット転送プロセスを次に示します。

- スイッチは、VPN からパケットを受信すると、入力ポリシー ラベル番号に基づいてルーティング テーブルを検索します。ルートが見つかると、スイッチはパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかると、ルータは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを削除し、そのラベルを使用して正しい VPN ルーティング テーブルを識別します。次に、通常のルート検索を実行します。ルートが見つかると、パケットを正しい隣接装置に転送します。
- CE は、出力 PE からパケットを受信すると、入力ポリシー ラベルを使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかると、パケットを VPN 内で転送します。

VRF を設定するには、VRF テーブルを作成し、VRF に関連付けられているレイヤ 3 インターフェイスを指定します。次に、VPN 内、および CE と PE 間でルーティング プロトコルを設定します。プロバイダーのバックボーン全体に VPN ルーティング情報を配信する場合は、ルーティング プロトコルとして BGP を使用することを推奨します。multi-VRF CE ネットワークでは、次の 3 つの主要コンポーネントを設定します。

- VPN ルート ターゲット コミュニティ：VPN コミュニティのその他すべてのメンバーのリスト。VPN ルート ターゲットは、VPN コミュニティ メンバーごとに設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング：VPN コミュニティのすべてのメンバーに VRF 到達可能性情報を伝播します。VPN コミュニティ内のすべての PE ルータに BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービス プロバイダー ネットワーク全体のすべての VPN コミュニティ メンバー間で、すべてのトラフィックを転送します。

multi-VRF CE のデフォルト設定

表 41-14 に、VRF のデフォルト設定を示します。

表 41-14　VRF のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル。VRF は定義されていません。
マップ	インポート マップ、エクスポート マップ、ルート マップは定義されていません。
VRF 最大ルート数	ファスト イーサネット スイッチ：8000。 ギガビット イーサネット スイッチ：12000。
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

multi-VRF CE 設定時の注意事項

（注）　multi-VRF CE を使用するには、IP サービス イメージをスイッチにインストールする必要があります。

ネットワークに VRF を設定する場合は、次の点に注意してください。

- multi-VRF CE が設定されたスイッチは、複数のカスタマーによって共有されます。各カスタマーには、独自のルーティング テーブルが設定されます。
- 各カスタマーは別々の VRF テーブルを使用するため、同じ IP アドレスを再利用できます。各 VPN では、IP アドレスを重複使用できます。
- multi-VRF CE では、複数のカスタマーが、プロバイダー エッジ（PE）とカスタマー エッジ（CE）の間で同じ物理リンクを共有できます。複数の VLAN が設定されたトランク ポートでは、パケットがカスタマーごとに分離されます。各カスタマーには独自の VLAN が設定されます。
- multi-VRF CE では、一部の MPLS-VRF 機能がサポートされません（ラベル交換、LDP 隣接、ラベル付きパケットなど）。
- PE ルータでは、multi-VRF CE を使用した場合と複数の CE を使用した場合の違いはありません。図 41-6 では、複数の仮想レイヤ 3 インターフェイスが multi-VRF CE 装置に接続されています。
- スイッチでは、物理ポート、VLAN SVI、またはこれら両方の組み合わせを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートを介して接続することができます。
- カスタマーは、他のカスタマーと重複しない限り、複数の VLAN を使用できます。カスタマーの VLAN は、特定のルーティング テーブル ID にマッピングされます。この ID は、スイッチに格納されている適切なルーティング テーブルを識別するために使用されます。
- IE3000 スイッチは、1 つのグローバル ネットワークと最大 26 の VRF をサポートします。
- CE と PE の間では、ほとんどのルーティング プロトコル（BGP、OSPF、RIP、およびスタティック ルーティング）を使用できます。ただし、次の理由により、外部 BGP（EBGP）を使用することを推奨します。
  - BGP では、複数の CE との通信に複数のアルゴリズムを必要としない。
  - BGP は、さまざまな管理者によって稼動されているシステム間でルーティング情報を交換するように設計されている。
  - BGP では、ルートの属性を CE に簡単に送信できる。
- multi-VRF CE は、パケットのスイッチング レートに影響しません。
- VPN マルチキャストはサポートされません。
- multi-VRF CE 内のラインレート マルチキャスト転送がサポートされます。
- マルチキャスト VRF は、同じインターフェイスのプライベート VLAN とは共存できません。
- 最大 1000 のマルチキャスト ルートがサポートされ、すべての VRF で共有できます。
- VRF を設定しない場合は、105 のポリシーを設定できます。
- VRF が 1 つでも設定されている場合は、41 のポリシーを設定できます。
- ポリシーが 42 以上設定されている場合は、VRF を設定できません。
- VRF とプライベート VLAN は、相互に排他的な関係にあります。プライベート VLAN では、VRF をイネーブルにすることはできません。同様に、VLAN インターフェイスで VRF が設定されている VLAN では、プライベート VLAN をイネーブルにすることはできません。
- スイッチ インターフェイスでは、VRF と Policy-Based Routing（PBR; ポリシーベース ルーティング）は、相互に排他的な関係にあります。PBR がインターフェイスでイネーブルになっている場合は、VRF をイネーブルにすることはできません。その逆も同様で、VRF がインターフェイスでイネーブルになっている場合は、PBR をイネーブルにすることはできません。
- スイッチ インターフェイスでは、VRF と Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）は、相互に排他的な関係にあります。WCCP がインターフェイスでイネーブルになっている場合は、VRF をイネーブルにすることはできません。その逆も同様で、VRF がインターフェイスでイネーブルになっている場合は、WCCP をイネーブルにすることはできません。

VRF の設定

1 つまたは複数の VRF を設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文および使用方法の詳細については、このリリースに対応したスイッチのコマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします。
ステップ 3	**ip vrf** *vrf-name*	VRF に名前を付けて、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher*	ルート識別子を指定して、VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community*	指定した VRF のインポート、エクスポート、またはインポートおよびエクスポートのルート ターゲット コミュニティのリストを作成します。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* には、ステップ 4 で入力した *route-distinguisher* と同じ値を指定する必要があります。
ステップ 6	**import map** *route-map*	（任意）ルート マップを VRF に関連付けます。
ステップ 7	**interface** *interface-id*	VRF に関連付けるレイヤ 3 インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには、ルーテッド ポートまたは SVI を設定できます。
ステップ 8	**ip vrf forwarding** *vrf-name*	VRF をレイヤ 3 インターフェイスに関連付けます。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VRF を削除して、そのインターフェイスをすべて削除するには、**no ip vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。VRF からインターフェイスを削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

マルチキャスト VRF の設定

VRF テーブル内にマルチキャストを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文および使用方法の詳細については、このリリースに対応したスイッチのコマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティング モードをイネーブルにします。
ステップ 3	**ip vrf** *vrf-name*	VRF に名前を付けて、VRF コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**rd** *route-distinguisher*	ルート識別子を指定して、VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community*	指定した VRF のインポート、エクスポート、またはインポートおよびエクスポートのルート ターゲット コミュニティのリストを作成します。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* には、ステップ 4 で入力した *route-distinguisher* と同じ値を指定する必要があります。
ステップ 6	**import map** *route-map*	（任意）ルート マップを VRF に関連付けます。
ステップ 7	**ip multicast-routing vrf** *vrf*-**name distributed**	（任意）VRF テーブルのグローバル マルチキャスト ルーティングをイネーブルにします。
ステップ 8	**interface** *interface-id*	VRF に関連付けるレイヤ 3 インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには、ルーテッド ポートまたは SVI を設定できます。
ステップ 9	**ip vrf forwarding** *vrf-name*	VRF をレイヤ 3 インターフェイスに関連付けます。
ステップ 10	**ip address** *ip-address* **mask**	レイヤ 3 インターフェイスの IP アドレスを設定します。
ステップ 11	ip pim sparse-dense mode	VRF 関連レイヤ 3 インターフェイスで Protocol Independent Multicast（PIM）をイネーブルにします。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

multi-VRF CE 内でのマルチキャストの設定に関する詳細については、『*Cisco IOS IP Multicast Configuration Guide, Release 12.4.*』を参照してください。

VRF 認識サービスの設定

IP サービスは、グローバル インターフェイス上に設定することができ、グローバル ルーティング インスタンス内で実行します。複数のルーティング インスタンスで実行するように拡張された IP サービスが VRF 認識です。システム内で設定された VRF は、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームとは独立したモジュールに実装されます。VRF とは、Cisco IOS における複数のルーティング インスタンスを表します。各プラットフォームがサポートする VRF 数にはそれぞれ制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、指定した VRF 内のホストに ping を実行することができる。
- アドレス解決プロトコル（ARP）エントリは個別の VRF で学習される。ユーザは特定の VRF の ARP エントリを表示できる。

次のサービスは VRF 認識です。

- ARP（アドレス解決プロトコル）
- ping
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
- Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）

- RADIUS
- Syslog
- traceroute
- FTP および TFTP

（注）　Unicast Reverse Path Forwarding（uRPF; ユニキャスト RPF）の VRF 認識サービスはサポートされていません。

ARP のユーザ インターフェイス

ARP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文および使用方法の詳細については、このリリースに対応したスイッチのコマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

コマンド	目的
show ip arp vrf *vrf-name*	指定された VRF 内の ARP テーブルを表示します。

ping のユーザ インターフェイス

ping の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文および使用方法の詳細については、このリリースに対応したスイッチのコマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

コマンド	目的
ping vrf *vrf-name* **ip-host**	指定された VRF 内の ARP テーブルを表示します。

SNMP のユーザ インターフェイス

SNMP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文および使用方法の詳細については、このリリースに対応したスイッチのコマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server trap authentication vrf**	VRF でのパケットの SNMP トラップをイネーブルにします。
ステップ 3	**snmp-server engineID remote** <*host*> **vrf** <*vpn instance*> <*engine-id string*>	スイッチ上のリモート SNMP エンジンの名前を設定します。
ステップ 4	**snmp-server host** <*host*> **vrf** <*vpn instance*> **traps** <*community*>	SNMP トラップ動作の受信側、および SNMP トラップの送信に使用する VRF テーブルを指定します。
ステップ 5	**snmp-server host** <***host***> **vrf** <*vpn instance*> **informs** <*community*>	SNMP インフォーム動作の受信側、および SNMP インフォームの送信に使用する VRF テーブルを指定します。

	コマンド	目的
ステップ 6	**snmp-server user** *<user> <group>* **remote** *<host>* **vrf** *<vpn instance> <security model>*	SNMP アクセスで使用する VRF でのリモート ホストの SNMP グループにユーザを追加します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

HSRP のユーザ インターフェイス

VRF の HSRP サポートにより、HSRP 仮想 IP アドレスが適切な IP ルーティング テーブルに追加されます。

HSRP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文および使用方法の詳細については、このリリースに対応したスイッチのコマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no switchport**	物理インターフェイスの場合、レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します。
ステップ 4	**ip vrf forwarding** *<vrf-name>*	インターフェイス上に VRF を設定します。
ステップ 5	**ip address** *ip address*	インターフェイスの IP アドレスを入力します。
ステップ 6	**standby 1 ip** *ip address*	HSRP をイネーブルにして、仮想 IP アドレスを設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

VRF 認識 RADIUS のユーザ インターフェイス

VRF 認識 RADIUS を設定するには、まず RADIUS サーバで AAA をイネーブルにする必要があります。スイッチでは、**ip vrf forwarding** *vrf-name* サーバ グループ コンフィギュレーション コマンドと **ip radius source-interface** グローバル コンフィギュレーション コマンドがサポートされています（次の URL の『*Per VRF AAA Feature Guide*』を参照）。
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html

Syslog のユーザ インターフェイス

Syslog の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文および使用方法の詳細については、このリリースに対応したスイッチのコマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging on**	ストレージ ルータ イベント メッセージのロギングをイネーブルにしたり、一時的にディセーブルにしたりします。
ステップ 3	**logging host** ***ip address*** **vrf** ***vrf name***	ロギング メッセージの送信先 Syslog サーバのホスト アドレスを指定します。

	コマンド	目的
ステップ 4	**logging buffered** *logging buffered size* **debugging**	内部バッファへのメッセージをログ記録します。
ステップ 5	**logging trap debugging**	Syslog サーバに送信されるロギング メッセージを制限します。
ステップ 6	**logging facility** *facility*	システム ロギング メッセージをロギング ファシリティに送信します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

traceroute のユーザ インターフェイス

traceroute の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文および使用方法の詳細については、このリリースに対応したスイッチのコマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

コマンド	目的
traceroute vrf *vrf-name ipaddress*	VPN VRF 内の宛先アドレスを検索するための VPN VRF の名前を指定します。

FTP および TFTP のユーザ インターフェイス

FTP および TFTP を VRF 認識にするには、FTP/TFTP CLI をいくつか設定する必要があります。たとえば、インターフェイスに付加されている VRF テーブルを使用する場合、E1/0 であれば、CLI **ip [t]ftp source-interface E1/0** を設定して、特定のルーティング テーブルを使用するように [t]ftp に通知します。この例では、VRF テーブルが宛先 IP アドレスを検索するために使用されます。これらの変更には下位互換性があり、既存の動作には影響しません。つまり、VRF が送信元インターフェイスに設定されていなくても、そのインターフェイスの CLI を使用してパケットを特定のインターフェイスに送信することができます。

FTP 接続の送信元 IP アドレスを指定するには、**ip ftp source-interface** show mode コマンドを使用します。接続が確立されているインターフェイスのアドレスを使用するには、このコマンドの **no** 形式を使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip ftp source-interface** *interface-type interface-number*	FTP 接続の送信元 IP アドレスを指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

TFTP 接続の送信元アドレスとしてインターフェイスの IP アドレスを指定するには、**ip tftp source-interface** show mode コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされている任意のルーティング プロトコル（RIP、OSPF、EIGRP、BGP）、またはスタティック ルーティングで設定できます。ここでは OSPF の設定について説明しますが、他のプロトコルでも手順は同じです。

（注）　VRF インスタンス内で実行する EIGRP ルーティング プロセスを設定する場合は、**autonomous-system** *autonomous-system-number* アドレス ファミリ コンフィギュレーション モード コマンドを入力して、AS（自律システム）番号を設定する必要があります。

VPN 内で OSPF を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id* **vrf** *vrf-name*	OSPF ルーティングのイネーブル化、VPN 転送テーブルの指定を行い、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**log-adjacency-changes**	（任意）隣接ステートの変更をログ記録します。これがデフォルトの状態になります。
ステップ 4	**redistribute bgp** *autonomous-system-number* **subnets**	BGP ネットワークから OSPF ネットワークに情報を再配信するようにスイッチを設定します。
ステップ 5	**network** *network-number* **area** *area-id*	OSPF が動作するネットワークのネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip ospf** *process-id*	OSPF ネットワークの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VPN 転送テーブルと OSPF ルーティング プロセスの関連付けを解除するには、**no router ospf** *process-id* **vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。

BGP PE/CE ルーティング セッションの設定

BGP PE/CE ルーティング セッションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number*	他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定して、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**network** *network-number* **mask** *network-mask*	ネットワークとマスクを指定して、BGP の使用をアナウンスします。
ステップ 4	**redistribute ospf** *process-id* **match internal**	OSPF 内部ルートを再配信するようにスイッチを設定します。
ステップ 5	**network** *network-number* **area** *area-id*	OSPF が動作するネットワークのネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。

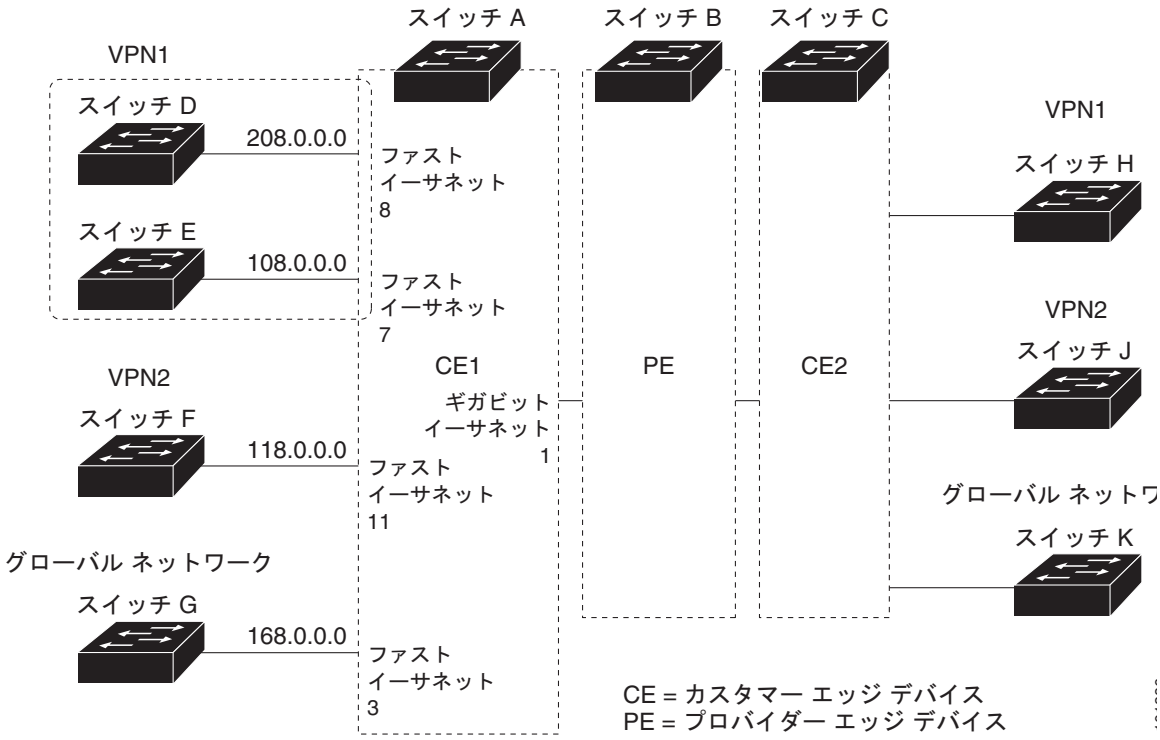
	コマンド	目的
ステップ 6	**address-family ipv4 vrf** *vrf-name*	PE/CE ルーティング セッションの BGP パラメータを定義して、VRF アドレス ファミリ モードを開始します。
ステップ 7	**neighbor** *address* **remote-as** *as-number*	PE と CE のルータ間の BGP セッションを定義します。
ステップ 8	**neighbor** *address* **activate**	IPv4 アドレス ファミリのアドバタイズをアクティブにします。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp** [**ipv4**] [**neighbors**]	BGP 設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BGP ルーティング プロセスを削除するには、**no router bgp** *autonomous-system-number* グローバル コンフィギュレーション コマンドを使用します。ルーティング特性を削除するには、キーワードを指定してこのコマンドを使用します。

multi-VRF CE の設定例

図 41-7 は、図 41-6 とほぼ同じネットワークの物理接続を簡素化した例です。VPN1、VPN2、およびグローバル ネットワークでは、プロトコルに OSPF が使用されています。CE/PE 接続には BGP が使用されています。図のあとには、IE3000 スイッチを CE スイッチ A として設定し、カスタマー スイッチ D および F に対して VRF を設定する例を示します。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容はほぼ同じです。この例には、PE ルータとして動作する Catalyst 6000 スイッチまたは Catalyst 6500 スイッチでのスイッチ A へのトラフィックを設定するためのコマンドも含まれています。

図 41-7　multi-VRF CE の設定例



スイッチ A の設定

スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ A のループバックおよび物理インターフェイスを設定します。ギガビット イーサネット ポート 1 は PE へのトランク接続です。ファスト イーサネット ポート 8 および 11 は VPN に接続されます。

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface gigabitethernet1/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet1/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet0/11
Switch(config)# interface fastethernet1/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 および 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

```
Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit
```

```
Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
```

VPN1 および VPN2 の OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf vl1
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf vl2
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE/PE ルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit

Switch(config-router)# address-family ipv4 vrf vl1
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

スイッチ D の設定

スイッチ D は VPN1 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

スイッチ F の設定

スイッチ F は VPN2 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
```

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

PE スイッチ B の設定

次のコマンドをスイッチ B（PE ルータ）に対して使用すると、CE 装置（スイッチ A）への接続だけが設定されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitthernet1/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitthernet1/0.10
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
```

```
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

multi-VRF CE のステータスの表示

multi-VRF CE の設定とステータスに関する情報を表示するには、表 41-15 の特権 EXEC コマンドを使用します。

表 41-15　multi-VRF CE の情報を表示するためのコマンド

コマンド	目的
show ip protocols vrf *vrf-name*	VRF に関連付けられているルーティング プロトコルの情報を表示します。
show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRF に関連付けられている IP ルーティング テーブルの情報を表示します。
show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義済みの VRF インスタンスに関する情報を表示します。

表示される情報の詳細については、『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

プロトコル独立機能の設定

ここでは、IP ルーティング プロトコル独立機能の設定方法について説明します。この章に記載されている IP ルーティング プロトコル独立コマンドの詳細については、Cisco.com のホーム ページにアクセスして、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「IP Routing Protocol-Independent Commands」を参照してください（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）。

ここでは、次の設定情報について説明します。

Cisco Express Forwarding の設定

Cisco Express Forwarding（CEF）は、ネットワーク パフォーマンスを最適化するために使用されるレイヤ 3 IP スイッチング テクノロジーです。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。CEF は、高速スイッチング ルート キャッシュよりも CPU 負荷が小さいため、より多くの CPU 処理能力をパケット転送に振り分けることができます。ダイナミックなネットワークでは、ルーティングの変更によって、高速スイッチング キャッシュ エントリが頻繁に無効化されます。高速スイッチング キャッシュ エントリが無効になると、トラフィックがルート キャッシュによって高速スイッチングされずに、ルーティング テーブルによってプロセス スイッチングされることがあります。CEF は、Forwarding Information Base（FIB; 転送情報ベース）検索テーブルを使用して、宛先ベースの IP パケット スイッチングを実行します。

CEF の主要コンポーネントは、分散 FIB と分散隣接テーブルの 2 つです。

- FIB では、ルーティング テーブルや情報ベースと同様に、IP ルーティング テーブルに転送情報のミラー イメージが保持されます。ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルが更新され、その変更内容が FIB に反映されます。FIB では、IP ルーティング テーブル内の情報に基づいて、ネクストホップ アドレス情報が保持されます。FIB にはルーティング テーブル内の既知のルートがすべて格納されるため、CEF ではルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。
- ネットワーク内のノードがあるリンク層において 1 ホップだけで相互に到達可能な場合、それらのノードは隣接関係にあると見なされます。CEF は、隣接テーブルを使用してレイヤ 2 アドレッシング情報を追加します。隣接テーブルには、すべての FIB エントリのレイヤ 2 ネクストホップ アドレスが格納されます。

スイッチは、ギガビット速度のラインレート IP トラフィックを達成するために Application Specific Integrated Circuit（ASIC; 特定用途向け集積回路）を使用するため、CEF 転送はソフトウェア転送パス（CPU によって転送されるトラフィック）にだけ適用されます。

デフォルトでは、CEF はグローバルにイネーブルになっています。何らかの理由でディセーブルになった場合は、**ip cef** グローバル コンフィギュレーション コマンドを使用すると、再度イネーブルにすることができます。

デフォルト設定では、すべてのレイヤ 3 インターフェイスで CEF がイネーブルになっています。**no ip route-cache cef** インターフェイス コンフィギュレーション コマンドを入力すると、ソフトウェアが転送するトラフィックに対して CEF がディセーブルになります。このコマンドは、ハードウェア転送パスには影響しません。CEF をディセーブルにして **debug ip packet detail** 特権 EXEC コマンドを使用すると、ソフトウェア転送トラフィックを簡単にデバッグできます。ソフトウェア転送パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。

注意　CLI には、インターフェイス上で CEF をディセーブルにするための **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、デバッグ以外の目的では、インターフェイス上で CEF をディセーブルにしないでください。

ディセーブルになっている CEF をグローバルにイネーブルにしたり、ソフトウェア転送トラフィックのインターフェイス上でイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip cef**	CEF の動作をイネーブルにします。

	コマンド	目的
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip route**-cache cef	ソフトウェア転送トラフィック用のインターフェイスで CEF をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip cef**	すべてのインターフェイスの CEF ステータスを表示します。
ステップ 7	**show cef linecard** [**detail**]	CEF 関連のインターフェイス情報を表示します。
ステップ 8	**show cef interface** [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスの CEF 詳細情報を表示します。
ステップ 9	**show adjacency**	CEF 隣接テーブルの情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

等価コスト ルーティング パスの個数の設定

同じネットワークへ向かう同じメトリックのルートがルータに複数存在する場合、これらのルートは等価コストであると見なされます。ルーティング テーブルに複数の等価コスト ルートが格納されている場合は、これらを*パラレル パス*と呼ぶこともあります。ネットワークへの等価コスト パスがルータに複数存在する場合、ルータはこれらを同時に使用できます。パラレル パスを使用すると、パスに障害が発生した場合でも冗長性を確保できます。また、使用可能なパスにパケットの負荷を分散させて、使用可能な帯域幅を有効利用することもできます。

等価コスト ルートはルータによって自動的に学習および設定されますが、ルーティング テーブルの IP ルーティング プロトコルでサポートされるパラレル パスの最大数は制御可能です。スイッチ ソフトウェアでは最大 32 の等価コスト ルートを使用できますが、スイッチ ハードウェアでは 1 ルートあたり 17 以上のパスは使用しません。

ルーティング テーブルに格納されるパラレル パスのデフォルトの最大数を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**maximum-paths** *maximum*	プロトコル ルーティング テーブルのパラレル パスの最大数を設定します。指定できる範囲は 1 ～ 16 です。ほとんどの IP ルーティング プロトコルのデフォルト値は 4 ですが、BGP の場合だけ 1 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols**	*Maximum path* フィールドの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト値に戻すには、**no maximum-paths** ルータ コンフィギュレーション コマンドを使用します。

スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートはユーザ定義のルートです。スタティック ユニキャスト ルートを使用すると、送信元と宛先の間のパケットの送受信が指定したパスによって行われるようになります。ルータが特定の宛先へのルートを作成できない場合、スタティック ルートが重要になる場合があります。スタティック ルートは、ルーティング不能なすべてのパケットの送信先であるラスト リゾート ゲートウェイを指定する場合に役立ちます。

スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip route** *prefix mask* {*address* | *interface*} [*distance*]	スタティック ルートを確立します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip route**	ルーティング テーブルの現在のステートを表示して、設定を確認します。
ステップ 5	**copy running-config startup-config**	(任意) 設定をコンフィギュレーション ファイルに保存します。

スタティック ルートを削除するには、**no ip route** *prefix mask* {*address* | *interface*} グローバル コンフィギュレーション コマンドを使用します。

スイッチは、ユーザが削除するまでスタティック ルートを保持します。ただし、スタティック ルートは、管理ディスタンスの値を割り当てることによって、ダイナミック ルーティング情報で上書きすることができます。各ダイナミック ルーティング プロトコルには、デフォルトの管理ディスタンスが設定されています（表 41-16 を参照）。ダイナミック ルーティング プロトコルの情報でスタティック ルートを上書きする場合は、スタティック ルートの管理ディスタンスがダイナミック ルーティング プロトコルの管理ディスタンスよりも大きくなるように設定します。

表 41-16　ダイナミック ルーティング プロトコルのデフォルトの管理ディスタンス

ルート送信元	デフォルトのディスタンス
接続されているインターフェイス	0
スタティック ルート	1
拡張 IGRP サマリー ルート	5
外部 BGP	20
内部拡張 IGRP	90
IGRP	100
OSPF	110
内部 BGP	200
不明	225

インターフェイスをポイントするスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルによってアドバタイズされます。**redistribute** スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、ルーティング テーブルでは、インターフェイスをポイントするスタティック ルートが接続されると、そのスタティックな性質が失われたと見なされるためです。ただし、network コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義した場合は、ダイナミック ルーティング プロトコルに **redistribute** スタティック コマンドを指定しない限り、ルートはアドバタイズされません。

インターフェイスがダウンすると、そのインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。転送ルータのアドレスとして指定されたアドレスの有効なネクストホップがスタティック ルート内に見つからなくなった場合は、そのスタティック ルートも IP ルーティング テーブルから削除されます。

デフォルトのルートおよびネットワークの指定

ルータが他のすべてのネットワークへのルートを学習することはできません。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートにスマート ルータを指定します（スマート ルータには、インターネットワーク全体のルーティング テーブル情報が格納されます）。これらのデフォルト ルートは、ダイナミックに学習されるか、ルータごとに設定されます。内部ダイナミック ルーティング プロトコルのほとんどは、スマート ルータを使用して生成したダイナミックなデフォルト情報を他のルータに転送するメカニズムを備えています。

指定されたデフォルト ネットワークに直接接続されたインターフェイスがルータに存在する場合は、その装置上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

ネットワーク用のデフォルトを生成しているルータでは、自身のデフォルト ルートが必要になる場合があります。ルータが自身のデフォルト ルートを生成する方法の 1 つとして、適切な装置を経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定する方法があります。

ネットワークへのスタティック ルートをスタティック デフォルト ルートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip default-network** *network number*	デフォルト ネットワークを指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip route**	ラスト リゾート ゲートウェイで選択されたデフォルト ルートを表示します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルートを削除するには、**no ip default-network** *network number* グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ルーティング プロトコルでデフォルト情報を送信する場合、これ以外の設定は必要ありません。ルーティング テーブルは定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。IGRP ネットワークでは、システムのデフォルト ネットワークの候補が複数存在する場合があります。Cisco ルータでは、管理ディスタンスとメトリック情報を使用して、デフォルト ルートやラスト リゾート ゲートウェイを設定します。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用して、デフォルト ルートの候補を指定します。このネットワークが任意の送信元のルーティング テーブルに格納されている場合は、デフォルト ルートの候補としてフラグ付けされます。ルータにデフォルト ネットワークのインターフェイスが存在しなくても、そこへのパスが格納されていれば、そのネットワークは候補の 1 つと見なされ、最適なデフォルト パスへのゲートウェイがラスト リゾート ゲートウェイになります。

ルート マップによるルーティング情報の再配信

スイッチでは複数のルーティング プロトコルを同時に実行し、ルーティング プロトコル間で情報を再配信することができます。ルーティング プロトコル間での情報の再配信は、サポートされているすべての IP ベース ルーティング プロトコルに適用されます。

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配信を条件付きで制御することもできます。**match** および **set** ルート マップ コンフィギュレーション コマンドは、ルート マップの条件部を定義します。**match** コマンドは、一致する必要がある基準を指定するコマンドです。**set** コマンドは、ルーティング アップデートが match コマンドで定義された条件を満たす場合に実行されるアクションを指定します。再配信はプロトコル独立機能ですが、**match** および **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコルに固有のものです。

match コマンドおよび **set** コマンドは、**route-map** のあとにそれぞれ 1 つまたは複数指定します。**match** コマンドを指定しない場合は、条件がすべて満たされていると見なされます。**set** コマンドを指定しない場合、match コマンド以外の処理は実行されません。このため、**match** または **set** コマンドを少なくとも 1 つ指定する必要があります。

（注）　**set** ルート マップ コンフィギュレーション コマンドが指定されていないルート マップは CPU に送られるため、CPU 使用率が高くなります。

ルート マップ ステートメントは、**permit** または **deny** として指定することもできます。ステートメントが拒否としてマークされている場合、一致基準を満たすパケットは通常の転送チャネルを通じて送り返されます（宛先ベース ルーティング）。ステートメントが許可としてマークされている場合は、一致基準を満たすパケットに set コマンドが適用されます。一致基準を満たしてないパケットは、通常のルーティング チャネルを通じて転送されます。

match コマンドと set コマンドによるエントリの実行が成功すると、BGP ルート マップ **continue** コマンドを使用して、ルート マップの追加エントリを実行できます。**continue** コマンドを使用すると、より多くのモジュラー ポリシー定義を設定および構成できるため、特定のポリシーを同じルート マップ内で繰り返し設定する必要がなくなります。スイッチは、発信ポリシーの **continue** コマンドをサポートしています。ルート マップの **continue** 句の使用方法の詳細については、次の URL にある『BGP Route-Map Continue Support for an Outbound Policy feature guide for Cisco IOS Release 12.4(4)T』を参照してください。
http://www.cisco.com/en/US/products/ps6441/products_feature_guides_list.html

（注）　次に示すステップ 3 ～ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

再配信用のルート マップを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [**permit** | **deny**] [*sequence number*]	再配信の制御に使用するルート マップを定義して、ルート マップ コンフィギュレーション モードを開始します。 *map-tag*：ルート マップ用のわかりやすい名前を指定します。**redistribute** ルータ コンフィギュレーション コマンドは、この名前を使用して対象のルート マップを参照します。複数のルート マップで同じマップ タグ名を共有することもできます。 （任意）**permit** が指定され、このルート マップの一致基準が満たされている場合は、set アクションの制御に従ってルートが再配信されます。**deny** が指定されている場合、ルートは再配信されません。 *sequence number*（任意）：同じ名前ですでに設定されているルート マップのリスト内に設定される、新しいルート マップの位置を示す番号です。
ステップ 3	**match as-path** *path-list-number*	BGP AS パス アクセス リストと一致させます。
ステップ 4	**match community-list** *community-list-number* [**exact**]	BGP コミュニティ リストと一致させます。
ステップ 5	**match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	名前または番号を指定して、標準アクセス リストと一致させます。番号には、1 ～ 199 の整数を指定できます。
ステップ 6	**match metric** *metric-value*	指定されたルート メトリックと一致させます。*metric-value* には、0 ～ 4294967295 の値が指定された EIGRP メトリックを指定できます。
ステップ 7	**match ip next-hop** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	指定されたアクセス リスト（番号 1 ～ 199）のいずれかで送信されるネクストホップ ルータ アドレスと一致させます。
ステップ 8	**match tag** *tag value* [*...tag-value*]	1 つまたは複数のルート タグ値からなるリスト内の指定されたタグ値と一致させます。それぞれ、0 ～ 4294967295 の整数を指定できます。
ステップ 9	**match interface** *type number* [*...type number*]	指定されたインターフェイスの 1 つから指定されたネクストホップへのルートと一致させます。
ステップ 10	**match ip route-source** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	指定されたアドバタイズ済みのアクセス リストによって指定されるアドレスと一致させます。
ステップ 11	**match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**]}	指定された **route-type** と一致させます。 • **local**：ローカルに生成された BGP ルート。 • **internal**：OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート。 • **external**：OSPF 外部ルート（タイプ 1 またはタイプ 2）、または EIGRP 外部ルート。
ステップ 12	**set dampening** *halflife reuse suppress max-suppress-time*	BGP ルート ダンプニングの各要素を設定します。
ステップ 13	**set local-preference** *value*	ローカル BGP パスに値を割り当てます。

	コマンド	目的
ステップ 14	**set origin** {**igp** | **egp** *as* | **incomplete**}	BGP 送信元コードを設定します。
ステップ 15	**set as-path** {**tag** | **prepend** *as-path-string*}	BGP 自律システム パスを変更します。
ステップ 16	**set level** {**level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone**}	ルーティング ドメインの指定エリアにアドバタイズされるルートのレベルを設定します。**stub-area** および **backbone** は、OSPF NSSA およびバックボーンのエリアです。
ステップ 17	**set metric** *metric value*	再配信されるルートに指定するメトリック値を設定します（EIGRP 専用）。*metric value* は、-294967295 ～ 294967295 の整数です。
ステップ 18	**set metric** *bandwidth delay reliability loading mtu*	再配信されるルートに指定するメトリック値を設定します（EIGRP 専用）。 • *bandwidth*：0 ～ 4294967295 の範囲のルートのメトリック値または IGRP 帯域幅（Kbps 単位）。 • *delay*：0 ～ 4294967295 の範囲のルート遅延（10 マイクロ秒単位）。 • *reliability*：パケット送信の成功可能性。0 ～ 255 の数値で表され、255 は信頼性が 100% であること、0 は信頼性がないことを意味します。 • *loading*：0 ～ 255 の数値で表されるルートの有効帯域幅（255 は 100% の負荷）。 • *mtu*：ルートの最大伝送ユニット（MTU）の最小サイズ（バイト単位）。範囲は 0 ～ 4294967295 です。
ステップ 19	**set metric-type** {**type-1** | **type-2**}	再配信されるルートの OSPF 外部メトリック タイプを設定します。
ステップ 20	**set metric-type internal**	ネクストホップの IGP メトリックと一致するように、外部 BGP ネイバーにアドバタイズされるプレフィクスの Multi Exit Discriminator（MED）値を設定します。
ステップ 21	**set weight**	ルーティング テーブルの BGP のウェイトを設定します。指定できる値の範囲は、1 ～ 65535 です。
ステップ 22	**end**	特権 EXEC モードに戻ります。
ステップ 23	**show route-map**	設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示して、設定を確認します。
ステップ 24	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

エントリを削除するには、**no route-map** *map tag* グローバル コンフィギュレーション コマンド、または **no match** や **no set** ルート マップ コンフィギュレーション コマンドを使用します。

ルーティング ドメイン間でルートを配信したり、ルートの再配信を制御したりすることができます。

ルートの再配信を制御するには、特権 EXEC モードで次の手順を実行します。キーワードは、上記の手順で定義されたキーワードと同じです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type** *type-value*] [**match internal** | **external** *type-value*] [**tag** *tag-value*] [**route-map** *map-tag*] [**weight** *weight*] [**subnets**]	ルーティング プロトコル間でルートを再配信します。route-map を指定しない場合、すべてのルートが再配信されます。キーワード **route-map** に *map-tag* を指定しないと、ルートは配信されません。
ステップ 4	**default-metric** *number*	現在のルーティング プロトコルで、再配信されたすべてのルートに対して同じメトリック値が使用されるように設定します（BGP、RIP、OSPF）。
ステップ 5	**default-metric** *bandwidth delay reliability loading mtu*	EIGRP ルーティング プロトコルで、EIGRP 以外で再配信されたすべてのルートに対して同じメトリック値が使用されるように設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show route-map**	設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示して、設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

再配信をディセーブルにするには、このコマンドの **no** 形式を使用します。

ルーティング プロトコルのメトリックは、必ずしも別のルーティング プロトコルのメトリックに変換する必要はありません。たとえば、RIP メトリックはホップ カウントで、IGRP メトリックは 5 つの特性の組み合わせです。このような場合は、設定したメトリックを再配信されたルートに割り当てます。さまざまなルーティング プロトコル間でルーティング情報を制御せずに交換すると、ルーティング ループが発生し、ネットワークの動作が著しく低下することもあります。

メトリック変換の代わりに使用されるデフォルトの再配信メトリックが定義されていない場合は、ルーティング プロトコル間で自動メトリック変換が行われることもあります。

- RIP はスタティック ルートを自動的に再配信することができます。スタティック ルートのメトリックには 1（直接接続）が割り当てられます。
- デフォルト モードが有効になっている場合、どのプロトコルでも他のルーティング プロトコルを再配信することができます。

ポリシーベース ルーティングの設定

ポリシーベース ルーティング（PBR）を使用すると、トラフィック フローの定義済みポリシーを設定できます。PBR を使用してルーティングをより細かく制御するには、ルーティング プロトコルから取得したルートの信頼度を小さくします。PBR では、次の基準に基づいて、パスを許可または拒否するルーティング ポリシーを指定したり、実装したりすることができます。

- 特定のエンド システムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスおよび送信元依存のルーティング、対話形式とバッチ トラフィックに基づくルーティング、専用リンクに基づくルーティングを実現できます。たとえば、在庫記録を本社に送信する場合は高帯域幅で高コストのリンクを短時間使用し、電子メールなど日常的に使用するアプリケーション データは低帯域幅で低コストのリンクで送信することができます。

PBR を使用する場合は、Access Control List（ACL; アクセス制御リスト）を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。PBR は着信パケットに適用されます。PBR がイネーブルのインターフェイスで受信されたすべてのパケットは、ルート マップを通過します。パケットは、ルート マップで定義された基準に基づいて、適切なネクストホップに転送（ルーティング）されます。

- パケットがどのルート マップ ステートメントとも一致しない場合は、すべての set コマンドが適用されます。
- ステートメントが許可としてマークされている場合、どのルート マップ ステートメントとも一致しないパケットは通常の転送チャネルを通じて送信され、宛先ベースのルーティングが実行されます。
- PBR では、拒否としてマークされているルート マップ ステートメントはサポートされていません。

ルート マップの設定の詳細については、「ルート マップによるルーティング情報の再配信」（P.41-94）を参照してください。

標準 IP ACL を使用すると、アプリケーション、プロトコル タイプ、またはエンド ステーションに基づいて一致基準を指定するように、送信元アドレスまたは拡張 IP ACL の一致基準を指定することができます。このプロセスは、一致が見つかるまでルート マップを介して行われます。一致が見つからない場合は、通常の宛先ベース ルーティングが行われます。match ステートメント リストの末尾には、暗黙的な拒否エントリがあります。

match コマンドの条件が満たされた場合は、set コマンドを使用して、パス内のネクストホップ ルータを識別する IP アドレスを指定することができます。

PBR のコマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。スイッチ プロンプトで疑問符を入力した場合に表示されるにもかかわらず、このスイッチでサポートされない PBR コマンドのリストについては、付録 C「Cisco IOS Release 12.2(55)SE でサポートされていないコマンド」を参照してください。

（注）　このソフトウェア リリースでは、IPv4 および IPv6 のトラフィックを処理する場合の PBR はサポートされていません。

PBR 設定時の注意事項

PBR を設定するときには、次の点に注意してください。

- PBR を使用するには、IP サービス イメージをスイッチにインストールする必要があります。
- マルチキャスト トラフィックに対しては、ポリシーによるルーティングは行われません。PBR は、ユニキャスト トラフィックに対してだけ適用されます。
- PBR は、ルーテッド ポートまたは SVI 上でイネーブルにできます。
- スイッチでは、PBR の **route-map deny** ステートメントはサポートされていません。
- レイヤ 3 モードの EtherChannel ポート チャネルにはポリシー ルート マップを適用できますが、EtherChannel のメンバーである物理インターフェイスには適用できません。適用しようとすると、コマンドが拒否されます。ポリシー ルートマップが適用されている物理インターフェイスは、EtherChannel のメンバーになることができません。
- スイッチでは、最大 246 の IP ポリシー ルートマップを定義できます。

- スイッチでは、最大 512 の Access Control Entry（ACE; アクセス制御エントリ）を PBR 用に定義できます。
- ルート マップ内に一致基準を設定する場合は、次の注意事項に従ってください。
  - ローカル アドレス宛てのパケットを許可する ACL と一致させないでください。PBR はこれらのパケットを転送するため、ping または Telnet が失敗したり、ルート プロトコルのフラッピングが発生したりする可能性があります。
  - 拒否 ACE を含む ACL と一致させないでください。拒否 ACE と一致するパケットは CPU に送られるため、CPU 使用率が高くなる可能性があります。
- PBR を使用するには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用して、まずルーティング テンプレートをイネーブルにする必要があります。VLAN またはデフォルトのテンプレートでは、PBR はサポートされません。SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」を参照してください。
- スイッチ インターフェイスでは、VRF と PBR は、相互に排他的な関係にあります。PBR がインターフェイスでイネーブルになっている場合は、VRF をイネーブルにすることはできません。その逆も同様で、VRF がインターフェイスでイネーブルになっている場合は、PBR をイネーブルにはできません。
- スイッチ インターフェイスでは、Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）と PBR は、相互に排他的な関係にあります。PBR がインターフェイスでイネーブルになっている場合は、WCCP をイネーブルにすることはできません。その逆も同様で、WCCP がインターフェイスでイネーブルになっている場合は、PBR をイネーブルにはできません。
- PBR で使用される ternary content addressable memory（TCAM; 三値連想メモリ）のエントリの数は、ルート マップ自体、使用される ACL、ACL とルート マップ エントリの順序によって異なります。
- パケット長、Type of Service（ToS; サービス タイプ）、set interface、set default next hop、または set default interface に基づくポリシーベース ルーティングはサポートされていません。有効な set アクションが設定されていないポリシー マップ、または set アクションが *Don't Fragment* に設定されているポリシー マップは、サポートされません。
- スイッチでは、サービス品質（QoS）DSCP および PBR ルート マップ内で一致する IP precedence がサポートされています。ただし、次の制限事項があります。
  - QoS DSCP 変換マップと PBR ルート マップを同じインターフェイスに適用することはできません。
  - DSCP の透過性と PBR DSCP ルート マップを同じスイッチに設定することはできません。
  - PBR を QoS DSCP とともに設定すると、QoS をイネーブルに設定（**mls qos** グローバル コンフィギュレーション コマンドを入力）することも、ディセーブルに設定（**no mls qos** コマンドを入力）することもできます。QoS がイネーブルになっている場合に、トラフィックの DSCP 値が変更されないようにするには、**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを入力して、トラフィックがスイッチに入るポートの DSCP 信頼状態を設定する必要があります。信頼状態が DSCP 以外の場合、デフォルトでは、信頼されていないすべてのトラフィックの DSCP 値が 0 に設定されます。

PBR のイネーブル化

デフォルトでは、スイッチの PBR はディセーブルになっています。PBR をイネーブルにするには、一致基準および match コマンドとすべて一致した場合のアクションを指定するルート マップを作成する必要があります。次に、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにします。指定したインターフェイスに着信したパケットのうち、match コマンドと一致したものはすべて PBR の対象になります。

PBR の高速スイッチングや実装は、スイッチの速度を低下させない速度で行うことができます。高速スイッチングされた PBR では、ほとんどの match および set コマンドを使用できます。PBR の高速スイッチングをイネーブルにするには、事前に PBR をイネーブルにしておく必要があります。デフォルトでは、PBR の高速スイッチングはディセーブルになっています。

スイッチで生成されたパケット（ローカル パケット）に対しては、通常のポリシー ルーティングは行われません。スイッチ上でローカル PBR をグローバルにイネーブルにすると、そのスイッチから送信されたすべてのパケットがローカル PBR の影響を受けます。デフォルトでは、ローカル PBR はディセーブルになっています。

PBR を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [**permit**] [*sequence number*]	パケットの出力場所の制御に使用するルート マップを定義して、ルート マップ コンフィギュレーション モードを開始します。 • *map-tag*：ルート マップ用のわかりやすい名前を指定します。**ip policy route-map** インターフェイス コンフィギュレーション コマンドは、この名前を使用してルート マップを参照します。複数のルート マップで同じマップ タグ名を共有することもできます。 • （任意）**permit** が指定され、このルート マップの一致基準が満たされている場合は、set アクションの制御に従ってルートがポリシー ルーティングされます。 **（注）** インターフェイスに適用される PBR ルート マップでは、**route-map deny** ステートメントはサポートされません。 • *sequence number*（任意）：同じ名前ですでに設定されているルート マップのリスト内で、新しいルート マップの位置を示す番号です。
ステップ 3	**match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	1 つまたは複数の標準または拡張アクセス リストで許可されている、送信元および宛先の IP アドレスを一致させます。 **（注）** 拒否 ACE を含む ACL、またはローカル アドレス宛てのパケットを許可する ACL は入力しないでください。 **match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。
ステップ 4	**set ip next-hop** *ip-address* [*...ip-address*]	基準と一致するパケットのアクションを指定します。パケットのルーティング先となるネクストホップを設定します（ネクストホップは隣接している必要があります）。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンド	目的
ステップ 7	**ip policy route-map** *map-tag*	レイヤ 3 インターフェイスの PBR をイネーブルにして、使用するルート マップを指定します。1 つのインターフェイスに設定できるルート マップは 1 つだけです。ただし、シーケンス番号が異なる複数のルート マップ エントリを設定することができます。これらのエントリは、最初の一致が見つかるまで、シーケンス番号順に評価されます。一致が見つからない場合、パケットは通常どおりにルーティングされます。 **（注）** IP ポリシー ルート マップに **deny** ステートメントが含まれている場合、設定が失敗します。
ステップ 8	**ip route-cache policy**	（任意）PBR の高速スイッチングをイネーブルにします。PBR の高速スイッチングをイネーブルにするには、まず PBR をイネーブルにする必要があります。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ip local policy route-map** *map-tag*	（任意）ローカル PBR をイネーブルにして、スイッチから送信されるパケットに対してポリシーベース ルーティングを実行します。ローカル PBR は、スイッチで生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show route-map** [*map-name*]	（任意）設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示して、設定を確認します。
ステップ 13	**show ip policy**	（任意）インターフェイスに適用されたポリシー ルート マップを表示します。
ステップ 14	**show ip local policy**	（任意）ローカル ポリシー ルーティングがイネーブルになっているかどうかを表示します。イネーブルになっている場合は、使用されているルート マップが表示されます。
ステップ 15	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

エントリを削除するには、**no route-map** *map-tag* グローバル コンフィギュレーション コマンド、または **no match** や **no set** ルート マップ コンフィギュレーション コマンドを使用します。インターフェイスの PBR をディセーブルにするには、**no ip policy route-map** *map-tag* インターフェイス コンフィギュレーション コマンドを使用します。PBR の高速スイッチングをディセーブルにするには、**no ip route-cache policy** インターフェイス コンフィギュレーション コマンドを使用します。スイッチから送信されたパケットに対するポリシーベース ルーティングをディセーブルにするには、**ip local policy route-map** *map-tag* グローバル コンフィギュレーション コマンドを使用します。

ルーティング情報のフィルタリング

ルーティング プロトコル情報をフィルタリングするには、次の手順を実行します。

（注） OSPF プロセス間でルートが再配信される場合、OSPF メトリックは保持されません。

受動インターフェイスの設定

ローカル ネットワーク上の他のルータがルートをダイナミックに学習しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用して、ルーティング アップデート メッセージがルータ インターフェイスから送信されないようにします。OSPF プロトコルでこのコマンドを使用すると、パッシブに指定したインターフェイス アドレスが OSPF ドメインのスタブ ネットワークとして表示されます。OSPF ルーティング情報は、指定されたルータ インターフェイスに対して送受信されません。

インターフェイスが多数存在するネットワークで、インターフェイスを手動でパッシブに設定する作業を省くためには、**passive-interface default** ルータ コンフィギュレーション コマンドを使用して隣接関係が必要なインターフェイスを手動で設定し、すべてのインターフェイスがデフォルトでパッシブになるように設定します。

パッシブ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**passive-interface** *interface-id*	指定されたレイヤ 3 インターフェイスによるルーティング アップデートの送信を抑制します。
ステップ 4	**passive-interface default**	（任意）すべてのインターフェイスを、デフォルトでパッシブとなるように設定します。
ステップ 5	**no passive-interface** *interface type*	（任意）隣接関係を送信する必要があるインターフェイスだけをアクティブにします。
ステップ 6	**network** *network-address*	（任意）ルーティング プロセス用のネットワーク リストを指定します。*network-address* は IP アドレスです。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

パッシブとしてイネーブルにしたインターフェイスを確認するには、**show ip ospf interface** などのネットワーク モニタ用特権 EXEC コマンドを使用します。アクティブとしてイネーブルにしたインターフェイスを確認するには、**show ip interface** 特権 EXEC コマンドを使用します。

ルーティング アップデートの送信を再度イネーブルにするには、**no passive-interface** *interface-id* ルータ コンフィギュレーション コマンドを使用します。**default** キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。次に、**no passive-interface** ルータ コンフィギュレーション コマンドを使用して、隣接関係を必要とする各インターフェイスを設定します。**default** キーワードは、多くの配信ルータに 200 を超えるインターフェイスが備えられているインターネット サービス プロバイダーや大規模な企業ネットワークの場合に役立ちます。

ルーティング アップデートのアドバタイズおよび処理の制御

distribute-list ルータ コンフィギュレーション コマンドをアクセス制御リストと組み合わせて使用すると、ルーティング アップデートにおけるルートのアドバタイズを抑制し、他のルータが 1 つまたは複数のルートを学習しないようにすることができます。この機能を OSPF で使用した場合は外部ルートにだけ適用されるため、インターフェイス名を指定することができません。

distribute-list ルータ コンフィギュレーション コマンドを使用すると、着信アップデートにリストされている特定のルートを処理しないようにすることもできます（OSPF にはこの機能は適用されません）。

ルーティング アップデートのアドバタイズまたは処理を制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distribute-list** {*access-list-number* | *access-list-name*} **out** [*interface-name* | *routing process* | *autonomous-system-number*]	アクセス リスト内のアクションに応じて、ルーティング アップデート内のルートのアドバタイズを許可または拒否します。
ステップ 4	**distribute-list** {*access-list-number* | *access-list-name*} **in** [*type-number*]	アップデートにリストされているルートの処理を抑制します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フィルタを変更またはキャンセルするには、**no distribute-list in** ルータ コンフィギュレーション コマンドを使用します。アップデートにおけるネットワーク アドバタイズの抑制をキャンセルするには、**no distribute-list out** ルータ コンフィギュレーション コマンドを使用します。

ルーティング情報の送信元のフィルタリング

ルーティング情報には他の情報よりも正確なものもあるため、フィルタリングを使用して、さまざまな送信元から送られる情報の優先付けを行うことができます。*管理ディスタンス*は、ルータやルータのグループなど、ルーティング情報の送信元の信頼性を示す数値です。大規模なネットワークでは、他のルーティング プロトコルよりも信頼性が高いルーティング プロトコルが存在する場合があります。管理ディスタンスの値を指定すると、ルータはルーティング情報の送信元をインテリジェントに区別できるようになります。ルータは常に、ルーティング プロトコルの管理ディスタンスが最短のルートを選択します。表 41-16（P.41-92）に、各ルーティング情報の送信元のデフォルトの管理ディスタンスを示します。

各ネットワークには独自の要件があるため、管理ディスタンスの割り当てにおける全般的な注意事項はありません。

ルーティング情報の送信元をフィルタリングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distance** *weight* {*ip-address* {*ip-address mask*}} [*ip access list*]	管理ディスタンスを定義します。 *weight*：管理ディスタンスは 10 ～ 255 の整数です。単独で使用する場合、*weight* はデフォルトの管理ディスタンスを示します。ルーティング情報の送信元として他に指定されているものがない場合に使用されます。管理ディスタンスが 255 のルートは、ルーティング テーブルに格納されません。 （任意）*ip access list*：着信ルーティング アップデートに適用される IP 標準または拡張アクセス リストです。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show ip protocols**	指定されたルーティング プロセス用のデフォルトの管理ディスタンスを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

管理ディスタンスの定義を削除するには、**no distance** ルータ コンフィギュレーション コマンドを使用します。

認証キーの管理

キーの管理は、ルーティング プロトコルで使用される認証キーを制御する方法です。一部のプロトコルでは、キーの管理を使用することができません。認証キーは、EIGRP および RIP バージョン 2 で使用できます。

認証キーを管理するには、認証をイネーブルにする必要があります。プロトコルの認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。認証キーを管理するには、キー チェーンを定義して、そのキー チェーンに属するキーと各キーの有効期間を指定します。各キーには、ローカルに格納される固有のキー ID が設定されます（**key** *number* キー チェーン コンフィギュレーション コマンドで指定）。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5（MD5）認証キーが一意に識別されます。

有効期間が指定された複数のキーを設定できます。存在する有効なキーの個数に関係なく、1 つの認証パケットだけが送信されます。キー番号は小さい方から大きい方へ順に調べられ、最初に見つかった有効なキーが使用されます。キーの変更中は、存続時間が重なっても問題ありません。これらの存続時間は、ルータで認識されている必要があります。

認証キーを管理するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**key chain** *name-of-chain*	キー チェーンを指定して、キー チェーン コンフィギュレーション モードを開始します。
ステップ 3	**key** *number*	キー番号を指定します。指定できる範囲は 0 ～ 2147483647 です。
ステップ 4	**key-string** *text*	キー文字列を指定します。キー文字列には 1 ～ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定することはできません。
ステップ 5	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）キーの受信可能期間を指定します。 *start-time* および *end-time* 構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。

	コマンド	目的
ステップ 6	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）キーの送信可能期間を指定します。 *start-time* および *end-time* 構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は infinite です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show key chain**	認証キーの情報を表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

キー チェーンを削除するには、**no key chain** *name-of-chain* グローバル コンフィギュレーション コマンドを使用します。

IP ネットワークのモニタおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。ルートの消去やステータスの表示を行うには、表 41-17 に示す特権 EXEC コマンドを使用します。

表 41-17　IP ルートの消去またはルート ステータスの表示を行うコマンド

コマンド	目的
clear ip route {*network* [*mask* | *]}	IP ルーティング テーブルから 1 つまたは複数のルートを消去します。
show ip protocols	アクティブなルーティング プロトコル プロセスのパラメータおよびステートを表示します。
show ip route [*address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]]	ルーティング テーブルの現在のステートを表示します。
show ip route summary	ルーティング テーブルの現在のステートをサマリー形式で表示します。
show ip route supernets-only	スーパーネットを表示します。
show ip cache	IP トラフィックのスイッチングに使用されるルーティング テーブルを表示します。
show route-map [*map-name*]	設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示します。

CHAPTER 42

IPv6 ユニキャスト ルーティングの設定

この章では、IE 3000 スイッチに IPv6 ユニキャスト ルーティングを設定する方法について説明します。

（注） この章のすべての IPv6 機能を使用するには、スイッチスタックで IP サービス イメージを実行している必要があります。IP ベース イメージを実行するスイッチは、IPv6 スタティック ルーティングおよび IPv6 用の RIP だけをサポートしています。

IPv6 Multicast Listener Discovery（MLD）スヌーピングの設定については、第 43 章「IPv6 MLD スヌーピングの設定」を参照してください。IPv6 Access Control List（ACL; アクセス制御リスト）の設定については、第 44 章「IPv6 ACL の設定」を参照してください。IPv4 ユニキャスト ルーティングの設定については、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。

IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを使用するように、スイッチを設定する必要があります。「デュアル IPv4/IPv6 プロトコル スタック」（P.42-5）を参照してください。

（注） この章で説明するコマンドの構文および使用方法の詳細については、手順に記載された Cisco IOS のマニュアルを参照してください。

この章で説明する内容は、次のとおりです。

IPv6 の概要

IPv4 ユーザは IPv6 に移行して、エンドツーエンド セキュリティ、Quality of Service（QoS; サービス品質）、グローバルに一意のアドレスなどのサービスを利用できます。IPv6 では、アドレス レンジが広いため、プライベート アドレスや、ネットワーク エッジの境界ルータでの Network Address Translation（NAT; ネットワーク アドレス変換）処理の必要性が削減されます。

シスコシステムズの IPv6 実装については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

この章での IPv6 およびその他の機能についての情報

- 次の URL にある『*Cisco IOS IPv6 Configuration Library*』を参照してください。
  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t.html
- [Search] フィールドを使用して、Cisco IOS ソフトウェア マニュアルを探してください。たとえば、スタティック ルートについての情報が必要な場合は、[Search] フィールドに「*Implementing Static Routes for IPv6*」と入力し、スタティック ルートについての次のマニュアルを見つけることができます。
  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html

ここでは、スイッチでの IPv6 の実装について説明します。

- 「IPv6 アドレス」（P.42-2）
- 「IPv6 ユニキャスト ルーティングのサポートされる機能」（P.42-3）
- 「IPv6 ユニキャスト ルーティングのサポートされない機能」（P.42-9）
- 「制限事項」（P.42-9）

IPv6 アドレス

スイッチは IPv6 ユニキャスト アドレスだけをサポートします。サイトローカル ユニキャスト アドレス、エニーキャスト アドレス、またはマルチキャスト アドレスはサポートしません。

IPv6 の 128 ビット アドレスは、コロンで区切られた 8 個の 16 ビットの 16 進数フィールドで表されます。n:n:n:n:n:n:n:n という形式です。次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするため、各フィールドの先行ゼロは省略可能です。上記のアドレスの先行ゼロをのぞいた表現を次に示します。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）でゼロが連続する 16 進数フィールドを表すこともできますが、この短縮バージョンを使用できるのは各アドレスの中で 1 回だけです。

2031:0:130F::09C0:080F:130B

IPv6 アドレスの形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

「Implementing Addressing and Basic Connectivity」では、次の項が IE 3000 スイッチに該当します。

- IPv6 Address Formats
- IPv6 Address Type: Unicast
- IPv6 Address Output Display
- Simplified IPv6 Packet Header

IPv6 ユニキャスト ルーティングのサポートされる機能

ここでは、スイッチでサポートされる IPv6 プロトコルの機能について説明します。

スイッチは、拡張アドレス機能、ヘッダー形式の単純化、拡張機能およびオプションのサポートの向上、拡張ヘッダーのハードウェア解析などをサポートします。また、ソフトウェアでルーティングまたはブリッジングされる、ホップバイホップ拡張ヘッダー パケットをサポートします。

スイッチが IPv6 ルーティング機能を提供する対象としては、ネイティブ イーサネットの Inter-Switch Link（ISL; スイッチ間リンク）またはスタティック ルートの 802.1Q トランク ポート、IPv6 用の Routing Information Protocol（RIP）、Open Shortest Path First（OSPF）バージョン 3 プロトコルなどがあります。スイッチは最大で 16 の等価コスト ルートをサポートし、IPv4 と IPv6 のフレームを同時にラインレートで転送できます。

128 ビット幅ユニキャスト アドレス

スイッチは、集約可能なグローバル ユニキャスト アドレスおよびリンクローカル ユニキャスト アドレスをサポートします。サイトローカル ユニキャスト アドレスはサポートしません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能なグローバル ユニキャスト プレフィクスからの IPv6 アドレスです。このアドレス構造により、ルーティング プレフィクスの厳密な集約が可能になり、グローバル ルーティング テーブルのルーティング テーブル エントリの数が制限されます。これらのアドレスは、組織を通して集約され、最終的にはインターネット サービス プロバイダーに集約されるリンクで使用されます。

  アドレスは、グローバル ルーティング プレフィクス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレスの割り当てでは、バイナリ値 001（2000::/3）で始まるアドレスの範囲が使用されます。プレフィクスが 2000::/3（001）から E000::/3（111）までのアドレスは、Extended Unique Identifier（EUI）-64 形式の 64 ビット インターフェイス ID を持つ必要があります。

- リンクローカル プレフィクス FE80::/10（1111 1110 10）および変更された EUI 形式のインターフェイス ID を使用することで、任意のインターフェイスにリンクローカル ユニキャスト アドレスを自動的に生成できます。Neighbor Discovery Protocol（NDP; ネイバー探索プロトコル）およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカル リンク上のノードはリンクローカル アドレスを使用するため、グローバルに一意のアドレスを必要としません。IPv6 ルータは、発信元または宛先がリンクローカル アドレスであるパケットを、他のリンクに転送しません。

詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」で IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 用の DNS

IPv6 は、Domain Name System（DNS; ドメイン ネーム システム）の名前からアドレスおよびアドレスから名前の検索処理で、DNS レコード タイプをサポートします。DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。スイッチは、IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU 検出

スイッチは、IPv6 ノードに対するシステムの Maximum Transmission Unit（MTU; 最大伝送ユニット）のアドバタイズと、パス MTU 検出をサポートします。パス MTU 検出を使用すると、ホストは特定のデータ パスに沿ったすべてのリンクの MTU サイズの違いをダイナミックに検出して、調整できます。IPv6 では、パスに沿ったリンクがパケット サイズに十分な大きさでない場合は、パケットの送信元がフラグメンテーションを処理します。スイッチは、マルチキャスト パケットのパス MTU 検出をサポートしません。

ICMPv6

IPv6 の Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理やその他の診断機能の実行中にエラーを通知します。IPv6 では、ICMP パケットはネイバー探索プロトコルおよびパス MTU 検出でも使用されます。

ネイバー探索

スイッチは、ICMPv6 上で動作するプロトコルである NDP を IPv6 に対してサポートします。また、NDP をサポートしない IPv6 ステーションのスタティック ネイバー エントリもサポートします。IPv6 ネイバー探索プロセスは、ICMP メッセージと送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）のネイバーのリンクレイヤ アドレスを特定し、ネイバーの到達可能性を確認して、ネイバー ルータを追跡します。

スイッチは、マスク長が 64 ビット未満のルートに対する ICMPv6 リダイレクトをサポートします。ICMP リダイレクトは、ホスト ルートまたはマスク長が 64 ビットより長い集約ルートについてはサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためのネクストホップ 転送情報を取得する処理の間に、スイッチの CPU の負荷が必要以上に大きくならないことが保証されます。スイッチは、アクティブに解決しようとしているものと同じネイバーがネクストホップとして指定されている追加の IPv6 パケットを廃棄します。この廃棄により、CPU の負荷の増大を防ぎます。

デフォルト ルータ プリファレンス

スイッチは、ルータ アドバタイズメント メッセージの拡張機能である IPv6 Default Router Preference（DRP; デフォルト ルータ プリファレンス）をサポートします。DRP を使用すると、ホストはより適切なルータを選択できます。特に、ホストがマルチホームで、ルータが異なるリンク上にある場合に有効です。スイッチは、RFC 4191 のルート情報オプションはサポートしません。

IPv6 ホストは、オフリンクの宛先へのトラフィックに対するルータを選択するためにデフォルト ルータ リストを保持しています。宛先に対して選択されたルータは、宛先キャッシュにキャッシュされます。IPv6 の NDP では、到達可能性が不明または信用できないルータより、到達可能または到達可能の可能性のあるルータが指定されます。到達可能ルータまたは到達可能性が高いルータについて、NDP は毎回同じルータを選択することも、リストのルータを順番に使用することもできます。DRP を使用すると、どちらも到達可能である、または到達可能性が高い 2 つのルータの間で一方を他方より優先するように、IPv6 ホストを設定できます。

IPv6 の DRP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチは、ステートレス自動設定を使用して、ホストとモバイルの IP アドレスの管理など、リンク、サブネット、サイト アドレッシングの変更を管理します。ホストは自立的に独自のリンクローカル アドレスを設定し、起動ノードはルータ送信請求を送信してインターフェイスを設定するためのルータ アドバタイズを要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

IPv6 アプリケーション

スイッチは以下のアプリケーションについて IPv6 をサポートします。

- ping、traceroute、Telnet、TFTP、FTP
- IPv6 トランスポートでの Secure Shell（SSH; セキュア シェル）
- IPv6 トランスポートでの HTTP サーバ アクセス
- IPv4 トランスポートでの AAAA 用 DNS リゾルバ
- IPv6 アドレスに対する Cisco Discovery Protocol（CDP; シスコ検出プロトコル）のサポート

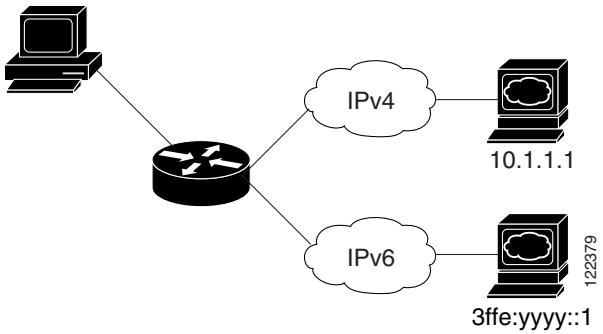
これらのアプリケーションの管理の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」および「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

Ternary Content Addressable Memory（TCAM）の使用を IPv4 プロトコルと IPv6 プロトコルの両方に割り当てるには、IPv4/IPv6 デュアル テンプレートを使用する必要があります。

図 42-1 は、IP パケットと宛先アドレスに基づいて、IPv4 と IPv6 の両方のトラフィックを同じインターフェイスで転送するルータを示しています。

図 42-1　インターフェイス上でのデュアル IPv4/IPv6 のサポート



IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを使用します。デュアル IPv4/IPv6 SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」を参照してください。

デュアル IPv4/IPv6 テンプレートを使用すると、デュアル スタック環境でスイッチを使用できるようになります。

- 先にデュアル IPv4/IPv6 テンプレートを選択しないで IPv6 を設定しようとすると、警告メッセージが表示されます。
- IPv4 だけの環境では、スイッチは IPv4 パケットをルーティングし、ハードウェアで IPv4 QoS と ACL を適用します。IPv6 パケットはサポートされません。
- デュアル IPv4/IPv6 環境では、スイッチは IPv4 と IPv6 の両方のパケットをルーティングし、ハードウェアで IPv4 QoS を適用します。
- IPv6 QoS はサポートされません。
- IPv6 を使用する予定がない場合は、デュアル スタック テンプレートを使用しないでください。このテンプレートを使用すると、各リソースに対する TCAM の容量が少なくなります。

IPv4 および IPv6 のプロトコル スタックの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

IPv6 アドレス割り当てのための DHCP

DHCPv6 を使用すると、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。アドレス割り当て機能は、ホストが接続されているネットワークに基づく正しいプレフィクスでの重複しないアドレス割り当てを管理します。1 つまたは複数のプレフィクス プールからアドレスを割り当てることができます。デフォルト ドメインや DNS ネーム サーバ アドレスなどの追加オプションを、クライアントに返すことができます。特定のインターフェイスや複数のインターフェイスで使用するためにアドレス プールを割り当てることも、サーバで適切なプールを自動的に検出することもできます。

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 のクライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」を参照してください。

IPv6 用のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング装置間の明示的なルートを定義します。スタティック ルートは、外部ネットワークへのパスが 1 つしかない小規模なネットワークの場合や、大規模なネットワークで特定の種類のトラフィックにセキュリティを提供する場合に便利です。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」を参照してください。

IPv6 用の RIP

IPv6 用の Routing Information Protocol（RIP）は、ルーティング メトリックとしてホップ カウントを使用する距離ベクトル プロトコルです。IPv6 のアドレスとプレフィクス、および RIP 更新メッセージの宛先アドレスとしての全 RIP ルータ マルチキャスト グループ アドレス FF02::9 をサポートしています。

IPv6 用の RIP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」を参照してください。

IPv6 用の OSPF

IP サービス イメージを実行するスイッチは、IPv6 の Open Shortest Path First（OSPF）（IP のリンクステート プロトコル）をサポートします。詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSFP for IPv6」の章を参照してください。

IPv6 用の EIGRP

IP サービス イメージを実行するスイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートします。EIGRP は実行しているインターフェイスに設定され、グローバル IPv6 アドレスを必要としません。

実行する前に、EIGRP IPv6 のインスタンスには暗黙的または明示的なルータ ID が必要です。暗黙的なルータ ID はローカル IPv4 アドレスから取得されるので、すべての IPv4 ノードは常に使用可能なルータ ID を持っています。ただし、EIGRP IPv6 は IPv6 ノードだけのネットワークで実行する場合があるため、使用可能な IPv4 ルータ ID がない可能性があります。

IPv6 用の EIGRP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」を参照してください。

IPv6 用の HSRP

IP サービス イメージを実行するスイッチは、IPv6 の Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）をサポートします。HSRP は、単一のルータのアベイラビリティに依存しない冗長なルーティングを IPv6 のトラフィックに提供します。IPv6 ホストは、IPv6 のネイバー探索ルータ アドバタイズメント メッセージを通して使用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP の IPv6 グループは、HSRP グループ番号から取得される仮想 MAC アドレスと、デフォルトでは HSRP の仮想 MAC アドレスから取得される仮想 IPv6 リンクローカル アドレスを持っています。HSRP グループがアクティブになると、HSRP の仮想 IPv6 リンクローカル アドレスに定期的にメッセージが送信されます。このメッセージは、グループがアクティブ状態ではなくなって、最後のメッセージが送信された後で停止します。

IPv6 用の HSRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Configuring First Hop Redundancy Protocols in IPv6」を参照してください。

IPv6 での SNMP と Syslog

IPv4 と IPv6 の両方をサポートするため、IPv6 のネットワーク管理には IPv6 と IPv4 の両方のトランスポートが必要です。IPv6 での Syslog は、これらのトランスポート用のアドレス データ タイプをサポートします。

IPv6 での SNMP と Syslog は、次の機能を提供します。

- IPv4 と IPv6 の両方のサポート
- SNMP 用の IPv6 トランスポート、および IPv6 ホスト用のトラップをサポートするために SNMP エージェントを変更するための IPv6 トランスポート
- IPv6 アドレッシングをサポートするための SNMP 関連および Syslog 関連の MIB
- トラップ レシーバーとしての IPv6 ホストの設定

IPv6 でのサポートの場合、SNMP は IPv4 と IPv6 を同時にサポートするために既存の IP トランスポート マッピングを変更します。次の SNMP 処理は IPv6 のトランスポート管理をサポートします。

- デフォルト設定で User Datagram Protocol（UDP; ユーザ データグラム プロトコル）SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供する
- IPv6 トランスポートで SNMP 通知を送信する
- IPv6 トランスポート用に SNMP 名前付きアクセス リストをサポートする
- IPv6 トランスポートを使用する SNMP プロキシ転送をサポートする
- IPv6 トランスポートでの SNMP マネージャ機能の動作を確認する

設定手順など、IPv6 での SNMP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順など、IPv6 での Syslog の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

IPv6 での HTTP（S）

HTTP クライアントは IPv4 と IPv6 の両方の HTTP サーバに要求を送信し、HTTP サーバは IPv4 と IPv6 の両方の HTTP クライアントからの要求に応答します。コロンで区切られた 16 ビット値を使用した 16 進数形式で、リテラル IPv6 アドレスの URL を指定する必要があります。

受け付けソケット呼び出しは、IPv4 または IPv6 のアドレス ファミリを選択します。受け付けソケットは、IPv4 または IPv6 ソケットです。リスニング ソケットは、接続を示す IPv4 と IPv6 の両方の信号を引き続き待ち受けます。IPv6 リスニング ソケットは、IPv6 のワイルドカード アドレスにバインドされます。

基になっている TCP/IP スタックは、デュアル スタック環境をサポートします。HTTP は TCP/IP スタックとソケットに依存して、ネットワーク層の相互作用を処理します。

HTTP 接続を確立するには、クライアントとサーバ ホストの間に基本的なネットワーク接続（**ping**）が存在している必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」を参照してください。

IPv6 ユニキャスト ルーティングのサポートされない機能

スイッチは、次の IPv6 機能をサポートしていません。

- IPv6 ポリシーベース ルーティング
- IPv6 の Virtual Private Network（VPN; 仮想私設網）Routing and Forwarding（VRF; VPN ルーティング/転送）テーブルのサポート
- IPv6 ルーティング プロトコルのサポート：マルチプロトコル Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）および Intermediate System-to-Intermediate System（IS-IS）ルーティング
- サイトローカル アドレス宛の IPv6 パケット
- IPv4-to-IPv6 や IPv6-to-IPv4 などのトンネリング プロトコル
- IPv4-to-IPv6 または IPv6-to-IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 ユニキャスト Reverse Path Forwarding（RPF）
- IPv6 の汎用プレフィクス

制限事項

IPv6 はスイッチのハードウェアで実装されるので、TCAM での IPv6 圧縮アドレスのために制限事項がいくつか発生します。ハードウェアに関するこれらの制限事項により、失われたり制限されたりする機能があります。

制限される機能は次のとおりです。

- ICMPv6 リダイレクト機能は、IPv6 ホスト ルート（特定のホストに到達するために使用されるルート）またはマスクが 64 ビットより大きい IPv6 ルートについてはサポートされません。スイッチは、ホスト ルートまたはマスクが 64 ビットより大きいルートを通して到達可能な特定の宛先に対するより優れたファーストホップ ルータにホストをリダイレクトすることはできません。
- 等価コスト ルートまたは不等価コスト ルートを使用するロード バランシングは、IPv6 ホスト ルートまたはマスクが 64 ビットより大きい IPv6 ルートについてはサポートされません。
- スイッチは、SNAP でカプセル化された IPv6 パケットを転送できません。

  （注）　IPv4 の SNAP でカプセル化されたパケットにも同様の制限がありますが、パケットはスイッチで廃棄されて転送されません。

- スイッチは IPv6-to-IPv4 および IPv4-to-IPv6 パケットをハードウェアでルーティングしますが、スイッチは IPv6-to-IPv4 トンネルまたは IPv4-to-IPv6 トンネルのエンドポイントになることはできません。
- ホップバイホップ拡張ヘッダーを含む IPv6 ブリッジド パケットは、ソフトウェアで転送されます。IPv4 では、このようなパケット対するルーティングはソフトウェアで行われますが、ブリッジングはハードウェアで行われます。
- ソフトウェア コンフィギュレーション ガイドで定義されている通常の SPAN および RSPAN の制限事項に加えて、IPv6 パケットに固有の次の制限事項があります。
  - IPv6 でルーティングされる RSPAN パケットを送信するとき、SPAN 出力パケットの送信元 MAC アドレスが正しくない場合がある。
  - IPv6 でルーティングされる RSPAN パケットを送信するとき、宛先 MAC アドレスが正しくない場合がある（通常のトラフィックには影響なし）。

- スイッチは、ソースルート IPv6 パケットに対してハードウェアで QoS 分類またはポリシーベース ルーティングを適用できません。
- スイッチは、マルチキャスト パケットに対して ICMPv6 の *パケット サイズ超過*メッセージを生成できません。

IPv6 の設定

ここでは、IPv6 フォワーディングの次の設定情報について説明します。

IPv6 のデフォルト設定

表 42-1 に、IPv6 のデフォルト設定を示します。

表 42-1　IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルト。
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル。
CEFv6 または dCEFv6	ディセーブル（IPv4 CEF および dCEF はデフォルトでイネーブル）。 **（注）** IPv6 ルーティングをイネーブルにすると、CEFv6 および dCEF6 は自動的にイネーブルになります。
IPv6 アドレス	設定なし。

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化

ここでは、IPv6 アドレスを個別のレイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチでグローバルに転送する方法について説明します。

スイッチで IPv6 を設定する場合は、次の注意事項を考慮してください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- この章で説明されている機能の中には、IP サービス イメージを実行する IE 3000 スイッチでサポートされていないものがあります。「IPv6 ユニキャスト ルーティングのサポートされない機能」（P.42-9）を参照してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドの *ipv6-address* および *ipv6-prefix* 変数には、コロンで区切られた 16 ビット値の 16 進数形式で指定したアドレスを入力する必要があります。*prefix-length* 変数（先頭にスラッシュ（/）が付加された値）は、アドレスの上位何ビットがプレフィクス（アドレスのネットワーク部）であるかを示す 10 進値です。

インターフェイスで IPv6 トラフィックを転送するには、そのインターフェイスにグローバル IPv6 アドレスを設定する必要があります。インターフェイスに IPv6 アドレスを設定すると、自動的にリンクローカル アドレスが設定され、そのインターフェイスで IPv6 がアクティブになります。設定されたインターフェイスは、次の必要なマルチキャスト グループをそのリンクに自動的に追加します。

- インターフェイスに割り当てられている各ユニキャスト アドレスに対する送信請求ノード マルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスは、ネイバー探索プロセスで使用されます）
- 全ノード リンクローカル マルチキャスト グループ FF02::1
- 全ルータ リンクローカル マルチキャスト グループ FF02::2

IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IPv6 DHCPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」を参照してください。

IPv6 アドレスをレイヤ 3 インターフェイスに割り当てて IPv6 ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer dual-ipv4-and-ipv6** {**default**| **routing**}	IPv4 と IPv6 をサポートする SDM テンプレートを選択します。 • **default**：スイッチをデフォルト テンプレートに設定して、システム リソースのバランスを取ります。 • **routing**：スイッチをルーティング テンプレートに設定して、IPv4 および IPv6 のルーティングをサポートします（IPv4 のポリシーベース ルーティングを含む）。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**reload**	オペレーティング システムをリロードします。
ステップ 5	**configure terminal**	スイッチのリロード後にグローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。インターフェイスは、物理インターフェイス、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、またはレイヤ 3 EtherChannel のいずれでもかまいません。

	コマンド	目的
ステップ 7	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 8	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **ipv6 address** *ipv6-address* **link-local** または **ipv6 enable**	IPv6 アドレスの下位 64 ビットに、Extended Unique Identifier（EUI）を設定したグローバル IPv6 アドレスを指定します。ネットワーク プレフィクスだけを指定します。最後の 64 ビットはスイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 の処理がイネーブルになります。 インターフェイスで IPv6 をイネーブルにすると自動的に設定されるリンクローカル アドレスの代わりに使用するリンクローカル アドレスをインターフェイスに指定します。このコマンドにより、インターフェイス上で IPv6 の処理がイネーブルになります。 インターフェイスで IPv6 リンクローカル アドレスを自動的に設定し、IPv6 処理用にインターフェイスをイネーブルにします。リンクローカル アドレスは、同じリンク上のノードと通信するためにだけ使用できます。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ip routing**	スイッチ上で IP ルーティングをイネーブルにします。
ステップ 11	**ipv6 unicast-routing**	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ipv6 interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **no ipv6 address** *ipv6-address* **link-local** インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、引数を指定せずに **no ipv6 address** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 アドレスで明示的に設定されていないインターフェイスの IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 プレフィクス 2001:0DB8:c18:1::/64 に基づいて、リンクローカル アドレスとグローバル アドレスの両方で IPv6 をイネーブルにする例を示します。EUI-64 インターフェイス ID は、両方のアドレスの下位 64 ビットで使用されています。**show ipv6 interface** EXEC コマンドの出力では、インターフェイス ID（20B:46FF:FE2F:D940）がインターフェイスのリンクローカル プレフィクス FE80::/64 にどのように追加されているかが示されます。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/1
GigabitEthernet1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
```

```
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

デフォルト ルータ プリファレンスの設定

ルータ アドバタイズメント メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドで設定されるデフォルト ルータ プリファレンス（DRP）の内容とともに送信されます。DRP が設定されていない場合、送信される RA のプリファレンス値は medium になります。

DRP は、リンク上の 2 つのルータが同等であっても、等価コスト ルーティングではなく、ポリシーではホストが一方のルータを優先するように示されている場合に使用すると便利です。

インターフェイス上でルータの DRP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、DRP を指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	**ipv6 nd router-preference** {**high** | **medium** | **low**}	スイッチ インターフェイスでルータに DRP を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IPv6 DRP をディセーブルにするには、**no ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイスでルータにハイの DRP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv6 に DRP を設定する方法の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」を参照してください。

IPv4 および IPv6 プロトコル スタックの設定

IPv6 ルーティングを設定する前に、IPv4 と IPv6 をサポートする SDM テンプレートを選択する必要があります。まだ設定していない場合は、**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} [**desktop**] グローバル コンフィギュレーション コマンドを使用して IPv6 をサポートするテンプレートを設定します。新しいテンプレートを選択する場合は、**reload** 特権 EXEC コマンドを使用してスイッチをリロードし、テンプレートを有効にする必要があります。

IPv4 と IPv6 の両方をサポートするようにレイヤ 3 インターフェイスを設定し、IPv6 ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	スイッチ上でルーティングをイネーブルにします。
ステップ 3	**ipv6 unicast-routing**	スイッチでの IPv6 データ パケットの転送をイネーブルにします。
ステップ 4	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 6	**ip address** *ip-address mask* [**secondary**]	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 7	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **ipv6 address** *ipv6-address* **link-local** または **ipv6 enable**	グローバル IPv6 アドレスを指定します。ネットワーク プレフィクスだけを指定します。最後の 64 ビットはスイッチの MAC アドレスから自動的に計算されます。 インターフェイスで IPv6 をイネーブルにすると自動的に設定されるリンクローカル アドレスの代わりに使用するリンクローカル アドレスをインターフェイスに指定します。 インターフェイスで IPv6 リンクローカル アドレスを自動的に設定し、IPv6 処理用にインターフェイスをイネーブルにします。リンクローカル アドレスは、同じリンク上のノードと通信するためにだけ使用できます。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show interface** *interface-id* **show ip interface** *interface-id* **show ipv6 interface** *interface-id*	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IPv4 ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。IPv6 ルーティングをディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。インターフェイスから IPv4 アドレスを削除するには、**no ip address** *ip-address mask* インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **no ipv6 address** *ipv6-address* **link-local** インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、引数を指定せずに **no ipv6 address** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 アドレスで明示的に設定されていないインターフェイスの IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイスで IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

IPv6 アドレス割り当てのための DHCP の設定

ここでは、Dynamic Host Configuration Protocol for IPv6（DHCPv6）アドレス割り当てを設定する方法について説明します。

デフォルトの DHCPv6 アドレス割り当ての設定

デフォルトでは、DHCPv6 機能はスイッチに設定されません。

DHCPv6 アドレス割り当て設定時の注意事項

DHCPv6 アドレス割り当ての設定時は、次の注意事項を考慮してください。

- 手順では、次のレイヤ 3 インターフェイスのいずれかを指定する必要があります。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイスでイネーブルにする必要があります。
  - SVI：**interface vlan** *vlan_id* コマンドを使用して作成された VLAN インターフェイス。
  - レイヤ 3 モードでの EtherChannel ポート チャネル：**interface port-channel port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。
- DHCPv6 を設定するには、IPv4 と IPv6 をサポートする Switch Database Management（SDM）テンプレートを選択する必要があります。
- スイッチは、DHCPv6 クライアント、サーバ、またはリレー エージェントとして動作できます。DHCPv6 クライアント、サーバ、およびリレー機能は、1 つのインターフェイスでは同時に指定できません。

DHCPv6 サーバ機能のイネーブル化

インターフェイスで DHCPv6 サーバ機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 dhcp pool** *poolname*	DHCP プール コンフィギュレーション モードを開始し、IPv6 DHCP プールの名前を定義します。プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 3	**address prefix** *IPv6-prefix* **lifetime** *{t1 t1* | **infinite***}*	(任意)アドレス割り当てのアドレス プレフィクスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数にする必要があります。 **lifetime** *t1 t1* : IPv6 アドレス プレフィクスが有効な状態を維持する時間（秒単位）を指定します。指定できる範囲は 5 ～ 4294967295 秒です。時間間隔を指定しない場合は、**infinite** を指定します。
ステップ 4	**link-address** *IPv6-prefix*	(任意）リンクアドレス IPv6 プレフィクスを指定します。 着信インターフェイスのアドレスまたはパケット内のリンクアドレスが指定の IPv6 プレフィクスと一致した場合、サーバは構成情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数にする必要があります。
ステップ 5	**vendor-specific** *vendor-id*	(任意）ベンダー固有コンフィギュレーション モードを開始し、ベンダー固有の ID 番号を入力します。この番号はベンダーの IANA 民間企業番号です。指定できる範囲は 1 ～ 4294967295 です。
ステップ 6	**suboption** *number {***address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string}*	(任意）*ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進数の文字列をサブオプション パラメータによって定義されたものとして入力します。*
ステップ 7	**exit**	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンド	目的
ステップ 10	**ipv6 dhcp server** [*poolname* | **automatic***]* *[***rapid-commit***]* *[***preference** *value]* *[***allow-hint***]*	インターフェイスで DHCPv6 サーバ機能をイネーブルにします。 • *poolname*：（任意）IPv6 DHCP プール用にユーザ定義された名前。プール名は、記号文字列（Engineering など）または整数（0 など）です。 • **automatic**：（任意）クライアントにアドレスを割り当てる際に使用するプールをシステムが自動的に決定できるようにします。 • **rapid-commit**：（任意）2 つのメッセージ交換方式を可能にします。 • **preference** *value*：（任意）サーバが送信するアドバタイズ メッセージの preference オプションで伝送される preference 値。指定できる範囲は 0 ～ 255 です。デフォルトの preference 値は 0 です。 • **allow-hint**：（任意）サーバが送信請求メッセージでクライアントの提案を考慮するかどうか指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ipv6 dhcp pool** または **show ipv6 dhcp interface**	DHCPv6 プールの設定を確認します。 インターフェイスで DHCPv6 サーバ機能がイネーブルになっていることを確認します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

DHCPv6 プールを削除するには、**no ipv6 dhcp pool** *poolname* グローバル コンフィギュレーション コマンドを使用します。DHCPv6 プールの特性を変更するには、DHCP プール コンフィギュレーション モード コマンドの **no** 形式を使用します。インターフェイスでの DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、*engineering with an IPv6 address prefix* というプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)#address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 つのリンクアドレスと IPv6 のアドレス プレフィクスで *testgroup* という名前のプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次の例では、ベンダー固有のオプションのある *350* というプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
```

```
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化

インターフェイスで DHCPv6 クライアント機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ipv6 address dhcp** [**rapid-commit**]	インターフェイスで DHCPv6 サーバから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当ての 2 つのメッセージ交換方式を可能にします。
ステップ 4	**ipv6 dhcp client request** [**vendor-specific**]	（任意）インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 dhcp interface**	インターフェイスで DHCPv6 クライアントがイネーブルになっていることを確認します。

DHCPv6 クライアント機能をディセーブルにするには、**no ipv6 address dhcp** インターフェイス コンフィギュレーション コマンドを使用します。DHCPv6 クライアント要求を削除するには、**no ipv6 address dhcp client request** インターフェイス コンフィギュレーション コマンドを使用します。

次に、IPv6 アドレスを取得し、rapid-commit オプションをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 のクライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」を参照してください。

IPv6 ICMP レート制限の設定

デフォルトでは、ICMP レート制限はイネーブルになっています。エラー メッセージ間のデフォルトの間隔は 100 ミリ秒、バケット サイズ（バケットに格納されるトークンの最大数）は 10 です。

ICMP のレート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 icmp error-interval** *interval* [*bucketsize*]	IPv6 ICMP エラー メッセージの間隔とバケット サイズを設定します。 • *interval*：バケットにトークンが追加される間隔（ミリ秒単位）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize*：（任意）バケットに格納されるバケットの最大数。指定できる範囲は 1 ～ 200 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 interface** [*interface-id*]	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ipv6 icmp error-interval** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 ICMP のエラー メッセージの間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Switch(config)#ipv6 icmp error-interval 50 20
```

IPv6 に対する CEF の設定

Cisco Express Forwarding（CEF）は、ネットワーク パフォーマンスを向上させるレイヤ 3 IP スイッチング テクノロジーです。IPv6 CEF はデフォルトではディセーブルですが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ユニキャスト パケットをルーティングするには、まず **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 ユニキャスト パケット転送をグローバルに設定する必要があります。**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用して、IPv6 アドレスと IPv6 処理をインターフェイスに設定する必要があります。

IPv6 CEF をディセーブルにするには、**no ipv6 cef** グローバル コンフィギュレーション コマンドを使用します。ディセーブルにした IPv6 CEF または dCEF を再びイネーブルにするには、**ipv6 cef** グローバル コンフィギュレーション コマンドを使用します。**show ipv6 cef** 特権 EXEC コマンドを入力すると、IPv6 ステートを確認できます。

CEF と dCEF の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

IPv6 に対するスタティック ルートの設定

スタティック IPv6 ルートを設定するには、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、少なくとも 1 つのレイヤ 3 インターフェイスに IPv6 アドレスを設定して IPv6 をイネーブルにする必要があります。

IPv6 スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*]	スタティック IPv6 ルートを設定します。 • *ipv6-prefix* : スタティック ルートの宛先である IPv6 ネットワーク。スタティック ホスト ルートの設定では、ホスト名を指定することもできます。 • */prefix length* : IPv6 プレフィクスの長さ。アドレスの上位何ビットがプレフィクス（アドレスのネットワーク部）であるかを示す 10 進値です。スラッシュ記号を 10 進値の前に付ける必要があります。 • *ipv6-address* : 指定されたネットワークに到達するために使用できるネクストホップの IPv6 アドレス。ネクストホップの IPv6 アドレスは直接接続されている必要はありません。直接接続されているネクストホップの IPv6 アドレスを検索するために、再帰処理が行われます。このアドレスは、コロンで区切られた 16 ビット値を使用した 16 進数形式で指定する必要があります。 • *interface-id* : ポイントツーポイント インターフェイスおよびブロードキャスト インターフェイスから直接スタティック ルートを指定します。ポイントツーポイント インターフェイスでは、ネクストホップの IPv6 アドレスを指定する必要はありません。ブロードキャスト インターフェイスでは、ネクストホップの IPv6 アドレスを常に指定するか、指定されたプレフィクスをリンクに割り当ててリンクローカル アドレスをネクストホップとして指定する必要があります。必要に応じて、パケットの送信先であるネクストホップの IPv6 アドレスを指定できます。 **（注）** ネクストホップとしてリンクローカル アドレスを使用する場合は（リンクローカル ネクストホップは、隣接ルータでもある必要があります）、*interface-id* を指定する必要があります。 • *administrative distance* :（任意）管理ディスタンスです。指定できる範囲は 1 ～ 254 です。デフォルト値は 1 で、接続されたルートを除く他のすべてのルート タイプより優先されるスタティック ルートを指定します。フローティング スタティック ルートを設定するには、ダイナミック ルーティング プロトコルの管理ディスタンスよりも大きい管理ディスタンスを使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**recursive**] [**detail**] または **show ipv6 route static** [*updated*]	IPv6 ルーティング テーブルの内容を表示して、設定を確認します。 • **interface** *interface-id*：（任意）指定されたインターフェイスを出力インターフェイスとして使用するスタティック ルートだけを表示します。 • **recursive**：（任意）再帰的なスタティック ルートだけを表示します。**recursive** キーワードは、**interface** キーワードと同時に指定することはできませんが、IPv6 プレフィクスとは同時に指定することもできます。 • **detail**：（任意）次の追加情報を表示します。 – 有効な再帰ルートの場合、出力パス セット、および解決の最大深さ。 – 無効なルートの場合、そのルートが無効である理由。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

設定されているスタティック ルートを削除するには、**no ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] グローバル コンフィギュレーション コマンドを使用します。

次に、管理ディスタンスが 130 であるフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130
```

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」を参照してください。

IPv6 用の RIP の設定

IPv6 RIP を実行するようにスイッチを設定するには、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 RIP をイネーブルにするすべてのレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 RIP を設定するには、特権 EXEC モードで次の必須および任意の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router rip** *name*	IPv6 RIP ルーティング プロセスを設定し、プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 3	**maximum-paths** *number-paths*	（任意）IPv6 RIP がサポートできる等価コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 64 です。デフォルト値は 4 ルートです。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6	**ipv6 rip** *name* **enable**	インターフェイスで指定した IPv6 RIP ルーティング プロセスをイネーブルにします。

	コマンド	目的
ステップ 7	**ipv6 rip** *name* **default-information** {**only** | **originate**}	（任意）IPv6 デフォルト ルート（::/0）を RIP ルーティング プロセス アップデートに格納し、指定したインターフェイスから送信します。 **（注）** IPv6 デフォルト ルート（::/0）を任意のインターフェイスから送信したあとにルーティング ループが発生しないようにするために、ルーティング プロセスはインターフェイスで受信するデフォルト ルートをすべて無視します。 • **only**：デフォルト ルートを送信し、現在のインターフェイスで送信されるアップデート内のその他のすべてのルートを抑制するように選択します。 • **originate**：デフォルト ルートに加えて、現在のインターフェイスで送信されるアップデート内のその他のすべてのルートを送信するように選択します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ipv6 rip** [*name*] [**interface** *interface-id*] [**database**] [**next-hops**] または **show ipv6 route rip** [*updated*]	IPv6 RIP プロセスに関する情報を表示します。 IPv6 ルーティング テーブルの内容を表示します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

RIP ルーティング プロセスをディセーブルにするには、**no ipv6 router rip** *name* グローバル コンフィギュレーション コマンドを使用します。インターフェイスの RIP ルーティング プロセスをディセーブルにするには、**no ipv6 rip** *name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、最大 8 つの等価コスト ルートで RIP ルーティング プロセス *cisco* をイネーブルにし、インターフェイスでそれをイネーブルにする例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface fastethernet2/0/11
Switch(config-if)# ipv6 rip cisco enable
```

IPv6 用の RIP ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」を参照してください。

IPv6 用の OSPF の設定

IPv6 用の OSPF は、各ネットワーク用にカスタマイズできます。ただし、IPv6 での OSPF に対するデフォルトは、ほとんどのユーザと機能の要件を満たすように設定されています。

次の注意事項に従ってください。

- スイッチは、IP サービス イメージを実行している必要があります。
- IPv6 コマンドのデフォルトを変更する場合は注意が必要です。デフォルトを変更すると、IPv6 ネットワーク用の OSPF に悪影響を及ぼす可能性があります。

- インターフェイスで IPv6 OSPF をイネーブルにするには、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 OSPF をイネーブルにするレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 OSPF を設定するには、特権 EXEC モードで次の必須および任意の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router ospf** *process-id*	プロセスの OSPF ルータ コンフィギュレーション モードをイネーブルにします。プロセス ID は、IPv6 ルーティング プロセスの OSPF をイネーブルにするときに管理用に割り当てた番号です。プロセス ID はローカルに割り当てられており、1 ～ 65535 の範囲の正の整数です。
ステップ 3	**area** *area-id* **range** {*ipv6-prefix/prefix length*} [**advertise** | **not-advertise**] [**cost** *cost*]	（任意）エリアの境界でルートを統合および集約します。 • *area-id* : ルートを集約するエリアの ID。10 進値または IPv6 プレフィクスとして指定できます。 • *ipv6-prefix/prefix length* : 宛先 IPv6 ネットワーク、およびアドレスの上位何ビットがプレフィクス（アドレスのネットワーク部）であるかを示す 10 進値です。スラッシュ記号（/）を 10 進値の前に付ける必要があります。 • **advertise** :（任意）Type 3 サマリー Link-State Advertisement（LSA; サマリー リンクステート アドバタイズ）をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。 • **not-advertise** :（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠されたままになります。 • **cost** *cost* :（任意）現在のサマリー ルートのメトリックまたはコスト。宛先までの最短のパスを判別する場合に、OSPF SPF 計算で使用されます。指定できる値の範囲は、0 ～ 16777215 です。
ステップ 4	**maximum paths** *number-paths*	（任意）IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等価コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 64 です。デフォルト値は 16 です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]	IPv6 用の OSPF をインターフェイスでイネーブルにします。 **instance** *instance-id* :（任意）インスタンス ID。
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*]	OSPF インターフェイスに関する情報を表示します。
	または	
	show ipv6 ospf [*process-id*] [*area-id*]	OSPF ルーティング プロセスに関する一般情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

OSPF ルーティング プロセスをディセーブルにするには、**ipv6 router ospf** *process-id* グローバル コンフィギュレーション コマンドを使用します。インターフェイスの OSPF ルーティング プロセスをディセーブルにするには、**no ipv6 ospf** *process-id* **area** *area-id* インターフェイス コンフィギュレーション コマンドを使用します。

IPv6 用の OSPF ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」を参照してください。

IPv6 用の EIGRP の設定

デフォルトでは、IPv6 用の EIGRP はディセーブルになっています。インターフェイスで IPv6 用の EIGRP を設定できます。EIGRP 用にルータとインターフェイスを設定してから、**no shutdown** 特権 EXEC コマンドを入力して EIGRP を開始します。

（注）　IPv6 用の EIGRP がシャットダウン モードではない場合、EIGRP の router-mode コマンドを入力してルータとインターフェイスを設定する前に、EIRGP が実行を開始する場合があります。

スイッチは、IP サービス イメージを実行している必要があります。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定されているルータ ID を確認してから、**router-id** コマンドを使用します。

EIGRP IPv4 と同様に、EIGRPv6 を使用して EIGRP IPv4 インターフェイスを指定し、そのサブセットを受動インターフェイスとして選択できます。すべてのインターフェイスをパッシブにするには、**passive-interface default** コマンドを使用します。すべてのインターフェイスをアクティブにするには、選択したインターフェイスで **no passive-interface** コマンドを使用します。受動インターフェイスでは EIGRP IPv6 を設定する必要はありません。

詳細な設定手順については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 用の HSRP の設定

Hot Standby Router Protocol（HSRP）は、単一のルータのアベイラビリティに依存しない冗長なルーティングを IPv6 のトラフィックに提供します。

IPv6 用の HSRP をスイッチでイネーブルにすると、IPv6 ホストは IPv6 のネイバー探索ルータ アドバタイズメント メッセージを通して使用可能な IPv6 ルータを学習します。HSRP IPv6 グループは、HSRP グループ番号から取得される仮想 MAC アドレスを持っています。また、デフォルトで、HSRP の仮想 MAC アドレスから取得される仮想 IPv6 リンクローカル アドレスを持っています。HSRP グループがアクティブになると、HSRP の仮想 IPv6 リンクローカル アドレスに定期的にメッセージが送信されます。

スイッチは、IP サービス イメージを実行している必要があります。

IPv6 用の HSRP を設定する場合は、HSRP バージョン 2（HSRPv2）をインターフェイスでイネーブルにする必要があります。

HSRPv1 および HSRPv2 で IPv6 用の HSRP を設定する場合の注意事項については、「HSRP 設定時の注意事項」（P.45-5）および 「HSRP のトラブルシューティング」（P.45-12）を参照してください。

IPv6 用の HSRP および HSRPv2 の詳細については、第 45 章「HSRP の設定」を参照してください。

（注）　IPv6 グループ用の HSRP を設定するには、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 グループ用の HSRP を設定するインターフェイスで IPv6 をイネーブルにする必要があります。

HSRP バージョン 2 のイネーブル化

レイヤ 3 インターフェイスで HSRP バージョン 2 をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、スタンバイ バージョンを指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby version** {**1** | **2**}	**2** を入力して HSRP のバージョンを変更します。デフォルトは 1 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show standby**	設定を確認します。
ステップ 6	**copy running-config startup-config**	(任意)設定をコンフィギュレーション ファイルに保存します。

IPv6 用の HSRP グループのイネーブル化

レイヤ 3 インターフェイスで IPv6 用の HSRP を作成またはイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、IPv6 用の HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。

	コマンド	目的
ステップ 3	**standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**}	IPv6 グループ用の HSRP を作成（またはイネーブルに）します。 • （任意）*group-number* : HSRP をイネーブルにするインターフェイスのグループ番号です。指定できる範囲は 0 ～ 4095 です。デフォルト値は 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • ホットスタンバイ ルータ インターフェイスのリンクローカル アドレスを入力するか、リンクローカル プレフィクスと変更された EUI-64 形式のインターフェイス ID からのリンクローカル アドレスの自動生成をイネーブルにします。EUI-64 形式のインターフェイス ID は、関連する HSRP 仮想 MAC アドレスから作成されます。
ステップ 4	**standby** [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]	ルータを **preempt** に設定します。これは、ローカル ルータのプライオリティがアクティブ ルータより高い場合は、そのローカル ルータがアクティブ ルータとして制御を行うことを意味します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 • （任意）**delay**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）です。デフォルト値は 0 です（引き継ぎ前の遅延なし）。 • （任意）**reload**：リロード後のプリエンプション遅延を設定します（秒単位）。遅延は、ルータがリロードしたあとの最初の interface-up イベントに対してだけ適用されます。 • （任意）**sync**：IP 冗長クライアントに対する最大同期期間を設定します（秒単位）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** [*group-number*] **priority** *priority*	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルトのプライオリティは 100 です。値が大きいほど、高いプライオリティを表します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show standby** [*interface-id* [*group-number*]]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IPv6 用の HSRP をディセーブルにするには、**no standby** [*group-number*] **ipv6** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートのグループ 1 で IPv6 用の HSRP をアクティブにする例を示します。ホットスタンバイ グループが使用する IP アドレスは、IPv6 用の HSRP を使用して学習されます。

（注） この手順は、IPv6 用の HSRP をイネーブルにするために必要な最低限の数のステップです。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

IPv6 用の HSRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Configuring First Hop Redundancy Protocols in IPv6」を参照してください。

IPv6 の表示

次の各コマンドの構文と使用方法の詳細については、Cisco IOS のコマンド リファレンスを参照してください。

表 42-2 に、スイッチで IPv6 をモニタするための特権 EXEC コマンドを示します。

表 42-2　IPv6 をモニタするためのコマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 cef	IPv6 用の Cisco Express Forwarding を表示します。
show ipv6 interface *interface-id*	IPv6 インターフェイスのステータスと設定を表示します。
show ipv6 mtu	宛先キャッシュごとの IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュのエントリを表示します。
show ipv6 ospf	IPv6 OSPF の情報を表示します。
show ipv6 prefix-list	IPv6 プレフィクス リストを表示します。
show ipv6 protocols	スイッチでの IPv6 ルーティング プロトコルを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコルのステータスを表示します。
show ipv6 route	IPv6 ルート テーブルのエントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 42-3 に、EIGRP IPv6 の情報を表示するための特権 EXEC コマンドを示します。

表 42-3　EIGRP IPv6 の情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [*as-number*] *interface*	EIGRP IPv6 用に設定されているインターフェイスに関する情報を表示します。
show ipv6 eigrp [*as-number*] *neighbor*	EIGRP IPv6 によって検出されたネイバーを表示します。
show ipv6 eigrp [*as-number*] *traffic*	送受信された EIGRP IPv6 パケットの数を表示します。
show ipv6 eigrp topology [*as-number* | *ipv6-address*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]	IPv6 トポロジ テーブルの EIGRP エントリを表示します。

表 42-4 に、IPv4 および IPv6 のアドレス タイプに関する情報を表示するための特権 EXEC コマンドを示します。

表 42-4　IPv4 および IPv6 のアドレス タイプを表示するためのコマンド

コマンド	目的
show ip http server history	最近の HTTP サーバへの接続を 20 個表示します。アクセスされた IP アドレスと、接続終了時刻も表示されます。
show ip http server connection	HTTP サーバへの現在の接続を表示します。アクセスされているローカルおよびリモートの IP アドレスも表示されます。
show ip http client connection	HTTP サーバに対する HTTP クライアント接続の設定値を表示します。
show ip http client history	HTTP クライアントがサーバに対して行った要求のリスト（最近の 20 個）を表示します。

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

次に、**show ipv6 cef** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 cef
::/0
  nexthop 3FFE:C000:0:7::777 Vlan7
3FFE:C000:0:1::/64
  attached to Vlan1
3FFE:C000:0:1:20B:46FF:FE2F:D940/128
  receive
3FFE:C000:0:7::/64
  attached to Vlan7
3FFE:C000:0:7::777/128
  attached to Vlan7
3FFE:C000:0:7:20B:46FF:FE2F:D97F/128
  receive
3FFE:C000:111:1::/64
  attached to FastEthernet1/0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to FastEthernet2/0/43
3FFE:C000:168:1:20B:46FF:FE2F:D94B/128
  receive
3FFE:C000:16A:1::/64
```

```
  attached to Loopback10

3FFE:C000:16A:1:20B:46FF:FE2F:D900/128
  receive

<テキスト出力は省略>
```

次に、**show ipv6 protocols** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
  Interfaces:
    Vlan6
    FastEthernet0/4
    FastEthernet0/11
    FastEthernet0/12
   FastEthernet1/4
    FastEthernet1/6
    FastEthernet1/7
Redistribution:
    None
```

次に、**show ipv6 rip** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 rip
RIP process "fer", port 521, multicast-group FF02::9, pid 190
     Administrative distance is 120.Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 9040, trigger updates 60
  Interfaces:
    Vlan6
    FastEthernet2/0/4
    FastEthernet2/0/11
    FastEthernet1/0/12
Redistribution:
    None
```

次に、**show ipv6 static** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via nexthop 3FFE:C000:0:7::777, distance 1
```

次に、**show ipv6 neighbor** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
3FFE:C000:0:7::777                          - 0007.0007.0007  REACH Vl7
3FFE:C101:113:1::33                         - 0000.0000.0033  REACH Fa1/0/13
```

次に、**show ipv6 route** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 route
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
L   FF00::/8 [0/0]
     via Null0, receive
```

次に、**show ipv6 traffic** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  36861 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
         0 RPF drops, 0 RPF suppressed drops
  Mcast: 1 received, 36861 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 9944 router advert, 0 redirects
        84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

CHAPTER 43

IPv6 MLD スヌーピングの設定

Multicast Listener Discovery（MLD）スヌーピングを使用すると、IE 3000 スイッチ上で、スイッチドネットワーク内のクライアントやルータに IP Version 6（IPv6）マルチキャスト データを効率的に配信することができます。

（注） IPv6 を使用するには、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定する必要があります。このテンプレートを選択するには、**sdm prefer dual-ipv4-and-ipv6 default** グローバル コンフィギュレーション コマンドを入力します。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」を参照してください。
- スイッチの IPv6 の詳細については、第 42 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

この章の内容は次のとおりです。

MLD スヌーピングの概要

IP version 4（IPv4）では、レイヤ 2 スイッチにおいて、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングを使用して、レイヤ 2 インターフェイスをダイナミックに設定することによりマルチキャスト トラフィックのフラッディングを抑制できます。これにより、マルチキャスト トラフィックは IP マルチキャスト装置に関連付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングでは、IPv6 マルチキャスト データは、VLAN のすべてのポートにフラッディングされるのではなく、データの受信を要求するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることによって作成されます。

MLD は、IPv6 マルチキャスト ルータで使用されるプロトコルで、直接接続されたリンク上のマルチキャスト リスナー（IPv6 マルチキャスト パケットの受信を要求しているノード）の存在、およびネイバー ノードを対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生したものです。MLD バージョン 1（MLDv1）は IGMPv2 に相当し、MLD バージョン 2（MLDv2）は IGMPv3 に相当します。MLD は Internet Control Message Protocol version 6（ICMPv6; インターネット制御メッセージ プロトコル バージョン 6）のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

このスイッチでは、次の 2 つのバージョンの MLD スヌーピングがサポートされます。

- MLDv1 スヌーピングは、MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 基本スヌーピング（MBSS）は、MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。

（注）　IPv6 の送信元および宛先マルチキャスト アドレスに基づく転送を設定する MLDv2 拡張スヌーピング（MESS）はサポートされません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルにすることができます。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト MAC アドレス テーブルはソフトウェアで作成され、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアとハードウェアで作成されます。その後、ハードウェアで IPv6 マルチキャスト アドレスに基づくブリッジングが実行されます。

ここでは、IPv6 MLD スヌーピングの一部のパラメータについて説明します。

- 「MLD メッセージ」（P.43-2）
- 「MLD クエリー」（P.43-3）
- 「マルチキャスト クライアント エージングのロバストネス」（P.43-3）
- 「マルチキャスト ルータ検出」（P.43-3）
- 「MLD レポート」（P.43-4）
- 「MLD Done メッセージと即時脱退」（P.43-4）
- 「トポロジ変更通知処理」（P.43-5）

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージがサポートされます。

- リスナー クエリー：IGMPv2 クエリーに相当し、一般的クエリーまたは Multicast-Address-Specific Query（MASQ; マルチキャスト アドレス固有クエリー）のいずれかになります。
- マルチキャスト リスナー レポート：IGMPv2 レポートに相当します。
- Multicast Listener Done メッセージ：IGMPv2 Leave メッセージに相当します。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートされます。

メッセージ タイマーおよびメッセージの送受信によるステート移行は、IGMPv2 メッセージの場合と同じです。有効なリンクローカル IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

このスイッチでは、MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに応答します。また、レポート抑制、レポート プロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト MAC アドレス設定もサポートされています。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーが CPU に送信されて処理されます。受信されたクエリーから、MLD スヌーピングにより IPv6 マルチキャスト アドレス データベースが作成されます。また、マルチキャスト ルータ ポートの検出、タイマーの維持、レポート応答時間の設定、VLAN のクエリア IP 送信元アドレスの学習、VLAN 内のクエリア ポートの学習、およびマルチキャスト アドレス エージングの維持が行われます。

（注）　IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用している場合は、IE 3000 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに応答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合には、MLD Done メッセージ（IGMP Leave メッセージに相当）を送信できます。スイッチでは、MLDv1 Done メッセージを受信すると、即時脱退がイネーブルでなければ、メッセージを受信したポートに MASQ を送信して、ポートに接続する他の装置がマルチキャスト グループに残る必要があるかどうかを判別します。

マルチキャスト クライアント エージングのロバストネス

クエリー数に基づいて、アドレスからのポート メンバーシップの削除を設定できます。特定のアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーについてポート上のアドレスに対するレポートがない場合だけです。デフォルト値は 2 です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは、次の特性を持つマルチキャスト ルータ検出を実行します。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート ラーニングは、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。

- 複数のルータが同じレイヤ 2 インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。
- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合だけです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出されたあとは、不明の IPv6 マルチキャスト データは、検出されたルータ ポートにだけ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 Join メッセージは、基本的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスおよび IPv6 マルチキャスト MAC アドレスが VLAN の MLD データベースに入力されます。そのあと、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）が自動的にイネーブルになります。レポート抑制により、グループで受信された最初の MLDv1 レポートが IPv6 マルチキャスト ルータに転送されます。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制はディセーブルになり、すべての MLDv1 レポートが入力 VLAN にフラッディングされます。

このスイッチでは、MLDv1 プロキシ レポート機能もサポートしています。スイッチでは、MLDv1 MASQ を受信すると、別のポート上にグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバー ポートが異なる場合は、クエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージと即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージに相当）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は、IGMP スヌーピングと同様に、ポートにシングル ホストが接続されている VLAN でだけこの機能を使用する必要があります。ポートがグループの最後のメンバーである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数に基づいて制御できます。特定のアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーについてポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、**ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルト値は 2 です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応答時間は、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドを使用して設定します。削除されたポートがマルチキャスト アドレスの最後のメンバーである場合は、マルチキャスト アドレスも削除され、検出されたマルチキャスト ルータのすべてにアドレス脱退情報が送信されます。

トポロジ変更通知処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して Topology Change Notification（TCN; トポロジ変更通知）送信請求をイネーブルにすると、MLDv1 スヌーピングでは、設定された数の MLDv1 クエリーについてすべての IPv6 マルチキャスト トラフィックをフラッディングするように VLAN を設定してから、選択されたポートにだけマルチキャスト データの送信を開始します。この値は、**ipv6 mld snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルトでは、2 つのクエリーが送信されます。スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、有効なリンクローカル IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。この動作は IGMP スヌーピングの場合と同じです。

IPv6 MLD スヌーピングの設定

ここでは、IPv6 MLD スヌーピングの設定手順について説明します。

MLD スヌーピングのデフォルト設定

表 43-1 に、MLD スヌーピングのデフォルト設定を示します。

表 43-1　MLD スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング（グローバル）	ディセーブル。
MLD スヌーピング（VLAN 単位）	イネーブル。VLAN MLD スヌーピングを実行するには、MLD スヌーピングをグローバルにイネーブルにする必要があります。
IPv6 マルチキャスト アドレス	設定なし。

表 43-1　MLD スヌーピングのデフォルト設定 （続き）

機能	デフォルト設定
IPv6 マルチキャスト ルータ ポート	設定なし。
MLD スヌーピング即時脱退	ディセーブル。
MLD スヌーピング ロバストネス変数	グローバル：2、VLAN 単位：0。 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、グローバル カウントが使用されます。
last listener クエリー カウント	グローバル：2、VLAN 単位：0。 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、グローバル カウントが使用されます。
last listener クエリー間隔	グローバル：1000（1 秒）、VLAN：0。 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、グローバル間隔が使用されます。
TCN クエリー送信請求	ディセーブル。
TCN クエリー カウント	2.
MLD リスナー抑制	イネーブル。

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項を考慮してください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にするには、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用している場合は、IE 3000 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにすることができます。
- スイッチで許容されるマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチで許容されるアドレス エントリの最大数は、1000 です。

MLD スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングをグローバルにディセーブルにすると、すべての VLAN でもディセーブルになります。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定によってグローバル設定が上書きされます。つまり、MLD スヌーピングがイネーブルになるのは、デフォルト状態（イネーブル）の VLAN インターフェイス上だけです。

MLD スヌーピングは、VLAN 単位または VLAN の特定の範囲でイネーブルおよびディセーブルにすることができますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルにすることができます。

スイッチで MLD スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping**	スイッチで MLD スヌーピングをグローバルにイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。
ステップ 5	**reload**	オペレーティング システムをリロードします。

スイッチで MLD スヌーピングをグローバルにディセーブルにするには、**no ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用します。

VLAN で MLD スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

（注） IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用している場合は、IE 3000 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping**	スイッチで MLD スヌーピングをグローバルにイネーブルにします。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id*	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 **（注）** VLAN スヌーピングをイネーブルにするには、MLD スヌーピングをグローバルにイネーブルにする必要があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN インターフェイスで MLD スヌーピングをディセーブルにするには、指定された VLAN 番号に対して **no ipv6 mld snooping vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

スタティックなマルチキャスト グループの設定

ホストまたはレイヤ 2 ポートは、通常、マルチキャスト グループにスタティックに加入しますが、VLAN に対して IPv6 マルチキャスト アドレスおよびメンバー ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **static** *ipv6_multicast_address* **interface** *interface-id*	レイヤ 2 ポートをマルチキャスト グループのメンバーとして、マルチキャスト グループをスタティックに設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *ipv6_multicast_address* は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式にする必要があります。 • *interface-id* は、メンバー ポートです。物理インターフェイスまたはポート チャネル（1 ～ 48）を指定できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping multicast-address user** または **show ipv6 mld snooping multicast-address vlan** *vlan-id* **user**	スタティックなメンバー ポートおよび IPv6 アドレスを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

マルチキャスト グループからレイヤ 2 ポートを削除するには、**no ipv6 mld snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。グループからすべてのメンバー ポートを削除すると、そのグループは削除されます。

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet1/1
Switch(config)# end
```

マルチキャスト ルータ ポートの設定

MLD スヌーピングでは、MLD クエリーおよび PIMv6 クエリーを介してルータ ポートについて学習しますが、CLI（コマンドライン インターフェイス）を使用して VLAN にマルチキャスト ルータ ポートを追加することもできます。マルチキャスト ルータ ポートを追加する（マルチキャスト ルータにスタティックな接続を追加する）には、スイッチで **ipv6 mld snooping vlan mrouter** グローバル コンフィギュレーション コマンドを使用します。

（注）　マルチキャスト ルータへのスタティックな接続は、スイッチ ポート上でだけサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id*	マルチキャスト ルータの VLAN ID を指定します。また、マルチキャスト ルータのインターフェイスを指定します。 • 指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping mrouter** [**vlan** *vlan-id*]	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN からマルチキャスト ルータ ポートを削除するには、**no ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet1/2
Switch(config)# exit
```

MLD 即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにした場合、ポートで MLD Done メッセージが検出されると、そのポートがマルチキャスト グループからただちに削除されます。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバーが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにしないでください。

MLDv1 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **immediate-leave**	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping vlan** *vlan-id*	VLAN インターフェイスで即時脱退がイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN で MLD 即時脱退をディセーブルにするには、**no ipv6 mld snooping vlan** *vlan-id* **immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit
```

MLD スヌーピング クエリーの設定

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成し、Done メッセージが送信された IPv6 マルチキャスト アドレスに MASQ を送信します。ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

スイッチまたは VLAN に MLD スヌーピング クエリーの特性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping robustness-variable** *value*	（任意）スイッチが一般的なクエリーに応答しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ～ 3 です。デフォルトは 2 です。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value*	（任意）VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャスト アドレスが期限切れになるまでに、MLD スヌーピングが送信する一般的なクエリー数が決定されます。指定できる範囲は 1 ～ 3 です。デフォルトは 0 です。0 に設定すると、使用される数はグローバル ロバストネス変数の値になります。

	コマンド	目的
ステップ 4	**ipv6 mld snooping last-listener-query-count** *count*	（任意）MLD クライアントが期限切れになる前にスイッチが送信する MASQ 数を設定します。指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。クエリーは 1 秒おきに送信されます。
ステップ 5	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-count** *count*	（任意）VLAN 単位で last-listener クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ～ 7 です。デフォルトは 0 です。0 に設定すると、グローバル カウント値が使用されます。クエリーは 1 秒おきに送信されます。
ステップ 6	**ipv6 mld snooping last-listener-query-interval** *interval*	（任意）スイッチが MASQ を送信してから、マルチキャスト グループからポートを削除する前に待機する最大応答時間を設定します。指定できる範囲は、100 ～ 32,768 ミリ秒です。デフォルト値は 1000（1 秒）です。
ステップ 7	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-interval** *interval*	（任意）VLAN 単位で last-listener クエリー間隔を設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ～ 32,768 ミリ秒です。デフォルト値は 0 です。0 に設定すると、グローバル last-listener クエリー間隔が使用されます。
ステップ 8	**ipv6 mld snooping tcn query solicit**	（任意）トポロジ変更通知（TCN）送信請求をイネーブルにします。これにより、VLAN では、設定された数のクエリーについて IPv6 マルチキャスト トラフィックをすべてフラッディングしてから、マルチキャスト データをマルチキャスト データの受信を要求するポートに対してだけ送信します。デフォルトでは、TCN はディセーブルです。
ステップ 9	**ipv6 mld snooping tcn flood query count** *count*	（任意）TCN がイネーブルの場合に、送信される TCN クエリー数を指定します。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ipv6 mld snooping querier** [**vlan** *vlan-id*]	（任意）スイッチまたは VLAN の MLD スヌーピング クエリア情報を確認します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、MLD スヌーピングのグローバル ロバストネス変数を 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

次に、VLAN の MLD スヌーピングの last-listener クエリー カウントを 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit
```

次に、MLD スヌーピングの last-listener クエリー間隔（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
```

MLD リスナー メッセージ抑制のディセーブル化

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、マルチキャスト ルータ クエリーごとに MLD レポートが 1 つだけ転送されます。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ipv6 mld snooping listener-message-suppression**	MLD メッセージ抑制をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping**	IPv6 MLD スヌーピング レポート抑制がディセーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

MLD メッセージ抑制を再びイネーブルにするには、**ipv6 mld snooping listener-message-suppression** グローバル コンフィギュレーション コマンドを使用します。

MLD スヌーピング情報の表示

ダイナミックに学習された、またはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの MLD スヌーピング情報を表示できます。MLD スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

MLD スヌーピング情報を表示するには、表 43-2 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 43-2　MLD スヌーピング情報を表示するためのコマンド

コマンド	目的
show ipv6 mld snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定した 1 つの VLAN の MLD スヌーピング設定情報を表示します。 （任意）1 つの VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習された、または手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスはダイナミックに学習されます。 （任意）1 つの VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。

表 43-2　MLD スヌーピング情報を表示するためのコマンド（続き）

コマンド	目的
show ipv6 mld snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意）1 つの VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping multicast-address [**vlan** *vlan-id*] [**count** | **dynamic** | **user**]	スイッチまたは VLAN に関する、すべての IPv6 マルチキャスト アドレス情報または特定の IPv6 マルチキャスト アドレス情報を表示します。 • スイッチまたは VLAN のグループ カウントを表示するには、**count** を入力します。 • スイッチまたは VLAN の MLD スヌーピング学習グループ情報を表示するには、**dynamic** を入力します。 • スイッチまたは VLAN の MLD スヌーピング ユーザ設定グループ情報を表示するには、**user** を入力します。
show ipv6 mld snooping multicast-address vlan *vlan-id* [*ipv6-multicast-address*]	指定した VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。

CHAPTER 44

IPv6 ACL の設定

この章では、IE3000 スイッチに IPv6 ACL を設定する方法について説明します。IP バージョン 4（IPv4）の名前付き Access Control List（ACL; アクセス制御リスト）を作成して適用する方法と同様に、IPv6 ACL を作成してインターフェイスに適用することにより、IP バージョン 6（IPv6）トラフィックをフィルタリングできます。入力ルータの ACL を作成して適用することにより、レイヤ 3 管理トラフィックのフィルタリングもできます。

（注） IPv6 を使用するには、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定する必要があります。テンプレートを選択するには、**sdm prefer** {**default** | **dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力します。IPv6 の ACL をサポートするのは、IP サービス イメージが稼動しているスイッチだけです。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」を参照してください。
- スイッチの ACL の詳細については、第 44 章「IPv6 ACL の設定」を参照してください。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

この章の内容は次のとおりです。

IPv6 ACL の概要

スイッチ イメージは、2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL
  - レイヤ 3 インターフェイス（ルーテッド ポート、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、またはレイヤ 3 EtherChannel）のアウトバウンド トラフィックまたはインバウンド トラフィックでサポートされます。
  - ルーティングされる IPv6 パケットだけに適用されます。

- IPv6 ポート ACL
  - レイヤ 2 インターフェイスのインバウンド トラフィックでだけサポートされます。
  - インターフェイスに着信するすべての IPv6 パケットに適用されます。

（注）　サポートされない IPv6 ACL を設定するとエラー メッセージが表示され、設定は有効になりません。

スイッチは、IPv6 トラフィックの VLAN ACL（VLAN マップ）をサポートしません。

（注）　スイッチでの ACL サポートについては、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。

1 つのインターフェイスに IPv4 と IPv6 両方の ACL を適用できます。

IPv4 ACL と同様に、IPv6 のポート ACL も、ルータ ACL より優先されます。

- 入力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信されたパケットには、ポートの ACL のフィルタが適用されます。他のポートで受信したルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- 出力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信されたパケットには、ポート ACL のフィルタが適用されます。発信するルーティング IPv6 パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。

（注）　*いずれか*のポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

ここでは、スイッチの IPv6 ACL の特性について説明します。

- 「サポートされる ACL 機能」（P.44-2）
- 「IPv6 ACL の制限事項」（P.44-3）

サポートされる ACL 機能

スイッチの IPv6 ACL には、次の特性があります。

- フラグメント化されたフレーム（IPv4 では **fragments** キーワード）がサポートされます。
- IPv4 と同じ統計情報が IPv6 ACL でもサポートされます。
- スイッチの TCAM 領域が足りなくなると、ACL ラベルに関連付けられているパケットが CPU に転送され、ACL がソフトウェアで適用されます。
- ホップバイホップ オプション付きのルーテッド パケットおよびブリッジド パケットでは、IPv6 ACL がソフトウェアに適用されます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。

IPv6 ACL の制限事項

IPv4 では、番号付きの標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 では、名前付き ACL だけサポートされます。

スイッチでは、一部の例外を除いて、Cisco IOS でサポートされる IPv6 ACL の大部分がサポートされます。

- IPv6 送信元アドレスと宛先アドレス：ACL 照合は、Universal Identifier（EUI）-64 形式の /0 ～ /64 のプレフィクスと、ホスト アドレス（/128）でだけサポートされます。スイッチは、サポートする情報の損失のないホスト アドレスは次のものだけです。
  - 集約可能なグローバル ユニキャスト アドレス
  - リンクローカル アドレス
- スイッチは **flowlabel**、**routing header**、および **undetermined-transport** キーワードの照合をサポートしません。
- スイッチは再帰 ACL（**reflect** キーワード）をサポートしません。
- このリリースでは、IPv6 のポート ACL およびルータ ACL だけがサポートされます。VLAN ACL（VLAN マップ）はサポートされません。
- スイッチは、IPv6 フレームに MAC ベース ACL を適用しません。
- IPv6 のポート ACL は、レイヤ 2 EtherChannel に適用できません。
- スイッチは、出力ポートの ACL をサポートしません。
- IPv6 の出力ルータの ACL および入力ポートの ACL は、スイッチでだけサポートされます。スイッチは、コントロール プレーン（着信）の IPv6 ACL だけをサポートします。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限はありません。ハードウェア転送を必要とするインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、スイッチはそのインターフェイスで ACL がサポートされるかどうかを判別します。サポートされない場合、ACL の付加が拒否されます。
- ACL をインターフェイスに適用して、サポートされないキーワードを含む Access Control Entry（ACE; アクセス制御エントリ）を追加しようとすると、スイッチは現在そのインターフェイスに適用されている ACL にその ACE を追加することを許可しません。

IPv6 ACL の設定

IPv6 の ACL を設定する前に、デュアル IPv4/IPv6 SDM テンプレートのいずれかを選択する必要があります。

IPv6 トラフィックをフィルタリングする手順は、次のとおりです。

ステップ 1　IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

ステップ 2　IPv6 ACL でトラフィックをブロックする（拒否）か通過させる（許可）かを設定します。

ステップ 3　インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

ここでは、IPv6 ACL を設定して適用する手順について説明します。

- 「IPv6 ACL のデフォルト設定」（P.44-4）

IPv6 ACL のデフォルト設定

IPv6 ACL は設定または適用されていません。

他の機能との相互作用

IPv6 ACL の設定には、他の機能またはスイッチ特性と次の相互作用があります。

- IPv6 ルータの ACL がパケットを拒否するように設定されている場合、パケットは廃棄されます。パケットのコピーが Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ポート ACL によりブリッジド フレームが廃棄されると、そのフレームはブリッジされません。
- IPv4 と IPv6 の両方の ACL を 1 つのスイッチに作成して、両方の ACL を同じインターフェイスに適用できます。それぞれの ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するときに間違ったコマンドを使用すると（たとえば、IPv4 のコマンドを使って IPv6 ACL を付加しようとすると）、エラー メッセージが表示されます。
- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は、非 IP フレームだけをフィルタリングできます。
- TCAM が満杯の場合に設定済み ACL を追加すると、パケットが CPU に転送されて、ACL はソフトウェアで適用されます。

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 access-list *access-list-name*	IPv6 アクセス リスト名を定義し、IPv6 アクセスリスト コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3a	**deny** | **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/ *prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]	**deny** または **permit** を入力して、条件が一致した場合にパケットを拒否するのか許可するのかを指定します。次に、条件について説明します。 • *protocol* には、インターネット プロトコルの名前（**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、または **udp**）、または番号（IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数）を入力します。ICMP、Transmission Control Protocol（TCP; 伝送制御プロトコル）、および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）の具体的なパラメータについては、ステップ 3b ～ 3d を参照してください。 • *source-ipv6-prefix*/*prefix-length* または *destination-ipv6-prefix*/ *prefix-length* は、拒否または許可の条件を設定する送信元または宛先 IPv6 ネットワーク（またはネットワーク クラス）で、コロンで区切られた 16 ビット値を使用した 16 進数形式で指定されます（RFC 2373 を参照してください）。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンクローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および EUI ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。 • IPv6 プレフィクス ::/0 の省略形として **any** を入力します。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、拒否または許可の条件を設定する発信元または宛先の IPv6 ホスト アドレスを、コロンで区切られた 16 ビット値を使用した 16 進数形式で入力します。 • （任意）*operator* には、指定のプロトコルの送信元または宛先ポートを比較するオペランドを指定します。オペランドは、**lt**（less than : 未満）、**gt**（greater than : より大きい）、**eq**（equal : 一致）、**neq**（not equal : 不一致）、**range** です。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が続く場合、送信元ポートと一致する必要があります。*destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が続く場合、宛先ポートと一致する必要があります。 • （任意）*port-number* 値は 0 ～ 65535 の範囲の 10 進数値か、TCP または UDP をフィルタリングするための TCP ポート名または UDP ポート名です。 • （任意）**dscp** *value* を入力して、各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント（DSCP）値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）**fragments** を入力して、非初期フラグメントを確認します。このキーワードは、プロトコルが **ipv6** の場合に限り表示されます。 • （任意）**log** を入力すると、エントリと一致するパケットを示すロギング メッセージがコンソールに送信されます。**log-input** を入力して、ログ エントリに入力インターフェイスを含めます。ロギングは、ルータ ACL に対してだけサポートされます。 • （任意）**sequence** *value* を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • （任意）**time-range** *name* を入力して、ステートメントの時間範囲を指定します。

	コマンド	目的
ステップ 3b	**deny** | **permit tcp** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示す任意のパラメータが追加されています。 • **ack**：確認応答ビット設定。 • **established**：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • **fin**：終了ビット設定。送信元からのデータはこれ以上ありません。 • **neq** {*port* | *protocol*}：指定のポート番号上にないパケットだけを照合します。 • **psh**：プッシュ機能ビット設定。 • **range** {*port* | *protocol*}：ポート番号範囲のパケットだけを照合します。 • **rst**：リセット ビット設定。 • **syn**：同期ビット設定。 • **urg**：緊急ポインタ ビット設定。
ステップ 3c	**deny** | **permit udp** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**sequence** *value*] [**time-range** *name*]	（任意）UDP アクセス リストおよびアクセス条件を定義します。 UDP の場合は、**udp** を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じですが、[*operator* [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP の場合、**established** パラメータは無効です。
ステップ 3d	**deny** | **permit icmp** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dscp** *value*] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 ICMP の場合は、**icmp** を入力します。ICMP パラメータはステップ 3a の IP プロトコルに関して説明されているパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。任意のキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプを基準にしてフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-code*：ICMP メッセージ コード タイプを基準にしてフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-message*：ICMP メッセージ タイプ名、または ICMP メッセージのタイプおよびコード名を基準にして、ICMP パケットをフィルタリングします。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	show ipv6 access-list	アクセス リスト コンフィギュレーションを確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定のアクセス リストから拒否または許可条件を削除するには、キーワードを指定して **no deny** | **permit** IPv6 アクセスリスト コンフィギュレーション コマンドを使用します。

次の例では、CISCO という IPv6 アクセス リストを設定します。リストの最初の拒否エントリは、5000 より大きい宛先 TCP ポート番号を持ったパケットをすべて拒否します。2 番めの拒否エントリは、5000 未満の送信元 UDP ポート番号を持ったパケットをすべて拒否します。また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。リストの最初の許可エントリは、すべての ICMP パケットを許可します。リストの 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 アクセス リストの末尾にあるので、この 2 番めの許可エントリが必要となります。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

インターフェイスへの IPv6 ACL の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する方法を説明します。ACL は、レイヤ 3 インターフェイスのアウトバウンドまたはインバウンド トラフィックに、あるいはレイヤ 2 インターフェイスのインバウンド トラフィックに適用できます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 インターフェイス（ルータ ACL 用）を指定し、インターフェイス コンフィギュレーション モードを開始します。 **（注）** IP ベース イメージが稼動しているスイッチは、ポート ACL をサポートしません。
ステップ 3	**no switchport**	ルータ ACL を適用する場合は、インターフェイスをレイヤ 2 モード（デフォルト）からレイヤ 3 モードに変更します。
ステップ 4	**ipv6 address** *ipv6-address*	レイヤ 3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。 このコマンドは、レイヤ 2 インターフェイスでは、またはインターフェイスに明示的な IPV6 アドレスが設定されている場合には、必要ありません。
ステップ 5	**ipv6 traffic-filter** *access-list-name* {**in** | **out**}	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。 **out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	show **running-config**	アクセス リスト コンフィギュレーションを確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスからアクセス リストを削除するには、**no ipv6 traffic-filter** *access-list-name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、レイヤ 3 インターフェイスのアウトバウンド トラフィックにアクセスリスト *Cisco* を適用する例を示します。

```
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

IPv6 ACL の表示

表 44-1 に示す 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

表 44-1　IPv6 アクセス リスト情報を表示するためのコマンド

コマンド	目的
show access-lists	スイッチに設定されたすべてのアクセス リストを表示します。
show ipv6 access-list [*access-list-name*]	設定済みのすべての IPv6 アクセス リスト、または名前で指定されたアクセス リストを表示します。

次の例では、**show access-lists** 特権 EXEC コマンドの出力を示します。出力では、スイッチに設定されたすべてのアクセス リストが表示されます。

```
Switch #show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

次の例では、**show ipv6 access-lists** 特権 EXEC コマンドの出力を示します。出力には、スイッチに設定された IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30

IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```

CHAPTER 45

HSRP の設定

この章では、IE 3000 スイッチで Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用する方法について説明します。HSRP は、IP トラフィック ルーティングに冗長性を提供し、特定のルータのアベイラビリティに依存しないルーティングを実現します。IPv4 用 HSRP は、IP サービス イメージが稼動しているスイッチでサポートされます。IPv6 用 HSRP を使用する場合は、第 42 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

また、HSRP のいずれかのバージョンをレイヤ 2 モードで使用することにより、クラスタ コマンド スイッチが故障した場合にクラスタ管理を引き継ぐ冗長コマンド スイッチを設定できます。クラスタリングの詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com にある『*Getting Started with Cisco Network Assistant*』を参照してください。

この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- このリリースに対応するスイッチ コマンド リファレンス
- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』 http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html
- *Hot Standby Router Protocol Version 2* フィーチャ モジュール http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gthsrpv2.html

この章で説明する内容は、次のとおりです。

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファーストホップ冗長性を提供することにより、ネットワークのアベイラビリティを高めるためのシスコの標準方式です。HSRP を使用すると、特定のルータのアベイラビリティに依存せずに IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせて、1 つの仮想ルータ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させることができます。ネットワークまたはセグメント上に HSRP を設定すると、設定済みのルータのグループで共有される仮想 MAC（メディア アクセス制御）アドレスおよび IP アドレス提供されます。HSRP が設定された複数のルータで仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは、実際に存在するルータではなく、相互にバックアップするように設定された複数のルータの共通のターゲットを表します。1 台のルータがアクティブなルータとして、別の 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御します。

（注）　HSRP グループのルータには、IE 3000 のルーテッド ポートや Switch Virtual Intertface（SVI; スイッチ仮想インターフェイス）など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRP は、ネットワーク上のホストからの IP トラフィックに冗長性を提供することで、ネットワークのアベイラビリティを高めます。ルータ インターフェイス グループ内のアクティブ ルータは、パケットのルーティングを実行するために選択されたルータで、スタンバイ ルータは、アクティブ ルータが故障した場合、または事前設定された条件が満たされた場合にルーティング作業を引き継ぐルータです。

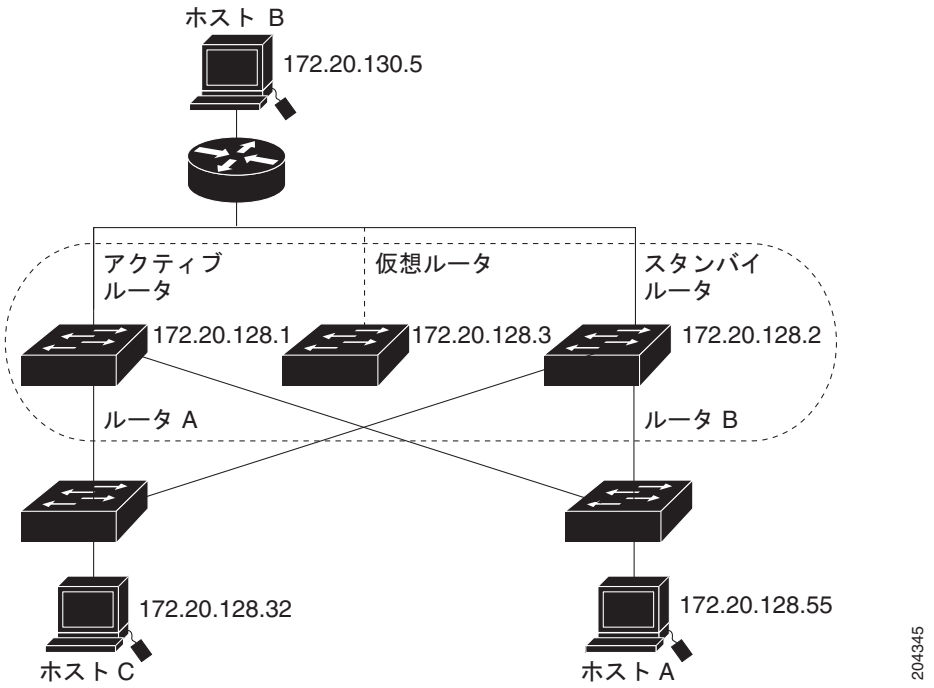
HSRP は、ホストがルータ検出プロトコルをサポートしておらず、選択されたルータのリロード時や電源切断時に新しいルータに切り替えることができない場合に有効です。ネットワーク セグメント上に HSRP を設定すると、HSRP が稼動しているルータ インターフェイス グループ内のルータ インターフェイス間で共有される仮想 MAC アドレスおよび IP アドレスが提供されます。プロトコルによってアクティブ ルータとして選択されたルータは、グループの MAC アドレス宛てのパケットを受信してルーティングします。*n* 台のルータで HSRP が稼動している場合、*n* +*1* 個の IP アドレスおよび MAC アドレスが割り当てられます。

指定されたアクティブ ルータの故障が HSRP によって検出されると、選択されたスタンバイ ルータがホット スタンバイ グループの MAC アドレスおよび IP アドレスの制御を引き継ぎます。このときには新しいスタンバイ ルータも選択されます。HSRP が稼動している装置は、マルチキャスト UDP ベースの hello パケットを送受信することで、ルータの故障の検出とアクティブ ルータおよびスタンバイ ルータの指定を行います。インターフェイスに HSRP が設定されている場合、そのインターフェイスでは Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）のリダイレクト メッセージが自動的にイネーブルになります。

レイヤ 3 で動作する IE 3000 スイッチ間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。これを行うには、インターフェイスに設定するホット スタンバイ コマンド グループごとにグループ番号を指定します。たとえば、スイッチ 1 のインターフェイスをアクティブ ルータに、スイッチ 2 のインターフェイスをスタンバイ ルータに設定し、スイッチ 2 の別のインターフェイスをアクティブ ルータに、スイッチ 1 の別のインターフェイスをそのスタンバイ ルータに設定することができます。

図 45-1 に、HSRP 用に設定されたネットワークのセグメントを示します。各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。ネットワーク上のホストにルータ A の IP アドレスを設定する代わりに、仮想ルータの IP アドレスをホストのデフォルト ルータとして設定します。ホスト C は、ホスト B にパケットを送信するときに、仮想ルータの MAC アドレスにパケットを送信します。何らかの理由でルータ A がパケットの転送を停止した場合は、ルータ B が仮想 IP アドレスおよび仮想 MAC アドレスに応答してアクティブ ルータになり、アクティブ ルータの役割を引き継ぎます。ホスト C は、引き続き仮想ルータの IP アドレスを使用してホスト B 宛てのパケットを処理します。このパケットは、今度はルータ B によって受信され、ホスト B に送信されます。ルータ B は、ルータ A が動作を再開するまで、ホスト B のセグメント上のユーザと通信する必要があるホスト C のセグメント上のユーザに継続的にサービスを提供し、ホスト A セグメントとホスト B の間で通常のパケット処理機能の実行を続行します。

図 45-1　HSRP の一般的な構成



HSRP バージョン

スイッチでは、次の Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）のバージョンがサポートされます。

- HSRPv1：HSRP のバージョン 1 で、HSRP のデフォルト バージョンです。このバージョンの特徴は次のとおりです。
  - 使用できる HSRP グループ番号は 0 ～ 255 までです。
  - HSRPv1 は、マルチキャスト アドレス 224.0.0.2 を使用して hello パケットを送信します。これは、Cisco Group Management Protocol（CGMP）の脱退処理と競合する場合があります。HSRPv1 と CGMP は相互に排他的であるため、同時にイネーブルにはできません。
- HSRPv2：HSRP のバージョン 2 です。このバージョンの特徴は次のとおりです。
  - HSRPv2 では、HSRP グループ番号とサブインターフェイスの VLAN ID を一致させるために、0 ～ 4095 のグループ番号と 0000.0C9F.F000 ～ 0000.0C9F.FFFF の MAC アドレスを使用できます。
  - HSRPv2 は、マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。HSRPv2 と CGMP の脱退処理は相互に排他的でないため、同時にイネーブルにすることができます。
  - HSRPv2 のパケット形式は HSRPv1 とは異なります。

    HSRPv1 を実行しているスイッチは、ルータの送信元 MAC アドレスが仮想 MAC アドレスであるため、hello パケットを送信した物理的なルータを特定できません

    HSRPv2 のパケット形式は HSRPv1 とは異なります。HSRPv2 パケットは Type Length Value（TLV）形式で、パケットを送信した物理ルータの MAC アドレスを格納する 6 バイトの識別子フィールドがあります。

    HSRPv1 を実行しているインターフェイスが HSRPv2 パケットを取得した場合、このタイプ フィールドは無視されます。

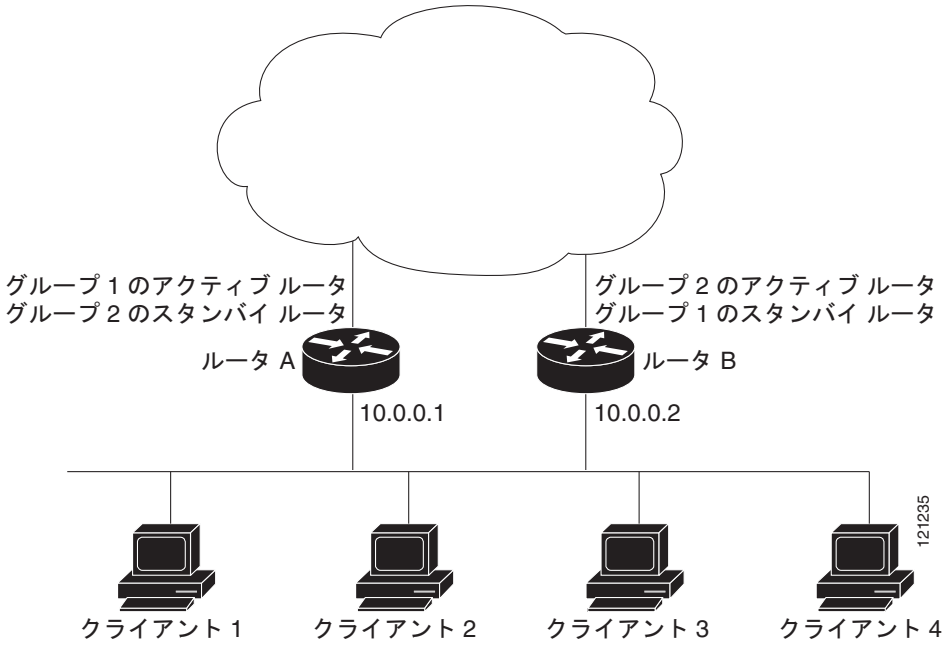
Multiple HSRP

スイッチでは、Multiple HSRP（MHSRP）がサポートされます。MHSRP は HSRP の拡張版で、複数の HSRP グループ間でのロード シェアリングが可能です。ホスト ネットワークからサーバ ネットワークにわたってロード バランシングを実現し、複数のスタンバイ グループ（およびパス）を使用するように MHSRP を設定できます。図 45-2 では、半分のクライアントがルータ A 用に、もう半分がルータ B 用に設定されています。ルータ A およびルータ B の設定により、2 つの HSRP グループが確立されています。グループ 1 では、ルータ A に最も高いプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータに、ルータ B がスタンバイ ルータになります。グループ 2 では、ルータ B に最も高いプライオリティが割り当てられているので、ルータ B がデフォルトのアクティブ ルータに、ルータ A がスタンバイ ルータになります。通常の運用では、IP トラフィックの負荷が 2 つのルータに分散されます。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータのパケット転送機能を引き継ぎます。

設定手順の例については、「MHSRP の設定」（P.45-10）を参照してください。

（注）　MHSRP では、故障したルータが回復した場合にプリエンプションによってロード シェアリングが復元されるように、HSRP インターフェイスで **standby preempt** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

図 45-2　　MHSRP ロード シェアリング



HSRP の設定

ここでは、次の設定情報について説明します。

- 「HSRP のデフォルト設定」（P.45-5）
- 「HSRP 設定時の注意事項」（P.45-5）
- 「HSRP のイネーブル化」（P.45-6）

HSRP のデフォルト設定

表 45-1 に、HSRP のデフォルト設定を示します。

表 45-1　HSRP のデフォルト設定

機能	デフォルト設定
HSRP バージョン	バージョン 1
HSRP グループ	設定なし
スタンバイ グループ番号	0
スタンバイ MAC アドレス	システムの割り当て：0000.0c07.acXX（*XX* は HSRP グループ番号）
スタンバイ プライオリティ	100
スタンバイ遅延	0（遅延なし）
スタンバイ追跡のインターフェイス プライオリティ	10
スタンバイ hello タイム	3 秒
スタンバイ ホールドタイム	10 秒

HSRP 設定時の注意事項

HSRP を設定するときには、次の注意事項に従ってください。

- IPv4 用 HSRP と IPv6 用 HSRP は相互に排他的です。両方を同時にイネーブルにはできません。
- HSRPv2 と HSRPv1 は相互に排他的です。HSRPv2 と HSRPv1 は、同じインターフェイス上で相互運用できません。
- 最大 32 個の HSRP グループ インスタンスを設定できます。

  複数のインターフェイスに同じ HSRP グループ番号を設定した場合、スイッチは各インターフェイスを 1 つのインスタンスとしてカウントします。

  たとえば、VLAN 1 とポート 1 に HSRP グループ 0 を設定した場合、スイッチはこれを 2 つのインスタンスとしてカウントします。
- 設定手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを入力することにより、レイヤ 3 ポートとして設定された物理ポートです。
  - SVI：**interface vlan** *vlan_id* グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイスです。デフォルトではレイヤ 3 インターフェイスです。

  - レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネル グループにバインドすることによって作成されたポートチャネル論理インターフェイスです。詳細については、「レイヤ 3 EtherChannel の設定」を参照してください。

- すべてのレイヤ 3 インターフェイスに IP アドレスを割り当てる必要があります。「レイヤ 3 インターフェイスの設定」（P.14-21）を参照してください。
- FHRP のインスタンスは 1 つだけ設定します。スイッチでは、HSRPv1、HSRPv2、および IPv6 用 HSRP がサポートされます。
- HSRP グループのバージョンは、グループ番号が 255 以下の場合に限り、HSRPv2 から HSRPv1 に変更できます。
- HSRPv2 および HSRP のグループ番号を設定する場合、256 の倍数の範囲のグループ番号を使用する必要があります。有効な範囲は、0 ～ 255、256 ～ 511、512 ～ 767、3840 ～ 4095 などです。

  次に、有効なグループ番号と無効なグループ番号の例を示します。

  - 番号 2、150、および 225 のグループを設定した場合は、番号 3850 の別のグループを設定できません。3850 は 0 ～ 255 の範囲内ではないからです。
  - 番号 520、600、および 700 のグループを設定した場合は、番号 900 の別のグループを設定できません。900 は 512 ～ 767 の範囲内ではないからです。
- インターフェイスの HSRP バージョンを変更すると、各 HSRP グループがリセットされます。各 HSRP グループに新しい MAC アドレスが割り当てられるからです。

HSRP のイネーブル化

standby ip インターフェイス コンフィギュレーション コマンドを実行すると、設定されたインターフェイスで HSRP がアクティブになります。IP アドレスを指定した場合は、その IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなかった場合は、スタンバイ機能によってアドレスが学習されます。指定アドレスを持つレイヤ 3 ポートを LAN 上に 1 つ以上設定する必要があります。IP アドレスを設定した場合、その IP アドレスは、現在使用されている別の指定アドレスよりも常に優先されます。

standby ip コマンドがインターフェイス上でイネーブルになっていて、プロキシ ARP がイネーブルの場合、インターフェイスのホットスタンバイ ステートがアクティブになると、プロキシ ARP 要求に対する応答は、ホットスタンバイ グループの MAC アドレスを使用して実行されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は実行されません。

レイヤ 3 インターフェイス上で HSRP を作成またはイネーブル化するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。

	コマンド	目的
ステップ 3	**standby version** {**1** | **2**}	（任意）インターフェイスに HSRP バージョンを設定します。 • 1：HSRPv1 を選択します。 • 2：HSRPv2 を選択します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、インターフェイスはデフォルトの HSRP バージョンである HSRPv1 を実行します。
ステップ 4	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブル化）します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号です。指定できる範囲は 0 ～ 255 です。デフォルト値は 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習できます。 • （任意）**secondary**：IP アドレスはセカンダリ ホットスタンバイ ルータ インターフェイスです。どのルータもセカンダリ ルータまたはスタンバイ ルータに指定されておらず、プライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、最も大きい IP アドレスを持つルータがアクティブ ルータに、2 番めに大きい IP アドレスを持つルータがスタンバイ ルータになります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show standby** [*interface-id* [*group*]]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

HSRP をディセーブルにするには、**no standby** [*group-number*] **ip** [*ip-address*] インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイスのグループ 1 で HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。

（注）　これは、HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```

HSRP プライオリティの設定

standby priority、**standby preempt**、および **standby track** の各インターフェイス コンフィギュレーション コマンドはいずれも、アクティブ ルータとスタンバイ ルータを検索するための特性や、新しいアクティブ ルータが処理を引き継いだ場合の動作を設定するために使用されます。

HSRP プライオリティを設定するときには、次の注意事項に従ってください。

- プライオリティを割り当てると、アクティブ ルータとスタンバイ ルータを選択できるようになります。プリエンプションがイネーブルの場合は、プライオリティが最も高いルータがアクティブ ルータになります。プライオリティが等しい場合、現在アクティブなルータは変更されません。
- 最も大きい数値（1 ～ 255）は、プライオリティが最も高い（アクティブ ルータになる確率が最も高い）ことを表します。
- プライオリティ、プリエンプト、またはその両方を設定するときには、少なくとも 1 つのキーワード（**priority**、**preempt**、または両方）を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、装置のプライオリティがダイナミックに変更されることがあります。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホットスタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。このコマンドは、HSRP 用に設定されていないインターフェイスを追跡する場合に有効です。追跡対象のインターフェイスが故障すると、追跡が設定されている装置のホットスタンバイ プライオリティが 10 だけ減少します。インターフェイスが追跡対象でない場合は、インターフェイスのステートが変わっても、設定済み装置のホットスタンバイ プライオリティは変わりません。ホットスタンバイ用に設定されたインターフェイスごとに、追跡するインターフェイスのリストを個別に設定できます。
- **standby track** *interface-priority* インターフェイス コンフィギュレーション コマンドでは、追跡対象のインターフェイスがダウンした場合のホットスタンバイ プライオリティの減少幅を指定します。インターフェイスが回復すると、プライオリティは同じ分だけ増加します。
- *interface-priority* 値が設定されている場合に複数の追跡対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。プライオリティ値が設定されていない追跡対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- 最初にインターフェイスでルーティングをイネーブルにしたときには、インターフェイスに完全なルーティング テーブルがありません。このインターフェイスは、プリエンプトに設定されている場合はアクティブ ルータになりますが、適切なルーティング サービスは提供できません。この問題を解決するには、ルータがルーティング テーブルを更新できるように遅延時間を設定します。

インターフェイスに HSRP プライオリティ特性を設定するには、特権 EXEC モードで次の 1 つまたは複数の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **priority** *priority*	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルトのプライオリティは 100 です。値が大きいほど、高いプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

	コマンド	目的
ステップ 4	**standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]]	ルータを **preempt** に設定します。これは、ローカル ルータのプライオリティがアクティブ ルータより高い場合は、そのローカル ルータがアクティブ ルータになることを意味します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 36000 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロード後にアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 36000 秒（1 時間）で、デフォルトは 0 です（リロード後に引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：ローカル ルータがアクティブ ルータの役割を引き継いで IP 冗長クライアントが（*ok* または *wait* 応答で）応答できるようにするまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 36000 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** [*group-number*] **track** *type number* [*interface-priority*]	他のインターフェイスを追跡するようにインターフェイスを設定します。この設定により、他のインターフェイスの 1 つがダウンした場合は、その装置のホットスタンバイ プライオリティが減少します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 • *type*：追跡対象のインターフェイス タイプを（インターフェイス番号とともに）入力します。 • *number*：追跡対象のインターフェイス番号を（インターフェイス タイプとともに）入力します。 • （任意）*interface-priority*：インターフェイスがダウンまたは回復した場合に、ルータのホットスタンバイ プライオリティを減少または増加させる幅を入力します。デフォルト値は 10 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

プライオリティ、プリエンプト、および遅延をデフォルト値に戻すには、**no standby** [*group-number*] **priority** *priority* [**preempt** [**delay** *delay*]] and **no standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** *delay*] インターフェイス コンフィギュレーション コマンドを使用します。

追跡を解除するには、**no standby** [*group-number*] **track** *type number* [*interface-priority*] インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをアクティブにし、IP アドレスとプライオリティ 120（デフォルト値よりも高いプライオリティ）を設定して、アクティブ ルータになるまで 300 秒（5 分間）待機する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
```

```
Switch(config-if)# end
```

MHSRP の設定

MHSRP およびロード バランシングをイネーブルにするには、2 台のルータをグループのアクティブ ルータとして設定し、仮想ルータをスタンバイ ルータとして設定します。次に、図 45-2 の MHSRP 設定をイネーブルにする例を示します。故障したルータが回復した場合にプリエンプションが発生してロード バランシングが復元されるように、各 HSRP インターフェイスで **standby preempt** インターフェイスコンフィギュレーション コマンドを入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。ルータ A の HSRP インターフェイスは、IP アドレスが 10.0.0.1 で、グループ 1 のスタンバイ プライオリティが 110（デフォルトは 100）です。ルータ B の HSRP インターフェイスは、IP アドレスが 10.0.0.2 で、グループ 2 のスタンバイ プライオリティが 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

ルータ A の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

HSRP の認証およびタイマーの設定

オプションで HSRP 認証ストリングを設定したり、hello タイムのインターバルやホールドタイムを変更することができます。

これらの属性を設定するときには、次の注意事項に従ってください。

- 認証ストリングはすべての HSRP メッセージで暗号化されずに送信されます。ケーブル上のすべてのルータとアクセス サーバに同じ認証ストリングを設定して、相互運用性を確保する必要があります。認証が一致しない場合、装置は指定されたホットスタンバイ IP アドレスとタイマー値を、HSRP が設定された他のルータから学習できません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を学習できます。アクティブ ルータに設定されたタイマーは、他のタイマー設定よりも常に優先されます。

- ホットスタンバイ グループのすべてのルータで同じタイマー値を使用する必要があります。通常、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスに HSRP の認証とタイマーを設定するには、特権 EXEC モードで次の 1 つまたは複数の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、認証を設定する HSRP インターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **authentication** *string*	（任意）**authentication** *string*：すべての HSRP メッセージで伝送されるストリングを入力します。認証ストリングには 8 文字までを指定できます。デフォルトのストリングは **cisco** です。 （任意）*group-number*：コマンドが適用されるグループ番号です。
ステップ 4	**standby** [*group-number*] **timers** *hellotime holdtime*	（任意）hello パケットのインターバルと、アクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 • *group-number*：コマンドが適用されるグループ番号です。 • *hellotime*：hello インターバル（秒）です。指定できる範囲は 1 ～ 255 です。デフォルトは 3 秒です。 • *holdtime*：アクティブまたはスタンバイ ルータのダウンが宣言されるまでの時間（秒）です。指定できる範囲は 1 ～ 255 です。デフォルトは 10 秒です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

認証ストリングを削除するには、**no standby** [*group-number*] **authentication** *string* インターフェイス コンフィギュレーション コマンドを使用します。タイマーをデフォルト値に戻すには、**no standby** [*group-number*] **timers** *hellotime holdtime* インターフェイス コンフィギュレーション コマンドを使用します。

次に、グループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証ストリングとして、*word* を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、hello パケットのインターバルが 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク レイヤ インターネット プロトコルです。ICMP には、ホストへのエラー パケットの送信や方向付けなどの診断機能があります。

スイッチで HSRP が稼動している場合は、ホストが HSRP グループ内のルータのインターフェイス（または実際の）MAC アドレスを検出しないことを確認してください。ICMP によってホストがルータの実際の MAC アドレスへリダイレクトされ、そのルータがあとで故障した場合、ホストからのパケットは消失します。

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク レイヤ インターネット プロトコルです。ICMP には、ホストへのエラー パケットの送信や方向付けなどの診断機能があります。

HSRP が設定されたインターフェイスでは、ICMP リダイレクト メッセージが自動的にイネーブルになります。この機能は、HSRP を介した発信 ICMP リダイレクト メッセージをフィルタリングします。このときに、ネクストホップ IP アドレスが HSRP 仮想 IP アドレスに変更される可能性があります。詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。

HSRP グループおよびクラスタリングの設定

装置が HSRP スタンバイ ルーティングに参加していて、クラスタリングがイネーブルになっている場合は、同じスタンバイ グループを使用してコマンド スイッチと HSRP の冗長性を確保できます。同じ HSRP スタンバイ グループをイネーブルにして、コマンド スイッチとルーティングの冗長性を確保するために使用するには、**cluster standby-group** *HSRP-group-name* [**routing-redundancy**] グローバル コンフィギュレーション コマンドを使用します。**routing-redundancy** キーワードを指定せずに同じ HSRP スタンバイ グループ名でクラスタを作成すると、そのグループの HSRP スタンバイルーティングがディセーブルになります。

次に、スタンバイ グループ my_hsrp をクラスタにバインドし、同じ HSRP グループをイネーブルにして、コマンド スイッチとルータの冗長性を確保するために使用する例を示します。このコマンドは、クラスタ コマンド スイッチだけで実行できます。スタンバイ グループの名前または番号が存在しないか、スイッチがクラスタ メンバー スイッチである場合は、エラー メッセージが表示されます。

```
Switch# configure terminal
Switch(config)# cluster standby-group my_hsrp routing-redundancy
Switch(config)# end
```

HSRP のトラブルシューティング

表 45-2 に示すいずれかの状況が発生した場合は、次のエラー メッセージが表示されます。

```
%FHRP group not consistent with already configured groups on the switch stack -
virtual MAC reservation failed
```

表 45-2　HSRP のトラブルシューティング

状況	アクション
33 個以上の HSPR グループ インスタンスが設定されている。	設定済みのグループ インスタンスが 32 個以内になるように HSRP グループを削除する。
IPv4 用 HSRP と IPv6 用 HSRP が同時に設定されている。	IPv4 用 HSRP または IPv6 用 HSRP のいずれかをスイッチに設定する。
256 の有効な範囲内にないグループ番号が設定されている。	有効な範囲内のグループ番号を設定する。

HSRP 設定の表示

HSRP 設定を表示するには、特権 EXEC モードで次のコマンドを使用します。

show standby [*interface-id* [*group*]] [**brief**] [**detail**]

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイス上の HSRP グループの HSRP 情報を表示できます。HSRP 情報の概要と詳細のどちらを表示するかを指定することもできます。デフォルト表示は **detail**（詳細）です。多数の HSRP グループがある場合に、修飾子を指定しないで **show standby** コマンドを使用すると、見づらい表示になることがあります。

次に、**show standby** 特権 EXEC コマンドを実行して、2 つのスタンバイ グループ（グループ 1 およびグループ 100）の HSRP 情報を表示する例を示します。

```
Switch# show standby
VLAN1 - Group 1
   Local state is Standby, priority 105, may preempt
   Hellotime 3 holdtime 10
   Next hello sent in 00:00:02.182
   Hot standby IP address is 172.20.128.3 configured
   Active router is 172.20.128.1 expires in 00:00:09
   Standby router is local
   Standby virtual mac address is 0000.0c07.ac01
   Name is bbb
VLAN1 - Group 100
   Local state is Active, priority 105, may preempt
   Hellotime 3 holdtime 10
   Next hello sent in 00:00:02.262
   Hot standby IP address is 172.20.138.51 configured
   Active router is local
   Standby router is unknown expired
   Standby virtual mac address is 0000.0c07.ac64
   Name is test
```

CHAPTER 46

Cisco IOS IP SLA 動作の設定

この章では、IE 3000 スイッチで Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）を使用する方法について説明します。Cisco IP SLA は Cisco IOS ソフトウェアの一部であり、シスコのお客様は、連続的で信頼性が高く予測可能な方法でトラフィックを生成するアクティブ トラフィック モニタリングを使用して、IP アプリケーションとサービスの IP サービス レベルを分析し、ネットワーク パフォーマンスを測定できます。Cisco IOS IP SLA を使用すると、サービス プロバイダーのお客様はサービス レベル契約の測定と提供を実施でき、企業のお客様はサービス レベルの確認、外部委託しているサービス レベル契約の確認、およびネットワーク パフォーマンスの把握を行うことができます。Cisco IOS IP SLA では、ネットワーク アセスメントの実行、Quality of Service（QoS; サービス品質）の確認、新規サービスの導入の簡素化、およびネットワークのトラブルシューティングの支援が可能です。

（注） LAN ベース イメージを実行するスイッチは、IP SLA 応答側の機能だけをサポートしており、IP SLA のすべての機能をサポートする他の装置（IP サービス イメージを実行する IE 3000 スイッチなど）とともに構成する必要があります。

IP SLA の詳細については、次の URL にアクセスして『*Cisco IOS IP SLAs Configuration Guide, Release 12.4T*』を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

コマンド構文の詳細については、次の URL のコマンド リファレンスを参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

この章の内容は次のとおりです。

Cisco IOS IP SLA の概要

Cisco IOS IP SLA は、ネットワーク上にデータを送信して複数のネットワーク ロケーション間または複数のネットワーク パス上のパフォーマンスを測定します。具体的には、ネットワーク データと IP サービスをシミュレートし、ネットワーク パフォーマンス情報をリアルタイムで収集します。Cisco IOS IP SLA は、Cisco IOS 装置間のトラフィック、または Cisco IOS 装置からリモート IP 装置（ネットワーク アプリケーション サーバなど）のトラフィックのいずれかを生成および分析します。各種 Cisco IP SLA 動作により取得される測定結果は、トラブルシューティング、問題分析、およびネットワーク トポロジの設計に利用できます。

実行する Cisco IOS IP SLA 動作に応じて、さまざまなネットワーク パフォーマンスに関する統計情報がシスコ デバイス内でモニタされ、CLI（コマンドライン インターフェイス）Management Information Base（MIB; 管理情報ベース）および SNMP（簡易ネットワーク管理プロトコル）MIB に格納されます。IP SLA パケットには設定可能な IP レイヤ オプションとアプリケーション レイヤ オプションがあります。たとえば、送信元および宛先の IP アドレス、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）/TCP ポート番号、Type of Service（ToS; サービス タイプ）バイト（Differentiated Services Code Point（DSCP）および IP プレフィクス ビットを含む）、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing/Forwarding（VRF; VPN ルーティング/転送）インスタンス、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ 2 トランスポートに依存しないので、異なるネットワーク間にエンドツーエンド動作を設定して、エンド ユーザの利用環境で想定されるメトリックを最大限に反映することができます。IP SLA は次のパフォーマンス メトリックについて、固有のサブセットを収集します。

- 遅延（往復および一方向）
- ジッタ（方向性あり）
- パケット損失（方向性あり）
- パケット シーケンス（パケット順序）
- パス（ホップ単位）
- 接続（方向性あり）
- サーバまたは Web サイトのダウンロード時間

Cisco IOS IP SLA は SNMP でアクセスできるので、CiscoWorks Internetwork Performance Monitor（IPM）のようなパフォーマンスモニタリング アプリケーションのほか、サードパーティ製のシスコ パートナーのパフォーマンス管理製品でも使用できます。Cisco IOS IP SLA を使用するネットワーク管理製品については、次の URL を参照してください。
http://www.cisco.com/go/ipsla

IP SLA を使用すると、次のような利点があります。

- サービスレベル契約のモニタリング、測定、確認。
- ネットワーク パフォーマンス モニタリング。
  - ネットワーク内のジッタ、遅延、パケット損失の測定。
  - 連続的で信頼性が高く予測可能な測定の提供。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに十分であることを確認できる。
- エッジツーエッジ ネットワーク アベイラビリティのモニタリングにより、ネットワーク リソースの予防的な確認と接続テストを行える（たとえば、業務上重要なデータを保存するのに使用される NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる）。
- ネットワーク動作のトラブルシューティングでは、信頼性の高い測定を連続的に実施することで、問題をただちに特定してトラブルシューティングの所用時間を短縮できる。
- Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）パフォーマンス モニタリングとネットワーク確認（スイッチが MPLS をサポートする場合）。

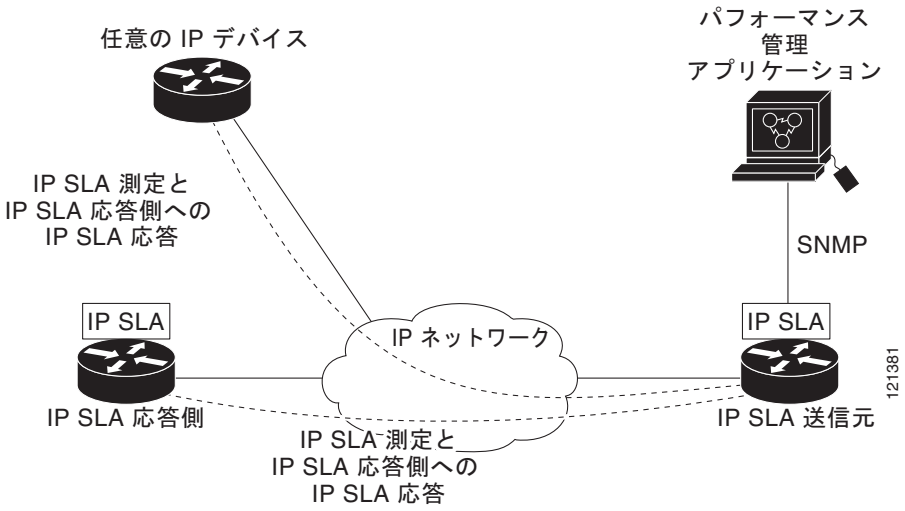
ここでは、次の IP SLA 機能について説明します。

- 「Cisco IOS IP SLA によるネットワーク パフォーマンスの測定」（P.46-3）
- 「IP SLA 応答側および IP SLA 制御プロトコル」（P.46-4）
- 「IP SLA の応答時間の計算」（P.46-4）
- 「IP SLA 動作のスケジューリング」（P.46-5）

Cisco IOS IP SLA によるネットワーク パフォーマンスの測定

IP SLA を使用すると、プローブを物理的に配置しなくても、ネットワーク内の任意のエリア（コア、ディストリビューション、エッジ）間のパフォーマンスをモニタできます。IP SLA は生成したトラフィックを使用して 2 つのネットワーク装置間のネットワーク パフォーマンスを測定します。図 46-1 に、生成したパケットを送信元装置が宛先装置に送信して IP SLA を開始する方法を示します。宛先装置がこのパケットを受信すると、IP SLA 動作のタイプに応じて、タイムスタンプ情報を含めて送信元装置に応答し、パフォーマンス メトリックを計算できるようにします。IP SLA 動作では、UDP などの特定のプロトコルを使用して、ネットワークの送信元装置から宛先までの間のネットワーク測定を実行します。

図 46-1　　Cisco IOS IP SLA 動作



IP SLA ネットワーク パフォーマンス測定を実装するには、次の作業を実行する必要があります。

1. IP SLA 応答側をイネーブルにします（必要な場合）。
2. IP SLA の必要な動作タイプを設定します。
3. 指定した動作タイプで使用可能なオプションを設定します。
4. スレッシュホールド条件を設定します（必要な場合）。
5. 実行する動作をスケジューリングし、ある期間動作させて統計情報を収集します。
6. Cisco IOS CLI を使用するか、SNMP 機能を備えた Network Management System（NMS; ネットワーク管理システム）を使用して、動作の結果を表示および分析します。

IP SLA 動作の詳細については、次の URL にアクセスして、『*Cisco IOS IP SLAs Configuration Guide*』で動作に関する章を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

（注）　スイッチは、ゲートキーパー登録遅延動作測定を使用する Voice over IP（VoIP）サービス レベルをサポートしません。IP SLA アプリケーションを設定する前に **show ip sla application** 特権 EXEC コマンドを使用すると、ご使用のソフトウェア イメージでその動作タイプがサポートされるかどうかを確認できます。

IP SLA 応答側および IP SLA 制御プロトコル

IP SLA 応答側は宛先のシスコ デバイスに組み込まれたコンポーネントで、IP SLA 要求パケットを予想してそれに応答します。応答側は、専用プローブを必要とせずに正確な測定を実施します。応答側は、Cisco IOS IP SLA 制御プロトコルを使用して、待ち受けと応答の実行ポートを通知できるメカニズムを提供します。宛先 IP SLA 応答側に対して送信元になれるのは、Cisco IOS 装置だけです。

（注）　IP SLA 応答側には、Cisco IOS レイヤ 2 応答側設定可能スイッチを使用できます（LAN ベース イメージを実行する Catalyst 2960 または IE 3000 スイッチ、IP ベース イメージを実行する Catalyst 3560 または 3750 スイッチなど）。応答側が IP SLA のすべての機能をサポートする必要はありません。

図 46-1 に、IP ネットワーク内での Cisco IOS IP SLA 応答側の配置例を示します。応答側は、IP SLA 動作が送信する制御プロトコル メッセージを特定のポートで待ち受けます。制御メッセージを受信すると、指定された UDP ポートまたは TCP ポートを、指定された期間、イネーブルにします。この期間中に、応答側は要求を受け付け、その応答を返します。ポートは IP SLA パケットに応答したあと、または指定された時間が経過したときにディセーブルにされます。セキュリティの強化には、制御メッセージに MD5 認証を利用できます。

すべての IP SLA 動作に対応するように宛先装置で応答側をイネーブルにする必要はありません。たとえば、宛先ルータですでに提供されているサービス（Telnet、HTTP など）に応答側は必要ありません。IP SLA 応答側は非シスコ デバイス上には設定できません。また、Cisco IOS IP SLA が動作パケットを送信できるのは、これらの装置で固有のサービスに対してだけです。

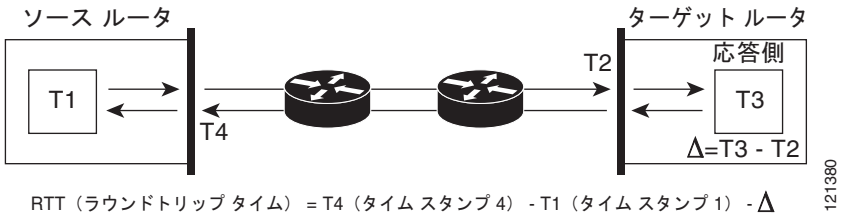
IP SLA の応答時間の計算

スイッチおよびルータの着信パケットの処理には、他にプライオリティの高い処理があるために数十ミリ秒かかることがあります。この遅延は応答時間に影響します。テストパケット応答が処理待ちのキューに入っていることもあるからです。このような場合、応答時間には本来のネットワーク遅延が正確に反映されません。IP SLA は、送信元装置および接続先装置（応答側が使用されている場合）での処理遅延をできるだけ小さくして、正しいラウンドトリップ時間が得られるようにしています。IP SLA テスト パケットでは処理遅延を最小化するためにタイム スタンプが使用されます。

IP SLA 応答側がイネーブルになっていると、接続先装置ではパケットがインターフェイスに着信したときに割り込みレベルでタイム スタンプを付加し、送信するときにも付加できるので、処理時間が省かれます。このタイム スタンプはサブミリ秒の精度で作成されます。

図 46-2 に、応答側の動作を示します。ラウンドトリップ時間の計算では、4 つのタイム スタンプを使用します。ターゲット ルータで応答側機能がイネーブルになっている場合、タイム スタンプ 3（TS3）からタイム スタンプ 2（TS2）を引いてテスト パケットの処理に使用された時間を求め、これをデルタ（Δ）とします。次に、全体のラウンドトリップ時間からこのデルタの値を引きます。IP SLA により、ソース ルータでも同じ方法が適用されます。その場合、割り込みレベルで着信のタイム スタンプ 4（TS4）が付加されるので精度が向上します。

図 46-2　Cisco IOS IP SLA 応答側のタイム スタンプ



接続先装置に 2 つのタイム スタンプがあると、一方向遅延、ジッタ、方向性を持つパケット損失を追跡できるという利点もあります。ネットワーク動作の多くは非同期なので、これらの統計情報を得ておくことが重要です。ただし、一方向遅延測定をキャプチャする場合は、ソース ルータとターゲット ルータの両方に Network Time Protocol（NTP; ネットワーク タイム プロトコル）を設定し、両方のルータを同じクロック ソースに同期させる必要があります。一方向ジッタの測定の場合、クロックを同期させる必要はありません。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合、統計情報のキャプチャとエラー情報の収集を開始するように動作をスケジューリングする必要があります。スケジューリングには、すぐに動作を開始する方法と、月、日、時間を指定して開始する方法があります。pending オプションを使用して、あとで動作を開始することもできます。pending オプションは動作の内部ステータスの 1 つで、SNMP を介して表示できます。トリガーを待つ反応（スレッショルド）動作の場合にも、この pending ステータスを使用します。IP SLA 動作を一度に 1 つスケジューリングすることも、複数スケジューリングすることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB からは、IP サービス イメージを実行するスイッチ上に 1 つのコマンドで複数の IP SLA 動作をスケジューリングできます。複数の動作を等間隔で実行するようにスケジューリングすれば、IP SLA モニタリングのトラフィック量を制御できます。IP SLA 動作を分散することで CPU 使用率を最小化できるので、ネットワークのスケーラビリティが向上します。

IP SLA 複数動作のスケジューリング機能の詳細については、次の URL の『*Cisco IOS IP SLAs Configuration Guide*』の「IP SLAs - Multiple Operation Scheduling」の章を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA 動作のスレッショルドのモニタリング

サービス レベル契約モニタリングを適切に利用するには、何らかの違反が予想される場合にすぐに通知されるメカニズムを設定する必要があります。IP SLA は次のようなイベントによってトリガーされる SNMP トラップを送信できます。

- 接続の切断
- タイムアウト
- ラウンドトリップ時間のスレッショルド
- 平均ジッタ スレッショルド
- 一方向パケット損失
- 一方向ジッタ
- 一方向 Mean Opinion Score（MOS; 平均オピニオン評点）
- 一方向遅延

IP SLA のスレッショルドを超過した場合に、もう 1 つ IP SLA 動作をトリガーさせて、さらに分析することもできます。たとえば、トラブルシューティングのために、頻度を増やしたり、ICMP パス エコーや ICMP パス ジッタ動作を開始させたりすることができます。

設定するスレッショルドのタイプとレベルの決定は複雑になる場合があり、ネットワークで使用されている IP サービスのタイプによっても変わってきます。Cisco IOS IP SLA 動作でスレッショルドを使用する方法の詳細については、次の URL にある『*Cisco IOS IP SLAs Configuration Guide*』の「IP SLAs—Proactive Threshold Monitoring」を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA 動作の設定

ここでは、利用可能なすべての動作に関する設定情報を説明するわけではありません。設定情報の詳細については、『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。ここでは、応答側の設定、UDP ジッタ動作の設定（応答側が必要）、ICMP エコー動作の設定（応答側は不要）などの動作の例を説明します。

（注）　LAN ベース イメージを実行するスイッチは、IP SLA 応答側の機能だけをサポートします。IP SLA のすべての機能を使用するには、スイッチで IP サービス イメージを実行している必要があります。

他の動作の設定の詳細については、次の URL の『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

ここでは、次の内容について説明します。

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA コマンドについては、次の URL の『*Cisco IOS IP SLAs Command Reference, Release 12.4T*』のコマンド リファレンスを参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

詳細な説明と設定手順については、次の URL の『*Cisco IOS IP SLAs Configuration Guide, Release 12.4T*』を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

スイッチは、このマニュアルで説明する IP SLA コマンドや動作をすべてサポートするわけではありません。スイッチがサポートするのは、UDP ジッタ、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッタ、FTP、DNS、および DHCP を使用する IP サービス レベル分析です。また、複数動作のスケジューリングおよび予防的スレッシュホールド モニタリングもサポートします。ゲートキーパー登録遅延動作測定を使用する VoIP サービス レベルはサポートしません。

IP SLA アプリケーションを設定する前に **show ip sla application** 特権 EXEC コマンドを使用すると、ご使用のソフトウェア イメージでその動作タイプがサポートされるかどうかを確認できます。次に、コマンドの出力例を示します。

```
Switch# show ip sla application
        IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0

        Supported Operation Types
Type of Operation to Perform: 802.1agEcho
Type of Operation to Perform: 802.1agJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho

IP SLAs low memory water mark: 21741224
```

IP SLA 応答側の設定

IP SLA 応答側を利用できるのは、IP SLA のすべての機能をサポートしていないレイヤ 2 スイッチ（例：LAN ベース イメージを実行する Catalyst 2960 または Cisco ME 2400 または IE 3000 スイッチ）などの Cisco IOS ソフトウェアベース装置だけです。接続先装置（動作対象）上で IP SLA 応答側を設定するには、特権 EXEC モードから開始して、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla responder** {**tcp-connect** | **udp-echo**} **ipaddress** *ip-address* **port** *port-number*	スイッチを IP SLA 応答側として設定します。 オプションのキーワードの意味は次のとおりです。 • **tcp-connect**：応答側の TCP 接続動作をイネーブルにします。 • **udp-echo**：応答側の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）エコー動作またはジッタ動作をイネーブルにします。 • **ipaddress** *ip-address*：宛先 IP アドレスを入力します。 • **port** *port-number*：宛先ポート番号を入力します。 （注）　IP アドレスおよびポート番号は、IP SLA 動作の送信元装置に設定されている IP アドレスおよびポート番号と一致する必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip sla responder**	装置の IP SLA 応答側設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IP SLA 応答側をディセーブルにするには、**no ip sla responder** グローバル コンフィギュレーション コマンドを入力します。次に、装置を UDP ジッタ IP SLA 動作の応答側に設定する例を示します。

```
Switch(config)# ip sla responder udp-echo 172.29.139.134 5000
```

（注）　IP SLA 応答側が機能するには、IP サービス イメージを実行する Catalyst 3750 または Catalyst 3560 スイッチなど、IP SLA のすべての機能をサポートする送信元装置も設定する必要があります。設定の詳細については、送信元装置のマニュアルを参照してください。

UDP ジッタ動作を使用した IP サービス レベルの分析

ジッタは、インターパケット遅延のばらつきです。送信元から宛先に複数のパケットが連続して 10 ミリ秒間隔で送信された場合、ネットワークが正しく動作していれば宛先でも同じパケット群を 10 ミリ秒間隔で受信するはずです。しかし、ネットワークに遅延があると（キューイング、別ルートでの到着など）、パケット間の到着遅延は 10 ミリ秒よりも長くなったり短くなったりすることがあります。ジッタ値がプラスの場合は、パケットが 10 ミリ秒より長い間隔で到着したことを意味します。パケットが 12 ミリ秒間隔で到着した場合、ジッタ値は +2 ミリ秒となり、パケットが 8 ミリ秒間隔で到着した場合、ジッタ値は -2 ミリ秒となります。遅延に影響されやすいネットワークでは、プラスのジッタ値は望ましくなく、ジッタ値は 0 が理想的です。

IP SLA UDP ジッタ動作は、ジッタのモニタリング以外に多目的のデータ収集動作に使用できます。パケット IP SLA は搬送パケットを生成し、送信元と動作対象間でシーケンス情報の送受信とタイム スタンプの送受信を行います。これらに基づいて、UDP ジッタ動作は次のデータを測定します。

- 方向別ジッタ（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均ラウンドトリップ時間）

データの送信と受信でパスが異なることがあるので（非対称）、方向別データを使用してネットワークで輻輳などの問題が発生している場所を簡単に特定できます。

UDP ジッタ動作では、合成（シミュレーション）UDP トラフィックを生成し、ソース ルータからターゲット ルータに多数の UDP パケットを送信します。パケットのサイズ、パケット同士の間隔（ミリ秒）、繰り返しの頻度は任意です。デフォルトでは、ペイロード サイズ 10 バイトのパケットフレームを 10 個、10 ミリ秒ごとに生成し、60 秒ごとに動作を繰り返します。これらのパラメータは、提供する IP サービスが最もよくシミュレートされるように設定します。

一方向遅延を正確に測定するには、送信元装置と接続先装置の間で時刻同期（NTP などにより提供される）が必要です。一方向ジッタとパケット損失を測定する場合は、時刻同期は必要ありません。送信元装置と接続先装置の間で時刻が同期していない場合、一方向ジッタとパケット損失のデータが戻りますが、UDP ジッタ動作による一方向遅延測定では *0* の値が戻ります。

（注） 送信元装置上で UDP ジッタ動作を設定する前に、接続先装置（動作対象）上で IP SLA 応答側をイネーブルにする必要があります。

送信元装置上で UDP ジッタ動作を設定するには、特権 EXEC モードから開始して、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]	IP SLA 動作を UDP ジッタ動作として設定し、UDP ジッタ コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 • （任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名を指定しない場合、IP SLA は宛先に最も近い IP アドレスを選択します。 • （任意）**source-port** *port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 • （任意）**control**：IP SLA 応答側への IP SLA コントロール メッセージの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA 応答側との接続を確立するために、宛先装置に IP SLA コントロール メッセージが送信されます。 • （任意）**num-packets** *number-of-packets*：生成するパケット数を入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 • （任意）**interval** *inter-packet-interval*：パケットの送信間隔（ミリ秒）を入力します。指定できる範囲は 1 ～ 6000 です。デフォルト値は 20 ミリ秒です。
ステップ 4	**frequency** *seconds*	（任意）指定した IP SLA 動作を繰り返すレートを設定します。指定できる範囲は 1 ～ 604800 秒です。デフォルトは 60 秒です。
ステップ 5	**exit**	UDP ジッタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**ip sla monitor schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 •（任意）**life**：動作の実行を無期限（**forever**）に設定するか、*seconds* に秒数を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time**：動作が情報の収集を開始する時刻を入力します。 – 特定の時刻に開始するには、時、分、秒（24 時間表記）、日にちを入力します。月を入力しない場合は、デフォルトで現在の月になります。 – **pending** と入力すると、開始時刻を指定するまで情報収集は行われません。 – **now** と入力すると、すぐに動作が開始されます。 – **after** *hh:mm:ss* と入力すると、指定した時間が経過してから動作が開始されます。 •（任意）**ageout** *seconds*：情報をアクティブに収集していない場合、動作をメモリに常駐させておく時間を秒数で入力します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒です（常駐したまま）。 •（任意）**recurring**：動作を毎日、自動的に実行するように設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip sla configuration** [*operation-number*]	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値とともに表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IP SLA 動作をディセーブルにするには、**no ip sla** *operation-number* グローバル コンフィギュレーション コマンドを入力します。次に、UDP ジッタ IP SLA 動作を設定する例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
```

```
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

ICMP エコー動作を使用した IP サービス レベルの分析

ICMP エコー動作では、シスコ デバイスと IP を使用する任意の装置との間のエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセージを宛先に送信してから ICMP エコー応答を受信するまでにかかった時間を測定して算出します。お客様の多くは、送信元 IP SLA 装置と宛先 IP 装置との間の応答時間の測定に、IP SLA ICMP ベース動作、社内 ping テスト、または ping ベースの専用プローブを使用しています。IP SLA ICMP エコー動作と ICMP ping テストは同じ仕様に準拠しているので、どちらの方法でも同じ応答時間が得られます。

（注） この動作では、IP SLA 応答側をイネーブルにする必要はありません。

送信元装置上で ICMP エコー動作を設定するには、特権 EXEC モードから開始して、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-id*]	IP SLA 動作を ICMP エコー動作として設定し、ICMP エコー コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • （任意）**source-ip** {*ip-address* | *hostname*} *:* 送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名を指定しない場合、IP SLA は宛先に最も近い IP アドレスを選択します。 • （任意）**source-interface** *interface-id*：この動作の送信元インターフェイスを指定します。
ステップ 4	**frequency** *seconds*	（任意）指定した IP SLA 動作を繰り返すレートを設定します。指定できる範囲は 1 ～ 604800 秒です。デフォルトは 60 秒です。
ステップ 5	**exit**	UDP ジッタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 •（任意）**life**：動作の実行を無期限（**forever**）に設定するか、*seconds* に秒数を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time**：動作が情報の収集を開始する時刻を入力します。 – 特定の時刻に開始するには、時、分、秒（24 時間表記）、日にちを入力します。月を入力しない場合は、デフォルトで現在の月になります。 – **pending** と入力すると、開始時刻を指定するまで情報収集は行われません。 – **now** と入力すると、すぐに動作が開始されます。 – **after** *hh:mm:ss* と入力すると、指定した時間が経過してから動作が開始されます。 •（任意）**ageout** *seconds*：情報をアクティブに収集していない場合、動作をメモリに常駐させておく時間を秒数で入力します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒です（常駐したまま）。 •（任意）**recurring**：動作を毎日、自動的に実行するように設定します。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	**show ip sla configuration** [*operation-number*]	（任意）すべての IP SLA 動作または指定した IP SLA 動作に関する設定値を、すべてのデフォルト値とともに表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

IP SLA 動作をディセーブルにするには、**no ip sla** *operation-number* グローバル コンフィギュレーション コマンドを入力します。次に、ICMP エコー IP SLA 動作を設定する例を示します。

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
```

```
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

IP SLA 動作のモニタリング

IP SLA 動作の設定と結果を表示するには、表 46-1 に示すユーザ EXEC または特権 EXEC コマンドを使用します。

表 46-1　IP SLA 動作のモニタリング

コマンド	目的
show ip sla application	Cisco IOS IP SLA に関するグローバル情報を表示します。
show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する設定値を、すべてのデフォルト値とともに表示します。
show ip sla enhanced-history {**collection-statistics** | **distribution statistics**} [*entry-number*]	収集した履歴バケットの拡張履歴統計情報、あるいはすべての IP SLA 動作または特定の IP SLA 動作に関する分散統計情報を表示します。
show ip sla ethernet-monitor configuration [*entry-number*]	IP SLA 自動イーサネット設定を表示します。
show ip sla group schedule [*schedule-entry-number*]	IP SLA グループ スケジューリング設定と詳細情報を表示します。
show ip sla history [*entry-number* | **full** | **tabular**]	すべての IP SLA 動作について収集した履歴を表示します。
show ip sla mpls-lsp-monitor {**collection-statistics** | **configuration** | **ldp operational-state** | **scan-queue** | **summary** [*entry-number*] | **neighbors**}	MPLS Label Switched Path（LSP; ラベル スイッチド パス）ヘルス モニタ動作を表示します。
show ip sla reaction-configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する、予防的スレッシュホールド モニタリングの設定を表示します。
show ip sla reaction-trigger [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する反応トリガー情報を表示します。
show ip sla responder	IP SLA 応答側に関する情報を表示します。
show ip sla statistics [*entry-number* | **aggregated** | **details**]	動作ステータスおよび統計情報の現在値または集約情報を表示します。

CHAPTER 47

拡張オブジェクト追跡の設定

この章では、IE 3000 スイッチに拡張オブジェクト追跡を設定する方法について説明します。この機能は、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）に代わる、より完全な追跡メカニズムを備えており、インターフェイスの回線プロトコル ステートを追跡できます。インターフェイスの回線プロトコル ステートがダウンすると、インターフェイスの HSRP プライオリティが減少して、よりプライオリティの高い他の HSRP 装置がアクティブになります。拡張オブジェクト追跡機能は、HSRP から追跡メカニズムを分離させて、独立した追跡プロセスを別途生成します。これにより、HSRP 以外のプロセスがこの追跡プロセスを使用できます。この機能を使用すると、インターフェイスの回線プロトコル ステートに加えて他のオブジェクトも追跡できます。HSRP のようなクライアント プロセスは、オブジェクトを追跡する対象を登録し、追跡対象のオブジェクトのステートが変化したら通知するように要求できます。この機能により、ルーティング システムのアベイラビリティと回復速度が向上し、停止回数と停止時間が減少します。

（注） この機能は、IP サービス イメージが稼動しているスイッチでだけサポートされます。

拡張オブジェクト追跡およびその設定に使用するコマンドの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541be.html

この章で説明する内容は、次のとおりです。

拡張オブジェクト追跡の概要

各追跡対象オブジェクトには、追跡 CLI（コマンドライン インターフェイス）で指定される一意の番号があります。クライアント プロセスは、この番号を使用して特定のオブジェクトを追跡します。追跡プロセスは、追跡対象オブジェクトに値の変化がないかどうかを定期的にポーリングし、（アップまたはダウン値など）変化があれば登録されているクライアント プロセスに通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。同じオブジェクトを複数のクライアントが追跡して、オブジェクトのステートが変化した場合に、それぞれが異なるアクションを実行することができます。

複数のオブジェクトを組み合わせて 1 つのリストにして追跡することもできます。このリストのステートの判定には、ウェイト スレッショルドまたはパーセンテージ スレッショルドを使用します。オブジェクトの組み合わせには、ブール論理を使用できます。「AND」ブール関数を使用する追跡リストの場合、リスト内の各オブジェクトがアップ ステートでないと追跡対象オブジェクトはアップになりません。「OR」ブール関数を使用する追跡リストの場合、リスト内の 1 つのオブジェクトだけがアップ ステートであれば追跡対象オブジェクトはアップになります。

拡張オブジェクト追跡機能の設定

ここでは、拡張オブジェクト追跡機能の設定について説明します。

デフォルト設定

オブジェクト追跡タイプは設定されていません。

インターフェイスの回線プロトコルまたは IP ルーティング ステートの追跡

インターフェイスの回線プロトコル ステートまたはインターフェイスの IP ルーティング ステートのいずれかを追跡できます。IP ルーティング ステートを追跡する場合、オブジェクトをアップにするには次の 3 つの条件が必要です。

- インターフェイス上で IP ルーティングがイネーブル、かつアクティブになっている。
- インターフェイスの回線プロトコル ステートがアップ ステートである。
- 既知のインターフェイス IP アドレスを使用している。

この 3 つの条件がすべて合致しないと、IP ルーティング ステートはダウンになります。

インターフェイスの回線プロトコル ステートまたは IP ルーティング ステートを追跡するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-number* **interface** *interface-id* **line-protocol**	（任意）インターフェイスの回線プロトコル ステートを追跡するための追跡リストを作成し、追跡コンフィギュレーション モードを開始します。 • *object-number*：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • **interface** *interface-id*：追跡されるインターフェイスです。

	コマンド	目的
ステップ 3	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**track** *object-number* **interface** *interface-id* **ip routing**	（任意）インターフェイスの IP ルーティング ステートを追跡するための追跡リストを作成し、追跡コンフィギュレーション モードを開始します。IP ルート追跡では、ルーティング テーブル内の IP ルートおよびインターフェイスの IP パケット ルーティング機能を追跡します。 • *object-number*：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • **interface** *interface-id*：追跡されるインターフェイスです。
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track** *object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、インターフェイスの回線プロトコル ステートの追跡を設定し、その設定を確認する例を示します。

```
Switch(config)# track 33 interface gigabitethernet 1/1 line-protocol
Switch(config-track)# end
Switch# show track 33
Track 33
Interface GigabitEthernet1/1 line-protocol
  Line protocol is Down (hw down)
    1 change, last change 00:18:28
```

追跡リストの設定

オブジェクトの追跡リストは、ブール式、ウェイト スレッシュホールド、またはパーセンテージ スレッシュホールドを使用して設定できます。追跡リストには 1 つまたは複数のオブジェクトを含みます。オブジェクトは存在していないと追跡リストに追加できません。

- 設定にブール式による演算を指定する場合は、「AND」または「OR」演算子を使用します。
- 追跡リストのステートをウェイト スレッシュホールドで判定する場合は、追跡リスト内の各オブジェクトにウェイト番号を割り当てます。追跡リストのステートは、このスレッシュホールドに合致したかどうかで判定されます。各オブジェクトのステートは、すべてのオブジェクトのウェイトの合計と各オブジェクトのスレッシュホールドのウェイトを比較して判定されます。
- 追跡リストをパーセンテージ スレッシュホールドで判定する場合は、追跡リスト内のすべてのオブジェクトにパーセンテージ スレッシュホールドを割り当てます。各オブジェクトのステートは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

ブール式による追跡リストの設定

ブール式を使用して追跡リストを設定すると、「AND」または「OR」演算子を使用した演算が可能になります。たとえば、「AND」演算子で 2 つのインターフェイスを追跡すると、*up* は両方のインターフェイスがアップであることを意味し、*down* はどちらかのインターフェイスがダウンであることを意味します。

ブール式を使用してオブジェクトの追跡リストを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *track-number* **list boolean** {**and** | **or**}	追跡リスト オブジェクトを設定し、追跡コンフィギュレーション モードを開始します。*track-number* に指定できる範囲は 1 ～ 500 です。 • **boolean** : 追跡リストのステートがブール演算に基づくことを指定します。 • **and** : すべてのオブジェクトがアップの場合にリストはアップであること、また、1 つまたは複数のオブジェクトがダウンの場合にリストはダウンであることを指定します。 • **or** : 1 つのオブジェクトがアップの場合にリストはアップであること、または、すべてのオブジェクトがダウンの場合にリストはダウンであることを指定します。
ステップ 3	**object** *object-number* [**not**]	追跡対象オブジェクトを指定します。指定できる範囲は 1 ～ 500 です。**not** キーワードはオブジェクトのステートを否定します。つまり、オブジェクトがアップの場合に、追跡リストはそのオブジェクトをダウンとして検出することを意味します。 **（注）**　オブジェクトは存在していないと追跡リストに追加できません。
ステップ 4	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show track** *object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

追跡リストを削除するには、**no track** *track-number* グローバル コンフィギュレーション コマンドを使用します。

次に、AND ブール式を使用して追跡リスト 4 を作成する例を示します。リストには 2 つのオブジェクトが含まれ、そのうち 1 つのオブジェクトが否定されます。このリストがアップの場合は、object 2 がダウンであることを検出しています。

```
Switch(config)# track 4 list boolean and
Switch(config-track)# object 1
Switch(config-track)# object 2 not
Switch(config-track)# exit
```

ウェイト スレッシュホールドによる追跡リストの設定

ウェイト スレッシュホールドによる追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、ウェイトをスレッシュホールドとして使用することを指定したあと、各オブジェクトにウェイトを設定します。各オブジェクトのステートは、アップであるすべてのオブジェクトのウェイトの合計と各オブジェクトのスレッシュホールドのウェイトを比較して判定されます。

ウェイト スレッシュホールドのリストには、「NOT」ブール演算子を使用できません。

ウェイト スレッシュホールドを使用してオブジェクトの追跡リストを作成し、各オブジェクトにウェイトを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *track-number* **list threshold weight**	追跡リスト オブジェクトを設定し、追跡コンフィギュレーション モードを開始します。*track-number* に指定できる範囲は 1 ～ 500 です。 • **threshold**：追跡リストのステートがスレッシュホールドに基づくことを指定します。 • **weight**：スレッシュホールドがウェイトに基づくことを指定します。
ステップ 3	**object** *object-number* [**weight** *weight-number*]	追跡対象オブジェクトを指定します。指定できる範囲は 1 ～ 500 です。任意の **weight** *weight-number* には、オブジェクトのスレッシュホールドのウェイトを指定します。指定できる範囲は 1 ～ 255 です。 **（注）**　オブジェクトは存在していないと追跡リストに追加できません。
ステップ 4	**threshold weight** {**up** *number* | [**down** *number*]}	スレッシュホールドのウェイトを指定します。 • **up** *number*：指定できる範囲は 1 ～ 255 です。 • **down** *number*：（任意）指定できる範囲は、**up** *number* で指定した値により異なります。**up** *number* を 25 に設定すると、down number の範囲は 0 ～ 24 です。
ステップ 5	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show track** *object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

追跡リストを削除するには、**no track** *track-number* グローバル コンフィギュレーション コマンドを使用します。

次に、ウェイト スレッシュホールドにより追跡する追跡リスト 4 を設定する例を示します。object 1 および object 2 がダウンの場合、object 3 が up 30 というスレッシュホールドを満たすので、追跡リスト 4 はアップです。object 3 がダウンの場合、object 1 および object 2 の両方がアップでないと、スレッシュホールドのウェイトを満たしません。

```
Switch(config)# track 4 list threshold weight
Switch(config-track)# object 1 weight 15
Switch(config-track)# object 2 weight 20
Switch(config-track)# object 3 weight 30
Switch(config-track)# threshold weight up 30 down 10
Switch(config-track)# exit
```

この設定は、object 1 および object 2 が 2 つの小さな帯域幅の接続を、object 3 が大きな帯域幅の接続を表す場合に有効です。設定した **down 10** の値は、追跡対象オブジェクトがいったんアップになると、スレッシュホールドが 10 以下になるまではダウンにならないことを意味します。この例で 10 以下は、すべての接続がダウンすることを意味します。

パーセンテージ スレッシュホールドによる追跡リストの設定

パーセンテージ スレッシュホールドによる追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、パーセンテージをスレッシュホールドとして使用することを指定したあと、リスト内のすべてのオブジェクトにパーセンテージを指定します。リストのステートは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

パーセンテージ スレッシュホールドのリストには、「NOT」ブール演算子を使用できません。

パーセンテージ スレッシュホールドを使用してオブジェクトの追跡リストを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *track-number* **list threshold percentage**	追跡リスト オブジェクトを設定し、追跡コンフィギュレーション モードを開始します。*track-number* に指定できる範囲は 1 ～ 500 です。 • **threshold**：追跡リストのステートがスレッシュホールドに基づくことを指定します。 • **percentage**：スレッシュホールドがパーセンテージに基づくことを指定します。
ステップ 3	**object** *object-number*	追跡対象オブジェクトを指定します。指定できる範囲は 1 ～ 500 です。 **（注）**　オブジェクトは存在していないと追跡リストに追加できません。
ステップ 4	**threshold percentage** {**up** *number* | [**down** *number*]}	スレッシュホールドのパーセンテージを指定します。 • **up** *number*：指定できる範囲は 1 ～ 100 です。 • **down** *number*：（任意）指定できる範囲は、**up** *number* で指定した値により異なります。**up** *number* を 25 に設定すると、down number の範囲は 0 ～ 24 です。
ステップ 5	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show track** *object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

追跡リストを削除するには、**no track** *track-number* グローバル コンフィギュレーション コマンドを使用します。

次に、3 つのオブジェクトを持つ追跡リスト 4 を作成し、パーセンテージを指定してリストのステートを判定する例を示します。

```
Switch(config)# track 4 list threshold percentage
Switch(config-track)# object 1
Switch(config-track)# object 2
Switch(config-track)# object 3
Switch(config-track)# threshold percentage up 51 down 10
Switch(config-track)# exit
```

HSRP オブジェクト追跡の設定

特定のオブジェクトを追跡し、そのオブジェクトのステートに基づいて HSRP プライオリティを変更できるようにスタンバイ HSRP グループを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-number* {**interface** *interface-id* {**line-protocol** | **ip routing**} | **ip route** *ip-address/prefix-length* {**metric threshold** | **reachability**} | **list** {**boolean** {**and** | **or**}} | {**threshold** {**weight** | **percentage**}}}	（任意）設定されたステートを追跡するための追跡リストを作成し、追跡コンフィギュレーション モードを開始します。 • *object-number* に指定できる範囲は 1 ～ 500 です。 • 追跡するインターフェイスを指定するには、**interface** *interface-id* を入力します。 • インターフェイスの回線プロトコル ステートを追跡するには、**line-protocol** を入力します。また、インターフェイスの IP ルーティング ステートを追跡するには、**ip routing** を入力します。 • IP ルートのステートを追跡するには、**ip route** *ip-address/prefix-length* を入力します。 • **metric threshold** を入力してスレッショルドのメトリックを追跡するか、**reachability** を入力してルートが到達可能かどうかを追跡します。 デフォルトの up スレッショルドは 254、デフォルトの down スレッショルドは 255 です。 • リスト内の一連のオブジェクトを追跡するには、**list** を入力します。リストはこれまでのページの説明に従って作成してください。 – **boolean** については、「ブール式による追跡リストの設定」（P.47-3）を参照してください。 – **threshold weight** については、「ウェイト スレッショルドによる追跡リストの設定」（P.47-4）を参照してください。 – **threshold percentage** については、「パーセンテージ スレッショルドによる追跡リストの設定」（P.47-6）を参照してください。 **（注）**　追跡するインターフェイスごとに、このステップを繰り返します。
ステップ 3	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を入力します。指定できる範囲は 0 ～ 255 です。デフォルト値は 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習できます。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 6	**standby** [*group-number*] **track** *object-number* [**decrement** [*priority-decrement*]]	特定のオブジェクトを追跡し、そのオブジェクト ステートに基づいてホットスタンバイ プライオリティを変更できるように HSRP を設定します。 • （任意）*group-number*：追跡が適用されるグループ番号を入力します。 • *object-number*：追跡対象のオブジェクト番号を入力します。指定できる範囲は 1 ～ 500 で、デフォルトは 1 です。 • （任意）**decrement** *priority-decrement*：追跡対象のオブジェクトがダウンになった場合（またはアップに戻った場合）に、ルータのホットスタンバイ プライオリティを減少（または増加）させる幅を指定します。指定できる範囲は 1 ～ 255 で、デフォルトは 10 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show standby**	スタンバイ ルータの IP アドレスおよび追跡ステートを確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

その他の追跡特性の設定

拡張オブジェクト追跡機能を使用して他の特性を追跡することもできます。

- **track ip route reachability** グローバル コンフィギュレーション コマンドを使用すると、IP ルートの到達可能性を追跡できます。
- **track ip route metric threshold** グローバル コンフィギュレーション コマンドを使用すると、ルートがスレッシュホールドを超えているか下回っているかを確認できます。
- **track resolution** グローバル コンフィギュレーション コマンドを使用すると、ルーティング プロトコルのメトリック解決のデフォルト値を変更できます。
- **track timer** 追跡コンフィギュレーション コマンドを使用すると、追跡対象オブジェクトを定期的にポーリングするように追跡プロセスを設定できます。

拡張オブジェクト追跡設定を確認するには、**show track** 特権 EXEC コマンドを使用します。

拡張オブジェクト追跡およびその設定に使用するコマンドの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541be.html

IP SLA オブジェクト追跡の設定

Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）は、ネットワーク パフォーマンスの測定と診断を行うツールです。ネットワーク パフォーマンスを測定するためのトラフィック生成には、アクティブ モニタリングが使用されます。Cisco IP SLA 動作は、ネットワークのトラブルシューティングや設計、分析に使用できるリアルタイム メトリックを収集します。

スイッチの Cisco IP SLA については、第 46 章「Cisco IOS IP SLA 動作の設定」を参照してください。IP SLA コマンドについては、次の URL の『*Cisco IOS IP SLAs Command Reference, Release 12.4T*』を参照してください。
http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a008049739b.html

IP SLA 動作のオブジェクト追跡を活用すると、クライアントは IP SLA オブジェクトの出力を追跡して、その情報をアクションのトリガーに使用できます。各 IP SLA 動作は、*OK* または *OverThreshold* のような Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）動作のリターン コード値を保持しているため、追跡プロセス側で解釈できます。IP SLA 動作は、ステートと到達可能性の 2 つの面を追跡できます。ステートの場合、リターン コードが OK のとき、追跡ステートがアップします。リターン コードが OK ではないとき、追跡ステートはダウンします。到達可能性の場合、リターン コードが OK または OverThreshold のとき、到達可能性がアップします。リターン コードが OK ではないとき、到達可能性はダウンします。

IP SLA 動作のステートまたは IP SLA IP ホストの到達可能性を追跡するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-number* **rtr** *operation-number* **state**	追跡コンフィギュレーション モードを開始し、IP SLA 動作のステートを追跡します。 • *object-number* に指定できる範囲は 1 ～ 500 です。 • *operation-number* に指定できる範囲は 1 ～ 2147483647 です。
ステップ 3	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**track** *object-number* **rtr** *operation-number* **reachability**	追跡コンフィギュレーション モードを開始し、IP SLA IP ホストの到達可能性を追跡します。 • *object-number* に指定できる範囲は 1 ～ 500 です。 • *operation-number* に指定できる範囲は 1 ～ 2147483647 です。
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track** *object-number*	追跡情報を表示し、設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、IP SLA ステート追跡を設定および表示する例を示します。

```
Switch(config)# track 2 200 state
Switch(config)# end
Switch# show track 2
Track 2
  Response Time Reporter 1 state
```

```
  State is Down
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (millisecs) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

次の出力例では、ルートが到達可能であるかどうかを示します。

```
Switch(config)# track 3 500 reachability
Switch(config)# end
Switch# show track 3
Track 3
  Response Time Reporter 1 reachability
  Reachability is Up
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (millisecs) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

スタティック ルーティング サポートの設定

Cisco IOS Release 12.2(46)SE 以降で IP サービス イメージを実行しているスイッチは、拡張オブジェクト追跡のスタティック ルーティングをサポートしています。拡張オブジェクト追跡を使用したスタティック ルーティング サポートを使用することで、スイッチが Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）ping を使用して設定済みのスタティック ルートまたは DHCP ルートのダウン時を特定できます。追跡を有効にしている場合、システムはルート ステートを追跡し、ステートの変化をクライアントに通知できます。スタティック ルート オブジェクト追跡は、プライマリ ゲートウェイへの接続状態をモニタするために、Cisco IP SLA を使用して ICMP ping を生成します。

- スイッチの Cisco IP SLA サポートの詳細については、第 46 章「Cisco IOS IP SLA 動作の設定」を参照してください。
- スタティック ルート オブジェクト追跡の詳細については、次の URL を参照してください。
  http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

次の手順に従って、スタティック ルート オブジェクト追跡を設定します。

ステップ 1　スタティック ルーティングまたは DHCP のプライマリ インターフェイスを設定します。

ステップ 2　IP SLA エージェントを設定し、プライマリ インターフェイスおよびエージェント状態をモニタする追跡オブジェクトを使用して IP アドレスへ ping を実行します。

ステップ 3　セカンダリ インターフェイスを使用してデフォルトのスタティック ルートを設定します。このルートは、プライマリ ルートが削除された場合にだけ使用します。

プライマリ インターフェイスの設定

スタティック ルーティングのプライマリ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	プライマリまたはセカンダリ インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**description** *string*	インターフェイスに説明を追加します。
ステップ 4	**ip address** *ip-address mask* [**secondary**]	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

DHCP のプライマリ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	プライマリまたはセカンダリ インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**description** *string*	インターフェイスに説明を追加します。
ステップ 4	**ip dhcp client route track** *number*	DHCP クライアントを設定し、追加されたルートを指定の追跡番号に関連付けます。有効な数値は 1 ～ 500 です。
ステップ 5	**ip address dhcp**	DHCP からイーサネット インターフェイスの IP アドレスを取得します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

Cisco IP SLA モニタリング エージェントおよび追跡オブジェクトの設定

Cisco IP SLA でネットワーク モニタリングを設定するには、特権 EXEC モードで次の手順を実行します。

ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	Cisco IP SLA 動作を設定し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	**icmp-echo** {*destination-ip-address* | *destination hostname* [**source- ipaddr** {*ip-address* | *hostname* **source-interface** *interface-id*]	Cisco IP SLA エンドツーエンド ICMP エコー応答時間動作を設定し、IP SLA ICMP エコー コンフィギュレーション モードを開始します。
ステップ 4	**timeout** *milliseconds*	要求パケットの応答に対する動作の待機時間を設定します。
ステップ 5	**frequency** *seconds*	動作がネットワークに送信される頻度を設定します。
ステップ 6	**threshold** *milliseconds*	反応イベントを生成し、その動作の履歴情報を保存する上限スレッシュホールド（ヒステリシス）を設定します。
ステップ 7	**exit**	IP SLA ICMP エコー コンフィギュレーション モードを終了します。

ステップ 8	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] **start-time** *time* | **pending** | **now** | **after** *time*] [**ageout** *seconds*] [**recurring**]	1 つの IP SLA 動作のスケジューリング パラメータを設定します。
ステップ 9	**track** *object-number* **rtr** *operation-number* {**state** | **reachability**}	Cisco IOS IP SLA 動作の状態を追跡し、追跡コンフィギュレーション モードを開始します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show track** *object-number*	追跡情報を表示し、設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルーティング ポリシーおよびデフォルト ルートの設定

オブジェクト追跡を使用してバックアップ スタティック ルーティングのルーティング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。手順内のコマンドの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number*	拡張 IP アクセス リストを定義します。オプションの特性を設定します。
ステップ 3	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]	ルート マップ コンフィギュレーション モードを開始し、特定のルーティング プロトコルから別のルーティング プロトコルへのルートの再配信の条件を定義します。
ステップ 4	**match ip address** {*access-list number* | *access-list name*}	標準または拡張アクセス リストに許可された宛先ネットワーク番号アドレスを持つルートを配信し、パケットのポリシー ルーティングを実行します。複数の番号または名前を入力できます。
ステップ 5	**set ip next-hop dynamic dhcp**	DHCP ネットワーク専用。DHCP クライアントが学習した最新のゲートウェイへのネクストホップを設定します。
ステップ 6	**set interface** *interface-id*	スタティック ルーティング ネットワーク専用。ポリシー ルーティングのルート マップの match コマンドをパスした出力パケットの送信場所を指定します。
ステップ 7	**exit**	ルート マップ コンフィギュレーション モードを終了します。
ステップ 8	**ip local policy route-map** *map-tag*	ルート マップを特定し、ローカル ポリシー ルーティングに使用します。
ステップ 9	**ip route** *prefix mask* {*ip-address* | *interface-id* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *track-number*] [*tag tag*]	スタティック ルーティング ネットワーク専用。スタティック ルートを確立します。 **track** *track-number* を入力すると、設定の追跡オブジェクトがアップした場合に限り、スタティック ルートがインストールされるようになります。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip route track table**	IP ルート追跡テーブルに関する情報を表示します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

設定例については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

拡張オブジェクト追跡のモニタ

表 47-1 に示す特権 EXEC コマンドまたはユーザ EXEC コマンドを使用して、拡張オブジェクトの追跡情報を表示します。

表 47-1　追跡情報を表示するためのコマンド

コマンド	目的
show ip route track table	IP ルート追跡テーブルに関する情報を表示します。
show track [*object-number*]	すべての追跡リストまたは指定リストの情報を表示します。
show track brief	追跡情報出力を 1 行表示します。
show track interface [**brief**]	追跡されたインターフェイス オブジェクトの情報を表示します。
show track ip [*object-number*] [**brief**] **route**	追跡された IP ルート オブジェクトの情報を表示します。
show track resolution	追跡されたパラメータの解析を表示します。
show track timers	追跡されたポーリング インターバル タイマーを表示します。

CHAPTER 48

WCCP によるキャッシュ サービスの設定

この章では、Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）を使用して、トラフィックを広域アプリケーション エンジン（Cisco Cache Engine 550 など）にリダイレクトするように IE 3000 スイッチを設定する方法について説明します。このソフトウェア リリースでは、WCCP バージョン 2（WCCPv2）だけをサポートします。

WCCP はシスコが開発したコンテンツ ルーティング技術です。WCCP を使用すると広域アプリケーション エンジン（以降、*アプリケーション エンジン*と呼ぶ）をネットワーク インフラストラクチャに統合できます。アプリケーション エンジンは、頻繁にアクセスされるコンテンツをトランスペアレントに格納して、同じコンテンツに対する連続する要求に応えます。これによりサーバは同じコンテンツを繰り返し送信する必要がなくなります。アプリケーション エンジンを使用することでコンテンツの配信が高速化され、コンテンツのスケーラビリティとアベイラビリティが最大限に確保されます。サービス プロバイダー ネットワークでは、WCCP とアプリケーション エンジンによるソリューションを Point of Presence（POP）に展開できます。企業ネットワークでは、WCCP とアプリケーション エンジンによるソリューションを地方のサイトや小規模の支店に展開できます。

この機能を使用するには、スイッチが IP サービス イメージを実行している必要があります。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* 』の「*System Management Commands*」の「WCCP Router Configuration Commands」を参照してください。このマニュアルには、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセス可能です。

この章で説明する内容は、次のとおりです。

WCCP の概要

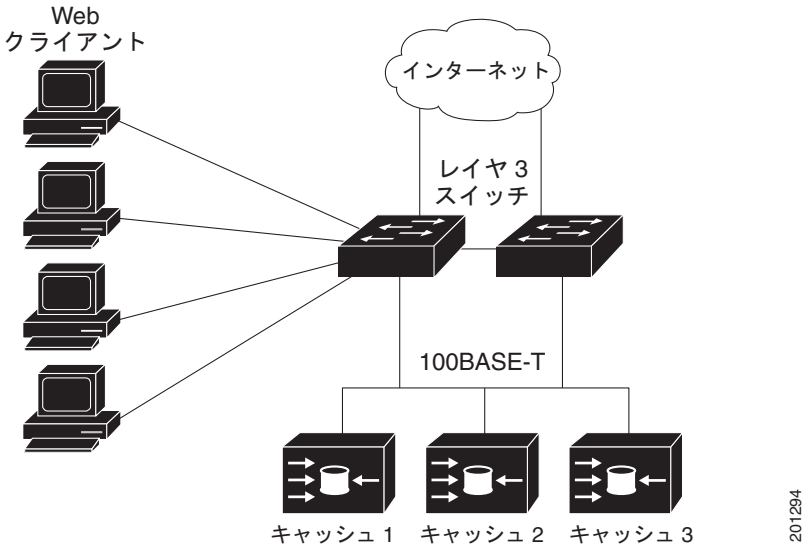
WCCP および Cisco Cache Engine（または WCCP が稼動する他のアプリケーション エンジン）は、ネットワークのトラフィック パターンをローカライズすることにより、コンテンツ要求にローカルで対応できます。

WCCP によって、WCCP をサポートする Cisco ルータおよびスイッチは、コンテンツ要求をトランスペアレントにリダイレクトできます。リダイレトはトランスペアレントに行われるので、ブラウザを設定して Web プロキシを使用する必要がありません。代わりに、ターゲット URL を使用してコンテンツを要求すると、要求が自動的にアプリケーション エンジンにリダイレクトされます。「*トランスペアレント*」という用語は、要求対象のファイル（Web ページなど）が初めに指定したサーバからではなく、アプリケーション エンジンから送られてきたことがエンド ユーザにはわからないことを指します。

アプリケーション エンジンは要求を受け取ると、専用のローカル キャッシュから対応しようとします。要求された情報が存在しない場合、アプリケーション エンジンは要求を独自にエンド サーバに送信して要求された情報を取得します。要求された情報を受信すると要求元のクライアントに転送し、その後の同じ要求に応えられるようにキャッシュにも格納します。

アプリケーション エンジン クラスタ（アプリケーション エンジンの集合）は、WCCP を使用することで複数のルータやスイッチの要求を処理できます（図 48-1 を参照）。

図 48-1　Cisco Cache Engine と WCCP ネットワークの設定



WCCP メッセージ交換

WCCP メッセージ交換の一連のイベントは、次のとおりです。

1. アプリケーション エンジンは、WCCP を使用して WCCP 対応スイッチに自己の IP アドレスを送信するとともに、*Here I am* メッセージで存在を伝えます。スイッチとアプリケーション エンジンは、UDP ポート 2048 に基づく制御チャネルを介して相互に通信します。
2. WCCP 対応スイッチは、アプリケーション エンジンの IP 情報を使用して、クラスタ ビュー（クラスタ内のアプリケーション エンジンの一覧）を作成します。このビューは *I see you* メッセージでクラスタ内の各アプリケーション エンジンに送信され、基本的にすべてのアプリケーション エンジンが相互の存在を認識できるようになります。クラスタのメンバーシップが一定時間変わらないと、安定したビューが確立されます。
3. 安定したビューが確立されると、クラスタ内で最も低い IP アドレスを持つアプリケーション エンジンが代表アプリケーション エンジンに選出されます。

WCCP ネゴシエーション

代表アプリケーション エンジンと WCCP 対応スイッチは、WCCP プロトコル メッセージを交換して次の項目のネゴシエートします。

- 転送方式（スイッチがアプリケーション エンジンにパケットを転送する方法）。スイッチは、パケットの宛先 MAC アドレスをターゲット アプリケーション エンジンの MAC アドレスに置き換えることで、レイヤ 2 ヘッダーを書き換えます。次に、そのパケットをアプリケーション エンジンに転送します。この転送方式を行うには、ターゲット アプリケーション エンジンとスイッチがレイヤ 2 で直接接続されている必要があります。
- 割り当て方式（クラスタ内のアプリケーション エンジン間にパケットを配信する方法）。スイッチは、宛先 IP アドレス、送信元 IP アドレス、宛先レイヤ 4 ポート、および送信元レイヤ 4 ポートの一部のビットを使用して、リダイレクトされたパケットを受信するアプリケーション エンジンを決定します。
- パケットリターン方式（パケットをアプリケーション エンジンからスイッチに戻して通常転送を行う方法）。アプリケーション エンジンがパケットを拒否してパケットリターン機能を実行する一般的な理由は、次のとおりです。
  - アプリケーション エンジンが過負荷状態で、パケットに対応する余裕がない場合。
  - アプリケーション エンジンがサーバからエラー メッセージ（プロトコル エラーや認証エラーなど）を受け取り、ダイナミック クライアント バイパス機能を使用している。この機能により、クライアントはアプリケーション エンジンを経由しないでサーバに直接接続することができます。

  アプリケーション エンジンはパケットを WCCP 対応スイッチに戻し、アプリケーション エンジンが存在しないかのようにサーバに転送します。アプリケーション エンジンは、再接続試行を代行受信しません。これにより、アプリケーション エンジンはアプリケーション エンジンへのパケットのリダイレクトを実質的に取り消し、バイパス フローを作成します。このリターン方法が Generic Route Encapsulation（GRE; 総称ルーティング カプセル化）の場合、スイッチはアプリケーション エンジンに設定されている GRE トンネルを介して戻されたパケットを受信します。スイッチの CPU は Cisco Express Forwarding（CEF）を使用して、これらのパケットをターゲット サーバに送信します。戻し方式がレイヤ 2 書き換えである場合、パケットはハードウェア内でターゲット サーバに転送されます。情報がサーバから返されると、スイッチは通常のレイヤ 3 転送を使用して要求元のクライアントに情報を戻します。

MD5 セキュリティ

WCCP の各プロトコル メッセージにはセキュリティ コンポーネントがオプションとして用意されているので、スイッチはアプリケーション エンジンとのメッセージ交換に MD5 認証を使用できます。MD5 で認証されないメッセージ（スイッチの認証機能がイネーブルの場合）は、スイッチにより廃棄されます。パスワード ストリングは MD5 値と組み合わされ、スイッチとアプリケーション エンジンとの接続にセキュリティが確保されます。各アプリケーション エンジンには、同じパスワードを設定する必要があります。

パケット リダイレクションおよびサービス グループ

WCCP を設定することで、トラフィックを FTP、プロキシ Web キャッシュ処理、オーディオおよびビデオ アプリケーションなどに分類してリダイレクトすることができます。この分類は、*サービス グループ*と呼ばれ、プロトコル タイプ（TCP または UDP）およびレイヤ 4 の送信元/宛先ポート番号に基づいて行われます。サービス グループは、Web キャッシュ（TCP ポート 80）などの well-known 名、またはサービス番号（0 ～ 99）で識別されます。サービス グループは、プロトコルとレイヤ 4 ポート番号にマッピングされ、個別に確立され管理されます。WCCP ではダイナミック サービス グループを使用できます。このグループでは参加するアプリケーション エンジンによって分類基準がダイナミックに提供されます。

スイッチまたはスイッチ スタック上には、最大 8 つのサービス グループと、サービス グループあたり最大 32 のキャッシュ エンジンを設定できます。WCCP は、グループ定義内にサービス グループのプライオリティを管理しています。プライオリティは、スイッチ ハードウェア内のサービス グループの設定に使用されます。たとえば、プライオリティ 100 のサービス グループ 1 が宛先ポート 80 を待ち受け、プライオリティ 50 のサービス グループ 2 が送信元ポート 80 を待ち受けている場合、送信元および宛先ポート 80 の着信パケットは、プライオリティの高いサービス グループ 1 を使用して転送されます。

WCCP は、サービス グループごとにアプリケーション エンジンのクラスタをサポートします。リダイレクトするトラフィックを、クラスタ内の任意のアプリケーション エンジンに送信できます。スイッチは、サービス グループのクラスタ内のアプリケーション エンジン間でトラフィックのロード バランシングを行うマスク割り当て方式をサポートしています。

スイッチに WCCP が設定されると、スイッチはクライアントから受信したすべてのサービス グループのパケットを、アプリケーション エンジンに転送します。ただし、次のパケットはリダイレクトされません。

- アプリケーション エンジンから発信されて、サーバを宛先とするパケット。
- アプリケーション エンジンから発信されて、クライアントを宛先とするパケット。
- アプリケーション エンジンによって戻されたか、拒否されたパケット。これらのパケットは、サーバに送信されます。

プロトコル メッセージの送受信用に、サービス グループあたり 1 つのマルチキャスト アドレスを設定できます。マルチキャスト アドレスが 1 つ設定されていると、アプリケーション エンジンは 1 つのアドレス（例：225.0.0.0）宛に通知を送信します。このアドレスは、サービス グループ内のすべてのルータを受信対象に含みます。1 つのマルチキャスト アドレスを使用すると、ルータをダイナミックに追加したり取り外したりする場合に、WCCP ネットワーク内のすべての装置のアドレスを個別に入力する手間が省けるので設定が容易になります。

アプリケーション エンジンから受信したプロトコル パケットの検証には、ルータ グループ リストを使用できます。グループ リスト内のアドレスに一致するパケットが処理され、一致しないパケットは廃棄されます。

特定のクライアント、サーバ、またはクライアント/サーバ ペアに対してキャッシングをディセーブルにするには、WCCP リダイレクト Access Control List（ACL; アクセス制御リスト）を使用します。リダイレクト ACL に一致しないパケットは、キャッシュをバイパスし正常に転送されます。

WCCP パケットをリダイレクトする前に、スイッチはインターフェイス上に設定されているすべての着信機能と関連付けられた ACL を検証し、パケットが ACL 内のエントリとどのように一致するかに基づいて、パケットの転送を許可または拒否します。

（注） WCCP リダイレクト リストでは、**permit**（許可）ACL エントリだけがサポートされます。

パケットがリダイレクトされる場合は、リダイレクトされるインターフェイスに関連付けられた出力 ACL がパケットに適用されます。元のポートに関連付けられた ACL は、リダイレクトされるインターフェイスに必要な出力 ACL を具体的に設定しない限り、適用されません。

サポートされない WCCP 機能

次の WCCP 機能は、このソフトウェア リリースではサポートされません。

- **ip wccp redirect out** インターフェイス コンフィギュレーション コマンドを使用して設定する、アウトバウンド インターフェイスでのパケット リダイレクション。このコマンドはサポートされません。
- パケット リダイレクションに GRE 転送方式は使用できません。
- ロード バランシングにハッシュ割り当て方式は使用できません。
- WCCP で SNMP はサポートされません。

WCCP の設定

ここでは、スイッチに WCCP を設定する手順について説明します。

- 「WCCP のデフォルト設定」（P.48-5）
- 「WCCP 設定時の注意事項」（P.48-5）
- 「キャッシュ サービスのイネーブル化」（P.48-6）（必須）

WCCP のデフォルト設定

表 48-1 に、WCCP のデフォルト設定を示します。

表 48-1　WCCP のデフォルト設定

機能	デフォルト設定
WCCP イネーブル ステート	WCCP サービスはディセーブル
プロトコル バージョン	WCCPv2
インターフェイスで受信したトラフィックのリダイレクト	ディセーブル

WCCP 設定時の注意事項

スイッチに WCCP を設定する前に、次に示す設定時の注意事項に従ってください。

- 同じサービス グループ内のアプリケーション エンジンとスイッチは、WCCP をイネーブルにしたスイッチに直接接続される同じサブネットワーク内にある必要があります。
- クライアント、アプリケーション エンジン、およびサーバに接続されるスイッチ インターフェイスは、レイヤ 3 インターフェイス（ルーテッド ポートおよび Switch Virtual Interface（SVI; スイッチ仮想インターフェイス））として設定します。WCCP パケット リダイレクションが動作するには、サーバ、アプリケーション エンジン、およびクライアントは異なるサブネット上にある必要があります。
- 各アプリケーション エンジンに単一のマルチキャスト アドレスを設定する場合は、予約されていないマルチキャスト アドレスだけを使用してください。
- WCCP エントリと Policy-Based Routing（PBR; ポリシーベース ルーティング）エントリは、同じ TCAM 領域を使用します。WCCP は、PBR をサポートするアクセス テンプレート、ルーティング テンプレート、およびデュアル IPv4/IPv6 ルーティング テンプレートでだけサポートされます。

- WCCP エントリを追加する際に TCAM エントリが使用できない場合、パケットはリダイレクトされずに標準のルーティング テーブルを使用して転送されます。
- WCCP 入力リダイレクションをイネーブルにしたインターフェイスの数が増えると、使用可能な PBR ラベルの数は減ります。ラベルは、サービス グループをサポートするインターフェイスごとに 1 つ消費されます。WCCP ラベルは PBR ラベルから取得されます。PBR と WCCP の間で使用可能なラベルをモニタし、管理するようにしてください。ラベルが使用できないと、スイッチはサービス グループを追加できません。ただし、同じ順番のサービス グループを持つインターフェイスが別にある場合は、新しいラベルがなくてもインターフェイスにグループを追加できます。
- スタック メンバー スイッチに設定するルーティング Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズは、クライアントの MTU サイズより大きい必要があります。アプリケーション エンジンに接続されるポートに設定する MAC レイヤの MTU サイズには、GRE トンネル ヘッダーのバイト数を含める必要があります。
- WCCP と VPN Routing/Forwarding（VRF; VPN ルーティング/転送）は、同じスイッチ インターフェイスに設定できません。
- WCCP と PBR は、同じスイッチ インターフェイスに設定できません。
- WCCP と Private VLAN（PVLAN）は、同じスイッチ インターフェイスに設定できません。

キャッシュ サービスのイネーブル化

WCCP パケット リダイレクションが動作するには、クライアントに接続されたスイッチ インターフェイスが、インバウンド パケットをリダイレクトするように設定されている必要があります。

次に、ルーテッド ポートにこれらの機能を設定する手順を示します。これらの機能を SVI に設定する場合は、この手順のあとの設定例を参照してください。

（注）　WCCP コマンドを設定する前に、SDM テンプレートを設定し、スイッチを再起動します。詳細については、第 10 章「SDM テンプレートの設定」を参照してください。

キャッシュ サービスをイネーブルにしたり、マルチキャスト グループ アドレスまたはグループ リストを設定したり、ルーテッド インターフェイスを設定したり、クライアントから受信した着信パケットをアプリケーション エンジンにリダイレクトしたり、マルチキャスト アドレスを受信するようにインターフェイスをイネーブルにしたり、パスワードを設定したりするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip wccp** {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]	キャッシュ サービスをイネーブルにし、アプリケーション エンジンで定義されているダイナミック サービスに対応するサービス番号を指定します。デフォルトでは、この機能はディセーブルです。 （任意）**group-address** *groupaddress* には、サービス グループに参加するスイッチおよびアプリケーション エンジンが使用するマルチキャスト グループ アドレスを指定します。 （任意）マルチキャスト グループ アドレスを使用しない場合、**group-list** *access-list* には、サービス グループに参加するアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。 （任意）**redirect-list** *access-list* には、特定のホストまたはホストからの特定のパケットに対するリダイレクト サービスを指定します。 （任意）**password** *encryption-number password* には、暗号化番号を指定します。指定できる範囲は 0 ～ 7 です。暗号化しない場合は 0 を、独自の暗号化方式の場合は 7 を使用します。パスワード名には最大 7 文字を指定します。スイッチは、パスワードと MD5 認証値を組み合わせて、スイッチとアプリケーション エンジンとの接続にセキュリティを確保します。デフォルトではパスワードは設定されません。認証も行われません。 各アプリケーション エンジンには、同じパスワードを設定する必要があります。 認証をイネーブルにした場合、認証されなかったメッセージは廃棄されます。
ステップ 3	**interface** *interface-id*	アプリケーション エンジンまたはサーバに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport**	レイヤ 3 モードを開始します。
ステップ 5	**ip address** *ip-address subnet-mask*	IP アドレスおよびサブネット マスクを設定します。
ステップ 6	**no shutdown**	インターフェイスをイネーブルにします。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。アプリケーション エンジンおよびサーバごとに、ステップ 3 ～ 7 を繰り返します。
ステップ 8	**interface** *interface-id*	クライアントに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**no switchport**	レイヤ 3 モードを開始します。
ステップ 10	**ip address** *ip-address subnet-mask*	IP アドレスおよびサブネット マスクを設定します。
ステップ 11	**no shutdown**	インターフェイスをイネーブルにします。
ステップ 12	**ip wccp** {**web-cache** | *service-number*} **redirect in**	クライアントから受信したパケットを、アプリケーション エンジンにリダイレクトします。クライアントに接続するインターフェイスで、これをイネーブルにします。

	コマンド	目的
ステップ 13	**ip wccp** {**web-cache** | *service-number*} **group-listen**	（任意）マルチキャスト グループ アドレスを使用する場合、**group-listen** によりインターフェイスでマルチキャスト アドレスの待ち受けが可能になります。アプリケーション エンジンに接続するインターフェイスで、これをイネーブルにします。
ステップ 14	**exit**	グローバル コンフィギュレーション モードに戻ります。各クライアントで、ステップ 8 ～ 13 を繰り返します。
ステップ 15	**end**	特権 EXEC モードに戻ります。
ステップ 16	**show ip wccp web-cache** および **show running-config**	設定を確認します。
ステップ 17	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

キャッシュ サービスをディセーブルにするには、**no ip wccp web-cache** グローバル コンフィギュレーション コマンドを使用します。インバウンド パケット リダイレクションをディセーブルにするには、**no ip wccp web-cache redirect in** インターフェイス コンフィギュレーション コマンドを使用します。この手順が完了したら、ネットワークのアプリケーション エンジンを設定します。

次に、ルーテッド インターフェイスを設定し、マルチキャスト グループ アドレスとリダイレクト アクセス リストでキャッシュ サービスをイネーブルにする例を示します。ギガビット イーサネットのポート 1 をアプリケーション エンジンに接続し、IP アドレス 172.20.10.30 のルーテッド ポートとして設定してから、再度イネーブルにします。ギガビット イーサネットのポート 2 をインターネット経由でサーバに接続し、IP アドレス 175.20.20.10 のルーテッド ポートとして設定してから、再度イネーブルにします。ギガビット イーサネットのポート 3 ～ 6 をクライアントに接続し、IP アドレス 175.20.30.20、175.20.40.30、175.20.50.40、および 175.20.60.50 のルーテッド ポートとして設定します。スイッチはマルチキャスト トラフィックを待ち受け、クライアント インターフェイスから受信したパケットをアプリケーション エンジンにリダイレクトします。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache 80 group-address 224.1.1.100 redirect list 12
Switch(config)# access-list 12 permit host 10.1.1.1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.10.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache group-listen
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.40.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/5
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip address 175.20.50.40 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/6
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.60.50 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
```

次に、SVI を設定し、マルチキャスト グループ リストを使用してキャッシュ サービスをイネーブルにする例を示します。VLAN 299 を作成し、IP アドレス 175.20.20.10 に設定します。ギガビット イーサネットのポート 1 をインターネット経由でサーバに接続し、VLAN 299 のアクセス ポートとして設定します。VLAN 300 を作成し、IP アドレス 172.20.10.30 に設定します。ギガビット イーサネットのポート 2 をアプリケーション エンジンに接続し、VLAN 300 のアクセス ポートとして設定します。VLAN 301 を作成し、IP アドレス 175.20.30.50 に設定します。ファスト イーサネットのポート 3 ～ 6 をクライアントに接続し、VLAN 301 のアクセス ポートとして設定します。スイッチはクライアント インターフェイスから受信したパケットをアプリケーション エンジンにリダイレクトします。

（注） リダイレクト リストでは、**permit**（許可）ACL エントリだけが使用されています。**deny**（拒否）エントリはサポートされません。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache 80 group-list 15
Switch(config)# access-list 15 permit host 171.69.198.102
Switch(config)# access-list 15 permit host 171.69.198.104
Switch(config)# access-list 15 permit host 171.69.198.106
Switch(config)# vlan 299
Switch(config-vlan)# exit
Switch(config)# interface vlan 299
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 299
Switch(config)# vlan 300
Switch(config-vlan)# exit
Switch(config)# interface vlan 300
Switch(config-if)# ip address 171.69.198.100 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 300
Switch(config-if)# exit
Switch(config)# vlan 301
Switch(config-vlan)# exit
Switch(config)# interface vlan 301
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/3 - 6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 301
Switch(config-if-range)# exit
```

WCCP のモニタおよびメンテナンス

WCCP をモニタおよびメンテナンスするには、表 48-2 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 48-2　WCCP のモニタおよびメンテナンスのためのコマンド

コマンド	目的
clear ip wccp web-cache	Web キャッシュ サービスの統計情報を削除します。
show ip wccp web-cache	WCCP に関連するグローバルな情報を表示します。
show ip wccp web-cache detail	スイッチおよび WCCP クラスタ内のすべてのアプリケーション エンジンの情報を表示します。
show ip interface	インターフェイスに設定されたすべての IP WCCP リダイレクション コマンドのステータスを表示します（`Web Cache Redirect is enabled / disabled` のように表示）。
show ip wccp web-cache view	他の検出されたメンバーまたは検出されなかったメンバーを表示します。

CHAPTER 49

IP マルチキャスト ルーティングの設定

この章では、IE 3000 スイッチに IP マルチキャスト ルーティングを設定する方法について説明します。IP マルチキャスティングは、ネットワーク リソースをより効率的に使用する方法です。特にオーディオやビデオなどの帯域幅を集中的に使用するサービスに対して効果があります。IP マルチキャスト ルーティングにより、ホスト（送信元）は、IP *マルチキャスト グループ アドレス*と呼ばれる IP アドレスの特殊な形式を使用して、IP ネットワーク内の任意の場所にあるホストのグループ（レシーバー）へのパケットの送信をイネーブルにします。送信ホストは、マルチキャスト グループ アドレスをそのパケットの IP 宛先アドレス フィールドに挿入し、IP マルチキャスト ルータおよびマルチレイヤ スイッチは、マルチキャスト グループのメンバーに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。ホストがグループのメンバーであるかどうかにかかわらず、すべてのホストをグループへ送信できます。ただし、そのメッセージを受信できるのはグループのメンバーだけです。

IP マルチキャスト ルーティング機能を使用するには、スイッチが IP サービス イメージを実行している必要があります。

（注） この章で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』を参照してください。

この章で説明する内容は、次のとおりです。

Multicast Source Discovery Protocol（MSDP）を設定する方法の詳細については、第 50 章「MSDP の設定」を参照してください。

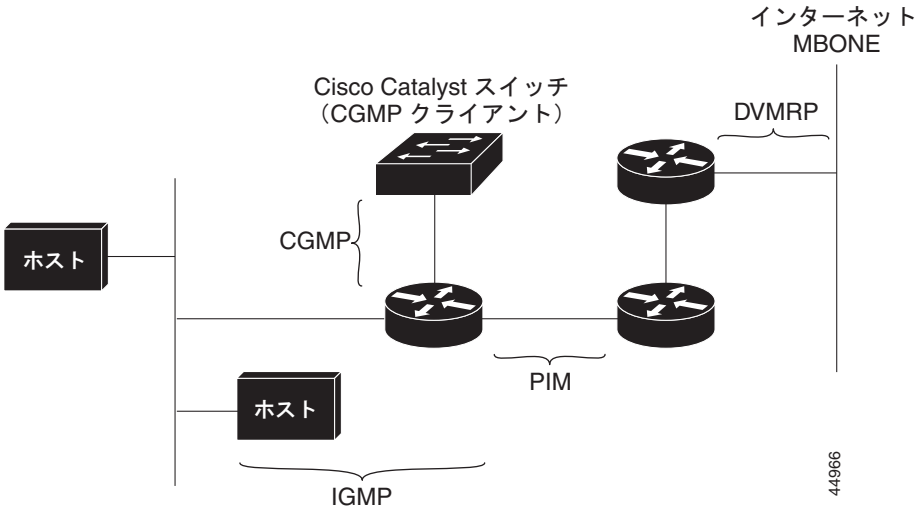
シスコの IP マルチキャスト ルーティング実装の概要

Cisco IOS ソフトウェアは、IP マルチキャスト ルーティングを実装するために次のプロトコルをサポートしています。

- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）は、LAN 上のホストとその LAN 上のルータ（およびマルチレイヤ スイッチ）間で使用され、ホストがメンバーとして属するマルチキャスト グループを追跡します。
- Protocol-Independent Multicast（PIM）プロトコルは、ルータとマルチレイヤ スイッチ間で使用され、相互に転送されるマルチキャスト パケット、および直接接続された LAN に転送されるマルチキャスト パケットを追跡します。
- Distance Vector Multicast Routing Protocol（DVMRP）は、インターネットのマルチキャスト バックボーン（MBONE）で使用されます。PIM と DVMRP の連携がサポートされています。
- Cisco Group Management Protocol（CGMP）は、レイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用され、IGMP で実行される作業と同様の作業を実行します。

図 49-1 に、これらのプロトコルが IP マルチキャスト環境内で動作する場所を示します。

図 49-1　　IP マルチキャスト ルーティング プロトコル



IPv4 マルチキャスト標準に従い、MAC 宛先マルチキャスト アドレスは 0100:5e で始まり、IP アドレスの末尾の 23 ビットが追加されます。Catalyst 3560 スイッチでは、スイッチのマルチキャスト アドレスに一致しないマルチキャスト パケットは、次のように処理されます。

- マルチキャスト IP アドレスおよびユニキャスト MAC アドレスを含むパケットである場合は、ソフトウェアで転送されます。これは、レガシー装置上の一部のプロトコルがマルチキャスト IP アドレスとユニキャスト MAC アドレスを併用するために発生することがあります。
- マルチキャスト IP アドレスおよび一致しない MAC アドレスを含むパケットである場合は、廃棄されます。

ここでは、次の内容について説明します。

- 「IGMP の概要」（P.49-3）
- 「PIM の概要」（P.49-4）
- 「DVMRP の概要」（P.49-9）
- 「CGMP の概要」（P.49-10）

IGMP の概要

IP マルチキャスティングに参加するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ スイッチで IGMP が動作している必要があります。このプロトコルは、クエリアおよびホストの役割を定義します。

- クエリアは、指定されたマルチキャスト グループのメンバーであるネットワーク装置を検出するためのクエリー メッセージを送信するネットワーク装置です。
- ホストは、クエリアにホスト メンバーシップを通知するためのレポート メッセージ（クエリー メッセージに応答するメッセージ）を送信するレシーバーです。

同じ送信元からマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは、IGMP メッセージを使用して、マルチキャスト グループに加入したりそこから脱退したりします。

ホストがグループのメンバーであるかどうかにかかわらず、すべてのホストをグループへ送信できます。ただし、そのメッセージを受信できるのはグループのメンバーだけです。マルチキャスト グループのメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャスト グループの場所またはメンバー数に制限はありません。ホストは一度に複数のマルチキャストのメンバーになることができます。マルチキャスト グループのアクティブ状態および所属メンバーは、グループや時間によって異なります。マルチキャスト グループは、長時間、またはごく短時間アクティブにすることもできます。グループのメンバーシップはいつでも変更可能です。メンバーを含むグループにアクティビティがない場合もあります。

IP マルチキャスト トラフィックは、グループ アドレス（クラス D アドレス）を使用します。クラス D アドレスの上位ビットは 1110 です。したがって、ホスト グループ アドレスは 224.0.0.0 ～ 239.255.255.255 の範囲になります。224.0.0.0 ～ 224.0.0.255 の範囲にあるマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは、次の IP マルチキャスト グループ アドレスを使用して送信されます。

- IGMP の一般的なクエリーは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、スイッチのクエリー対象となるグループ IP アドレスを宛先とします。
- IGMP グループ メンバーシップ レポートは、スイッチのレポート対象となるグループ IP アドレスを宛先とします。
- IGMP バージョン 2（IGMPv2）Leave メッセージは、アドレス 224.0.0.2（サブネット上のすべてのマルチキャスト ルータ）を宛先とします。古いホスト IP スタックでは、Leave メッセージの宛先がすべてのルータのアドレスでなく、グループ IP アドレスである場合があります。

IGMP バージョン 1

IGMP バージョン 1（IGMPv 1）では主にクエリー応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤ スイッチは、ローカル サブネット上のどのマルチキャスト グループがアクティブであるか（マルチキャスト グループに関係するホストが 1 つまたは複数存在するか）を判別できます。IGMPv1 では、別のプロセスを使用して、ホストをマルチキャスト グループに加入したりそこから脱退したりできます。詳細については、RFC 1112 を参照してください。

IGMP バージョン 2

IGMPv2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退の待ち時間を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。また、IGMPv2 では、この作業を実行する際に、マルチキャスト プロトコルに依存することなく IGMP クエリアを選定する機能がルータに追加されています。詳細については、RFC 2236 を参照してください。

PIM の概要

PIM は*プロトコル独立型*マルチキャストと呼ばれます。ユニキャスト ルーティング テーブルを読み込むために使用されるユニキャスト ルーティング プロトコルに関係なく、PIM は、マルチキャスト ルーティング テーブルを個別に維持せずに、この情報を使用してマルチキャスト転送を実行します。

PIM は、RFC 2362『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』で定義されています。PIM は次の Internet Engineering Task Force（IETF）インターネット ドラフトに定義されています。

- 『*Protocol Independent Multicast (PIM): Motivation and Architecture*』
- 『*Protocol Independent Multicast (PIM), Dense Mode Protocol Specification*』
- 『*Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*』
- 『*draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2*』
- 『*draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode*』

PIM のバージョン

PIMv2 では、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ Rendezvous Point（RP; ランデブー ポイント）を持つアクティブな RP が 1 つ存在します。この単一の RP は、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同等の処理を行います。
- Bootstrap Router（BSR; ブートストラップ ルータ）は、フォールトトレラントな自動化された RP 検出と配信メカニズムを提供します。このメカニズムにより、ルータおよびマルチレイヤ スイッチは、グループ /RP マッピングをダイナミックに学習できます。
- sparse（疎）モードおよび dense（密）モードは、インターフェイスではなく、グループに関するプロパティです。sparse（疎）モードまたは dense（密）モードのいずれか一方だけでなく、sparse-dense モードを使用することを強く推奨します。
- PIM の Join メッセージおよびプルーニング メッセージを使用すると、複数のアドレス ファミリを柔軟に符号化できます。
- 現在は以降の機能オプションを符号化するため、クエリー パケットではなく、より柔軟な hello パケット形式が使用されています。
- RP への登録メッセージが境界ルータによって送信されるか、指定ルータによって送信されるかどうかは、メッセージ自身によって指定されます。
- PIM パケットは IGMP パケット内に格納されず、スタンドアロンのパケットとして処理されます。

PIM のモード

PIM は Dense Mode（DM; dense（密）モード）、Sparse Mode（SM; sparse（疎）モード）、または sparse-dense モード（PIM SM-DM）のいずれかのモードで動作します。PIM DM-SM では、sparse（疎）グループと dense（密）グループの両方が同時に処理されます。

PIM DM

PIM DM では、送信元ベースのマルチキャスト分散ツリーが構築されます。dense（密）モードの場合、PIM DM のルータまたはマルチレイヤ スイッチは、他のすべてのルータまたはマルチレイヤ スイッチでグループ宛てのマルチキャスト パケットが転送されると想定しています。直接接続されたメンバーまたは PIM ネイバーが存在しない場合、PIM DM 装置がマルチキャスト パケットを受信すると、プルーニング メッセージが送信元に返送され、不要なマルチキャスト トラフィックが停止します。このプルーニング済みブランチ上のこのルータまたはスイッチでは、後続のマルチキャスト パケットがフラッディングしません。レシーバーを含まないブランチが分散ツリーからプルーニングされ、レシーバーを含むブランチだけが残るためです。

事前にプルーニングされたツリー内ブランチのレシーバーがマルチキャスト グループに新規に加入すると、PIM DM 装置は新しいレシーバーを検出し、接合メッセージをただちに送信元に向けて分散ツリーの上方向に送信します。アップストリームの PIM DM 装置が接合メッセージを受信すると、この装置は接合メッセージを受信したインターフェイスをただちにフォワーディング ステートにし、レシーバーへのマルチキャスト トラフィックの転送を開始します。

PIM SM

PIM SM は共有ツリーおよび Shortest-Path-Tree（SPT）を使用し、マルチキャスト トラフィックをネットワーク内のマルチキャスト レシーバーに配布します。PIM SM の場合、ルータまたはマルチレイヤ スイッチは、トラフィックに関する明示的な要求（Join メッセージ）がない限り、他のルータまたはスイッチではグループ宛てのパケットが転送されないことを想定しています。ホストが IGMP を使用してマルチキャスト グループに加入すると、直接接続された PIM SM 装置は、RP と呼ばれるルートに向けて PIM Join メッセージを送信します。この Join メッセージはルートに向かってルータを順次移動しながら、共有ツリーのブランチを作成します。

RP はマルチキャスト レシーバーを追跡します。また、送信元のファーストホップ ルータである *Designated Router*（DR; 指定ルータ）から受信した登録メッセージを使用して送信元を登録し、送信元からレシーバーへの共有ツリー パスを完成させます。共有ツリーを使用する場合、送信元は RP にトラフィックを送信することで、これらのトラフィックをすべてのレシーバーに到達させるようにする必要があります。

マルチキャスト グループ トラフィックをプルーニングする場合は、プルーニング メッセージが分散ツリーの上方向に送信されます。この結果、明示的な Join メッセージによって作成された共有ツリーまたは SPT のブランチが不要になった場合、これらを解除することが可能となります。

PIM スタブ ルーティング

PIM スタブ ルーティング機能は、ルーテッド トラフィックをエンド ユーザにより近い場所に移動することでリソース使用量を削減します。

PIM スタブ ルーティングを使用するネットワークでは、ユーザに対して許容される IP トラフィックのルートは、PIM スタブ ルーティングで設定されたスイッチを介したルートだけです。PIM 受動インターフェイスは、VLAN のようなレイヤ 2 アクセス ドメインに接続したり、その他のレイヤ 2 装置に接続されたインターフェイスに接続しています。レイヤ 2 アクセス ドメインでは、直接接続されたマルチキャスト（IGMP）レシーバーと送信元だけが許可されています。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理することはありません。

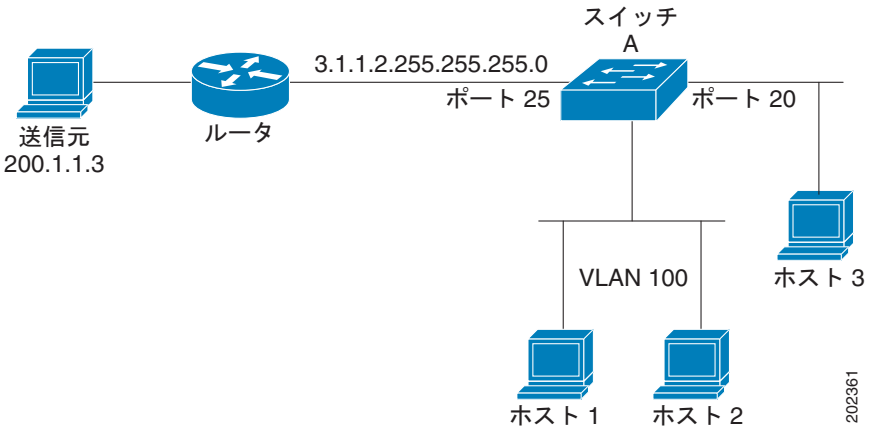
PIM スタブ ルーティングを使用する場合、ディストリビューション ルータとリモート ルータが IP マルチキャスト ルーティングを使用できるように設定し、PIM スタブ ルータとして機能するものがスイッチだけになるように設定する必要があります。スイッチは、ディストリビューション ルータ間の中継トラフィックのルーティングを行いません。また、スイッチにはルーテッド アップリンク ポートを設定する必要があります。スイッチのアップリンク ポートは Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）と併用することができません。SVI アップリンク ポートで PIM が必要な場合は、IP サービス フィーチャ セットにアップグレードする必要があります。

また、スイッチに PIM スタブ ルーティングを設定する場合は、Enhanced Interior Gateway Routing Protocol（EIGRP）スタブ ルーティングを設定する必要もあります。詳細については、「EIGRP スタブ ルーティングの設定」（P.41-41）を参照してください。

冗長 PIM スタブ ルータのトポロジはサポートされません。冗長トポロジは、マルチキャスト トラフィックを 1 つのアクセス ドメインに転送している PIM ルータが複数ある場合に存在します。PIM メッセージはブロックされ、PIM アセットと指定ルータ選定メカニズムは PIM 受動インターフェイスでサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジだけがサポートされます。非冗長トポロジを使用すると、PIM 受動インターフェイスは、非冗長トポロジをそのアクセス ドメイン上の唯一のインターフェイスおよび指定ルータであると想定します。

図 49-2 では、スイッチ A のルーテッド アップリンク ポート 25 がルータに接続し、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。このように設定することで、直接接続されているホストがマルチキャストの送信元である 200.1.1.3 からトラフィックを受信できます。詳細については、「PIM スタブ ルーティングの設定」（P.49-23）を参照してください。

図 49-2　　PIM スタブ ルータの設定



IGMP ヘルパー

PIM スタブ ルーティングは、ルーテッド トラフィックをエンド ユーザにより近い場所に移動し、ネットワーク トラフィックを削減します。また、IGMP ヘルパー機能を使用してスタブ ルータ（スイッチ）を設定することで、トラフィックを削減することもできます。

スタブ ルータ（スイッチ）を **igmp helper help-address** インターフェイス コンフィギュレーション コマンドで設定することにより、スイッチはネクストホップ インターフェイスにレポートを送信できます。これにより、ダウンストリーム ルータに直接接続されていないホストは、アップストリーム ネットワークを送信元とするマルチキャスト グループに加入できます。この機能が設定されると、マルチキャスト ストリームへの加入を待機しているホストからの IGMP パケットは、アップストリームからネクストホップ装置へ転送されます。アップストリームのセントラル ルータがヘルパー IGMP のレポートを受信した場合または脱退した場合、ルータはそのグループの発信インターフェイスのリストで、インターフェイスの追加または削除を行います。

ip igmp helper-address コマンドの構文と使用方法の詳細については、『*Cisco IOS IP and IP Routing Command Reference, Release 12.1*』を参照してください。

Auto-RP

この独自の機能により、ネットワーク内のルータまたはマルチレイヤ スイッチごとに RP 情報を手動で設定する必要がなくなります。Auto-RP を機能させるには、Cisco ルータまたはマルチレイヤ スイッチをマッピング エージェントとして設定します。マッピング エージェントは IP マルチキャストを使用して、候補 RP アナウンスを受信する候補 RP として設定可能なネットワーク内のルータまたはスイッチを取得します。候補 RP はマルチキャスト RP アナウンス メッセージを特定のグループまたはグループ範囲に定期的に送信し、それらのアベイラビリティをアナウンスします。

マッピング エージェントはこれらの候補 RP アナウンスを待ち受け、この情報を使用して、グループ/RP マッピング キャッシュにエントリを作成します。受信されたグループ/RP 範囲に対して複数の候補 RP が RP アナウンスを送信した場合でも、この範囲にはマッピング キャッシュ エントリが 1 つだけ作成されます。RP アナウンス メッセージ着信時に、マッピング エージェントは最大の IP アドレスを持つルータまたはスイッチをアクティブ RP として選択し、この RP アドレスをグループ/RP マッピング キャッシュ内に保存します。

マッピング エージェントは、グループ/RP マッピング キャッシュの内容を定期的にマルチキャストします。このため、すべてのルータおよびスイッチで、サポート対象のグループに使用される RP が自動的に検出されます。ルータまたはスイッチが RP ディスカバリ メッセージの受信に失敗し、グループ/RP マッピング情報が期限切れになると、ルータまたはスイッチは、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって定義された、スタティックに設定された RP に変更されます。スタティックに設定された RP が存在しない場合、ルータまたはスイッチはグループの動作を dense（密）モードに変更します。

複数の RP がさまざまなグループ範囲として、または相互にホット バックアップとして機能します。

ブートストラップ ルータ

PIMv2 BSR は、グループ/RP マッピング情報をネットワーク内のすべての PIM ルータおよびマルチレイヤ スイッチに配信するもう 1 つの方法です。これにより、ネットワーク内のルータまたはスイッチごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ/RP マッピング情報を配布する代わりに、特殊な BSR メッセージのホップバイホップのフラッディングを使用してマッピング情報を配布します。

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよびスイッチから選定されます。選定メカニズムは、ブリッジ接続された LAN で使用されるルートブリッジ選定メカニズムと類似しています。BSR の選定は、ネットワークを経由してホップバイホップで送信される BSR メッセージに含まれている装置の BSR プライオリティに基づいて行われます。各 BSR 装置は BSR メッセージを調べ、BSR プライオリティが自身の BSR プライオリティと同等またはそれ以上で、BSR IP アドレスが大きいメッセージだけを、すべてのインターフェイスから転送します。この方法によって、BSR が選定されます。

選定された BSR によって、Time to Live（TTL）値が 1 である BSR メッセージが送信されます。ネイバー PIMv2 ルータまたはマルチレイヤ スイッチは BSR メッセージを受信し、TTL 値が 1 である他のすべてのインターフェイス（BSR メッセージの着信インターフェイスを除く）にマルチキャストします。このように、BSR メッセージは PIM ドメイン内をホップバイホップで移動します。BSR メッセージには現在の BSR の IP アドレスが含まれているため、候補 RP はフラッディング メカニズムを使用し、どの装置が選定された BSR であるかを自動的に学習します。

候補 RP は候補 RP アドバタイズを送信し、対象となるグループ範囲を BSR に指示します。この情報は、ローカルな候補 RP キャッシュに格納されます。BSR はドメイン内の他のすべての PIM 装置に、BSR メッセージ内のこのキャッシュの内容を定期的にアドバタイズします。これらのメッセージはネットワークをホップバイホップで移動し、すべてのルータおよびスイッチに送信されます。BSR メッセージ内の RP 情報は、到達したルータおよびスイッチのローカルな RP キャッシュに格納されます。すべてのルータおよびスイッチには一般的な RP ハッシュ アルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

マルチキャスト転送およびリバース パス チェック

ユニキャスト ルーティングの場合、ルータおよびマルチレイヤ スイッチは、送信元から IP パケットの宛先アドレス フィールドに IP アドレスが表示されている宛先ホストへ、ネットワーク内の単一のパスに沿ってトラフィックを転送します。パス上の各ルータおよびスイッチは、ユニキャスト ルーティング テーブル内の宛先アドレスを参照し、指定されたインターフェイスを経由して宛先方向のネクスト ホップへパケットを転送してから、パケット内の宛先 IP アドレスを使用してユニキャスト フォワーディングを判断します。

マルチキャスティングの場合、送信元は IP パケットの宛先アドレス フィールドに表示された、マルチキャスト グループ アドレスで表されるホストの任意のグループにトラフィックを送信します。着信マルチキャスト パケットの転送または廃棄を決定するため、ルータまたはマルチレイヤ スイッチで、パケットに対する Reverse Path Forwarding（RPF）チェックを実行します（図 49-3 を参照）。

1. ルータまたはマルチレイヤ スイッチは着信したマルチキャスト パケットの送信元アドレスを調べ、リバース パス上のインターフェイスに着信したパケットを送信元に戻すかどうかを決定します。
2. パケットが送信元に逆戻りするインターフェイスに着信した場合、RPF チェックは成功し、発信インターフェイス リスト内のすべてのインターフェイス（ルータのすべてのインターフェイスとは限らない）にパケットが転送されます。
3. RPF チェックに失敗した場合、パケットは廃棄されます。

DVMRP などの一部のマルチキャスト ルーティング プロトコルでは、マルチキャスト ルーティング テーブルは個別に維持され、RPF チェックに使用されます。ただし、PIM では RPF チェックを実行するためにユニキャスト ルーティング テーブルが使用されます。

図 49-3 に、送信元 151.10.3.21 からのマルチキャスト パケットを受信するポート 2 を示します。表 49-1 に、送信元へのリバース パス上にあるポートはポート 2 ではなく、ポート 1 であることを示します。RPF チェックに失敗したため、マルチレイヤ スイッチはパケットを廃棄します。送信元 151.10.3.21 からの別のマルチキャスト パケットは、ポート 1 に受信します。ルーティング テーブルには、このポートが送信元へのリバース パス上にあることが示されています。RPF チェックに合格したため、スイッチはパケットを発信ポート リスト内のすべてのポートに転送します。

図 49-3　　RPF チェック

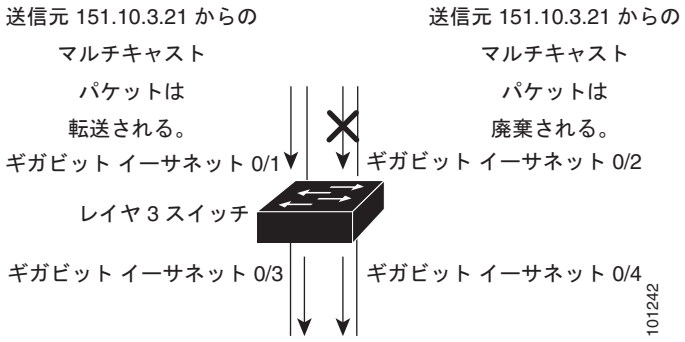


表 49-1　RPF チェックのルーティング テーブル例

ネットワーク	Port
151.10.0.0/16	ギガビット イーサネット 0/1
198.14.32.0/32	ギガビット イーサネット 0/3
204.1.16.0/24	ギガビット イーサネット 0/4

PIM は送信元ツリーと RP でルーティングされた共有ツリーの両方を使用して、データグラムを転送します（「PIM DM」（P.49-5）および「PIM SM」（P.49-5）を参照）。RPF チェックは、それぞれ異なる方法で実行されます。

- PIM ルータまたはマルチレイヤ スイッチが送信元ツリー ステートである場合（つまり（S,G）エントリがマルチキャスト ルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤ スイッチが共有ツリー ステートである場合（および明示的な送信元ツリー ステートがない場合）、（メンバーがグループに加入している場合は既知である）RP アドレスについて RPF チェックが実行されます。

PIM sparse（疎）モードは RPF 検索機能を使用し、加入およびプルーニング メッセージを送信する必要があるかどうかを決定します。

- （S,G）Join メッセージ（送信元ツリー ステート）は送信元に向けて送信されます。
- （*,G）Join メッセージ（共有ツリー ステート）は RP に向けて送信されます。

DVMRP と PIM dense（密）モードでは送信元ツリーだけが使用され、前述の RPF が使用されます。

DVMRP の概要

DVMRP は多くのベンダーの装置に実装されており、パブリック ドメインのマルチキャスト ルーティングされたプログラムに基づいて動作します。このプロトコルは MBONE、およびその他のドメイン内マルチキャスト ネットワークに導入されています。

Cisco ルータおよびマルチレイヤ スイッチでは PIM が実行されているため、DVMRP ネイバーへのマルチキャスト パケットの 転送、および DVMRP ネイバーからのマルチキャスト パケットの受信が可能です。DVMRP ルートを PIM クラウド内に伝播したり、PIM クラウドを経由して伝播することもできます。ソフトウェアは DVMRP ルートを伝播し、ルータやマルチレイヤ スイッチごとにこれらのルートのデータベースを個別に構築します。ただし、PIM はこのルーティング情報をパケット転送の判断に使用します。ソフトウェアに完全な DVMRP は実装されていません。ただし、DVMRP ルータのダイナミック検出をサポートし、従来のメディア（イーサネットや Fiber Distributed Data Interface（FDDI; ファイバ分散データ インターフェイス）など）または DVMRP 固有のトンネルを通して、これらを相互運用します。

DVMRP ネイバーは、ルートレポート メッセージの送信元ネットワーク ルーティング情報を定期的に交換することで、ルート テーブルを構築します。DVMRP ルーティング テーブルに格納されているルーティング情報は、ユニキャスト ルーティング テーブルから独立し、送信元分散ツリーの構築や、RPF を使用したマルチキャスト転送の実行に使用されます。

DVMRP は dense（密）モード プロトコルであり、抑制されたマルチキャスト モデルを使用して親子データベースを構築し、マルチキャスト パケットの送信元でルーティングされた転送ツリーを構築します。マルチキャスト パケットは、最初にこの送信元ツリーの下方向にフラッディングされます。冗長パスが送信元ツリー上にある場合、パケットはこれらのパスに沿って転送されません。これらの親子リンクでプルーニング メッセージが受信されるまで転送が行われ、これによってマルチキャスト パケットのブロードキャストが抑制されます。

CGMP の概要

このソフトウェア リリースは、スイッチで CGMP サーバ サポート機能を提供しています。クライアント側の機能は提供されません。スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれている装置用の CGMP サーバとして機能します。

CGMP は、レイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用されるプロトコルであり、IGMP で実行される作業と同様の作業を実行します。CGMP を使用すると、レイヤ 2 グループ メンバーシップ情報を CGMP サーバからスイッチに通信できます。これにより、スイッチはすべてのスイッチ インターフェイスにマルチキャスト トラフィックをフラッディングせずに、マルチキャスト メンバーが存在するインターフェイスを取得できるようになります（IGMP スヌーピングは、マルチキャスト パケットのフラッディングを抑制するもう 1 つの方法です。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください）。

CGMP が必要となるのは、レイヤ 2 スイッチで IP マルチキャスト データ パケットと IGMP レポート メッセージを区別できないためです。これらはともに MAC レベルで、同じグループ アドレスにアドレス指定されます。

CGMP は HSRPv1 と相互に排他的な関係にあります。CGMP 脱退処理と HSRPv1 を同時にイネーブルにはできません。ただし、CGMP と HSRPv2 を同時にイネーブルにすることはできます。詳細については、「HSRP バージョン」（P.45-3）を参照してください。

IP マルチキャスト ルーティングの設定

ここでは、次の設定情報について説明します。

マルチキャスト ルーティングのデフォルト設定

表 49-2 に、マルチキャスト ルーティングのデフォルト設定を示します。

表 49-2　マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM バージョン	バージョン 2

表 49-2　マルチキャスト ルーティングのデフォルト設定 （続き）

機能	デフォルト設定
PIM モード	モードは未定義
PIM スタブ ルーティング	設定なし
PIM RP アドレス	設定なし
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし
候補 BSR	ディセーブル
候補 RP	ディセーブル
Shortest-Path-Tree スレッシュホールド レート	0 KB/秒
PIM ルータクエリー メッセージ インターバル	30 秒

マルチキャスト ルーティング設定時の注意事項

スイッチ上でのマルチキャスト ルーティングの設定ミスを回避するには、ここに記載する情報を確認してください。

- 「PIMv1 および PIMv2 の相互運用性」（P.49-11）
- 「Auto-RP および BSR 設定時の注意事項」（P.49-12）

PIMv1 および PIMv2 の相互運用性

シスコの PIMv2 実装を使用すると、バージョン 1 とバージョン 2 間での相互運用性および移行が可能となりますが、若干の問題が発生する場合もあります。

PIMv2 に付加的にアップグレードできます。PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤ スイッチに設定できます。内部的には、共有メディア ネットワーク上のすべてのルータおよびマルチレイヤ スイッチで同じ PIM バージョンを実行する必要があります。したがって、PIMv2 装置が PIMv1 装置を検出した場合は、バージョン 1 装置がシャットダウンするかアップグレードされるまで、バージョン 2 装置はバージョン 1 にダウングレードされます。

PIMv2 は BSR を使用して各グループ プレフィクスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ スイッチにアナウンスします。Auto-RP 機能を組み合わせることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。ただし、Auto-RP は PIMv1 から独立したシスコ独自のスタンドアロン プロトコルです。PIMv2 は IETF 標準の追跡プロトコルです。そのため、PIMv2 の使用を推奨します。BSR メカニズムは、Cisco ルータおよびマルチレイヤ スイッチ上の Auto-RP と相互運用します。詳細については、「Auto-RP および BSR 設定時の注意事項」（P.49-12）を参照してください。

PIMv2 装置を PIMv1 装置と相互運用させる場合は、Auto-RP を事前に導入しておく必要があります。Auto-RP マッピング エージェントでもある PIMv2 BSR は、Auto-RP で選択された RP を自動的にアドバタイズします。つまり、Auto-RP によって、グループ内のルータまたはマルチレイヤごとに 1 つの RP が設定されます。ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 と PIMv2 が混在する領域内の dense（密）モード グループは、特別な設定を行わなくても自動的に相互運用します。

PIMv1 の Auto-RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に parse（疎）モード グループを設定できます。すべての PIMv2 装置で PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。PIMv2 への移行を簡単に行うための推奨事項を次に示します。

- 領域全体で Auto-RP を使用します。
- 領域全体で sparse-dense モードを設定します。

Auto-RP がまだ PIMv1 領域に設定されていない場合は、Auto-RP を設定してください。詳細については、「Auto-RP の設定」（P.49-27）を参照してください。

Auto-RP および BSR 設定時の注意事項

PIMv2 は 2 つの方法で使用できます。1 つはバージョン 2 をネットワーク内で排他的に使用する方法、もう 1 つは PIM バージョンの混在環境を導入してバージョン 2 に移行する方法です。

- 使用するネットワークがすべて Cisco ルータおよびマルチレイヤ スイッチである場合は、Auto-RP または BSR を使用します。
- ネットワークに非 Cisco ルータがある場合は、BSR を使用する必要があります。
- シスコ製 PIMv1 ルータと PIMv2 ルータ、マルチレイヤ スイッチ、および非 Cisco ルータがある場合は、Auto-RP と BSR の両方を使用する必要があります。使用するネットワークに他のベンダー製のルータが含まれる場合は、シスコ製 PIMv2 装置上に Auto-RP マッピング エージェントと BSR を設定します。BSR と他社製の PIMv2 装置間のパス上に、PIMv1 装置が配置されていないことを確認してください。
- ブートストラップ メッセージはホップバイホップで送信されるため、PIMv1 装置は、これらのメッセージがネットワーク内のすべてのルータおよびマルチレイヤ スイッチに到達することを回避します。したがって、ネットワーク内に PIMv1 装置があり、Cisco ルータおよびマルチレイヤ スイッチだけが存在する場合は、Auto-RP を使用するのが最良です。
- ネットワーク内に非 Cisco ルータがある場合は、シスコ製 PIMv2 ルータまたはマルチレイヤ スイッチに Auto-RP マッピング エージェントと BSR を設定します。BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 装置が配置されていないことを確認してください。
- シスコ製 PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、Auto-RP と BSR の両方が必要です。シスコ製 PIMv2 装置を、Auto-RP マッピング エージェントと BSR の両方に設定することを推奨します。詳細については、「Auto-RP および BSR の使用」（P.49-35）を参照してください。

基本的なマルチキャスト ルーティングの設定

IP マルチキャスト ルーティングをイネーブルにし、PIM バージョンおよび PIM モードを設定する必要があります。これにより、ソフトウェアはマルチキャスト パケットを転送し、スイッチがそのマルチキャスト ルーティング テーブルを読み込むことができます。

インターフェイスは PIM dense（密）モード、sparse（疎）モード、または sparse-dense モードのいずれかに設定できます。スイッチはモード設定に従ってマルチキャスト ルーティング テーブルを読み込み、直接接続された LAN から受信したマルチキャスト パケットを転送します。IP マルチキャスト ルーティングを実行するには、インターフェイスに対して、これらの PIM モードのいずれかをイネーブルにする必要があります。インターフェイスで PIM をイネーブルにすると、同じインターフェイス上で IGMP 動作もイネーブルになります。

（注）　複数のインターフェイスで PIM がイネーブルに設定されており、これらのインターフェイスのほとんどが発信インターフェイス リストに存在せず、IGMP スヌーピングがディセーブルになっている場合、発信インターフェイスは、余分なレプリケーションが作成されるためにマルチキャスト トラフィックのラインレートを維持できない可能性があります。

マルチキャスト ルーティング テーブルの読み込みでは、dense（密）モード インターフェイスは常にテーブルに追加されます。sparse（疎）モード インターフェイスがテーブルに追加されるのは、ダウンストリーム装置から定期的な Join メッセージを受信した場合、またはインターフェイスに直接接続されたメンバーが存在する場合だけです。LAN から転送する場合、グループが認識している RP があれば、sparse（疎）モード動作が行われます。その場合、パケットはカプセル化され、RP に送信されます。認識している RP がなければ、パケットは dense（密）モード方式でフラッディングされます。特定の送信元からのマルチキャスト トラフィックが十分である場合、レシーバーのファーストホップ ルータから送信元に向けて Join メッセージが送信され、送信元ベースの分散ツリーが構築されます。

デフォルトでは、マルチキャスト ルーティングはディセーブルになっており、モードは設定されていません。この手順は必須です。

IP マルチキャスティングをイネーブルにし、PIM バージョンおよび PIM モードを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip multicast-routing distributed**	IP マルチキャスト分散スイッチングをイネーブルにします。
ステップ 3	**interface** *interface-id*	マルチキャスト ルーティングをイネーブルにするレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。詳細については、「レイヤ 3 インターフェイスの設定」（P.14-21）を参照してください。
ステップ 4	**ip pim version** [**1** | **2**]	インターフェイスに PIM バージョンを設定します。 デフォルトでは、バージョン 2 はイネーブルになっています（推奨設定）。 PIMv2 モードのインターフェイスに PIMv1 ネイバーがある場合、インターフェイスは自動的に PIMv1 モードにダウングレードされます。バージョン 1 のすべてのネイバーがシャットダウンするかアップグレードされると、インターフェイスはバージョン 2 モードに戻ります。 詳細については、「PIMv1 および PIMv2 の相互運用性」（P.49-11）を参照してください。

	コマンド	目的
ステップ 5	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}	インターフェイスで PIM モードをイネーブルにします。 デフォルトでは、モードは設定されていません。 キーワードの意味は次のとおりです。 • **dense-mode**：動作の dense（密）モードをイネーブルにします。 • **sparse-mode**：動作の sparse（疎）モードをイネーブルにします。sparse（疎）モードを設定する場合は、RP を設定する必要もあります。詳細については、「ランデブー ポイントの設定」（P.49-25）を参照してください。 • **sparse-dense-mode**：グループが属するモードでインターフェイスが処理されます。sparse-dense モード設定を推奨します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

マルチキャスティングをディセーブルにするには、**no ip multicast-routing distributed** グローバル コンフィギュレーション コマンドを使用します。デフォルトの PIM バージョンに戻すには、**no ip pim version** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで PIM をディセーブルにするには、**no ip pim** インターフェイス コンフィギュレーション コマンドを使用します。

Source-Specific Multicast の設定

ここでは、Source-Specific Multicast（SSM; 送信元固有マルチキャスト）を設定する方法を説明します。この項で使用している SSM コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』の「IP Multicast Routing Commands」を参照してください。この章で扱うその他のコマンドについては、コマンド リファレンス マスター インデックスを使用するか、オンライン検索を実行して該当するドキュメントを検索してください。

SSM は、IP マルチキャストの拡張機能です。この機能を使用すると、レシーバーに転送されるデータグラム トラフィックは、そのレシーバーが明示的に加入しているマルチキャスト送信元からのトラフィックだけになります。SSM 用に設定されたマルチキャスト グループでは、共有ツリーではなく、SSM 分散ツリーだけが作成されます。

SSM コンポーネントの概要

1 対多アプリケーションを最大限にサポートするデータグラム デリバリ モデルである SSM は、ブロードキャスト アプリケーションとも呼ばれます。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューション実装のコア ネットワーキング テクノロジーです。スイッチは SSM の実装をサポートする次のコンポーネントをサポートします。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）

  PIM-SSM は SSM の実装をサポートするルーティング プロトコルであり、Protocol-Independent Multicast Sparse-Mode（PIM-SM; Protocol-Independent Multicast sparse（疎）モード）から派生したものです。

- Internet Group Management Protocol version 3（IGMPv3）

  IGMPv3 を使用して SSM を実行するには、Cisco IOS ルータ、アプリケーションを実行しているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

SSM と Internet Standard Multicast の違い

インターネットの現在の IP マルチキャスト インフラストラクチャや多くの企業イントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。これらのプロトコルには、Internet Standard Multicast（ISM）サービス モデルの制限があります。たとえば、ISM では、ネットワークは、ネットワーク内のどのホストがマルチキャスト トラフィックをアクティブに送信しているかについての情報を維持する必要があります。

ISM サービスは、任意の送信元からマルチキャスト ホスト グループと呼ばれるレシーバー グループへの IP データグラムの配信で構成されます。マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス S と IP 宛先アドレスとしてのマルチキャスト グループ アドレス G のデータグラムで構成されます。システムは、ホスト グループのメンバーになることによって、このトラフィックを受信します。

ホスト グループのメンバーシップに必要なのは、IGMP バージョン 1、2、または 3 によるホスト グループへのシグナリングだけです。SSM では、データグラムは（S, G）チャネルに基づいて配信されます。SSM と ISM のいずれにおいても、送信元になるためのシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決定するために、（S, G）チャネルへの加入またはそこからの脱退を行う必要があります。つまり、レシーバーは加入した（S, G）チャネルからのトラフィックだけを受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを認識する必要はありません。チャネル加入シグナリングの標準的な手法として、IGMP include モード メンバーシップ レポートの使用が提案されますが、この手法をサポートしているのは IGMP バージョン 3 だけです。

SSM IP アドレス範囲

IP マルチキャスト グループ アドレス範囲の設定済みサブセットに SSM デリバリ モデルを適用することにより、SSM と ISM サービスは共存できます。Cisco IOS ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の SSM 設定ができます。SSM 範囲が定義されている場合、既存の IP マルチキャスト レシーバー アプリケーションが SSM 範囲のアドレスの使用しようとしても、（アプリケーションが明示的な（S, G）チャネル加入を使用するように修正されない限り）トラフィックを受信できません。

SSM の動作

SSM サービスは、IP マルチキャスト サービスが PIM SM に基づいている確立されたネットワークでサポートされます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要なすべてのプロトコル範囲（たとえば、MSDP、Auto-RP、またはブートストラップ ルータ（BSR）など）ではなく、SSM を単独でネットワークに配置することもできます。

PIM-SM 用に設定されたネットワークに SSM を配置する場合、SSM をサポートするのはラストホップ ルータだけです。レシーバーに直接接続されていないルータは SSM をサポートする必要はありません。一般的に、これらのラストホップ ルータ以外のルータでは、SSM 範囲内の PIM-SM だけを実行する必要があります。このようなルータは SSM 範囲内での MSDP シグナリング、登録、または PIM-SM 共有ツリー動作を抑制するために、追加のアクセス制御設定が必要になる場合もあります。

SSM 範囲を設定して SSM をイネーブルにするには、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用します。この設定が及ぼす影響を次に示します。

- SSM 範囲内のグループの場合、（S, G）チャネルへの加入は、IGMPv3 include モード メンバーシップ レポートを通して受け入れられます。

- SSM 範囲内のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、ルータで生成されるのは PIM（S, G）の join およびプルーニング メッセージだけであり、（S, G）の Rendezvous Point Tree（RPT; ランデブー ポイント ツリー）や（*, G）の RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視されるか拒否されます。着信 PIM 登録メッセージに対してはただちに register-stop メッセージで応答が行われます。ラストホップ ルータ以外のルータでは、PIM-SSM には PIM-SM との下位互換性があります。したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内の MSDP Source-Active（SA）メッセージの受け入れ、生成、転送は行われません。

IGMPv3 ホスト シグナリング

IGMPv3 では、ホストはマルチキャスト グループのラストホップ ルータにメンバーシップ シグナルを送信します。ホストは、グループ メンバーシップ シグナルの送信に、送信元に関するフィルタリング機能を使用できます。ホストは、いくつかの特定の送信元を除いてすべての送信元からグループへのトラフィックを受信する（exclude モードと呼ばれる）シグナルか、または、いくつかの特定の送信元からグループへのトラフィックだけを受信する（include モードと呼ばれる）シグナルを送信できます。

IGMPv3 は、ISM および SSM と連携して動作できます。ISM では、exclude と include の両方のモードのレポートを適用できます。SSM では、ラストホップ ルータは include モードのレポートだけを受け入れます。exclude モードのレポートは無視されます。

設定時の注意事項

ここでは、SSM の設定時の注意事項について説明します。

SSM 範囲のレガシー アプリケーションに関する制約事項

ネットワーク内の SSM 未対応の既存のアプリケーションは、（S, G）チャネル加入をサポートするように変更しない限り SSM 範囲内で機能しません。したがって、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題を引き起こす可能性があります。

アドレス管理に関する制約事項

SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）でサポートされるのはグループ固有のフィルタリングだけであり、（S, G）チャネル固有のフィルタリングはサポートされません。同じスイッチド ネットワーク内の異なるレシーバーが、同じグループを共有している異なる（S, G）チャネルを要求する場合、レシーバーはこれらの既存メカニズムの利点を活用できません。代わりに、どちらのレシーバーも、すべての（S, G）チャネル トラフィックを受信し、不要なトラフィックを入力時にフィルタリングします。SSM は、独立した多くのアプリケーションに SSM 範囲のグループ アドレスを再利用できるため、この状況では、スイッチド ネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を最小限にすることが重要です。たとえば、テレビ チャネル セットを提供するアプリケーション サービスでは、SSM を使用する場合でも、各テレビ（S, G）チャネルに異なるグループを使用する必要があります。この設定により、同じアプリケーション サービス内の異なるチャネルに複数のレシーバーが接続されていても、レイヤ 2 スイッチを含むネットワークでトラフィック エイリアシングが発生しなくなります。

IGMP スヌーピングおよび CGMP の制限事項

IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、古い IGMP スヌーピング スイッチでは正しく認識されない場合があります。

IGMP（特に CGMP）に関連したスイッチング問題に関する詳細については、「IGMP の概要」（P.49-3）を参照してください。

ステート維持の制限事項

PIM-SSM では、ラストホップ ルータは、そのインターフェイス上に適切な（S, G）加入登録があると、定期的に（S, G）Join メッセージを送信し続けます。そのため、レシーバーが（S, G）加入メッセージを送信する限り、送信元から長時間（またはまったく）トラフィックが送信されなくても、レシーバーから送信元への Shortest Path Tree（SPT）ステートは維持されます。

これは、送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ（S, G）ステートが維持される PIM-SM とは対照的です。PIM-SM では、（S, G）ステートは送信元がトラフィックの送信を 3 分以上停止すると削除され、その送信元からのパケットが RPT を通じて再度到達した場合だけ再確立されます。PIM-SSM では、送信元がアクティブであることをレシーバーに通知するメカニズムがないため、レシーバーが（S, G）チャネルの受信を要求している限り（S, G）ステートを維持する必要があります。

SSM の設定

SSM を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**ip pim ssm** [**default** | **range** *access-list*]	IP マルチキャスト アドレスの SSM 範囲を定義します。
ステップ 2	**interface** type number	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim** {**sparse-mode** | **sparse-dense-mode**}	インターフェイスで PIM をイネーブルにします。**sparse（疎）モード**と **sparse-dense モード**のいずれかを使用する必要があります。
ステップ 4	**ip igmp version 3**	このインターフェイスで IGMPv3 をイネーブルにします。デフォルトでは、IGMP のバージョン 2 が設定されます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SSM のモニタ

SSM をモニタするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
show ip igmp groups detail	IGMPv3 による（S, G）チャネル加入登録を表示します。
show ip mroute	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートが受信されたかどうかを表示します。

Source Specific Multicast（SSM）マッピングの設定

Source Specific Multicast（SSM）マッピング機能は、管理上または技術上の理由からエンド システムで SSM をサポートすることができない場合、またはサポートすることが望ましくない場合に、SSM 移行をサポートします。SSM マッピングを使用すると、IGMPv3 をサポートしないレガシー Set-Top Box（STB; セットトップ ボックス）へのビデオ配信や、IGMPv3 ホスト スタックを使用しないアプリケーションに SSM を活用できます。

ここでは、次の内容について説明します。

設定時の注意事項

SSM マッピング設定時の注意事項を次に示します。

- SSM マッピングを設定する前に、IP マルチキャスト ルーティングをイネーブルにし、PIM sparse（疎）モードをイネーブルにして、SSM を設定します。IP マルチキャスト ルーティングおよび PIM sparse（疎）モードのイネーブル化については、「マルチキャスト ルーティングのデフォルト設定」（P.49-10）を参照してください。
- スタティック SSM マッピングを設定する前に、Access Control List（ACL; アクセス制御リスト）を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。ACL の設定手順については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- SSM マッピングと DNS ルックアップを設定して使用する前に、実行している DNS サーバにレコードを追加できるようにする必要があります。実行している DNS サーバがない場合は、DNS サーバをインストールする必要があります。

  Cisco ネットワーク レジストラなどの製品を使用できます。詳細については、次の URL を参照してください。

  http://www.cisco.com/warp/public/cc/pd/nemnsw/nerr/index.shtml

SSM マッピングには次のような制約があります。

- SSM マッピング機能には、SSM のすべての利点はありません。SSM マッピング機能では、ホストからグループ加入を得て、このグループを 1 つまたは複数の送信元に関連付けられた 1 つのアプリケーションで識別するため、サポートできるアプリケーションは各グループに 1 つだけとなります。すべての SSM アプリケーションが SSM マッピング内の同じグループを共有することは可能です。
- すべての SSM 用の移行ソリューションとして SSM マッピングだけを使用する場合は、ラスト ホップ ルータの IGMPv3 をイネーブルにする際に十分な注意が必要です。SSM マッピングと IGMPv3 を両方イネーブルにした場合、すでに IGMPv3 をサポートしている（SSM はサポートしていない）ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、このような IGMPv3 グループ レポートをサポートしないため、ルータは送信元をこれらのレポートと正しく関連付けることができません。

SSM マッピングの概要

一般的な STB 配置では、各 TV チャネルは独立した 1 つの IP マルチキャスト グループを使用し、その TV チャネルを送信するアクティブなサーバ ホストは 1 つです。単一のサーバから複数の TV チャネルを送信できますが、各チャネルのグループはそれぞれ異なります。このようなネットワーク環境で、ルータが特定のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信した場合、レポートの宛先は、そのマルチキャスト グループに関連付けられている TV チャネルの既知の TV サーバになります。

SSM マッピングが設定されている場合、特定のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信したルータは、このレポートを、このグループに関連付けられている既知の送信元の 1 つまたは複数のチャネル メンバーシップに変換します。

ルータは、グループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、SSM マッピングを使用して、そのグループに対する 1 つまたは複数の送信元 IP アドレスを決定します。その後、SSM マッピングによって、そのメンバーシップ レポートが IGMPv3 レポートに変換され、IGMPv3 レポートを受信した場合と同様に処理が続行されます。IGMPv1 または IGMPv2 のメンバーシップ レポートの受信が続き、そのグループの SSM マッピングが同じである限り、ルータは PIM Join を送信し、これらのグループに加入し続けます。

SSM マッピング機能を使用すると、ラストホップ ルータは、スタティックに設定されたルータ上のテーブルまたは DNS サーバを使用して送信元アドレスを決定できます。スタティックに設定されたテーブルまたは DNS マッピングが変更された場合、ルータは加入しているグループに関連付けられている現在の送信元から脱退します。

SSM マッピングの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

スタティック SSM マッピング

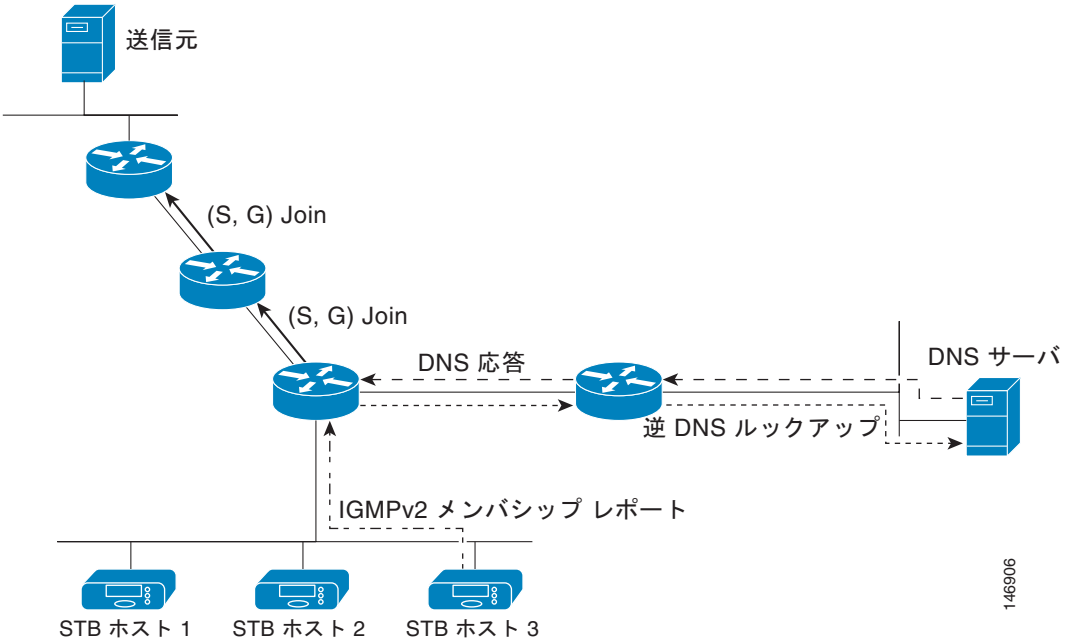
スタティック SSM マッピングでは、ラストホップ ルータが、グループに送信する送信元をスタティック マップを使用して決定するように設定できます。スタティック SSM マッピングを使用するには、グループ範囲を定義した ACL を設定する必要があります。次に、**ip igmp static ssm-map** グローバル コンフィギュレーション コマンドを使用して、ACL で許可されたグループを送信元にマッピングします。

DNS が必要とされない場合やローカルで DNS マッピングが上書きされる場合、小規模なネットワークではスタティック SSM マッピングを設定できます。設定された場合、スタティック SSM マッピングは DNS マッピングより優先されます。

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用して、ラストホップ ルータが逆 DNS ルックアップを実行し、グループの送信元を決定するように設定できます。DNS ベースの SSM マッピングが設定された場合、ルータはグループ アドレスを含むドメイン名を構築し、DNS への逆ルックアップを実行します。ルータは IP アドレス リソース レコードを検索し、それらをこのグループに関連付けられた送信元アドレスとして使用します。SSM マッピングは、グループごとに最大 20 の送信元をサポートします。ルータは各グループに設定されているすべての送信元に加入します（図 49-4 を参照）。

図 49-4　DNS ベースの SSM マッピング



ラストホップ ルータが 1 つのグループの複数の送信元に加入できる SSM マッピング メカニズムによって、TV ブロードキャストの送信元に冗長性を持たせることができます。この場合、ラストホップ ルータは SSM マッピングを使用して、同じ TV チャネルに対して 2 つのビデオ送信元に同時に加入する冗長性を持たせます。ただし、ラストホップ ルータでのビデオ トラフィックの重複を防ぐため、ビデオ送信元がサーバ側でスイッチオーバー メカニズムを使用する必要があります。一方のビデオ送信元はアクティブ、もう一方のバックアップ ビデオ送信元はパッシブになります。パッシブの送信元は、TV チャネルのビデオ トラフィックを送信する前に、アクティブな送信元の障害が検出されるまで待機します。このため、サーバ側のスイッチオーバー メカニズムにより、TV チャネルのビデオ トラフィックをアクティブに送信するサーバは 1 つだけになります。

G1、G2、G3、G4 を含むグループの 1 つまたは複数の送信元アドレスを検索するには、DNS サーバに次のような DNS レコードを設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout]IN A source-address-1
    IN A source-address-2
    IN A source-address-n
```

DNS リソース レコード設定の詳細については、DNS サーバのマニュアルを参照してください。SSM マッピングの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

SSM マッピングの設定

- 「スタティック SSM マッピングの設定」（P.49-21）（必須）
- 「DNS ベースの SSM マッピングの設定」（P.49-21）（必須）
- 「SSM マッピングを使用したスタティック トラフィック転送の設定」（P.49-22）（任意）

スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp ssm-map enable**	設定されている SSM 範囲のグループに対する SSM マッピングをイネーブルにします。 **（注）** デフォルトでは、このコマンドを使用すると DNS ベースの SSM マッピングがイネーブルになります。
ステップ 3	**no ip igmp ssm-map query dns**	（任意）DNS ベースの SSM マッピングをディセーブルにします。 **（注）** スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、**ip igmp ssm-map** グローバル コンフィギュレーション コマンドを使用すると DNS ベースの SSM マッピングがイネーブルになります。
ステップ 4	**ip igmp ssm-map static** *access-list source-address*	スタティック SSM マッピングを設定します。 *access-list* に入力した ACL によって、*source-address* に入力した送信元 IP アドレスにマッピングされるグループが定義されます。 **（注）** 追加のスタティック SSM マッピングを設定できます。追加の SSM マッピングを設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、スイッチは、設定済みの各 **ip igmp ssm-map static** コマンドを使用して、そのグループに関連付けられている送信元アドレスを決定します。スイッチは、グループごとに最大 20 の送信元を関連付けます。
ステップ 5	必要に応じて、ステップ 4 を繰り返して追加のスタティック SSM マッピングを設定します。	—
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SSM マッピングの設定例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

DNS ベースの SSM マッピングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバ ゾーンを作成するか、既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用するルータが他の目的のためにも DNS を使用している場合は、通常の設定の DNS サーバを使用する必要があります。DNS ベースの SSM マッピングだけがそのルータで使用されている DNS 実装である場合、空のルート ゾーン、またはそれ自体を示すルート ゾーンで false の DNS セットアップを設定できます。

DNS ベースの SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp ssm-map enable**	設定されている SSM 範囲のグループに対する SSM マッピングをイネーブルにします。
ステップ 3	**ip igmp ssm-map query dns**	（任意）DNS ベースの SSM マッピングをイネーブルにします。 デフォルトでは、**ip igmp ssm-map** コマンドを使用すると DNS ベースの SSM マッピングがイネーブルになります。実行コンフィギュレーションに保存されるのは、このコマンドの **no** 形式だけです。 **（注）** DNS ベースの SSM マッピングがディセーブルの場合に DNS ベースの SSM マッピングを再びイネーブルにするには、このコマンドを使用します。
ステップ 4	**ip domain multicast** *domain-prefix*	（任意）スイッチが DNS ベースの SSM マッピングに使用するドメイン プレフィクスを変更します。 デフォルトでは、スイッチは *ip-addr.arpa* ドメイン プレフィクスを使用します。
ステップ 5	**ip name-server** *server-address1* [*server-address2... server-address6*]	名前とアドレスの解決に使用する、1 つまたは複数のネーム サーバのアドレスを指定します。
ステップ 6	必要に応じて、ステップ 5 を繰り返して追加の DNS サーバを設定して冗長性を確保します。	—
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SSM マッピングを使用したスタティック トラフィック転送の設定

SSM マッピングを使用したスタティック トラフィック転送によって、特定のグループに SSM トラフィックをスタティックに転送できます。

SSM マッピングを使用したスタティック トラフィック転送を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number*	SSM マッピングを使用してマルチキャスト グループにスタティックにトラフィックを転送するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 **（注）** SSM マッピングを使用したトラフィックのスタティック転送は、DNS ベースの SSM マッピングかスタティックに設定された SSM マッピングのいずれかで機能します。

	コマンド	目的
ステップ 3	**ip igmp static-group** *group-address* **source ssm-map**	インターフェイスから（S, G）チャネルをスタティックに転送するには、SSM マッピングを設定します。 このコマンドは、特定のグループに SSM トラフィックをスタティックに転送する場合に使用します。チャネルの送信元アドレスを決定するには、DNS ベースの SSM マッピングを使用します。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SSM マッピングのモニタ

SSM マッピングをモニタするには、表 49-3 に示す各特権 EXEC コマンドを使用します。

表 49-3　SSM マッピング モニタ コマンド

コマンド	目的
show ip igmp ssm-mapping	SSM マッピングに関する情報を表示します。
show ip igmp ssm-mapping *group-address*	SSM マッピングが特定のグループに使用する送信元を表示します。
show ip igmp groups [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]	ルータに直接接続され、IGMP を通じて学習されたレシーバーのマルチキャスト グループを表示します。
show host	デフォルトのドメイン名、名前検索サービスの方式、ネーム サーバ ホストのリスト、およびキャッシュされたホスト名とアドレスのリストを表示します。
debug ip igmp *group-address*	送受信された IGMP パケットと IGMP ホスト関連イベントを表示します。

SSM マッピングのモニタリングの例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html#wp1047772

PIM スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM 受動インターフェイスの 2 種類です。PIM passive モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過と転送を行うのは IGMP トラフィックだけです。

PIM スタブ ルーティング設定時の注意事項

インターフェイスで PIM スタブ ルーティングをイネーブルにする場合には、次の注意事項に従ってください。

- PIM スタブ ルーティングを設定する前に、スタブ ルータとセントラル ルータの両方に IP マルチキャスト ルーティングが設定されている必要があります。さらに、スタブ ルータのアップリンク インターフェイスに PIM モード（dense（密）モード、sparse（疎）モード、または dense-sparse モード）が設定されている必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間の中継トラフィックのルーティングを行いません。ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制されます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。詳細については、「EIGRP スタブ ルーティングの設定」（P.41-41）を参照してください。
- レイヤ 2 アクセス ドメインでは、直接接続されたマルチキャスト（IGMP）レシーバーと送信元だけが許可されています。PIM プロトコルはアクセス ドメインではサポートされません。
- 冗長 PIM スタブ ルータのトポロジはサポートされません。

PIM スタブ ルーティングのイネーブル化

インターフェイス上で PIM スタブ ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	PIM スタブ ルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim passive**	インターフェイスに PIM スタブ機能を設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip pim interface**	各インターフェイスでイネーブルになっている PIM スタブを表示します。
ステップ 6	show running-config	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスで PIM スタブ ルーティングをディセーブルにするには、**no ip pim passive** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、IP マルチキャスト ルーティングをイネーブルに設定し、スイッチ A の PIM アップリンク ポート 25 を **spare-dense-mode enabled** を使用するルーテッド アップリンク ポートとして設定しています。図 49-2 では、VLAN 100 インターフェイスとギガビット イーサネット ポート 20 で PIM スタブ ルーティングがイネーブルになっています。

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet1/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/20
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/20
```

```
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

各インターフェイスの PIM スタブがイネーブルになっていることを確認するには、**show ip pim interface** 特権 EXEC コマンドを使用します。

```
Switch# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet1/25 v2/SD 1 30 1 3.1.1.2

100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet1/20 v2/P 0 30 1 10.1.1.1
```

PIM スタブの設定とステータスの情報を表示するには、次の特権 EXEC コマンドを使用します。

- **show ip pim interface** は、各インターフェイスでイネーブルになっている PIM スタブを表示します。
- **show ip igmp detail** は、特定のマルチキャスト送信元グループに参加した対象クライアントを表示します。
- **show ip igmp mroute** は、送信元から対象クライアントへマルチキャスト ストリームが転送されていることを確認します。

ランデブー ポイントの設定

インターフェイスが sparse-dense モードで、グループを sparse（疎）グループとして扱う場合には、RP を設定する必要があります。いくつかの方法を使用できます。

- 「手動でのマルチキャスト グループへの RP の割り当て」（P.49-25）
- 「Auto-RP の設定」（P.49-27）（PIMv1 から独立したシスコ独自のスタンドアロン プロトコル）
- 「PIMv2 BSR の設定」（P.49-31）（Internet Engineering Task Force（IETF）標準の追跡プロトコル）

実行している PIM バージョン、およびネットワーク内のルータ タイプに応じて、Auto-RP、BSR、またはこれらを組み合わせて使用できます。詳細については、「PIMv1 および PIMv2 の相互運用性」（P.49-11）および「Auto-RP および BSR 設定時の注意事項」（P.49-12）を参照してください。

手動でのマルチキャスト グループへの RP の割り当て

ここでは、RP を手動で設定する方法を説明します。ダイナミック メカニズム（Auto-RP やBSR など）を通じてグループの RP を学習する場合、その RP に対してこの作業を実行する必要はありません。

マルチキャスト トラフィックの送信側は、送信元のファーストホップ ルータ（指定ルータ）から受信して RP に転送される登録メッセージを通して自身の存在をアナウンスします。マルチキャスト パケットの受信側は、RP を使用してマルチキャスト グループに加入します。この場合は、明示的な Join メッセージが使用されます。RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの「合流地点」として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤ スイッチは PIM dense（密）モード技術を使用して、グループを dense（密）として処理します。

手動で RP のアドレスを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-address** *ip-address* [*access-list-number*] [**override**]	PIM RP のアドレスを設定します。 デフォルトでは、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤ スイッチ（RP を含む）で、RP の IP アドレスを設定する必要があります。グループに RP が設定されていない場合、スイッチは PIM dense（密）モード技術を使用して、グループを dense（密）として処理します。 PIM 装置を、複数のグループの RP にできます。PIM ドメイン内で一度に使用できる RP アドレスは 1 つだけです。アクセス リスト条件により、装置がどのグループの RP であるかを指定します。 • *ip-address* には、RP のユニキャスト アドレスをドット付き 10 進表記で入力します。 • （任意）*access-list-number* には、1 ～ 99 までの標準 IP アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • （任意）**override** キーワードを指定すると、このコマンドによって設定された RP と、Auto-RP または BSR で学習された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループ アドレスを入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

RP アドレスを削除するには、**no ip pim rp-address** *ip-address* [*access-list-number*] [**override**] グローバル コンフィギュレーション コマンドを使用します。

次に、RP のアドレスを、マルチキャスト グループ 225.2.2.2 の場合だけ 147.106.6.22 に設定する例を示します。

```
Switch(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Switch(config)# ip pim rp-address 147.106.6.22 1
```

Auto-RP の設定

Auto-RP は IP マルチキャストを使用して、グループ/RP マッピングを PIM ネットワーク内のすべての Cisco ルータおよびマルチレイヤ スイッチに自動配布します。Auto-RP には、次のような利点があります。

- さまざまなグループ範囲として機能するネットワーク内の複数の RP を使用するのが簡単になります。
- 異なる RP 間で負荷を分散し、グループに加入する場所に従って RP を配置できます。
- PIM ネットワーク内のすべてのルータおよびマルチレイヤ スイッチで矛盾が発生しなくなり、手動による RP 設定が不要になります。この結果、接続の問題を引き起こす原因が取り除かれます。

Auto-RP を設定する場合、次の注意事項に従ってください。

- PIM を sparse（疎）モードまたは sparse-dense モードに設定し、Auto-RP を設定しない場合は、RP を手動で設定する必要があります（「手動でのマルチキャスト グループへの RP の割り当て」（P.49-25）を参照）。
- ルーテッド インターフェイスが sparse（疎）モードに設定されていると、すべての装置が Auto-RP グループの手動 RP アドレスによって設定されている場合でも、Auto-RP を使用できます。
- ルーテッド インターフェイスが sparse（疎）モードに設定され、**ip pim autorp listener** グローバル コンフィギュレーション コマンドを入力すると、すべての装置が Auto-RP グループの手動 RP アドレスを使用して設定されていない場合でも、Auto-RP を使用できます。

ここでは、Auto-RP の設定手順について説明します。

- 「新規インターネットワークでの Auto-RP の設定」（P.49-27）（任意）
- 「既存の sparse（疎）モード クラウドへの Auto-RP の追加」（P.49-27）（任意）
- 「問題のある RP への Join メッセージ送信の防止」（P.49-29）（任意）
- 「着信 RP アナウンス メッセージのフィルタリング」（P.49-30）（任意）

概要については、「Auto-RP」（P.49-7）を参照してください。

新規インターネットワークでの Auto-RP の設定

新規インターネットワーク内に Auto-RP を設定している場合は、すべてのインターフェイスが sparse-dense モードに設定されるため、デフォルトの RP は不要です。「既存の sparse（疎）モード クラウドへの Auto-RP の追加」（P.49-27）のプロセスに従ってください。ただし、PIM ルータをローカル グループの RP として設定する場合は、ステップ 3 を省略してください。

既存の sparse（疎）モード クラウドへの Auto-RP の追加

ここでは、Auto-RP を既存の sparse（疎）モード クラウドに最初に導入する際に、既存のマルチキャスト インフラストラクチャの破壊を最小限に抑える方法について説明します。

既存の sparse（疎）モード クラウドに Auto-RP を導入するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**show running-config**	すべての PIM 装置上でデフォルトの RP がすでに設定されていること、および RP が sparse（疎）モード ネットワーク内にあることを確認します。RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって事前に設定されています。 spare-dense モード環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワーク全体で使用可能である必要があります。この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用します。この RP で処理されるグループ アドレス範囲は再設定しないでください。Auto-RP によってダイナミックに検出された RP は、スタティックに設定された RP よりも優先されます。ローカル グループ用に 2 番めの RP を使用することもできます。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*	別の PIM 装置をローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイスのタイプと番号を入力します。有効なインターフェイスとしては、物理ポート、ポート チャネル、および VLAN があります。 • **scope** *ttl* には、ホップの Time to Live 値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達できるように、十分なホップ カウントを入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。 • **group-list** *access-list-number* には、1 ～ 99 までの標準 IP アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval** *seconds* には、アナウンス メッセージを送信する頻度を指定します。デフォルト値は 60 秒です。指定できる範囲は 1 ～ 16383 です。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny**　キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループ アドレス範囲を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。

	コマンド	目的
ステップ 5	**ip pim send-rp-discovery scope** *ttl*	接続が中断される可能性がないスイッチを検索し、RP マッピング エージェントの役割を割り当てます。 **scope** *ttl* には、ホップの Time to Live 値を指定し、RP 検出パケットを制限します。ホップ カウント内にあるすべての装置は、送信元装置から Auto-RP ディスカバリ メッセージを受信します。これらのメッセージは他の装置に対し、矛盾（グループ /RP 範囲の重複など）を回避するために使用されるグループ /RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
	show ip pim rp mapping	関連付けられたマルチキャスト ルーティング エントリとともにキャッシュされたアクティブ RP を表示します。
	show ip pim rp	ルーティング テーブルにキャッシュされた情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

候補 RP として設定された PIM 装置を解除するには、**no ip pim send-rp-announce** *interface-id* グローバル コンフィギュレーション コマンドを使用します。RP マッピング エージェントとして設定されたスイッチを解除するには、**no ip pim send-rp-discovery** グローバル コンフィギュレーション コマンドを使用します。

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセス リスト 5 には、このスイッチが RP として機能するグループが記述されています。

```
Switch(config)# ip pim send-rp-announce gigabitethernet1/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

問題のある RP への Join メッセージ送信の防止

ip pim accept-rp コマンドがネットワーク全体に設定されているかどうかを判別するには、**show running-config** 特権 EXEC コマンドを使用します。**ip pim accept-rp** コマンドが設定されていない装置がある場合は、あとでこの問題に対処できます。ルータまたはマルチレイヤ スイッチが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新しくアドバタイズされた RP を許可する必要があります。

Auto-RP でアドバタイズされたすべての RP を許可し、他のすべての RP をデフォルトで拒否するには、**ip pim accept-rp auto-rp** グローバル コンフィギュレーション コマンドを使用します。この手順は任意です。

すべてのインターフェイスが sparse（疎）モードの場合はデフォルト設定の RP を使用し、224.0.1.39 および 224.0.1.40 の 2 つの既知のグループをサポートします。Auto-RP はこれら 2 つの既知のグループを使用し、RP マッピング情報を収集および配布します。このように **ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定する必要があります。

```
Switch(config)# ip pim accept-rp 172.10.20.1 1
Switch(config)# access-list 1 permit 224.0.1.39
Switch(config)# access-list 1 permit 224.0.1.40
```

着信 RP アナウンス メッセージのフィルタリング

マッピング エージェントにコンフィギュレーション コマンドを追加すると、不正に設定されたルータが候補 RP になりすまして問題を引き起こすことを回避できます。

着信 RP アナウンス メッセージをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-announce-filter rp-list** *access-list-number* **group-list** *access-list-number*	着信 RP アナウンス メッセージをフィルタリングします。 このコマンドは、ネットワーク内のマッピング エージェントごとに入力します。このコマンドを使用しなければ、すべての着信 RP アナウンス メッセージがデフォルトで受け入れられます。 **rp-list** *access-list-number* には、候補 RP アドレスのアクセス リストを設定します。アクセス リストが許可されている場合は、**group-list** *access-list-number* 変数で指定されたグループ範囲に対してアクセス リストを使用できます。この変数を省略した場合は、すべてのマルチキャスト グループにフィルタが適用されます。 複数のマッピング エージェントを使用する場合は、グループ/RP マッピング情報に矛盾が発生しないように、すべてのマッピング エージェント間でフィルタが一貫している必要があります。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • マッピング エージェントが、どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンス（rp-list ACL）を許可するかを指定するアクセス リストを作成します。 • 許可または拒否するマルチキャスト グループの範囲を指定するアクセス リスト（group-list ACL）を作成します。 • *source* には、RP が使用されるマルチキャスト グループ アドレス範囲を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

着信 RP アナウンス メッセージに関するフィルタを削除するには、**no ip pim rp-announce-filter rp-list** *access-list-number* [**group-list** *access-list-number*] グローバル コンフィギュレーション コマンドを使用します。

次に、不正な候補 RP が候補 RP アナウンスを許可することを防ぐために使用される Auto-RP マッピング エージェントを設定する例を示します。

```
Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config)# access-list 10 permit host 172.16.5.1
Switch(config)# access-list 10 permit host 172.16.2.1
Switch(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Switch(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

この例では、マッピング エージェントは、172.16.5.1 および 172.16.2.1 の 2 つの装置からの候補 RP アナウンスだけを許可します。マッピング エージェントは 2 つの装置からの候補 RP アナウンスのうち、グループ範囲が 224.0.0.0 ～ 239.255.255.255 であるマルチキャスト グループ宛てのアナウンスだけを許可します。マッピング エージェントは、ネットワーク内の他の装置からの候補 RP アナウンスを許可しません。さらに、候補 RP アナウンスが 239.0.0.0 ～ 239.255.255.255 の範囲のグループに宛てたものである場合、マッピング エージェントは 172.16.5.1 または 172.16.2.1 からの候補 RP アナウンスを許可しません。この範囲は、管理用スコープのアドレス範囲です。

PIMv2 BSR の設定

ここでは、PIMv2 ネットワークでの BSR の設定手順について説明します。

- 「PIM ドメイン境界の定義」（P.49-31）（任意）
- 「IP マルチキャスト境界の定義」（P.49-32）（任意）
- 「候補 BSR の設定」（P.49-33）（任意）
- 「候補 RP の設定」（P.49-33）（任意）

概要については、「ブートストラップ ルータ」（P.49-7）を参照してください。

PIM ドメイン境界の定義

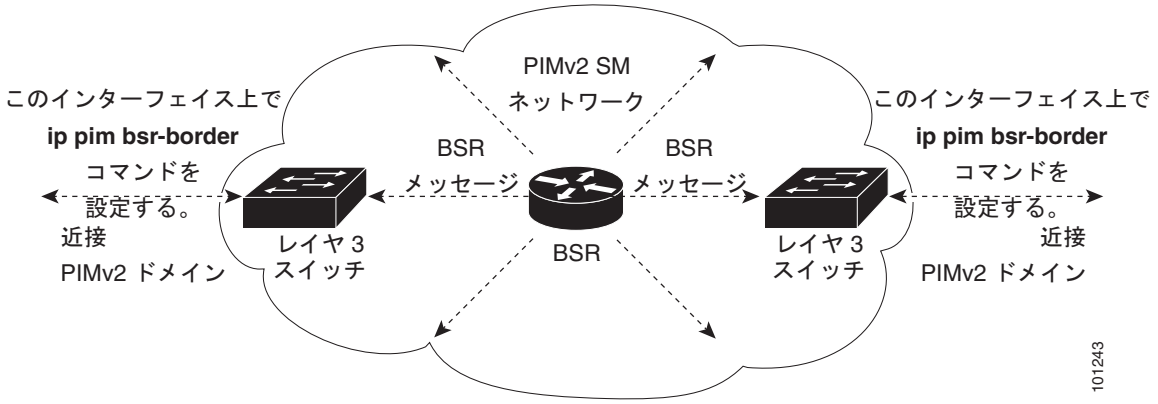
IP マルチキャストの普及に伴い、1 つの PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する機会が増えています。これらの 2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していない可能性があるため、PIMv2 BSR メッセージがドメインの内外に流れないように抑制する必要があります。これらメッセージのドメイン境界通過を許可すると、通常の BSR 選定メカニズムに悪影響を与えたり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズが共存し、誤ったドメイン内で RP が選択されたりすることがあります。

PIM ドメイン境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim bsr-border**	PIM ドメイン用の PIM ブートストラップ メッセージ境界を定義します。 このコマンドは、境界に位置する他の PIM ドメインに接続されているインターフェイスごとに入力します。このコマンドを実行すると、スイッチは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指定されます（図 49-5 を参照）。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

PIM 境界を削除するには、**no ip pim bsr-border** インターフェイス コンフィギュレーション コマンドを使用します。

図 49-5　PIMv2 BSR メッセージの抑制



IP マルチキャスト境界の定義

Auto-RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。Auto-RP 情報を伝送する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセス リストを作成します。

マルチキャスト境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **deny** *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • *source* には、Auto-RP 情報を伝送するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip multicast boundary** *access-list-number*	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

境界を削除するには、**no ip multicast boundary** インターフェイス コンフィギュレーション コマンドを使用します。

次に、Auto-RP 情報を拒否する IP マルチキャスト境界を設定する例の一部を示します。

```
Switch(config)# access-list 1 deny 224.0.1.39
Switch(config)# access-list 1 deny 224.0.1.40
Switch(config)# access-list 1 permit all
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip multicast boundary 1
```

候補 BSR の設定

候補 BSR を 1 つまたは複数設定できます。候補 BSR として機能する装置は、他の装置との接続が良好で、ネットワークのバックボーン部分に配置されている必要があります。

スイッチを候補 BSR として設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*]	スイッチが候補 BSR になるように設定します。 • *interface-id* には、スイッチを候補 BSR に設定するときに BSR アドレスが取得される、スイッチのインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必要があります。有効なインターフェイスとしては、物理ポート、ポート チャネル、および VLAN があります。 • *hash-mask-length* には、ハッシュ機能をコールする前の、グループ アドレスと AND 条件となるマスク長（最大 32 ビット）を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、この値が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。 • （任意）*priority* には、0 ～ 255 までの番号を入力します。プライオリティの高い BSR が優先されます。プライオリティ値が同じである場合は、最大の IP アドレスを持つ装置が BSR として選択されます。デフォルト値は 0 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

候補 BSR として設定されたこの装置を解除するには、**no ip pim bsr-candidate** グローバル コンフィギュレーション コマンドを使用します。

次に、候補 BSR を設定する例を示します。この例では、アドバタイズされる BSR アドレスとしてポートの IP アドレス 172.21.24.18 を使用し、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

```
Switch(config)# interface gigabitethernet1/2
```

候補 RP の設定

候補 RP を 1 つまたは複数設定できます。BSR と同様に RP は、他の装置との接続が良好で、ネットワークのバックボーン部分に配置されている必要があります。RP は IP マルチキャスト アドレス空間全体、またはその一部を処理します。候補 RP は候補 RP アドバタイズを BSR に送信します。RP となる装置を決定するときには、次のオプションを考慮してください。

- Cisco ルータおよびマルチレイヤ スイッチで構成される、Auto-RP だけが使用されているネットワークでは、すべての装置を RP として設定できます。
- シスコ製 PIMv2 ルータおよびマルチレイヤ スイッチと、他のベンダー製のルータだけで構成されるネットワークでは、すべての装置を RP として使用できます。
- シスコ製 PIMv1 ルータ、PIMv2 ルータ、および他のベンダー製のルータで構成されるネットワークでは、シスコ製 PIMv2 ルータおよびマルチレイヤ スイッチだけを RP として設定します。

スイッチが自身を PIMv2 候補 RP として BSR にアドバタイズするように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*]	スイッチが候補 RP になるように設定します。 • *interface-id* には、関連付けられた IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスとしては、物理ポート、ポート チャネル、および VLAN があります。 •（任意）**group-list** *access-list-number* には、1 ～ 99 までの標準 IP アクセス リスト番号を入力します。group-list が指定されていない場合は、スイッチがすべてのグループの候補 RP となります。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 •（任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

候補 RP として設定されたこの装置を解除するには、**no ip pim rp-candidate** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチが自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするように設定する例を示します。標準アクセス リスト番号 4 は、ポートによって識別されるアドレスを持つ RP に関連付けられたグループ プレフィクスを指定します。この RP は、プレフィクスが 239 であるグループを処理します。

```
Switch(config)# ip pim rp-candidate gigabitethernet1/2 group-list 4
Switch(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

Auto-RP および BSR の使用

ネットワーク上のルータがすべてシスコ デバイスである（他のベンダー製のルータが存在しない）場合には、BSR を設定する必要はありません。PIMv1 と PIMv2 が両方とも動作しているネットワークに、Auto-RP を設定します。

シスコ製 PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、Auto-RP と BSR の両方が必要です。シスコ製 PIMv2 ルータまたはマルチレイヤ スイッチを、Auto-RP マッピング エージェントと BSR の両方に設定することを推奨します。

BSR を 1 つまたは複数使用する必要がある場合の推奨事項を次に示します。

- 候補 BSR を Auto-RP 用の RP マッピング エージェントとして設定します。詳細については、「Auto-RP の設定」（P.49-27）および「候補 BSR の設定」（P.49-33）を参照してください。
- グループ プレフィクスが Auto-RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループ プレフィクスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。PIMv1 と PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループ プレフィクスが処理されるように設定します。この設定により、PIMv2 DR は、RP マッピング データベースでの最長一致検索のために、これらの PIMv1 DR から異なる RP を選択できなくなります。

グループ/RP マッピングの整合性を確認するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**show ip pim rp** [[*group-name* | *group-address*] | **mapping**]	任意のシスコ デバイスについて、使用可能な RP マッピングを表示します。 • （任意）*group-name* には、RP を表示するグループの名前を指定します。 • （任意）*group-address* には、RP を表示するグループのアドレスを指定します。 • （任意）シスコ デバイスが認識する（設定または Auto-RP から学習された）すべてのグループ/RP マッピングを表示するには、**mapping** キーワードを使用します。
ステップ 2	**show ip pim rp-hash** *group*	PIMv2 ルータまたはマルチレイヤ スイッチで、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。 *group* には、RP 情報を表示するグループ アドレスを入力します。

RP マッピング情報のモニタ

RP マッピング情報をモニタするには、特権 EXEC モードで次のコマンドを使用します。

- **show ip pim bsr** は、選定された BSR の情報を表示します。
- **show ip pim rp-hash** *group* は、指定グループに選択された RP を表示します。
- **show ip pim rp** [*group-name* | *group-address* | **mapping**] は、スイッチが（BSR 経由で、または Auto-RPRP メカニズムによって）RP を学習する方法を表示します。

PIMv1 および PIMv2 相互運用性の問題のトラブルシューティング

PIMv1 および PIMv2 間の相互運用性の問題をデバッグする場合、次の点を順に確認します。

1. **show ip pim rp-hash** 特権 EXEC コマンドを使用して RP マッピングを確認し、すべてのシステムが同じグループの同じ RP に同意していることを確認します。
2. DR と RP の各バージョン間の相互運用性を確認します。RP が DR と適切に相互作用していることを確認します（この場合は、register-stop メッセージに応答し、カプセル化が解除されたデータ パケットをレジスタから転送します）。

高度な PIM 機能の設定

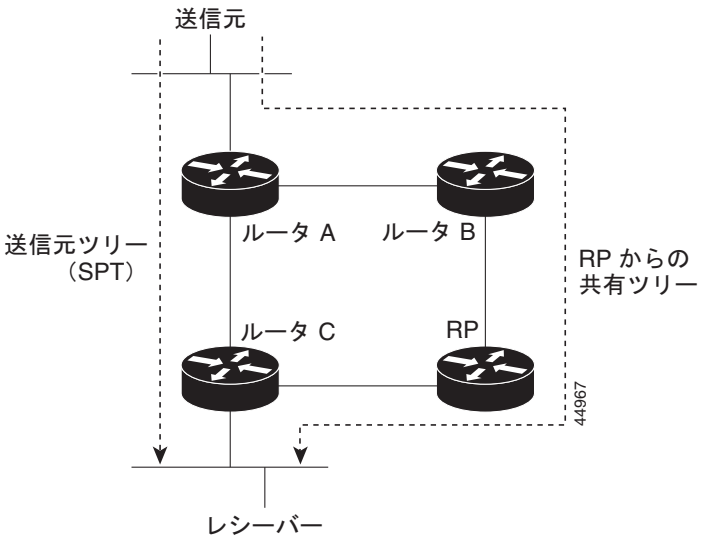
ここでは、オプションの高度な PIM 機能について説明します。

- 「PIM 共有ツリーおよび送信元ツリーの概要」（P.49-36）
- 「PIM Shortest-Path Tree 使用の延期」（P.49-37）（任意）
- 「PIM ルータクエリー メッセージ インターバルの変更」（P.49-39）（任意）

PIM 共有ツリーおよび送信元ツリーの概要

デフォルトでは、グループのメンバーが受信するデータは、RP でルーティングされた単一のデータ分散ツリーを経由して、送信側からグループに送信されます。図 49-6 に、このタイプの共有分散ツリーを示します。送信側からのデータは RP に配信され、共有ツリーに加入しているグループ メンバーへ配布されます。

図 49-6　　共有ツリーおよび送信元ツリー（Shortest-Path Tree）



データ レートが保証されている場合は、送信元でルーティングされたデータ分散ツリーを共有ツリーのリーフ ルータ（ダウンストリーム接続がないルータ）で使用できます。このタイプの分散ツリーは、Shortest-Path Tree または送信元ツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

共有ツリーから送信元ツリーへの移動プロセスを次に示します。

1. レシーバーがグループに加入します。リーフ ルータ C は Join メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。ルータ A はデータを登録メッセージにカプセル化して RP に送信します。
4. RP はデータをルータ C に向けて共有ツリーの下方向に転送し、送信元に向けて Join メッセージを送信します。この時点で、データはルータ C に 2 回着信する可能性があります。1 つはカプセル化されたデータ、もう 1 つはネイティブ状態のデータです。
5. データがネイティブ状態（カプセル化されていない状態）で着信すると、RP は register-stop メッセージをルータ A に送信します。
6. デフォルトでは、最初のデータ パケットを受信すると、ルータ C が送信元に Join メッセージを送信するように求められます。
7. （S,G）に関するデータを受信すると、ルータ C は送信元宛のプルーニング メッセージを共有ツリーの上方向に送信します。
8. RP は（S,G）の発信インターフェイスからルータ C へのリンクを削除します。RP は送信元に向けてプルーニング メッセージをトリガーします。

Join メッセージとプルーニング メッセージが送信元および RP に送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP へのパス上にある各 PIM 装置で処理されます。登録メッセージと register-stop メッセージはホップバイホップで送信されません。これらのメッセージは、送信元に直接接続された指定ルータで送信され、グループの RP で受信されます。

グループへ送信する複数の送信元は、共有ツリーを使用します。

PIM 装置を共有ツリー上に存在するように設定できます。詳細については、「PIM Shortest-Path Tree 使用の延期」（P.49-37）を参照してください。

PIM Shortest-Path Tree 使用の延期

共有ツリーから送信元ツリーへの変更は、最初のデータ パケットがラストホップ ルータ（図 49-6 のルータ C）に着信すると発生します。この変更は、**ip pim spt-threshold** グローバル コンフィギュレーション コマンドによってタイミングが制御されるために発生します。

Shortest-Path Tree では共有ツリーよりも多くのメモリが必要となりますが、遅延が短縮されます。Shortest-Path Tree の使用を延期することも可能です。リーフ ルータを Shortest-Path Tree にすぐ移動する代わりに、トラフィックがスレッシュホールドに先に到達するように指定できます。

PIM リーフ ルータが指定グループの Shortest-Path Tree に加入する時期を設定できます。送信元の送信速度が指定速度（KB/秒）以上の場合、マルチレイヤ スイッチは PIM Join メッセージを送信元に向けてトリガーし、送信元ツリー（Shortest-Path Tree）を構築します。送信元からのトラフィック レートがスレッシュホールド値を下回ると、リーフ ルータは共有ツリーに再び切り替わり、送信元にプルーニング メッセージを送信します。

Shortest-Path Tree スレッシュホールドを適用するグループを指定するには、グループ リスト（標準アクセス リスト）を使用します。値 0 を指定する場合、またはグループ リストを使用しない場合、スレッシュホールドはすべてのグループに適用されます。

マルチキャスト ルーティングが送信元ツリーから Shortest-Path Tree に切り替わる前の上限値となるトラフィック レートのスレッシュホールドを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、スレッシュホールドを適用するマルチキャスト グループを指定します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list-number*]	Shortest-Path Tree（SPT）に移動する前の上限値となるスレッシュホールドを指定します。 • *kbps* には、トラフィック レートを Kbps で指定します。デフォルト値は 0 KB/秒です。 **（注）** 指定できる範囲は 0 ～ 4294967 ですが、スイッチ ハードウェアの制限により、0 KB/秒だけが有効となります。 • 指定グループのすべての送信元で共有ツリーを使用し、送信元ツリーに切り替わらないようにするには、**infinity** を指定します。 • （任意）**group-list** *access-list-number* には、ステップ 2 で作成したアクセス リストを指定します。値 が 0 の場合、または group-list を使用しない場合、スレッシュホールドはすべてのグループに適用されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip pim spt-threshold** {*kbps* | **infinity**} グローバル コンフィギュレーション コマンドを使用します。

PIM ルータクエリー メッセージ インターバルの変更

PIM ルータおよびマルチレイヤ スイッチでは、各 LAN セグメント（サブネット）の DR になる装置を判別するために、PIM ルータクエリー メッセージが送信されます。DR は、直接接続されている LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。

PIM DM 動作では、DR は IGMPv1 を使用している場合だけ意味があります。IGMPv1 には IGMP クエリア選定プロセスがないため、選定された DR は IGMP クエリアとして機能します。PIM SM 動作では、マルチキャスト送信元に直接接続されている装置が DR になります。DR は PIM 登録メッセージを送信し、送信元からのマルチキャスト トラフィックを共有ツリーの下方向へ転送する必要があることを RP に通知します。この場合、最大の IP アドレスを持つ装置が DR となります。

ルータクエリー メッセージ インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim query-interval** *seconds*	スイッチが PIM ルータクエリー メッセージを送信する頻度を設定します。 デフォルト値は 30 秒です。指定できる範囲は 1 ～ 65535 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip pim query-interval** [*seconds*] インターフェイス コンフィギュレーション コマンドを使用します。

オプションの IGMP 機能の設定

ここでは、次の設定情報について説明します。

- 「IGMP のデフォルト設定」（P.49-40）
- 「グループのメンバーとしてのスイッチの設定」（P.49-40）（任意）
- 「IP マルチキャスト グループへのアクセスの制御」（P.49-41）（任意）
- 「IGMP バージョンの変更」（P.49-42）（任意）
- 「IGMP ホストクエリー メッセージ インターバルの変更」（P.49-42）（任意）
- 「IGMPv2 の IGMP クエリー タイムアウトの変更」（P.49-43）（任意）
- 「IGMPv2 の最大クエリー応答時間の変更」（P.49-44）（任意）
- 「スタティックに接続されたメンバーとしてのスイッチの設定」（P.49-44）（任意）

IGMP のデフォルト設定

表 49-4 に、IGMP のデフォルト設定を示します。

表 49-4　IGMP のデフォルト設定

機能	デフォルト設定
マルチキャスト グループのメンバーとしてのマルチレイヤ スイッチ	グループ メンバーシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを許可
IGMP バージョン	すべてのインターフェイスでバージョン 2
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
スタティックに接続されたメンバーとしてのマルチレイヤ スイッチ	ディセーブル

グループのメンバーとしてのスイッチの設定

スイッチをマルチキャスト グループのメンバーとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理しているすべてのマルチキャスト対応ルータおよびマルチレイヤ スイッチがマルチキャスト グループのメンバーである場合、グループに ping を使用すると、これらのすべての装置が応答します。装置は、属するグループにアドレス指定された ICMP エコー要求パケットに応答します。もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。

注意　この手順を実行すると、CPU がグループ アドレスのデータ トラフィックをすべて受信するため、CPU のパフォーマンスに影響を与える場合があります。

スイッチがグループのメンバーになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp join-group** *group-address*	マルチキャスト グループに加入するスイッチを設定します。 デフォルトでは、グループ メンバーシップは定義されていません。 *group-address* には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

グループのメンバーシップをキャンセルするには、**no ip igmp join-group** *group-address* インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチをマルチキャスト グループ 255.2.2.2 の加入をイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp join-group 255.2.2.2
```

IP マルチキャスト グループへのアクセスの制御

スイッチは IGMP ホストクエリー メッセージを送信し、接続されたローカル ネットワーク上のメンバーが属しているマルチキャスト グループを判別します。次に、スイッチはマルチキャスト グループにアドレス指定されたすべてのパケットをこれらのグループ メンバーに転送します。各インターフェイスにフィルタを適用することで、インターフェイスで処理されるサブネット上のホストが加入できるマルチキャスト グループを制限できます。

インターフェイスで許可されるマルチキャスト グループをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp access-group** *access-list-number*	インターフェイスで処理されるサブネット上のホストが加入できるマルチキャスト グループを指定します。 デフォルトでは、インターフェイスのすべてのグループが許可されています。 *access-list-number* には、標準 IP アクセス リスト番号を指定します。指定できる範囲は 1 ～ 99 です。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。 • *access-list-number* には、ステップ 3 で作成したアクセス リストを指定します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、サブネット上のホストが加入できるマルチキャスト グループを指定します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスでグループをディセーブルにするには、**no ip igmp access-group** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに接続されたホストが、グループ 255.2.2.2 だけに加入できるように設定する例を示します。

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp access-group 1
```

IGMP バージョンの変更

デフォルトでは、スイッチは IGMP クエリー タイムアウトや最大クエリー応答時間などの機能を提供する IGMP バージョン 2 を使用します。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。スイッチは、バージョン 1 システムを自動的に検出せず、バージョン 1 への切り替えも行いません。バージョン 2 のルータまたはスイッチは、常に IGMPv1 ホストと正しく連動しているため、サブネット上でバージョン 1 とバージョン 2 のホストを混在できます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

IGMP バージョンを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp version** {**1** | **2**}	スイッチが使用する IGMP バージョンを指定します。 **（注）** バージョン 1 に変更する場合、**ip igmp query-interval** または **ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを設定できません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip igmp version** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP ホストクエリー メッセージ インターバルの変更

スイッチは IGMP ホストクエリー メッセージを定期的に送信し、接続されたネットワーク上に存在するマルチキャスト グループを検出します。これらのメッセージは、Time to Live（TTL）が 1 であるすべてのホスト マルチキャスト グループ（224.0.0.1）に送信されます。スイッチはホストクエリー メッセージを送信し、ネットワーク上に存在するメンバーシップについての情報を更新します。クエリーをいくつか実行したあとで、マルチキャスト グループのメンバーであるローカル ホストが存在しないことをソフトウェアが検出した場合、ソフトウェアは、そのグループのリモート送信元からローカル ネットワークへのマルチキャスト パケット転送を停止し、送信元のアップストリーム方向へプルーニング メッセージを送信します。

スイッチはLAN（サブネット）用の PIM 指定ルータ（DR）を選定します。DR は、最大の IP アドレスを持つ、IGMPv2 用のルータまたはマルチレイヤ スイッチです。IGMPv1 の場合、DR は LAN 上で動作するマルチキャスト ルーティング プロトコルに従って選定されます。DR は、LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。sparse（疎）モードの場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。

ホストクエリー インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp query-interval** *seconds*	DR が IGMP ホストクエリー メッセージを送信する頻度を設定します。 デフォルトでは、DR は IGMP ホストクエリー メッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。指定できる範囲は 1 ～ 65535 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip igmp query-interval** インターフェイス コンフィギュレーション コマンドを使用します。

IGMPv2 の IGMP クエリー タイムアウトの変更

IGMPv2 を使用している場合、スイッチがインターフェイスのクエリアとして処理を引き継ぐまでの時間を指定できます。デフォルトでは、スイッチは **ip igmp query-interval** インターフェイス コンフィギュレーション コマンドによって制御されるクエリー間隔の 2 倍の時間待機します。この時間を経過してもスイッチがクエリーを受信しない場合は、スイッチがクエリアになります。

クエリー間隔を設定するには、**show ip igmp interface** *interface-id* 特権 EXEC コマンドを入力します。

IGMP クエリー タイムアウトを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp querier-timeout** *seconds*	IGMP クエリー タイムアウトを指定します。 デフォルト値は 60 秒です（クエリー間隔の 2 倍）。指定できる範囲は 60 ～ 300 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip igmp querier-timeout** インターフェイス コンフィギュレーション コマンドを使用します。

IGMPv2 の最大クエリー応答時間の変更

IGMPv2 を使用している場合、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。最大クエリー応答時間により、LAN 上に直接接続されているグループ メンバーが存在しないことを短時間で検出するようにスイッチをイネーブルにします。値を小さくすると、グループのプルーニング速度が向上します。

最大クエリー応答時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp query-max-response-time** *seconds*	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルト値は 10 秒です。指定できる範囲は 1 ～ 25 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを使用します。

スタティックに接続されたメンバーとしてのスイッチの設定

ネットワーク セグメント上にグループ メンバーが存在しない場合や、ホストが IGMP を使用してグループ メンバーシップをレポートできない場合があります。ただし、そのネットワーク セグメントにマルチキャスト トラフィックを送り込むことが必要な場合があります。次に、マルチキャスト トラフィックをネットワーク セグメントに送り込む方法を示します。

- **ip igmp join-group** インターフェイス コンフィギュレーション コマンドを使用します。この方法の場合、スイッチはマルチキャスト パケットの受け入れに加えて転送もします。マルチキャスト パケットを受け入れる場合は、高速スイッチングを実行できません。
- **ip igmp static-group** インターフェイス コンフィギュレーション コマンドを使用します。この方法の場合、スイッチはパケットそのものを受け入れず、転送だけを実行します。この方法の場合は高速スイッチングをイネーブルにします。発信インターフェイスは IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに *L*（ローカル）フラグがないことからわかるように、スイッチ自体はメンバーではありません。

スタティックに接続されたグループのメンバーになるように（および高速スイッチングをイネーブルにできるように）スイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp static-group** *group-address*	スイッチをスタティックに接続されたグループのメンバーとして設定します。 デフォルトでは、この機能はディセーブルです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

グループのメンバーとして設定されたスイッチを解除するには、**no ip igmp static-group** *group-address* インターフェイス コンフィギュレーション コマンドを使用します。

オプションのマルチキャスト ルーティング機能の設定

ここでは、オプションのマルチキャスト ルーティング機能の設定手順について説明します。

- レイヤ 2 接続と MBONE マルチメディア会議セッションに関する機能と設定
  - 「CGMP サーバ サポートのイネーブル化」（P.49-45）（任意）
  - 「sdr リスナー サポートの設定」（P.49-47）（任意）
- 帯域利用率を制御する機能
  - 「IP マルチキャスト境界の設定」（P.49-48）（任意）
- Virtual Private Network（VPN; 仮想私設網）Routing/Forwarding（VRF; VPN ルーティング / 転送）テーブル内のマルチキャストの設定手順
  - 「マルチキャスト VRF の設定」（P.41-79）

CGMP サーバ サポートのイネーブル化

スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれている装置用の CGMP サーバとして機能します。CGMP は、レイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用されるプロトコルであり、IGMP で実行される作業と同様の作業を実行します。CGMP が必要となるのは、レイヤ 2 スイッチで IP マルチキャスト データ パケットと IGMP レポート メッセージを区別できないためです。これらはともに MAC レベルで、同じグループ アドレスにアドレス指定されます。

スイッチインターフェイスで CGMP サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レイヤ 2 Catalyst スイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip cgmp** [**proxy**]	インターフェイスで CGMP をイネーブルにします。 デフォルトでは、CGMP はすべてのインターフェイスでディセーブルになっています。 CGMP をイネーブルにすると、CGMP Join メッセージがトリガーされます。CGMP は、レイヤ 2 Catalyst スイッチに接続されたレイヤ 3 インターフェイスでだけイネーブルにします。 （任意）**proxy** キーワードを入力すると、CGMP プロキシ機能がイネーブルになります。プロキシ ルータは、CGMP 非対応ルータの MAC アドレスおよびグループ アドレス 0000.0000.0000 が格納された CGMP Join メッセージを送信することで、CGMP 非対応ルータの存在をアドバタイズします。 **（注）** CGMP プロキシを実行するには、スイッチを IGMP クエリアに設定する必要があります。**ip cgmp proxy** コマンドを設定する場合は、ネットワークで動作中の IGMP のバージョンに応じて、最大または最小の IP アドレスのスイッチが IGMP クエリアになるように、IP アドレスを処理する必要があります。IGMP バージョン 2 クエリアは、インターフェイスの最小の IP アドレスに基づいて選択されます。IGMP バージョン 1 クエリアは、インターフェイスで使用されるマルチキャスト ルーティング プロトコルに基づいて選択されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。
ステップ 7		レイヤ 2 Catalyst スイッチ CGMP クライアントの設定を確認します。詳細については、製品に付属のマニュアルを参照してください。

インターフェイスで CGMP をディセーブルにするには、**no ip cgmp** インターフェイス コンフィギュレーション コマンドを使用します。

複数のシスコ製 CGMP 対応装置がスイッチド ネットワークに接続されている状態で **ip cgmp proxy** コマンドを使用する必要がある場合は、すべての装置を同じ CGMP オプションで設定し、IGMP クエリアを非 Cisco ルータよりも優先させることを推奨します。

sdr リスナー サポートの設定

MBONE は、相互接続され、IP マルチキャスト トラフィックの転送が可能なインターネット ルータおよびホストの小さなサブセットです。その他のマルチメディア コンテンツも、多くの場合、MBONE を通してブロードキャストされます。マルチメディア セッションに加入する前に、このセッションで使用されているマルチキャスト グループ アドレスとポート、セッションがアクティブになる時期、およびワークステーションで必要とされるアプリケーションの種類（オーディオやビデオなど）を把握する必要があります。この情報は、MBONE Session Directory バージョン 2（sdr）ツールによって提供されます。このフリーウェア アプリケーションは WWW 上の複数のサイト（http://www.video.ja.net/mice/index.html など）からダウンロードできます。

SDR は、Session Announcement Protocol（SAP; セッション通知プロトコル）マルチキャスト パケット用の既知のマルチキャスト グループ アドレスとポートを、会議セッションをアナウンスする SAP クライアントから待ち受けるマルチキャスト アプリケーションです。これらの SAP パケットには、セッションの説明、セッションがアクティブな期間、IP マルチキャスト グループ アドレス、メディア形式、担当者、およびアドバタイズされたマルチメディア セッションに関するその他の情報が含まれています。SAP パケットの情報は、[SDR Session Announcement] ウィンドウに表示されます。

sdr リスナー サポートのイネーブル化

デフォルトでは、スイッチはセッション ディレクトリのアドバタイズを待ち受けません。

スイッチがインターフェイスのデフォルトのセッション ディレクトリ グループ（224.2.127.254）に加入し、セッション ディレクトリ アドバタイズを待ち受けられるようにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	sdr に対してイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip sdr listen**	sdr リスナー サポートをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

sdr サポートをディセーブルにするには、**no ip sdr listen** インターフェイス コンフィギュレーション コマンドを使用します。

sdr キャッシュ エントリの存在期間の制限

デフォルトでは、エントリは sdr キャッシュから削除されません。送信元が SAP 情報のアドバタイズを停止した場合に、古いアドバタイズが不必要に保持されることを防ぐために、エントリがアクティブである期間を制限できます。

sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sdr cache-timeout** *minutes*	sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限します。 デフォルトでは、エントリは sdr キャッシュから削除されません。 *minutes* に指定できる範囲は 1 ～ 4294967295 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip sdr cache-timeout** グローバル コンフィギュレーション コマンドを使用します。キャッシュ全体を削除するには、**clear ip sdr** 特権 EXEC コマンドを使用します。

セッション ディレクトリ キャッシュを表示するには、**show ip sdr** 特権 EXEC コマンドを使用します。

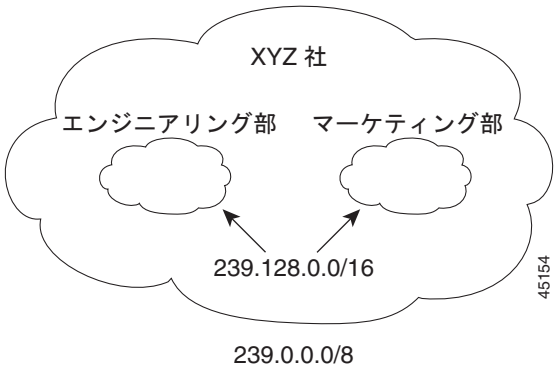
IP マルチキャスト境界の設定

管理用スコープの境界を使用して、ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限できます。この方法では、*管理用スコープのアドレス* と呼ばれる特殊なマルチキャスト アドレス範囲が境界のメカニズムとして使用されます。管理用スコープの境界をルーテッド インターフェイスに設定すると、マルチキャスト グループ アドレスがこの範囲内にあるマルチキャスト トラフィックは、このインターフェイスに出入りすることができません。したがって、このアドレス範囲内のマルチキャスト トラフィックに対するファイアウォールが提供されます。

（注）　マルチキャスト境界および TTL スレッシュホールドは、マルチキャスト ドメインのスコープを制御しますが、TTL スレッシュホールドはこのスイッチでサポートされません。ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限するには、TTL スレッシュホールドではなくマルチキャスト境界を使用する必要があります。

図 49-7 に、XYZ 社が自社ネットワーク周辺にあるすべてのルーテッド インターフェイス上で、管理用スコープの境界をマルチキャスト アドレス範囲 239.0.0.0/8 に設定した例を示します。この境界では、239.0.0.0 ～ 239.255.255.255 の範囲のマルチキャスト トラフィックは、ネットワークに入ることやそこから出ることができません。同様に、エンジニアリング部およびマーケティング部が、各自のネットワークの周辺で、管理用スコープの境界を 239.128.0.0/16 に設定しました。この境界では、239.128.0.0 ～ 239.128.255.255 の範囲のマルチキャスト トラフィックは、それぞれのネットワークに入ることやそこから出ることができません。

図 49-7　管理用スコープの境界



マルチキャスト グループ アドレスに対して、管理用スコープの境界をルーテッド インターフェイスに定義できます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。境界が定義されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過することができません。境界を使用することにより、異なる管理ドメイン内で同じマルチキャスト グループ アドレスを再利用できます。

IANA は、マルチキャスト アドレス範囲 239.0.0.0 ～ 239.255.255.255 を管理用スコープのアドレスとして指定しました。このアドレス範囲は、異なる組織が管理するドメイン内で再利用できます。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

管理用スコープの境界を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip multicast boundary** *access-list-number*	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

境界を削除するには、**no ip multicast boundary** インターフェイス コンフィギュレーション コマンドを使用します。

次に、すべての管理用スコープのアドレスに対して境界を設定する例を示します。

```
Switch(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Switch(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip multicast boundary 1
```

基本的な DVMRP 相互運用性機能の設定

ここでは、次の設定情報について説明します。

- 「DVMRP 相互運用性の設定」（P.49-50）（任意）
- 「DVMRP トンネルの設定」（P.49-52）（任意）
- 「DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ」（P.49-54）（任意）
- 「mrinfo 要求への応答」（P.49-55）（任意）

高度な DVMRP 機能の詳細については、「高度な DVMRP 相互運用性機能の設定」（P.49-55）を参照してください。

DVMRP 相互運用性の設定

PIM を使用するシスコ製マルチキャスト ルータおよびマルチレイヤ スイッチは、DVMRP を使用する他社製のマルチキャスト ルータとの相互運用が可能になります。

PIM 装置は、DVMR プローブ メッセージを待ち受け、接続されたネットワーク上にある DVMRP マルチキャスト ルータをダイナミックに検出します。DVMRP ネイバーが検出されると、PIM 装置は、PIM ドメイン内の到達可能なユニキャスト送信元をアドバタイズする DVMRP レポート メッセージを定期的に送信します。デフォルトでは、直接接続されたサブネットおよびネットワークがアドバタイズされます。装置は DVMRP ルータによって転送されたマルチキャスト パケットを転送し、次に、DVMRP ルータにマルチキャスト パケットを転送します。

MBONE に接続された PIM ルーテッド インターフェイスにアクセス リストを設定することで、DVMRP ルート レポート内でアドバタイズされるユニキャスト ルート数を制限できます。設定していない場合、ユニキャスト ルーティング テーブル内のすべてのルートがアドバタイズされます。

（注）　マルチキャスト ルーティングされたプロトコルは、DVMRP のパブリック ドメインの実装です。Cisco ルータおよびマルチレイヤ スイッチを DVMRP ルータに直接接続する場合、または MBONE トンネルを通して DVMRP ルータと相互運用する場合は、マルチキャスト ルーティングされたバージョン 3.8 を使用する必要があります（バージョン 3.8 には、DVMRP の非プルーニング バージョンが実装されています）。Cisco IOS ソフトウェアで作成された DVMRP アドバタイズを使用すると、古いバージョンのマルチキャスト ルーティングされたプロトコルにより、ルーティング テーブルやネイバーのルーティング テーブルが破壊されることがあります。

ip dvmrp metric インターフェイス コンフィギュレーション コマンドを設定することで、アドバタイズされる送信元、および使用されるメトリックを設定できます。特定のユニキャスト ルーティング プロセスによって学習されたすべての送信元を、DVMRP にアドバタイズするように指示することもできます。

DVMRP ルートレポート メッセージが送信されるときに、アドバタイズされる送信元と使用されるメトリックを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**interface** *interface-id*	MBONE に接続されている、マルチキャスト ルーティングがイネーブルであるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip dvmrp metric** *metric* [**list** *access-list-number*] [[*protocol process-id*] | [**dvmrp**]]	DVMRP レポートの一連の宛先に関連付けられているメトリックを設定します。 • *metric* に指定できる範囲は 0 ～ 32 です。0 の値は、ルートがアドバタイズされないことを意味します。32 の値は、無限（到達不能）を意味します。 • （任意）**list** *access-list-number* には、ステップ 2 で作成したアクセス リストを入力します。指定されている場合は、アクセス リストと一致するマルチキャスト宛先だけが、設定されたメトリックとともにレポートされます。 • （任意）*protocol process-id* には、**eigrp**、**igrp**、**ospf**、**rip**、**static**、または **dvmrp** などのユニキャスト ルーティング プロトコルの名前と、ルーティング プロトコルのプロセス ID 番号を入力します。指定されている場合は、指定されたルーティング プロトコルによって学習されたルートだけが、DVMRP レポート メッセージでアドバタイズされます。 • （任意）指定されている場合は、**dvmrp** キーワードにより、設定された *metric* を使用して DVMRP ルーティング テーブルのルートをアドバタイズしたり、フィルタリングできます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

メトリックまたはルート マップをディセーブルにするには、**no ip dvmrp metric** *metric* [**list** *access-list-number*] [[*protocol process-id*] | [**dvmrp**]] または **no ip dvmrp metric** *metric* **route-map** *map-name* インターフェイス コンフィギュレーション コマンドを使用します。

より詳細な方法で上記コマンドと同じ結果を得るには、アクセス リストの代わりに、ルート マップ（**ip dvmrp metric** *metric* **route-map** *map-name* インターフェイス コンフィギュレーション コマンド）を使用します。ユニキャスト ルートが DVMRP に入る前に、ルート マップ条件にユニキャスト ルートを適用します。

次に、PIM 装置および DVMRP ルータが同じネットワーク セグメントにある場合に、DVMRP 相互運用性を設定する例を示します。この例では、アクセス リスト 1 はネットワーク（198.92.35.0、198.92.36.0、198.92.37.0、131.108.0.0、および 150.136.0.0）を DVMRP ルータにアドバタイズし、アクセス リスト 2 は他のすべてのネットワークのアドバタイズを禁止します（**ip dvmrp metric 0** インターフェイス コンフィギュレーション コマンド）。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip address 131.119.244.244 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config-if)# ip dvmrp metric 1 list 1
Switch(config-if)# ip dvmrp metric 0 list 2
Switch(config-if)# exit
Switch(config)# access-list 1 permit 198.92.35.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.36.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
Switch(config)# access-list 1 permit 131.108.0.0 0.0.255.255
Switch(config)# access-list 1 permit 150.136.0.0 0.0.255.255
Switch(config)# access-list 1 deny   0.0.0.0 255.255.255.255
Switch(config)# access-list 2 permit 0.0.0.0 255.255.255.255
```

DVMRP トンネルの設定

ソフトウェアは MBONE への DVMRP トンネルをサポートしています。一端で DVMRP が動作しているルータまたはマルチレイヤ スイッチには、DVMRP トンネルを設定できます。これにより、ソフトウェアはトンネルを介してマルチキャスト パケットを送受信します。この方法によって、パス上のすべてのルータでマルチキャスト ルーティングがサポートされていない場合でも、PIM ドメインを DVMRP ルータに接続できます。2 つのルータ間で DVMRP トンネルを設定できません。

Cisco ルータまたはマルチレイヤ スイッチがトンネルを介して DVMRP を実行している場合は、DVMRP レポート メッセージ内の送信元が、実際のネットワークと同様にアドバタイズされます。また、受信した DVMRP レポート メッセージはキャッシュに格納され、RPF 計算に使用されます。この動作により、トンネルを介して受信されたマルチキャスト パケットの転送をイネーブルにします。

次の場合は、DVMRP トンネルの設定時に IP アドレスをトンネルに割り当てる必要があります。

- トンネルを介して IP パケットを送信する場合
- DVMRP サマライズを実行するようにソフトウェアを設定する場合

トンネルとサブネットのネットワーク番号が異なる場合、サブネットはトンネルを介してアドバタイズされません。この場合は、ネットワーク番号だけがトンネルを介してアドバタイズされます。

DVMRP トンネルを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**interface tunnel** *number*	トンネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**tunnel source** *ip-address*	トンネル インターフェイスの送信元アドレスを指定します。スイッチのインターフェイスの IP アドレスを入力します。
ステップ 5	**tunnel destination** *ip-address*	トンネル インターフェイスの宛先アドレスを指定します。マルチキャスト ルーティングされたルータの IP アドレスを入力します。
ステップ 6	**tunnel mode dvmrp**	DVMRP へのトンネルに対してカプセル化モードを設定します。
ステップ 7	**ip address** *address mask* または **ip unnumbered** *type number*	インターフェイスに IP アドレスを割り当てます。 または インターフェイスを番号付けせずに設定します。
ステップ 8	**ip pim** [**dense-mode** | **sparse-mode**]	インターフェイスに PIM モードを設定します。
ステップ 9	**ip dvmrp accept-filter** *access-list-number* [*distance*] **neighbor-list** *access-list-number*	着信 DVMRP レポートに対して許可フィルタを設定します。 デフォルトでは、距離が 0 のすべての宛先レポートが許可されます。すべてのネイバーからのレポートが許可されます。 • *access-list-number* には、ステップ 2 で作成したアクセス リスト番号を指定します。アクセス リストに一致するすべての送信元は、距離とともに DVMRP ルーティング テーブルに格納されます。 • （任意）*distance* には、宛先への管理ディスタンスを入力します。デフォルトでは、DVMRP ルートへの管理ディスタンスは 0 で、ユニキャスト ルーティング テーブル ルートよりも優先されます。送信元へのパスが、1 つはユニキャスト ルーティングによるパス（マルチキャスト ルーティング プロトコルとして PIM を使用）、もう 1 つは DVMRP を使用するパスの 2 つのパスである場合、PIM パスを使用するときは、DVMRP ルートの管理ディスタンスを増加させます。指定できる範囲は 1 ～ 255 です。 • **neighbor-list** *access-list-number* には、ステップ 2 で作成したネイバー リストの番号を入力します。DVMRP レポートは、リスト内のネイバーでだけ許可されます。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	**show running-config**	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フィルタをディセーブルにするには、**no ip dvmrp accept-filter** *access-list-number* [*distance*] **neighbor-list** *access-list-number* インターフェイス コンフィギュレーション コマンドを使用します。

次に、DVMRP トンネルを設定する例を示します。この設定では、Cisco スイッチ上のトンネルの IP アドレスに *unnumbered* が割り当てられます。これにより、トンネルにはポート 1 と同じ IP アドレスが設定されます。トンネルのエンドポイント送信元アドレスは 172.16.2.1 になり、トンネルの接続先であるリモート DVMRP ルータのトンネルのエンドポイント アドレスは 192.168.1.10 になります。トンネルを介して送信されるすべてのパケットは、外部 IP ヘッダーにカプセル化されます。Cisco スイッチは 198.92.37.0 ～ 198.92.37.255 への距離が 100 である着信 DVMRP レポートを受信するように設定されます。

```
Switch(config)# ip multicast-routing
Switch(config)# interface tunnel 0
Switch(config-if)# ip unnumbered gigabitethernet1/1
Switch(config-if)# ip pim dense-mode
Switch(config-if)# tunnel source gigabitethernet1/1
Switch(config-if)# tunnel destination 192.168.1.10
Switch(config-if)# tunnel mode dvmrp
Switch(config-if)# ip dvmrp accept-filter 1 100
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# ip address 172.16.2.1 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config)# exit
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
```

DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ

使用しているスイッチがマルチキャスト ルーティング バージョン 3.6 の装置のネイバーである場合は、ネットワーク 0.0.0.0（デフォルト ルート）を DVMRP ネイバーにアドバタイズするように、ソフトウェアを設定できます。DVMRP デフォルト ルートでは、具体的なルートと一致しないマルチキャスト送信元の RPF 情報が計算されます。

DVMRP のデフォルト ルートを MBONE にアドバタイズしないでください。

インターフェイスの DVMRP ネイバーにネットワーク 0.0.0.0 をアドバタイズするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ip dvmrp default-information** {**originate** | **only**}	DVMRP ネイバーにネットワーク 0.0.0.0 をアドバタイズします。 このコマンドは、スイッチがマルチキャスト ルーティングバージョン 3.6 マシンのネイバーである場合に限り使用します。 キーワードの意味は次のとおりです。 • **originate** : 0.0.0.0 以外の具体的なルートもアドバタイズできるように指定します。 • **only** : 0.0.0.0 以外の DVMRP ルートがアドバタイズされないように指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト ルートのアドバタイズを禁止するには、**no ip dvmrp default-information** インターフェイス コンフィギュレーション コマンドを使用します。

mrinfo 要求への応答

ソフトウェアは、マルチキャスト ルーティングされたシステム、Cisco ルータ、およびマルチレイヤ スイッチによって送信された mrinfo 要求に応答します。ソフトウェアは、DVMRP トンネルとすべてのルーテッド インターフェイスを介してネイバーに関する情報を戻します。この情報には、メトリック（常に 1 に設定）、設定された TTL スレッショルド、インターフェイスのステータス、およびさまざまなフラグが含まれます。次の例に示すように、**mrinfo** 特権 EXEC コマンドを使用して、ルータまたはスイッチ自体をクエリーすることもできます。

```
Switch# mrinfo
  171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
  171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
  171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
  171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
  171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
  171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
  171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
  171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
  171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

高度な DVMRP 相互運用性機能の設定

Cisco ルータおよびマルチレイヤ スイッチは PIM を実行し、マルチキャスト パケットをレシーバーに転送し、送信元から受信します。DVMRP ルートを PIM クラウド内に伝播したり、PIM クラウドを経由して伝播することもできます。PIM はこの情報を使用しますが、Cisco ルータおよびマルチレイヤ スイッチでは、DVMRP を実装してマルチキャスト パケットを転送することはありません。

ここでは、次の設定情報について説明します。

- 「DVMRP ユニキャスト ルーティングのイネーブル化」（P.49-56）（任意）
- 「DVMRP の非プルーニング ネイバーの拒否」（P.49-57）（任意）
- 「ルート交換の制御」（P.49-59）（任意）

基本的な DVMRP 機能の詳細については、「基本的な DVMRP 相互運用性機能の設定」（P.49-50）を参照してください。

DVMRP ユニキャスト ルーティングのイネーブル化

マルチキャスト ルーティングおよびユニキャスト ルーティングには個別のトポロジが必要となるため、PIM はマルチキャスト トポロジに従って、ループのない分散ツリーを構築する必要があります。Cisco ルータ、マルチレイヤ スイッチ、およびマルチキャスト ルーティング ベースのマシンは、DVMRP ユニキャスト ルーティングを使用して、DVMRP ユニキャスト ルートを交換します。PIM はこれらのルートにリバースパスを転送できます。

シスコ デバイスは DVMRP マルチキャスト ルーティングを相互に実行しませんが、DVMRP ルートを交換できます。DVMRP ルートは、ユニキャスト トポロジと異なるマルチキャスト トポロジを提供します。これにより、マルチキャスト トポロジを通して PIM を実行し、この結果 MBONE トポロジを通した PIM sparse（疎）モードがイネーブルになります。

DVMRP ユニキャスト ルーティングがイネーブルの場合、ルータまたはスイッチは、DVMRP ルーティング テーブル内の DVMRP レポート メッセージで学習されたルートをキャッシュに格納します。PIM を実行中の場合、これらのルートはユニキャスト ルーティング テーブル内のルートよりも優先される場合があります。そのため、MBONE トポロジがユニキャスト トポロジと異なる場合、PIM を MBONE トポロジで実行することが可能になります。

DVMRP ユニキャスト ルーティングは、すべてのインターフェイスで実行できます。DVMRP トンネルの場合は、DVMRP マルチキャスト ルーティングが使用されます。この機能を使用しても、Cisco ルータおよびマルチレイヤ スイッチ間で DVMRP マルチキャスト ルーティングはイネーブルになりません。ただし、DVMRP 対応マルチキャスト ルータがある場合は、シスコ デバイスで PIM/DVMRP マルチキャスト ルーティングを実行できます。

DVMRP ユニキャスト ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

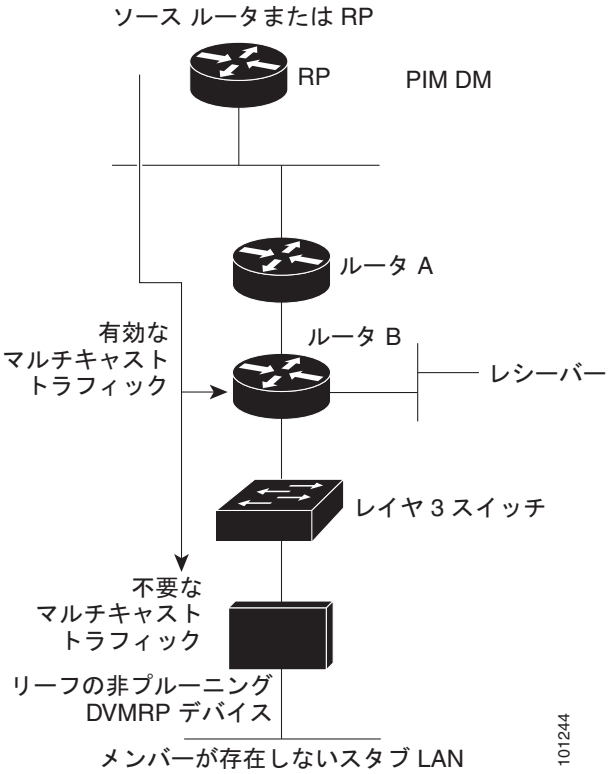
	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip dvmrp unicast-routing**	DVMRP ユニキャスト ルーティングをイネーブルにします（DVMRP ルートを送受信します）。デフォルトでは、この機能はディセーブルになっています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

この機能をディセーブルにするには、**no ip dvmrp unicast-routing** インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP の非プルーニング ネイバーの拒否

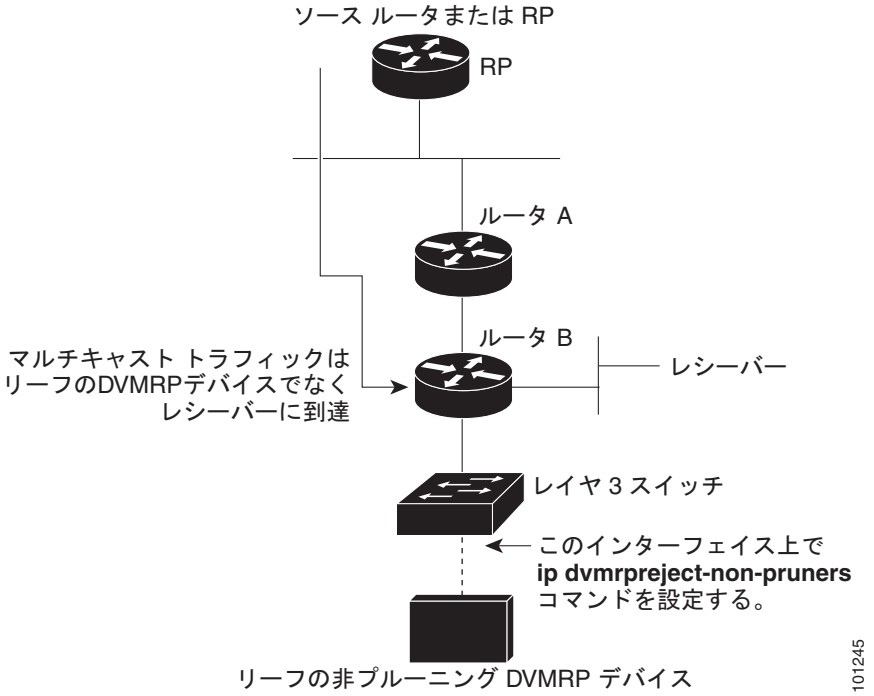
デフォルトでは、DVMRP 機能にかかわらず、シスコ デバイスはすべての DVMRP ネイバーをピアとして受け入れます。ただし、一部の非シスコ デバイスでは、プルーニングできない古いバージョンの DVMRP が実行されているため、転送パケットを常時受信し、帯域幅を浪費します。図 49-8 に、このシナリオを示します。

図 49-8　リーフの非プルーニング DVMRP ネイバー



DVMRP ネイバーで DVMRP プルーニングまたは接合がサポートされていない場合、スイッチとこのネイバーとのピアリング（通信）を防止できます。これを行うには、非プルーニング マシンに接続されたインターフェイスで **ip dvmrp reject-non-pruners** インターフェイス コンフィギュレーション コマンドを使用し、スイッチ（リーフの非プルーニング DVMRP マシンのネイバー）を設定します（図 49-9 を参照）。この場合、スイッチがプルーニング対応フラグの設定されていない DVMRP プローブまたはレポート メッセージを受信すると、Syslog メッセージが記録され、メッセージが廃棄されます。

図 49-9　ルータが非プルーニング DVMRP ネイバーを拒否する例



ip dvmrp reject-non-pruners インターフェイス コンフィギュレーション コマンドを使用すると、ネイバーとのピアリングだけが防止されます。（レシーバー候補へのダウンストリーム方向に）数ホップ離れた拒否されていない非プルーニング ルータが存在する場合、非プルーニング DVMRP ネットワークが存在する場合があります。

非プルーニング DVMRP ネイバーとのピアリングを防止するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	非プルーニング DVMRP ネイバーに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip dvmrp reject-non-pruners**	非プルーニング DVMRP ネイバーとのピアリングを防止します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

この機能をディセーブルにするには、**no ip dvmrp reject-non-pruners** インターフェイス コンフィギュレーション コマンドを使用します。

ルート交換の制御

ここでは、DVMRP ルートに関するシスコ デバイスのアドバタイズを調整する方法について説明します。

- 「アドバタイズされる DVMRP ルート数の制限」（P.49-59）（任意）
- 「DVMRP ルート スレッシュホールドの変更」（P.49-59）（任意）
- 「DVMRP サマリー アドレスの設定」（P.49-60）（任意）
- 「DVMRP 自動サマライズのディセーブル化」（P.49-62）（任意）
- 「DVMRP ルートへのメトリック オフセットの追加」（P.49-62）（任意）

アドバタイズされる DVMRP ルート数の制限

デフォルトでは、DVMRP を実行するためにイネーブル化されたインターフェイス（つまり、DVMRP トンネル、DVMRP ネイバーが検出されたインターフェイス、または **ip dvmrp unicast-routing** インターフェイス コンフィギュレーション コマンドを実行するように設定されたインターフェイス）を介して、7000 DVMRP ルートだけがアドバタイズされます。

DVMRP ルートの制限を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dvmrp route-limit** *count*	DVMRP に対してイネーブル化されたインターフェイスを介してアドバタイズされる DVMRP ルート数を変更します。 このコマンドを使用すると、**ip dvmrp metric** インターフェイス コンフィギュレーション コマンドの設定ミスによって大量のルートが MBONE に入るのを防ぐことができます。 デフォルトでは、7000 のルートがアドバタイズされます。指定できる範囲は 0 ～ 4294967295 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルート数が制限されないように設定するには、**no ip dvmrp route-limit** グローバル コンフィギュレーション コマンドを使用します。

DVMRP ルート スレッシュホールドの変更

デフォルトでは、1 つのインターフェイスにつき、1 分間に 10,000 の DVMRP ルートを受信できます。この速度を超えると、ルート サージが発生した可能性を警告する Syslog メッセージが発行されます。この警告は、通常、装置の設定ミスによって大量のルートが MBONE に入った場合に、短時間で検出を行うために使用されます。

警告をトリガーするルート数のスレッシュホールドを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dvmrp routehog-notification** *route-count*	Syslog メッセージをトリガーするルート数を設定します。 デフォルト値は 10,000 ルートです。指定できる範囲は 1 ～ 4294967295 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip dvmrp routehog-notification** グローバル コンフィギュレーション コマンドを使用します。

動作中のルート数を表示するには、**show ip igmp interface** 特権 EXEC コマンドを使用します。このルート数を超えると、*** *ALERT* *** が行に追加されます。

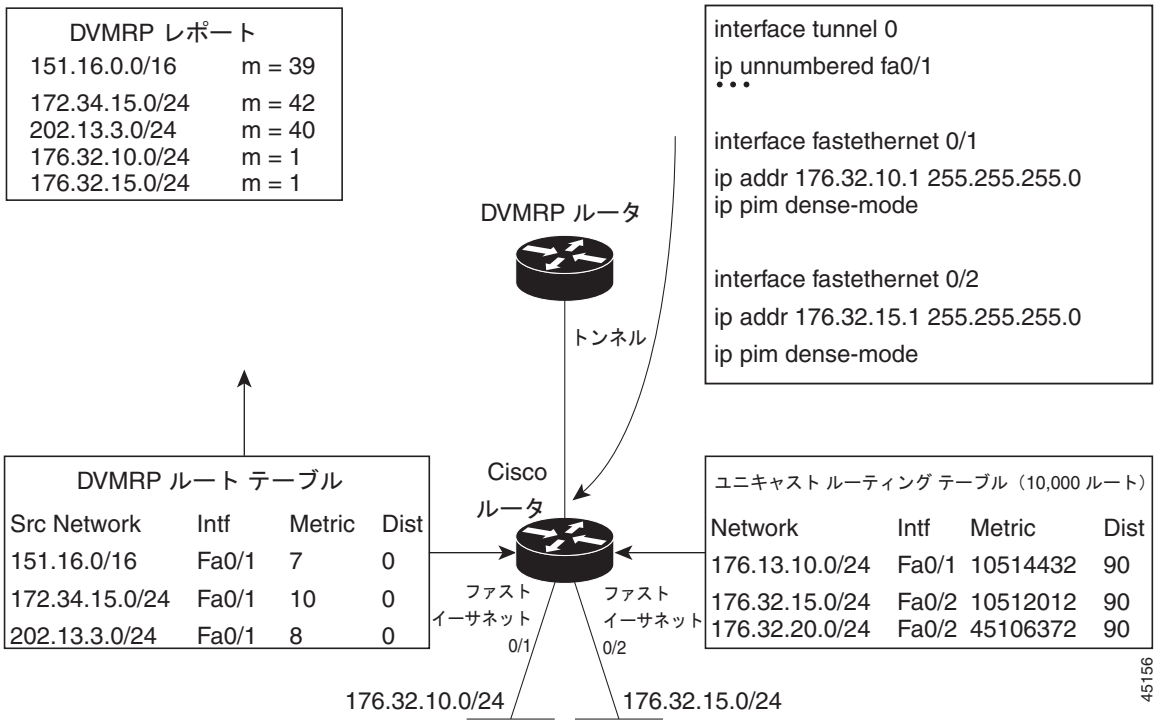
DVMRP サマリー アドレスの設定

デフォルトでは、シスコ デバイスは、ユニキャスト ルーティング テーブル内の接続されたユニキャスト ルートだけ（つまり、ルータに直接接続されたサブネットへのルートだけ）を DVMRP ルート レポート メッセージでアドバタイズします。これらのルートでは、通常の DVMRP のクラスフル ルート サマライズが行われます。このプロセスは、アドバタイズされているルートと、ルートがアドバタイズで経由するインターフェイスが、同じクラスフル ネットワーク内にあるかどうかによって異なります。

図 49-10 に、デフォルト動作の例を示します。この例では、Cisco ルータによって送信される DVMRP レポートに、DVMRP ルータから受信した 3 つの元のルートが含まれています。この DVMRP ルータは、DVMRP メトリックに 32 を追加してポイズンリバースされたものです。これらのルートのあとに、ユニキャスト ルーティング テーブルから取得した、直接接続された 2 つのネットワーク（176.32.10.0/24 および 176.32.15.0/24）のアドバタイズである 2 つのルートがリストされています。DVMRP トンネルはファスト イーサネット ポート 1 と同じ IP アドレスを共有し、直接接続された 2 つのサブネットと同じクラス B ネットワークに分類されるため、これらのルートに対するクラスフル サマライズは実行されません。そのため、DVMRP ルータは、直接接続されたサブネットにこれらの 2 つのルートだけをポイズンリバースし、これらの 2 つのイーサネット セグメント上の送信元によって送信されたマルチキャスト トラフィックに対しては、RPF だけを適切に実行できます。これら 2 つのイーサネット セグメント上にはない、Cisco ルータ背後のネットワーク内の他のマルチキャスト送信元では、DVMRP ルータで RPF チェックは適切に行われず、廃棄されます。

サマリー アドレス（**ip dvmrp summary-address** *address mask* インターフェイス コンフィギュレーション コマンドのアドレスおよびマスクのペアで指定）の範囲内にあるルートの代わりに、サマリー アドレスをアドバタイズするように Cisco ルータを設定できます。この範囲内にあるルートがユニキャスト ルーティング テーブルに少なくとも 1 つ含まれている場合は、サマリー アドレスが DVMRP ルート レポートで送信されます。それ以外の場合は、サマリー アドレスはアドバタイズされません。図 49-10 では、Cisco ルータのトンネル インターフェイスに **ip dvmrp summary-address** コマンドを設定します。そのため、Cisco ルータは、ユニキャスト ルーティング テーブルのネットワーク 176.32.0.0/16 に対し、サマライズされた単一のクラス B アドバタイズだけを送信します。

図 49-10　接続されたユニキャスト ルートだけアドバタイズ（デフォルト）する例



デフォルトのクラスフル自動サマライズがニーズを満たさない場合に DVMRP ルートのサマライズをカスタマイズするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

（注）　設定されたサマリー アドレスをアドバタイズする前に、ユニキャスト ルーティング テーブルに具体的なルートを少なくとも 1 つ設定する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション コマンドを入力します。
ステップ 3	**ip dvmrp summary-address** *address mask* [**metric** *value*]	DVMRP サマリー アドレスを指定します。 • **summary-address** *address mask* には、サマリー IP アドレス、および具体的なルートの代わりにアドバタイズされるマスクを指定します。 • （任意）**metric** *value* には、サマリー アドレスとともにアドバタイズされるメトリックを指定します。デフォルトは 1 です。指定できる範囲は 1 ～ 32 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

サマリー アドレスを削除するには、**no ip dvmrp summary-address** *address mask* [**metric** *value*] インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP 自動サマライズのディセーブル化

デフォルトでは、一部のレベルの DVMRP サマライズがソフトウェアで自動的に実行されます。サマリーだけではなくすべてのルートをアドバタイズする場合は、この機能をディセーブルにします。特別な場合には、すべてのサブネット情報が格納されたネイバー DVMRP ルータを使用して、DVMRP ネットワーク内のマルチキャスト トラフィック フローを詳細に制御できます。一例としては、PIM ネットワークが DVMRP クラウドに複数のポイントで接続されており、具体的な（集約されていない）ルートが DVMRP ネットワークに送信され、PIM クラウド内の各サブネットに対するさらに適切なパスがアドバタイズされる場合などがあります。

ip dvmrp summary-address インターフェイス コンフィギュレーション コマンドを設定し、**no ip dvmrp auto-summary** を設定しなかった場合は、カスタムと自動サマリーの両方を取得します。

DVMRP 自動サマライズをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no ip dvmrp auto-summary**	DVMRP 自動サマライズをディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

自動サマライズを再びイネーブルにするには、**ip dvmrp auto-summary** インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP ルートへのメトリック オフセットの追加

デフォルトでは、スイッチは着信 DVMRP レポートでアドバタイズされた DVMRP ルートのメトリック（ホップ カウント）を 1 つ増加させます。特定のルートの優先度を上下させる場合は、メトリックを変更できます。

たとえば、マルチレイヤ スイッチ A からルートが学習され、より大きなメトリックを持つ同じルートがマルチレイヤ スイッチ B から学習されたとします。スイッチ B を経由するパスの方が高速であるという理由でこのパスを使用する場合は、スイッチ A によって学習されたルートにメトリック オフセットを適用し、スイッチ B によって学習されたメトリックよりもメトリックを大きくすることで、スイッチ B を経由するパスを選択できます。

デフォルト メトリックを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip dvmrp metric-offset** [**in** | **out**] *increment*	着信レポートでアドバタイズされる DVMRP ルートに追加されたメトリックを変更します。 キーワードの意味は次のとおりです。 • （任意）**in**：増分値が着信 DVMRP レポートに追加され、mrinfo 応答で報告されるように指定します。 • （任意）**out**：増分値が DVMRP ルーティング テーブルのルートに対する発信 DVMRP レポートに追加されるように指定します。 **in** と **out** のどちらも指定されていない場合、**in** がデフォルトになります。 *increment* には、レポート メッセージでアドバタイズされる DVMRP ルータのメトリックに追加する値を指定します。指定できる範囲は 1 ～ 31 です。 **ip dvmrp metric-offset** コマンドがインターフェイス上で設定されていない場合、着信ルートのデフォルトの増分値は 1 となり、発信ルートのデフォルト値は 0 になります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip dvmrp metric-offset** インターフェイス コンフィギュレーション コマンドを使用します。

IP マルチキャスト ルーティングのモニタおよびメンテナンス

ここでは、IP マルチキャスト ルーティングをモニタする方法およびメンテナンスする方法について説明します。

- 「キャッシュ、テーブル、およびデータベースの消去」（P.49-64）
- 「システムおよびネットワーク統計情報の表示」（P.49-64）
- 「IP マルチキャスト ルーティングのモニタ」（P.49-65）

キャッシュ、テーブル、およびデータベースの消去

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の構造の内容が無効になる場合、または無効である疑いがある場合に、キャッシュ、テーブル、またはデータベースを消去する必要があります。

表 49-5 に示す特権 EXEC コマンドのいずれかを使用すると、IP マルチキャストのキャッシュ、テーブル、データベースを消去できます。

表 49-5　キャッシュ、テーブル、およびデータベースを消去するためのコマンド

コマンド	目的
clear ip cgmp	Catalyst スイッチによってキャッシュされたすべてのグループ エントリを消去します。
clear ip dvmrp route {***** | *route*}	DVMRP ルーティング テーブルからルートを削除します。
clear ip igmp group [*group-name* | *group-address* | *interface*]	IGMP キャッシュからエントリを削除します。
clear ip mroute {***** | *group* [*source*]}	IP マルチキャスト ルーティング テーブルからエントリを削除します。
clear ip pim auto-rp *rp-address*	Auto-RP キャッシュを消去します。
clear ip sdr [*group-address* | "*session-name*"]	Session Directory Protocol バージョン 2 キャッシュまたは sdr キャッシュ エントリを削除します。

システムおよびネットワーク統計情報の表示

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注） このリリースは、ルート単位の統計情報をサポートしません。

また、リソース使用量を学習したり、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、装置のパケットがネットワーク上で通過するルーティング パスを検出することもできます。

表 49-6 に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 49-6　システムおよびネットワーク統計情報を表示するためのコマンド

コマンド	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレスに ICMP エコー要求を送信します。
show ip dvmrp route [*ip-address*]	DVMRP ルーティング テーブルのエントリを表示します。
show ip igmp groups [*group-name* | *group-address* | *type number*]	スイッチに直接接続され、IGMP を通じて学習されたマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	インターフェイスについてのマルチキャスト関連情報を表示します。

表 49-6　システムおよびネットワーク統計情報を表示するためのコマンド （続き）

コマンド	目的
show ip mcache [*group* [*source*]]	IP 高速スイッチング キャッシュの内容を表示します。
show ip mpacket [*source-address* | *name*] [*group-address* | *name*] [**detail**]	循環キャッシュヘッダー バッファの内容を表示します。
show ip mroute [*group-name* | *group-address*] [*source*] [**summary**] [**count**] [**active** *kbps*]	IP マルチキャスト ルーティング テーブルの内容を表示します。
show ip pim interface [*type number*] [**count**] [**detail**]	PIM 用に設定されたインターフェイスの情報を表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip pim neighbor [*type number*]	スイッチによって検出された PIM ネイバーのリストを示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip pim rp [*group-name* | *group-address*]	sparse（疎）モードのマルチキャスト グループに関連付けられた RP ルータを表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip rpf {*source-address* | *name*}	スイッチが Reverse Path Forwarding（RPF）を実行する方法（つまり、ユニキャスト ルーティング テーブルから、DVMRP ルーティング テーブルから、またはスタティック マルチキャスト ルーティングからのいずれか）を表示します。
show ip sdr [*group* | “*session-name*” | **detail**]	Session Directory Protocol バージョン 2 のキャッシュを表示します。

IP マルチキャスト ルーティングのモニタ

表 49-7 に示す特権 EXEC コマンドを使用すると、IP マルチキャスト ルータ、パケット、パスをモニタできます。

表 49-7　IP マルチキャスト ルーティングをモニタするためのコマンド

コマンド	目的
mrinfo [*hostname* | *address*] [*source-address* | *interface*]	マルチキャスト ルータまたはマルチレイヤ スイッチとピアリングしているネイバー マルチキャスト装置を特定するために、そのマルチキャスト ルータまたはマルチレイヤ スイッチをクエリーします。
mstat *source* [*destination*] [*group*]	IP マルチキャスト パケットのレートおよび損失情報を表示します。
mtrace *source* [*destination*] [*group*]	指定されたグループのマルチキャスト分散ツリーに対して、送信元から宛先ブランチへのパスを追跡します。

CHAPTER 50

MSDP の設定

この章では、IE 3000 スイッチに Multicast Source Discovery Protocol（MSDP）を設定する手順について説明します。MSDP により、複数の Protocol-Independent Multicast Sparse-Mode（PIM-SM; Protocol-Independent Multicast sparse（疎）モード）ドメインが接続されます。

このソフトウェア リリースでは、MSDP と密接に連携する Multicast Border Gateway Protocol（MBGP）がサポートされていないため、MSDP は完全にはサポートされていません。ただし、MBGP が動作していない場合は、MSDP と連携して動作するデフォルト ピアを作成できます。

この機能を使用するには、スイッチが IP サービス イメージを実行している必要があります。

（注） この章で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』を参照してください。

この章で説明する内容は、次のとおりです。

MSDP の概要

MSDP を使用すると、さまざまなドメイン内のすべての Rendezvous Point（RP; ランデブー ポイント）に、グループのマルチキャスト送信元を通知できます。各 PIM-SM ドメインは独自の RP を使用し、他のドメインの RP には依存しません。RP は Transmission Control Protocol（TCP; 伝送制御プロトコル）を通じて MSDP を実行し、他のドメイン内のマルチキャスト送信元を検出します。

PIM-SM ドメイン内の RP は、他のドメイン内の MSDP 対応装置と MSDP ピアリング関係にあります。このピアリング関係は、TCP 接続を介して確立されます。この関係では、主に、マルチキャスト グループの送信元のリストが交換されます。RP 間の TCP 接続は、基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送信元パスを確立します。

このトポロジの目的は、ドメインが他のドメイン内のマルチキャスト送信元を検出できるようにすることです。レシーバーが配置されているドメインをマルチキャスト送信元が対象としている場合、マルチキャスト データは PIM-SM の通常の送信元ツリー構築メカニズムを通じて配信されます。MSDP は、グループの送信元をアナウンスする場合にも使用します。このアナウンスは、ドメインの RP で発信する必要があります。

MSDP のドメイン間の動作は、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）または MBGP に大きく依存します。ドメイン内の RP（グローバル グループの送信元をインターネットにアナウンスするための RP）で、MSDP を実行することを推奨します。

MSDP の動作

図 50-1 に、2 つの MSDP ピア間での MSDP の動作を示します。Protocol Independent Multicast（PIM）では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP を使用します。MSDP が設定されている場合、次のシーケンスが発生します。

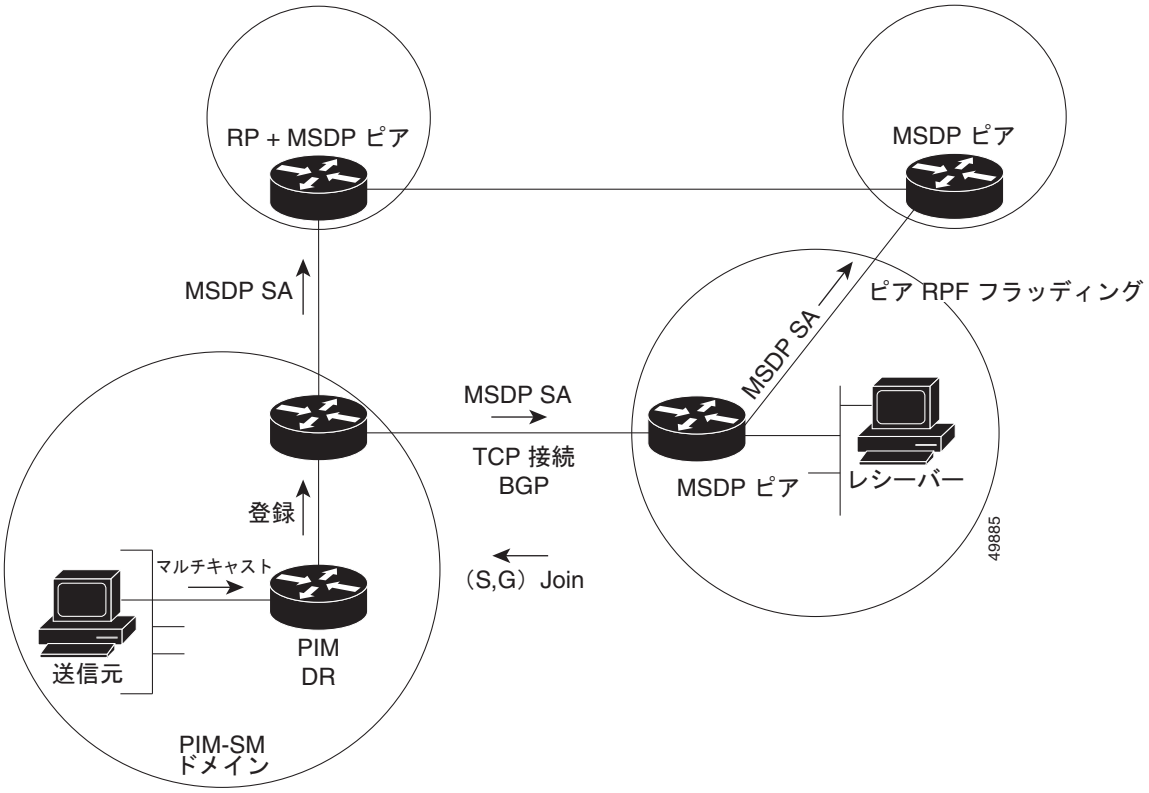
送信元が最初のマルチキャスト パケットを送信すると、送信元に直接接続されたファーストホップ ルータ（*指定ルータ*または RP）が PIM 登録メッセージを RP に送信します。RP は、この登録メッセージを使用し、アクティブな送信元を登録したり、ローカル ドメイン内の共有ツリーの下方向にマルチキャスト パケットを転送します。MSDP が設定されている場合は、Source-Active（SA）メッセージもすべての MSDP ピアに転送されます。送信元、送信元の送信先グループ、および RP のアドレスまたは送信元 ID（RP アドレスとして使用されるインターフェイスの IP アドレス）が設定されている場合は、SA メッセージによってこれらが識別されます。

各 MSDP ピアは SA メッセージを発信元 RP から受信および転送し、ピア Reverse-Path Flooding（RPF）を実現します。MSDP 装置は、BGP または MBGP ルーティング テーブルを調べ、SA メッセージの発信元 RP へのネクストホップであるピアを検出します。このようなピアは、*Reverse-Path Forwarding*（RPF）ピアと呼びます。MSDP 装置は、RPF ピア以外のすべての MSDP ピアにメッセージを転送します。BGP および MBGP がサポートされていない場合に MSDP ピアを設定する方法については、「デフォルトの MSDP ピアの設定」（P.50-4）を参照してください。

MSDP ピアは、非 RPF ピアから発信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージを廃棄します。それ以外の場合、MSDP ピアは、すべての MSDP ピアにメッセージを転送します。

ドメインの RP は、MSDP ピアからの SA メッセージを受信します。SA メッセージに記述されたグループの Join 要求を RP が受信し、空でない出力インターフェイス リストに（*,G）エントリが存在する場合、そのグループはドメインの対象となり、RP は（S,G）Join を送信元にトリガーします。（S,G）Join が送信元の Designated Router（DR; 指定ルータ）に到達すると、送信元ツリーのブランチが送信元からリモート ドメイン内の RP に構築されます。この結果、マルチキャスト トラフィックを送信元から送信元ツリーを経由して RP へ、そしてリモート ドメイン内の共有ツリーを下ってレシーバーへと送信できます。

図 50-1　RP ピア間での MSDP の動作



MSDP の利点

MSDP には、次のような利点があります。

- 共有のマルチキャスト分散ツリーが分割されるので、共有ツリーがドメインに対してローカルになるように設定できます。ローカル メンバーはローカル ツリーに加わります。共有ツリーへの Join メッセージをドメイン外に送信する必要はありません。
- PIM sparse（疎）モード ドメインは独自の RP だけに依存するため、他のドメインの RP に対する依存度は低くなります。このため、送信元の情報がドメイン外部に漏れないようにすることができ、セキュリティが高まります。
- レシーバーだけが配置されているドメインは、グループ メンバーシップをグローバルにアドバタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャスト ルーティング テーブル ステートが必要ないので、メモリを節約できます。

MSDP の設定

ここでは、次の設定情報について説明します。

- 「MSDP のデフォルト設定」（P.50-4）
- 「デフォルトの MSDP ピアの設定」（P.50-4）（必須）
- 「Source-Active ステートのキャッシング」（P.50-6）（任意）

- 「MSDP ピアからの送信元情報の要求」（P.50-8）（任意）
- 「スイッチから発信される送信元情報の制御」（P.50-8）（任意）
- 「スイッチから転送される送信元情報の制御」（P.50-11）（任意）
- 「スイッチで受信される送信元情報の制御」（P.50-13）（任意）
- 「MSDP メッシュ グループの設定」（P.50-15）（任意）
- 「MSDP ピアのシャットダウン」（P.50-15）（任意）
- 「MSDP への境界 PIM dense（密）モード領域の追加」（P.50-16）（任意）
- 「RP アドレス以外の発信元アドレスの設定」（P.50-17）（任意）

MSDP のデフォルト設定

MSDP はイネーブルになっておらず、デフォルトの MSDP ピアは存在しません。

デフォルトの MSDP ピアの設定

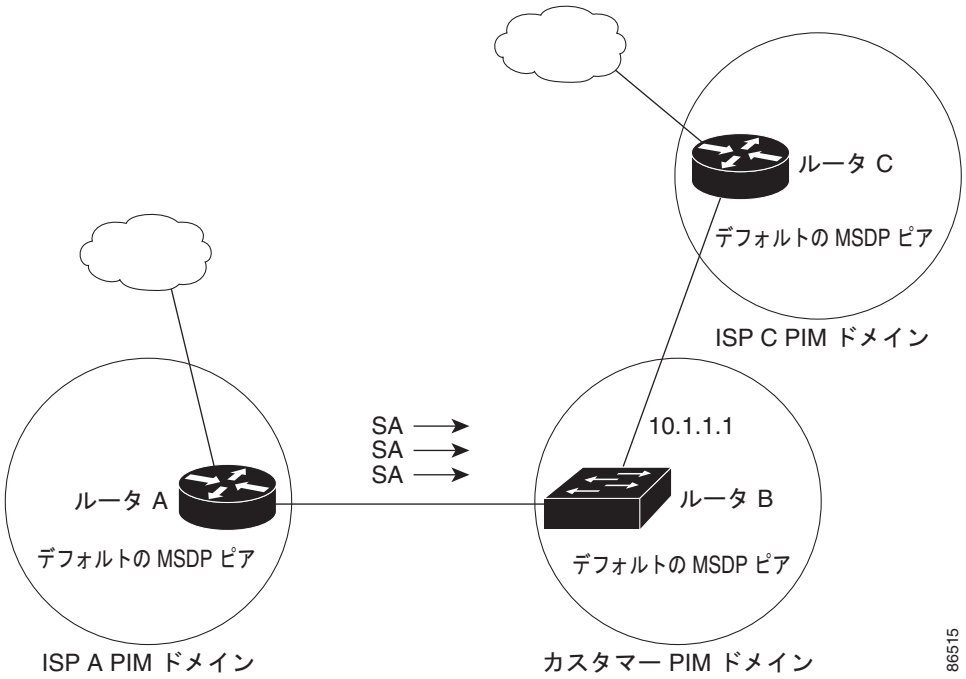
このソフトウェア リリースでは、BGP および MBGP がサポートされていないため、**ip msdp peer** グローバル コンフィギュレーション コマンドを使用して、ローカル スイッチに MSDP ピアを設定できません。代わりに、（**ip msdp default-peer** グローバル コンフィギュレーション コマンドを使用して）デフォルトの MSDP ピアを定義します。このピアでは、スイッチのすべての SA メッセージを受信します。デフォルトの MSDP ピアには、事前に設定済みの MSDP ピアを使用する必要があります。MSDP ピアによる BGP または MBGP ピアリングをスイッチが行わない場合、デフォルトの MSDP ピアを設定します。単一の MSDP ピアが設定されている場合、スイッチはそのピアから常にすべての SA メッセージを受信します。

図 50-2 に、デフォルトの MSDP ピアを使用したネットワークの例を示します。図 50-2 では、スイッチ B を所有するカスタマーが、2 つの Internet Service Provider（ISP; インターネット サービス プロバイダー）に接続されています。一方の ISP はルータ A、もう一方の ISP はルータ C を所有しています。これらの ISP 間では、BGP または MBGP は動作していません。ISP のドメイン内、または他のドメイン内の送信元を学習するために、カスタマー サイトのスイッチ B はルータ A をデフォルトの MSDP ピアとして識別します。スイッチ B は、ルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、受信するのはルータ A またはルータ C のどちらか一方の SA メッセージだけです。コンフィギュレーション ファイルでルータ A が最初に記述されている場合、ルータ A が動作していると、ルータ A が使用されます。ルータ A が動作していない場合にだけ、スイッチ B はルータ C からの SA メッセージを受信します。これが、プレフィクス リストを指定しない場合のデフォルトの動作です。

プレフィクス リストを指定すると、ピアはリスト内のプレフィクスに対してだけデフォルト ピアになります。プレフィクス リストが各デフォルト ピアに関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。プレフィクス リストを指定しなくても、複数のデフォルト ピアを設定することは可能です。ただし、最初のピアにルータが接続されていて、このピアが動作している限り、アクティブなデフォルト ピアになるのは最初のピアだけです。最初に設定したピアに障害が発生したり、このピアへの接続に障害が発生した場合、2 番めに設定したピアがアクティブなデフォルト ピアになります。以降、アクティブなデフォルト ピアに障害が発生すると、そのピアの次に設定したピアがアクティブなデフォルト ピアになります。

ISP は通常、プレフィクス リストを使用して、カスタマーのルータから受信するプレフィクスを定義します。

図 50-2　デフォルトの MSDP ピア ネットワーク



デフォルトの MSDP ピアを指定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp default-peer** *ip-address* | *name* [**prefix-list** *list*]	すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。 • *ip-address* | *name* には、MSDP デフォルト ピアの IP アドレスまたは Domain Name System（DNS; ドメイン ネーム システム）サーバ名を入力します。 • （任意）**prefix-list** *list* には、リストされたプレフィクスに対してだけデフォルト ピアとなるピアを指定するリスト名を入力します。プレフィクス リストが各デフォルト ピアに関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 **prefix-list** キーワードを指定して複数の **ip msdp default-peer** コマンドを入力すると、すべてのデフォルト ピアが複数の RP プレフィクスに対して同時に使用されます。この構文は通常、スタブ サイト クラウドに接続されたサービス プロバイダー クラウドで使用されます。 **prefix-list** キーワードを指定せずに複数の **ip msdp default-peer** コマンドを入力すると、すべての SA メッセージが単一のアクティブ ピアで受信されます。このピアに障害が発生した場合、このピアの次に設定したデフォルト ピアがすべての SA メッセージを受信します。この構文は通常、スタブ サイトで使用されます。

	コマンド	目的
ステップ 3	**ip prefix-list** *name* [**description** *string*] | **seq** *number* {**permit** | **deny**} *network length*	（任意）ステップ 2 で指定した名前を使用し、プレフィクス リストを作成します。 • （任意）**description** *string* には、このプレフィクス リストの説明を最大 80 文字で入力します。 • **seq** *number* には、エントリのシーケンス番号を入力します。指定できる範囲は 1 ～ 4294967294 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *network length* には、許可または拒否されるネットワーク マスクのネットワーク番号および長さ（ビット単位）を指定します。
ステップ 4	**ip msdp description** {*peer-name* | *peer-address*} *text*	（任意）指定したピアを設定内または **show** コマンド出力内で識別しやすいように、そのピアの説明を設定します。 デフォルトでは、MSDP ピアに説明は関連付けられていません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト ピアを削除するには、**no ip msdp default-peer** *ip-address* | *name* グローバル コンフィギュレーション コマンドを使用します。

次に、図 50-2 のルータ A とルータ C の設定の一部の例を示します。これらの各 ISP には、（図 50-2 のカスタマーと同様に）BGP または MBGP 以外のデフォルトのピアリングを使用する複数のカスタマーが存在します。この場合、これら 2 つの ISP の設定は類似したものになります。つまり、これらの ISP では、対応するプレフィクス リストで SA が許可されている場合、デフォルト ピアからの SA だけを受信します。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

Source-Active ステートのキャッシング

デフォルトでは、スイッチが受信した SA メッセージの送信元とグループのペアはキャッシュされません。スイッチは、MSDP SA 情報を転送するとき、この情報をメモリに格納しません。このため、ローカル RP で SA メッセージが受信された直後にメンバーがグループに加入した場合、そのメンバーは、次の SA メッセージから送信元についての情報を取得するまで待機する必要があります。この遅延は加入遅延と呼ばれます。

メモリを消費して送信元情報の遅延を短縮するには、SA メッセージをキャッシュするようにスイッチを設定します。

送信元とグループのペアのキャッシングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp cache-sa-state** [**list** *access-list-number*]	送信元とグループのペアのキャッシングをイネーブルにします（SA ステートを作成します）。これらのペアのうち、アクセス リストを通過したペアがキャッシュされます。 **list** *access-list-number* の範囲は 100 ～ 199 です。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	必要な数だけこのコマンドを繰り返し、IP 拡張アクセス リストを作成します。 • *access-list-number* の範囲は 100 ～ 199 です。ステップ 2 で指定した数値と同じ値を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 • *destination* には、パケットの送信先となるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　このコマンドの代わりに、**ip msdp sa-request** グローバル コンフィギュレーション コマンドも使用できます。ip msdp sa-request コマンドを使用すると、グループの新しいメンバーがアクティブになったときに、SA 要求メッセージがスイッチから MSDP ピアに送信されます。詳細については、次の項を参照してください。

デフォルト設定（SA ステートが作成されていない状態）に戻すには、**no ip msdp cache-sa-state** グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.0.0/16 の範囲内にある、グループ 224.2.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
Switch(config)# ip msdp cache-sa-state 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

MSDP ピアからの送信元情報の要求

ローカル RP は、SA 要求を送信し、特定グループのすべてのアクティブな送信元に対する応答をすぐに取得できます。デフォルトでは、新しいメンバーがグループに加入してマルチキャスト トラフィックを受信する必要が生じた場合、スイッチは MSDP ピアに SA 要求メッセージを送信しません。新しいメンバーは、次の定期的な SA メッセージの受信を待機する必要があります。

グループの送信元である接続済み PIM sparse（疎）モード ドメイン内にあるアクティブなマルチキャスト送信元を、グループの新しいメンバーが学習する必要がある場合、新しいメンバーがグループに加入したときに、指定した MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。ピアは、SA キャッシュ内の情報で応答します。ピアにキャッシュが設定されていない場合は、このコマンドを実行しても何も起こりません。この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバーがグループに加入し、マルチキャスト トラフィックを受信する必要が生じた場合に、MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp sa-request** {*ip-address* | *name*}	指定した MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定します。 *ip-address* | *name* には、グループの新しいメンバーがアクティブになるときにローカル スイッチが SA メッセージを要求する MSDP ピアの IP アドレスまたは名前を入力します。 SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip msdp sa-request** {*ip-address* | *name*} グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定する例を示します。

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

スイッチから発信される送信元情報の制御

スイッチから発信される次のマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元（送信元に基づく）
- 送信元情報のレシーバー（要求元の認識に基づく）

詳細については、「送信元の再配布」（P.50-9）および「Source-Active 要求メッセージのフィルタリング」（P.50-10）を参照してください。

送信元の再配布

SA メッセージは、送信元が登録されている RP で発信されます。デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。送信元が登録されている場合は、RP に *A フラグ*が設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA にアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元をさらに制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp redistribute** [**list** *access-list-name*] [**asn** *aspath-access-list-number*] [**route-map** *map*]	SA メッセージにアドバタイズされる、マルチキャスト ルーティング テーブル内の（S,G）エントリを設定します。 デフォルトでは、ローカル ドメイン内の送信元だけがアドバタイズされます。 • （任意）**list** *access-list-name* には、IP 標準アクセス リストまたは IP 拡張アクセス リストの名前または番号を入力します。標準アクセス リストの範囲は 1 ～ 99、拡張リストの範囲は 100 ～ 199 です。アクセス リストでは、アドバタイズされるローカルの送信元とその送信先となるグループを制御します。 • （任意）**asn** *aspath-access-list-number* には、1 ～ 199 の範囲の IP 標準アクセス リスト番号または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、**ip as-path access-list** コマンドでも設定する必要があります。 • （任意）**route-map** *map* には、1 ～ 199 の範囲の IP 標準アクセス リスト番号または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、**ip as-path access-list** コマンドでも設定する必要があります。 アドバタイズされる（S,G）ペアは、アクセス リストまたは自律システム パス アクセス リストによって決まります。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	必要な数だけこのコマンドを繰り返し、IP 標準アクセス リストを作成します。
	または	または
	access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	必要な数だけこのコマンドを繰り返し、IP 拡張アクセス リストを作成します。 • *access-list-number* では、標準アクセス リストの範囲は 1 ～ 99、拡張リストの範囲は 100 ～ 199 です。ステップ 2 で指定した数値と同じ値を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 • *destination* には、パケットの送信先となるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フィルタを削除するには、**no ip msdp redistribute** グローバル コンフィギュレーション コマンドを使用します。

Source-Active 要求メッセージのフィルタリング

デフォルトでは、SA 情報をキャッシュしているスイッチだけが SA 要求に応答します。デフォルトでは、このようなスイッチは、MSDP ピアからのすべての SA 要求メッセージを受け入れ、アクティブな送信元の IP アドレスを提供します。

ただし、MSDP ピアからの SA 要求をすべて無視するようにスイッチを設定できます。また、標準アクセス リストに記述されたグループのピアからの SA 要求メッセージだけを受け入れることもできます。アクセス リストでグループが通過すると、そのグループのピアからの SA 要求メッセージが受信されます。他のグループのピアからのメッセージは、すべて無視されます。

これらの方法のいずれかを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp filter-sa-request** *ip-address* | *name* または **ip msdp filter-sa-request** {*ip-address* | *name*} **list** *access-list-number*	指定した MSDP ピアからの SA 要求メッセージをすべてフィルタリングします。 または 指定した MSDP ピアからの SA 要求メッセージを、標準アクセス リストを通過したグループに対してフィルタリングします。アクセス リストには、マルチキャスト グループ アドレスが記述されています。access-list-number の範囲は 1 ～ 99 です。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	必要な数だけこのコマンドを繰り返し、IP 標準アクセス リストを作成します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip msdp filter-sa-request** {*ip-address* | *name*} グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.2.2 にある MSDP ピアからの SA 要求メッセージをフィルタリングするようにスイッチを設定する例を示します。ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージは、アクセス リスト 1 を通過して受信され、それ以外のメッセージはすべて無視されます。

```
Switch(config)# ip msdp filter sa-request 171.69.2.2 list 1
Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

スイッチから転送される送信元情報の制御

デフォルトでは、スイッチが受信したすべての SA メッセージが、すべての MSDP ピアに転送されます。ただし、フィルタリングしたり、Time To Live（TTL; 存続可能時間）値を設定することで、発信メッセージがピアに転送されないようにすることができます。以降の項では、この方法について説明します。

フィルタの使用

フィルタを作成すると、次のいずれかの処理を実行できます。

- 送信元とグループのペアをすべてフィルタリングする
- 特定の送信元とグループのペアだけが通過するように IP 拡張アクセス リストを指定する
- ルート マップの一致基準に基づいてフィルタリングする

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp sa-filter out** *ip-address* | *name*	指定した MSDP ピアへの SA メッセージをすべてフィルタリングします。
	または	または
	ip msdp sa-filter out {*ip-address* | *name*} **list** *access-list-number*	IP 拡張アクセス リストを通過した SA メッセージだけを、指定したピアに渡します。*access-list-number*（拡張アクセス リスト番号）の範囲は 100 ～ 199 です。 **list** と **route-map** の両方のキーワードを使用すると、すべての条件が true である場合に、発信 SA メッセージ内のすべての（S,G）ペアが通過します。
	または	または
	ip msdp sa-filter out {*ip-address* | *name*} **route-map** *map-tag*	ルート マップ *map-tag* 内の一致基準を満たしている SA メッセージだけを、指定した MSDP ピアに渡します。 すべての一致基準が true であり、ルート マップに **permit** を指定している場合、ルートはフィルタを通過します。**deny** を指定していると、ルートはフィルタリングされます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	（任意）必要な数だけこのコマンドを繰り返し、IP 拡張アクセス リストを作成します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 • *destination* には、パケットの送信先となるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フィルタを削除するには、**no ip msdp sa-filter out** {*ip-address* | *name*} [**list** *access-list-number*] [**route-map** *map-tag*] グローバル コンフィギュレーション コマンドを使用します。

次に、アクセス リスト 100 を通過した（S,G）ペアだけが SA メッセージに格納され、*switch.cisco.com* という名前のピアに転送されるように設定する例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter out switch.cisco.com list 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

SA メッセージで送信されるマルチキャスト データの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。IP ヘッダー TTL 値が *ttl* 引数以上であるマルチキャスト パケットだけを、指定した MSDP ピアに送信します。たとえば、内部トラフィックの TTL 値を 8 に制限できます。他のグループを外部に送信する場合は、これらのパケットの送信時に TTL を 8 より大きく設定する必要があります。

TTL スレッシュホールドを確立するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp ttl-threshold** {*ip-address* | *name*} *ttl*	指定した MSDP ピアへの最初の SA メッセージにカプセル化されるマルチキャスト データを制限します。 • *ip-address* | *name* には、TTL の制限を適用する MSDP ピアの IP アドレスまたは名前を入力します。 • *ttl* には、TTL 値を入力します。デフォルトは 0 です。この場合、TTL がなくなるまで、すべてのマルチキャスト データ パケットがピアに転送されます。指定できる範囲は 0 ～ 255 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip msdp ttl-threshold** {*ip-address* | *name*} グローバル コンフィギュレーション コマンドを使用します。

スイッチで受信される送信元情報の制御

デフォルトでは、スイッチは、MSDP の RPF ピアが送信したすべての SA メッセージを受信します。ただし、着信 SA メッセージをフィルタリングすることで、MSDP ピアから受信する送信元情報を制御できます。つまり、特定の着信 SA メッセージを受信しないようにスイッチを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージをフィルタリングする
- 特定の送信元とグループのペアが通過するように IP 拡張アクセス リストを指定する

- ルート マップの一致基準に基づいてフィルタリングする

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp sa-filter in** *ip-address* | *name* または **ip msdp sa-filter in** {*ip-address* | *name*} **list** *access-list-number* または **ip msdp sa-filter in** {*ip-address* | *name*} **route-map** *map-tag*	指定した MSDP ピアからの SA メッセージをすべてフィルタリングします。 または IP 拡張アクセス リストを通過した SA メッセージだけを、指定されたピアから受信します。*access-list-number*（拡張アクセス リスト番号）の範囲は 100 ～ 199 です。 **list** と **route-map** の両方のキーワードを使用すると、すべての条件が true である場合に、着信 SA メッセージ内のすべての（S,G）ペアが通過します。 または ルート マップ *map-tag* 内の一致条件を満たしている SA メッセージだけを、指定した MSDP ピアから受信します。 すべての一致基準が true であり、ルート マップに **permit** を指定している場合、ルートはフィルタを通過します。**deny** を指定していると、ルートはフィルタリングされます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	（任意）必要な数だけこのコマンドを繰り返し、IP 拡張アクセス リストを作成します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元となるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 • *destination* には、パケットの送信先となるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フィルタを削除するには、**no ip msdp sa-filter in** {*ip-address* | *name*} [**list** *access-list-number*] [**route-map** *map-tag*] グローバル コンフィギュレーション コマンドを使用します。

次に、*switch.cisco.com* という名前のピアからの SA メッセージをすべてフィルタリングする例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter in switch.cisco.com
```

MSDP メッシュ グループの設定

MSDP メッシュ グループは、フル メッシュ構造の MSDP 相互接続ができる MSDP スピーカーのグループです。メッシュ グループ内のピアから受信された SA メッセージは、同じメッシュ グループ内の他のピアに転送されません。このため、SA メッセージのフラッディングが削減され、ピア RPF フラッディングが簡素化されます。ドメイン内に複数の RP が存在する場合は、**ip msdp mesh-group** グローバル コンフィギュレーション コマンドを使用します。特に、ドメイン全体に SA メッセージを送信する場合に使用します。単一のスイッチに複数のメッシュ グループを（異なる名前で）設定できます。

メッシュ グループを作成するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp mesh-group** *name* {*ip-address* | *name*}	MSDP メッシュ グループを設定し、そのメッシュ グループに属する MSDP ピアを指定します。 デフォルトでは、MSDP ピアはメッシュ グループに属しません。 • *name* には、メッシュ グループの名前を入力します。 • *ip-address* | *name* には、メッシュ グループのメンバーになる MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。
ステップ 6		グループ内の MSDP ピアごとに、この手順を繰り返します。

メッシュ グループから MSDP ピアを削除するには、**no ip msdp mesh-group** *name* {*ip-address* | *name*} グローバル コンフィギュレーション コマンドを使用します。

MSDP ピアのシャットダウン

複数の MSDP コマンドが設定された単一のピアをアクティブにしない場合は、ピアをシャットダウンして設定することにより、あとで起動できます。ピアをシャットダウンすると、TCP 接続が終了し、再起動されません。ピアの設定情報を保持したまま、MSDP セッションをシャットダウンすることもできます。

ピアをシャットダウンするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp shutdown** {*peer-name* | *peer address*}	設定情報を保持したまま、指定した MSDP ピアを管理上のシャットダウン状態にします。 *peer-name* | *peer address* には、シャットダウンする MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ピアを再起動するには、**no ip msdp shutdown** {*peer-name* | *peer address*} グローバル コンフィギュレーション コマンドを使用します。これにより、TCP 接続が再確立されます。

MSDP への境界 PIM dense（密）モード領域の追加

PIM sparse（疎）モード領域と dense（密）モード領域の境界となるスイッチに MSDP を設定できます。デフォルトでは、dense（密）モード領域のアクティブな送信元は MSDP に参加しません。

（注）　**ip msdp border sa-address** グローバル コンフィギュレーション コマンドを使用することは推奨できません。dense（密）モード ドメイン内の送信元を sparse（疎）モード ドメインの RP にプロキシ登録するように sparse（疎）モード ドメイン内の境界ルータを設定し、MSDP の標準的な手順を使用してこれらの送信元をアドバタイズするように sparse（疎）モード ドメインを設定してください。

dense（密）モード領域内でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp border sa-address** *interface-id*	dense（密）モード領域内のアクティブな送信元に関する SA メッセージを送信するように、dense（密）モード領域と sparse（疎）モード領域の境界スイッチを設定します。 *interface-id* には、SA メッセージ内の RP アドレスとして使用される、IP アドレスが取得されるインターフェイスを指定します。 インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。
ステップ 3	**ip msdp redistribute** [**list** *access-list-name*] [**asn** *aspath-access-list-number*] [**route-map** *map*]	SA メッセージにアドバタイズされる、マルチキャスト ルーティング テーブル内の（S,G）エントリを設定します。 詳細については、「送信元の再配布」（P.50-9）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ip msdp originator-id グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。**ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスによって RP アドレスが決まります。

デフォルト設定（dense（密）モード領域のアクティブな送信元が MSDP に参加しない設定）に戻すには、**no ip msdp border sa-address** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

RP アドレス以外の発信元アドレスの設定

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用する場合は、送信元 ID を変更します。次のいずれかの場合に送信元 ID を変更できます。

- MSDP メッシュ グループ内の複数のスイッチ上で、論理 RP を設定する場合。
- PIM sparse（疎）モード ドメインと dense（密）モード ドメインの境界スイッチがある場合。サイトの dense（密）モード ドメインの境界となるスイッチがあり、sparse（疎）モードがその外部で使用されている場合は、dense（密）モードの送信元を外部に通知する必要があります。このスイッチは RP ではないので、SA メッセージで使用される RP アドレスを含みません。したがって、このコマンドによりインターフェイスのアドレスを指定して、RP アドレスが取得されます。

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp originator-id** *interface-id*	発信元装置のインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。 *interface-id* には、ローカル スイッチのインターフェイスを指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ip msdp border sa-address と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスによって RP アドレスが決まります。

この方法で RP アドレスが取得されないようにするには、**no ip msdp originator-id** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

MSDP のモニタおよびメンテナンス

MSDP SA メッセージ、ピア、ステート、またはピア ステータスをモニタするには、表 50-1 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 50-1　MSDP のモニタおよびメンテナンスのためのコマンド

コマンド	目的
debug ip msdp [*peer-address* | *name*] [**detail**] [**routes**]	MSDP アクティビティをデバッグします。
debug ip msdp resets	MSDP ピアがリセットされた原因をデバッグします。
show ip msdp count [*autonomous-system-number*]	SA メッセージに格納され、各自律システムから発信された送信元およびグループの数を表示します。このコマンドによって出力を生成するには、**ip msdp cache-sa-state** コマンドを設定する必要があります。
show ip msdp peer [*peer-address* | *name*]	MSDP ピアに関する詳細情報を表示します。
show ip msdp sa-cache [*group-address* | *source-address* | *group-name* | *source-name*] [*autonomous-system-number*]	MSDP ピアから学習した（S,G）ステートを表示します。
show ip msdp summary	MSDP ピア ステータスおよび SA メッセージ数を表示します。

MSDP 接続、統計情報、または SA キャッシュ エントリを消去するには、表 50-2 に示す各特権 EXEC コマンドを使用します。

表 50-2　MSDP 接続、統計情報、または SA キャッシュ エントリを消去するためのコマンド

コマンド	目的
clear ip msdp peer *peer-address* | *name*	指定した MSDP ピアへの TCP 接続を消去し、すべての MSDP メッセージ カウンタをリセットします。
clear ip msdp statistics [*peer-address* | *name*]	セッションをリセットせずに、特定の MSDP ピアまたはすべての MSDP ピアの統計カウンタをクリアします。
clear ip msdp sa-cache [*group-address* | *name*]	すべてのエントリの SA キャッシュ エントリ、特定グループのすべての送信元、または特定の送信元とグループのペアのすべてのエントリを消去します。

CHAPTER 51

フォールバック ブリッジングの設定

この章では、IE 3000 スイッチ上でフォールバック ブリッジング（VLAN ブリッジング）を設定する手順について説明します。フォールバック ブリッジングでは、スイッチが VLAN ブリッジ ドメインとルーテッド ポートの間でルーティングしていない非 IP パケットを転送できます。

（注） この機能を使用するには、スイッチが IP サービス イメージを実行している必要があります。この章で使用しているコマンドの構文および使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある、『*Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2, Release 12.2*』を参照してください。

この章で説明する内容は、次のとおりです。

フォールバック ブリッジングの概要

フォールバック ブリッジングを使用して、スイッチは、基本的に 1 つのブリッジ ドメイン内の複数の VLAN を接続して、複数の VLAN またはルーテッド ポートをまとめてブリッジします。フォールバック ブリッジングでは、スイッチがルーティングしなかったトラフィックや、DECnet などの非ルーティング プロトコルに属するトラフィックを転送します。

VLAN ブリッジ ドメインは、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を使用して表します。（VLAN が関連付けられていない）一連の SVI とルーテッド ポートは、ブリッジ グループを形成するように設定（グループ化）できます。SVI は、システム内のルーティングまたはブリッジング機能に対する 1 つのインターフェイスとしてスイッチ ポートの VLAN を表します。1 つの VLAN に関連付けることができる SVI は、1 つだけです。VLAN 間でのルーティング、VLAN 間での非ルーティング プロトコルのフォールバック ブリッジング、またはスイッチに対する IP ホスト接続を実現する場合にだけ、1 つの VLAN に 1 つの SVI を設定します。ルーテッド ポートは、ルータ上でポートのように動作する物理ポートですが、ルータには接続されていません。ルーテッド ポートは、特定の VLAN に関連付けられておらず、VLAN サブインターフェイスをサポートしませんが、標準のルーテッド ポートのように動作します。SVI とルーテッド ポートの詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。

ブリッジ グループは、スイッチ上のネットワーク インターフェイスの内部構造です。ブリッジ グループが定義されたスイッチの外側にあるブリッジ グループ内では、スイッチングされたトラフィックを識別するためにブリッジ グループを使用できません。スイッチ上のブリッジ グループは、個別のブリッジとして機能します。つまり、ブリッジド トラフィックと Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）はスイッチ上のさまざまなブリッジ グループ間で交換されません。

フォールバック ブリッジングは、ブリッジングされている VLAN からのスパニング ツリーを縮小できません。各 VLAN には独自のスパニング ツリー インスタンスと、ループを防ぐためにブリッジ グループの上部で実行される VLAN ブリッジ スパニング ツリーと呼ばれる個別のスパニング ツリーがあります。

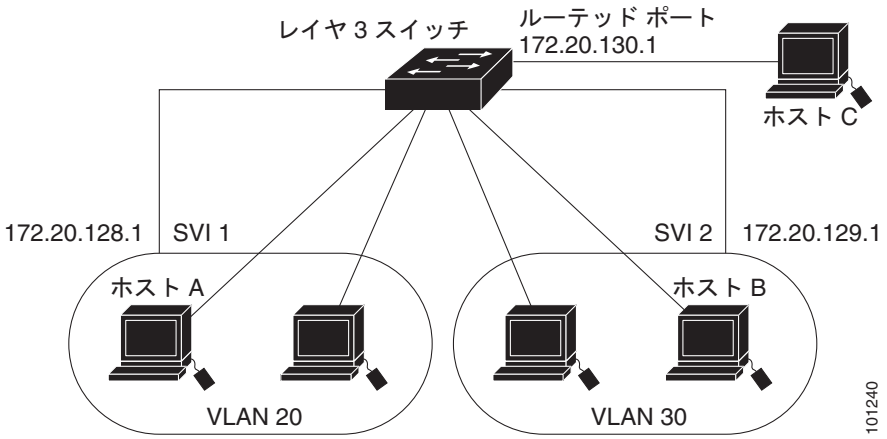
スイッチは、ブリッジ グループが作成されたときに、VLAN ブリッジ スパニング ツリー インスタンスを作成します。スイッチはブリッジ グループを実行し、SVI とルーテッド ポートをブリッジ グループでスパニング ツリー ポートとして取り扱います。

次に、ブリッジ グループにネットワーク インターフェイスを配置する理由を示します。

- ブリッジ グループを構成しているネットワーク インターフェイス間でルーティングされていないすべてのトラフィックをブリッジングするため。パケットの宛先アドレスがブリッジ テーブル内にある場合は、そのパケットはブリッジ グループ内の単一のインターフェイスに転送されます。パケットの宛先アドレスがブリッジ テーブル内にない場合は、そのパケットはブリッジ グループ内のすべての転送インターフェイス上でフラッディングされます。送信元 MAC アドレスがブリッジ グループ上で学習されるのは、そのアドレスが VLAN 上で学習される場合だけです（その逆の場合は学習されません）。
- 接続されている LAN 上の BPDU を受信（場合によっては送信）することによって、スパニング ツリー アルゴリズムに参加するため。個別のスパニング ツリー プロセスは、設定された各ブリッジ グループに対して実行されます。各ブリッジ グループは個別のスパニング ツリー インスタンスに参加します。ブリッジ グループは、そのメンバー インターフェイス上だけで受信する BPDU に基づいて、スパニング ツリー インスタンスを確立します。VLAN がブリッジ グループに属していないポートで受信されたブリッジ Spanning Tree Protocol（STP; スパニング ツリー プロトコル）BPDU は、その VLAN のすべての転送ポート上でフラッディングします。

図 51-1 にフォールバック ブリッジング ネットワークの例を示します。スイッチには SVI として 2 つのポートが設定されています。それらは、異なる IP アドレスを割り当てられ、2 つの異なる VLAN に接続されています。もう 1 つのポートは、独自の IP アドレスを持つルーテッド ポートとして設定されています。これらの 3 つのすべてのポートが同じブリッジ グループに割り当てられている場合、それらが異なるネットワーク上にあり、異なる VLAN 内にある場合でも、スイッチに接続されているエンド ステーションの間で非 IP プロトコル フレームを転送できます。フォールバック ブリッジングを機能させるために、ルーテッド ポートや SVI に IP アドレスを割り当てる必要はありません。

図 51-1　フォールバック ブリッジング ネットワークの例



フォールバック ブリッジングの設定

- 「フォールバック ブリッジングのデフォルト設定」（P.51-3）
- 「フォールバック ブリッジングの設定時の注意事項」（P.51-4）
- 「ブリッジ グループの作成」（P.51-4）（必須）
- 「スパニング ツリー パラメータの調整」（P.51-6）（任意）

フォールバック ブリッジングのデフォルト設定

表 51-1 にデフォルトのフォールバック ブリッジングの設定を示します。

表 51-1　フォールバック ブリッジングのデフォルト設定

機能	デフォルト設定
ブリッジ グループ	ポートに対して定義されていたり割り当てられているものはありません。VLAN ブリッジ STP は定義されていません。
スイッチがダイナミックに学習したステーションに対するフレームの転送	イネーブル。
スパニング ツリー パラメータ	
• スイッチ プライオリティ	• 32768。
• ポート プライオリティ	• 128。
• ポート パス コスト	• 10 Mb/s：100。 100 Mb/s：19。 1000 Mb/s：4。
• hello BPDU の間隔	• 2 秒。
• 転送遅延間隔	• 20 秒。
• 最大アイドル間隔	• 30 秒。

フォールバック ブリッジングの設定時の注意事項

最大 32 ブリッジ グループまでスイッチ上で設定できます。

インターフェイス（SVI またはルーテッド ポート）は 1 つのブリッジ グループ上だけのメンバーにすることができます。

スイッチに接続している個別のブリッジ型ネットワーク（トポロジが明確）ごとに、ブリッジ グループを使用します。

プライベート VLAN が設定されたスイッチに対してはフォールバック ブリッジングを設定しないでください。

IP（Version 4 および Version 6）、Address Resolution Protocol（ARP; アドレス解決プロトコル）、Reverse ARP（ARP; 逆 ARP）、LOOPBACK、フレーム リレー ARP、および共有 STP パケット以外のすべてのプロトコルがフォールバック ブリッジングされます。

ブリッジ グループの作成

一連の SVI またはルーテッド ポートに対してフォールバック ブリッジングを設定するには、次のインターフェイスをブリッジ グループに割り当てる必要があります。同じグループ内のすべてのインターフェイスは、同じブリッジ ドメインに属します。各 SVI またはルーテッド ポートは、1 つのブリッジ グループにだけ割り当てることができます。

（注） 保護ポート機能は、フォールバック ブリッジングに対する互換性はありません。フォールバック ブリッジングがイネーブルであるときに、複数のポートがさまざまな VLAN 上にある場合、スイッチ上の保護ポートから同じスイッチ上の別の保護ポートにパケットが転送される可能性があります。

ブリッジ グループを作成して、それに対するインターフェイスを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**bridge** *bridge-group* **protocol vlan-bridge**	ブリッジ グループ番号を割り当て、ブリッジ グループ内で実行する VLAN ブリッジ スパニング ツリー プロトコルを指定します。**ibm** および **dec** キーワードはサポートされていません。 *bridge-group* には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。最大 32 のブリッジ グループを作成できます。 フレームは、同じグループ内のインターフェイス間でだけブリッジングされます。

	コマンド	目的
ステップ 3	**interface** *interface-id*	ブリッジ グループを割り当てるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを入力してレイヤ 3 ポートとして設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 **（注）** IP アドレスをルーテッド ポートまたは SVI に割り当てることができますが、必須ではありません。
ステップ 4	**bridge-group** *bridge-group*	ステップ 2 で作成したブリッジ グループにインターフェイスを割り当てます。 デフォルトでは、インターフェイスはブリッジ グループに割り当てられています。インターフェイスは、1 つのブリッジ グループだけに割り当てることができます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ブリッジ グループを削除するには、**no bridge** *bridge-group* グローバル コンフィギュレーション コマンドを使用します。**no bridge** *bridge-group* コマンドは、そのブリッジ グループからすべての SVI とルーテッド ポートを自動的に削除します。ブリッジ グループからインターフェイスを削除し、ブリッジ グループを削除するには、**no bridge-group** *bridge-group* インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 を作成し、そのブリッジ グループ内で VLAN ブリッジ STP が実行されるように指定し、ポートをルーテッド ポートとして定義し、ブリッジ グループにポートを割り当てる例を示します。

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# bridge-group 10
```

次に、ブリッジ グループ 10 を作成し、そのブリッジ グループ内で VLAN ブリッジ STP が実行されるように指定する例を示します。これによって、VLAN 2 に対する SVI が定義され、それがブリッジ グループに割り当てられます。

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# interface vlan2
Switch(config-if)# bridge-group 10
Switch(config-if)# exit
```

スパニング ツリー パラメータの調整

デフォルト値が適切ではない場合、特定のスパニング ツリー パラメータを調整する必要がある場合があります。さまざまな **bridge** グローバル コンフィギュレーション コマンドを使用して、スパニング ツリー全体に影響を与えるパラメータを設定します。さまざまな **bridge-group** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス固有のパラメータを設定します。

次のいずれかの作業を実行することによって、スパニング ツリー パラメータを調整できます。

- 「VLAN ブリッジ スパニング ツリーのプライオリティの変更」（P.51-6）（任意）
- 「インターフェイス プライオリティの変更」（P.51-7）（任意）
- 「パス コストの割り当て」（P.51-7）（任意）
- 「BPDU の間隔の調整」（P.51-8）（任意）
- 「インターフェイス上のスパニング ツリーのディセーブル化」（P.51-10）（任意）

（注）　スパニング ツリー パラメータの調整は、スイッチおよび STP の機能に精通しているネットワーク管理者だけが行ってください。計画が不十分なまま調整を行うと、パフォーマンスの低下を招くことがあります。スイッチングに関する資料としては、IEEE 802.1D 仕様が適しています。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』の付録「References and Recommended Reading」を参照してください。

VLAN ブリッジ スパニング ツリーのプライオリティの変更

ルート スイッチの候補として別のスイッチと同レベルにあるスイッチには、スイッチの VLAN ブリッジ スパニング ツリーのプライオリティをグローバルに設定できます。スイッチがルート スイッチとして選択される可能性も設定できます。

スイッチ プライオリティを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**bridge** *bridge-group* **priority** *number*	スイッチの VLAN ブリッジ スパニング ツリーのプライオリティを変更します。 • *bridge-group* には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。 • *number* には、0 ～ 65535 の値を入力します。デフォルト値は 32768 です。番号の値が小さくなるほど、スイッチがルートとして選択される可能性は高くなります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no bridge** *bridge-group* **priority** グローバル コンフィギュレーション コマンドを使用します。ポートのプライオリティを変更するには、（次の項の説明に従って）**bridge-group priority** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 のスイッチ プライオリティを 100 に設定する例を示します。

```
Switch(config)# bridge 10 priority 100
```

インターフェイス プライオリティの変更

ポートに対するプライオリティを変更できます。2 つのスイッチがルート スイッチの候補として同等のレベルにある場合、その均衡を破るようにポート プライオリティを設定します。最もインターフェイス値が低いスイッチが選択されます。

インターフェイス プライオリティを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	プライオリティを設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**bridge-group** *bridge-group* **priority** *number*	ポートのプライオリティを変更します。 • *bridge-group* には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。 • *number* には、4 単位で 0 ～ 255 の番号を入力します。番号が小さくなるほど、スイッチ上でポートがルートとして選択される可能性が高くなります。デフォルト値は 128 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no bridge-group** *bridge-group* **priority** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内のポートに対するプライオリティを 20 に変更する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# bridge-group 10 priority 20
```

パス コストの割り当て

各ポートには、パス コストが関連付けられています。規定では、パス コストは 1000/データ レート（接続された LAN のデータ速度）の値を Mbps 単位で表したものです。

パス コストを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	パス コストを設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**bridge-group** *bridge-group* **path-cost** *cost*	ポートのパス コストを割り当てます。 • *bridge-group* には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。 • *cost* には、0 ～ 65535 の番号を入力します。値が大きくなるほどコストが高くなります。 – 10 Mb/s の場合は、デフォルト パス コストは 100 です。 – 100 Mb/s の場合は、デフォルト パス コストは 19 です。 – 1000 Mb/s の場合は、デフォルト パス コストは 4 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト パス コストに戻すには、**no bridge-group** *bridge-group* **path-cost** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内のポートに対するパス コストを 20 に変更する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# bridge-group 10 path-cost 20
```

BPDU の間隔の調整

ここでの説明に従って、BPDU の間隔を調整できます。

- 「Hello BPDU の間隔の調整」（P.51-8）（任意）
- 「転送遅延間隔の変更」（P.51-9）（任意）
- 「最大アイドル間隔の変更」（P.51-9）（任意）

（注）　スパニング ツリー内の各スイッチは、個別の設定に関係なく、ルート スイッチの hello BPDU の間隔、転送遅延間隔、および最大アイドル間隔のパラメータを採用します。

Hello BPDU の間隔の調整

hello BPDU の間隔を調整するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**bridge** *bridge-group* **hello-time** *seconds*	hello BPDU の間隔を指定します。 • *bridge-group* には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。 • *seconds* には、1 ～ 10 の値を入力します。デフォルト値は 2 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no bridge** *bridge-group* **hello-time** グローバル コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内の hello 間隔を 5 秒に変更する例を示します。

```
Switch(config)# bridge 10 hello-time 5
```

転送遅延間隔の変更

転送遅延間隔は、ポートでスイッチングがアクティブにされてから実際に転送が開始されるまでの間のトポロジ変更情報の待ちに費やされた時間の長さです。

転送遅延間隔を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**bridge** *bridge-group* **forward-time** *seconds*	転送遅延間隔を指定します。 • *bridge-group* には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。 • *seconds* には、4 ～ 200 の値を入力します。デフォルト値は 20 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no bridge** *bridge-group* **forward-time** グローバル コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内の転送遅延間隔を 10 秒に変更する例を示します。

```
Switch(config)# bridge 10 forward-time 10
```

最大アイドル間隔の変更

指定した間隔内にスイッチがルート スイッチから BPDU を受信しない場合は、スパニング ツリー トポロジが再計算されます。

最大アイドル間隔（最大エージング タイム）を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**bridge** *bridge-group* **max-age** *seconds*	ルート スイッチからの BPDU を受信するのをスイッチが待機する間隔を指定します。 • *bridge-group* には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。 • *seconds* には、6 ～ 200 の値を入力します。デフォルト値は 30 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no bridge** *bridge-group* **max-age** グローバル コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内の最大アイドル間隔を 30 秒に変更する例を示します。

```
Switch(config)# bridge 10 max-age 30
```

インターフェイス上のスパニング ツリーのディセーブル化

任意の 2 つのスイッチド サブネットワークの間にループフリー パスが存在する場合、1 つのスイッチド サブネットワークで生成された BPDU が、ネットワーク全体としてはスイッチングを許可したままで、もう 1 つのスイッチド サブネットワーク内の装置に影響を与えないようにすることができます。たとえば、スイッチド LAN サブネットワークが WAN によって分離されている場合、BPDU が WAN リンクを経由して送信されないようにすることができます。

ポート上のスパニング ツリーをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**bridge-group** *bridge-group* **spanning-disabled**	ポート上のスパニング ツリーをディセーブルにします。 *bridge-group* には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポート上でスパニング ツリーを再度イネーブルにするには、**no bridge-group** *bridge-group* **spanning-disabled** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内のポートに対するスパニング ツリーをディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# bridge group 10 spanning-disabled
```

フォールバック ブリッジングのモニタおよびメンテナンス

ネットワークをモニタおよびメンテナンスするには、表 51-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 51-2　フォールバック ブリッジングのモニタおよびメンテナンスのためのコマンド

コマンド	目的
clear bridge *bridge-group*	転送データベースから任意の学習されたエントリを削除します。
show bridge [*bridge-group*] **group**	ブリッジ グループの詳細を表示します。
show bridge [*bridge-group*] [*interface-id* | *mac-address* | **verbose**]	ブリッジ グループ内の学習された MAC アドレスを表示します。

これらの表示内のフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択し、『*Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2, Release 12.2*』を参照してください。

CHAPTER 52

トラブルシューティング

この章では、IE 3000 スイッチの Cisco IOS ソフトウェアに関する問題を特定し解決する方法について説明します。問題の特定と解決には、問題の性質に応じて、CLI（コマンドライン インターフェイス）、デバイス マネージャ、または Network Assistant を使用できます。

ハードウェア インストレーション ガイドにも、LED に関する説明など、その他のトラブルシューティング情報が記載されています。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスおよび Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Commands Master List, Release 12.2*』を参照してください。

この章で説明する内容は、次のとおりです。

（注） 回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

ソフトウェア障害からの回復

アップグレード時に、誤ったファイルをスイッチにダウンロードした場合や、イメージ ファイルを削除した場合に、スイッチ ソフトウェアが破損することがあります。いずれの場合も、スイッチは Power-on Self-Test（POST; 電源投入時セルフテスト）に失敗し、接続できません。

この手順では、Xmodem プロトコルを使用して、破損したイメージ ファイルまたは誤ったイメージ ファイルを回復します。Xmodem プロトコルは多数のソフトウェア パッケージでサポートされており、使用しているエミュレーション ソフトウェアによって手順が異なります。

この回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

ステップ 1　PC 上で、Cisco.com からソフトウェア イメージの tar ファイル（*image_filename.tar*）をダウンロードします。

Cisco IOS イメージが bin ファイルとして、tar ファイル内のディレクトリに格納されます。Cisco.com のソフトウェア イメージ ファイルの検索方法については、リリース ノートを参照してください。

ステップ 2　tar ファイルから bin ファイルを抽出します。

- Windows では、tar ファイルの読み取り機能を持つ zip プログラムを使用します。zip プログラムを使用して、bin ファイルに移動し、抽出します。
- UNIX では、次の手順を実行します。

1. **tar -tvf** <*image_filename.tar*> UNIX コマンドを使用して、tar ファイルの内容を表示します。

```
unix-1% tar -tvf image_filename.tar
```

2. **tar -xvf** <*image_filename.tar*> <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルを特定し、抽出します。

```
unix-1% tar -xvf image_filename.tar image_filename.bin
x ies-lanbase-mz.122-52.SE/ies-ipservices-mz.122-52.SE.bin, 2928176 bytes, 5720
tape blocks
```

3. **ls -l** <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。

```
unix-1% ls -l image_filename.bin
-rwxr-xr-x   1 bschuett eng      6365325 May 19 13:03
ies-lanbase-mz.122-52.SE/ies-ipservices-mz.122-52.SE.bin
```

ステップ 3　Xmodem プロトコルをサポートするターミナル エミュレーション ソフトウェアを備えた PC を、スイッチのコンソール ポートに接続します。

ステップ 4　エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 5　スイッチの電源コードを取り外します。

ステップ 6　[Express Setup] ボタンを押しながら、電源コードをスイッチに再接続します。

ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、[Express Setup] ボタンを放します。ソフトウェアに関する数行の情報と手順が表示されます。

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software#

flash_init
load_helper
boot
```

ステップ 7　フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

ステップ 8　コンソール ポートの速度を 9600 以外に設定していた場合は、9600 にリセットされています。エミュレーション ソフトウェアの回線速度を、スイッチのコンソール ポートの速度に合わせて変更します。

ステップ 9　ヘルパー ファイルをロードします。

```
switch: load_helper
```

ステップ 10　Xmodem プロトコルを使用して、ファイル転送を開始します。

```
switch: copy xmodem: flash:image_filename.bin
```

ステップ 11　Xmodem 要求が表示されたら、ターミナル エミュレーション ソフトウェアの適切なコマンドを使用して転送を開始し、ソフトウェア イメージをフラッシュ メモリにコピーします。

ステップ 12　新しくダウンロードした Cisco IOS イメージを起動します。

```
switch:boot flash:image_filename.bin
```

ステップ 13　**archive download-sw** 特権 EXEC コマンドを使用して、ソフトウェア イメージをスイッチにダウンロードします。

ステップ 14　**reload** 特権 EXEC コマンドを使用してスイッチを再起動し、新しいソフトウェア イメージが正常に動作することを確認します。

ステップ 15　スイッチから flash:*image_filename.bin* ファイルを削除します。

パスワードを忘れた場合の回復

パスワードを忘れた場合は、スイッチのパスワードを削除して新しく設定できます。

手順を開始する前に、次の点を確認してください。

- スイッチに物理的にアクセスできること。
- イネーブルになっていて装置に接続されていないスイッチ ポートが 1 つ以上あること。

スイッチのパスワードを削除して新しく設定するには、次の手順を実行します。

ステップ 1　SETUP LED がグリーンに点滅し、使用可能なスイッチ ダウンリンク ポートの LED がグリーンに点滅するまで、[Express Setup] ボタンを押し続けます。

PC またはラップトップの接続に使用できるスイッチ ダウンリンク ポートの空きがない場合は、いずれかのスイッチ ダウンリンク ポートから装置を接続解除します。もう一度、SETUP LED とポートの LED がグリーンに点滅するまで [Express Setup] ボタンを押し続けます。

ステップ 2　LED がグリーンに点滅しているポートに、PC またはラップトップを接続します。

SETUP LED とスイッチ ダウンリンク ポートの LED が点滅を中止し、グリーンに点灯します。

ステップ 3　[Express Setup] ボタンを押し続けます。SETUP LED が再度グリーンに点滅し始めます。SETUP LED がグリーンに点灯するまで（約 5 秒間）、ボタンを押したままにします。すぐに [Express Setup] ボタンを放します。

この手順によって、他の設定に影響を与えることなく、パスワードが削除されます。これで、パスワードを入力せずに、コンソール ポートまたはデバイス マネージャからスイッチにアクセスできるようになりました。

ステップ 4　デバイス マネージャの [Express Setup] ウィンドウを使用するか、コマンドライン インターフェイスで **enable secret** グローバル コンフィギュレーション コマンドを使用して、新しいパスワードを入力します。

```
11  -rwx       5825   Mar 01 1993 22:31:59  config.text
```

コマンド スイッチ障害からの回復

ここでは、コマンド スイッチの障害から回復する方法について説明します。Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用すると、冗長コマンド スイッチ グループを設定できます。詳細については、第 6 章「スイッチのクラスタ化」および第 45 章「HSRP の設定」を参照してください。また、Cisco.com の『*Getting Started with Cisco Network Assistant*』も参照してください。

（注）　クラスタに冗長性を持たせるには、HSRP の使用を推奨します。

スタンバイ コマンド スイッチを設定していない場合に、コマンド スイッチに電源故障などの障害が発生すると、メンバー スイッチとの管理接続が失われ、新しいコマンド スイッチに交換する必要が生じます。ただし、接続されているスイッチ間の接続は影響を受けず、メンバー スイッチは通常どおりパケットを転送します。メンバーは、コンソール ポートを通してスタンドアロンのスイッチとして管理できます。また、メンバーに IP アドレスがある場合は、他の管理インターフェイスを通して管理することもできます。

コマンド スイッチ障害に備えるには、コマンド対応のメンバー スイッチやその他のスイッチに IP アドレスを割り当て、コマンド スイッチのパスワードを書き留め、メンバー スイッチと交換用コマンド スイッチの間に冗長接続が得られるようにクラスタを配線します。ここでは、故障したコマンド スイッチの 2 通りの交換方法について説明します。

- 「故障したコマンド スイッチをクラスタ メンバーに交換する場合」（P.52-4）
- 「故障したコマンド スイッチを別のスイッチに交換する場合」（P.52-6）

これらの回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

コマンド対応スイッチの詳細については、リリース ノートを参照してください。

故障したコマンド スイッチをクラスタ メンバーに交換する場合

故障したコマンド スイッチを、同じクラスタ内にあるコマンド対応のメンバー スイッチに交換するには、次の手順を実行します。

ステップ 1　コマンド スイッチとメンバー スイッチの接続を解除し、クラスタからコマンド スイッチを物理的に取り外します。

ステップ 2　故障したコマンド スイッチの代わりにメンバー スイッチを取り付け、同じようにクラスタ メンバーと接続します。

ステップ 3　新しいコマンド スイッチで CLI セッションを開始します。

CLI にはコンソール ポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet も使用できます。コンソール ポートの使用方法の詳細については、スイッチのハードウェア インストレーション ガイドを参照してください。

ステップ 4　スイッチ プロンプトで特権 EXEC モードを開始します。

```
Switch> enable
Switch#
```

ステップ 5　*故障したコマンド スイッチ*のパスワードを入力します。

ステップ 6　グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

ステップ 7　メンバー スイッチをクラスタから削除します。

```
Switch(config)# no cluster commander-address
```

ステップ 8　特権 EXEC モードに戻ります。

```
Switch(config)# end
Switch#
```

ステップ 9　セットアップ プログラムを使用して、スイッチの IP 情報を設定します。このプログラムを実行すると、IP アドレス情報とパスワードの入力を求められます。特権 EXEC モードで「**setup**」と入力し、Return を押します。

```
Switch# setup
         --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:
```

ステップ 10　最初のプロンプトに「**Y**」と入力します。

セットアップ プログラムで表示されるプロンプトは、コマンド スイッチとして選択したメンバー スイッチによって異なります。

```
Continue with configuration dialog? [yes/no]: y
```

または

```
Configuring global parameters:
```

このプロンプトが表示されない場合は、「**enable**」と入力し、Return を押します。「**setup**」と入力し、Return を押して、セットアップ プログラムを開始します。

ステップ 11　セットアップ プログラムの質問に応答します。

ホスト名が要求されたら、コマンド スイッチでは 28 文字以内、メンバー スイッチでは 31 文字以内に制限されていることに注意してください。どのスイッチのホスト名でも、最後の文字には *-n*（*n* は数字）を使用しないでください。

Telnet（仮想端末）パスワードが要求されたら、1 ～ 25 文字の英数字を使用できること、大文字と小文字の区別があること、スペースは使用できるが先行スペースは無視されることに注意してください。

ステップ 12　**イネーブル シークレット** パスワードと**イネーブル** パスワードが要求されたら、再度、*故障したコマンド スイッチ*のパスワードを入力します。

ステップ 13　プロンプトが表示されたら、スイッチをクラスタ コマンド スイッチとしてイネーブルにし、Return を押します。

ステップ 14　プロンプトが表示されたら、クラスタに名前を割り当て、Return を押します。

クラスタ名には、1 ～ 31 文字の英数字、ダッシュ、および下線を使用できます。

ステップ 15　初期設定が表示されたら、アドレスが正しいことを確認します。

ステップ 16　表示された情報が正しい場合は、「**Y**」と入力して Return を押します。

この情報が正しくない場合は、「**N**」と入力して Return を押し、ステップ 9 からやり直します。

ステップ 17　ブラウザを起動して、新しいコマンド スイッチの IP アドレスを入力します。

ステップ 18　クラスタに追加する候補スイッチのリストを表示するには、[Cluster] メニューの [Add to Cluster] を選択します。

故障したコマンド スイッチを別のスイッチに交換する場合

故障したコマンド スイッチを、クラスタ外にあるコマンド対応のスイッチに交換するには、次の手順を実行します。

ステップ 1　故障したコマンド スイッチの代わりに新しいスイッチを取り付け、同じようにクラスタ メンバーと接続します。

ステップ 2　新しいコマンド スイッチで CLI セッションを開始します。

CLI にはコンソール ポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet も使用できます。コンソール ポートの使用方法の詳細については、スイッチのハードウェア インストレーション ガイドを参照してください。

ステップ 3　スイッチ プロンプトで特権 EXEC モードを開始します。

```
Switch> enable
Switch#
```

ステップ 4　*故障したコマンド スイッチ*のパスワードを入力します。

ステップ 5　セットアップ プログラムを使用して、スイッチの IP 情報を設定します。

このプログラムを実行すると、IP アドレス情報とパスワードの入力を求められます。特権 EXEC モードで「**setup**」と入力し、Return を押します。

```
Switch# setup
        --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:
```

ステップ 6　最初のプロンプトに「**Y**」と入力します。

セットアップ プログラムで表示されるプロンプトは、コマンド スイッチとして選択したスイッチによって異なります。

```
Continue with configuration dialog? [yes/no]: y
```

または

```
Configuring global parameters:
```

このプロンプトが表示されない場合は、「**enable**」と入力し、Return を押します。「**setup**」と入力し、Return を押して、セットアップ プログラムを開始します。

ステップ 7　セットアップ プログラムの質問に応答します。

ホスト名が要求されたら、コマンド スイッチでは 28 文字以内に制限されていることに注意してください。どのスイッチのホスト名でも、最後の文字には *-n*（*n* は数字）を使用しないでください。

Telnet（仮想端末）パスワードが要求されたら、1 ～ 25 文字の英数字を使用できること、大文字と小文字の区別があること、スペースは使用できるが先行スペースは無視されることに注意してください。

ステップ 8　**イネーブル シークレット** パスワードと**イネーブル** パスワードが要求されたら、再度、*故障したコマンド スイッチ*のパスワードを入力します。

ステップ 9　プロンプトが表示されたら、スイッチをクラスタ コマンド スイッチとしてイネーブルにし、Return を押します。

ステップ 10　プロンプトが表示されたら、クラスタに名前を割り当て、Return を押します。

クラスタ名には、1 ～ 31 文字の英数字、ダッシュ、および下線を使用できます。

ステップ 11　初期設定が表示されたら、アドレスが正しいことを確認します。

ステップ 12　表示された情報が正しい場合は、「**Y**」と入力して Return を押します。

この情報が正しくない場合は、「**N**」と入力して **Return** を押し、ステップ 9 からやり直します。

ステップ 13　ブラウザを起動して、新しいコマンド スイッチの IP アドレスを入力します。

ステップ 14　クラスタに追加する候補スイッチのリストを表示するには、[Cluster] メニューの [Add to Cluster] を選択します。

クラスタ メンバーとの接続が切断された場合の回復

構成によっては、コマンド スイッチとメンバー スイッチとの間の接続を維持できない場合があります。メンバーとの管理接続を維持できないが、メンバー スイッチ自体は正常にパケットを転送している場合は、次の点を確認してください。

- メンバー スイッチ（Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ）を、ネットワーク ポートとして定義されたポートを通してコマンド スイッチに接続できません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 メンバー スイッチは、同じ管理 VLAN に属するポートを通してコマンド スイッチに接続する必要があります。
- セキュア ポートを通してコマンド スイッチに接続されたメンバー スイッチ（Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ）は、セキュリティ違反が原因でポートがディセーブルになった場合、接続不能になることがあります。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは、スイッチの速度（SFP モジュール ポートを除く 10 Mbps、100 Mbps、および 1000 Mbps）およびデュプレックス（半二重または全二重）の設定を管理します。このプロトコルによって設定の不一致が生じ、パフォーマンスが低下する場合があります。次のような場合に不一致が発生します。

- 手動で設定した速度またはデュプレックス パラメータが、接続先ポートの手動で設定された速度またはデュプレックス パラメータと異なる。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている。

スイッチのパフォーマンスを最大限に引き出してリンクを確実にするには、次のいずれかの注意事項に従ってデュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。

（注）　接続先装置が自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定を一致させます。速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

SFP モジュールのセキュリティと識別

シスコの着脱可能小型フォーム ファクタ（SFP）モジュールに搭載されているシリアル EEPROM には、モジュールのシリアル番号、ベンダーの名前と ID、固有のセキュリティ コード、および Cyclic Redundancy Check（CRC; 巡回冗長検査）が記録されています。SFP モジュールをスイッチに取り付けると、スイッチ ソフトウェアが EEPROM を読み取って、シリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードと CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効である場合は、セキュリティ エラー メッセージが生成され、インターフェイスが errdisable ステートになります。

（注）　セキュリティ エラー メッセージでは、GBIC_SECURITY ファシリティが参照されます。スイッチは SFP モジュールをサポートしていますが、GBIC モジュールはサポートしていません。エラー メッセージのテキストに GBIC インターフェイスまたはモジュールとあっても、セキュリティ メッセージであれば、実際は SFP モジュールまたはモジュール インターフェイスを意味します。エラー メッセージの詳細については、このリリースに対応するシステム メッセージ ガイドを参照してください。

他社製の SFP モジュールを使用している場合は、スイッチから SFP モジュールを取り外し、シスコ製モジュールと交換してください。シスコ製 SFP モジュールを取り付けた後、**errdisable recovery cause gbic-invalid** グローバル コンフィギュレーション コマンドを使用してポートのステータスを確認し、errdisable ステートから回復する時間間隔を入力します。この時間間隔が経過すると、スイッチはインターフェイスを errdisable ステートから復帰させ、再試行します。**errdisable recovery** コマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダー データ情報を読み取って正確な情報であるかどうかを確認できない場合は、SFP モジュールのエラー メッセージが生成されます。この場合は、SFP モジュールを取り外してから、取り付け直してください。それでもエラーが発生する場合は、SFP モジュールが破損している可能性があります。

SFP モジュール ステータスのモニタ

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理ステータスまたは動作ステータスを確認できます。このコマンドで表示される動作ステータスは、特定インターフェイス上の SFP モジュールの温度や電流、アラーム ステータスなどです。また、このコマンドを使用すると、SFP モジュールの速度とデュプレックスの設定も確認できます。詳細については、このリリースのコマンド リファレンスで、**show interfaces transceiver** コマンドを参照してください。

ping の使用

ここでは、次の情報について説明します。

ping の概要

スイッチは、リモート ホストへの接続テストに使用できる IP ping をサポートしています。ping は、アドレスに対してエコー要求パケットを送信し、応答を待機します。ping は、次のいずれかの応答を返します。

- 正常な応答：正常な応答（*hostname* is alive）は、ネットワーク トラフィックによって異なりますが、1 ～ 10 秒以内に返されます。
- 宛先が応答しない：ホストが応答しない場合は、*no-answer* メッセージが返されます。
- 不明ホスト：ホストが存在しない場合は、*unknown host* メッセージが返されます。
- 宛先到達不能：指定したネットワークにデフォルト ゲートウェイが到達できない場合は、*destination-unreachable* メッセージが返されます。
- ネットワークまたはホストに到達不能：ホストまたはネットワークのルート テーブルにエントリがない場合は、*network or host unreachable* メッセージが返されます。

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、サブネット間の IP ルーティングを設定する必要があります。詳細については、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。

デフォルトでは、すべてのスイッチ上で IP ルーティングがディセーブルになっています。IP ルーティングのイネーブル化または設定が必要な場合は、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。

ネットワーク上の別の装置に対してスイッチから ping を実行するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
ping ip *host* | *address*	IP を通して、またはホスト名やネットワーク アドレスを指定して、リモート ホストに ping を実行します。

（注）　**ping** コマンドには他のプロトコル キーワードもありますが、このリリースではサポートされていません。

次に、IP ホストに ping を実行する例を示します。

```
Switch# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

表 52-1 に、表示される ping 文字出力について説明します。

表 52-1　ping 出力表示文字

文字	説明
!	各感嘆符は、応答が受信されたことを意味します。
.	各ピリオドは、応答待機中にネットワーク サーバがタイムアウトになったことを意味します。
U	宛先到達不能エラー PDU が受信されました。
C	輻輳に遭遇したパケットが受信されました。
I	ユーザがテストを中断しました。
?	パケット タイプが不明です。
&	パケットの存続時間を超過しました。

ping セッションを終了するには、エスケープ シーケンス（デフォルトは Ctrl+^+X）を入力します。Ctrl、Shift、6 の各キーを同時に押してから放し、次に X キーを押します。

レイヤ 2 traceroute の使用

ここでは、次の情報について説明します。

- 「レイヤ 2 traceroute の概要」（P.52-10）
- 「使用上の注意事項」（P.52-11）
- 「物理パスの表示」（P.52-12）

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能を使用すると、送信元装置から宛先装置までパケットが通過する物理パスを、スイッチで識別できます。レイヤ 2 traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。パスの検索には、パス上のスイッチの MAC アドレス テーブルが使用されます。レイヤ 2 traceroute をサポートしていない装置をパス上で検出すると、スイッチはレイヤ 2 トレース クエリーを送信し続け、タイムアウトにします。

スイッチで識別できるのは、送信元装置から宛先装置までのパスだけです。送信元ホストから送信元装置へ、または宛先装置から宛先ホストへのパケットのパスを識別できません。

使用上の注意事項

レイヤ 2 traceroute の使用上の注意事項は次のとおりです。

- ネットワーク内のすべての装置で、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）をイネーブルにする必要があります。CDP をディセーブルにすると、レイヤ 2 traceroute が正しく動作しません。

  レイヤ 2 traceroute をサポートするスイッチの一覧については、「使用上の注意事項」（P.52-11）を参照してください。物理パス内のいずれかの装置が CDP に対してトランスペアレントである場合、スイッチはその装置を通るパスを識別できません。CDP のイネーブル化の詳細については、第 32 章「CDP の設定」を参照してください。

- **ping** 特権 EXEC コマンドを使用して接続をテストできれば、そのスイッチは別のスイッチから到達可能です。物理パス内のすべてのスイッチは、互いに到達可能である必要があります。
- パス内で識別できるホップ数は最大で 10 です。
- 送信元装置から宛先装置までの物理パス上にないスイッチでは、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このスイッチから到達可能である必要があります。
- **traceroute mac** コマンドの出力結果としてレイヤ 2 パスが表示されるのは、指定の送信元および宛先 MAC アドレスが、同一の VLAN に属している場合だけです。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- マルチキャストの送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラー メッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN にある場合、送信元および宛先 MAC アドレス両方の属する VLAN を指定する必要があります。VLAN が指定されないと、パスは識別されず、エラー メッセージが表示されます。
- **traceroute mac ip** コマンドの出力結果にレイヤ 2 パスが表示されるのは、指定の送信元および宛先 IP アドレスが同一のサブネットに属している場合です。IP アドレスを指定した場合、スイッチは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を関連付けます。
  - 指定の IP アドレスの ARP のエントリが存在していた場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
  - ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスが解決されないと、パスは識別されず、エラー メッセージが表示されます。
- 複数の装置がハブを介して 1 つのポートに接続されている場合（1 つのポート上で複数の CDP ネイバーが検出された場合など）は、レイヤ 2 traceroute 機能がサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

物理パスの表示

パケットが通過した送信元装置から宛先装置までの物理パスを表示するには、次のいずれかの特権 EXEC コマンドを使用します。

- **tracetroute mac** [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]
- **tracetroute mac ip** {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

詳細については、このリリースのコマンド リファレンスを参照してください。

IP traceroute の使用

ここでは、次の情報について説明します。

IP traceroute の概要

IP traceroute を使用すると、パケットがネットワークを通過するパスを、ホップバイホップ ベースで識別できます。コマンド出力には、トラフィックが宛先に到達するまでに通過するルータなど、ネットワーク レイヤ（レイヤ 3）のすべての装置が表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先になることができますが、**traceroute** コマンド出力にホップとして表示されるとは限りません。スイッチが traceroute の宛先である場合、traceroute の出力には最終的な宛先として表示されます。同じ VLAN 内のポート間でパケットをブリッジするだけの中間スイッチは、traceroute 出力に表示されません。ただし、中間スイッチが特定のパケットをルーティングするマルチレイヤ スイッチである場合は、traceroute 出力にホップとして表示されます。

traceroute 特権 EXEC コマンドでは、IP ヘッダーの Time To Live（TTL; 存続可能時間）フィールドを使用して、ルータやサーバから特定のメッセージが返されるようにします。traceroute は、まず、TTL フィールドを 1 に設定した User Datagram Protocol（UDP; ユーザ データグラム プロトコル）データグラムを宛先ホストに送信します。ルータは、TTL 値 1 または 0 を検出すると、データグラムを廃棄し、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）の time-to-live-exceeded メッセージを送信元に返します。traceroute は、この ICMP time-to-live-exceeded メッセージの送信元アドレス フィールドを調べることによって、最初のホップのアドレスを判別します。

次のホップを特定するために、traceroute は TTL 値が 2 の UDP パケットを送信します。最初のルータは、TTL フィールドを 1 だけ減らし、次のルータにデータグラムを送信します。2 番めのルータが TTL 値 1 を検出すると、データグラムを廃棄して、time-to-live-exceeded メッセージを送信元に返します。データグラムが宛先ホストに到達できる値に TTL が増分されるまで（または最大 TTL に達するまで）、このプロセスが続行されます。

データグラムが宛先に到達したことを判別できるように、traceroute では、データグラムの UDP 宛先ポート番号を、実際の宛先ホストで使用されないような非常に大きい値に設定します。宛先のホストが受け取ったデータグラムに、ローカルで使用されていない宛先ポート番号が含まれていると、ICMP の *port-unreachable* エラーが送信元に返されます。port-unreachable エラー以外のエラーはすべて中間ホップから生成されるため、port-unreachable エラーの受信は、このメッセージが宛先ポートから送信されたことを意味します。

IP traceroute の実行

パケットがネットワーク上で通過するパスを追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
traceroute ip *host*	パケットがネットワーク上で通過するパスを追跡します。

（注）　**traceroute** 特権 EXEC コマンドには他のプロトコル キーワードもありますが、このリリースではサポートされていません。

次に、IP ホストに **traceroute** を実行する例を示します。

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

  1 172.2.52.1 0 msec 0 msec 4 msec
  2 172.2.1.203 12 msec 8 msec 0 msec
  3 171.9.16.6 4 msec 0 msec 0 msec
  4 171.9.4.5 0 msec 4 msec 0 msec
  5 171.9.121.34 0 msec 4 msec 4 msec
  6 171.9.15.9 120 msec 132 msec 128 msec
  7 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

この表示には、ホップ カウント、ルータの IP アドレス、および送信された 3 つのプローブそれぞれのラウンドトリップ時間（ミリ秒単位）が示されています。

表 52-2　traceroute 出力表示文字

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。
A	管理上の理由で到達不能です。通常、この出力は、アクセス リストでトラフィックがブロックされていることを意味します。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	ソース クエンチ（始点抑制要求）です。
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトは Ctrl+^+X）を入力します。Ctrl、Shift、6 の各キーを同時に押してから放し、次に X キーを押します。

TDR の使用

ここでは、次の情報について説明します。

TDR の概要

Time Domain Reflector（TDR; タイム ドメイン反射率計）機能を使用すると、ケーブル接続の問題を診断および解決できます。TDR を実行すると、ローカルの装置がケーブルに信号を送信し、反射した信号を最初の信号と比較します。

TDR は、銅線のイーサネット 10/100 および 10/100/1000 ポートでサポートされます。SFP モジュール ポートではサポートされません。

TDR で検出できるケーブル接続の問題は、次のとおりです。

- ツイストペア ワイヤのオープン、破損、切断：ワイヤが、リモート装置のワイヤと接続されていません。
- ショートしたツイストペア ワイヤ：ワイヤどうしが接触しているか、リモート装置のワイヤと接触しています。たとえば、ツイストペアのワイヤの一方をもう一方にはんだ付けすると、ショートする可能性があります。

ツイストペア ワイヤの一方がオープンである場合、TDR でオープンであるワイヤの長さを特定できます。

次のような場合にケーブル接続の問題を診断および解決するには、TDR を使用します。

- スイッチの交換
- 配線クローゼットの設定
- 2 つの装置間の接続で、リンクを確立できない場合や、リンクが正常に動作しない場合のトラブルシューティング

TDR の実行と結果の表示

TDR を実行するには、**test cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを入力します。

結果を表示するには、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを入力します。表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

debug コマンドの使用

ここでは、**debug** コマンドを使用してインターネットワーキングの問題を診断および解決する方法について説明します。

注意　デバッグ出力には、CPU プロセスで高いプライオリティが割り当てられるので、システムが使用不能になる可能性があります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合だけにしてください。**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザ数が少ないときに使用するのが最良です。このような時間帯を選んでデバッグを実行すると、**debug** コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。

（注）　特定の **debug** コマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

特定の機能に関するデバッグのイネーブル化

debug コマンドはすべて、特権 EXEC モードで実行します。ほとんどの **debug** コマンドには引数がありません。たとえば、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）に関するデバッグをイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# debug span-session
```

スイッチからの出力の生成は、このコマンドの **no** 形式を入力するまで続きます。

debug コマンドをイネーブルにしても出力が表示されない場合、次の可能性が考えられます。

- スイッチが適切に設定されていないため、モニタ対象のトラフィック タイプが生成されていない可能性があります。**show running-config** コマンドを使用して設定を確認してください。
- スイッチが正しく設定されていても、デバッグをイネーブルにした時点で、モニタ対象のトラフィック タイプが生成されていない可能性があります。デバッグ対象の機能に応じて、TCP/IP **ping** コマンドなどを使用し、ネットワーク トラフィックを生成してください。

SPAN のデバッグをディセーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# no debug span-session
```

また、この代わりに、特権 EXEC モードで、このコマンドの **undebug** 形式を入力することもできます。

```
Switch# undebug span-session
```

各デバッグ オプションのステートを表示するには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# show debugging
```

システム全体の診断のイネーブル化

システム全体の診断をイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# debug all
```

注意　デバッグ出力は、他のネットワーク トラフィックよりも優先されます。また、**debug all** 特権 EXEC コマンドでは、他の **debug** コマンドよりも大量の出力が生成されます。このため、スイッチのパフォーマンスが大幅に低下したり、場合によっては使用不能になったりする可能性があります。**debug** コマンドは、対象をなるべく限定して使用してください。

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。**no debug all** コマンドを使用すると、誤ってイネーブルにされたままの **debug** コマンドも、確実にディセーブルにできます。

デバッグ メッセージとエラー メッセージのリダイレクト

デフォルトでは、ネットワーク サーバからの **debug** コマンド出力やシステム エラー メッセージがコンソールに送信されます。このデフォルトを使用する場合、コンソール ポートに接続する代わりに仮想端末接続を使用して、デバッグ出力をモニタすることもできます。

宛先として使用できるのは、コンソール、仮想端末、内部バッファ、syslog サーバが動作している UNIX ホストなどです。syslog 形式は、4.3 Berkeley Standard Distribution（BSD）UNIX およびその派生 OS と互換性があります。

（注）　デバッグの宛先によって、システムのオーバーヘッドが異なります。ログ メッセージの宛先をコンソールにすると、オーバーヘッドが非常に大きくなりますが、宛先を仮想端末にすると、それよりも小さくなります。ログ メッセージの宛先を syslog サーバにすると、オーバーヘッドはさらに小さくなります。最もオーバーヘッドが小さいのは、内部バッファへの出力です。

システム メッセージ ロギングの詳細については、第 35 章「システム メッセージ ロギングの設定」を参照してください。

show platform forward コマンドの使用

show platform forward 特権 EXEC コマンドを使用すると、システム経由でインターフェイスに入るパケットの転送結果に関して、有用な情報が出力されます。パケットに関して入力されたパラメータに応じて、検索テーブル結果、転送先の計算に使用されるポート マップ、ビットマップ、および出力側の情報が表示されます。

（注）　**show platform forward** コマンドの構文および使用方法の詳細については、このリリースのスイッチのコマンド リファレンスを参照してください。

このコマンド出力の大部分はテクニカル サポート担当者向けの情報で、スイッチの application-specific integrated circuit（ASIC; 特定用途向け集積回路）に関する調査に役立ちます。しかし、パケット転送情報はトラブルシューティングにも役立ちます。

次に、VLAN 5 のポート 1 に入るパケットの宛先が未知の MAC アドレスである場合の、**show platform forward** コマンドの出力例を示します。このパケットは、VLAN 5 内のすべてのポートにフラッディングされます。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2
udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                    Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA    03000000
L2Local  80_00050002_00020002-00_00000000_00000000     00C71    0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

=========================================
```

```
Egress:Asic 2, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/1    0005 0001.0001.0001  0002.0002.0002

----------------------------------------
Packet 2
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/1    0005 0001.0001.0001  0002.0002.0002

----------------------------------------
<output truncated>
----------------------------------------
Packet 10
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000
Packet dropped due to failed DEJA_VU Check on Gi1/0/2
Packet dropped due to failed DEJA_VU Check on Gi1/2
```

次に、VLAN 5 のポート 1 に着信するパケットが、VLAN 内の別のポートで学習済みのアドレスに送信される場合の出力例を示します。この場合、アドレスが学習されているポートから転送されます。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                   Key-Used                    Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050009_43A80145-00_00000000_00000000     00086   02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003

========================================
Egress:Asic 3, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port            Vlan      SrcMac          DstMac    Cos  Dscpv
interface-id    0005 0001.0001.0001  0009.43A8.0145
```

次に、VLAN 5 のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されており、宛先 IP アドレスが未知である場合の出力例を示します。デフォルト ルートが設定されていないため、パケットは廃棄されます。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
```

```
Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_0D020202     010F0   01880290
L3Scndr  12_0D020202_0D010101-00_40000014_000A0000     034E0   000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000
```

次に、VLAN 5 のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されており、宛先 IP アドレスが IP ルーティング テーブル内の IP アドレスに設定されている場合の出力例を示します。この場合、ルーティング テーブルの指定どおりに転送されます。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_10010A05_0A010505-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_10010A05     010F0   01880290
L3Scndr  12_10010A05_0A010505-00_40000014_000A0000     01D28   30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

========================================
Egress:Asic 3, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                    Key-Used                     Index-Hit  A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/2    0007 XXXX.XXXX.0246  0009.43A8.0147
```

crashinfo ファイルの使用

crashinfo ファイルには、シスコのテクニカル サポート担当者が Cisco IOS イメージの障害（クラッシュ）の原因となる問題をデバッグする際に役立つ情報が保存されます。スイッチのクラッシュ情報は、障害発生時にコンソールに出力されます。スイッチによって作成される crashinfo ファイルは、次の 2 種類です。

- 基本 crashinfo ファイル：障害発生後、初めて Cisco IOS イメージを起動するときに、自動的に作成されます。
- 拡張 crashinfo ファイル：システム障害発生時に自動的に作成されます。

基本 crashinfo ファイル

基本ファイルには、障害が発生した Cisco IOS のイメージ名とバージョン、プロセッサ レジスタのリスト、およびその他のスイッチ固有の情報が含まれます。**show tech-support** 特権 EXEC コマンドを使用すると、この情報をシスコのテクニカル サポート担当者に提供できます。

基本 crashinfo ファイルは、フラッシュ ファイル システムの次のディレクトリに格納されます。

flash:/crashinfo/

ファイル名は crashinfo_*n*（*n* はシーケンス番号）です。

新しい crashinfo ファイルが作成されるたびに、既存のシーケンス番号よりも大きいシーケンス番号が使用されます。したがって、最大のシーケンス番号を持つファイルには、最新の障害が記述されています。スイッチにはリアルタイム クロックがないため、タイムスタンプの代わりにバージョン番号が使用されます。ファイル作成時にシステムによって使用されるファイル名を変更できません。ファイルの作成後に、**rename** 特権 EXEC コマンドを使用して名前を変更することはできますが、ファイル名を変更した場合、**show tech-support** 特権 EXEC コマンドで内容を表示できなくなります。**delete** 特権 EXEC コマンドを使用すると、crashinfo ファイルを削除できます。

最新の基本 crashinfo ファイル（ファイル名末尾のシーケンス番号が最も大きいファイル）を表示するには、**show tech-support** 特権 EXEC コマンドを入力します。このファイルには、**more** または **copy** 特権 EXEC コマンドなど、コピーや表示を行うコマンドを使用してアクセスすることもできます。

拡張 crashinfo ファイル

スイッチの拡張 crashinfo ファイルは、システム障害発生時に作成されます。拡張ファイルには、スイッチの障害の原因を判別するのに役立つその他の追加情報が含まれます。この情報をシスコのテクニカル サポート担当者に提供するには、ファイルに手動でアクセスし、**more** または **copy** 特権 EXEC コマンドを使用します。

拡張 crashinfo ファイルは、フラッシュ ファイル システムの次のディレクトリに格納されます。
flash:/crashinfo_ext/

ファイル名は crashinfo_ext_*n*（*n* はシーケンス番号）です。

no exception crashinfo グローバル コンフィギュレーション コマンドを使用すると、拡張 creashinfo ファイルが作成されないようにスイッチを設定できます。

トラブルシューティング用の表

次の表に、Cisco.com のトラブルシューティング関連マニュアルの抜粋を示します。

- 「CPU 使用率のトラブルシューティング」（P.52-19）

CPU 使用率のトラブルシューティング

ここでは、CPU 使用率が高すぎる場合に起きる可能性のある症状と、CPU 使用率の問題を確認する方法について説明します。表 52-3 に、特定可能な CPU 使用率の問題の主な種類を示します。考えられる原因と修正措置を述べ、Cisco.com の『*Troubleshooting High CPU Utilization*』へのリンクも示します。

高 CPU 使用率による症状

CPU 使用率が高すぎると次のような症状が起きることがありますが、これらの症状が他の原因で起きる場合もあります。

- スパニング ツリー トポロジの変更
- 通信切断による EtherChannel リンクのダウン
- 管理要求への応答なし（ICMP ping、SNMP タイムアウト、Telnet セッションや SSH セッションの速度低下）
- UDLD フラッピング
- 容認可能なスレッシュホールドを超えた SLA 応答が原因の IP SLA 障害

- スイッチが要求を転送しないか応答しない場合の DHCP または IEEE 802.1x の障害

レイヤ 3 スイッチの場合

- パケットの廃棄、またはソフトウェアでルーティングされるパケットの遅延増大
- BGP または OSPF ルーティング トポロジの変更
- HSRP フラッピング

問題と原因の確認

高 CPU 使用率が問題になるかどうかを判断するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の最初の行の下線部を見てください。

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

次に、正常な CPU 使用率の例を示します。出力によると、過去 5 秒間の使用率は *8%/0%* で、意味は次のとおりです。

- 合計 CPU 使用率は、Cisco IOS プロセスの実行時間と割り込みの処理時間を含めて 8% です。
- 割り込みの処理時間は 0% です。

表 52-3　CPU 使用率の問題のトラブルシューティング

問題の種類	原因	修正措置
割り込みの比率と合計 CPU 使用率の値がほぼ等しい。	CPU がネットワークから受け取るパケット数が多すぎます。	ネットワーク パケットの送信元を特定します。フローを停止するか、スイッチの設定を変更します。「Analyzing Network Traffic」を参照してください。
合計 CPU 使用率が 50% を超えているが、割り込みの処理時間が最小。	1 つ以上の Cisco IOS プロセスに非常に多くの CPU 時間が消費されています。通常、プロセスをアクティブ化したイベントがきっかけで発生します。	異常なイベントを特定し、根本原因をトラブルシューティングします。「Debugging Active Processes」を参照してください。

CPU 使用率と、使用率の問題のトラブルシューティング方法の詳細については、Cisco.com の『*Troubleshooting High CPU Utilization*』を参照してください。

APPENDIX A

サポートされる MIB

この付録では、このリリースでサポートされる IE 3000 スイッチの Management Information Base（MIB; 管理情報ベース）の一覧を示します。この付録で説明する内容は、次のとおりです。

MIB の一覧

- BRIDGE-MIB

（注） BRIDGE-MIB は、単一の VLAN のコンテキストをサポートします。デフォルトでは、設定済みのコミュニティ ストリングを使用している Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）メッセージは、常に VLAN 1 の情報を提供します。他の VLAN（VLAN x など）の BRIDGE-MIB 情報を取得するには、SNMP メッセージ内でコミュニティ ストリング「設定済みのコミュニティ ストリング@x」を使用します。

- CISCO-ADMISSION-POLICY-MIB
- CISCO-AUTH-FRAMEWORK-MIB
- CISCO-CABLE-DIAG-MIB
- CISCO-CDP-MIB
- CISCO-CLUSTER-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-ERR-DISABLE-MIB
- CISCO-FLASH-MIB（すべてのスイッチのフラッシュ メモリがリムーバブル フラッシュ メモリとしてモデル化されています）
- CISCO-FTP-CLIENT-MIB

- CISCO-HSRP-MIB
- CISCO-HSRP-EXT-MIB（一部サポート）
- CISCO-IETF-IP-MIB
- CISCO-IETF-IP-FORWARDING-MIB
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO IP-STAT-MIB
- CISCO-L2L3-INTERFACE-CONFIG-MIB
- CISCO-LAG-MIB
- CISCO-MAC-AUTH-BYPASS
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NAC-NAD-MIB
- CISCO-PAE-MIB
- CISCO-PAGP-MIB
- CISCO-PING-MIB
- CISCO-PORT-QOS-MIB（パケット カウンタだけをサポート。オクテット カウンタは対象外）
- CISCO-PRODUCTS-MIB
- CISCO-PROCESS-MIB
- CISCO-RTTMON-MIB
- CISCO-SMI-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SYSLOG-MIB
- CISCO-TC-MIB
- CISCO-TCP-MIB
- CISCO-UDLDP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- CISCO-CONFIG-COPY-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- IEEE8021-PAE-MIB
- IEEE8023-LAG-MIB
- IF-MIB（VLAN の入出力カウンタはサポートされません）
- IGMP-MIB
- INET-ADDRESS-MIB
- IPMROUTE-MIB

- LLDP MED MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TCP-MIB
- OLD-CISCO-TS-MIB
- PIM-MIB
- RFC1213-MIB（機能は CISCO-RFC1213-CAPABILITY.my で指定されているエージェント機能によります）
- RFC1253-MIB（OSPF-MIB）
- RMON-MIB
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- TCP-MIB
- UDP-MIB

（注）　IE3000 スイッチでサポートされる MIB の一覧については、次も参照してください。
ftp://ftp.cisco.com/pub/mibs/supportlists/ie3000/ie3000-supportlist.html

MIB とシスコ製品に関するその他の情報については、シスコの Web サイトを参照してください。
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

FTP による MIB ファイルへのアクセス

各 MIB ファイルを入手する手順は、次のとおりです。

ステップ 1　使用する FTP クライアントが passive モードであることを確認してください。

（注）　passive モードがサポートされていない FTP クライアントもあります。

ステップ 2　FTP を使用してサーバ **ftp.cisco.com** にアクセスします。

ステップ 3　ユーザ名 **anonymous** を使用してログインします。

ステップ 4　パスワードが要求されたら、E メールのユーザ名を入力します。

ステップ 5　`ftp>` プロンプトで、ディレクトリを **/pub/mibs/v1** および **/pub/mibs/v2** に変更します。

ステップ 6　**get** *MIB_filename* コマンドを使用して、MIB ファイルのコピーを入手します。

APPENDIX B

Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作

この付録では、IE 3000 スイッチ フラッシュ ファイル システムの操作方法、コンフィギュレーション ファイルのコピー方法、およびスイッチへのソフトウェア イメージのアーカイブ（アップロードとダウンロード）方法について説明します。

（注） この章で使用しているコマンドの構文と使用方法の詳細については、このリリースのスイッチのコマンド リファレンスおよび Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。

この付録で説明する内容は、次のとおりです。

フラッシュ ファイル システムの操作

フラッシュ ファイル システムは、ファイルを格納できる単一のフラッシュ装置です。また、このシステムには、ソフトウェア イメージとコンフィギュレーション ファイルを管理するのに役立つ複数のコマンドも用意されています。スイッチのデフォルトのフラッシュ ファイル システムは *flash:* です。

スイッチには、Cisco IOS ソフトウェアのイメージおよびコンフィギュレーション ファイルを格納するリムーバブル コンパクト フラッシュ カードがあります。コンパクト フラッシュ カードを取り外しても、Cisco IOS ソフトウェアのリロードが必要にならない限り、スイッチ動作は中断されません。ただし、コンパクト フラッシュ カードを取り外すと、フラッシュ ファイル システムにアクセスできなくなり、アクセスを試みるとエラー メッセージが生成されます。

コンパクト フラッシュ ファイルの設定を表示するには、**show flash:** 特権 EXEC コマンドを使用します。このコマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf009.html#wp1018357

スイッチのコンパクト フラッシュ メモリ カードの取り外しまたは交換方法については、『*Cisco IE 3000 Hardware Installation Guide*』を参照してください。

ここでは、次の設定情報について説明します。

使用可能なファイル システムの表示

スイッチで使用可能なファイル システムを表示するには、**show file systems** 特権 EXEC コマンドを使用します（次の例を参照）。

```
Switch# show file systems
File Systems:
     Size(b)     Free(b)      Type  Flags   Prefixes
*   15998976     5135872     flash     rw   flash:flash3:
           -           -    opaque     rw   bs:
           -           -    opaque     rw   vb:
      524288      520138     nvram     rw   nvram:
           -           -   network     rw   tftp:
           -           -    opaque     rw   null:
           -           -    opaque     rw   system:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
```

表 B-1　show file systems のフィールドの説明

フィールド	値
Size(b)	ファイル システムのメモリの容量（バイト単位）。
Free(b)	ファイル システムのメモリの空き容量（バイト単位）。
Type	ファイル システムのタイプ。 **flash**：ファイル システムはフラッシュ メモリ装置用です。 **nvram**：ファイル システムは Nonvolatile RAM（NVRAM; 不揮発性 RAM）装置用です。 **opaque**：ファイル システムはローカルに生成された *pseudo* ファイル システム（*system* など）または brimux などのダウンロード インターフェイスです。 **unknown**：ファイル システムのタイプは不明です。

表 B-1　show file systems のフィールドの説明 （続き）

フィールド	値
Flags	ファイル システムの権限。 **ro**：読み取り専用です。 **rw**：読み取り / 書き込みです。 **wo**：書き込み専用です。
Prefixes	ファイル システムのエイリアス。 **flash:**：フラッシュ ファイル システムです。 **nvram:**：NVRAM です。 **null:**：コピーのヌル宛先です。リモート ファイルをヌルにコピーして、サイズを判別できます。 **rcp:**：Remote Copy Protocol（RCP; リモート コピー プロトコル）ネットワーク サーバです。 **system:**：実行コンフィギュレーションを含むシステム メモリを格納しています。 **tftp:**：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）ネットワーク サーバです。 **xmodem:**：Xmodem プロトコルを使用してネットワーク マシンからファイルを取得します。 **ymodem:**：Ymodem プロトコルを使用してネットワーク マシンからファイルを取得します。

デフォルトのファイル システムの設定

システムでデフォルトのファイル システムとして使用されるファイル システムまたはディレクトリを指定するには、**cd** *filesystem:* 特権 EXEC コマンドを使用します。デフォルトのファイル システムを設定すると、関連コマンドから *filesystem:* 引数を省略できます。たとえば、オプションの *filesystem:* 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは *flash:* です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

ファイル システムのファイルに関する情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコンフィギュレーション ファイルがすでに含まれていないかどうかを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマンドで使用できます。

ファイル システムのファイルに関する情報を表示するには、表 B-2 に示す特権 EXEC コマンドのいずれかを使用します。

表 B-2　ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [**/all**] [*filesystem***:**][*filename*]	ファイル システムのファイルのリストを表示します。
show file systems	ファイル システムの各ファイルの詳細を表示します。
show file information *file-url*	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイル記述子のリストを表示します。ファイル記述子は、開いているファイルの内部表現です。このコマンドを使用して、別のユーザがファイルを開いているかどうかを確認できます。

ディレクトリの変更および作業ディレクトリの表示

ディレクトリの変更や作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 システム ボード フラッシュ装置の場合、*filesystem***:** に **flash:** を使用します。
ステップ 2	**cd new_configs**	目的のディレクトリに変更します。 コマンド例では、*new_configs* というディレクトリに変更する方法を示します。
ステップ 3	**pwd**	作業ディレクトリを表示します。

ディレクトリの作成および削除

ディレクトリを作成および削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 システム ボード フラッシュ装置の場合、*filesystem***:** に **flash:** を使用します。
ステップ 2	**mkdir old_configs**	新しいディレクトリを作成します。 コマンド例では、*old_configs* というディレクトリを作成する方法を示します。 ディレクトリ名は、大文字と小文字が区別されます。 スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。
ステップ 3	**dir** *filesystem***:**	設定を確認します。

ディレクトリを、そのディレクトリのすべてのファイルおよびサブディレクトリとともに削除するには、**delete /force /recursive** *filesystem***:***/file-url* 特権 EXEC コマンドを使用します。

指定したディレクトリとそのディレクトリに含まれるすべてのサブディレクトリおよびファイルを削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに削除を確認するプロンプトを抑制するには、**/force** キーワードを使用します。削除プロセスの最初に 1 回だけプロンプトが表示されます。**archive download-sw** コマンドを使用してインストールされたが、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

システム ボード フラッシュ装置の場合、*filesystem* に **flash:** を使用します。*file-url* には、削除するディレクトリの名前を入力します。ディレクトリ内のすべてのファイルとディレクトリが削除されます。

注意　ファイルとディレクトリが削除されると、その内容は回復できません。

ファイルのコピー

ファイルをコピー元からコピー先にコピーするには、**copy** *source-url destination-url* 特権 EXEC コマンドを使用します。コピー元とコピー先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドを実行すると、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存されて、システム初期化中の設定として使用されます。

Xmodem または Ymodem プロトコルを使用するネットワーク マシンのファイルのコピー元として特殊なファイル システム（**xmodem:**、**ymodem:**）を指定し、そこからコピーすることもできます。

ネットワーク ファイル システムの URL には、**ftp:**、**rcp**:、および **tftp:** が含まれます。構文は次のとおりです。

- File Transfer Protocol（FTP; ファイル転送プロトコル）：**ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/filename*
- RCP：**rcp:**[[*//username***@***location*]*/directory*]*/filename*
- TFTP：**tftp:**[[*//location*]*/directory*]*/filename*

ローカルの書き込み可能なファイル システムには flash: が含まれます。

コピー元とコピー先の組み合わせには無効なものがあります。特に、次の組み合わせはコピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- ある装置から同じ装置へ（たとえば、**copy flash: flash:** コマンドは無効）

コンフィギュレーション ファイルでの **copy** コマンドの具体的な使用例については、「コンフィギュレーション ファイルの操作」（P.B-9）を参照してください。

新しいバージョンをダウンロードするか、または既存のバージョンをアップロードしてソフトウェア イメージをコピーするには、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドを使用します。詳細については、「ソフトウェア イメージの操作」（P.B-25）を参照してください。

ファイルの削除

フラッシュ メモリ装置のファイルが不要になった場合は、そのファイルを完全に削除できます。指定したフラッシュ装置からファイルまたはディレクトリを削除するには、**delete** [**/force**] [**/recursive**] [*filesystem***:**]*/file-url* 特権 EXEC コマンドを使用します。

ディレクトリとそのディレクトリに含まれるすべてのサブディレクトリおよびファイルを削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに削除を確認するプロンプトを抑制するには、**/force** キーワードを使用します。削除プロセスの最初に 1 回だけプロンプトが表示されます。**archive download-sw** コマンドを使用してインストールされたが、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

*filesystem***:** オプションを省略すると、スイッチでは **cd** コマンドで指定されたデフォルトの装置が使用されます。*file-url* には、削除するファイルのパス（ディレクトリ）と名前を指定します。

ファイルを削除しようとすると、削除の確認を要求するプロンプトが表示されます。

注意　ファイルが削除されると、その内容は回復できません。

次に、デフォルトのフラッシュ メモリ装置からファイル *myconfig* を削除する例を示します。

```
Switch# delete myconfig
```

tar ファイルの作成、表示、および抽出

以降の項で説明するように、tar ファイルを作成してその tar ファイルにファイルを書き込んだり、tar ファイル内のファイルを一覧表示したり、tar ファイルからファイルを抽出したりできます。

（注）　ソフトウェア イメージをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドを使用する代わりに、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

tar ファイルの作成

tar ファイルを作成してその tar ファイルにファイルを書き込むには、次の特権 EXEC コマンドを使用します。

archive tar /create *destination-url* **flash:***/file-url*

destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL エイリアスおよび作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:
- FTP の場合の構文は次のとおりです。
  ftp:[[*//username*[**:***password*]**@***location*]*/directory]/tar-filename***.tar**
- RCP の場合の構文は次のとおりです。
  rcp:[[*//username***@***location*]*/directory*]*/tar-filename***.tar**
- TFTP の場合の構文は次のとおりです。
  tftp:[[*//location*]*/directory*]*/tar-filename***.tar**

*tar-filename***.tar** は、作成する tar ファイルです。

flash:*/file-url* には、新しい tar ファイルが作成されるローカル フラッシュ ファイル システムの場所を指定します。送信元ディレクトリ内のファイルまたはディレクトリのオプションのリストを指定して、新しい tar ファイルに書き込むこともできます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

次の例では、tar ファイルを作成する方法を示します。このコマンドはローカル フラッシュ装置の *new-configs* ディレクトリの内容を、172.20.10.30 の TFTP サーバの *saved.tar* というファイルに書き込みます。

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

tar ファイルの内容の表示

tar ファイルの内容を画面に表示するには、次の特権 EXEC コマンドを使用します。

archive tar /table *source-url*

source-url には、ローカルまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:
- FTP の場合の構文は次のとおりです。
  ftp:[[*//username*[**:***password*]**@***location*]*/directory*]*/tar-filename***.tar**
- RCP の場合の構文は次のとおりです。
  rcp:[[*//username***@***location*]*/directory*]*/tar-filename***.tar**
- TFTP の場合の構文は次のとおりです。
  tftp:[[*//location*]*/directory*]*/tar-filename***.tar**

*tar-filename***.tar** は、表示する tar ファイルです。

tar ファイルの後ろにファイルまたはディレクトリのオプションのリストを指定して、表示するファイルを制限することもできます。この場合は、リスト内のファイルだけが表示されます。何も指定されないと、すべてのファイルとディレクトリが表示されます。

次に、フラッシュ メモリ内にあるスイッチ tar ファイルの内容を表示する例を示します。

```
Switch# archive tar /table flash:image-name.tar
image-name/ (directory)
image-name/html/ (directory)
image-name/html/foo.html (0 bytes)
image-name/image-name.bin (610856 bytes)
image-name/info (219 bytes)
```

次に、*/html* ディレクトリおよびその内容だけを表示する例を示します。

```
Switch# archive tar /table flash: image-name/html
cimage-name/html
cimage-name/html/ (directory)
cimage-name/html/const.htm (556 bytes)
cimage-name/html/xhome.htm (9373 bytes)
cimage-name/html/menu.css (1654 bytes)
<output truncated>
```

tar ファイルの抽出

tar ファイルをフラッシュ ファイル システム上のディレクトリに抽出するには、次の特権 EXEC コマンドを使用します。

archive tar /xtract source-url flash:/file-url [*dir/file...***]**

source-url には、ローカル ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:
- FTP の場合の構文は次のとおりです。
  ftp:[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar**
- RCP の場合の構文は次のとおりです。
  rcp:[[//*username***@***location*]/*directory*]/*tar-filename***.tar**
- TFTP の場合の構文は次のとおりです。
  tftp:[[//*location*]/*directory*]/*tar-filename***.tar**

*tar-filename***.tar** は、ファイルの抽出が行われる tar ファイルです。

flash:/*file-url* [*dir/file...*] には、tar ファイルが抽出されるローカル フラッシュ ファイル システムの場所を指定します。tar ファイルから抽出されるファイルまたはディレクトリのオプション リストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

次に、172.20.10.30 の TFTP サーバにある tar ファイルの内容を抽出する例を示します。このコマンドは、*new-configs* ディレクトリだけを、ローカル フラッシュ ファイル システムのルート（root）ディレクトリに抽出します。*saved.tar* ファイルの残りのファイルは無視されます。

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

ファイルの内容の表示

リモート ファイル システム上のファイルを含む、読み取り可能ファイルの内容を表示するには、**more** [**/ascii** | **/binary** | **/ebcdic**] *file-url* 特権 EXEC コマンドを使用します。

次に、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示する例を示します。

```
Switch# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

コンフィギュレーション ファイルの操作

ここでは、コンフィギュレーション ファイルを作成、ロード、およびメンテナンスする方法を説明します。

コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力されたコマンドが含まれています。基本のコンフィギュレーション ファイルを作成するには、**setup** プログラムを使用するか、**setup** 特権 EXEC コマンドを入力します。詳細については、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」を参照してください。

TFTP、FTP、または RCP サーバからスイッチの実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにコンフィギュレーション ファイルをコピー（*ダウンロード*）できます。この操作は、次のいずれかの理由で実行できます。

- バックアップ コンフィギュレーション ファイルを復元するため。
- コンフィギュレーション ファイルを別のスイッチに使用するため。たとえば、別のスイッチをネットワークに追加して、そのスイッチを元のスイッチと同様に設定できます。ファイルを新しいスイッチにコピーすると、ファイル全体を再作成しないで、関連する部分を変更できます。
- ネットワーク内のすべてのスイッチに対して同じコンフィギュレーション コマンドをロードして、すべてのスイッチを同様に設定するため。

TFTP、FTP、または RCP を使用して、スイッチからファイル サーバにコンフィギュレーション ファイルをコピー（*アップロード*）できます。この作業を行って、あとでサーバから元のコンフィギュレーション ファイルを復元できるように、現在のコンフィギュレーション ファイルの内容を変更する前にそのファイルをサーバにバックアップできます。

使用するプロトコルは、使用しているサーバのタイプによって異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが高速になり、より確実にデータが配信されます。このような改善が実現できるのは、FTP と RCP が、コネクション型 TCP/IP スタックに基づいて構築され、このスタックを使用しているからです。

ここでは、次の設定情報について説明します。

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成すると、スイッチを設定するときに役に立ちます。コンフィギュレーション ファイルには、1 つまたは複数のスイッチを設定するために必要なコマンドの一部、またはすべてを含めることができます。たとえば、ハードウェア設定が同じ複数のスイッチに、同じコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成する場合、次の注意事項があります。

- スイッチを初期設定する場合は、コンソール ポートから接続することを推奨します。コンソール ポートへの直接接続ではなく、ネットワーク接続を介してスイッチにアクセスすると、設定の変更（スイッチの IP アドレスの変更やポートのディセーブル化など）によっては、スイッチとの接続が失われる場合があることに注意してください。
- スイッチにパスワードを設定していない場合は、**enable secret** *secret-password* グローバル コンフィギュレーション コマンドを使用してパスワードを設定することを推奨します。

（注）　**copy** {**ftp:** | **rcp:** | **tftp:**} **system:running-config** 特権 EXEC コマンドを実行すると、コマンドラインにコマンドを入力している場合と同じように、スイッチにコンフィギュレーション ファイルがロードされます。コマンドを追加するまで、スイッチは既存の実行コンフィギュレーションを消去しません。コピーされたコンフィギュレーション ファイル内のコマンドによって、既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドが消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存の設定に格納されている IP アドレスと異なる場合は、コピーされた設定内の IP アドレスが使用されます。ただし、既存の設定内のコマンドの中には、置き換えたり無効にできないものがあります。この場合、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わされた（コピーされたコンフィギュレーション ファイルが優先する）コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルを、サーバに格納されているファイルの正確なコピーに復元するには、コンフィギュレーション ファイルを直接スタートアップ コンフィギュレーションにコピーして（**copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** 特権 EXEC コマンドを使用して）、スイッチをリロードします。

コンフィギュレーション ファイルのタイプおよび場所

スタートアップ コンフィギュレーション ファイルは、ソフトウェアを設定するために、システムの起動中に使用されます。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が含まれています。2 つのコンフィギュレーション ファイルは異なる場合があります。たとえば、一時的に設定を変更する場合があります。この場合は、実行コンフィギュレーションを変更したあと、**copy running-config startup-config** 特権 EXEC コマンドで設定を保存しないようにします。

実行コンフィギュレーションは Dynamic Random Access Memory（DRAM; ダイナミック ランダム アクセス メモリ）に保存されます。スタートアップ コンフィギュレーションは、フラッシュ メモリの NVRAM セクションに格納されます。

テキスト エディタを使用したコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成する場合は、システムが適切に応答できるように、コマンドを論理的にリストする必要があります。次に、コンフィギュレーション ファイルの作成方法を 1 つ示します。

ステップ 1　スイッチからサーバに既存の設定をコピーします。

詳細については、「TFTP を使用したコンフィギュレーション ファイルのダウンロード」（P.B-12）、「FTP を使用したコンフィギュレーション ファイルのダウンロード」（P.B-14）、または「RCP を使用したコンフィギュレーション ファイルのダウンロード」（P.B-18）を参照してください。

ステップ 2　UNIX の場合は vi や emacs、PC の場合はメモ帳などのテキスト エディタでコンフィギュレーション ファイルを開きます。

ステップ 3　目的のコマンドを含むコンフィギュレーション ファイルの部分を抽出して、新しいファイルに保存します。

ステップ 4　コンフィギュレーション ファイルをサーバの適切な場所にコピーします。たとえば、ファイルをワークステーションの TFTP ディレクトリ（UNIX ワークステーションの場合は、通常は /tftpboot ）にコピーします。

ステップ 5　ファイルの権限が world-read に設定されていることを確認します。

TFTP を使用したコンフィギュレーション ファイルのコピー

作成したコンフィギュレーション ファイル、あるいは別のスイッチまたは TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定できます。コンフィギュレーション ファイルを TFTP サーバにコピー（アップロード）して、格納できます。

ここでは、次の設定情報について説明します。

- 「TFTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-11）
- 「TFTP を使用したコンフィギュレーション ファイルのダウンロード」（P.B-12）
- 「TFTP を使用したコンフィギュレーション ファイルのアップロード」（P.B-13）

TFTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードまたはアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションで、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

（注）　/etc/inetd.conf ファイルおよび /etc/services ファイルを変更したあとに、inetd デーモンを再起動する必要があります。デーモンを再起動するには、inetd プロセスを停止して再起動するか、**fastboot** コマンド（SunOS 4.x 上）または **reboot** コマンド（Solaris 2.x または SunOS 5.x 上）を入力します。TFTP デーモンの詳細については、使用しているワークステーションのマニュアルを参照してください。

- スイッチに、TFTP サーバへのルートがあることを確認します。サブネット間のトラフィックをルーティングするルータがない場合は、スイッチと TFTP サーバが同じサブネットワーク内にある必要があります。TFTP サーバへの接続を確認するには、**ping** コマンドを使用します。
- ダウンロードするコンフィギュレーション ファイルが、TFTP サーバ上の正しいディレクトリ（UNIX ワークステーションの場合は通常 /tftpboot）にあることを確認します。
- ダウンロード処理の場合は、ファイルに対する権限が正しく設定されていることを確認します。ファイルに対する権限は world-read である必要があります。
- コンフィギュレーション ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要がある場合があります。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* は、ファイルをサーバにアップロードするときに使用するファイル名です。
- アップロード処理中に、サーバで既存のファイル（空のファイルを作成する必要があった場合は空のファイルも含む）を上書きする場合は、ファイルに対する権限が正しく設定されていることを確認します。ファイルに対する権限は world-write である必要があります。

TFTP を使用したコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

ステップ 1　コンフィギュレーション ファイルをワークステーション上の適切な TFTP ディレクトリにコピーします。

ステップ 2　「TFTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-11）を参照して、TFTP サーバが適切に設定されていることを確認します。

ステップ 3　コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。

ステップ 4　TFTP サーバからコンフィギュレーション ファイルをダウンロードし、スイッチを設定します。

TFTP サーバの IP アドレスまたはホスト名とダウンロードするファイルの名前を指定します。

次のいずれかの特権 EXEC コマンドを使用します。

- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **system:running-config**
- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **nvram:startup-config**

コンフィギュレーション ファイルがダウンロードされ、ファイルが行単位で解析されるときにコマンドが実行されます。

次に、IP アドレス 172.16.2.155 にあるファイル *tokyo-confg* からソフトウェアを設定する例を示します。

```
Switch# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

TFTP を使用したコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして格納するには、次の手順を実行します。

ステップ 1　「TFTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-11）を参照して、TFTP サーバが適切に設定されていることを確認します。

ステップ 2　コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。

ステップ 3　スイッチ設定を TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名および宛先のファイル名を指定します。

次のいずれかの特権 EXEC コマンドを使用します。

- **copy system:running-config tftp:**[[[*//location*]*/directory*]*/filename*]
- **copy nvram:startup-config tftp:**[[[*//location*]*/directory*]*/filename*]

ファイルは TFTP サーバにアップロードされます。

次に、スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードする例を示します。

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [OK]
```

FTP を使用したコンフィギュレーション ファイルのコピー

FTP サーバに、または FTP サーバから、コンフィギュレーション ファイルをコピーできます。

FTP では、クライアントが FTP 要求ごとにリモート ユーザ名とパスワードをサーバに送信する必要があります。FTP を使用してスイッチからサーバにコンフィギュレーション ファイルをコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- anonymous。

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）。
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）。
- スイッチは、*username@switchname.domain* というパスワードを作成します。変数 *username* は現在のセッションに関連付けられているユーザ名です。*switchname* は設定されたホスト名です。*domain* はスイッチのドメインです。

ユーザ名とパスワードは、FTP サーバのアカウントに関連付けられる必要があります。サーバに書き込んでいる場合は、FTP の書き込み要求が受け付けられるように FTP サーバを適切に設定する必要があります。

ip ftp username および **ip ftp password** コマンドを使用して、すべてのコピー操作のユーザ名とパスワードを指定します。そのコピー操作だけのユーザ名を指定する場合は、**copy** コマンドにユーザ名を含めます。

サーバがディレクトリ構造である場合、コンフィギュレーション ファイルは、サーバ上のユーザ名に関連付けられているディレクトリに対して書き込まれるか、そのディレクトリからコピーされます。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、使用している FTP サーバのマニュアルを参照してください。

ここでは、次の設定情報について説明します。

- 「FTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-14）
- 「FTP を使用したコンフィギュレーション ファイルのダウンロード」（P.B-14）
- 「FTP を使用したコンフィギュレーション ファイルのアップロード」（P.B-16）

FTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルをダウンロードまたはアップロードを開始する前に、次の作業を実行します。

- スイッチに、FTP サーバへのルートがあることを確認します。サブネット間のトラフィックをルーティングするルータがない場合は、スイッチと FTP サーバが同じサブネットワーク内にある必要があります。FTP サーバへの接続を確認するには、**ping** コマンドを使用します。
- コンソールまたは Telnet セッションを通じてスイッチにアクセスしているときに、有効なユーザ名がない場合は、現在の FTP ユーザ名が、FTP のダウンロードに使用するユーザ名であることを確認します。有効なユーザ名を表示するには、**show users** 特権 EXEC コマンドを入力します。このユーザ名を使用しない場合は、すべてのコピー操作時に **ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを通じてスイッチにアクセスしているときに、有効なユーザ名がある場合は、このユーザ名が使用され、FTP ユーザ名を設定する必要はありません。そのコピー操作だけのユーザ名を指定する場合は、**copy** コマンドにユーザ名を含めます。
- コンフィギュレーション ファイルを FTP サーバにアップロードするには、スイッチのユーザからの書き込み要求が受け付けられるようにファイルを適切に設定する必要があります。

詳細については、使用している FTP サーバのマニュアルを参照してください。

FTP を使用したコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-14）を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。

	コマンド	目的
ステップ 3	**configure terminal**	スイッチでグローバル コンフィギュレーション モードを開始します。 この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合に限り必要です（ステップ 4、5、6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] **system:running-config** または **copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] **nvram:startup-config**	FTP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、IP アドレスが 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリから *host1-confg* というコンフィギュレーション ファイルをコピーし、これらのコマンドをスイッチでロードおよび実行する例を示します。

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。ソフトウェアにより、IP アドレスが 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリからスイッチのスタートアップ コンフィギュレーションに、コンフィギュレーション ファイル *host2-confg* がコピーされます。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

FTP を使用したコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
		「FTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-14）を参照して、FTP サーバが適切に設定されていることを確認します。
		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合に限り必要です（ステップ 4、5、6 を参照）。
ステップ 2	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 3	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy system:running-config ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] または **copy nvram:startup-config ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]	FTP を使用して、スイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定した場所に格納します。

次に、IP アドレスが 172.16.101.101 のリモート ホストにある *netadmin1* ディレクトリに *switch2-confg* という実行コンフィギュレーション ファイルをコピーする例を示します。

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-confg
Write file switch2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをコピーし、サーバに格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

RCP を使用したコンフィギュレーション ファイルのコピー

RCP では、別の方法を使用してリモート ホストとスイッチとの間でコンフィギュレーション ファイルのダウンロード、アップロード、およびコピーを実行できます。コネクションレス型の UDP（ユーザ データグラム プロトコル）を使用する TFTP とは異なり、RCP ではコネクション型の TCP を使用します。

RCP を使用してファイルをコピーするには、ファイルのコピー元またはコピー先のサーバが RCP をサポートしている必要があります。RCP の copy コマンドは、リモート システムの rsh サーバ（デーモン）に依存します。RCP を使用してファイルをコピーする場合は、TFTP のようにファイル配布用のサーバを作成する必要はありません。必要なのは、リモート シェル（rsh）をサポートするサーバにアクセスできることだけです（ほとんどの UNIX システムは rsh をサポートします）。ファイルを特定の場所から別の場所へコピーするため、コピー元のファイルに対する読み取り権限と、コピー先のファイルに対する書き込み権限が必要です。コピー先のファイルが存在しない場合は、RCP によって作成されます。

RCP では、クライアントが RCP 要求ごとににリモート ユーザ名をサーバに送信する必要があります。スイッチからサーバにコンフィギュレーション ファイルをコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- 現在の TTY（端末）プロセスに関連付けられているリモート ユーザ名。たとえば、ユーザが Telnet を通じてルータに接続され、**username** コマンドを使って認証された場合、スイッチ ソフトウェアによって、Telnet のユーザ名がリモート ユーザ名として送信されます。
- スイッチのホスト名。

RCP コピー要求を成功させるには、リモート ユーザ名のアカウントをネットワーク サーバで定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイルは、サーバ上のリモート ユーザ名に関連付けられているディレクトリに対して書き込まれるか、そのディレクトリからコピーされます。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

ここでは、次の設定情報について説明します。

- 「RCP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-17）
- 「RCP を使用したコンフィギュレーション ファイルのダウンロード」（P.B-18）
- 「RCP を使用したコンフィギュレーション ファイルのアップロード」（P.B-19）

RCP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルをダウンロードまたはアップロードする前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションがリモート シェル（rsh）をサポートすることを確認します。
- スイッチに、RCP サーバへのルートがあることを確認します。サブネット間のトラフィックをルーティングするルータがない場合は、スイッチとサーバが同じサブネットワーク内にある必要があります。RCP サーバへの接続を確認するには、**ping** コマンドを使用します。

- コンソールまたは Telnet セッションを通じてスイッチにアクセスしているときに、有効なユーザ名がない場合は、現在の RCP ユーザ名が、RCP のダウンロードに使用するユーザ名であることを確認します。有効なユーザ名を表示するには、**show users** 特権 EXEC コマンドを入力します。このユーザ名を使用しない場合は、すべてのコピー処理中に **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用し、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを通じてスイッチにアクセスしているときに、有効なユーザ名がある場合は、このユーザ名が使用され、RCP ユーザ名を設定する必要はありません。そのコピー操作だけのユーザ名を指定する場合は、**copy** コマンドにユーザ名を含めます。
- ファイルを RCP サーバにアップロードするには、スイッチのユーザからの RCP 書き込み要求が受け付けられるようにファイルを適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザの .rhosts ファイルにエントリを追加する必要があります。たとえば、スイッチに次の設定行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

スイッチの IP アドレスが *Switch1.company.com* に変換される場合は、RCP サーバ上の User0 の .rhosts ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、使用している RCP サーバのマニュアルを参照してください。

RCP を使用したコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-17）を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順は、デフォルトのリモート ユーザ名を上書きする場合に限り必要です（ステップ 4 と 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **system:running-config** または **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **nvram:startup-config**	RCP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、IP アドレスが 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリから *host1-confg* というコンフィギュレーション ファイルをコピーし、これらのコマンドをスイッチでロードおよび実行する例を示します。

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。次に、IP アドレスが 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリからスタートアップ コンフィギュレーションに、コンフィギュレーション ファイル *host2-confg* がコピーされます。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

RCP を使用したコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-17）を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順は、デフォルトのリモート ユーザ名を上書きする場合に限り必要です（ステップ 4 と 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy system:running-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] または **copy nvram:startup-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]	RCP を使用して、コンフィギュレーション ファイルをスイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコピーします。

次に、IP アドレスが 172.16.101.101 のリモート ホストにある *netadmin1* ディレクトリに *switch2-confg* という実行コンフィギュレーション ファイルをコピーする例を示します。

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-confg
Write file switch-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバに格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

設定情報の消去

スタートアップ コンフィギュレーションから設定情報を消去できます。スタートアップ コンフィギュレーションを使用せずにスイッチを再起動すると、スイッチはセットアップ プログラムを開始し、すべて新しい設定でスイッチを再設定できます。

スタートアップ コンフィギュレーション ファイルの消去

スタートアップ コンフィギュレーションの内容を消去するには、**erase nvram:** または **erase startup-config** 特権 EXEC コマンドを使用します。

注意　削除されたスタートアップ コンフィギュレーション ファイルは復元できません。

格納されたコンフィギュレーション ファイルの削除

保存されている設定をフラッシュ メモリから削除するには、**delete flash:***filename* 特権 EXEC コマンドを使用します。**file prompt** グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削除する前に確認を求められます。デフォルトでは、スイッチは、破壊的なファイル操作に関する確認をプロンプトで要求します。**file prompt** コマンドの詳細については、『*Cisco IOS Command Reference for Release 12.2*』を参照してください。

注意　削除されたファイルは復元できません。

コンフィギュレーションの交換およびロールバック

コンフィギュレーションの交換およびロールバックの機能を使用すると、実行コンフィギュレーションと保存済みの任意の Cisco IOS コンフィギュレーション ファイルを交換できます。ロールバック機能を使用して、以前の設定にロールバックできます。

ここでは、次の情報について説明します。

- 「コンフィギュレーションの交換およびロールバックの概要」（P.B-21）

コンフィギュレーションの交換およびロールバックの概要

コンフィギュレーションの交換およびロールバック機能を使用するには、次の概念を理解する必要があります。

コンフィギュレーション アーカイブ

コンフィギュレーション アーカイブにより、コンフィギュレーション ファイルのアーカイブを格納、構成、および管理するためのメカニズムが提供されます。**configure replace** 特権 EXEC コマンドによって、コンフィギュレーションのロールバック機能が向上します。また、**copy running-config** *destination-url* 特権 EXEC コマンドを使用し、交換ファイルをローカルまたはリモートで格納して、実行コンフィギュレーションのコピーを保存することもできます。ただし、この方法では、ファイルを自動的に管理できません。コンフィギュレーションの交換およびロールバック機能を使用すると、実行コンフィギュレーションのコピーをコンフィギュレーション アーカイブに自動的に保存できます。

archive config 特権 EXEC コマンドを使用して、コンフィギュレーション アーカイブに設定を保存します。その際、標準の場所、および連続ファイルが保存されるたびに増分するバージョン番号（および任意のタイムスタンプ）が自動的に付与されるファイル名プレフィクスを使用します。アーカイブに保持する実行コンフィギュレーションのバージョン数を指定できます。最大数のファイルが保存されると、次の最新のファイルが保存されるときに最も古いファイルが自動的に削除されます。**show archive** 特権 EXEC コマンドを使用すると、コンフィギュレーション アーカイブに保存されているすべてのコンフィギュレーション ファイルの情報が表示されます。

Cisco IOS のコンフィギュレーション アーカイブでは、コンフィギュレーション ファイルが格納され、そのファイルを **configure replace** コマンドで使用できます。このアーカイブは、FTP、HTTP、RCP、TFTP のどのファイル システムにも含めることができます。

設定の交換

configure replace 特権 EXEC コマンドを使用すると、実行コンフィギュレーションと保存済みの任意のコンフィギュレーション ファイルを交換できます。**configure replace** コマンドを入力すると、実行コンフィギュレーションが指定された交換コンフィギュレーションと比較され、設定の差分が生成されます。結果の差分は、設定の交換に使用されます。コンフィギュレーションの交換は通常 3 回までのパスで完了します。ループを防ぐために、実行されるのは 5 回のパスまでです。

copy *source-url* **running-config** 特権 EXEC コマンドを使用して、格納されているコンフィギュレーション ファイルを実行コンフィギュレーションにコピーできます。このコマンドを **configure replace** *target-url* 特権 EXEC コマンドの代わりに使用する場合は、次のような大きな違いがあることに注意してください。

- **copy** *source-url* **running-config** コマンドは結合動作であり、コピー元のファイルと実行コンフィギュレーションの両方のコマンドをすべて保持します。このコマンドは、コピー元ファイル内には含まれていないコマンドを実行コンフィギュレーションから削除しません。一方、**configure replace** *target-url* コマンドは、交換ファイル内に含まれていないコマンドを実行コンフィギュレーションから削除し、存在していないコマンドを実行コンフィギュレーションに追加します。

- 部分的なコンフィギュレーション ファイルを、**copy** *source-url* **running-config** コマンドのコピー元ファイルとして使用できます。完全なコンフィギュレーション ファイルは、**configure replace** *target-url* コマンドの交換ファイルとして使用する必要があります。

コンフィギュレーションのロールバック

configure replace コマンドを使用して、以前の設定が保存されたあとに行われた変更をロールバックすることもできます。コンフィギュレーションのロールバック機能では、適用された特定の変更に基づいてロールバックが実行されるのではなく、保存済みのコンフィギュレーション ファイルに基づいて特定の設定に戻ります。

コンフィギュレーションのロールバック機能が必要な場合は、設定を変更する前に、まず実行コンフィギュレーションを保存する必要があります。これで、設定の変更を入力したあとに、保存したそのコンフィギュレーション ファイルを使用して、**configure replace** *target-url* コマンドで変更をロールバックできます。

保存済みの任意のコンフィギュレーション ファイルをロールバック コンフィギュレーションとして指定できます。一部のロールバック モデルと同様に、ロールバックの回数は制限されません。

設定時の注意事項

コンフィギュレーションの交換およびロールバックを設定および実行する場合、次の注意事項に従ってください。

- スイッチのメモリの空き容量が、2 つのコンフィギュレーション ファイル（実行コンフィギュレーションと保存された交換コンフィギュレーション）の合計容量よりも大きいことを確認します。空き容量が足りない場合、コンフィギュレーションの交換は失敗します。
- また、スイッチのメモリに、コンフィギュレーションの交換またはロールバックのコンフィギュレーション コマンドを実行できるだけの空き容量があることも確認します。
- ネットワーキング装置の物理コンポーネント（物理インターフェイスなど）に関連するコマンドなどの特定のコンフィギュレーション コマンドは、実行コンフィギュレーションに対して追加または削除できません。
  - コンフィギュレーションの交換では、インターフェイスが物理的に装置上に存在する場合、**interface** *interface-id* コマンドラインを実行コンフィギュレーションから削除できません。
  - そのようなインターフェイスが装置上に存在しない場合は、**interface** *interface-id* コマンドラインを実行コンフィギュレーションに追加できません。
- **configure replace** コマンドを使用する場合は、保存した設定を、実行コンフィギュレーションの交換コンフィギュレーション ファイルとして指定する必要があります。交換ファイルは、Cisco IOS 装置によって生成された完全な設定（**copy running-config** *destination-url* コマンドで生成された設定など）である必要があります。

（注） 交換コンフィギュレーション ファイルを外部で生成する場合は、Cisco IOS 装置によって生成されたファイル形式に準ずる必要があります。

コンフィギュレーション アーカイブの設定

configure replace コマンドをコンフィギュレーション アーカイブおよび **archive config** コマンドとともに使用することは任意ですが、この方法を使用すると、コンフィギュレーションをロールバックするうえで大きな利点があります。**archive config** コマンドを使用する前に、まずコンフィギュレーション アーカイブを設定する必要があります。コンフィギュレーション アーカイブを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**archive**	アーカイブ コンフィギュレーション モードを開始します。
ステップ 3	**path** *url*	コンフィギュレーション アーカイブにファイルの場所とファイル名プレフィクスを指定します。
ステップ 4	**maximum** *number*	（任意）コンフィギュレーション アーカイブに保存する実行コンフィギュレーションのアーカイブ ファイルの最大数を設定します。 *number*：コンフィギュレーション アーカイブ内の実行コンフィギュレーション ファイルの最大数。有効値の範囲は 1 ～ 14 です。デフォルト値は 10 です。 **（注）** このコマンドを使用する前に、まず **path** アーカイブ コンフィギュレーション コマンドを入力して、コンフィギュレーション アーカイブにファイルの場所とファイル名プレフィクスを指定しておく必要があります。
ステップ 5	**time-period** *minutes*	（任意）コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動的に保存する頻度を指定します。 *minutes*：コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動的に保存する頻度を分単位で指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

コンフィギュレーションの交換またはロールバック操作の実行

実行コンフィギュレーション ファイルを保存済みのコンフィギュレーション ファイルと交換するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**archive config**	（任意）実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。 **（注）** このコマンドを使用する前に、**path** アーカイブ コンフィギュレーション コマンドを入力します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3		実行コンフィギュレーションに必要な変更を行います。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**configure replace** *target-url* [**list**] [**force**] [**time** *seconds*] [**nolock**]	実行コンフィギュレーション ファイルを保存済みのコンフィギュレーション ファイルと交換します。 *target-url*：実行コンフィギュレーション ファイルと交換する保存済みのコンフィギュレーション ファイル（ステップ 1 で **archive config** 特権 EXEC コマンドを使用して作成したコンフィギュレーション ファイルなど）の URL（ファイル システムでアクセス可能）。 **list**：コンフィギュレーション交換操作の各パス中にソフトウェア パーサーで適用されたコマンド エントリのリストを表示します。パスの合計数も表示されます。 **force**：確認を求めるプロンプトが表示されずに、実行コンフィギュレーション ファイルを指定された保存済みコンフィギュレーション ファイルと交換します。 **time** *seconds*：**configure confirm** コマンドを入力して実行コンフィギュレーション ファイルの交換を確認するまでの時間（秒単位）を指定します。指定された時間制限内に **configure confirm** コマンドを入力しない場合、コンフィギュレーションの交換操作は自動的に停止します（つまり、実行コンフィギュレーション ファイルは、**configure replace** コマンドを入力する前の設定に復元されます）。 **（注）** **time** *seconds* コマンドライン オプションを使用する前に、まずコンフィギュレーション アーカイブをイネーブルにする必要があります。 **nolock**：コンフィギュレーションの交換操作中に他のユーザが実行コンフィギュレーションを変更しないようにするための実行コンフィギュレーション ファイルのロックをディセーブルにします。
ステップ 6	**configure confirm**	（任意）実行コンフィギュレーションを保存済みコンフィギュレーション ファイルと交換するかどうかを確認します。 **（注）** このコマンドは、**configure replace** コマンドの **time** *seconds* キーワードと引数が指定されている場合に限り使用します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ソフトウェア イメージの操作

ここでは、システム ソフトウェア、Cisco IOS コード、および組み込みデバイス マネージャ ソフトウェアが含まれる、ソフトウェア イメージ ファイルをアーカイブ（ダウンロードとアップロード）する方法を説明します。

（注）　ソフトウェア イメージをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドを使用する代わりに、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。.

スイッチ イメージ ファイルを TFTP、FTP、または RCP サーバからダウンロードし、スイッチ ソフトウェアをアップグレードできます。TFTP サーバにアクセスできない場合は、Web ブラウザ（HTTP）を使用してソフトウェア イメージ ファイルを PC またはワークステーションに直接ダウンロードし、デバイス マネージャまたは Cisco Network Assistant を使用してスイッチをアップグレードできます。TFTP サーバまたは Web ブラウザ（HTTP）を使用してスイッチをアップグレードする方法の詳細については、リリース ノートを参照してください。

ダウンロードのあとは、現在のイメージを新しいイメージと交換することも、現在のイメージをフラッシュ メモリ内に維持することもできます。

スイッチ イメージ ファイルを、バックアップ目的で TFTP、FTP、または RCP サーバにアップロードします。アップロードされたこのイメージを、あとから同じスイッチまたは同じタイプの別のスイッチにダウンロードできます。

使用するプロトコルは、使用しているサーバのタイプによって異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが高速になり、より確実にデータが配信されます。このような改善が実現できるのは、FTP と RCP が、コネクション型 TCP/IP スタックに基づいて構築され、このスタックを使用しているからです。

ここでは、次の設定情報について説明します。

- 「スイッチ上のイメージの場所」（P.B-26）
- 「サーバまたは Cisco.com 上のイメージの tar ファイル形式」（P.B-26）
- 「TFTP を使用したイメージ ファイルのコピー」（P.B-27）
- 「FTP を使用したイメージ ファイルのコピー」（P.B-30）
- 「RCP を使用したイメージ ファイルのコピー」（P.B-35）

（注）　ソフトウェア イメージおよびサポートされるアップグレード パスのリストについては、リリース ノートを参照してください。

スイッチ上のイメージの場所

Cisco IOS イメージは、バージョン番号を示すディレクトリ内の *.bin* ファイルとして格納されます。サブディレクトリには、Web 管理に必要なファイルが格納されます。イメージは、システム ボード フラッシュ メモリ（flash:）に格納されます。

show version 特権 EXEC コマンドを使用して、スイッチで現在実行されているソフトウェア バージョンを確認できます。表示された内容で、`System image file is...` から始まる行を確認します。この行には、イメージが格納されているフラッシュ メモリ内のディレクトリ名が示されます。

また、**dir** *filesystem*: 特権 EXEC コマンドを使用して、フラッシュ メモリに格納されている他のソフトウェア イメージのディレクトリ名も確認できます。**archive download-sw /directory** 特権 EXEC コマンドを使用すると、各 tar ファイルで完全なパスを指定せずに、ダウンロードする tar ファイルまたは tar ファイルのリストの前にディレクトリを一時的に指定できます。

サーバまたは Cisco.com 上のイメージの tar ファイル形式

サーバにあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは tar ファイル形式で提供され、そのイメージには次のファイルが含まれています。

- tar ファイルの目次として機能する *info* ファイル
- Cisco IOS イメージや Web 管理ファイルなど、他のイメージやファイルを含む 1 つまたは複数のサブディレクトリ

次に、info ファイルに含まれている情報の一部の例を示します。表 B-3 に、次の情報の詳細を示します。

```
system_type:0x00000000:image-name
    image_family:xxxx
    stacking_number:x
    info_end:
version_suffix:xxxx
    version_directory:image-name
    image_system_type_id:0x00000000
    image_name:image-nameB.bin
    ios_image_file_size:6398464
    total_image_file_size:8133632
    image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
    image_family:xxxx
    stacking_number:x
    board_ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002
0x40110000
    info_end:
```

（注）　stacking_number フィールドは無視してください。このフィールドは、スイッチに適用されません。

表 B-3　info ファイルの説明

フィールド	説明
version_suffix	Cisco IOS イメージのバージョン文字列サフィクスを指定します。
version_directory	Cisco IOS イメージおよび HTML サブディレクトリがインストールされるディレクトリを指定します。
image_name	tar ファイル内の Cisco IOS イメージの名前を指定します。
ios_image_file_size	tar ファイル内の Cisco IOS イメージ のサイズを指定します。このサイズは、Cisco IOS イメージだけを格納するために必要なフラッシュ メモリの概算容量を示します。

表 B-3　info ファイルの説明 （続き）

フィールド	説明
total_image_file_size	tar ファイル内のすべてのイメージ（Cisco IOS イメージと Web 管理ファイル）のサイズを指定します。このサイズは、それらのイメージを格納するために必要なフラッシュ メモリの概算容量を示します。
image_feature	イメージのコア機能を示します。
image_min_dram	このイメージの実行に必要な DRAM の最小容量を指定します。
image_family	ソフトウェアをインストールできる製品のファミリを示します。

TFTP を使用したイメージ ファイルのコピー

スイッチ イメージを TFTP サーバからダウンロードすることも、イメージをスイッチから TFTP サーバにアップロードすることもできます。

サーバからスイッチ イメージ ファイルをダウンロードして、スイッチ ソフトウェアをアップグレードします。ダウンロードのあとは、現在のイメージを新しいイメージで上書きすることも、現在のイメージを維持することもできます。

スイッチ イメージ ファイルを、バックアップの目的でサーバにアップロードします。アップロードされたこのイメージを、あとから同じスイッチまたは同じタイプの別のスイッチにダウンロードできます。

（注）　ソフトウェア イメージをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドを使用する代わりに、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「TFTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-27）
- 「TFTP を使用したイメージ ファイルのダウンロード」（P.B-28）
- 「TFTP を使用したイメージ ファイルのアップロード」（P.B-30）

TFTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージ ファイルのダウンロードまたはアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションで、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  （注）　/etc/inetd.conf ファイルおよび /etc/services ファイルを変更したあとに、inetd デーモンを再起動する必要があります。デーモンを再起動するには、inetd プロセスを停止して再起動するか、**fastboot** コマンド（SunOS 4.x 上）または **reboot** コマンド（Solaris 2.x または SunOS 5.x 上）を入力します。TFTP デーモンの詳細については、使用しているワークステーションのマニュアルを参照してください。

- スイッチに、TFTP サーバへのルートがあることを確認します。サブネット間のトラフィックをルーティングするルータがない場合は、スイッチと TFTP サーバが同じサブネットワーク内にある必要があります。TFTP サーバへの接続を確認するには、**ping** コマンドを使用します。
- ダウンロードするイメージが、TFTP サーバ上の正しいディレクトリ（UNIX ワークステーションの場合は通常 /tftpboot）にあることを確認します。
- ダウンロード処理の場合は、ファイルに対する権限が正しく設定されていることを確認します。ファイルに対する権限は world-read である必要があります。
- イメージ ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要がある場合があります。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* は、イメージをサーバにアップロードするときに使用するファイル名です。
- アップロード処理中に、サーバで既存のファイル（空のファイルを作成する必要があった場合は空のファイルも含む）を上書きする場合は、ファイルに対する権限が正しく設定されていることを確認します。ファイルに対する権限は world-write である必要があります。

TFTP を使用したイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして現在のイメージと交換することも、現在のイメージを維持することもできます。

TFTP サーバから新しいイメージをダウンロードし、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 3 を実行します。現在のイメージを維持するには、ステップ 3 に進みます。

	コマンド	目的
ステップ 1		イメージをワークステーション上の適切な TFTP ディレクトリにコピーします。TFTP サーバが適切に設定されていることを確認します。「TFTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-27）を参照してください。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。

	コマンド	目的
ステップ 3	**archive download-sw /overwrite /reload tftp:**[[*//location*]/*directory*]/*image-name*.**tar**	TFTP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージで上書きされます。 • **/reload** オプションを指定すると、変更された設定が保存されていない場合を除き、イメージをダウンロードしたあとでシステムがリロードされます。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）とダウンロードするイメージを指定します。ディレクトリ名では、大文字と小文字が区別されます。
ステップ 4	**archive download-sw /leave-old-sw /reload tftp:**[[*//location*]/*directory*]/*image-name*.**tar**	TFTP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージを維持します。 • **/leave-old-sw** オプションを指定すると、ダウンロードしたあと、古いソフトウェア バージョンが維持されます。 • **/reload** オプションを指定すると、変更された設定が保存されていない場合を除き、イメージをダウンロードしたあとでシステムがリロードされます。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）とダウンロードするイメージを指定します。ディレクトリ名では、大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに適していること、および DRAM の容量が十分であることが確認されます。この条件を満たさない場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定すると、ダウンロード アルゴリズムによって、フラッシュ装置上の既存のイメージが新しいイメージと同じであるかどうかにかかわらず、そのイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注）　フラッシュ装置に 2 つのイメージを格納する十分な領域があり、それらのイメージの 1 つを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールしたり、実行中のイメージを維持する十分な領域がない場合、ダウンロード プロセスが停止し、エラー メッセージが表示されます。

アルゴリズムによって、ダウンロードされたイメージがシステム ボード フラッシュ装置（flash:）にインストールされます。イメージは、ソフトウェアのバージョン文字列を使用した名前付きの新しいディレクトリに格納されます。また、BOOT 環境変数は、新しくインストールされたイメージを指定するよう更新されます。

ダウンロード プロセス中に古いイメージを維持した場合（**/leave-old-sw** キーワードを指定した場合）は、**delete /force /recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力して、このイメージを削除できます。システム ボード フラッシュ装置の場合、*filesystem* に **flash:** を使用します。*file-url* には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルとディレクトリが削除されます。

注意　ダウンロードおよびアップロード アルゴリズムを正常に動作させるために、イメージの名前を*変更しないでください。*

TFTP を使用したイメージ ファイルのアップロード

イメージをスイッチから TFTP サーバにアップロードできます。このイメージを、あとからそのスイッチまたは同じタイプの別のスイッチにダウンロードできます。

組み込みデバイス マネージャに関連付けられている Web 管理ページが既存のイメージとともにインストールされている場合にだけ、アップロード機能を使用します。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		TFTP サーバが適切に設定されていることを確認します。「TFTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-27）を参照してください。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。
ステップ 3	**archive upload-sw tftp:**[[*//location*]*/directory*]*/image-name*.**tar**	現在実行中のスイッチ イメージを TFTP サーバにアップロードします。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）とアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名では、大文字と小文字が区別されます。*image-name*.**tar** は、サーバに保存するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、および Web 管理ファイルの順序でアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、アップロード アルゴリズムによって tar ファイル形式が作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを正常に動作させるために、イメージの名前を*変更しないでください。*

FTP を使用したイメージ ファイルのコピー

スイッチ イメージを FTP サーバからダウンロードすることも、イメージをスイッチから FTP サーバにアップロードすることもできます。

サーバからスイッチ イメージ ファイルをダウンロードして、スイッチ ソフトウェアをアップグレードします。ダウンロードのあとは、現在のイメージを新しいイメージで上書きすることも、現在のイメージを維持することもできます。

スイッチ イメージ ファイルを、バックアップの目的でサーバにアップロードします。アップロードされたこのイメージを、あとからそのスイッチまたは同じタイプの別のスイッチにダウンロードできます。

（注）　ソフトウェア イメージをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドを使用する代わりに、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「FTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-31）
- 「FTP を使用したイメージ ファイルのダウンロード」（P.B-32）
- 「FTP を使用したイメージ ファイルのアップロード」（P.B-34）

FTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備

FTP サーバに、または FTP サーバから、イメージ ファイルをコピーできます。

FTP では、クライアントが FTP 要求ごとにリモート ユーザ名とパスワードをサーバに送信する必要があります。FTP を使用してスイッチからサーバにイメージ ファイルをコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- anonymous。

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたパスワード（パスワードが指定されている場合）。
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）。
- スイッチは、*username@switchname.domain* というパスワードを作成します。変数 *username* は現在のセッションに関連付けられているユーザ名です。*switchname* は設定されたホスト名です。*domain* はスイッチのドメインです。

ユーザ名とパスワードは、FTP サーバのアカウントに関連付けられる必要があります。サーバに書き込んでいる場合は、FTP の書き込み要求が受け付けられるように FTP サーバを適切に設定する必要があります。

ip ftp username および **ip ftp password** コマンドを使用して、すべてのコピー操作のユーザ名とパスワードを指定します。その操作だけのユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドにユーザ名を含めます。

サーバがディレクトリ構造である場合、イメージ ファイルは、サーバのユーザ名に関連付けられているディレクトリに対して書き込まれるか、そのディレクトリからコピーされます。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

FTP を使用してイメージ ファイルのダウンロードまたはアップロードを開始する前に、次の作業を実行します。

- スイッチに、FTP サーバへのルートがあることを確認します。サブネット間のトラフィックをルーティングするルータがない場合は、スイッチと FTP サーバが同じサブネットワーク内にある必要があります。FTP サーバへの接続を確認するには、**ping** コマンドを使用します。
- コンソールまたは Telnet セッションを通じてスイッチにアクセスしているときに、有効なユーザ名がない場合は、現在の FTP ユーザ名が、FTP のダウンロードに使用するユーザ名であることを確認します。有効なユーザ名を表示するには、**show users** 特権 EXEC コマンドを入力します。このユーザ名を使用しない場合は、**ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して新しい FTP ユーザ名を作成します。この新しい名前は、すべてのアーカイブ操作時に使用されます。新しいユーザ名は NVRAM に格納されます。Telnet セッションを通じてスイッチにアクセスしているときに、有効なユーザ名がある場合は、このユーザ名が使用され、FTP ユーザ名を設定する必要はありません。その操作だけのユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドにユーザ名を含めます。
- イメージ ファイルを FTP サーバにアップロードするには、スイッチのユーザからの書き込み要求が受け付けられるようにファイルを適切に設定する必要があります。

詳細については、使用している FTP サーバのマニュアルを参照してください。

FTP を使用したイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして現在のイメージを上書きすることも、現在のイメージを維持することもできます。

FTP サーバから新しいイメージをダウンロードし、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 7 を実行します。現在のイメージを維持する場合は、ステップ 7 に進みます。

	コマンド	目的
ステップ 1		「FTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-31）を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合に限り必要です（ステップ 4、5、6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/image-name*.**tar**	FTP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージで上書きされます。 • **/reload** オプションを指定すると、変更された設定が保存されていない場合を除き、イメージをダウンロードしたあとでシステムがリロードされます。 • *//username*[**:***password*] には、ユーザ名とパスワードを指定します。これらは FTP サーバのアカウントに関連付けられる必要があります。詳細については、「FTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-31）を参照してください。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • *directory*/*image-name*.**tar** には、ディレクトリ（任意）とダウンロードするイメージを指定します。ディレクトリ名では、大文字と小文字が区別されます。
ステップ 8	**archive download-sw /leave-old-sw /reload ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/image-name*.**tar**	FTP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージを維持します。 • **/leave-old-sw** オプションを指定すると、ダウンロードしたあと、古いソフトウェア バージョンが維持されます。 • **/reload** オプションを指定すると、変更された設定が保存されていない場合を除き、イメージをダウンロードしたあとでシステムがリロードされます。 • *//username*[**:***password*] には、ユーザ名とパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられる必要があります。詳細については、「FTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-31）を参照してください。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • *directory*/*image-name*.**tar** には、ディレクトリ（任意）とダウンロードするイメージを指定します。ディレクトリ名では、大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに適していること、および DRAM の容量が十分であることが確認されます。この条件を満たさない場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定すると、ダウンロード アルゴリズムによって、フラッシュ装置上の既存のイメージが新しいイメージと同じであるかどうかにかかわらず、そのイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注）　フラッシュ装置に 2 つのイメージを格納する十分な領域があり、それらのイメージの 1 つを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールしたり、実行中のイメージを維持する十分な領域がない場合、ダウンロード プロセスが停止し、エラー メッセージが表示されます。

アルゴリズムによって、ダウンロードされたイメージがシステム ボード フラッシュ装置（flash:）にインストールされます。イメージは、ソフトウェアのバージョン文字列を使用した名前付きの新しいディレクトリに格納されます。また、BOOT 環境変数は、新しくインストールされたイメージを指定するよう更新されます。

ダウンロード プロセス中に古いイメージを維持した場合（**/leave-old-sw** キーワードを指定した場合）は、**delete /force /recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力して、このイメージを削除できます。システム ボード フラッシュ装置の場合、*filesystem* に **flash:** を使用します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルとディレクトリが削除されます。

注意　ダウンロードおよびアップロード アルゴリズムを正常に動作させるために、イメージの名前を*変更しないでください*。

FTP を使用したイメージ ファイルのアップロード

イメージをスイッチから FTP サーバにアップロードできます。このイメージを、あとから同じスイッチまたは同じタイプの別のスイッチにダウンロードできます。

組み込みデバイス マネージャに関連付けられている Web 管理ページが既存のイメージとともにインストールされている場合にだけ、アップロード機能を使用します。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP を使用したコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-14）を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合に限り必要です（ステップ 4、5、6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。

	コマンド	目的
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**archive upload-sw** **ftp:**[[//[*username*[**:***password*]**@**]*location*]/*directory*]/ *image-name*.**tar**	現在実行中のスイッチ イメージを FTP サーバにアップロードします。 • *//username***:***password* には、ユーザ名とパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられる必要があります。詳細については、「FTP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-31）を参照してください。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）とアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名では、大文字と小文字が区別されます。*image-name*.**tar** は、サーバに保存するソフトウェア イメージの名前です。

archive upload-sw コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、および Web 管理ファイルの順序でアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、アップロード アルゴリズムによって tar ファイル形式が作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを正常に動作させるために、イメージの名前を*変更しないでください*。

RCP を使用したイメージ ファイルのコピー

スイッチ イメージを RCP サーバからダウンロードすることも、イメージをスイッチから RCP サーバにアップロードすることもできます。

サーバからスイッチ イメージ ファイルをダウンロードして、スイッチ ソフトウェアをアップグレードします。ダウンロードのあとは、現在のイメージを新しいイメージで上書きすることも、現在のイメージを維持することもできます。

スイッチ イメージ ファイルを、バックアップの目的でサーバにアップロードします。アップロードされたこのイメージを、あとから同じスイッチまたは同じタイプの別のスイッチにダウンロードできます。

（注）　ソフトウェア イメージをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドを使用する代わりに、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「RCP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-36）
- 「RCP を使用したイメージ ファイルのダウンロード」（P.B-37）
- 「RCP を使用したイメージ ファイルのアップロード」（P.B-39）

RCP を使用したイメージ ファイルのダウンロードまたはアップロードの準備

RCP では、別の方法を使用してリモート ホストとスイッチとの間でイメージ ファイルのダウンロードおよびアップロードを実行できます。コネクションレス型の UDP（ユーザ データグラム プロトコル）を使用する TFTP とは異なり、RCP ではコネクション型の TCP を使用します。

RCP を使用してファイルをコピーするには、ファイルのコピー元またはコピー先のサーバが RCP をサポートしている必要があります。RCP の copy コマンドは、リモート システムの rsh サーバ（デーモン）に依存します。RCP を使用してファイルをコピーする場合は、TFTP のようにファイル配布用のサーバを作成する必要はありません。必要なのは、リモート シェル（rsh）をサポートするサーバにアクセスできることだけです（ほとんどの UNIX システムは rsh をサポートします）。ファイルを特定の場所から別の場所へコピーするため、コピー元のファイルに対する読み取り権限と、コピー先のファイルに対する書き込み権限が必要です。コピー先のファイルが存在しない場合は、RCP によって作成されます。

RCP では、クライアントが RCP 要求ごとににリモート ユーザ名をサーバに送信する必要があります。RCP を使用してスイッチからサーバにイメージをコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが入力されている場合）。
- 現在の TTY（端末）プロセスに関連付けられているリモート ユーザ名。たとえば、ユーザが Telnet を通じてルータに接続され、**username** コマンドを使って認証された場合、スイッチ ソフトウェアによって、Telnet のユーザ名がリモート ユーザ名として送信されます。
- スイッチのホスト名。

RCP コピー要求を成功させるには、リモート ユーザ名のアカウントをネットワーク サーバで定義する必要があります。サーバがディレクトリ構造である場合、イメージ ファイルは、サーバ上のリモート ユーザ名に関連付けられているディレクトリに対して書き込まれるか、そのディレクトリからコピーされます。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージ ファイルのダウンロードまたはアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションがリモート シェル（rsh）をサポートすることを確認します。
- スイッチに、RCP サーバへのルートがあることを確認します。サブネット間のトラフィックをルーティングするルータがない場合は、スイッチとサーバが同じサブネットワーク内にある必要があります。RCP サーバへの接続を確認するには、**ping** コマンドを使用します。
- コンソールまたは Telnet セッションを通じてスイッチにアクセスしているときに、有効なユーザ名がない場合は、現在の RCP ユーザ名が、RCP のダウンロードに使用するユーザ名であることを確認します。有効なユーザ名を表示するには、**show users** 特権 EXEC コマンドを入力します。このユーザ名を使用しない場合は、すべてのアーカイブ操作時に **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用して新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを通じてスイッチにアクセスしているときに、有効なユーザ名がある場合は、このユーザ名が使用され、RCP ユーザ名を設定する必要はありません。その操作だけのユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドにユーザ名を含めます。
- イメージを RCP サーバにアップロードするには、スイッチのユーザからの RCP 書き込み要求が受け付けられるようにイメージを適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザの .rhosts ファイルにエントリを追加する必要があります。

たとえば、スイッチに次の設定行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

スイッチの IP アドレスが *Switch1.company.com* に変換される場合は、RCP サーバ上の User0 の .rhosts ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、使用している RCP サーバのマニュアルを参照してください。

RCP を使用したイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして現在のイメージと交換することも、現在のイメージを維持することもできます。

RCP サーバから新しいイメージをダウンロードし、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 6 を実行します。現在のイメージを維持する場合は、ステップ 6 に進みます。

	コマンド	目的
ステップ 1		「RCP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-36）を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順は、デフォルトのリモート ユーザ名を上書きする場合に限り必要です（ステップ 4 と 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**archive download-sw /overwrite /reload rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	RCP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージで上書きされます。 • **/reload** オプションを指定すると、変更された設定が保存されていない場合を除き、イメージをダウンロードしたあとでシステムがリロードされます。 • *//username* には、ユーザ名を指定します。RCP コピー要求を成功させるには、リモート ユーザ名のアカウントをネットワーク サーバで定義する必要があります。詳細については、「RCP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-36）を参照してください。 • *@location* には、RCP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）とダウンロードするイメージを指定します。ディレクトリ名では、大文字と小文字が区別されます。

	コマンド	目的
ステップ 7	**archive download-sw /leave-old-sw /reload rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	RCP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージを維持します。 • **/leave-old-sw** オプションを指定すると、ダウンロードしたあと、古いソフトウェア バージョンが維持されます。 • **/reload** オプションを指定すると、変更された設定が保存されていない場合を除き、イメージをダウンロードしたあとでシステムがリロードされます。 • *//username* には、ユーザ名を指定します。RCP コピー要求を実行するには、リモート ユーザ名のアカウントをネットワーク サーバで定義する必要があります。詳細については、「RCP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-36）を参照してください。 • *@location* には、RCP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）とダウンロードするイメージを指定します。ディレクトリ名では、大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに適していること、および DRAM の容量が十分であることが確認されます。この条件を満たさない場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定すると、ダウンロード アルゴリズムによって、フラッシュ装置上の既存のイメージが新しいイメージと同じであるかどうかにかかわらず、そのイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注） フラッシュ装置に 2 つのイメージを格納する十分な領域があり、それらのイメージの 1 つを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールしたり、実行中のイメージを維持する十分な領域がない場合、ダウンロード プロセスが停止し、エラー メッセージが表示されます。

アルゴリズムによって、ダウンロードされたイメージがシステム ボード フラッシュ装置（flash:）にインストールされます。イメージは、ソフトウェアのバージョン文字列を使用した名前付きの新しいディレクトリに格納されます。また、BOOT 環境変数は、新しくインストールされたイメージを指定するよう更新されます。

ダウンロード プロセス中に古いソフトウェアを維持した場合（**/leave-old-sw** キーワードを指定した場合）は、**delete /force /recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力して、このソフトウェアを削除できます。システム ボード フラッシュ装置の場合、*filesystem* に **flash:** を使用します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルとディレクトリが削除されます。

注意 ダウンロードおよびアップロード アルゴリズムを正常に動作させるために、イメージの名前を*変更しないでください*。

RCP を使用したイメージ ファイルのアップロード

イメージをスイッチから RCP サーバにアップロードできます。このイメージを、あとから同じスイッチまたは同じタイプの別のスイッチにダウンロードできます。

組み込みデバイス マネージャに関連付けられている Web 管理ページが既存のイメージとともにインストールされている場合にだけ、アップロード機能を使用します。

イメージを RCP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-36）を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを通じてスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順は、デフォルトのリモート ユーザ名を上書きする場合に限り必要です（ステップ 4 と 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**archive upload-sw rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	現在実行中のスイッチ イメージを RCP サーバにアップロードします。 • //*username* には、ユーザ名を指定します。RCP コピー要求を実行するには、リモート ユーザ名のアカウントをネットワーク サーバで定義する必要があります。詳細については、「RCP を使用したイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-36）を参照してください。 • @*location* には、RCP サーバの IP アドレスを指定します。 • /*directory*]/*image-name*.**tar** には、ディレクトリ（任意）とアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名では、大文字と小文字が区別されます。 • *image-name*.**tar** は、サーバに保存するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、および Web 管理ファイルの順序でアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、アップロード アルゴリズムによって tar ファイル形式が作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを正常に動作させるために、イメージの名前を*変更しないでください*。

APPENDIX C

Cisco IOS Release 12.2(55)SE でサポートされていないコマンド

この付録では、IE 3000 スイッチのプロンプトに疑問符（?）を入力したときに表示される CLI（コマンドライン インターフェイス）コマンドの中で、まだテストされていないため、またはスイッチのハードウェアの制限により、このリリースではサポートされていないコマンドをいくつか示します。このリストは完全ではありません。サポートされていないコマンドを、ソフトウェア機能およびコマンドモード別に示します。

アクセス制御リスト

サポートされていない特権 EXEC コマンド

access-enable [**host**] [**timeout** *minutes*]

access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*] [**timeout** *minutes*]

clear access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*].

show access-lists rate-limit [*destination*]

show accounting

show ip accounting [**checkpoint**] [**output-packets** | **access violations**]

show ip cache [*prefix-mask*] [*type number*]

サポートされていないグローバル コンフィギュレーション コマンド

access-list rate-limit *acl-index* {*precedence* | **mask** *prec-mask*}

access-list dynamic extended

サポートされていないルート マップ コンフィギュレーション コマンド

match ip address prefix-list *prefix-list-name* [*prefix-list-name...*]

アーカイブ コマンド

サポートされていない特権 EXEC コマンド

archive config

logging persistent

show archive config

show archive log

ARP コマンド

サポートされていないグローバル コンフィギュレーション コマンド

arp *ip-address hardware-address* **smds**

arp *ip-address hardware-address* **srp-a**

arp *ip-address hardware-address* **srp-b**

サポートされていないインターフェイス コンフィギュレーション コマンド

arp probe

ip probe proxy

ブート ローダ コマンド

サポートされていないグローバル コンフィギュレーション コマンド

boot buffersize

Embedded Event Manager

サポートされていない特権 EXEC コマンド

event manager update user policy [*policy-filename* | *group* [*group name expression*]] | *repository* [*url location*]

このコマンドでは、パラメータはサポートされていません。

event manager run [*policy name*] |<*paramater1*>|... <***paramater15***>|

サポートされていないグローバル コンフィギュレーション コマンド

no event manager directory user repository [*url location*]

event manager applet [*applet-name*] maxrun

アプレット コンフィギュレーション モードにおいてサポートされていないコマンド

no event interface name [*interface-name*] parameter [*counter-name*] entry-val [*entry counter value*] entry-op {*gt*|*ge*|*eq*|*ne*|*lt*|*le*} [**entry-type {increment | rate | value**] [exit-val [*exit value*] exit-op {*gt*|*ge*|*eq*|*ne*|*lt*|*le*} **exit-type { increment | rate | value}**][**average-factor <average-factor-value>**]

no trigger

tag

debug コマンド

サポートされていない特権 EXEC コマンド

debug platform cli-redirection main

debug platform configuration

フォールバック ブリッジング

サポートされていない特権 EXEC コマンド

clear bridge [*bridge-group*] **multicast** [**router-ports** | **groups** | **counts**] [*group-address*] [*interface-unit*] [**counts**]

clear vlan statistics

show bridge [*bridge-group*] **circuit-group** [*circuit-group*] [*src-mac-address*] [*dst-mac-address*]

show bridge [*bridge-group*] **multicast** [**router-ports** | **groups**] [*group-address*]

show bridge vlan

show interfaces crb

show interfaces {**ethernet** | **fastethernet**} [*interface* | *slot/port*] **irb**

show subscriber-policy *range*

サポートされていないグローバル コンフィギュレーション コマンド

bridge *bridge-group* **acquire**

bridge *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-id*]

bridge *bridge-group* **aging-time** *seconds*

bridge *bridge-group* **bitswap_l3_addresses**

bridge *bridge-group* **bridge ip**

bridge *bridge-group* **circuit-group** *circuit-group* **pause** *milliseconds*

bridge *bridge-group* **circuit-group** *circuit-group* **source-based**

bridge cmf

bridge crb

bridge *bridge-group* **domain** *domain-name*

bridge irb

bridge *bridge-group* **mac-address-table limit** *number*

bridge *bridge-group* **multicast-source**

bridge *bridge-group* **protocol dec**

bridge *bridge-group* **route** *protocol*

bridge *bridge-group* **subscriber policy** *policy*

subscriber-policy *policy* [**no** | **default**] *packet* [**permit** | **deny**]]

サポートされていないインターフェイス コンフィギュレーション コマンド

bridge-group *bridge-group* **cbus-bridging**

bridge-group *bridge-group* **circuit-group** *circuit-number*

bridge-group *bridge-group* **input-address-list** *access-list-number*

bridge-group *bridge-group* **input-lat-service-deny** *group-list*

bridge-group *bridge-group* **input-lat-service-permit** *group-list*

bridge-group *bridge-group* **input-lsap-list** *access-list-number*

bridge-group *bridge-group* **input-pattern-list** *access-list-number*

bridge-group *bridge-group* **input-type-list** *access-list-number*

bridge-group *bridge-group* **lat-compression**

bridge-group *bridge-group* **output-address-list** *access-list-number*

bridge-group *bridge-group* **output-lat-service-deny** *group-list*

bridge-group *bridge-group* **output-lat-service-permit** *group-list*

bridge-group *bridge-group* **output-lsap-list** *access-list-number*

bridge-group *bridge-group* **output-pattern-list** *access-list-number*

bridge-group *bridge-group* **output-type-list** *access-list-number*

bridge-group *bridge-group* **sse**

bridge-group *bridge-group* **subscriber-loop-control**

bridge-group *bridge-group* **subscriber-trunk**

bridge *bridge-group* **lat-service-filtering**

frame-relay map bridge *dlci* **broadcast**

interface bvi *bridge-group*

x25 map bridge *x.121-address* **broadcast** [*options-keywords*]

ハイ アベイラビリティ

サポートされていない SSO 認識 HSRP コマンド

すべて

HSRP

サポートされていないグローバル コンフィギュレーション コマンド

interface Async

interface BVI

interface Dialer

interface Group-Async

interface Lex

interface Multilink

interface Virtual-Template

interface Virtual-Tokenring

サポートされていないインターフェイス コンフィギュレーション コマンド

mtu

standby mac-refresh *seconds*

standby use-bia

IGMP スヌーピング コマンド

サポートされていないグローバル コンフィギュレーション コマンド

ip igmp snooping tcn

インターフェイス コマンド

サポートされていない特権 EXEC コマンド

show interfaces [*interface-id* | **vlan** *vlan-id*] [**crb** | **fair-queue** | **irb** | **mac-accounting** | **precedence** | **irb** | **random-detect** | **rate-limit** | **shape**]

サポートされていないグローバル コンフィギュレーション コマンド

interface tunnel

サポートされていないインターフェイス コンフィギュレーション コマンド

transmit-interface *type number*

IP マルチキャスト ルーティング

サポートされていない特権 EXEC コマンド

clear ip rtp header-compression [*type number*]

debug ip packet コマンドを実行すると、スイッチの CPU で受信したパケットが表示されます。ハードウェア スイッチングされたパケットは表示されません。

debug ip mcache コマンドは、スイッチの CPU で受信したパケットに影響します。ハードウェア スイッチングされたパケットは表示されません。

debug ip mpacket [**detail**] [*access-list-number* [*group-name-or-address*] コマンドは、スイッチの CPU で受信したパケットだけに影響します。ほとんどのマルチキャスト パケットはハードウェア スイッチングされるので、このコマンドは、ルートによってパケットが CPU に転送されるとわかっている場合にだけ使用します。

debug ip pim atm

show frame-relay ip rtp header-compression [**interface** *type number*]

show ip mcache コマンドを実行すると、スイッチの CPU に送信されたパケットのキャッシュ内のエントリが表示されます。ほとんどのマルチキャスト パケットは CPU に送信されずにハードウェアでスイッチングされるので、このコマンドは使用できますが、マルチキャスト パケット情報は表示されません。

show ip mpacket コマンドはサポートされていますが、スイッチの CPU で受信されたパケットに対してだけ役立ちます。ルートがハードウェア スイッチングされる場合は、CPU でパケットが受信されず、パケットを表示できないので、コマンドを使用しても無効です。

show ip pim vc [*group-address* | *name*] [*type number*]

show ip rtp header-compression [*type number*] [**detail**]

サポートされていないグローバル コンフィギュレーション コマンド

ip pim accept-rp {*address* | **auto-rp**} [*group-access-list-number*]

ip pim message-interval *seconds*

サポートされていないインターフェイス コンフィギュレーション コマンド

frame-relay ip rtp header-compression [**active** | **passive**]

frame-relay map ip *ip-address dlci* [**broadcast**] **compress**

frame-relay map ip *ip-address dlci* **rtp header-compression** [**active** | **passive**]

ip igmp helper-address *ip-address*

ip multicast helper-map {*group-address* | **broadcast**} {*broadcast-address* | *multicast-address*} *extended-access-list-number*

ip multicast rate-limit {**in** | **out**} [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*] *kbps*

ip multicast ttl-threshold *ttl-value*（代わりに、**ip multicast boundary** *access-list-number* インターフェイス コンフィギュレーション コマンドを使用してください）

ip multicast use-functional

ip pim minimum-vc-rate *pps*

ip pim multipoint-signalling

ip pim nbma-mode

ip pim vc-count *number*

ip rtp compression-connections *number*

ip rtp header-compression [**passive**]

IP SLA

サポートされていない MPLS ヘルス モニタ コマンド

すべて

サポートされていないイーサネット ゲートキーパー登録コマンド

すべて

サポートされていない VoIP コール セットアップ プローブ コマンド

すべて

IP ユニキャスト ルーティング

サポートされていない特権 EXEC コマンドまたはユーザ EXEC コマンド

clear ip accounting [**checkpoint**]
clear ip bgp *address* flap-statistics
clear ip bgp prefix-list
debug ip cef stats
show cef [**drop** | **not-cef-switched**]
show ip accounting [**checkpoint**] [**output-packets** | **access-violations**]
show ip bgp dampened-paths
show ip bgp inconsistent-as
show ip bgp regexp *regular expression*
show ip prefix-list *regular expression*

サポートされていないグローバル コンフィギュレーション コマンド

ip accounting precedence {**input** | **output**}
ip accounting-list ***ip-address wildcard***
ip as-path access-list
ip accounting-transits *count*
ip cef traffic-statistics [**load-interval** *seconds*] [**update-rate** *seconds*]]
ip flow-aggregation
ip flow-cache
ip flow-export
ip gratuitous-arps
ip local
ip prefix-list
ip reflexive-list
router egp
router-isis
router iso-igrp
router mobile
router odr
router static

サポートされていないインターフェイス コンフィギュレーション コマンド

ip accounting

ip load-sharing [**per-packet**]

ip mtu *bytes*

ip ospf dead-interval minimal hello-multiplier *multiplier*

ip verify

ip unnumbered *type number*

すべての **ip security** コマンド

サポートされていない BGP ルータ コンフィギュレーション コマンド

address-family vpnv4

default-information originate

neighbor advertise-map

neighbor allowas-in

neighbor default-originate

neighbor description

network backdoor

table-map

サポートされていない VPN コンフィギュレーション コマンド

すべて

サポートされていないルート マップ コマンド

match route-type（Policy-Based Routing（PBR; ポリシーベース ルーティング）用）

set as-path {**tag** | **prepend** *as-path-string*}

set automatic-tag

set dampening *half-life reuse suppress max-suppress-time*

set default interface *interface-id* [*interface-id.....*]

set interface *interface-id* [*interface-id.....*]

set ip default next-hop *ip-address* [*ip-address.....*]

set ip destination *ip-address mask*

set ip next-hop verify-availability

set ip precedence *value*

set ip *qos-group*

set metric-type internal

set origin

set metric-type internal

set tag *tag-value*

IPv6

IPv4-v6 トンネリング コマンド

すべて

レイヤ 3

BGP

次の機能に対するすべてのコマンド

- ネットワーク AS 移行のためのデュアル AS 設定の BGP サポート
- グローバル テーブルから VRF テーブルへの IP プレフィクス インポートのための BGP サポート
- 名前付き拡張コミュニティ リストのための BGP サポート
- 拡張コミュニティ リストのシーケンス エントリのための BGP サポート
- TTL セキュリティ チェックのための BGP サポート
- BGP ルートマップ ポリシー リスト サポート
- BGP ネクストホップ伝播
- BGP ポリシー アカウンティング
- BGP ポリシー アカウンティングの出力インターフェイス アカウンティング
- BGP リンク帯域幅
- BGP ハイブリッド CLI サポート
- BGP コスト コミュニティ
- BGP ダイナミック アップデート ピアグループ
- BGP 条件付きルート インジェクション
- BGP ピア テンプレート使用コンフィギュレーション
- AS パス アクセス リスト 500 までの番号に対する BGP のサポートの強化

その他のサポートされていない BGP コマンド

address-family l2vpn

address-family vpnv4

bgp-policyclear bgp nsapaddress-family nsap

clear bgp nsap dampening
clear bgp nsap external
clear bgp nsap flap-statistics
clear bgp nsap peer-group
clear ip bgp ipv6
clear ip bgp l2vpn
clear ip bgp vpnv4
clear ip bgp vpnv6
ha-mode graceful-restartip extcommunity-list redistribute（BGP から ISO IS-IS）
ip policy-listredistribute（ISO IS-IS から BGP）
match extcommunity
neighbor ha-mode graceful-restart
neighbor sooredistribute dvmrp
neighbor ttl-securityset extcommunity
set extcommunity cost
show bgp nsap
show bgp nsap community
show bgp nsap community-list
show bgp nsap dampening
show bgp nsap dampened-paths
show bgp nsap filter-list
show bgp nsap flap-statistics
show bgp nsap inconsistent-as
show bgp nsap neighbors
show bgp nsap paths
show bgp nsap quote-regexp
show bgp nsap regexp
show bgp nsap summary
show ip bgp ipv4 multicast
show ip bgp ipv4 multicast summary
show ip bgp l2vpn
show ip bgp vpnv4
show ip extcommunity-list
show ip policy-list

OSPF

area sham-link
ignore lsa mospf
nsf ietf
nsf ietf helper disable
nsf ietf helper strict-lsa-checking
show ip ospf sham-links

VRF 認識 AAA

すべて

MAC アドレス コマンド

サポートされていない特権 EXEC コマンド

show mac-address-table
show mac-address-table address
show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table interface
show mac-address-table multicast
show mac-address-table notification
show mac-address-table static
show mac-address-table vlan
show mac address-table multicast

（注）　VLAN のレイヤ 2 マルチキャスト アドレス テーブル エントリを表示するには、**show ip igmp snooping groups** 特権 EXEC コマンドを使用します。

サポートされていないグローバル コンフィギュレーション コマンド

mac-address-table aging-time
mac-address-table notification
mac-address-table static

その他

サポートされていないユーザ EXEC コマンド

verify

サポートされていない特権 EXEC コマンド

file verify auto

remote command

show cable-diagnostics prbs

test cable-diagnostics prbs

サポートされていないグローバル コンフィギュレーション コマンド

errdisable recovery cause unicast flood

l2protocol-tunnel global drop-threshold

memory reserve critical

service compress-config

track *object-number* **rtr**

stack-mac persistent timer

MSDP

サポートされていない特権 EXEC コマンド

show access-expression

show exception

show location

show pm LINE

show smf [*interface-id*]

show subscriber-policy [*policy-number*]

show template [*template-name*]

サポートされていないグローバル コンフィギュレーション コマンド

ip msdp default-peer *ip-address* | *name* [**prefix-list** *list*] （BGP および MBGP はサポートされていないので、このコマンドの代わりに **ip msdp peer** コマンドを使用してください）

マルチキャスト

サポートされていない双方向 PIM コマンド

すべて

サポートされていないマルチキャスト ルーティング マネージャ コマンド

すべて

サポートされていない IP マルチキャスト レート制限コマンド

すべて

サポートされていない UDLR コマンド

すべて

サポートされていない Multicast over GRE コマンド

すべて

NetFlow コマンド

サポートされていないグローバル コンフィギュレーション コマンド

ip flow-aggregation cache

ip flow-cache entries

ip flow-export

ネットワーク アドレス変換（NAT）コマンド

サポートされていない特権 EXEC コマンド

show ip nat statistics

show ip nat translations

QoS

サポートされていないグローバル コンフィギュレーション コマンド

priority-list

サポートされていないインターフェイス コンフィギュレーション コマンド

priority-group

rate-limit

サポートされていないポリシーマップ コンフィギュレーション コマンド

class class-default（ここで、**class-default** は *class-map-name* です）

RADIUS

サポートされていないグローバル コンフィギュレーション コマンド

aaa nas port extended

aaa authentication ***feature*** **default enable**

aaa authentication ***feature*** **default line**

aaa nas port extended

radius-server attribute nas-port

radius-server configure

radius-server extended-portnames

SNMP

サポートされていないグローバル コンフィギュレーション コマンド

snmp-server enable informs

snmp-server ifindex persist

SNMPv3

サポートされていない 3DES 暗号化コマンド

すべて

スパニング ツリー

サポートされていないグローバル コンフィギュレーション コマンド

spanning-tree pathcost method {long | short}

サポートされていないインターフェイス コンフィギュレーション コマンド

spanning-tree stack-port

VLAN

サポートされていないグローバル コンフィギュレーション コマンド

vlan internal allocation policy {ascending | descending}

サポートされていないユーザ EXEC コマンド

show running-config vlan

show vlan ifindex

vlan database

サポートされていない VLAN データベース コマンド

vtp

vlan

VTP

サポートされていない特権 EXEC コマンド

vtp {**password** *password* | **pruning** | **version** *number*}

（注）　このコマンドは、**vtp** グローバル コンフィギュレーション コマンドに置き換えられています。

INDEX

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

は

ひ

へ

ほ

ま

み

む

め

も

ゆ

よ

ら

り

る

れ

ろ

わ