Cisco IE 2000 スイッチ ソフトウェア コンフィギュレーション ガイド
Cisco IOS Release 15.0(2)EB

2013 年 2 月

Text Part Number: 78-21162-01-J

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

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

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

Cisco IE 2000 スイッチ ソフトウェア コンフィギュレーション ガイド
Cisco IOS Release 15.0(2)EB

CONTENTS

はじめに

対象読者

このマニュアルでは、スイッチを管理するネットワーキング専門家を対象としています。Cisco IOS ソフトウェアの使用経験があり、イーサネットおよび LAN の概念や専門用語を十分理解していることが前提です。

目的

このマニュアルでは、スイッチ上で Cisco IOS ソフトウェア機能を設定するために必要な情報について説明します。

このマニュアルでは、スイッチで使用するために作成または変更されたコマンドの使用手順を扱っています。これらのコマンドの詳細は扱いません。これらのコマンドの詳細については、このリリースに対応する『*CiscoIE 2000 Switch Command Reference*』を参照してください。

標準の Cisco IOS コマンドの詳細については、Cisco.com のホーム ページから使用できる Cisco IOS 15.0 のマニュアル セットを参照してください。

このマニュアルでは、組み込みデバイス マネージャのグラフィカル ユーザ インターフェイス（GUI）については詳しく説明しません。ただし、記述されている概念は、GUI ユーザにも有益なものです。デバイス マネージャについては、スイッチのオンライン ヘルプを参照してください。

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

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

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

対話形式の例では、次の表記法を使用しています。

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

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

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

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

関連資料

次に挙げる、スイッチに関する詳細情報が記載されているマニュアルは、次の Cisco.com サイトから入手できます。

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

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

スイッチに関するその他の情報については、次の資料を参照してください。

- *リリース ノート*
- *ソフトウェア コンフィギュレーション ガイド*
- *コマンド リファレンス*
- *システム メッセージ ガイド*
- *ハードウェア インストレーション ガイド*
- *スタートアップ ガイド*
- *法令準拠および安全上の注意*
- *インストレーション ノートおよびアップグレード方法などのその他のマニュアル*
- Device Manager のオンライン ヘルプ（スイッチで利用可能）
- *ネットワーク アドミッション コントロール ソフトウェア コンフィギュレーション ガイド*

- 互換性マトリクス ドキュメントは、Cisco.com の次のページで入手可能です。
  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

マニュアルの入手方法およびテクニカル サポート

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

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

CHAPTER 1

設定の概要

機能

スイッチは暗号化イメージ（暗号化対応）をサポートするために Cisco IOS ソフトウェア ライセンス（CISL）アーキテクチャを使用しています。このイメージは、スイッチ モデルによって LAN Base または LAN Lite 機能を実装しています。

- LAN Base イメージは、Quality Of Service (QoS)、ポート セキュリティ、1588v2 PTP、およびスタティック ルーティング機能を提供します。
- LAN Lite イメージは、SSH や SNMPv3 などの重要なセキュリティ機能を除き、レイヤ 2 機能が制限されて提供されます。

フィーチャ ソフトウェア ライセンス

フィーチャ ライセンスは、ソフトウェア ライセンスによって LAN Base または LAN Lite 機能を実装する、単一のユニバーサル イメージでサポートされます。

- LAN Base 機能には、Quality Of Service（QoS）、ポート セキュリティ、PTP およびスタティック ルーティングが含まれます。
- LAN Lite 機能は、SSH や SNMPv3 などの重要なセキュリティ機能を除き、レイヤ 2 機能が制限されて提供されます。

暗号化機能はユニバーサル イメージに含まれています。

これらのガイドラインは、スイッチ上でどのイメージが動作しているかを特定することができます。

- **show version** 特権 EXEC コマンドを入力します。たとえば、IE-2000-8TC-G-E はデフォルトで LAN Base イメージを実行し、IE-2000-4T-G-L は LAN Lite イメージを実行します。
- **show license** 特権 EXEC コマンドを入力し、アクティブなイメージを確認します。

```
Switch# show license
Index 1 Feature: lanbase
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Priority: Medium
        License Count: Non-Counted

Index 2 Feature: lanlite
        Period left: 0  minute  0  second
```

使用および導入を簡素化する機能

- Express Setup : 基本的な IP 情報、コンタクト情報、スイッチおよび Telnet のパスワード、および Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）に関する情報を使用し、ブラウザ ベースのプログラムを通じて、スイッチの初回設定を迅速に行うことができます。Express Setup の詳細については、スタートアップ ガイドを参照してください。
- ユーザ定義およびデフォルト設定の SmartPort マクロ：ネットワークへの配置を簡単にするためにカスタム スイッチ設定を作成します。
- 着脱式の SD フラッシュ カードに、Cisco IOS ソフトウェア イメージと、スイッチのコンフィギュレーション ファイルが格納されています。ソフトウェア機能を再設定せずに、スイッチの交換やアップグレードを実行できます。
- 組み込みのデバイス マネージャ GUI：単体のスイッチを Web ブラウザから設定、管理します。デバイス マネージャの起動については、スタートアップ ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。

パフォーマンス向上機能

- すべてのスイッチ ポートの速度自動検知、およびデュプレックス モードの自動ネゴシエーション。帯域幅の利用を最適化します。
- 10/100 Mbps インターフェイス、10/100/1000 Mbps インターフェイス、および 10/100/1000 BASE-TX SFP モジュール インターフェイス上の Auto MDIX 機能により、インターフェイスが必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定します。
- ルーテッド フレームの場合は最大 1546 バイト、ハードウェアでブリッジングされるフレームの場合は最大 9000 バイト、ソフトウェアでブリッジングされるフレームの場合は最大 2000 バイトのサポート。
- すべてのポートにおける IEEE 802.3x フロー制御（スイッチはポーズ フレームを送信しません）。
- 最大 6 個の EtherChannel グループのサポート。
- ポート集約プロトコル（PAgP）および Link Aggregation Control Protocol（LACP）により、EtherChannel リンクを自動的に作成。
- ポート単位のストーム制御。ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームを防止します。
- レイヤ 2 の不明なユニキャスト、マルチキャスト、およびブリッジド ブロードキャスト トラフィック転送に対するポート ブロッキング。
- Cisco Group Management Protocol（CGMP）サーバのサポートおよび Internet Group Management Protocol（IGMP）バージョン 1、バージョン 2、およびバージョン 3 対応の IGMP スヌーピング。
  - （CGMP デバイスの場合）CGMP が特定のエンド ステーションへのマルチキャスト トラフィックを制限し、ネットワーク全般のトラフィックを軽減
  - （IGMP デバイスの場合）IGMP スヌーピングによってマルチメディア トラフィックとマルチキャスト トラフィックを転送
- IGMP レポート抑制。1 つのマルチキャスト ルータ クエリーにつき 1 つの IGMP レポートだけをマルチキャスト デバイスへ送信します（IGMPv1 または IGMPv2 クエリーだけをサポート）。
- IGMP スヌーピング クエリー サポート。IGMP 一般クエリー メッセージを定期的に生成するようにスイッチを設定します。

- IGMP ヘルパーにより、スイッチでホスト要求を転送して、特定の IP 宛先アドレスにマルチキャスト ストリームを加入させることが可能。
- IGMP フィルタリングにより、スイッチ ポート上のホストが所属できるマルチキャスト グループセットを管理します。
- IGMP スロットリング。IGMP 転送テーブルのエントリ数が最大になったときのアクションを設定します。
- ネットワーク終了の待ち時間を設定できる IGMP の Leave タイマー。
- Switch Database Management（SDM）テンプレートにより、ユーザ側で選択する機能へのサポートを最大化するようにシステム リソースを割り当てられます。
- Cisco IOS IP サービス レベル契約（SLA）は、Cisco IOS ソフトウェアの一部で、ネットワーク パフォーマンスを測定するアクティブ トラフィック モニタリングを使用します。
- 設定可能なスモールフレーム着信しきい値により、スモール フレーム（64 バイト以下）が指定されたレート（しきい値）でインターフェイスに着信した場合のストーム制御を防止します。
- FlexLink に障害が発生したあとのマルチキャスト トラフィックのコンバージェンス時間を短縮するための FlexLink マルチキャスト高速コンバージェンス。
- RADIUS サーバのロード バランシングにより、サーバ グループにおける認証要求の均等な配信が可能 。
- CPU 生成トラフィックの QoS マーキングのサポートと、出力ネットワーク ポートへの CPU 生成トラフィックのキュー。

管理オプション

- 組み込みデバイス マネージャ：GUI アプリケーションのデバイス マネージャがソフトウェア イメージに組み込まれています。このデバイス マネージャは、単体のスイッチの設定、管理に使用します。デバイス マネージャの起動については、スタートアップ ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Network Assistant：Network Assistant は、Cisco.com からダウンロードできるネットワーク管理アプリケーションです。単一のスイッチ、スイッチ クラスタ、デバイスのコミュニティの管理に使用します。Network Assistant の詳細については、Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。
- CLI：Cisco IOS ソフトウェアは、デスクトップ スイッチングおよびマルチレイヤ スイッチング機能をサポートします。CLI にアクセスするには、管理ステーションをスイッチ コンソール ポートに直接接続するか、リモート管理ステーションから Telnet を利用します。CLI の詳細については、第 2 章「コマンドライン インターフェイスの使用」を参照してください。
- SNMP：CiscoWorks 2000 LAN Management Suite（LMS）および HP OpenView などの SNMP 管理アプリケーション。HP OpenView、SunNet Manager などのプラットフォームが稼働している SNMP 対応管理ステーションから管理できます。スイッチは豊富な MIB 拡張機能および 4 つの Remote Monitoring（RMON）グループをサポートします。SNMP の詳しい使用方法については、第 36 章「SNMP の設定」を参照してください。
- Cisco IOS Configuration Engine（旧称 Cisco IOS CNS エージェント）：コンフィギュレーション サービスは、ネットワーク デバイスおよびサービスの導入と管理を自動化します。スイッチごとに設定変更の内容を生成してスイッチに送信し、その設定変更を適用した後、その結果を記録することで初期設定および設定の更新を自動化できます。

  CNS の詳細については、第 5 章「Cisco IOS Configuration Engine の設定」を参照してください。

工業用アプリケーション

- CIP：Common Industrial Protocol（CIP）はピアツーピアのアプリケーション プロトコルであり、スイッチと工業用装置（I/O コントローラ、センサー、リレーなど）間でアプリケーション レベルの接続を実現します。CIP ベースの管理ツール（RSLogix など）を使用してスイッチを管理できます。スイッチでサポートされる CIP コマンドの詳細については、コマンド リファレンスを参照してください。
- PROFINET Version 2：PROFINET IO（分散型オートメーション アプリケーション用のモジュラ通信フレームワーク）をサポートします。スイッチから I/O コントローラへの PROFINET 管理接続が可能です。

管理の簡易性に関する機能

- スイッチ管理、設定ストレージ、および配信を自動化するための CNS の組み込み型エージェント。
- Dynamic Host Configuration Protocol（DHCP）によるスイッチ情報（IP アドレス、デフォルト ゲートウェイ、ホスト名、ドメイン ネーム システム（DNS）、TFTP サーバ名）の自動設定。
- DHCP リレーによる DHCP クライアントからのユーザ データグラム プロトコル（UDP）ブロードキャストの転送（IP アドレス要求を含む）。
- DHCP サーバによる IP アドレスおよびその他の DHCP オプションの IP ホストへの自動割り当て。
- 新しいイメージの指定された設定を多数のスイッチにダウンロードするために、DHCP ベースの自動設定およびイメージをアップデート。
- 新しいバルク リース クエリー タイプ（RFC5460 で定義）をサポートする DHCPv6 バルクリース クエリー。
- DHCPv6 リレー エージェントの送信元アドレスを設定する DHCPv6 リレー送信元設定機能。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにしたアドレス割り当て。
- IP アドレスおよび対応するホスト名からスイッチを特定することを目的とした、ユニキャスト要求の DNS サーバへの転送、および TFTP サーバからソフトウェア アップグレードを管理することを目的とした、ユニキャスト要求の TFTP サーバへの転送。
- アドレス解決プロトコル（ARP）。IP アドレスおよび対応する MAC アドレスによってスイッチを特定します。
- 特定の送信元 MAC アドレスおよび宛先 MAC アドレスを持ったパケットをドロップするユニキャスト MAC アドレス フィルタリング。
- 設定可能な MAC アドレス スケーリング。これにより、VLAN で MAC アドレス ラーニングをディセーブルにし、MAC アドレス テーブルのサイズを制限することができます。
- Cisco Discovery Protocol（CDP）バージョン 1 および 2。ネットワーク トポロジを検出し、ネットワーク上のスイッチと他のシスコ デバイスとのマッピングを行います。
- リンク層検出プロトコル（LLDP）および LLDP Media Endpoint Discovery（LLDP-MED）によるサードパーティ製 IP 電話との相互運用性の確保。
- スイッチからエンドポイント デバイスへロケーション情報を提供する LLDP メディア拡張（LLDP-MED）ロケーション TLV。
- ネットワーク タイム プロトコル（NTP）により、外部ソースから全スイッチに一貫したタイムスタンプを提供します。

- IPv4 と IPv6 の両方をサポートし、NTPv3 と互換性のある Network Time Protocol version 4（NTPv4）。
- IEEE 1588 標準で定められた高精度時間プロトコル（PTP）により、ネットワーク内の装置のリアルタイム クロックをナノ秒精度で同期できます。
  - 拡張モジュール ポートの PTP メッセージをサポートする PTP 拡張機能。
- Cisco IOS File System（IFS）。スイッチが使用するすべてのファイル システムに対して単一インターフェイスを提供します。
- ビデオなどのマルチキャスト アプリケーションを最適化するための SSM PIM プロトコルのサポート。
- スイッチの設定変更を記録して表示させるコンフィギュレーション ロギング。
- 一意のデバイス ID。**show inventory** ユーザ EXEC コマンドで製品の ID 情報が表示されます。
- Netscape Communicator または Microsoft Internet Explorer ブラウザ セッションでデバイス マネージャを使用した帯域内管理アクセス。
- 最大 16 の Telnet 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます。
- ネットワーク上の複数の CLI セッションに対する、最大 5 つの同時暗号化セキュア シェル（SSH）接続の確立によって帯域内管理アクセス。
- SNMP のバージョン 1、バージョン 2c、およびバージョン 3 の get および set 要求による帯域内管理アクセス。
- 帯域外管理アクセス。スイッチのコンソール ポートに端末を直接接続するか、またはシリアル接続とモデム経由でリモート端末に接続します。
- Secure Copy Protocol（SCP）機能により、セキュアかつ認証済みの方法でスイッチ設定またはスイッチ イメージ ファイルをコピーできます（暗号化バージョンのソフトウェアが必要）。
- 設定の交換およびロールバックは、スイッチ上で一意の保存された Cisco IOS コンフィギュレーション ファイルで稼働している設定を交換します。
- Cisco IOS の HTTP クライアントは、IPv4 と IPv6 の両方の HTTP サーバに要求を送信することができます。また、Cisco IOS の HTTP サーバは、IPv4 と IPv6 の両方の HTTP クライアントから、HTTP 要求にサービスを提供することができます。
- 簡易ネットワーク管理プロトコル（SNMP）を IPv6 トランスポートを介して設定できるため、IPv6 ホストは SNMP クエリーを送信し、IPv6 を実行中のデバイスから SNMP 通知を受信できます。
- ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイト アドレス指定の変更を管理するための IPv6 ステートレス自動設定。
- VLAN の MAC アドレス ラーニングをディセーブルにします。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにしたアドレス割り当て。
- CPU 使用率しきい値トラップによる CPU 使用率の監視。
- VLAN、サービス クラス（CoS）、DiffServ コード ポイント（DSCP）、およびタグ付けモードを指定して音声と音声シグナリングのプロファイルを作成する LLDP-MED ネットワークポリシー プロファイル Time、Length、Value（TLV; 時間、長さ、時間）。
- DHCPDISCOVER パケットの Option 12 フィールドにホスト名の入力をサポート。これにより、DHCP プロトコルを使用して同一のコンフィギュレーション ファイルを複数送信できます。
- DHCP スヌーピング拡張機能。これにより、Option 82 DHCP フィールドで指定する回線 ID サブオプションに、固定文字列ベースのフォーマットを選択できるようになります。

- PROFINET IO（分散型オートメーション アプリケーション用のモジュラ通信フレームワーク）をサポートします。スイッチから I/O コントローラへの PROFINET 管理接続が可能です。

アベイラビリティおよび冗長性に関する機能

- Unidirectional Link Detection（UDLD; 単一方向リンク検出）およびアグレッシブ UDLD。光ファイバ ケーブルの配線ミスまたはポート障害に起因する光ファイバ インターフェイス上の単一方向リンクを検出し、ディセーブルにします。
- IEEE 802.1D Spanning-Tree Protocol（STP; スパニングツリー プロトコル）による冗長バックボーン接続およびループフリー ネットワーク。STP には次の機能があります。
  - 最大 128 のスパニングツリー インスタンスをサポート。
  - Per-VLAN Spanning-Tree Plus（PVST+）による VLAN 間でのロード バランシング。
  - Rapid PVST+ による、VLAN 間でのロード バランシングおよびスパニングツリー インスタンスの高速コンバージェンスの実現。
- IEEE 802.1s Multiple Spanning-Tree Protocol（MSTP）により、VLAN をスパニングツリー インスタンスに分類、またデータ トラフィックおよびロード バランシング用に複数の転送パスを確保します。また、IEEE 802.1w Rapid Spanning-Tree Protocol（RSTP）に基づいた Rapid Per-VLAN Spanning-Tree plus（Rapid PVST+）により、ルートと指定ポートをただちにフォワーディング ステートに変更することで、スパニングツリーの高速コンバージェンスが実現されます。
- PVST+、Rapid-PVST+、および MSTP モードで使用できるスパニングツリーのオプション機能は次のとおりです。
  - PortFast。ポートをブロッキング ステートからフォワーディング ステートへただちに変更させることによって、転送遅延を防ぎます。
  - BPDU ガード。Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信する PortFast 対応ポートをシャットダウンします。
  - BPDU フィルタリング。PortFast 対応ポートで BPDU の送受信ができなくなります。
  - ルート ガード。ネットワーク コア外のスイッチがスパニングツリー ルートになることを防ぎます。
  - ループ ガード。代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。
- FlexLink レイヤ 2 インターフェイス。基本リンク冗長の STP に代わるものとして、互いにバックアップします。（LAN Base イメージが必要）
- リンクステート トラッキング。接続されたホストとサーバからのアップストリーム トラフィックを伝送するポートの状態をミラーリングします。また、別のシスコ製イーサネット スイッチで動作するリンクへサーバ トラフィックをフェールオーバーすることができます。

VLAN 機能

- 最大 255 個の VLAN をサポート。適切なネットワーク リソース、トラフィック パターン、および帯域幅を対応付けて、VLAN にユーザを割り当てることができます。
- IEEE 802.1Q 規格で認められている 1 ～ 4096 の範囲で VLAN ID をサポート。
- ダイナミック VLAN メンバーシップに対応する VLAN Query Protocol（VQP）。

- すべてのポート上で稼働する IEEE 802.1Q トランキング カプセル化。ネットワークの移動、追加、変更や、ブロードキャストおよびマルチキャスト トラフィックの管理および制御、さらに、ハイ セキュリティ ユーザおよびネットワーク リソース別の VLAN グループの確立によるネットワーク セキュリティを実現します。
- ダイナミック トランキング プロトコル（DTP）。2 台のデバイス間のリンク上でトランキングをネゴシエートするだけでなく、使用するトランキング カプセル化のタイプ（IEEE 802.1Q）もネゴシエートします。
- VLAN トランキング プロトコル（VTP）および VTP プルーニング。トラフィックのフラッディングをそのトラフィックを受信するステーションへのリンクだけに制限することによって、ネットワーク トラフィックを削減します。
- 音声 VLAN。Cisco IP Phone から音声トラフィック用のサブネットを作成します。
- VLAN 1 の最小化：VLAN 1 を任意の個々の VLAN トランク リンクでディセーブル化することで、スパニングツリー ループまたはストームのリスクを軽減。この機能をイネーブルに設定すると、トランク上でユーザ トラフィックは送受信されません。スイッチの CPU は、引き続き制御プロトコル フレームの送受信を行います。
- VLAN FlexLink ロード バランシング：スパニングツリー プロトコル（STP）を必要としないレイヤ 2 冗長性を提供。プライマリおよびバックアップ リンクとして設定したインターフェイスのペアを使用して、VLAN ベースによるトラフィックのロード バランシングが可能です。
- 制限付き VLAN（*認証失敗 VLAN* とも呼ばれる）による 802.1X 認証のサポート。
- VTP バージョン 3 のサポート。具体的には、任意の VTP モードによる拡張範囲 VLAN（VLAN 1006 ～ 4096）設定のサポート、認証の拡張機能（非表示パスワードまたはシークレット パスワード）、VTP に加えて他のデータベースの伝播、VTP プライマリ サーバおよびセカンダリ サーバ、VTP のポートによるオン / オフの切り替えオプションがあります。

セキュリティ機能

- アクティブ トラフィック モニタリングを使用してネットワーク パフォーマンスを測定するための IP サービス レベル契約（IP SLA）のサポート。
- LAN SLA EOT により、スタンバイ ルータのフェールオーバー引き継ぎを行うために、遅延、ジッター、パケット損失などのアクションによってトリガーされる IP SLA 追跡動作からの出力を使用できます（LAN Base イメージが必要）。
- Web 認証。IEEE 802.1x 機能をサポートしないサプリカント（クライアント）に Web ブラウザを使用して認証可能になります。
- ローカル Web 認証バナー。これにより、カスタム バナー、またはイメージ ファイルを Web 認証ログイン画面に表示することができます。
- MAC authentication bypass（MAB; MAC 認証バイパス）エージング タイマー。MAB を使用して認証した後に認証された非アクティブのホストを検出します。
- 管理インターフェイス（デバイス マネージャ、Network Assistant、CLI）へのパスワード保護付きアクセス（読み取り専用および読み書きアクセス）。不正な設定変更を防止します。
- セキュリティ レベル、通知、および対応するアクションを選択できる、マルチレベル セキュリティ。
- セキュリティを確保できるスタティック MAC アドレッシング。
- 保護ポート オプション。同一スイッチ上の指定ポートへのトラフィック転送を制限します。
- ポートにアクセスできるステーションの MAC アドレスを制限または特定するポート セキュリティ オプション。

- 違反発生時に、ポート全体をシャットダウンするのではなく、そのポートの VLAN をシャットダウンする VLAN 対応ポート セキュリティ オプション。
- ポート セキュリティ エージング。ポートのセキュア アドレスにエージング タイムを設定します。
- 指定した入力割合を超えたパケットをドロップして、スイッチへの着信プロトコル トラフィックの割合を制御する、プロトコル ストーム プロテクション。
- BPDU ガード。無効なコンフィギュレーションが発生した場合に、PortFast が設定されているポートをシャットダウンします。
- 標準および拡張 IP ACL。ルーテッド インターフェイス（ルータ ACL）と VLAN の双方向およびレイヤ 2 インターフェイス（ポート ACL）の受信方向に関するセキュリティ ポリシーを定義します。
- MAC 拡張アクセス コントロール リスト。レイヤ 2 インターフェイスの着信方向のセキュリティ ポリシーを定義します。
- 非 IP トラフィックをフィルタリングする、送信元および宛先 MAC ベースの ACL。
- untrusted（信頼性のない）ホストと DHCP サーバの間の untrusted DHCP メッセージをフィルタリングする DHCP スヌーピング。
- DHCP スヌーピング データベース、および IP ソース バインディングに基づいてトラフィックをフィルタリングすることにより、非ルーテッド インターフェイスでのトラフィックを制限する IP ソース ガード。
- 不正な ARP 要求や応答を同じ VLAN 上のその他のポートにリレーしないことにより、スイッチに対する悪意のある攻撃を回避するためのダイナミック ARP インスペクション。
- レイヤ 2 プロトコル トンネリングのバイパス機能。サードパーティ ベンダーとの相互運用性を実現します。
- IEEE 802.1x ポートベース認証。不正なデバイス（クライアント）によるネットワーク アクセスを防止します。次の機能がサポートされています。
  - データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が、同じ IEEE 802.1x 対応スイッチ ポートにおいて、単独で認証できるようにする Multidomain Authentication（MDA; マルチドメイン認証）。
  - MDA のダイナミック音声 VLAN（仮想 LAN）。ダイナミック音声 VLAN が MDA 対応ポートで可能になります。
  - VLAN 割り当て。802.1x 認証ユーザを特定の VLAN に制限します。
  - ポート セキュリティ。802.1x ポートへのアクセスを制御します。
  - 音声 VLAN。ポートが許可ステートか無許可ステートかにかかわらず、Cisco IP Phone の音声 VLAN へのアクセスを許可します。
  - Cisco IP Phone を検出および認識するための IP Phone 拡張検出機能。
  - ゲスト VLAN。802.1x に適合しないユーザに限定的なサービスを提供します。
  - 制限付き VLAN。802.1x に準拠はしているが、標準の 802.1x で認証するためのクレデンシャルを持っていないユーザに制限付きのサービスを提供します。
  - 802.1x アカウンティング。ネットワーク使用をトラッキングします。
  - 802.1x と LAN の Wake-on-LAN（WoL）機能。休止状態の PC に、特定のイーサネット フレームを送信して起動させます。
  - 802.1x 準備状態チェック。スイッチで IEEE 802.1x を設定する前に、接続されたエンド ホストの準備状態を判断します。

  - セキュリティ違反が発生した VLAN だけでトラフィック違反アクションを適用するための音声認識 802.1x セキュリティ。
  - MAC 認証バイパス。クライアントの MAC アドレスに基づいてクライアントを許可します。
  - 802.1X スイッチ サプリカントを使用する Network Edge Access Topology（NEAT）、CISP を使用するホスト許可、および自動イネーブル。ワイヤリング クローゼットの外にあるスイッチを別のスイッチのサプリカントとして認証します。
  - オープン アクセス対応 IEEE 802.1x により、ホストは認証される前にネットワークにアクセスできます。
  - IEEE 802.1x 認証機能。ACL のダウンロードおよび URL のリダイレクトが可能で、これによって Cisco Secure ACS サーバから認証対象のスイッチにユーザ単位で ACL をダウンロードできます。
  - 柔軟な認証シーケンス機能。新規ホストの認証時にポートが試みる認証方式の順序を設定します。
  - 複数ユーザの認証機能により、802.1x がイネーブルになっているホストに対し、2 つ以上のホストを認証できます。

- Network Admission Control（NAC）機能：
  - デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウイルス対策の状態または*ポスチャ*に関する NAC レイヤ 2 802.1x 検証

    NAC レイヤ 2 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 802.1x 検証の設定」（P.13-46）を参照してください。
  - デバイスのネットワーク アクセスを許可する前の、エンドポイント システムまたはクライアントのポスチャに関する NAC レイヤ 2 IP 検証

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

    この機能の設定については、「アクセス不能認証バイパスの設定」（P.13-44）を参照してください。
  - 認証、許可、アカウンティング（AAA）ダウン ポリシー。ポスチャ検証が発生したときに、AAA サーバが利用できない場合のホストの NAC レイヤ 2 IP 検証

    この機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- Terminal Access Controller Access Control System Plus（TACACS+）。TACACS サーバを介してネットワーク セキュリティを管理する独自の機能です。
- RADIUS により、AAA サービスを通じてリモート ユーザの ID の確認、アクセス権の付与、アクションの追跡を実行できます。
- IPv6 上での機能向けに、RADIUS、TACACS+、および SSH を拡張。
- Kerberos セキュリティ システム。信頼できるサードパーティを使用して、ネットワーク リソースに対する要求を認証します（ソフトウェアの暗号化バージョンが必要）。
- HTTP 1.1 サーバ認証、暗号化、メッセージ整合性、HTTP クライアント認証用に Secure Socket Layer（SSL）バージョン 3.0 がサポートされ、安全な HTTP 通信が可能になります（ソフトウェアの暗号化バージョンが必要）。
- 音声認識 IEEE 802.1X および MAB セキュリティ違反。セキュリティ違反が発生すると、ポートのデータ VLAN だけがシャットダウンされます。
- スタティック ホストでの IP ソース ガードのサポート。

- RADIUS 認証の変更（CoA）。特定のセッション認証された後で、その属性を変更します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は AAA サーバから、Cisco Secure ACS などの RADIUS CoA パケットを送信し、新しいポリシーに適用することができます。
- IEEE 802.1x ユーザ ディストリビューション。さまざまな VLAN にわたってユーザをロード バランシングすることにより、（ユーザ グループに対して）複数の VLAN を使った配置で、ネットワークのスケーラビリティを向上させることができます。認証されたユーザは、RADIUS サーバにより割り当てられた、グループ内で最も空いている VLAN に割り当てられます。
- 複数のホスト認証を行うクリティカル VLAN では、ポートがマルチ認証用に設定されており、AAA サーバが到達不能となった場合でも、重要なリソースにアクセスできるように、ポートがクリティカル VLAN に配置されます。
- ローカル Web 認証のために、ユーザ定義の *login*、*success*、*failure* および *expire* Web ページを作成できるカスタマイズ可能な Web 認証拡張。
- ポート ホスト モードの変更および認証スイッチ ポート上の標準ポート設定の適用を行う Network Edge Access Topology（NEAT）のサポート。
- 認証されていない VLAN からのネットワーク アクセスを回避するためのユーザ認証に、VLAN および MAC のアドレス情報の組み合わせを使用する VLAN ID ベースの MAC 認証。
- MAC Move。モビリティのイネーブル化を制約することなく、ホスト（IP 電話の背後で接続されたホストを含む）が同じスイッチ内のポート間を移動できるようになります。MAC Move では、もう 1 つのポートに同じ MAC アドレスが再登場した場合、スイッチはこれをまったく新しい MAC アドレスと同様に扱います。
- Simple Network Management Protocol バージョン 3（SNMPv3; 簡易ネットワーク管理プロトコル バージョン 3）を使った 3DES および AES のサポート。このリリースでは、168 ビット Triple Data Encryption Standard（3DES）と、SNMPv3 への 128 ビット、192 ビット、および 256 ビットの Advanced Encryption Standard（AES; 高度暗号化規格）暗号化アルゴリズムに対するサポートが追加されます。

QoS および CoS 機能

（注） これらの機能には、LAN Base イメージが必要です。

- auto-QoS（自動 QoS）。トラフィックの分類と出力キューの設定を自動化することで既存の QoS 機能の展開を簡略化します。
- ポートベースの信頼の自動 Quality of Service（QoS）VoIP 拡張と DSCP および出トラフィックのプライオリティ キューイング
- 分類
  - IP Type of Service/Differentiated Services Code Point（IP ToS/DSCP）および IEEE 802.1p CoS のポート単位でのプライオリティ設定。ミッション クリティカルなアプリケーションのパフォーマンスを保護します。
  - IP ToS/DSCP および IEEE 802.1p CoS（サービス クラス）のフローベースのパケット分類（MAC、IP、および TCP/UDP ヘッダーに含まれる情報に基づく）によるマーキング。ネットワーク エッジで高性能な QoS 機能を提供し、ネットワーク トラフィックのタイプ別に差別化されたサービス レベルを可能にするとともに、ネットワーク上のミッション クリティカルなトラフィックにプライオリティを設定します。

  - QoS ドメイン内および別の QoS ドメインとの境界ポートにおける、trusted（信頼性のある）ポート ステート（CoS、DSCP、および IP precedence）。
  - 信頼境界機能。Cisco IP Phone の存在を検出し、受信した CoS 値を信頼して、ポート セキュリティを確保します。
- ポリシング
  - 特定のトラフィック フローに対してどの程度のポート帯域幅を割り当てるかを管理する、スイッチ ポート上のトラフィック ポリシング ポリシー。
  - 階層型のポリシーマップで複数のクラスマップを作成する場合、各クラスマップを自身のポートレベル（第 2 レベル）ポリシーマップと関連付けることができます。第 2 レベルのポリシーマップは、それぞれ異なるポリサーを保有できます。
  - トラフィック フローのポリシングをまとめて行う集約ポリシング。特定のアプリケーションまたはトラフィック フローをあらかじめ定義された特定のレートに制限します。
- 不適合
  - 帯域幅の使用制限を超過したパケットの不適合マークダウン。
- 入力キューイングおよびスケジューリング
  - ユーザ トラフィック用に設定可能な 2 つの入力キュー（一方のキューをプライオリティ キューにできます）。
  - 輻輳回避メカニズムとしての Weighted Tail Drop（WTD）。キュー長を管理し、トラフィックの分類ごとに異なる廃棄優先順位を設定します。
  - シェイプド ラウンドロビン（SRR）。パケットがキューからリングへ送出されるときのレートを決定するスケジューリング サービス（入力キューでサポートされる唯一のモードはシェアリング）。
- 出力キューおよびスケジューリング
  - 1 ポートに 4 つの出力キュー。
  - 輻輳回避メカニズムとしての WTD。キュー長を管理し、トラフィックの分類ごとに異なる廃棄優先順位を設定します。
  - スケジューリング サービスとしての SRR。キューからパケットを出して出力インターフェイスに入れる速度を指定します（出力キューではシェーピングおよび共有がサポートされます）。シェーピング型出力キューは、ポート帯域幅の割り当てが保証されますが、割り当てられたポート帯域幅の使用に制限されています。共有型出力キューは、設定された帯域幅の割り当てが保証されるだけではなく、他のキューが空になり、その割り当て分の帯域幅が使用されない場合、保証された割り当てより多く使用できます。

モニタ機能

- EOT および IP SLA EOT スタティック ルートのサポート。事前に設定したスタティック ルートまたは DHCP ルートがダウンした場合に特定します。
- MAC アドレス通知トラップおよび RADIUS アカウンティング。スイッチが学習または削除した MAC アドレスを保存することによって、ネットワーク上のユーザをトラッキングします。
- スイッチド ポート アナライザ（スイッチド ポート アナライザ（SPAN）および Remote SPAN（RSPAN）。任意のポートまたは VLAN について、トラフィック モニタリングが可能です。（RSPAN には LAN Base イメージが必要です）
- 侵入検知システム（IDS）における SPAN および RSPAN のサポート。ネットワーク セキュリティ違反をモニタ、撃退、およびレポートします。（RSPAN には LAN Base イメージが必要です）

- 組み込み RMON エージェントの 4 つのグループ（履歴、統計、アラーム、およびイベント）を使用して、ネットワークをモニタし、トラフィック解析を行うことができます。
- Syslog 機能。認証または許可エラー、リソースの問題、およびタイムアウト イベントに関するシステム メッセージを記録します。
- レイヤ 2 traceroute。パケットが送信元デバイスから宛先デバイスへ送られる物理パスを識別します。
- Time Domain Reflector（TDR）。10/100 および 10/100/1000 の銅線イーサネット ポートでケーブル接続の問題を診断し、解決します。
- SFP モジュール診断管理インターフェイス。SFP モジュールの物理または動作ステータスをモニタします。
- 温度、電源状態、イーサネット ポートのステータスに関するアラームの処理機能が備わっています。
- 外部のリレー システムに使用できるアラーム リレー接点が備わっています。
- Digital Optical Monitoring（DOM; デジタル オプティカル モニタリング）。X2 SFP モジュールのステータスを確認します。

スイッチ初期設定後のデフォルト値

スイッチはプラグアンドプレイ動作に対応しているため、必要なのはスイッチに基本的な IP 情報を割り当て、ネットワーク内の他のデバイスに接続することだけです。特定のネットワーク ニーズがある場合には、インターフェイス固有の設定値やシステム全体の設定値を変更できます。

（注）　ブラウザベースの Express Setup プログラムによる IP アドレスの割り当てについては、スタートアップ ガイドを参照してください。CLI ベースの設定プログラムによる IP アドレスの割り当てについては、ハードウェア インストレーション ガイドを参照してください。

スイッチをまったく設定しなかった場合、スイッチは次のデフォルト設定で動作します。

- デフォルト スイッチ IP アドレス、サブネット マスク、デフォルト ゲートウェイは 0.0.0.0 です。詳細については、第 4 章「スイッチ セットアップの設定」および第 25 章「DHCP の設定」を参照してください。
- ドメイン名はデフォルトで設定されていません。詳細については、第 4 章「スイッチ セットアップの設定」を参照してください。
- DHCP クライアントはイネーブル、DHCP サーバはイネーブルに設定されています（DHCP サーバとして動作するデバイスが設定されていて、イネーブルの場合にのみ）。DHCP リレー エージェントはイネーブルに設定されています（DHCP リレー エージェントとして動作するデバイスが設定されていて、イネーブルの場合にのみ）。詳細については、第 4 章「スイッチ セットアップの設定」および第 25 章「DHCP の設定」を参照してください。
- スイッチ クラスタはディセーブルに設定されています。スイッチ クラスタの詳細は、第 6 章「スイッチ クラスタの設定」および Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。
- パスワードは定義されていません。詳細については、第 7 章「スイッチ管理の実行」を参照してください。
- システム名とプロンプトは *Switch* です。詳細については、第 7 章「スイッチ管理の実行」を参照してください。
- NTP はイネーブルに設定されています。詳細については、第 7 章「スイッチ管理の実行」を参照してください。

- DNS はイネーブルに設定されています。詳細については、第 7 章「スイッチ管理の実行」を参照してください。
- TACACS+ はディセーブルに設定されています。詳細については、第 12 章「スイッチ ベース認証の設定」を参照してください。
- RADIUS はディセーブルに設定されています。詳細については、第 12 章「スイッチ ベース認証の設定」を参照してください。
- 標準の HTTP サーバおよび SSL HTTPS サーバは両方ともイネーブルに設定されています。詳細については、第 12 章「スイッチ ベース認証の設定」を参照してください。
- IEEE 802.1x はディセーブルに設定されています。詳細については、第 13 章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- ポート パラメータ
  - 動作モードはレイヤ 2（スイッチポート）です。詳細については、第 15 章「インターフェイス特性の設定」を参照してください。
  - インターフェイス速度およびデュプレックス モードが自動ネゴシエーションに設定されています。詳細については、第 15 章「インターフェイス特性の設定」を参照してください。
  - Auto MDIX は、イネーブルです。詳細については、第 15 章「インターフェイス特性の設定」を参照してください。
  - フロー制御はディセーブルに設定されています。詳細については、第 15 章「インターフェイス特性の設定」を参照してください。
- VLAN
  - デフォルト VLAN は VLAN 1 です。詳細については、第 17 章「VLAN の設定」を参照してください。
  - VLAN トランキング設定は dynamic auto（DTP）です。詳細については、第 17 章「VLAN の設定」を参照してください。
  - トランク カプセル化はネゴシエーションです。詳細については、第 17 章「VLAN の設定」を参照してください。
  - VTP モードはサーバです。詳細については、第 18 章「VTP の設定」を参照してください。
  - VTP バージョンはバージョン 1 です。詳細については、第 18 章「VTP の設定」を参照してください。
  - 音声 VLAN はディセーブルに設定されています。詳細については、第 19 章「音声 VLAN の設定」を参照してください。
- STP、PVST+ は VLAN 1 でイネーブルに設定されています。詳細については、第 20 章「STP の設定」を参照してください。
- MSTP はディセーブルに設定されています。詳細については、第 21 章「MSTP の設定」を参照してください。
- オプションのスパニングツリー機能はディセーブルに設定されています。詳細については、第 22 章「オプションのスパニングツリー機能の設定」を参照してください。
- FlexLink は設定されていません。詳細については、第 24 章「FlexLink および MAC アドレステーブル移動更新の設定」を参照してください。
- DHCP スヌーピングは、ディセーブルです。DHCP スヌーピング情報オプションはイネーブルに設定されています。詳細については、第 25 章「DHCP の設定」を参照してください。
- IP 送信元ガードはディセーブルです。詳細については、第 25 章「DHCP の設定」を参照してください。

- DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。詳細については、第 25 章「DHCP の設定」を参照してください。
- すべての VLAN 上でダイナミック ARP インスペクションがディセーブルになっています。詳細については、第 26 章「ダイナミック ARP インスペクションの設定」を参照してください。
- IGMP スヌーピングはイネーブルです。IGMP のフィルタは適用されていません。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スロットリング設定は拒否されます。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スヌーピング クエリア機能はディセーブルに設定されています。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- MVR はディセーブルに設定されています。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- ポートベース トラフィック
  - ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルに設定されています。詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。
  - 保護ポートは定義されていません。詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。
  - ユニキャストおよびマルチキャスト トラフィック フラッディングはブロックされていません。詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。
  - セキュア ポートは設定されていません。詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。
- CDP はイネーブルに設定されています。詳細については、第 32 章「CDP の設定」を参照してください。
- UDLD はディセーブルです。詳細については、第 33 章「UDLD の設定」を参照してください。
- SPAN および RSPAN はディセーブルに設定されています。詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。
- RMON はディセーブルに設定されています。詳細については、第 34 章「RMON の設定」を参照してください。
- Syslog メッセージはイネーブルに設定され、コンソール上に表示されます。詳細については、第 35 章「システム メッセージ ロギングの設定」を参照してください。
- SNMP はイネーブルに設定されています（バージョン 1）。詳細については、第 36 章「SNMP の設定」を参照してください。
- ACL は設定されていません。詳細については、第 37 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- QoS はディセーブルです。詳細については、第 38 章「標準 QoS の設定」を参照してください。
- EtherChannel は設定されていません。詳細については、第 40 章「EtherChannel の設定」を参照してください。
- IP ユニキャスト ルーティングはディセーブルに設定されています。詳細については、第 41 章「スタティック IP ユニキャスト ルーティングの設定」を参照してください。

（注）

ネットワークの構成例

ここでは、ネットワーク構成の概要について説明します。スイッチを使用して専用ネットワーク セグメントを作成してファスト イーサネットおよびギガビット イーサネット接続でセグメントを相互接続する例も示します。

スイッチを使用する場合の設計概念

ネットワーク帯域幅をめぐってネットワーク ユーザが競合すると、データの送受信に要する時間が長くなります。ネットワークを設計する時点で、ネットワーク ユーザが必要とする帯域幅を考慮するとともに、ユーザが使用する各種ネットワーク アプリケーションの相対的な優先順位について検討する必要があります。

表 1-1 に、ネットワーク パフォーマンスが低下する原因を説明するとともに、ネットワーク ユーザが使用できる帯域幅を増加させるための、ネットワークの設計方法を示します。

表 1-1　ネットワーク パフォーマンスの向上

ネットワークに対する需要	推奨する設計方式
1 つのネットワーク セグメントに多くのユーザが集中しすぎ、インターネットへアクセスするユーザが増加している	• 帯域幅を共有するユーザ数が少なくなるように、より小さいネットワーク セグメントを作成します。さらに VLAN および IP サブネットを使用して、ネットワーク リソースに頻繁にアクセスするユーザと同じ論理ネットワーク上に、そのリソースを配置します。 • スイッチと接続先ワークステーションとの間で、全二重通信を使用します。
• 新しい PC、ワークステーション、およびサーバのパワーの増大 • ネットワーク アプリケーション（大容量の添付ファイル付き電子メールなど）および帯域幅を多用するアプリケーション（マルチメディアなど）による帯域幅需要の増大	• ネットワーク ユーザが等しくアクセスする必要があるサーバ、ルータなどのグローバル リソースを高速スイッチ ポートに直接接続し、各ユーザに専用の高速セグメントを与えます。 • スイッチと接続先サーバおよびルータ間で EtherChannel 機能を使用します。

ネットワーク設計では、帯域幅が唯一の考慮事項というわけではありません。ネットワーク トラフィックのプロファイルが発展するにしたがって、音声とデータの統合、マルチメディアの統合、アプリケーションのプライオリティ処理、およびセキュリティに対応するアプリケーションをサポートできるようなネットワーク サービスの提供を検討してください。表 1-2 で、ネットワークに対する需要について説明し、その需要を満たす方法を示します。

表 1-2　ネットワーク サービスの提供

ネットワークに対する需要	推奨する設計方式
マルチメディア アプリケーションにおける帯域幅の効率的な利用およびミッション クリティカルなアプリケーションに対する帯域幅保証	• IGMP スヌーピングを利用して、マルチメディアおよびマルチキャスト トラフィックを効率的に転送します。 • パケット分類、マーキング、スケジューリング、輻輳回避など、他の QoS メカニズムを使用し、適切なプライオリティ レベルを指定してトラフィックを分類し、最大限の柔軟性を得ながら、ミッション クリティカルなユニキャスト、マルチキャスト、およびマルチメディア アプリケーションをサポートできるようにします。 • MVR を使用して、マルチキャスト VLAN 上でマルチキャスト ストリームを継続的に送信し、なおかつ帯域幅およびセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。
*常時オン*のミッション クリティカルなアプリケーションを実現するための、ネットワークの冗長性およびアベイラビリティに対する大きな需要	• VLAN トランク、および BackboneFast を使用して、アップリンク ポート上でトラフィックのロード バランシングを実行し、VLAN トラフィックの転送時にポート コストが低いアップリンク ポートが選択されるようにします。
IP テレフォニーに対する新しい需要	• QoS を使用して、輻輳の発生時に IP テレフォニーなどのアプリケーションを優先順位付けし、ネットワーク内で発生する遅延およびジッターを制御できるようにします。 • 1 ポートあたり少なくとも 2 つのキューをサポートするスイッチを使用して、音声およびデータ トラフィックのプライオリティを IEEE 802.1p/Q に基づくハイ プライオリティまたはロー プライオリティのいずれかに設定します。スイッチは、1 ポートあたり少なくとも 4 つのキューをサポートします。 • Voice VLAN ID（VVID）を使用して、音声トラフィックに別個の VLAN を用意します。

Ethernet-to-the-Factory アーキテクチャ

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

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

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

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

http://www.cisco.com/web/strategy/manufacturing/ettf_overview.html

企業ゾーン

*企業ゾーン*は、一元管理されている IT システムと機能で構成されます。企業リソース管理サービス、企業間（B2B）サービス、企業/顧客間（B2C）サービスなどの企業ネットワーク サービスへの有線およびワイヤレス アクセスが可能です。サイト ビジネス プランニングやロジスティクスなどの基本的な

ビジネス管理作業はここで実行され、標準の IT サービスに依存します。ゲスト アクセス システムは多くの場合ここに置かれますが、企業レベルでは実現しにくい柔軟性を得るために、より下位レベルのフレームワークに置かれることも珍しくありません。

非武装ゾーン

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

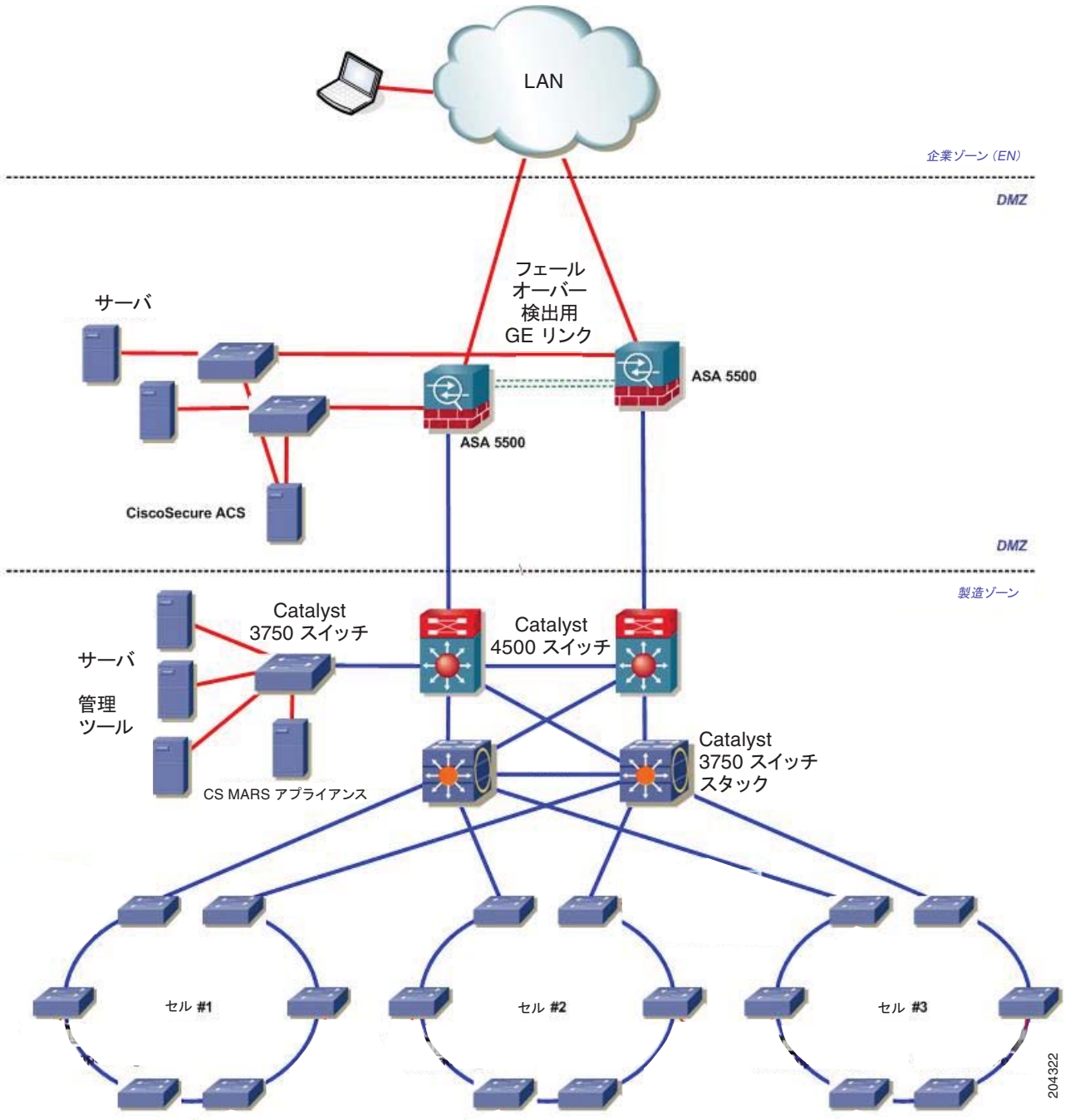
製造ゾーン

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

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

図 1-1 に、EttF アーキテクチャを示します。

図 1-1　Ethernet-to-the-Factory アーキテクチャ



トポロジのオプション

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

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

接続に関する主な考慮事項は次のとおりです。

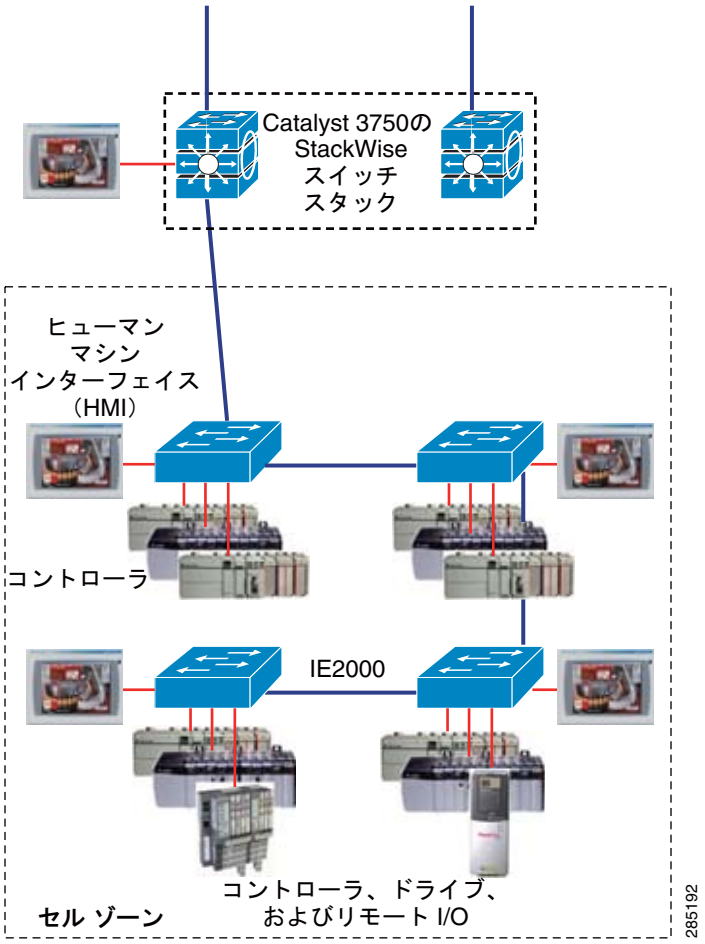
- 装置は、単一のネットワーク接続または IP 対応の I/O ブロックやリンク装置（イーサネットがサポートされていない場合）を通じてスイッチに接続されます。大半の装置にはフェールオーバー機能がないか、あっても機能が制限されているため、冗長構成のネットワーク接続を効果的に利用できません。
- 冗長構成の接続は、基幹インフラストラクチャに該当するプロセス関連の産業など、特定の産業やアプリケーションで利用されます。

セル ネットワーク：トランク廃棄トポロジ

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

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

図 1-2　セル ネットワーク：トランク廃棄トポロジ

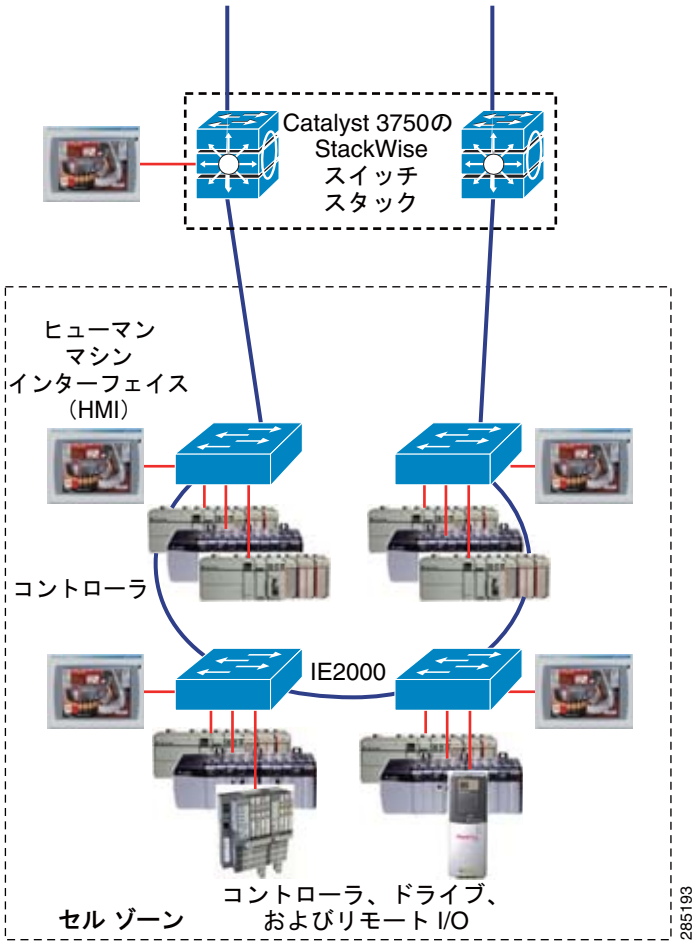


セル ネットワーク：リング トポロジ

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

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

図 1-3　セル ネットワーク：リング トポロジ

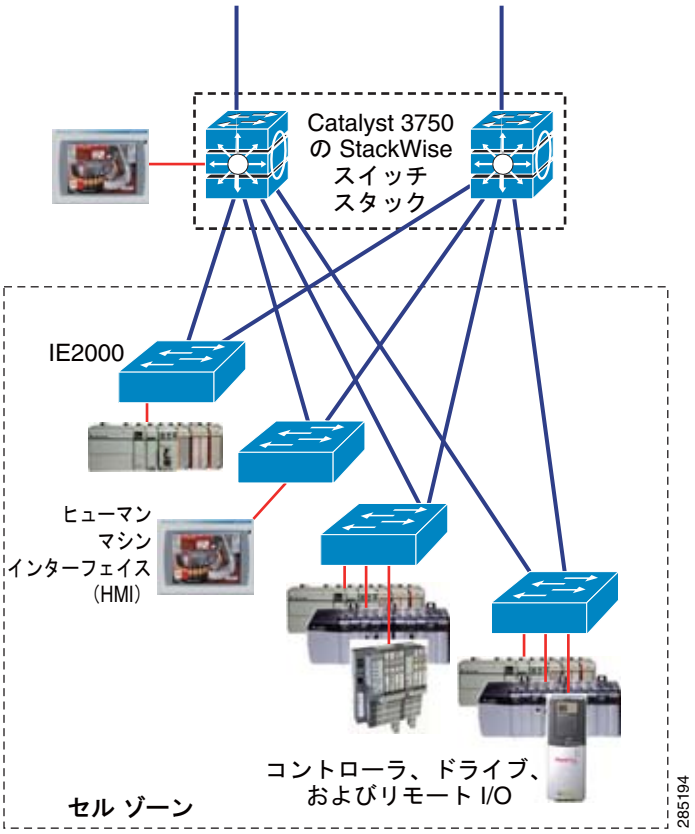


セル ネットワーク：冗長構成のスター トポロジ

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

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

図 1-4　セル ネットワーク：冗長構成のスター トポロジ



次の作業

スイッチを設定する前に、スタートアップ情報について次の各章を参照してください。

- 第 2 章「コマンドライン インターフェイスの使用」
- 第 4 章「スイッチ セットアップの設定」

特定のシスコ製品およびリリースに対する MIB の検索とダウンロードには、Cisco MIB Locator を使用します。
http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

CHAPTER 2

コマンドライン インターフェイスの使用

コマンドライン インターフェイスの使用に関する情報

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

コマンド モード

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。使用できるコマンドの種類は、現在のモードによって異なります。システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。

スイッチとのセッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーション ステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。スイッチの再起動時には、ユーザ EXEC コマンドは保存されません。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、パスワードが必要です。このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバル コンフィギュレーション モードを開始することもできます。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。コンフィギュレーションを保存するとこれらのコマンドは保存され、スイッチの再起動時に使用されます。各種のコンフィギュレーション モードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードに移行できます。

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

表 2-1　コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとのセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Switch(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードを使用して、スイッチ全体に適用されるパラメータを設定します。
config-vlan	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、VLAN（仮想 LAN）パラメータを設定します。VTP モードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成してスイッチのスタートアップ コンフィギュレーション ファイルに設定を保存できます。
VLAN コンフィギュレーション	特権 EXEC モードで、**vlan database** コマンドを入力します。	`Switch(vlan)#`	終了して特権 EXEC モードに戻るには、**exit** を入力します。	このモードを使用して、VLAN データベースに VLAN 1 ～ 1005 の VLAN パラメータを設定します。

表 2-1　コマンド モードの概要 （続き）

モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	`Switch(config-if)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、イーサネット ポートのパラメータを設定します。 インターフェイスの定義については、「インターフェイス コンフィギュレーション モードの使用方法」（P.15-5）を参照してください。 同じパラメータを指定して複数のインターフェイスを設定する場合は、「インターフェイス範囲の設定」（P.15-12）を参照してください。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**linevty** または **line console** コマンドを使用して回線を指定します。	`Switch(config-line)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、端末回線のパラメータを設定します。

コマンド モードの詳細については、このリリースに対応するコマンド リファレンス ガイドを参照してください。

ヘルプ システム

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

表 2-2　ヘルプの概要

コマンド	目的
help	任意のコマンド モードで、ヘルプ システムの概要を表示します。

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

コマンドの先頭部分<Tab>	途中まで入力したコマンド名を完全なコマンドにします。
	次に例を示します。
	`Switch# sh conf<tab>`
	`Switch# show configuration`

表 2-2　ヘルプの概要 （続き）

コマンド	目的
?	特定のコマンド モードで使用できるすべてのコマンドの一覧を表示します。 次に例を示します。 `Switch> ?`
*コマンド***?**	コマンドのキーワードの一覧を表示します。 次に例を示します。 `Switch> show ?`

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

コマンドの省略形

コマンドの先頭から、スイッチが特定のコマンドとして認識できる文字数だけを入力し、後は省略できます。

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

```
Switch# show conf
```

コマンドの no 形式および default 形式

大部分のコンフィギュレーション コマンドに、**no** 形式があります。**no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのシャットダウンが取り消されます。**no** キーワードなしでコマンドを使用すると、ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージ

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

表 2-3　CLI の代表的なエラー メッセージ

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

コンフィギュレーション ロギング

スイッチの設定変更を記録して表示させることができます。Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザ ベースごとに変更内容をトラッキングできます。ログに記録されるのは、適用された各コンフィギュレーション コマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターン コードです。この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。Syslog へこの通知を送信することも選択できます。

（注） CLI または HTTP の変更のみがログとして記録されます。

CLI を使用して機能を設定する方法

コマンド履歴の設定

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。コマンド履歴機能は、アクセス コントロール リストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。ユーザのニーズに合わせてこの機能をカスタマイズできます。

- 「コマンド履歴バッファ サイズの変更」（P.2-6）（任意）
- 「コマンドの呼び出し」（P.2-6）（任意）
- 「コマンド履歴機能のディセーブル化」（P.2-7）（任意）

コマンド履歴バッファ サイズの変更

デフォルトでは、10 のコマンドラインが履歴バッファに保存されます。現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。これらの手順は任意です。

現在の端末セッションで保存されるコマンドライン数を変更するには、特権 EXEC モードで次のコマンドを入力します。

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

指定できる範囲は 0 ～ 256 です。

特定の回線に関するすべてのセッションで保存されるコマンドライン数を設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

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

指定できる範囲は 0 ～ 256 です。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、表 2-4 のいずれかの操作を行います。これらの操作は任意です。

表 2-4　コマンドの呼び出し

アクション[1]	結果
Ctrl+P キーまたは↑キーを押します。	履歴バッファに保存されているコマンドを、最新のコマンドから順に呼び出します。キーを押すたびに、より古いコマンドが順次表示されます。
Ctrl+N キーまたは↓キーを押します。	Ctrl+P キーまたは↑キーを使用してコマンドを呼び出した後、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
show history	特権 EXEC モードで、直前に入力したいくつかのコマンドを表示します。表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定値によって指定されます。

1. 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルになっています。現在の端末セッションまたはコマンドラインでディセーブルにできます。これらの手順は任意です。

現在の端末セッションでこの機能をディセーブルにするには、**terminal no history** 特権 EXEC コマンドを使用します。

回線に関するセッションでコマンド履歴をディセーブルにするには、**no history** ライン コンフィギュレーション コマンドを使用します。

編集機能の使用方法

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

- 「編集機能のイネーブル化およびディセーブル化」（P.2-7）（任意）
- 「キー入力によるコマンドの編集」（P.2-7）（任意）
- 「画面幅よりも長いコマンドラインの編集」（P.2-9）（任意）

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的にイネーブルになりますが、ディセーブルにする、再びイネーブルにする、または特定の回線で拡張編集機能を使用できるように設定できます。これらの手順は任意です。

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

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

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

```
Switch# terminal editing
```

特定の回線について拡張編集モードを再び設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

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

キー入力によるコマンドの編集

表 2-5 に、コマンドラインの編集に必要なキーストロークを示します。これらのキーストロークは任意です。

表 2-5　キーストロークによるコマンドの編集

機能	キーストローク[1]	目的
コマンドライン上を移動して、変更または訂正を行います。	Ctrl+B キーまたは←キーを押します。	カーソルを 1 文字分だけ後ろに戻します。

表 2-5　キーストロークによるコマンドの編集 （続き）

機能	キーストローク[1]	目的
	Ctrl+F キーまたは→キーを押します。	カーソルを 1 文字分だけ前に進めます。
	Ctrl+A を押します。	カーソルをコマンドラインの先頭に移動させます。
	Ctrl+E を押します。	カーソルをコマンドラインの末尾に移動させます。
	Esc+B を押します。	カーソルを 1 ワード分だけ後ろに戻します。
	Esc+F を押します。	カーソルを 1 ワード分だけ前に進めます。
	Ctrl+T を押します。	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
バッファからコマンドを呼び出し、コマンドラインにペーストします。最後に削除した 10 項目がバッファに保存されています。	Ctrl+Y を押します。	バッファから最新のエントリを呼び出します。
	Esc+Y を押します。	バッファから次のエントリを呼び出します。 バッファには、最後に削除またはカットした 10 項目しか保存されません。Esc+Y を 11 回以上押すと、最初のバッファ エントリに戻って表示されます。
不要なエントリを削除します。	Delete キーまたは Backspace キーを押します。	カーソルの左にある文字を消去します。
	Ctrl+D を押します。	カーソル位置にある文字を削除します。
	Ctrl+K を押します。	カーソル位置からコマンドラインの末尾までの全文字を削除します。
	Ctrl+U または Ctrl+X を押します。	カーソル位置からコマンドラインの先頭までの全文字を削除します。
	Ctrl+W を押します。	カーソルの左にあるワードを消去します。
	Esc+D を押します。	カーソル位置からワードの末尾までを削除します。
ワードを大文字または小文字にします。または、一連の文字をすべて大文字にします。	Esc+C を押します。	カーソル位置のワードを大文字にします。
	Esc+L を押します。	カーソル位置のワードを小文字に変更します。
	Esc+U を押します。	カーソル位置からワードの末尾までの文字を大文字にします。
特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。	Ctrl+V または Esc+Q キーを押します。	

表 2-5　キーストロークによるコマンドの編集 （続き）

機能	キーストローク[1]	目的
1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注）　**show** コマンドの出力など、端末画面に一度に表示できない長い出力では、More プロンプトが使用されます。More プロンプトが表示された場合は、Return キーおよび Space キーを使用してスクロールできます。	Return キーを押します。	1 行下へスクロールします。
	Space キーを押します。	1 画面下へスクロールします。
スイッチから画面にメッセージが突然送られた場合に、現在のコマンドラインを再表示します。	Ctrl+L キーまたは Ctrl+R キーを押します。	現在のコマンドラインを再表示します。

1.　矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

画面幅よりも長いコマンドラインの編集

画面上で 1 行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは 10 文字分だけ左へシフトされます。コマンドラインの先頭から 10 文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、Ctrl+B キーまたは←キーを繰り返し押します。コマンドラインの先頭に直接移動するには、Ctrl+A を押します。

矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次の例では、**access-list** グローバル コンフィギュレーション コマンド エントリが 1 行分よりも長くなっています。最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。ドル記号（$）は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び 10 文字分だけ左へシフトされます。

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

コマンドの入力が終わった後、Ctrl+A を押して全体の構文をチェックし、その後 Return キーを押してコマンドを実行してください。行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。

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

ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。

ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンド エントリを呼び出して変更できます。前に入力したコマンド エントリの呼び出し方法については、「キー入力によるコマンドの編集」（P.2-7）を参照してください。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。これらのコマンドの使用は任意です。

この機能を使用するには、**show** または **more** コマンドを入力した後、パイプ記号（|）、**begin**、**include**、または **exclude** のいずれかのキーワード、および文字列（検索またはフィルタの条件）を指定します。

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

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

次に、**protocol** が使用されている行だけを出力するように指定する例を示します。

```
Switch# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
```

CLI のアクセス

CLI にはコンソール接続、Telnet、またはブラウザを使用することによってアクセスできます。

コンソール接続または Telnet による CLI アクセス

CLI にアクセスするには、スイッチのスタートアップ ガイドに記載されている手順で、スイッチのコンソール ポートに端末または PC を接続し、スイッチの電源をオンにする必要があります。また、起動プロセスおよび IP 情報を指定する場合に使用できるオプションについて理解するため、第 4 章「スイッチ セットアップの設定」を参照してください。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。詳細については、「端末回線に対する Telnet パスワードの設定」（P.12-29）を参照してください。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチのコンソール ポートに、管理ステーションまたはダイヤルアップ モデムを接続します。コンソール ポートへの接続の詳細については、*スイッチのハードウェア インストレーション ガイド*を参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化セキュア シェル（SSH）パッケージを使用します。スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブル シークレット パスワードを設定しておくことも必要です。

  Telnet アクセスのためのスイッチ設定については、「端末回線に対する Telnet パスワードの設定」（P.12-29）を参照してください。スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

  SSH のためのスイッチ設定については、「SSH サーバの設定」（P.12-41）を参照してください。スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

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

CHAPTER 3

スイッチ アラームの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

スイッチ アラームに関する情報

スイッチ ソフトウェアは、ポート単位またはスイッチ単位でスイッチの状態をモニタします。スイッチまたはポートの現在の状態と設定されているパラメータとが一致しない場合、スイッチ ソフトウェアはアラームを発生させるかシステム メッセージを表示します。デフォルトでは、スイッチ ソフトウェアは、システム メッセージ ロギング ファシリティ（*syslog* ファシリティ）にシステム メッセージを送信します。また、簡易ネットワーク管理プロトコル（SNMP）トラップを SNMP サーバに送信するようにスイッチを設定することもできます。アラーム リレーを使用すると、外部のアラーム デバイスをトリガーするようにスイッチを設定できます。

グローバル ステータス モニタリング アラーム

スイッチは、グローバル アラームまたはファシリティ アラームと呼ばれる、温度と電源装置の状態に関連するアラームを処理します。

表 3-1　グローバル ステータス モニタリング アラーム

アラーム	説明
電源装置アラーム	デフォルトでは、スイッチは 1 つの電源装置をモニタします。デュアル電源装置を設定した場合、1 台の電源装置が故障した場合にアラームがトリガーされます。電源装置アラームをハードウェア リレーに接続するように設定できます。詳細については、「電源装置アラームの設定」（P.3-6）を参照してください。
温度アラーム	スイッチには、プライマリおよびセカンダリ温度設定のある 1 台の温度センサーを備えています。センサーは、スイッチ内部の環境条件をモニタします。 プライマリ温度アラームおよびセカンダリ温度アラームは次のように設定します。 • プライマリ アラームは、低温時 -4 °F（–20 °C）および高温時 203 °F（95 °C）で、発生し自動的にイネーブルになります。これをディセーブルにはできません。デフォルトでは、プライマリ温度アラームはメジャー リレーに関連付けられています。 • セカンダリ アラームは、設定されている高温と低音の温度しきい値よりシステムの温度が高くなった場合もしくは低くなった場合に発生します。デフォルトでは、セカンダリ アラームはディセーブルになっています。 詳細については、「スイッチの温度アラームの設定」（P.3-6）を参照してください。
SD カード	デフォルトでアラームはディセーブルです。

FCS エラー ヒステリシスしきい値

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

実際のビット エラー レートが設定値付近を変動する場合に、FCS エラー ヒステリシスしきい値を設定することによってアラームの切り替えを防ぐことができます。ヒステリシスしきい値は、アラーム設定しきい値に対するアラーム クリアしきい値の値を比率（%）で定義します。

たとえば、FCS ビット エラー レートのアラーム値が 10^{-8} に設定されている場合、この値がアラーム設定しきい値です。アラーム クリアしきい値を $5*10^{-10}$ に設定するには、ヒステリシス、つまり値 *h* を次のように設定します。

h = アラーム クリアしきい値 / アラーム設定しきい値

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

FCS ヒステリシスしきい値は、スイッチのすべてのポートに適用されます。指定できる範囲は 1 ～ 10% です。デフォルト値は 10% です。詳細については、「FCS Bit Error Rate アラームの設定」（P.3-7）を参照してください。

ポート ステータス モニタリング アラーム

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

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

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

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

表 3-2　ポート ステータス モニタリング アラーム

AlarmList ID	アラーム	説明
1	Link Fault アラーム	ポートの物理層に問題があり、データ伝送の信頼性が低い場合、スイッチは Link Fault アラームを生成します。一般的なリンク障害は信号またはクロック消失です。リンク障害がクリアされると、Link Fault アラームも自動的にクリアされます。このアラームの重大度は、レベル 3、*エラー状態*です。
2	Port not Forwarding アラーム	ポートでパケット転送が行われていない場合、スイッチは Port not Forwarding アラームを生成します。ポートでパケット転送が開始されると、このアラームは自動的にクリアされます。このアラームの重大度は、レベル 4、*警告*です。
3	Port not Operating アラーム	起動時のセルフテスト中にポート障害が発生すると、スイッチは Port not Operating アラームを生成します。発生した Port not Operating アラームは、スイッチの再起動時にポートが動作可能である場合にだけ、クリアされます。このアラームの重大度は、レベル 3、*エラー状態*です。
4	FCS Bit Error Rate アラーム	設定されている FCS ビット エラー レートに実際のレートが近づくと、スイッチは FCS Bit Error Rate アラームを生成します。各ポートの FCS ビット エラー レートは、インターフェイス コンフィギュレーション CLI を使用して設定できます。詳細については、「FCS Bit Error Rate アラームの設定」（P.3-7）を参照してください。このアラームの重大度は、レベル 3、*エラー状態*です。

アラーム発生のオプション

スイッチでは、次のアラーム発生方法がサポートされています。

- 設定可能なリレー

スイッチは、1 つの独立したアラーム リレーを備えています。アラーム リレーは、ポート ステータスおよび SD フラッシュ カードの状態によってグローバルに発生させることができます。リレーを設定すると、外部のアラーム装置（ベル、ライト、その他の信号装置など）に障害信号を送信できます。任意のアラーム条件を、アラーム リレーに関連付けることができます。各障害には、Cisco IOS システム エラー メッセージ重大度に基づく重大度が割り当てられています。

リレーを設定する方法については、「電源装置アラームの設定」（P.3-6）を参照してください。

- SNMP トラップ

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

  snmp-server enable traps コマンドを変更すると、アラーム トラップを SNMP サーバに送信できるようになります。アラーム プロファイルを使用して、SNMP アラーム トラップを送信するための環境またはポート ステータス アラーム条件を設定できます。詳細については、「SNMP トラップの有効化」（P.3-9）を参照してください。

- Syslog メッセージ

  アラーム プロファイルを使用すると、システム メッセージを Syslog サーバに送信できます。詳細については、「電源装置アラームの設定」（P.3-6）を参照してください。

外部アラーム

このスイッチは、2 個のアラーム入力と 1 個のアラーム出力をサポートしています。アラーム入力回路は、Alarm-In（アラーム入力）リファレンス ピンに基づき、ドライ接点がオープンかクローズかを検出するように設計されています。Alarm_Out（アラーム出力）はノーマル オープン接点およびノーマル クローズ接点を持つリレーです。スイッチ ソフトウェアは、リレー コイルへの通電に使用する障害を検出するように設定されており、リレー接点の両方のステートを切り替えます。ノーマル オープン接点をクローズ、またはノーマル クローズ接点をオープンにします。

- **open** とは、接点（通常は閉接点）を介して電流が流れている通常の状態を意味します。電流の流れが停止すると、アラームが生成されます。
- **closed** とは、接点（通常は開接点）を介して電流が流れていないことを意味します。電流が流れると、アラームが生成されます。

（注）　ソフトウェアは、open または closed 設定でアラームをトリガーするように Alarm_In をプログラミングすることができます。

アラーム コネクタは、6 ピンのネジ端子です。この表では、アラーム ポートのピン割り当てを示します。

ピン番号	信号名	説明
6	Alarm_Out_NO	通常は接点を開くためのアラーム出力リレー
5	Alarm_Out_Com	共有接点のアラーム出力リレー
4	Alarm_Out-NC	通常は接点を閉じるためのアラーム出力リレー
3	Alarm_In2	アラーム入力番号 2
2	Alarm_In_Ref	アラーム入力基準
1	Alarm_In1	アラーム入力番号 1

アラーム重大度に、major、minor、または none を設定できます。重大度はアラーム メッセージに表示され、また、重大度によって、アラームがトリガーされたときの LED の色も設定されます。LED は、マイナー アラームの場合は赤、メジャー アラームの場合は赤で点滅します。設定されていない場合、デフォルトのアラームの重大度は minor になります。

アラーム コネクタ、LED、アラーム回路および配線の設置、アラーム評価とポートに関する詳細については、『*Hardware Installation Guide.*』を参照してください。

スイッチ アラームのデフォルト設定

表 3-3　スイッチ アラームのデフォルト設定

	アラーム	デフォルト設定
グローバル	電源装置アラーム	スイッチのシングル電源モードの場合にイネーブルになります。アラームはありません。 デュアル電源装置モードの場合、デフォルトのアラーム通知として、システム メッセージがコンソールに表示されます。
	プライマリ温度アラーム	スイッチ温度が最高 203 °F（95 °C）から最低 –4 °F（–20 °C）の範囲のときにイネーブルになります。 プライマリ スイッチの温度アラームはメジャー リレーに関連付けられています。
	セカンダリ温度アラーム	ディセーブル
	出力リレー モード アラーム	通常、電源をオフにします。アラーム出力がオフされるまたはオフ状態です。
ポート	Link fault アラーム	すべてのインターフェイスでディセーブル
	Port not forwarding アラーム	すべてのインターフェイスでディセーブル
	Port not operating アラーム	すべてのインターフェイスでイネーブル。
	FCS bit error rate アラーム	すべてのインターフェイスでディセーブル

スイッチ アラームの設定方法

外部アラームの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm contact** *contact-number* **description** ***string***	（任意）アラーム接点番号の説明を設定します。 • *contact-number* 値は 1 ～ 4 です。 • 説明の文字列は 80 文字までの英数字で指定し、この文字列は、生成されるすべてのシステム メッセージに表示されます。

	コマンド	目的
ステップ 3	**alarm contact** {*contact-number* | **all**} {**severity** { **major** | **minor** | **none**} | **trigger** {**closed** | **open**}}	アラーム接点番号またはすべての接点番号の、トリガーおよび重大度を設定します。 • 接点番号（1 ～ 4）を入力するか、すべての（**all**）アラームを設定することを指定します。 • **severity** には、**major**、**minor** または **none** を入力します。重大度を設定しない場合、デフォルトは **minor** となります。 • **trigger** には、**open** または **closed** を入力します。トリガーを設定しない場合、回路が **closed** のときにアラームがトリガーされます。
ステップ 4	**alarm relay-mode energized**	（任意）通電するように出力リレー モードを設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show env alarm-contact**	設定したアラーム接点を表示ます。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

電源装置アラームの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**power-supply dual**	デュアル電源装置を設定します。
ステップ 3	**alarm facility power-supply disable**	電源装置アラームをディセーブルにします。
ステップ 4	**alarm facility power-supply relay major**	電源装置アラームをリレーに関連付けます。
ステップ 5	**alarm facility power-supply notifies**	電源装置アラーム トラップを SNMP サーバに送信します。
ステップ 6	**alarm facility power-supply syslog**	電源装置アラーム トラップを Syslog サーバに送信します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show env power**	スイッチの電源の状態を表示します。
ステップ 9	**show facility-alarm status**	スイッチに生成されたすべてのアラームを表示します。
ステップ 10	**show alarm settings**	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチの温度アラームの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm facility temperature** {**primary** | **secondary**} **high** *threshold*	高温しきい値を設定します。しきい値は、–238 °F（–150 °C）～ 572 °F（300 °C）の範囲に設定します。
ステップ 3	**alarm facility temperature primary low** *threshold*	低温しきい値を設定します。しきい値は、–328 °F（–200 °C）～ 482 °F（250 °C）の範囲に設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show alarm settings**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

温度アラームのリレーへの関連付け

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

（注）　スイッチのシングル リレーは、メジャー リレーと呼ばれます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm facility temperature** {**primary** | **secondary**} **relay major**	プライマリ温度アラームまたはセカンダリ温度アラームをリレーに関連付けます。
ステップ 3	**alarm facility temperature** {**primary** | **secondary**} **notifies**	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを SNMP サーバに送信します。
ステップ 4	**alarm facility temperature** {**primary** | **secondary**} **syslog**	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを Syslog サーバに送信します。 セカンダリ温度アラームをディセーブルにするには、**no alarm facility temperature secondary** コマンドを使用します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show alarm settings**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

FCS Bit Error Rate アラームの設定

FCS エラーしきい値の設定

設定されているレートに実際のレートが近づくと、スイッチは FCS Bit Error Rate アラームを生成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**fcs-threshold** *value*	FCS エラー レートを設定します。 *value* に 6 ～ 11 の範囲の値を指定することにより、最大ビット エラー レート 10^{-6} ～ 10^{-11} を設定できます。 デフォルトの FCS ビット エラー レートは 10^{-8} です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show fcs-threshold**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

FCS エラー ヒステリシスしきい値の設定

実際のビット エラー レートが設定値付近を変動する場合に、ヒステリシスを設定することによってアラームの切り替えを防ぐことができます。FCS ヒステリシスしきい値は、スイッチのすべてのポートに適用されます。

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

アラーム プロファイルの設定

アラーム プロファイルの作成

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm profile** *name*	新しいプロファイルを作成するか、既存のプロファイルを指定して、アラーム プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show alarm profile** *name*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アラーム プロファイルの変更

アラーム プロファイル コンフィギュレーション モードからアラーム プロファイルを変更できます。スペースで区切ることにより、複数のアラーム タイプを入力できます。

コマンド	目的
alarm {fcs-error | link-fault | not-forwarding | not-operating}	（任意）特定のアラームのアラーム パラメータを追加または変更します。
notifies {fcs-error | link-fault | not-forwarding | not-operating}	（任意）SNMP トラップを SNMP サーバに送信するようにアラームを設定します。
relay-major {fcs-error | link-fault | not-forwarding | not-operating}	（任意）アラーム トラップをリレーに送信するようにアラームを設定します。
syslog {fcs-error | link-fault | not-forwarding | not-operating}	（任意）アラーム トラップを Syslog サーバに送信するようにアラームを設定します。

特定のポートへのアラーム プロファイルの割り当て

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

SNMP トラップの有効化

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

スイッチ アラームのモニタリングおよびメンテナンス

表 3-4　グローバルおよびポートのアラーム ステータスを表示するコマンド

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

スイッチ アラームの設定例

外部アラームの設定：例

次に、*door sensor* という名前のアラーム入力 1 を、ドアの回路が閉じたときにメジャー アラームをアサートするように設定し、次に、すべてのアラームのステータスおよび設定を表示する例を示します。

```
Switch(config)# alarm contact 1 description door sensor
Switch(config)# alarm contact 1 severity major
Switch(config)# alarm contact 1 trigger closed
Switch(config)# end
Switch(config)# show env alarm-contact
Switch# show env alarm-contact

ALARM CONTACT 1
   Status:      not asserted
   Description: door sensor
   Severity:    major
   Trigger:     closed
ALARM CONTACT 2
   Status:      not asserted
   Description: external alarm contact 2
   Severity:    minor
   Trigger:     closed
```

温度アラームのリレーへの関連付け：例

次に、高温しきい値を 45 °C にして、セカンダリ温度アラームをメジャー リレーに設定する例を示します。このアラームに関連付けられたすべてのアラームとトラップは、Syslog サーバと SNMP サーバに送信されます。

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

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

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

アラーム プロファイルの作成または変更：例

次の例では、リンク ダウン（*alarmList* ID 3）アラームがイネーブルになっているファスト イーサネット ポートのアラーム プロファイル *fastE* を作成または変更します。リンク ダウン アラームはメジャー リレーに接続されています。また、このアラームは、SNMP サーバに通知を、Syslog サーバにシステム メッセージを送信します。

```
Switch(config)# alarm profile fastE
Switch(config-alarm-profile)# alarm fcs-error
Switch(config-alarm-profile)# relay major link-fault
Switch(config-alarm-profile)# notifies not-forwarding
Switch(config-alarm-profile)# syslog not-forwarding
```

FCS エラー ヒステリシスしきい値の設定：例

次の例では、ポートの FCS ビット エラー レートを 10^{-10} に設定する方法を示します。

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

デュアル電源装置の設定：例

次に、2 台の電源装置を設定する例を示します。

```
Switch# configure terminal
Switch(config)# power-supply dual
```

次に、2 台の電源装置がない結果、アラームが発生する際にどのように情報が表示されるかを示します。

```
Switch# show facility-alarm status
Source Severity Description Relay Time
Switch MAJOR 5 Redundant Pwr missing or failed NONE Mar 01
1993 00:23:52

Switch# show env power
POWER SUPPLY A is DC OK
POWER SUPPLY B is DC FAULTY <--

Switch# show hard led
SWITCH: 1
SYSTEM: GREEN
ALARM : ALT_RED_BLACK <--
```

アラーム設定の表示：例

```
Switch# show alarm settings
Alarm relay mode: De-energized
Power Supply
```

```
        Alarm                   Enabled
        Relay
        Notifies                Disabled
        Syslog                  Enabled
Temperature-Primary
        Alarm                   Enabled
        Thresholds              MAX: 95C                MIN:  -20C
        Relay                   MAJ
        Notifies                Enabled
        Syslog                  Enabled
Temperature-Secondary
        Alarm                   Disabled
        Threshold
        Relay
        Notifies                Disabled
        Syslog                  Disabled
SD-Card
        Alarm                   Disabled
        Relay
        Notifies                Disabled
        Syslog                  Enabled
Input-Alarm 1
        Alarm                   Enabled
        Relay
        Notifies                Disabled
        Syslog                  Enabled
Input-Alarm 2
        Alarm                   Enabled
        Relay
        Notifies                Disabled
        Syslog                  Enabled
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	*『Cisco IOS Configuration Fundamentals Command Reference』*
アラーム入力/出力ポート	*ハードウェア インストレーション ガイド*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 4

スイッチ セットアップの設定

スイッチ セットアップの設定の制約事項

- ネットワーク内に割り当てられた IP アドレスがなく、1 つ以上のレイヤ 3 インターフェイスが起動してない場合は、設定プロセスが保存された DHCP ベースの自動設定は停止します。
- タイムアウトを設定しない限り、設定機能を備えている DHCP ベースの自動設定は IP アドレスのダウンロードを無期限に繰り返します。
- コンフィギュレーション ファイルをダウンロードできないか破損している場合は、自動インストールプロセスが停止します。

（注） TFTP からダウンロードされたコンフィギュレーション ファイルは、実行コンフィギュレーション内の既存コンフィギュレーションとマージされますが、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを入力しない限り、NVRAM に保存されません。ダウンロードされたコンフィギュレーションがスタートアップ コンフィギュレーションに保存されると、後続のシステムシステム再起動中に、この機能が実行されないことに注意してください。

スイッチのセットアップの実行に関する情報

この章では、IP アドレスの割り当てと DHCP 自動設定を含む、スイッチの初期設定作業の実行方法について説明します。

スイッチ ブート プロセス

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

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

- 下位レベルの CPU 初期化を行います。CPU レジスタを初期化することにより、物理メモリがマッピングされる場所、容量、速度などを制御します。
- CPU サブシステムの電源投入時自己診断テスト (POST) を実行します。CPU DRAM とフラッシュ ファイル システムを構成するフラッシュ デバイスの部分をテストします。
- システム ボードのフラッシュ メモリ カード上のファイル システムを初期化します。

- デフォルトの OS（オペレーティング システム）ソフトウェアをメモリにロードし、スイッチを起動します。

ブートローダによってフラッシュ ファイル システムにアクセスしてから、オペレーティング システムをロードします。ブートローダの使用目的は通常、オペレーティング システムのロード、圧縮解除、および起動に限定されます。オペレーティング システムが CPU を制御できるようになると、ブートローダは、次にシステムがリセットされるか電源が投入されるまでは非アクティブになります。

このスイッチは、フラッシュ メモリ カードをサポートしています。フラッシュ メモリ カードを使えば、再設定を行わずに障害が発生したスイッチを新しいスイッチと交換できます。フラッシュ メモリ カードのスロットは、ホット スワップおよび前面アクセスされます。フラッシュ カードはカバーによって保護および保持されます。カバーは非脱落型ネジで蝶番が付けられ、閉じられます。これによってカードが固定され、衝撃および振動から保護されます。

フラッシュ メモリ カード ファイルの設定を表示するには、**show flash** 特権 EXEC コマンドを使用します。スイッチのフラッシュ メモリ カードの取り外しまたは交換方法については、*ハードウェア インストレーション ガイド*を参照してください。

また、オペレーティング システムが使用不可能になるほどの重大な障害が発生した場合は、ブートローダはシステムにトラップドアからアクセスします。トラップドアからシステムへアクセスして、必要があれば、フラッシュ ファイル システムをフォーマットし、XMODEM プロトコルを使用して OS のソフトウェアイメージを再インストールし、失われたパスワードを回復し、最終的に OS を再起動できます。詳細については、「ソフトウェア障害からの回復」および「パスワードを忘れた場合の回復」を参照してください。

（注） パスワードの回復をディセーブルにできます。詳細については、「「パスワード回復のディセーブル化」」を参照してください。

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

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

（注） データ ビット オプションを 8 に設定した場合、パリティ オプションは「なし」に設定します。

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

スイッチのデフォルト ブート設定

機能	デフォルト設定
オペレーティング システム ソフトウェア イメージ	スイッチは BOOT 環境変数の情報を使用して、システムを自動的に起動しようとします。この変数が設定されていない場合、スイッチはフラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出した実行可能イメージをロードして実行しようとします。 Cisco IOS イメージは、イメージ ファイルと（.bin 拡張子を除いて）同名のディレクトリに保存されます。 ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。
コンフィギュレーション ファイル	設定されているスイッチは、システムボードのフラッシュ メモリに保存されている *config.text* ファイルを使用します。 新しいスイッチの場合、コンフィギュレーション ファイルはありません。

スイッチ ブートの最適化

通常のスイッチのブート プロセスには、メモリ テスト、ファイル システム チェック（FSCK）、および電源投入時自己診断テスト（POST）が含まれます。

グローバル コンフィギュレーション モードの **boot fast** コマンドはデフォルトでスイッチのブート最適化を可能にし、このためこれらのテストをディセーブルにして起動時間を最小化します。ただし、システム障害の発生後は、この機能は自動的にディセーブルになります。

スイッチが BOOT 環境変数内の情報を使用して、自動的にシステムを起動するように設定している場合、すぐにリロード シーケンスが実行されます。他の方法では、ブートローダ コンフィギュレーション モードで手動で **boot** コマンドを入力してもリロード シーケンスが実行されます。

初回リロード

スイッチは高速起動機能をディセーブルにし、次の警告メッセージを表示します。

```
"Reloading with boot fast feature disabled"
```

システム メッセージが表示された後、システムはクラッシュ情報を保存し、自動的に次のリロード サイクルのためにリセットします。

2 回目リロード

ブートローダは通常のフル メモリ テストおよび FSCK のチェックを実施し、LED ステータスは進行状況を表示します。メモリおよび FSCK テストが成功すると、システムは追加 POST テストを実行し、その結果がコンソールに表示されます。

高速起動機能は、システムが正常に起動した後に再びイネーブルになります。

スイッチ情報の割り当て

IP 情報を割り当てるには、スイッチのセットアップ プログラムを使用する方法、Dynamic Host Configuration Protocol（DHCP）サーバを使用する方法、または手動で実行する方法があります。

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

サーバの設定後は DHCP サーバを使用して、IP 情報の集中管理と自動割り当てを行います。

（注） DHCP を使用している場合は、スイッチが動的に割り当てられた IP アドレスを受信してコンフィギュレーション ファイルを読み込むまでは、セットアップ プログラムからの質問に応答しないでください。

スイッチの設定手順を熟知している経験豊富なユーザの場合は、スイッチを手動で設定してください。それ以外のユーザは、セットアップ プログラムを使用してください。

スイッチのデフォルト設定

表 4-1　スイッチのデフォルト設定

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

DHCP ベースの自動設定の概要

DHCP は、インターネットホストおよびインターネットワーキング デバイスに設定情報を提供します。このプロトコルには、2 つのコンポーネントがあります。1 つは DHCP サーバからデバイスにコンフィギュレーション パラメータを提供するコンポーネント、もう 1 つはデバイスにネットワーク アドレスを割り当てるコンポーネントです。DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバが、動的に設定されるデバイスに対して、ネットワーク アドレスを割り当て、コンフィギュレーション パラメータを提供します。スイッチは、DHCP クライアントおよび DHCP サーバとして機能できます。

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

DHCP ベースの自動設定を使用すると、スイッチ上で DHCP クライアント側の設定を行う必要はありません。ただし、DHCP サーバで、IP アドレスに関連した各種リース オプションを設定する必要があります。DHCP を使用してネットワーク上でコンフィギュレーション ファイルをリレーする場合は、TFTP サーバおよびドメイン ネーム システム（DNS）サーバの設定が必要なこともあります。

スイッチの DHCP サーバは、スイッチと同じ LAN 上に配置することも、そのスイッチとは別の LAN 上に配置することもできます。DHCP サーバが異なる LAN 上で動作している場合、スイッチと DHCP サーバ間に、DHCP のリレー デバイスを設定する必要があります。リレー デバイスは、直接接続されている 2 つの LAN 間でブロードキャスト トラフィックを転送します。ルータはブロードキャスト パケットを転送しませんが、受信したパケットの宛先 IP アドレスに基づいてパケットを転送します。

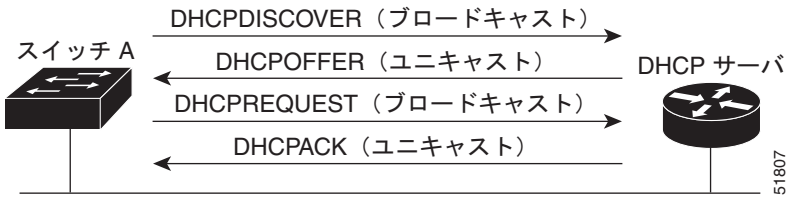
DHCP ベースの自動設定は、スイッチの BOOTP クライアント機能に代わるものです。

DHCP クライアント要求プロセス

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

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

図 4-1　　DHCP クライアント/サーバ間のメッセージ交換



クライアントであるスイッチ A は、DHCP サーバの場所を特定するために、DHCPDISCOVER メッセージをブロードキャストします。DHCP サーバは、DHCPOFFER ユニキャスト メッセージによって、使用可能なコンフィギュレーション パラメータ（IP アドレス、サブネット マスク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレス用のリースなど）をクライアントに提示します。

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

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバウンドされ、クライアントはサーバから受信した設定情報を使用します。スイッチが受信する情報量は、TFTP サーバと関連して提供される DHCP の設定方法によって異なります。詳細については、「TFTP サーバ」（P.4-8）を参照してください。

DHCPOFFER ユニキャスト メッセージによって送信されたコンフィギュレーション パラメータが無効である（コンフィギュレーション エラーがある）場合、クライアントは DHCP サーバに、DHCPDECLINE ブロードキャスト メッセージを戻します。

DHCP サーバはクライアントに、提示されたコンフィギュレーション パラメータが割り当てられていない、パラメータのネゴシエーション中にエラーが発生した、または DHCPOFFER メッセージに対するクライアントの応答が遅れているという意味の DHCPNAK 拒否ブロードキャスト メッセージを送信します （DHCP サーバはパラメータをクライアントに割り当てました）。

DHCP クライアントは、複数の DHCP サーバまたは BOOTP サーバから提示を受け取り、そのうちの任意の 1 つを受け入れることができますが、通常は最初に受け取った提示を受け入れます。DHCP サーバから提示された IP アドレスが必ずしもスイッチに割り当てられるわけではありません。ただし、サーバは通常、クライアントが正式にアドレスを要求するまではアドレスを確保しておきます。スイッチが BOOTP サーバからの応答を受け入れて、自身を設定する場合、スイッチはスイッチ コンフィギュレーション ファイルを入手するために、TFTP 要求をユニキャストするのではなくブロードキャストします。

DHCP ホスト名オプションにより、スイッチのグループはホスト名および標準コンフィギュレーションを集中管理型 DHCP サーバから取得できます。クライアント（スイッチ）は DCHPDISCOVER メッセージ内に、DHCP サーバからのホスト名および他のコンフィギュレーション パラメータの要求に使用される Option 12 フィールドを加えます。すべてのクライアントのコンフィギュレーション ファイルは、DHCP から取得したホスト名を除き、まったく同じです。

クライアントにデフォルトのホスト名がある場合（**hostname** *name* グローバル コンフィギュレーション コマンドを設定していないか、**no hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を削除していない場合）は、**ip address dhcp** インターフェイス コンフィギュレーション コマンドを入力すると、DHCP のホスト名オプションがパケットに含まれません。この場合、インターフェイスの IP アドレスを取得中にクライアントが DHCP との相互作用で DHCP ホスト名オプションを受信した場合、クライアントは DHCP ホスト名オプションを受け入れて、システムに設定済みのホスト名があることを示すフラグが設定されます。

DHCP ベースの自動設定およびイメージ アップデート

DHCP イメージ アップグレード機能を使用すると、ネットワーク内の 1 つ以上のスイッチに新しいイメージ ファイルおよび新しいコンフィギュレーション ファイルをダウンロードするように DHCP サーバを設定できます。これにより、ネットワークに加えられた新しいスイッチが、同じイメージとコンフィギュレーションを確実に受信するようになります。

DHCP イメージ アップグレードには、自動設定およびイメージ アップデートの 2 つのタイプがあります。

DHCP 自動設定

DHCP 自動設定は、コンフィギュレーション ファイルを DHCP サーバからネットワーク内の 1 つ以上のスイッチにダウンロードします。ダウンロードされたコンフィギュレーション ファイルは、スイッチの実行コンフィギュレーション ファイルになります。このファイルは、スイッチがリロードされるまで、フラッシュ メモリに保存された起動コンフィギュレーションを上書きしません。

DHCP 自動イメージ アップデート

DHCP 自動設定とともに DHCP 自動イメージ アップグレードを使用すると、コンフィギュレーション*および*新しいイメージをネットワーク内の 1 つ以上のスイッチにダウンロードできます。新しいコンフィギュレーションおよび新しいイメージをダウンロードしている 1 つ以上のスイッチは、ブランク（つまり、出荷時のデフォルト設定がロードされている状態）にできます。

コンフィギュレーションをすでに持っているスイッチに新しいコンフィギュレーションをダウンロードすると、ダウンロードされたコンフィギュレーションは、スイッチに保存されているコンフィギュレーション ファイルに追加されます （どの既存のコンフィギュレーション ファイルも、ダウンロードされたファイルに上書きされません）。

（注）　スイッチの DHCP 自動イメージ アップデートをイネーブルにするには、イメージ ファイルおよびコンフィギュレーション ファイルがある TFTP サーバを、正しいオプション 67（コンフィギュレーション ファイル名）、オプション 66（DHCP サーバ ホスト名）、オプション 150（TFTP サーバ アドレス）、およびオプション 125（ファイルの説明）の設定で設定する必要があります。

スイッチを DHCP サーバとして設定する場合の手順については、「DHCP サーバ設定時の注意事項」（P.4-7）および『*Cisco IOS IP DHCP Configuration Guide, Release 15.0*』の「IP Addressing and Services」の章にある「Configuring DHCP」を参照してください。

スイッチをネットワークに設置すると、自動イメージ アップデート機能が開始します。ダウンロードされたコンフィギュレーション ファイルはスイッチの実行コンフィギュレーションに保存され、新しいイメージがダウンロードされてスイッチにインストールされます。スイッチを再起動すると、このコンフィギュレーションがスイッチのコンフィギュレーションに保存されます。

DHCP サーバ設定時の注意事項

デバイスを DHCP サーバとして設定する場合、次の注意事項に従ってください。

- DHCP サーバには、スイッチのハードウェア アドレスによって各スイッチと結び付けられている予約済みのリースを設定します。
- スイッチに IP アドレス情報を受信させるには、DHCP サーバに次のリース オプションを設定する必要があります。
  - クライアントの IP アドレス（必須）
  - クライアントのサブネット マスク（必須）
  - ルータの IP アドレス（スイッチで使用するデフォルト ゲートウェイ アドレス）（必須）
  - DNS サーバの IP アドレス（任意）
- スイッチに TFTP サーバからコンフィギュレーション ファイルを受信させる場合は、DHCP サーバに次のリース オプションを設定する必要があります。
  - TFTP サーバ名（必須）
  - ブート ファイル名（クライアントが必要とするコンフィギュレーション ファイル名）（推奨）
  - ホスト名（任意）
- DHCP サーバの設定によっては、スイッチは IP アドレス情報またはコンフィギュレーション ファイル、あるいはその両方を受信できます。
- 前述のリース オプションを設定しなかった場合、DHCP サーバは、設定されたパラメータのみを使用してクライアントの要求に応答します。

  IP アドレスおよびサブネット マスクが応答に含まれていないと、スイッチは設定されません。ルータの IP アドレスまたは TFTP サーバ名が見つからなかった場合、スイッチは TFTP 要求をユニキャストしないでブロードキャストする場合があります。その他のリース オプションは、使用できなくても自動設定には影響しません。
- スイッチは、DHCP サーバとして機能できます。デフォルトでは、Cisco IOS DHCP サーバおよび DHCP リレー エージェント機能はスイッチ上でイネーブルにされていますが、設定されていません。これらの機能は動作しません。DHCP サーバがシスコ デバイスの場合、DHCP 設定に関する詳細については、Cisco.com で『*Cisco IOS IP Configuration Guide*』の「IP Addressing and Services」の章にある「Configuring DHCP」の部分を参照してください。

TFTP サーバ

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

コンフィギュレーション ファイル名、および TFTP サーバを指定しなかった場合、またはコンフィギュレーション ファイルをダウンロードできなかった場合は、スイッチはファイル名と TFTP サーバアドレスをさまざまに組み合わせてコンフィギュレーション ファイルをダウンロードしようとします。ファイルには、（存在する場合）特定のコンフィギュレーション ファイル名と次のファイルが指定されています。network-config、cisconet.cfg、*hostname.config*、または *hostname.cfg* です。この場合、*hostname* はスイッチの現在のホスト名です。使用される TFTP サーバアドレスには、（存在する場合）指定された TFTP サーバのアドレス、およびブロードキャスト アドレス（255.255.255.255）が含まれています。

スイッチが正常にコンフィギュレーション ファイルをダウンロードするには、TFTP サーバのベースディレクトリに 1 つまたは複数のコンフィギュレーション ファイルが含まれていなければなりません。含めることのできるファイルは、次のとおりです。

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

DHCP サーバ リース データベースに TFTP サーバ名を指定する場合は、DNS サーバのデータベースに TFTP サーバ名と IP アドレスのマッピングを設定することも必要です。

使用する TFTP サーバが、スイッチとは異なる LAN 上にある場合、またはスイッチがブロードキャスト アドレスを使用してアクセスした場合（前述のすべての必須情報が DHCP サーバの応答に含まれていない場合に発生）は、リレーを設定して TFTP サーバに TFTP パケットを転送する必要があります。詳細については、「リレー デバイス」（P.4-9）を参照してください。適切な解決方法は、必要なすべての情報を使用して DHCP サーバを設定することです。

DNS サーバ

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

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

DNS サーバは、スイッチと同じ LAN 上に配置することも、そのスイッチとは別の LAN 上に配置することもできます。DHCP サーバが別の LAN 上に存在する場合、スイッチはルータを介して DHCP サーバにアクセスできなければなりません。

リレー デバイス

異なる LAN 上にあるホストからの応答が必要なブロードキャスト パケットをスイッチが送信する場合は、リレー デバイス（*リレー エージェント*）を設定する必要があります。スイッチが送信する可能性のあるブロードキャスト パケットの例として DHCP パケット、DNS パケット、場合によっては TFTP パケットが挙げられます。リレー デバイスは、インターフェイス上の受信ブロードキャスト パケットを宛先ホストに転送するように設定する必要があります。

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

図 4-2 では、ルータ インターフェイスを次のように設定しています。

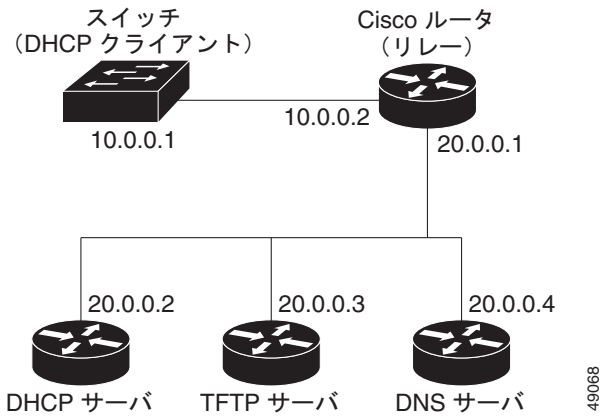
インターフェイス 10.0.0.2 の場合：

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

インターフェイス 20.0.0.1 の場合：

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

図 4-2　　自動設定でのリレー デバイスの使用



コンフィギュレーション ファイルの入手方法

IP アドレスおよびコンフィギュレーション ファイル名が DHCP で専用のリースとして取得できるかどうかに応じて、スイッチは次の方法で設定情報を入手します。

- IP アドレスおよびコンフィギュレーション ファイル名が、スイッチ用に予約され、DHCP 応答（1 ファイル読み込み方式）で提供されている場合

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

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

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

- IP アドレスだけがスイッチ用に予約され、DHCP 応答で提供されており、コンフィギュレーション ファイル名は提供されない場合（2 ファイル読み込み方式）

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

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

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

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

（注） DHCP 応答から TFTP サーバを入手できなかった場合、ユニキャスト伝送によるコンフィギュレーション ファイルの読み込みに失敗した場合、または TFTP サーバ名を IP アドレスに変換できない場合には、スイッチは TFTP サーバ要求をブロードキャストします。

環境変数の制御方法

正常に動作しているスイッチでは、9600 bps 対応に設定されたスイッチ コンソール接続でのみブートローダ モードが開始されます。スイッチの電源コードを取り外し、電源コードの再接続中に Mode ボタンを押します。ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、Mode ボタンを離します。これにより、ブートローダの *switch:* プロンプトが表示されます。

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

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保存されます。

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

環境変数には 2 種類のデータが保存されます。

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

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

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

代表的な環境変数

表 4-2 で、代表的な環境変数の機能について説明します。

表 4-2　環境変数

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BOOT	**set BOOT** *filesystem*:*/file-url ...* 自動起動時にロードして実行を試みる、セミコロンで区切られた実行可能ファイルのリスト。BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。	**boot system** *filesystem:/file-url ...* 次回の起動時に読み込む Cisco IOS イメージを指定します。このコマンドは、BOOT 環境変数の設定を変更します。
MANUAL_BOOT	**set MANUAL_BOOT yes** スイッチの起動を自動で行うか手動で行うかを決定します。 有効値は 1、yes、0、および no です。no または 0 に設定されている場合、ブートローダはシステムの自動起動を試みます。それ以外の値に設定されている場合は、ブートローダ モードから手動でスイッチを起動する必要があります。	**boot manual** 次回の起動時にスイッチを手動で起動できるようにします。MANUAL_BOOT 環境変数の設定が変更されます。 次回のシステム再起動時には、スイッチはブートローダ モードになります。システムを起動するには、**boot flash:***filesystem*:*/file-url* ブートローダ コマンドを使用し、起動可能イメージの名前を指定します。
CONFIG_FILE	**set CONFIG_FILE flash:***/file-url* Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を変更します。	**boot config-file flash:***/file-url* Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。このコマンドによって、CONFIG_FILE 環境変数が変更されます。

ソフトウェア イメージのリロードのスケジューリング

スイッチ上でソフトウェア イメージのリロードを後で（深夜、週末などスイッチをあまり使用しないときに）行うように、スケジュールを設定できます。または（ネットワーク内のすべてのスイッチでソフトウェアをアップグレードする場合など）ネットワーク全体でリロードを同時に行うことができます。

（注）　リロードのスケジュールは、約 24 日以内に設定する必要があります。

次のリロード オプションがあります。

- 指定した分数、または時間および分数が経過したときに実施するソフトウェアがリロード。リロードは、約 24 日以内に実行する必要があります。最大 255 文字で、リロードの理由を指定できます。
- （24 時間制で）指定された時刻に実施するソフトウェアのリロード。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。00:00 を指定すると、深夜 0 時のリロードが設定されます。

reload コマンドはシステムを停止させます。手動で起動することが設定されていない限り、システムは自動的に再起動します。

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

コンフィギュレーション ファイルを変更すると、リロードの前にコンフィギュレーションを保存するように指示するプロンプトが表示されます。保存操作時に、CONFIG_FILE 環境変数がすでに存在しないスタートアップ コンフィギュレーション ファイルを示していた場合、保存を続行するかどうかという問い合わせがシステムから出されます。その状況のまま続けると、リロード時にセットアップ モードが開始されます。

スケジュールがすでに設定されたリロードを取り消すには、**reload cancel** 特権 EXEC コマンドを使用します。

スイッチのセットアップの設定方法

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

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定

この作業では、新しいスイッチに TFTP および DHCP 設定の DHCP 自動設定を設定して新しいコンフィギュレーション ファイルをダウンロードする方法について説明します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp** *pool name*	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**bootfile** *filename*	ブート イメージとして使用されるコンフィギュレーション ファイルの名前を指定します。
ステップ 4	**network** *network-number mask prefix-length*	DHCP アドレス プールのサブネット ネットワーク番号およびマスクを指定します。 **（注）** プレフィックス長は、アドレス プレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワーク マスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
ステップ 5	**default-router** *address*	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。
ステップ 6	**option 150** *address*	TFTP サーバの IP アドレスを指定します。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**tftp-server flash**:*filename.text*	TFTP サーバ上のコンフィギュレーション ファイルを指定します。
ステップ 9	**interface** ***interface-id***	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ 10	**no switchport**	インターフェイスをレイヤ 3 モードにします。
ステップ 11	**ip address** *address mask*	インターフェイスの IP アドレスおよびマスクを指定します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定

この作業では、DHCP 自動設定の設定により新しいスイッチに TFTP および DHCP を設定して、新しいイメージおよび新しいコンフィギュレーション ファイルをダウンロードする方法について説明します。

はじめる前に

スイッチにアップロードされるテキスト ファイル（たとえば、autoinstall_dhcp）を作成する必要があります。このテキスト ファイル内に、ダウンロードするイメージの名前を含めます。このイメージは、bin ファイルでなく、tar ファイルである必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *name*	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**bootfile** *filename*	ブート イメージとして使用されるファイルの名前を指定します。
ステップ 4	**network** *network-number mask prefix-length*	DHCP アドレス プールのサブネット ネットワーク番号およびマスクを指定します。 （注）　プレフィックス長は、アドレス プレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワーク マスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
ステップ 5	**default-router** *address*	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。
ステップ 6	**option 150** *address*	TFTP サーバの IP アドレスを指定します。
ステップ 7	**option 125** *hex*	イメージ ファイルへのパスを記述するテキスト ファイルへのパスを指定します。
ステップ 8	**copy tftp flash** *filename.txt*	テキスト ファイルをスイッチにアップロードします。
ステップ 9	**copy tftp flash** *imagename.tar*	新しいイメージの tar ファイルをスイッチにアップロードします。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**tftp-server flash:*config.text***	TFTP サーバの Cisco IOS コンフィギュレーション ファイルを指定します。
ステップ 12	**tftp-server flash:*imagename.tar***	TFTP サーバ上のイメージ名を指定します。
ステップ 13	**tftp-server flash:*filename.txt***	ダウンロードするイメージ ファイルの名前を含んでいるテキスト ファイルを指定します。
ステップ 14	**interface *interface-id***	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ 15	**no switchport**	インターフェイスをレイヤ 3 モードにします。
ステップ 16	**ip address** *address mask*	インターフェイスの IP アドレスおよびマスクを指定します。
ステップ 17	**end**	特権 EXEC モードに戻ります。
ステップ 18	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

クライアントの設定

レイヤ 3 インターフェイスだけを設定してイネーブルにする必要があります。保存されているコンフィギュレーションの DHCP ベースの自動設定に IP アドレスを割り当てないでください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot host dhcp**	保存されているコンフィギュレーションで自動設定をイネーブルにします。

	コマンド	目的
ステップ 3	**boot host retry timeout** *timeout-value*	（任意）システムがコンフィギュレーション ファイルをダウンロードしようとする時間を設定します。 **（注）** タイムアウトを設定しないと、システムは無期限に DHCP サーバから IP アドレスを取得しようとします。
ステップ 4	**banner config-save ^C** *warning-message* **^C**	（任意）コンフィギュレーション ファイルを NVRAM に保存しようとするときに表示される警告メッセージを作成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show boot**	設定を確認します。

手動でのルーテッド ポートの IP 情報の割り当て

この作業は、手動でレイヤ 3 ルーテッド ポートに IP 情報を割り当てる方法について説明します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport**	インターフェイスをレイヤ 3 モード に設定します。
ステップ 4	**ip address** *address mask*	インターフェイスの IP アドレスおよびマスクを指定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip default-gateway** *ip-address*	スイッチに直接接続しているネクスト ホップのルータ インターフェイスの IP アドレスを入力します。このスイッチにはデフォルト ゲートウェイが設定されています。デフォルト ゲートウェイは、スイッチから宛先 IP アドレスを取得していない IP パケットを受信します。 デフォルト ゲートウェイが設定されると、スイッチは、ホストが接続する必要のあるリモート ネットワークに接続できます。 **（注）** IP でルーティングするようにスイッチを設定した場合、デフォルト ゲートウェイの設定は不要です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip redirects**	設定されたデフォルト ゲートウェイを確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

手動での SVI への IP 情報の割り当て

この作業は、手動で複数のスイッチ仮想インタフェース（SVI）に IP 情報を割り当てる方法について説明します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id*	インターフェイス コンフィギュレーション モードを開始して、IP 情報が割り当てられている VLAN を指定します。指定できる VLAN 範囲は 1 ～ 4096 です。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスとサブネット マスクを入力します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip default-gateway** *ip-address*	スイッチに直接接続しているネクスト ホップのルータ インターフェイスの IP アドレスを入力します。このスイッチにはデフォルト ゲートウェイが設定されています。デフォルト ゲートウェイは、スイッチから宛先 IP アドレスを取得していない IP パケットを受信します。 デフォルト ゲートウェイが設定されると、スイッチは、ホストが接続する必要のあるリモート ネットワークに接続できます。 **（注）** IP でルーティングするようにスイッチを設定した場合、デフォルト ゲートウェイの設定は不要です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces vlan** *vlan-id*	設定された IP アドレスを確認します。
ステップ 8	**show ip redirects**	設定されたデフォルト ゲートウェイを確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スタートアップ コンフィギュレーションの変更

システム コンフィギュレーションを読み書きするためのファイル名の指定

Cisco IOS ソフトウェアは、デフォルトで *config.text* ファイルを使用して、システム コンフィギュレーションの不揮発性コピーを読み書きします。別のファイル名を指定することもできます。次回の起動時には、その名前のファイルが読み込まれます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot config-file flash:**/*file-url*	次回の起動時に読み込むコンフィギュレーション ファイルを指定します。 *file-url* に、パス（ディレクトリ）およびコンフィギュレーション ファイル名を指定します。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show boot**	入力を確認します。 **boot config-file** グローバル コンフィギュレーション コマンドによって、CONFIG_FILE 環境変数の設定が変更されます。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

手動でのスイッチ起動

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

はじめる前に

この作業では、スタンドアロン スイッチを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot manual**	次回の起動時に、スイッチを手動で起動できるようにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show boot**	入力を確認します。 **boot manual** グローバル コンフィギュレーション コマンドによって、MANUAL_BOOT 環境変数の設定が変更されます。 次回、システムを再起動したときには、スイッチはブートローダ モードになり、ブートローダ モードであることが switch: プロンプトによって示されます。システムを起動するには、**boot** *filesystem***:**/*file-url* ブートローダ コマンドを使用します。 • *filesystem***:** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。 • *file-url* には、パス（ディレクトリ）および起動可能なイメージの名前を指定します。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定のソフトウェア イメージを起動する場合

スイッチはデフォルトで、BOOT 環境変数の情報を使用して、システムを自動的に起動しようとします。この変数が設定されていない場合、スイッチは、フラッシュ ファイル システム全体に再帰的に縦型検索し、最初の実行可能イメージをロードして実行しようとします。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。起動する具体的なイメージを指定することもできます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot system** *filesystem***:**/*file-url*	次回の起動時に、フラッシュ メモリ内の特定のイメージを起動するようにスイッチを設定します。 • *filesystem***:** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。 • *file-url* には、パス（ディレクトリ）および起動可能なイメージの名前を指定します。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show boot**	入力を確認します。 **boot system** グローバル コンフィギュレーション コマンドによって、BOOT 環境変数の設定が変更されます。 次回の起動時に、スイッチは BOOT 環境変数の情報を使用して、システムを自動的に起動しようとします。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ セットアップの設定のモニタリング

スイッチ実行コンフィギュレーションの確認

次の特権 EXEC コマンドを使用すると、入力した設定や変更を確認できます。

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

Current configuration: 1363 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch A
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
.
<output truncated>
.
```

```
interface gigabitethernet1/1
no switchport
ip address 172.20.137.50 255.255.255.0
!
interface gigabitethernet1/2
mvr type source

<output truncated>

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

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

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

このコマンドにより、入力した設定値が保存されます。保存できなかった場合、設定は次のシステム リロード時に失われます。フラッシュ メモリの NVRAM（不揮発性 RAM）セクションに保存されている情報を表示するには、**show startup-config** または **more startup-config** 特権 EXEC コマンドを使用します。

コンフィギュレーション ファイルの他のコピー元については、付録 A「Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作」を参照してください。

スイッチのセットアップの設定例

DHCP ベースの自動設定を使用して IP 情報を取得：例

スイッチ A はコンフィギュレーション ファイルを次のようにして読み込みます。

- DHCP サーバから IP アドレス 10.0.0.21 を入手します。
- DHCP サーバの応答でコンフィギュレーション ファイル名が提供されない場合、スイッチ A は TFTP サーバのベース ディレクトリから network-confg ファイルを読み込みます。
- ホスト テーブルに network-confg ファイルの内容を追加します。
- IP アドレス 10.0.0.21 をもとにホスト テーブルを検索し、ホスト名（switcha）を取得します。
- ホスト名に対応するコンフィギュレーション ファイルを読み込みます。たとえば、TFTP サーバから *switch1-confg* を読み込みます。

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

図 4-3 に、DHCP ベースの自動設定を使用して IP 情報を検索するネットワークの構成例を示します。

図 4-3　DHCP ベースの自動設定を使用するネットワークの構成例

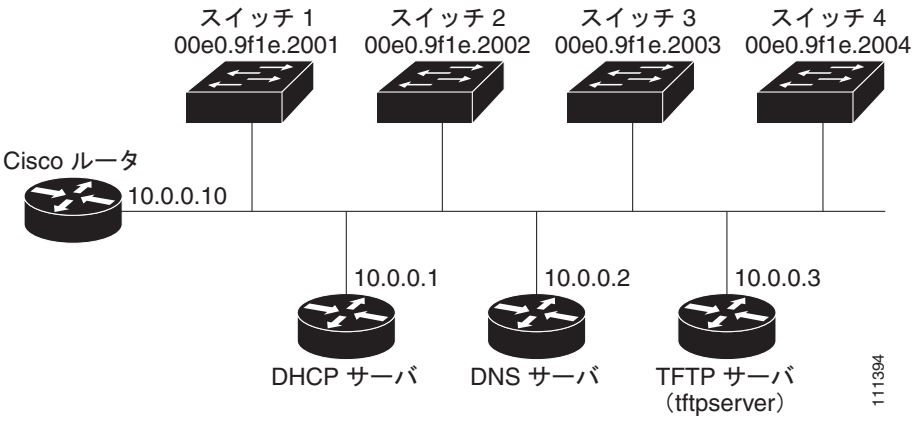


表 4-3 は、DHCP サーバ上の予約リースの設定例です。

表 4-3　DHCP サーバ コンフィギュレーション

	スイッチ A	スイッチ B	スイッチ C	スイッチ D
バインディング キー（ハードウェア アドレス）	00e0.9f1e.2001	00e0.9f1e.2002	00e0.9f1e.2003	00e0.9f1e.2004
IP アドレス	10.0.0.21	10.0.0.22	10.0.0.23	10.0.0.24
サブネット マスク	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
ルータ アドレス	10.0.0.10	10.0.0.10	10.0.0.10	10.0.0.10
DNS サーバ アドレス	10.0.0.2	10.0.0.2	10.0.0.2	10.0.0.2
TFTP サーバ名	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*
ブート ファイル名（コンフィギュレーション ファイル）（任意）	switcha-confg	switchb-confg	switchc-confg	switchd-confg
ホスト名（任意）	switcha	switchb	switchc	switchd

DNS サーバの設定

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

TFTP サーバ コンフィギュレーション（UNIX）

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

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

```
ip host switchb 10.0.0.22
ip host switchc 10.0.0.23
ip host switchd 10.0.0.24
```

DHCP クライアント コンフィギュレーション

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

ソフトウェア イメージのリロードのスケジューリング：例

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

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

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

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

スケジュールがすでに設定されたリロードを取り消すには、**reload cancel** 特権 EXEC コマンドを使用します。

DHCP 自動イメージ アップデートの設定：例

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

DHCP サーバとしてスイッチを設定：例

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

```
Switch# config terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:c-ipservices-mz.122-44.3.SE.tar
Switch(config)# tftp-server flash:ies-lanbase-tar.122-44.EX.tar
Switch(config)# tftp-server flash:boot-config.text
```

```
Switch(config)# tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

DHCP サーバからファイルをダウンロードするクライアントの設定

次に、VLAN 99 上のレイヤ 3 SVI インターフェイスを使用し、保存されているコンフィギュレーションで DHCP ベースの自動設定をイネーブルにする例を示します。

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

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 5

Cisco IOS Configuration Engine の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Cisco IOS Configuration Engine 設定の前提条件

CNS DeviceID を設定します。

- Cisco Configuration Engine ユーザ インターフェイスを使用する場合は、スイッチで **cns config initial** グローバル コンフィギュレーション コマンドを使用する前ではなく、使用した後にスイッチが取得したホスト名の値に、最初に DeviceID フィールドを設定する必要があります。そうしないと、後続の **cns config partial** グローバル コンフィギュレーション コマンドの操作が誤動作します。

自動 CNS 設定のイネーブル化

- スイッチの自動 CNS 設定をイネーブルにするには、まず表 5-1 の条件を満たす必要があります。条件設定を完了したらスイッチの電源を入れます。**setup** プロンプトでコマンドを入力する必要はありません。「初期設定」（P.5-5）で説明したように、スイッチが初期設定を開始します。コンフィギュレーション ファイル全体がスイッチにロードされると作業は完了です。

表 5-1　　自動設定イネーブル化の条件

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

表 5-1　自動設定イネーブル化の条件 （続き）

デバイス	必要な設定
DHCP サーバ	• IP アドレスの割り当て • TFTP サーバの IP アドレス • TFTP サーバのブートストラップ コンフィギュレーション ファイルへのパス • デフォルト ゲートウェイの IP アドレス
TFTP サーバ	• スイッチと Configuration Engine との通信を可能にする CNS コンフィギュレーション コマンドを含むブートストラップ コンフィギュレーション ファイル • （デフォルトのホスト名の代わりに）スイッチ MAC アドレスまたはシリアル番号のいずれかを使用して ConfigID および EventID を生成するように設定されたスイッチ • スイッチにコンフィギュレーション ファイルをプッシュするように設定された CNS イベント エージェント
CNS Configuration Engine	デバイス タイプ別の 1 つまたは複数のテンプレートで、テンプレートにデバイスの ConfigID がマッピングされています。

Cisco IOS Configuration Engine の設定に関する情報

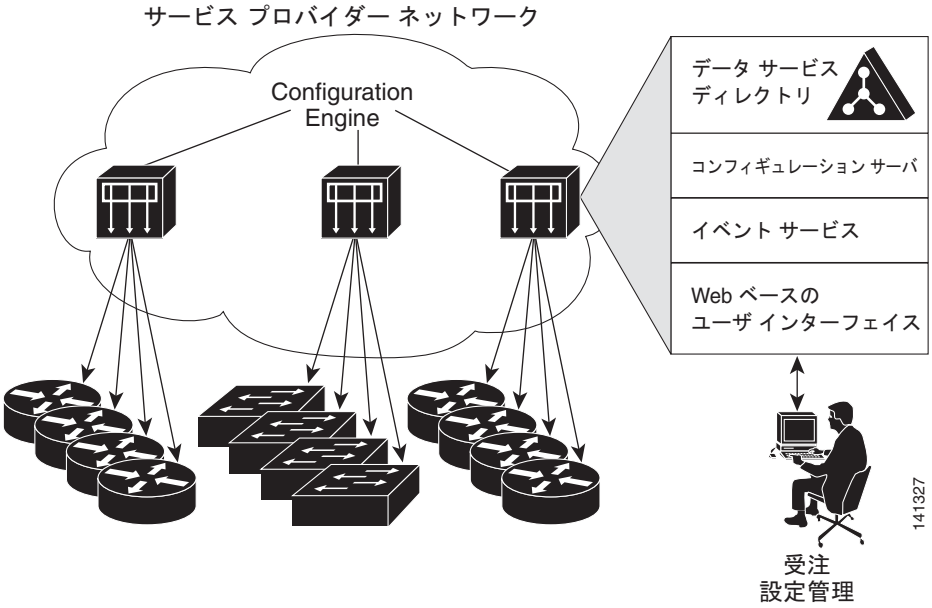
Cisco Configuration Engine は、ネットワーク管理ソフトウェアで、ネットワーク デバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーション サービスとして機能します（図 5-1 を参照）。各 Cisco Configuration Engine サービスは、シスコ デバイス（スイッチとルータ）のグループとデバイスが提供するサービスを管理し設定を保存して、必要に応じて配信します。Cisco Configuration Engine はデバイス固有の設定変更を生成してデバイスに送信し、設定変更を実行してその結果をロギングすることで、初期設定および設定の更新を自動化します。

Cisco Configuration Engine は、スタンドアロン モードおよびサーバ モードをサポートし、次の CNS コンポーネントを備えています。

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

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

図 5-1　Configuration Engine アーキテクチャの概要



コンフィギュレーション サービス

コンフィギュレーション サービスは、Cisco Configuration Engine の中核コンポーネントです。スイッチ上にある Cisco IOS CNS エージェントと連携して動作するコンフィギュレーション サーバで構成されています。コンフィギュレーション サービスは、初期設定と論理グループによる大規模な再設定のために、デバイスとサービスの設定をスイッチに配信します。スイッチはネットワーク上で初めて起動するときに、コンフィギュレーション サービスから初期設定を受信します。

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

コンフィギュレーション サーバは Web サーバであり、コンフィギュレーション テンプレートと組み込み型ディレクトリ（スタンドアロン モード）またはリモート ディレクトリ（サーバ モード）に保存されているデバイス固有の設定情報を使用します。

コンフィギュレーション テンプレートは、CLI（コマンドライン インターフェイス）コマンド形式で静的な設定情報を含んだテキスト ファイルです。テンプレートでは、変数は、Lightweight Directory Access Protocol（LDAP）URL を使用して指定します。この URL はディレクトリに保存されているデバイス固有の設定情報を参照します。

Cisco IOS エージェントは受信したコンフィギュレーション ファイルの構文をチェックし、イベントを発行して構文チェックが成功または失敗したかを表示します。コンフィギュレーション エージェントは設定をただちに適用することも、あるいは同期化イベントをコンフィギュレーション サーバから受信するまで適用を遅らせることもできます。

イベント サービス

Cisco Configuration Engine は、設定イベントの受信および生成にイベント サービスを使用します。イベント エージェントはスイッチ上にあり、スイッチと Configuration Engine のイベント ゲートウェイ間の通信を容易にします。

イベント サービスは、非常に有効なパブリッシュ サブスクライブ通信方式です。イベント サービスは、サブジェクトベースのアドレス指定を使用して、メッセージを宛先に送信します。サブジェクトベースのアドレス表記法では、メッセージおよび宛先には簡単で均一なネームスペースを定義します。

NSM

Cisco Configuration Engine には NameSpace Mapper（NSM）が装備されています。NSM は、アプリケーション、デバイスまたはグループ ID、およびイベントに基づいてデバイスの論理グループ管理用に検索サービスを提供します。

Cisco IOS デバイスは、たとえば cisco.cns.config.load といった、Cisco IOS ソフトウェアで設定されたサブジェクト名と一致するイベント サブジェクト名のみを認識します。ネームスペース マッピング サービスを使用すると、希望する命名規則を使用することでイベントを指定できます。サブジェクト名でデータ ストアにデータを入力した場合、NSM はイベント サブジェクト名ストリングを、Cisco IOS が認識するものに変更します。

サブスクライバの場合、一意のデバイス ID とイベントが指定されると、ネームスペース マッピング サービスは、サブスクライブ対象のイベント セットを返します。同様にパブリッシャの場合、一意のグループ ID、デバイス ID、およびイベントが指定されると、マッピング サービスは、パブリッシュ対象のイベント セットを返します。

CNS ID とデバイスのホスト名

Configuration Engine は、設定済みのスイッチごとに一意の識別子が関連付けられていることを想定しています。一意の識別子は複数の同義語を持つことができますが、各同義語は特定のネームスペース内で一意です。イベント サービスは、ネームスペースの内容を使用してメッセージのサブジェクトベース アドレス指定を行います。

Configuration Engine では、2 つのネームスペース（イベント バス用とコンフィギュレーション サーバ用）があります。コンフィギュレーション サーバのネームスペースでは、*ConfigID* という用語がデバイスの一意な識別子です。イベント バスのネームスペースでは、*DeviceID* という用語がデバイスの CNS 一意識別子です。

Configuration Engine は、イベント バスとコンフィギュレーション サーバの両方を使用してデバイスに設定を提供するので、設定済みのスイッチごとに ConfigID と DeviceID の両方を定義する必要があります。

コンフィギュレーション サーバの 1 つのインスタンスでは、設定済みの 2 つのスイッチが同じ ConfigID 値を共有できません。イベント バスの 1 つのインスタンスでは、設定済みの 2 つのスイッチが同じ DeviceID 値を共有できません。

ConfigID

設定済みのスイッチごとに一意の ConfigID があります。これは対応するスイッチ CLI 属性に対する Configuration Engine ディレクトリへのキーの役割を果たします。スイッチ上で定義された ConfigID は、Configuration Engine の対応するスイッチ定義の ConfigID と一致している必要があります。

ConfigID は起動時に固定され、スイッチ ホスト名を再設定した場合でもデバイスを再起動するまで変更できません。

DeviceID

イベント バスに参加している設定済みのスイッチごとに一意の DeviceID があります。これはスイッチの送信元アドレスに似ているので、スイッチをバス上の特定の宛先として指定できます。**cns config partial** グローバル コンフィギュレーション コマンドを使用して設定されたすべてのスイッチは、イベント バスにアクセスする必要があります。したがって、スイッチから発信される DeviceID は、Configuration Engine の対応するスイッチ定義の DeviceID と一致する必要があります。

DeviceID の発信元は、スイッチの Cisco IOS ホスト名によって定義されます。ただし、DeviceID 変数およびその使用は、スイッチに隣接するイベント ゲートウェイ内にあります。

イベント バス上の Cisco IOS の論理上の終点は、イベント ゲートウェイに組み込まれ、それがスイッチの代わりにプロキシとして動作します。イベント ゲートウェイはイベント バスに対して、スイッチおよび対応する DeviceID を表示します。

スイッチは、イベント ゲートウェイとの接続が成功するとすぐに、そのホスト名をイベント ゲートウェイに宣言します。接続が確立されるたびに、イベント ゲートウェイは DeviceID 値を Cisco IOS ホスト名に組み合わせます。イベント ゲートウェイは、スイッチと接続している間にこの DeviceID 値をキャッシュします。

ホスト名および DeviceID の相互作用

DeviceID は、イベント ゲートウェイと接続したときに固定され、スイッチ ホスト名を再設定した場合でも変更されません。

スイッチのスイッチ ホスト名を変更する場合、DeviceID を更新する唯一の方法はスイッチとイベント ゲートウェイ間の接続を中断することです。**no cns event** グローバル コンフィギュレーション コマンドを入力してから、**cns event** グローバル コンフィギュレーション コマンドを入力します。

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

ホスト名、DeviceID、ConfigID の使用方法

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

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

Configuration Engine で **Setup** を実行する場合、これらの属性および関連する属性（タグ値のペア）を設定します。

Cisco IOS エージェント

CNS イベント エージェント機能によって、スイッチはイベント バス上でイベントにパブリッシュおよびサブスクライブを行い、Cisco IOS エージェントと連携できます。

初期設定

スイッチが最初に起動すると、ネットワークで Dynamic Host Configuration Protocol（DHCP）要求をブロードキャストすることで IP アドレスを取得しようとします。サブネット上には DHCP サーバがないものと想定し、ディストリビューション スイッチは DHCP リレー エージェントとして動作し、要求

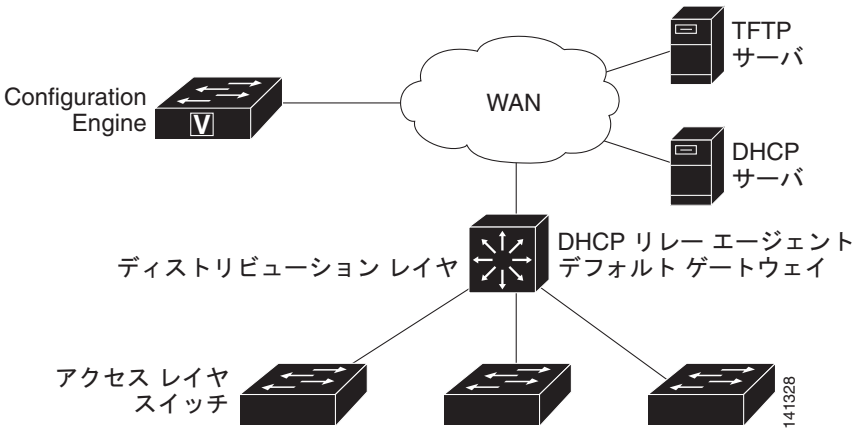
を DHCP サーバに転送します。DHCP サーバは要求を受信すると、新しいスイッチに IP アドレスを割り当て、TFTP サーバの IP アドレス、ブートストラップ コンフィギュレーション ファイルへのパス、デフォルト ゲートウェイの IP アドレスを、DHCP リレー エージェントに対するユニキャスト応答に組み入れます。DHCP リレー エージェントは、この応答をスイッチに転送します。

スイッチは、割り当てられた IP アドレスを自動的にインターフェイス VLAN 1（デフォルト）に設定し、TFTP サーバからブートストラップ コンフィギュレーション ファイルをダウンロードします。ブートストラップ コンフィギュレーション ファイルが正常にダウンロードされると、スイッチはそのファイルを実行コンフィギュレーションにロードします。

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

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

図 5-2　　初期設定の概要



差分（部分）設定

ネットワークが稼働すると、Cisco IOS エージェントを使用して新しいサービスを追加できます。差分（部分）設定は、スイッチに送信できます。実際の設定を、イベント ペイロードとしてイベント ゲートウェイを介して（プッシュ処理）、またはスイッチにプル オペレーションを開始させる信号イベントとして送信できます。

スイッチは、適用する前に設定の構文をチェックできます。構文が正しい場合は、スイッチは差分設定を適用し、コンフィギュレーション サーバに成功を信号で伝えるイベントを発行します。スイッチが差分設定を適用しない場合、エラー ステータスを示すイベントを発行します。スイッチが差分設定を適用した場合、NVRAM（不揮発性 RAM）に書き込むか、または書き込むように指示されるまで待つことができます。

同期設定

スイッチは、設定を受信した場合、書き込み信号イベントの受信時に設定の適用を遅らせることができます。書き込み信号イベントは、更新された設定を NVRAM に保存しないようにスイッチに指示します。スイッチは更新された設定を実行コンフィギュレーションとして使用します。これによりスイッチの設定は、次の再起動時の使用のために NVRAM に設定を保存する前に、他のネットワーク アクティビティと同期化されます。

Cisco IOS Configuration Engine の設定方法

Cisco IOS エージェントの設定

スイッチの Cisco IOS ソフトウェアの CNS イベント エージェントおよび Cisco IOS CNS エージェントでは、スイッチが接続されて自動的に設定することができます。エージェントは両方ともイネーブルにする必要があり、CNS は**初期**設定または**部分**設定が可能です。部分設定では、リモート スイッチに差分設定を送信するために Configuration Engine を使用できます。

CNS イベント エージェントのイネーブル化

はじめる前に

スイッチ上で Cisco IOS CNS イベント エージェントをイネーブルにしてから、Cisco IOS CNS エージェントをイネーブルにする必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cns event** {*hostname* | *ip-address*} [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**reconnect** *time*] [**source** *ip-address*]	イベント エージェントをイネーブルにして、ゲートウェイ パラメータを入力します。 • {*hostname* | *ip-address*}：イベント ゲートウェイのホスト名または IP アドレスを入力します。 • （任意）*port number*：イベント ゲートウェイのポート番号を入力します。デフォルトのポート番号は 11011 です。 • （任意）**backup**：ゲートウェイがバックアップ ゲートウェイであることを示します。（省略した場合は、プライマリ ゲートウェイになります）。 • （任意）**failover-time** *seconds*：バックアップ ゲートウェイが確立された後にスイッチがプライマリ ゲートウェイ ルートを待つ時間を入力します。 • （任意）**keepalive** *seconds*：スイッチがキープアライブ メッセージを送信する間隔を入力します。*retry-count* に、キープアライブ メッセージへの応答がない場合に接続を終了するまでのメッセージ送信回数を入力します。デフォルト値はいずれも 0 です。 • （任意）**reconnect** *time*：スイッチがイベント ゲートウェイに再接続しようとする前の最大時間間隔を入力します。 • （任意）**source** *ip-address*：このデバイスの送信元 IP アドレスを入力します。 （注）　**encrypt** キーワードおよび **clock-timeout** *time* キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show cns event connections**	イベント エージェントに関する情報を確認します。

Cisco IOS CNS エージェントと初期設定のイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cns template connect** *name*	CNS テンプレート接続コンフィギュレーション モードを開始して、CNS 接続テンプレートの名前を指定します。
ステップ 3	**cli** *config-text*	CNS 接続テンプレートにコマンドラインを入力します。テンプレート内の各コマンドラインにこの手順を繰り返します。
ステップ 4		別の CNS 接続テンプレートを設定する場合は、ステップ 2 ～ 3 を繰り返します。

	コマンド	目的
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**cns connect** *name* [**retries** *number*] [**retry-interval** *seconds*] [**sleep** *seconds*] [**timeout** *seconds*]	CNS 接続コンフィギュレーション モードを開始し、CNS 接続プロファイルの名前を指定し、プロファイル パラメータを定義します。スイッチは CNS 接続プロファイルを使用して Configuration Engine に接続します。 • （任意）**retries** *number*：接続の再試行回数を入力します。指定できる範囲は 1 ～ 30 です。デフォルトは 3 です。 • （任意）**retry-interval** *seconds*：Configuration Engine への連続する接続の試行間隔を入力します。指定できる範囲は 1 ～ 40 秒です。デフォルトは 10 秒です。 • （任意）**sleep** *seconds*：最初の接続試行を実行するまで待機する時間を入力します。指定できる範囲は 0 ～ 250 秒です。デフォルトは 0 です。 • （任意）**timeout** *seconds*：接続が終了しようとした後に待機する時間を入力します。指定できる範囲は 10 ～ 2000 秒です。デフォルトは 120 です。
ステップ 7	**discover** {**controller** *controller-type* | **dlci** [**subinterface** *subinterface-number*] | **interface** [*interface-type*] | **line** *line-type*}	CNS 接続プロファイル内のインターフェイス パラメータを入力します。 • **controller** *controller-type*：コントローラ タイプを入力します。 • **dlci**：アクティブなデータリンク接続識別子（DLCI）を入力します。 （任意）**subinterface** *subinterface-number*：アクティブな DLCI の検索に使用するポイントツーポイント サブインターフェイス番号を指定します。 • **interface** [*interface-type*]：インターフェイスのタイプを入力します。 • **line** *line-type*：回線タイプを入力します。
ステップ 8	**template** *name* [*... name*]	スイッチの設定に適用する CNS 接続プロファイル内の CNS 接続テンプレートのリストを指定します。複数のテンプレートを指定できます。
ステップ 9		ステップ 7 ～ 8 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイス パラメータと CNS 接続テンプレートを指定します。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**hostname** *name*	スイッチのホスト名を入力します。
ステップ 12	**ip route** *network-number*	（任意）IP アドレスが *network-number* の Configuration Engine へのスタティック ルートを確立します。

	コマンド	目的
ステップ 13	**cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] または **cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**]	（任意）Configuration Engine が使用する一意の EventID または ConfigID を設定します。 • *interface num*：インターフェイスの種類（たとえば、ethernet、group-async、loopback、virtual-template）を入力します。この設定では、一意の ID を定義するためにどのインターフェイスから IP アドレスまたは MAC アドレスを取得するかを指定します。 • **dns-reverse**：ホスト名を取得し、一義的な ID として割り当てます。 • **ipaddress**：IP アドレスを使用します。 • **mac-address**：一義的な ID として MAC アドレスを使用します。 • （任意）**event**：ID をスイッチの識別に使用する eventID 値になるように設定します。 • （任意）**image**：ID をスイッチの識別に使用する imageID 値になるように設定します。 （注）　**event** と **image** キーワードを省略した場合は、スイッチの識別には imageID 値が使用されます。 • **hardware-serial**：一義的な ID としてスイッチのシリアル番号を設定します。 • **hostname**（デフォルト）：一意の ID としてスイッチ ホスト名を選択します。一意の ID として任意の文字列 **string** *string* を使用し、**udi** で一意の ID として Unique Device Identifier（UDI）を設定します。

	コマンド	目的
ステップ 14	**cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**]	Cisco IOS をイネーブルにし、初期設定を開始します。 • {*hostname* | *ip-address*}：コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port-number*：コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • （任意）**event**：設定が完了したときの設定の成功、失敗、または警告メッセージをイネーブルにします。 • （任意）**no-persist**：**cns config initial** グローバル コンフィギュレーション コマンドの入力結果によってプルされた設定の NVRAM への自動書き込みを抑制します。**no-persist** キーワードを入力しない場合、**cns config initial** コマンドを使用すると、その結果の設定が自動的に NVRAM に書き込まれます。 • （任意）**page** *page*：初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。 • （任意）**source** *ip-address*：送信元 IP アドレスを入力します。 • （任意）**syntax-check***：*このパラメータが入力された場合、構文をチェックします。 （注）　**encrypt** キーワード、**status** キーワード、*url* キーワードおよび **inventory** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 15	**end**	特権 EXEC モードに戻ります。

部分設定のイネーブル化

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

Cisco IOS Configuration Engine のモニタリングとメンテナンス

コマンド	目的
show cns config connections	CNS Cisco IOS エージェントの接続のステータスを表示します。
show cns config outstanding	開始されたがまだ終了していない差分（部分）CNS 設定に関する情報を表示します。
show cns config stats	Cisco IOS エージェントに関する統計情報を表示します。
show cns event connections	CNS イベント エージェントの接続のステータスを表示します。
show cns event stats	CNS イベント エージェントに関する統計情報を表示します。
show cns event subject	アプリケーションによってサブスクライブされたイベント エージェントのサブジェクト一覧を表示します。

Cisco IOS Configuration Engine の設定例

CNS イベント エージェントのイネーブル化：例

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

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

CNS の初期設定：例

次に、スイッチの設定が不明な場合に、リモート スイッチに初期設定を設定する例（CNS ゼロ タッチ機能）を示します。

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

次に、スイッチ IP アドレスが不明の場合に、リモート スイッチに初期設定を設定する例を示します。Configuration Engine の IP アドレスは 172.28.129.22 です。

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

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
ネットワーク管理コマンド	『*Cisco IOS Network Management Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 6

スイッチ クラスタの設定

この章では、スイッチ上でのスイッチ クラスタの作成と管理に関する概念と手順を説明します。Cisco Network Assistant アプリケーション（CNA）、コマンドライン インターフェイス（CLI）、または SNMP（簡易ネットワーク管理プロトコル）を使用してスイッチ クラスタを作成、管理できます。CNA の完全な具体的な手順については、オンラインヘルプを参照してください。CLI クラスタコマンドについては、スイッチ コマンド リファレンスを参照してください。

この章では、スイッチ クラスタに関する情報を提供します。クラスタ内に他のクラスタに対応した Catalyst スイッチが混在している場合の注意事項や制限事項も紹介しますが、クラスタ中のスイッチに対するクラスタ機能の詳細な説明は割愛します。特定の Catalyst プラットフォームにおけるクラスタの詳細情報は、該当するスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

スイッチ クラスタの設定の前提条件

- スタティック ルーティングおよびルーテッド ポートがサポートされるのは、スイッチで LAN Base イメージが実行されている場合だけです。

クラスタ コマンド スイッチの特性

クラスタ コマンド スイッチは、次の要件を満たしている必要があります。

- Cisco IOS Release 15.0(1)EY 以降を実行している。
- I P アドレスが指定されている。
- Cisco Discovery Protocol（CDP）バージョン 2 がイネーブル（デフォルト）に設定されている。
- 他のクラスタのクラスタ コマンド スイッチまたはクラスタ メンバ スイッチではない。

- 管理 VLAN を介してスタンバイ クラスタ コマンド スイッチに、そして共通 VLAN を介してクラスタ メンバ スイッチに接続されている。

スタンバイ クラスタ コマンド スイッチの特性

スタンバイ クラスタ コマンド スイッチは、次の要件を満たしている必要があります。

- Cisco IOS 15.0(1)EY 以降を実行している。
- I P アドレスが指定されている。
- CDP バージョン 2 がイネーブルに設定されている。
- 管理 VLAN を介してコマンド スイッチに接続されていて、なおかつ他のスタンバイ コマンド スイッチに接続されている。
- 共通 VLAN を介して（クラスタ コマンド スイッチおよびスタンバイ コマンド スイッチを除く）他のすべてのクラスタ メンバ スイッチに接続されている。
- クラスタ メンバ スイッチとの接続能力を維持するために、クラスタに冗長接続されている。
- 他のクラスタのコマンド スイッチまたはメンバ スイッチではない。

候補スイッチおよびクラスタ メンバ スイッチの特性

*候補スイッチ*とは、クラスタ対応ですが、クラスタにまだ追加されていないスイッチを意味します。クラスタ メンバ スイッチは、スイッチ クラスタにすでに追加されているスイッチです。候補スイッチまたはクラスタ メンバ スイッチには必須ではありませんが、専用の IP アドレスおよびパスワードを指定できます（「IP アドレス」（P.6-11）および「パスワード」（P.6-12）を参照してください）。

クラスタに加入する候補スイッチは、次の要件を満たしている必要があります。

- クラスタ対応のソフトウェアが稼働している。
- CDP バージョン 2 がイネーブルに設定されている。
- 他のクラスタのクラスタ コマンド スイッチまたはクラスタ メンバ スイッチではない。
- クラスタ スタンバイ グループが存在する場合、少なくとも 1 つの共通 VLAN を介して、そのスイッチにすべてのスタンバイ クラスタ コマンド スイッチが接続されている。各スタンバイ クラスタ コマンド スイッチに対応する VLAN は、異なる場合があります。
- 少なくとも 1 つの共通 VLAN を介して、クラスタ コマンド スイッチに接続されている。

（注） Catalyst1900、Catalyst2820、Catalyst2900XL、Catalyst2950、Catalyst3500XL 候補およびクラスタ メンバ スイッチは、管理 VLAN を介してクラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチに接続する必要があります。スイッチクラスタ環境におけるこれらのスイッチの詳細情報は、該当するスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 クラスタ コマンド スイッチを使用する場合、この要件は当てはまりません。候補およびクラスタ メンバ スイッチは、クラスタ コマンド スイッチと共通の任意の VLAN を介して接続できます。

スイッチ クラスタの設定に関する制約事項

特定のホストまたはネットワークに対してアクセスを制限する場合、**ip http access-class** グローバル コンフィギュレーション コマンドは使用しないことを推奨します。アクセスをコントロールするには、クラスタ コマンド スイッチを使用するか、または IP アドレスが設定されているインターフェイス上にアクセス コントロール リスト（ACL）を適用します。ACL の詳細については、第 37 章「ACL によるネットワーク セキュリティの設定」を参照してください。

スイッチ クラスタの設定に関する情報

*スイッチ クラスタ*はクラスタ対応 Catalyst スイッチで構成されており、最大 16 台接続できます。接続されたスイッチは 1 つのエンティティとして管理されます。クラスタ内のスイッチは、スイッチ クラスタ化テクノロジーによって、単一の IP アドレスから異なる Catalyst デスクトップ スイッチ プラットフォームで構成されたグループを設定したり、トラブルシューティングを行ったりできます。

スイッチ クラスタでは、1 台のスイッチが*クラスタ コマンド スイッチ*として動作する必要があり、最大 15 台の他のスイッチが*クラスタ メンバ スイッチ*として動作できます。1 つのクラスタは、16 台以内のスイッチで構成する必要があります。クラスタ コマンド スイッチは、クラスタ メンバ スイッチの設定、管理、およびモニタを実行できる唯一のスイッチです。クラスタ メンバは、一度に 1 つのクラスタにしか所属できません。

クラスタリング スイッチの利点

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

  クラスタ メンバは、「クラスタ候補およびクラスタ メンバの自動検出」（P.6-5）で説明している接続方法に従ってクラスタ コマンド スイッチに接続します。ここでは、Catalyst 1900、Catalyst 2820、Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL スイッチに対する管理 VLAN（仮想 LAN）の検討事項を説明します。スイッチクラスタ環境におけるこれらのスイッチの詳細情報は、該当するスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

- クラスタ コマンドスイッチに冗長性を持たせることで、コマンド スイッチに障害が発生した場合でも対応できます。1 つまたは複数のスイッチを*スタンバイ クラスタ コマンド*に指定すると、クラスタ メンバ間の競合を回避できます。*クラスタ スタンバイ グループ*は、スタンバイ クラスタ コマンド スイッチのグループです。

- さまざまなスイッチを、1 つの IP アドレスで管理できます。これは、特に IP アドレスの数が限られている場合に効果があります。スイッチ クラスタとの通信はすべてクラスタ コマンド スイッチの IP アドレスで行われます。

クラスタ対応のスイッチ

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

表 6-1　スイッチ ソフトウェアおよびクラスタへの対応性

スイッチ	Cisco IOS リリース	クラスタへの対応性
IE 2000 スイッチ	15.0(1)EY 以降	メンバまたはコマンド スイッチ
IE 3010 スイッチ	12.2(53)EZ 以降	メンバまたはコマンド スイッチ
IE 3000 スイッチ	12.2(40)EX 以降	メンバまたはコマンド スイッチ
Catalyst 3750-X または Catalyst 3560-X	12.2(53)SE2 以降	メンバまたはコマンド スイッチ
Catalyst 3750-E または Catalyst 3560-E	12.2(35)SE2 以降	メンバまたはコマンド スイッチ
Catalyst 3750	12.1(11)AX 以降	メンバまたはコマンド スイッチ
Catalyst 3560	12.1(19)EA1b 以降	メンバまたはコマンド スイッチ
Catalyst 3550	12.1(4)EA1 以降	メンバまたはコマンド スイッチ
Catalyst 2975	12.2(46)EX 以降	メンバまたはコマンド スイッチ
Catalyst 2970	12.1(11)AX 以降	メンバまたはコマンド スイッチ
Catalyst 2960-S	12.2(53)SE 以降	メンバまたはコマンド スイッチ
Catalyst 2960	12.2(25)FX 以降	メンバまたはコマンド スイッチ
Catalyst 2955	12.1(12c)EA1 以降	メンバまたはコマンド スイッチ
Catalyst 2950	12.0(5.2)WC(1) 以降	メンバまたはコマンド スイッチ
Catalyst 2950 LRE	12.1(11)JY 以降	メンバまたはコマンド スイッチ
Catalyst 2940	12.1(13)AY 以降	メンバまたはコマンド スイッチ
Catalyst 3500 XL	12.0(5.1)XU 以降	メンバまたはコマンド スイッチ
Catalyst 2900 XL（8 MB スイッチ）	12.0(5.1)XU 以降	メンバまたはコマンド スイッチ

表 6-1　スイッチ ソフトウェアおよびクラスタへの対応性 （続き）

スイッチ	Cisco IOS リリース	クラスタへの対応性
Catalyst 2900 XL（4 MB スイッチ）	11.2(8.5)SA6（推奨）	メンバ スイッチのみ
Catalyst 1900 および Catalyst 2820	9.00（-A または -EN）以降	メンバ スイッチのみ

スイッチ クラスタのプランニングについて

複数のスイッチをクラスタで管理する場合、予想される競合や互換性の問題解決に重点を置きます。ここでは、クラスタを作成する前に理解すべき注意事項、要件、および警告について説明します。

- 「クラスタ候補およびクラスタ メンバの自動検出」（P.6-5）
- 「IP アドレス」（P.6-11）
- 「ホスト名」（P.6-11）
- 「パスワード」（P.6-12）
- 「SNMP コミュニティ ストリング」（P.6-12）
- 「TACACS+ および RADIUS」（P.6-12）
- 「LRE プロファイル」（P.6-13）

クラスタに対応している Catalyst スイッチについては、各スイッチのリリース ノートを参照してください。リリース ノートでは、クラスタ コマンド スイッチになれるスイッチとクラスタ メンバ スイッチにしかなれないスイッチ、また、それらに必要なソフトウェア バージョンやブラウザだけでなく、Java プラグインの設定も参照できます。

クラスタ候補およびクラスタ メンバの自動検出

クラスタ コマンド スイッチは Cisco Discovery Protocol（CDP）を使用して、複数の VLAN の中からクラスタ メンバ スイッチ、候補スイッチ、ネイバー スイッチクラスタ、エッジ デバイスを検出します。また、スター型のトポロジやカスケード型のトポロジ内からも検出できます。

（注）　クラスタ コマンド スイッチを使用してクラスタに対応したスイッチを検出する場合、クラスタ コマンド スイッチ、クラスタ メンバ、またはクラスタ対応スイッチの CDP を無効にしないでください。CDP の詳細については、第 32 章「CDP の設定」を参照してください。

次の接続に関する注意事項に従って、スイッチ クラスタ、クラスタ候補、接続されたスイッチ クラスタ、ネイバー エッジ デバイスを自動検出してください。

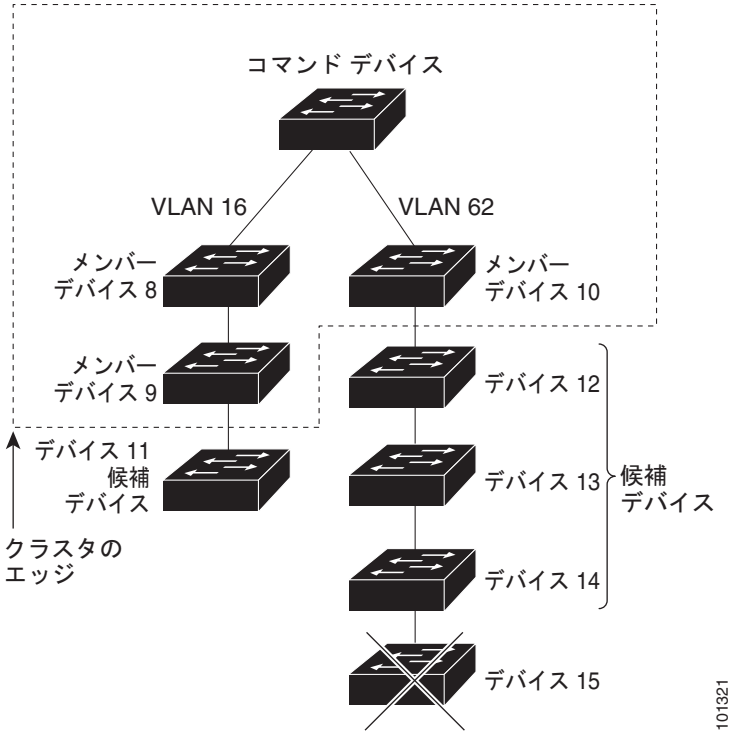
- 「CDP ホップを使用しての検出」（P.6-6）
- 「CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出」（P.6-7）
- 「異なる VLAN からの検出」（P.6-7）
- 「異なる管理 VLAN からの検出」（P.6-8）
- 「RP による検出」（P.6-9）
- 「新しく設置したスイッチの検出」（P.6-10）

CDP ホップを使用しての検出

クラスタ コマンド スイッチは CDP を使用して、クラスタ エッジから最大 7 CDP ホップ（デフォルトは 3 ホップ）までスイッチを検出できます。クラスタ エッジは、クラスタや候補スイッチに接続している最後のクラスタ スイッチの部分を指します。たとえば、図 6-1 のクラスタ メンバ スイッチ 9 と 10 はクラスタのエッジにあります。

図 6-1 では、クラスタ コマンド スイッチのポートに VLAN 16 と 62 が割り当てられています。CDP ホップのカウントは 3 です。クラスタ エッジから 3 ホップ以内にあるので、クラスタ コマンド スイッチはスイッチ 11、12、13、14 を検出します。スイッチ 15 はクラスタ エッジから 4 ホップ先なので検出されません。

図 6-1　　CDP ホップを使用しての検出

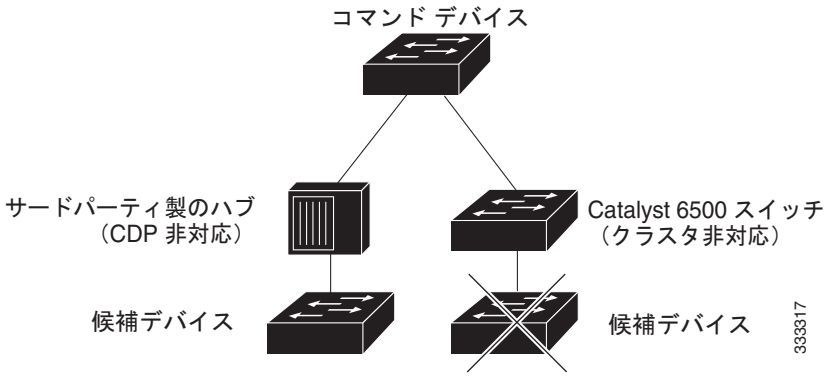


CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

クラスタ コマンド スイッチを *CDP 非対応のサードパーティ製のハブ*（他社製のハブなど）に接続している場合、そのサードパーティ製のハブを介して接続しているクラスタ対応デバイスを検出できます。ただし、クラスタ コマンド スイッチを*クラスタ非対応のシスコ デバイス*に接続している場合、クラスタ非対応のシスコ デバイスより先にあるクラスタ対応のデバイスは検出できません。

図 6-2 に、サードパーティ製のハブに接続したスイッチを検出するクラスタ コマンド スイッチを示します。ただし、クラスタ コマンド スイッチは Catalyst 5000 スイッチに接続しているスイッチは検出しません。

図 6-2　　CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

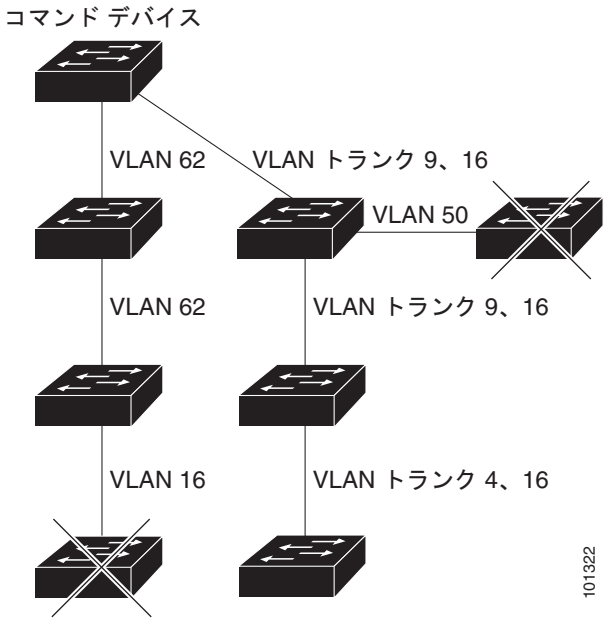


異なる VLAN からの検出

クラスタ コマンド スイッチが Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 の場合、異なる VLAN のクラスタ メンバ スイッチもクラスタに加えることができます。クラスタ メンバ スイッチとして、Catalyst スイッチもクラスタ コマンド スイッチと共通の VLAN に少なくとも 1 つは接続している必要があります。図 6-3 のクラスタ コマンド スイッチのポートには VLAN 9、16、62 が割り当てられているため、これらの VLAN のスイッチは検出できます。VLAN 50 にあるスイッチは検出できません。また、最初の列の VLAN 16 にあるスイッチも、クラスタ コマンド スイッチに接続されていないため検出できません。

Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL のクラスタ メンバ スイッチは、それぞれの管理 VLAN を介してクラスタ コマンド スイッチに接続している必要があります。管理 VLAN からの検出については、「異なる管理 VLAN からの検出」（P.6-8）を参照してください。VLAN の詳細については、第 17 章「VLAN の設定」を参照してください。

図 6-3　異なる VLAN からの検出



異なる管理 VLAN からの検出

Catalyst 2970、Catalyst 3550、Catalyst 3560、Catalyst 3750 クラスタ コマンド スイッチは、異なる VLAN や管理 VLAN のクラスタ メンバ スイッチを検出して管理できます。クラスタ メンバ スイッチとして、Catalyst スイッチもクラスタ コマンド スイッチと共通の VLAN に少なくとも 1 つは接続している必要があります。ただし、管理 VLAN を介してクラスタ コマンド スイッチに接続する必要はありません。デフォルトの管理 VLAN は VLAN 1 です。

（注）　スイッチ クラスタに Catalyst 3750 スイッチ、Catalyst 2975 スイッチ、またはスイッチ スタックがある場合は、Catalyst 3750 スイッチ、Catalyst 2975 スイッチ、またはスイッチ スタックをクラスタ コマンド スイッチにする必要があります。

図 6-5 に示されているクラスタ コマンド スイッチおよびスタンバイ コマンド スイッチ（Catalyst 2960、Catalyst 2970、Catalyst 2975、Catalyst 3550、Catalyst 3560、Catalyst 3750 と想定します）のポートには、VLAN 9、16、および 62 が割り当てられています。クラスタ コマンド スイッチの管理 VLAN は VLAN 9 です。各クラスタ コマンド スイッチは、次の例外を除き、異なる管理 VLAN のスイッチを検出します。

- スイッチ 7 およびスイッチ 10（管理 VLAN 4 のスイッチ）。クラスタ コマンド スイッチと共通の VLAN（VLAN 62 および VLAN 9）に接続していないため検出されません。
- スイッチ 9。自動検出は非候補デバイス（スイッチ 7）より先は検出できないため、検出されません。

RP による検出

（注）　LAN ベース イメージでは、スタティック ルーティングおよび RIP をサポートします。

ルーテッド ポート（RP）が設定されているクラスタ コマンド スイッチは、RP と*同じ* VLAN 内の候補スイッチおよびクラスタ メンバー スイッチだけを検出します。

図 6-4 のレイヤ 3 クラスタ コマンド スイッチにより、VLAN 9 および 62 のスイッチは検出されますが、VLAN 4 のスイッチは検出されません。クラスタ コマンド スイッチとクラスタ メンバー スイッチ 7 間の RP パスが損失している場合、VLAN 9 を介する冗長パスがあるため、クラスタ メンバー スイッチ 7 との接続は維持されます。

図 6-4　　RP による検出

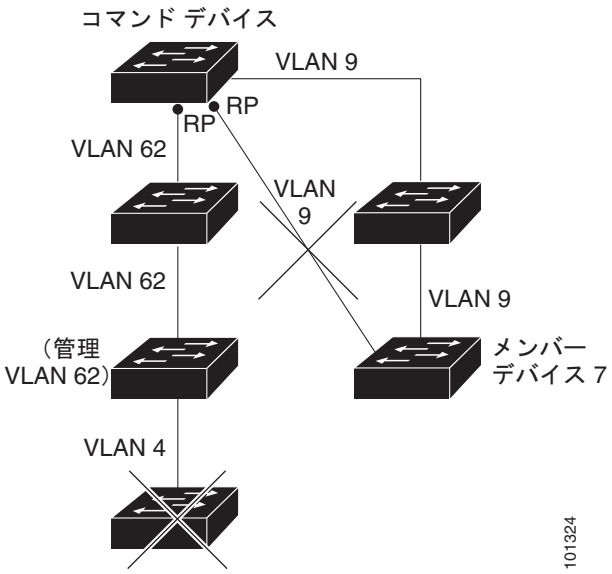
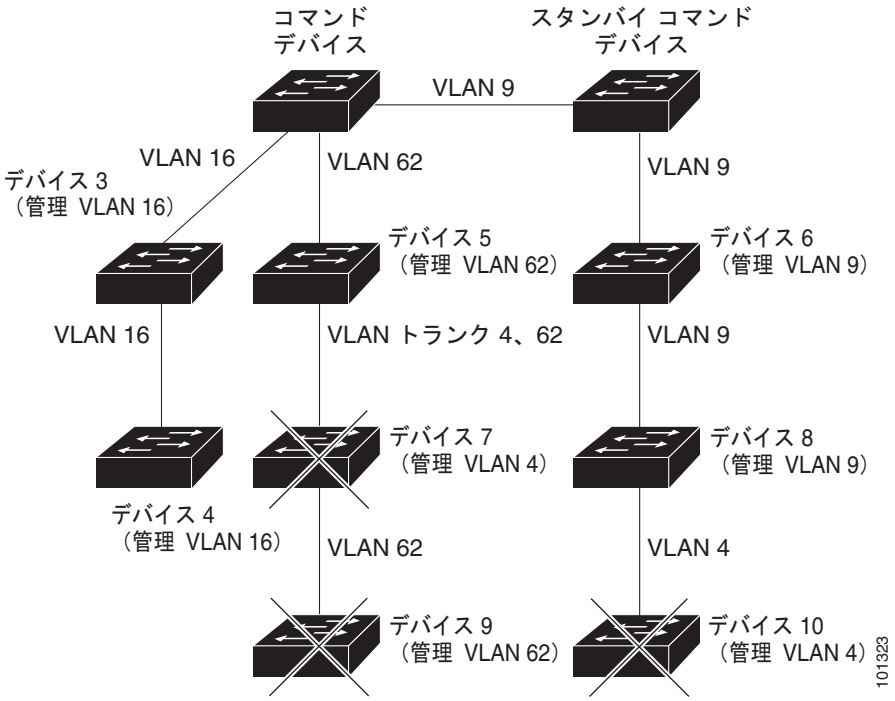


図 6-5　レイヤ 3 クラスタ コマンド スイッチを使用して異なる管理 VLAN から検出



新しく設置したスイッチの検出

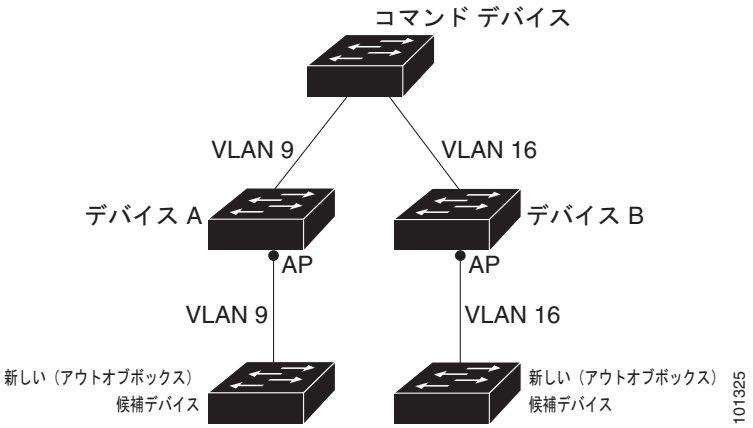
新しいアウトオブボックス スイッチをクラスタに加入させるには、アクセスポートの 1 つにクラスタを接続する必要があります。アクセス ポート（AP）は 1 つの VLAN にのみ属し、そのトラフィックを転送します。デフォルトでは、新しいスイッチとそのアクセス ポートに対して VLAN 1 が割り当てられます。

新しいスイッチがクラスタに加入すると、デフォルトの VLAN は即座にアップストリーム ネイバーの VLAN に変わります。また、新しいスイッチも自身のアクセス ポートを変更して、そのネイバーの VLAN に加わります。

図 6-6 のクラスタ コマンド スイッチは、VLAN 9 および 16 に加入しています。新しいクラスタ対応のスイッチがクラスタに加入すると、次の処理が行われます。

- 1 つのクラスタ対応のスイッチとそのアクセス ポートに VLAN 9 が割り当てられます。
- 他のクラスタ対応のスイッチとそのアクセス ポートに管理 VLAN 16 が割り当てられます。

図 6-6　新しく設置したスイッチの検出



IP アドレス

IP 情報をクラスタ コマンド スイッチに割り当てる必要があります。クラスタ コマンド スイッチには複数の IP アドレスを割り当てることができます。クラスタには、これらのコマンドスイッチの IP アドレスを介してアクセスできます。クラスタ スタンバイ グループを設定する場合、アクティブ クラスタ コマンド スイッチからスタンバイグループの仮想 IP アドレスを使用して、クラスタを管理する必要があります。仮想 IP アドレスを使用すると、アクティブ クラスタ コマンド スイッチに障害が発生してスタンバイ クラスタ コマンド スイッチがアクティブ クラスタ コマンド スイッチになった場合でも、クラスタへの接続を確保できます。

アクティブ クラスタ コマンド スイッチに障害が発生してスタンバイ クラスタ コマンド スイッチがその役割を引き継いだ場合、クラスタのアクセスには、スタンバイグループの仮想 IP アドレスも、新しいアクティブ クラスタ コマンド スイッチで使える IP アドレスも使用できます。

必須ではありませんが、IP アドレスはクラスタ対応のスイッチにも割り当てることができます。クラスタ メンバ スイッチは、コマンドスイッチの IP アドレスを使用して他のクラスタ メンバ スイッチと通信します。IP アドレスが割り当てられていないクラスタ メンバ スイッチがそのクラスタを離れる場合、スタンドアロン スイッチとして管理する IP アドレスを割り当てる必要があります。

IP アドレスの詳細については、第 4 章「スイッチ セットアップの設定」を参照してください。

ホスト名

クラスタ コマンド スイッチと対象のクラスタ メンバにはホスト名を割り当てる必要はありません。ただし、クラスタ コマンド スイッチに割り当てられたホスト名は、スイッチ クラスタを識別するのに役立ちます。スイッチのデフォルトのホスト名は *Switch* です。

クラスタに加入するスイッチにホスト名がない場合、クラスタ コマンド スイッチは一意のメンバ番号を自身のホスト名に追加し、そのスイッチに割り当てます。この処理はクラスタに加入するスイッチごとに順番に行われます。ここでいう番号とは、スイッチがクラスタに追加された順番を指します。たとえば、*eng-cluster* という名前のクラスタ コマンド スイッチには、5 番めのクラスタ メンバとして *eng-cluster-5* という名前が割り当てられます。

スイッチにホスト名がある場合、クラスタへの加入時もクラスタからの脱退時もその名前が使用されます。

クラスタ脱退時、または新しいクラスタへの加入時にそのメンバ番号（*5* など）を確保するため、クラスタ コマンド スイッチからスイッチにホスト名を送信した場合、それを受信したスイッチは、新しいクラスタのクラスタ コマンド スイッチのホスト名（*mkg-cluster-5* など）で古いホスト名（*eng-cluster-5* など）を上書きします。新しいクラスタではスイッチのメンバ番号を変更する場合（*3* など）、スイッチは前回の名前（*eng-cluster-5*）を控えます。

パスワード

クラスタのメンバになるスイッチにはパスワードを割り当てる必要はありません。スイッチはコマンドスイッチのパスワードを継承してクラスタに加入し、脱退するときもその情報を保有したまま離れます。コマンドスイッチのパスワードが設定されていない場合、クラスタ メンバ スイッチはヌル パスワードを代わりに継承します。クラスタ メンバ スイッチが継承するのはコマンドスイッチのパスワードのみです。

コマンドスイッチのパスワードと異なるメンバスイッチのパスワードを指定してその設定を保存してしまうと、クラスタ コマンド スイッチからそのスイッチを管理できなくなります。この状態はメンバスイッチのパスワードをコマンドスイッチのパスワードに戻すまで続きます。メンバスイッチを再起動しても、パスワードは元のコマンドスイッチ パスワードには戻りません。スイッチをクラスタに加入させた後は、メンバスイッチ パスワードを変更しないことを推奨します。

パスワードの詳細については、「スイッチへの無許可アクセスの防止」（P.12-2）を参照してください。

Catalyst 1900 および Catalyst 2820 スイッチ固有のパスワードの考慮事項については、これらのスイッチのインストレーション コンフィギュレーション ガイドを参照してください。

SNMP コミュニティ ストリング

クラスタ メンバ スイッチは、次のようにコマンドスイッチの Read-Only（RO）と Read-Write（RW）の後ろに *@esN* を追加した形でコミュニティ ストリングを継承します。

- *command-switch-readonly-community-string@esN* : *N* にはメンバスイッチの番号が入ります。
- *command-switch-readwrite-community-string@esN* : *N* にはメンバスイッチの番号が入ります。

クラスタ コマンド スイッチに複数の Read-Only または Read-Write コミュニティ ストリングがある場合、クラスタ メンバ スイッチには最初の Read-Only または Read-Write ストリングのみ伝播されます。

スイッチのコミュニティ ストリング数とその長さには制限がありません。SNMP およびコミュニティ ストリングの詳細については、第 36 章「SNMP の設定」を参照してください。

Catalyst 1900 および Catalyst 2820 スイッチ固有の SNMP の考慮事項については、これらのスイッチのインストレーション コンフィギュレーション ガイドを参照してください。

TACACS+ および RADIUS

TACACS+ をクラスタ メンバに設定する場合、すべてのクラスタ メンバに設定する必要があります。同様に、RADIUS をクラスタ メンバに設定する場合、すべてのクラスタ メンバに設定する必要があります。同じスイッチ クラスタでは、一部のメンバを TACACS+ で設定し、残りのメンバを RADIUS で設定することはできません。

TACACS+ の詳細については、「TACACS+ の設定」（P.12-31）を参照してください。RADIUS の詳細については、「RADIUS サーバ通信の設定」（P.12-34）を参照してください。

LRE プロファイル

スイッチ クラスタに、個人のプロファイルと公開プロファイルの両方を使用した Long-Reach Ethernet（LRE）スイッチがある場合、設定の競合が発生します。クラスタの 1 つの LRE スイッチに公開プロファイルが割り当てられている場合、クラスタ内のすべての LRE スイッチにも同じプロファイルを割り当てる必要があります。LRE スイッチをクラスタに追加する前に、クラスタ内の他の LRE スイッチが同じ公開プロファイルを使用しているかどうかを確認してください。

クラスタ内に異なる個人プロファイルを使用している LRE スイッチを混在させることはできます。

スイッチ クラスタの管理

CLI によるスイッチ クラスタの管理

クラスタ コマンド スイッチにログインすることにより、CLI からクラスタ メンバ スイッチを設定できます。**rcommand** ユーザ EXEC コマンドおよびクラスタ メンバ スイッチ番号を入力して、（コンソールまたは Telnet 接続を経由して）Telnet セッションを開始し、クラスタ メンバ スイッチの CLI にアクセスします。コマンド モードが変更され、通常どおりに Cisco IOS コマンドを使用できるようになります。クラスタ メンバ スイッチで **exit** 特権 EXEC コマンドを入力すると、コマンド スイッチの CLI に戻ります。

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

```
switch# rcommand 3
```

メンバ スイッチ番号が不明の場合は、クラスタ コマンド スイッチで **show cluster members** 特権 EXEC コマンドを入力します。**rcommand** コマンドおよび他のすべてのクラスタ コマンドについての詳細は、スイッチ コマンド リファレンスを参照してください。

Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバ スイッチの CLI にアクセスします。その後、Cisco IOS コマンドを通常どおりに使用できます。スイッチの Telnet セッションの設定手順については、「パスワード回復のディセーブル化」（P.12-28）を参照してください。

Catalyst1900 および Catalyst2820 の CLI に関する考慮事項

スイッチ クラスタに Standard Edition ソフトウェアが稼働している Catalyst 1900 および Catalyst 2820 スイッチがある場合、クラスタ コマンド スイッチの権限レベルが 15 であれば、Telnet セッションは管理コンソール（メニュー方式インターフェイス）にアクセスします。クラスタ コマンド スイッチの権限レベルが 1 ～ 14 であれば、パスワードの入力を要求するプロンプトが表示され、入力後にメニュー コンソールにアクセスできます。

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

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

（注）　Catalyst 1900 および Catalyst 2820 の CLI は、Enterprise Edition ソフトウェアが稼働しているスイッチに限って使用できます。

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

SNMP によるスイッチ クラスタの管理

スイッチの最初の起動時にセットアップ プログラムを使用して IP 情報を入力し、提示されたコンフィギュレーションを採用した場合、SNMP はイネーブルに設定されています。セットアップ プログラムを使用して IP 情報を入力していない場合は、SNMP はイネーブルではありません。その場合は、第 36 章「SNMP の設定」の説明に従って、SNMP をイネーブルに設定します。Catalyst 1900 スイッチ、Catalyst 2820 スイッチでは、SNMP はデフォルトでイネーブルです。

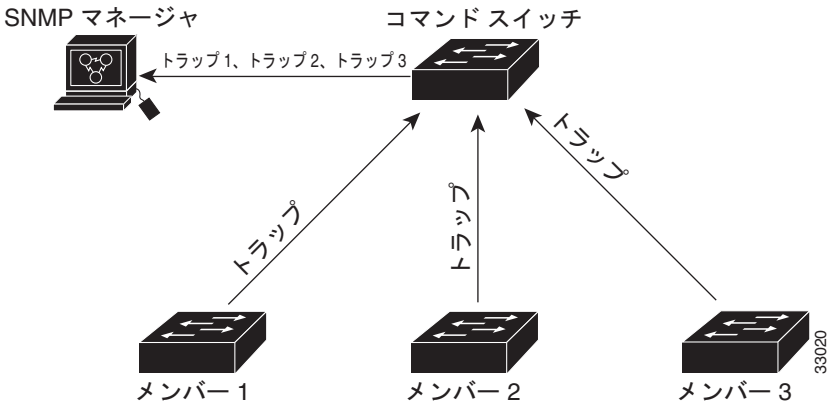
クラスタを作成すると、クラスタ コマンド スイッチがクラスタ メンバ スイッチと SNMP アプリケーション間のメッセージ交換を管理します。クラスタ コマンド スイッチ上のクラスタ ソフトウェアは、クラスタ コマンド スイッチ上で最初に設定された Read-Write および Read-Only コミュニティ ストリングにクラスタ メンバ スイッチ番号（*@esN*、*N* はスイッチ番号）を追加し、これらのストリングをクラスタ メンバ スイッチに送信します。クラスタ コマンド スイッチは、このコミュニティ ストリングを使用して、SNMP 管理ステーションとクラスタ メンバ スイッチ間で、get、set、および get-next メッセージの転送を制御します。

（注）　クラスタ スタンバイ グループを設定すると、ユーザが気付かないうちにクラスタ コマンド スイッチが変更される場合があります。クラスタにクラスタ スタンバイ グループを設定している場合は、クラスタ コマンド スイッチとの通信には、最初に設定された Read-Write および Read-Only コミュニティ ストリングを使用してください。

クラスタ メンバ スイッチに IP アドレスが割り当てられていない場合、図 6-7 に示すように、クラスタ コマンド スイッチはクラスタ メンバ スイッチからのトラップを管理ステーションにリダイレクトします。クラスタ メンバ スイッチに専用の IP アドレスおよびコミュニティ ストリングが割り当てられている場合、そのクラスタ メンバ スイッチはクラスタ コマンド スイッチを経由せず、管理ステーションに直接トラップを送信できます。

クラスタ メンバ スイッチに専用の IP アドレスとコミュニティ ストリングが割り当てられている場合、クラスタ コマンド スイッチによるアクセスの他に、その IP アドレスとコミュニティ ストリングも使用できます。SNMP およびコミュニティ ストリングの詳細については、第 36 章「SNMP の設定」を参照してください。

図 6-7　　SNMP によるクラスタ管理



その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 7

スイッチ管理の実行

この章ではスイッチを管理するための 1 回限りの手順について説明しています。

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

スイッチ管理の実行に関する情報

システム日時の管理

ネットワーク タイム プロトコル（NTP）などの自動設定方式、または手動設定方式を使用して、スイッチのシステム日時を管理します。

システム クロック

時刻サービスの基準となるのはシステム クロックです。このクロックはシステムがスタートアップした瞬間から稼働し、日時を常時トラッキングします。

システム クロックは、次のソースにより設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

- ユーザの **show** コマンド
- ログおよびデバッグ メッセージ

システム クロックは、協定世界時（UTC）（別名グリニッジ標準時（GMT））に基づいてシステム内部の時刻を常時トラッキングします。ローカルのタイム ゾーンおよび夏時間に関する情報を設定することにより、時刻がローカルのタイム ゾーンに応じて正確に表示されるようにできます。

システム クロックは、時刻に*信頼性がある*かどうか（つまり、信頼できると見なされるタイム ソースによって時刻が設定されているか）を常時トラッキングします。信頼性のない場合は、時刻は表示目的でのみ使用され、再配信されません。設定については、「手動での日時の設定」（P.7-9）を参照してください。

ネットワーク タイム プロトコル

NTP は、ネットワーク上のデバイス間の時刻の同期化を目的に設計されています。NTP はユーザ データグラム プロトコル（UDP）で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 に規定されています。

NTP ネットワークは通常、ラジオ クロックやタイム サーバに接続された原子時計など、信頼できるタイム ソースからその時刻を取得します。NTP は、ネットワークにこの時刻を分配します。NTP はきわめて効率的で、1 分間に 1 パケットを使用するだけで、2 台のデバイスを 1 ミリ秒以内に同期化できます。

NTP は、*ストラタム（階層）*という概念を使用して、信頼できるタイム ソースとデバイスが離れている NTP ホップを記述します。ストラタム 1 タイム サーバには、ラジオ クロックまたは原子時計が直接接続されており、ストラタム 2 タイム サーバは、NTP を使用してストラタム 1 タイム サーバから時刻を取得します（以降のストラタムも同様です）。NTP が稼働するデバイスは、タイム ソースとして、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この方法によって、NTP 時刻配信の自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

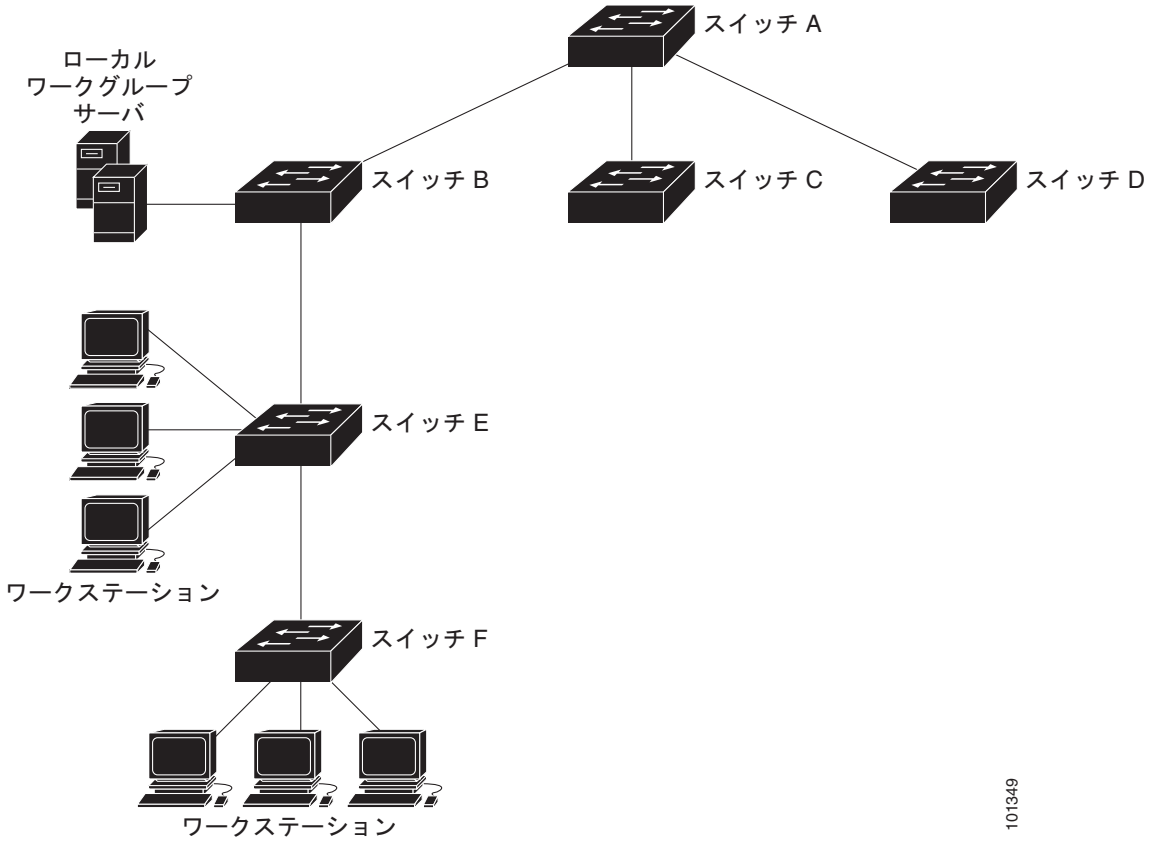
NTP が稼働するデバイス間の通信（*アソシエーション*）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤ってあるいは意図的に設定されることを防止してください。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

シスコの NTP ではストラタム 1 サービスをサポートしていないので、ラジオ クロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバから取得することを推奨します。

図 7-1 に、NTP を使用する一般的なネットワーク例を示します。スイッチ A は、NTP サーバ モードで設定したスイッチ B、C、D の NTP マスターです。スイッチ B、C、D とスイッチ A との間にはサーバ アソシエーションが設定されています。スイッチ E は、アップストリーム スイッチ（スイッチ B）およびダウンストリーム スイッチ（スイッチ F）の NTP ピアとして設定されています。

図 7-1　　一般的な NTP ネットワークの構成



ネットワークがインターネットから切り離されている場合、シスコの NTP によって、実際には、他の方法で時刻を学習しているにもかかわらず、デバイスが NTP を使用して同期化しているように動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

複数のタイム ソースがある場合は、NTP は常に、より信頼性があると見なされます。NTP の時刻は、他の方法による時刻に優先します。

自社のホスト システムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホスト システムも時間が同期化されます。

NTP バージョン 4

NTP バージョン 4 が、スイッチに実装されています。NTPv4 は NTP バージョン 3 の拡張版です。NTPv4 は IPv4 と IPv6 の両方をサポートし、NTPv3 との下位互換性があります。

NTPv4 は次の互換性を提供します。

- IPv6 のサポート。

- NTPv3 よりさらに向上したセキュリティ。NTPv4 プロトコルは、公開キー暗号化および標準 X509 認証に基づくセキュリティ フレームワークを提供します。
- ネットワークに対する時間分布ヒエラルキーの自動計算。特定のマルチキャスト グループを使用して、NTPv4 は、最も低い帯域幅コストで最高の時間精度を達成するサーバのヒエラルキーを自動的に設定します。この機能では、サイトローカル IPv6 マルチキャスト アドレスが活用されます。

NTPv4 設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Guide*』を参照してください。

DNS

ドメイン ネーム システム（DNS）プロトコルは、分散型データベース DNS を制御し、これによりホスト名を IP アドレスにマッピングできます。スイッチ上に DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドや、関連する Telnet サポート操作時に、IP アドレスの代わりにホスト名を使用できます。

IP によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com* となります。このドメイン内の特定のデバイス、たとえばファイル転送プロトコル（FTP）システムは、*ftp.cisco.com* で表されます。

IP ではドメイン名をトラッキングするために、ドメイン ネーム サーバという概念が定義されています。ドメイン ネーム サーバの役割は、名前から IP アドレスへのマッピングをキャッシュ（またはデータベース）に保存することです。ドメイン名を IP アドレスにマッピングするには、まず、ホスト名を明示し、ネットワーク上に存在するネーム サーバを指定し、DNS をイネーブルにします。

DNS のデフォルト設定

表 7-1 に、DNS のデフォルト設定を示します。

表 7-1　DNS のデフォルト設定

機能	デフォルト設定
DNS イネーブル ステート	イネーブル
DNS デフォルト ドメイン名	未設定
DNS サーバ	ネーム サーバのアドレスが未設定

ログイン バナー

今日のお知らせ（MOTD）バナーとログイン バナーを設定できます。MoTD バナーはログイン時に接続しているすべての端末で表示され、すべてのネットワーク ユーザに影響のあるメッセージ（システムのシャットダウン予告など）を送信するのに便利です。

ログイン バナーも、接続しているすべての端末で表示されます。表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

MoTD およびログイン バナーは設定されません。

システム名およびプロンプト

スイッチにシステム名を設定して特定します。デフォルトでは、システム名およびプロンプトは *Switch* です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字をシステム プロンプトとして使用します。大なり記号（>）が付加されます。システム名が変更されると、プロンプトは更新されます。

MAC アドレス テーブル

MAC アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

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

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、アドレスに対応付けられたポート番号、およびタイプ（スタティックまたはダイナミック）のリストです。

アドレス テーブル

すべてのポートでサポートされる複数の MAC アドレスによって、スイッチの任意のポートを各ワークステーション、リピータ、スイッチ、ルータ、あるいはその他のネットワークデバイスに接続できます。各ポートで受信するパケットの送信元アドレスを取得し、アドレス テーブルにアドレスとその対応するポート番号を追加することによって、スイッチは動的なアドレス指定を行います。ネットワークでステーションの増設または取り外しが行われると、スイッチはアドレス テーブルを更新し、新しいダイナミック アドレスを追加し、使用されていないアドレスは期限切れにします。

エージング間隔はグローバルに設定されます。ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、STP（スパニングツリー プロトコル）によって VLAN 単位で有効期間を短縮できます。

スイッチは、受信したパケットの宛先アドレスに基づいて、任意の組み合わせのポート間でパケットを送信します。MAC アドレス テーブルを使用することによって、スイッチは、宛先アドレスに対応付けられたポート（複数可）に限定してパケットを転送します。宛先アドレスがパケットを送信したポート上にある場合は、パケットはフィルタリング処理され、転送されません。スイッチは、常にストア アンド フォワード方式を使用します。このため、完全なパケットをいったん保存してエラーがないか検査してから伝送します。

MAC アドレスおよび VLAN

アドレスはすべて、VLAN と対応付けられます。1 つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定できます。たとえば、ユニキャスト アドレスを VLAN 1 のポート 1 および VLAN 5 のポート 9、10、1 に転送するといったことが可能です。

VLAN ごとに、独自の論理アドレス テーブルが維持されます。ある VLAN で認識されているアドレスが別の VLAN で認識されるには、別の VLAN 内のポートによって学習されるか、または別の VLAN 内のポートにスタティックに対応付けられる必要があります。

プライベート VLAN が設定されている場合、アドレス学習は次のように MAC アドレスのタイプに左右されます。

- プライベート VLAN の 1 つの VLAN で学習したダイナミック MAC アドレスは、関連 VLAN で複製されます。たとえば、プライベート VLAN のセカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN に複製されます。
- プライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは関連 VLAN には複製されません。プライベート VLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての関連 VLAN に設定する必要があります。

MAC アドレス テーブルのデフォルト設定

表 7-2　MAC アドレス テーブルのデフォルト設定

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

VLAN のアドレス エージング タイム

ダイナミック アドレスは、スイッチが学習し、使用されなくなると期限切れになる送信元 MAC アドレスです。すべての VLAN または指定された VLAN に対して、エージング タイムの設定を変更できます。

エージング タイムを短く設定しすぎると、アドレスが活用されないままテーブルから削除される可能性があります。その場合、スイッチは宛先が不明のパケットを受信すると、受信ポートと同じ VLAN 内のすべてのポートに、そのパケットをフラッディングさせます。この不必要なフラッディングによって、パフォーマンスに悪影響を及ぼす可能性があります。また、エージング タイムを長く設定しすぎると、アドレス テーブルが未使用のアドレスでいっぱいになり、これによって新しいアドレスを学習できなくなります。この結果フラッディングとなり、スイッチのパフォーマンスに悪影響を及ぼす可能性があります。

MAC アドレス変更通知トラップ

MAC アドレス変更通知は、MAC アドレス変更アクティビティを保存することでネットワーク上のユーザを追跡できます。スイッチが MAC アドレスを学習または削除すると、SNMP 通知トラップを NMS に送信させることができます。ネットワークから多数のユーザの出入りがある場合は、トラップ インターバル タイムを設定して通知トラップを組み込み、ネットワーク トラフィックを削減できます。MAC 通知履歴テーブルは、トラップが設定されたポートごとの MAC アドレス アクティビティを保存します。MAC アドレス変更通知は、ダイナミックまたはセキュア MAC アドレスに対してだけ生成されます。自アドレス、マルチキャスト アドレス、または他のスタティック アドレスについては、通知は生成されません。

スタティック アドレス

スタティック アドレスには、次の特性があります。

- アドレス テーブルへの追加およびアドレス テーブルからの削除は、手動で行う必要があります。
- ユニキャストまたはマルチキャスト アドレスとして設定できます。
- 期限切れになることはなく、スイッチが再起動しても維持されます。

スタティック アドレスを追加および削除でき、また、スタティック アドレスの転送動作を定義できます。転送動作は、パケットを受信したポートが、別のポートにパケットを転送する動作を決定します。ポートは必ず少なくとも 1 つの VLAN と対応しているので、スイッチは指定されたポートから、アドレスに対応する VLAN ID を取得します。送信元ポートごとに、宛先ポートのリストを別々に指定できます。

特定のアドレスがスタティックとして入力されていない VLAN に、そのスタティック アドレスを持つパケットが到着すると、すべてのポートにパケットがフラッディングされ、学習されません。

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

プライベート VLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての関連 VLAN に設定する必要があります。プライベート VLAN のプライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは関連 VLAN には複製されません。VLAN の詳細については、第 17 章「VLAN の設定」を参照してください。

ユニキャスト MAC アドレス フィルタリング

ユニキャスト MAC アドレス フィルタリングがイネーブルの場合、スイッチは、特定の送信元 MAC アドレスまたは宛先 MAC アドレスを持つパケットをドロップします。この機能はデフォルトではディセーブルで、ユニキャスト スタティック アドレスだけをサポートしています。

この機能を使用する場合は、次の注意事項に従ってください。

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

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

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

- CPU に転送されるパケットもサポートされません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、またはその MAC アドレスを持つパケットをドロップします。2 番めに入力したコマンドは、最初のコマンドを上書きします。

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

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

ユニキャスト MAC アドレス フィルタリングをイネーブルにして、スイッチが特定のアドレスを持つパケットをドロップするように設定するには、送信元または宛先ユニキャスト MAC アドレスおよび受信側の VLAN を指定します。

VLAN の MAC アドレス ラーニング

デフォルトでは、MAC アドレス ラーニングは、スイッチのすべての VLAN でイネーブルです。VLAN で MAC アドレス ラーニングを制御すると、MAC アドレスを学習できる VLAN、さらにポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。MAC アドレス ラーニングをディセーブルにする前に、ネットワーク トポロジとスイッチ システム設定に詳しいことを確認してください。VLAN で MAC アドレス ラーニングをディセーブルにすると、ネットワークでフラッディングを引き起こす可能性があります。

VLAN の MAC アドレス ラーニングをディセーブルにするときは、次の注意事項に従ってください。

- スイッチ仮想インターフェイス（SVI）スイッチを設定済みの VLAN で MAC アドレス ラーニングをディセーブルにする場合は、十分注意してください。この場合、スイッチはレイヤ 2 ドメインにすべての IP パケットをフラッディングします。
- MAC アドレス ラーニングは、1 つの VLAN ID（例：**no mac address-table learning vlan 223**）または VLAN ID の範囲（例：**no mac address-table learning vlan 1-20, 15**）でディセーブルにすることができます。
- MAC アドレス ラーニングのディセーブル化は、ポートを 2 つ含む VLAN だけで行うことを推奨します。3 つ以上のポートを含む VLAN で MAC アドレス ラーニングをディセーブルにした場合は、スイッチに着信するすべてのパケットは、その VLAN ドメインでフラッディングします。
- スイッチが内部的に使用する VLAN では、MAC アドレス ラーニングをディセーブルにできません。入力した VLAN ID が内部 VLAN である場合は、スイッチはエラーメッセージを生成してコマンドを拒否します。使用している内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。
- プライベート VLAN のプライマリ VLAN として設定された VLAN で MAC アドレス ラーニングをディセーブルにすると、MAC アドレスは、そのプライベート VLAN に属するセカンダリ VLAN 上で引き続き学習された後、プライマリ VLAN 上で複製されます。プライベート VLAN のプライマリ VLAN でなく、セカンダリ VLAN で MAC アドレス ラーニングをディセーブルにすると、MAC アドレス ラーニングはプライマリ VLAN 上で実行されてセカンダリ VLAN 上で複製されます。
- RSPAN VLAN で MAC アドレス ラーニングはディセーブルにできません。設定すること自体できません。
- セキュア ポートを含む VLAN で MAC アドレス ラーニングをディセーブルにする場合、そのポートで MAC アドレス ラーニングはディセーブルになりません。ポート セキュリティをディセーブルにすると、設定された MAC アドレス ラーニングの状態がイネーブルになります。

VLAN で MAC アドレス ラーニングを再びイネーブルにするには、**default mac address-table learning vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。**mac address-table learning vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用しても、VLAN で MAC アドレス ラーニングを再びイネーブルにできます。最初の（**default**）コマンドを使用するとデフォルト状態に戻るため、**show running-config** コマンドからの出力に設定が表示されません。2 番めのコマンドを使用すると、**show running-config** 特権 EXEC コマンド出力に設定が表示されます。

ARP テーブルの管理

デバイスと通信するには（イーサネット上のデバイスなど）、ソフトウェアは最初にそのデバイスの 48 ビット MAC アドレスまたはローカル データ リンク アドレスを学習する必要があります。IP アドレスからローカル データ リンク アドレスを学習するプロセスを、*アドレス解決*といいます。

アドレス解決プロトコル（ARP）は、ホスト IP アドレスを、該当するメディアまたは MAC アドレスおよび VLAN ID に対応付けます。IP アドレスを使用して、ARP は対応する MAC アドレスを見つけます。MAC アドレスが見つかると、IP と MAC アドレスとの対応を ARP キャッシュに格納し、すばやく検索できるようにします。その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求/応答については、サブネットワーク アクセス プロトコル（SNAP）で規定されています。IP インターフェイスでは、標準的なイーサネット形式の ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイネーブルに設定されています。

手動でテーブルに追加された ARP エントリは期限切れにならないので、手動で削除する必要があります。

スイッチ管理の実行方法

手動での日時の設定

他のタイム ソースが使用できない場合は、システムの再起動後、手動で日時を設定できます。時刻は、次にシステムを再起動するまで正確です。手動設定は最後の手段としてのみ使用することを推奨します。スイッチを同期化できる外部ソースがある場合は、手動でシステム クロックを設定する必要はありません。

システム クロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステム クロックを設定する必要はありません。

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

	コマンド	目的
ステップ 1	**clock set** *hh*:*mm*:*ss day month year* または **clock set** *hh*:*mm*:*ss month day year*	次のいずれかの形式で、手動でシステム クロックを設定します。 • *hh*:*mm*:*ss*：時間（24 時間形式）、分、秒を指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day*：月の日で日付を指定します。 • *month*：月を名前で指定します。 • *year*：年を指定します（常に 4 桁で指定）。

タイム ゾーンの設定

clock timezone グローバル コンフィギュレーション コマンドの **minutes-offset** 変数は、現地のタイム ゾーンと UTC との時差が分単位である場合に使用できます。たとえば、カナダ大西洋沿岸のある区域のタイム ゾーン（大西洋標準時（AST））は UTC-3.5 です。この場合、3 は 3 時間、.5 は 50% を意味します。この場合、必要なコマンドは **clock timezone AST -3 30** です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	時間帯を設定します。 スイッチは内部時刻を UTC で管理するので、このコマンドは表示目的の場合および手動で時刻を設定した場合に限って使用します。 • *zone*：標準時が適用されているときに表示されるタイム ゾーンの名前を入力します。デフォルトは UTC です。 • *hours-offset*：UTC からのオフセット時間数を入力します。 • （任意）*minutes-offset*：UTC からのオフセット分数を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

夏時間の設定

毎年特定の日に夏時間が開始および終了する地域に夏時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定された日に開始および終了する夏時間を設定します。 夏時間はデフォルトでディセーブルに設定されています。パラメータなしで **clock summer-time** *zone* **recurring** を指定すると、夏時間のルールは米国のルールをデフォルトにします。 • *zone*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 • （任意）*week*：月の何週目かを指定します（1 ～ 5、または **last**）。 • （任意）*day*：曜日を指定します（Sunday、Monday など）。 • （任意）*month*：月を指定します（January、February など）。 • （任意）*hh*:*mm*：時間と分で時刻（24 時間形式）を指定します。 • （任意）*offset*：夏時間の間、追加する分数を指定します。デフォルトは 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

夏時間の設定（正確な日付と時刻）

ユーザの居住地域の夏時間が定期的なパターンに従わない（次の夏時間の正確な日時を設定する）場合の設定では、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 • *zone*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 • （任意）*week*：月の何週目かを指定します（1 ～ 5、または **last**）。 • （任意）*day*：曜日を指定します（Sunday、Monday など）。 • （任意）*month*：月を指定します（January、February など）。 • （任意）*hh*:*mm*：時間と分で時刻（24 時間形式）を指定します。 • （任意）*offset*：夏時間の間、追加する分数を指定します。デフォルトは 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

システム名の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *name*	手動でシステム名を設定します。 デフォルト設定は *switch* です。 名前は ARPANET ホスト名のルールに従う必要があります。このルールではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。名前には 63 文字まで使用できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

DNS の設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip domain-name** *name*	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 起動時にはドメイン名は設定されていませんが、BOOTP または Dynamic Host Configuration Protocol（DHCP）サーバからスイッチ コンフィギュレーションを取得している場合は、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（サーバにこの情報が設定されている場合）。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバ アドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。スイッチは、最初にプライマリ サーバに DNS クエリーを送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 4	**ip domain-lookup**	（任意）スイッチで、DNS ベースのホスト名のアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 5	**end**	特権 EXEC モードに戻ります。

ログイン バナーの設定

MoTD ログイン バナーの設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner motd** *c message c*	MoTD を指定します。 • *c*：任意の区切り文字、たとえばポンド記号（#）を入力して、**Return** キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 • *message*：255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。

ログイン バナーの設定

接続されたすべての端末でログイン バナーが表示されるように設定できます。バナーが表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner login** *c message c*	ログイン メッセージを指定します。 • *c*：任意の区切り文字、たとえばポンド記号（#）を入力して、**Return** キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 • *message*：255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。

MAC アドレス テーブルの管理

アドレス エージング タイムの変更

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]	ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ～ 1000000 秒です。デフォルトは 300 です。0 を入力して期限切れをディセーブルにすることもできます。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 • *vlan-id*：指定できる ID の範囲は 1 ～ 4096 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

MAC アドレス変更通知トラップの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* : NMS の名前または IP アドレスを指定します。 • **traps**（デフォルト）: SNMP トラップをホストに送信します。 • **informs** : SNMP 情報をホストに送信します。 • サポートする SNMP バージョンを指定します。informs にはバージョン 1（デフォルト）を使用できません。 • *community-string* : 通知動作時に送信するストリングを指定します。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* : **mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification change**	スイッチが MAC アドレス変更通知を NMS に送信できるようにします。
ステップ 4	**mac address-table notification change**	MAC アドレス変更通知機能をイネーブルにします。
ステップ 5	**mac address-table notification change** [**interval** *value*] [**history-size** *value*]	トラップ インターバル タイムと履歴テーブルのサイズを入力します。 • （任意）**interval** *value* : NMS に生成されるトラップの各セット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ～ 2147483647 秒です。デフォルトは 1 秒です。 • （任意）**history-size** *value* : MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0 ～ 500 です。デフォルトは 1 です。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。

	コマンド	目的
ステップ 7	**snmp trap mac-notification change** {**added** | **removed**}	インターフェイス上で MAC アドレス変更通知トラップをイネーブルにします。 • MAC アドレスがインターフェイスに**追加された**場合にトラップをイネーブルにします。 • MAC アドレスがインターフェイスから**削除された**場合に MAC 通知トラップをイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。

MAC アドレス移動通知トラップの設定

MAC 移動通知を設定する場合は、MAC アドレスが、同じ VLAN 内のあるポートから別のポートに移動すると常に、SNMP 通知が生成されてネットワーク管理システムに送信されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* : NMS の名前または IP アドレスを指定します。 • **traps**（デフォルト）: ホストに SNMP トラップを送信します。 • **informs** : SNMP 情報をホストに送信します。 • **version** : サポートする SNMP バージョンを指定します。informs にはバージョン 1（デフォルト）を使用できません。 • *community-string* : 通知動作時に送信するストリングを指定します。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* : **mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification move**	スイッチが MAC アドレス移動通知トラップを NMS に送信できるようにします。
ステップ 4	**mac address-table notification mac-move**	MAC アドレス移動通知機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。

MAC しきい値通知トラップの設定

MAC しきい値通知を設定する場合は、MAC アドレス テーブルのしきい値の制限値に達するか、その値を超えると、SNMP 通知が生成されてネットワーク管理システムに送信されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* : NMS の名前または IP アドレスを指定します。 • **traps**（デフォルト）: ホストに SNMP トラップを送信します。 • **informs** : SNMP 情報をホストに送信します。 • **version** : サポートする SNMP バージョンを指定します。informs にはバージョン 1（デフォルト）を使用できません。 • *community-string* : 通知動作時に送信するストリングを指定します。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* : **mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification threshold**	スイッチによる MAC しきい値通知トラップの NMS への送信をイネーブルにします。
ステップ 4	**mac address-table notification threshold**	MAC アドレスしきい値通知機能をイネーブルにします。
ステップ 5	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]	MAC アドレスしきい値の使用状況モニタのしきい値を入力します。 • （任意）**limit** *percentage* : MAC アドレス テーブルの使用率を指定します。有効な値は 1 ～ 100 です。デフォルト値は 50% です。 • （任意）**interval** *time* : 通知間隔を指定します。有効な値は、120 秒以上です。デフォルトは 120 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。

スタティック アドレス エントリの追加および削除

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	MAC アドレス テーブルにスタティック アドレスを追加します。 • *mac-addr*：宛先 MAC ユニキャスト アドレスをアドレス テーブルに追加します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 • *vlan-id*：指定された MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4096 です。 • *interface-id*：受信したパケットの転送先インターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポート チャネルです。スタティック マルチキャスト アドレスの場合、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合、インターフェイスは同時に 1 つしか入力できません。ただし、同じ MAC アドレスおよび VLAN ID を指定すると、コマンドを複数回入力できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

ユニキャスト MAC アドレス フィルタリングの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、スイッチが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットをドロップするように設定します。 • *mac-addr*：送信元または宛先ユニキャスト MAC アドレスを指定します。この MAC アドレスを持つパケットはドロップされます。 • *vlan-id*：指定された MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4096 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

VLAN の MAC アドレス ラーニングのディセーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no mac address-table learning vlan** *vlan-id*	指定された 1 つまたは複数の VLAN で MAC アドレス ラーニングをディセーブルにします。1 つの VLAN ID を指定、または VLAN ID の範囲をハイフンまたはカンマで区切って指定できます。指定できる VLAN ID の範囲は 1 ～ 4096 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

スイッチ管理のモニタリングおよびメンテナンス

コマンド	目的
clear mac address-table dynamic	すべてのダイナミック エントリを削除します。
clear mac address-table dynamic address *mac-address*	特定の MAC アドレスを削除します。
clear mac address-table dynamic interface *interface-id*	指定された物理ポートまたはポート チャネル上のすべてのアドレスが削除されます。
clear mac address-table dynamic vlan *vlan-id*	特定の VLAN 上のすべてのアドレスが削除されます。
show clock [**detail**]	時刻と日付の設定を表示します。
show ip igmp snooping groups	すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャスト エントリを表示します。
show mac address-table address	指定された MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table learning	すべての VLAN または指定した VLAN の MAC アドレス ラーニングのステータスを表示します。
show mac address-table notification	MAC 通知パラメータおよび履歴テーブルを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

スイッチ Admininistration を実行する場合のコンフィギュレーション例

システム クロックの設定例

次に、システム クロックを手動で 2001 年の 7 月 23 日午後 1 時 32 分に設定する例を示します。

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

夏時間：例

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

次に、夏時間が、4 月の第 1 日曜日の 02:00 に開始し、10 月の最終日曜日の 02:00 で終了するように指定する例を示します。

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

次に、夏時間が 2000 年 10 月 12 日の 2 時に始まり、2001 年 4 月 26 日の 2 時に終わるように設定する例を示します。

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

MOTD バナーの設定：例

次に、ポンド記号（#）を開始および終了の区切り文字として使用し、スイッチの MoTD バナーを設定する例を示します。

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

次に、前の設定により表示されたバナーの例を示します。

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

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

User Access Verification

Password:
```

ログイン バナーの設定：例

次に、ドル記号（$）を開始および終了の区切り文字として使用し、スイッチのログイン バナーを設定する例を示します。

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

設定の MAC アドレス変更通知トラップ：例

次に、NMS として 172.20.10.10 を指定し、スイッチによる NMS への MAC アドレス通知トラップの送信をイネーブルにし、MAC アドレス変更通知機能をイネーブルにし、インターバル タイムを 123 秒に設定し、履歴サイズを 100 エントリに設定し、特定のポートで MAC アドレスが追加された場合のトラップをイネーブルにする例を示します。

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

Switch(config-if)# snmp trap mac-notification change added
```

MAC アドレス移動通知トラップの送信：例

次に、NMS として 172.20.10.10 を指定し、スイッチによる NMS への MAC アドレス移動通知トラップの送信をイネーブルにし、MAC アドレス移動通知機能をイネーブルにし、あるポートから別のポートに MAC アドレスが移動した場合にトラップをイネーブルにする例を示します。

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

設定 MAC しきい値通知トラップ：例

次に、NMS として 172.20.10.10 を指定し、MAC アドレスしきい値通知機能をイネーブルにし、インターバル タイムを 123 秒に設定し、制限を 78% に設定する例を示します。

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

MAC アドレス テーブルにスタティック アドレスを追加：例

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

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

設定するユニキャスト MAC アドレス フィルタリング：例

次の例では、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つパケットをドロップするようにスイッチを設定する方法を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS ルーティング コマンド	『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 8

PTP の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

PTP の設定の前提条件

- この機能を使用するには、スイッチが PTP に対応している必要があります。スイッチのリリース ノートを参照してください。

PTP の設定に関する制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

PTP の設定に関する情報

高精度時間プロトコル

IEEE 1588 標準では、ネットワーク上のリアルタイム クロックのフォールトトレラント同期の PTP の使用について記述されています。

PTP ネットワークのクロックは、マスター / スレーブ階層で構成されています。グランドマスター クロックはベスト マスター クロック（BMC）と呼ばれ、マスター / スレーブ クロック階層のルートです。PTP は同期するマスター クロックの識別に BMC アルゴリズムを使用します。

マスター クロックは、Global Positioning System（GPS）クロックなどの正確な時刻源と同期できる、ネットワークの時刻源です。スレーブは、マスター クロックに自分のクロックを同期する他のネットワーク デバイスです。親は、メンバのスレーブ クロックが同期するクロックです。マスター クロックとスレーブ クロック間のタイミング メッセージは、継続的な同期を保証します。

同期動作は、スイッチで設定する PTP クロック設定モードによって異なります。モードには、境界、エンドツーエンド トランスペアレント、または転送があります。

- 境界モードのスイッチ クロックは、最も正確なマスター クロックの選択に参加します。より正確なクロックが検出されない場合、そのスイッチ クロックがマスター クロックになります。スレーブ クロック間でより正確なクロックが検出された場合、スイッチはそのクロックに同期し、スレーブ クロックになります。最初の同期のあと、スイッチと接続済み装置は、タイミング メッセージを交換して、クロックのオフセットとネットワークの遅延による時間の変更を修正します。
- エンドツーエンド トランスペアレント モードのスイッチ クロックは、すべてのスイッチ ポートをマスター クロックに同期します。このスイッチは、マスター クロックの選択に参加せず、すべてのポートでデフォルト PTP クロック モードを使用します。
- 転送モードのスイッチ クロックにより、受信 PTP パケットがスイッチを通常のマルチキャスト トラフィックとしてパススルーできるようにします。

スイッチが PTP 転送モードの場合、PTP モードを他のモードに変更する場合を除き、PTP 設定を使用することはできません。スイッチが境界モードの場合は、ポート単位の PTP だけを設定できます。

PTP の設定方法

PTP のデフォルト設定

デフォルトでは、ベース スイッチ モジュールのすべてのファスト イーサネット ポートおよびギガビット イーサネット ポートで PTP がイネーブルになっています。すべてのポートにおけるデフォルトの PTP モードは、エンドツーエンド トランスペアレントです。

表 8-1　PTP のデフォルト設定

機能	デフォルト設定
PTP 境界モード	ディセーブル
PTP 転送モード	ディセーブル
PTP エンドツーエンド トランスペアレント モード	イネーブル
PTP プライオリティ 1 および PTP プライオリティ 2	デフォルトのプライオリティ番号は 128 です。
PTP アナウンス間隔	2 秒
PTP アナウンス受信タイムアウト	3 アナウンス間隔
PTP 遅延要求間隔	32 秒
PTP 同期間隔	1 秒
PTP 同期制限	500000000 ナノ秒

PTP の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ptp** {**announce** {**interval** *value* | **timeout** *value*} | **delay-req interval** *value* | **enable** | **sync** {**interval** *value* | **limit** *value*}}	タイミング メッセージの設定を指定します。これらのオプションは、スイッチが境界モードの場合にのみ使用できます。 • **announce interval** *value*：アナウンス メッセージを送信する時間を設定します。指定できる範囲は 0 ～ 4 秒です。デフォルトは 1（2 秒）です。 • **announce timeout** *value*：タイムアウト メッセージをアナウンスする時間を設定します。指定できる範囲は 2 ～ 10 秒です。デフォルトは 3（8 秒）です。 • **delay-req interval** *value*：ポートがマスター クロック状態の場合に、スレーブ デバイスが遅延要求メッセージを送信する時間を設定します。指定できる範囲は -1 ～ 6 秒です。デフォルトは 5（32 秒）です。 • **enable**：ポート ベースのモジュールで PTP をイネーブルにします。 • **sync interval** *value*：同期メッセージを送信する時間を設定します。入力できる範囲は –1 ～ 1 秒です。デフォルト値は 1 秒です。 • **sync limit** *value*：PTP が再同期を試みるまでの、最大クロック オフセット値を設定します。範囲は 50 ～ 500000000 ナノ秒です。デフォルトは 500000000 ナノ秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PTP 設定のモニタリングおよびメンテナンス

表 8-2　PTP 設定を表示するためのコマンド

コマンド	目的
show ptp clock	PTP クロック プロパティを表示します。
show ptp foreign-master-record	PTP 外部マスター データ セットを表示します。
show ptp parent	親およびグランドマスター クロックのプロパティを表示します。
show ptp port	すべての PTP ポート プロパティを表示します。
show ptp port FastEthernet *interface*	指定したポートの PTP FastEthernet プロパティを表示します。
show ptp port GigabitEthernet *interface*	指定したポートの PTP ギガビット イーサネット プロパティを表示します。
show ptp time-property	PTP 時間プロパティを表示します。

PTP 設定のトラブルシューティング

表 8-3　PTP 設定をトラブルシューティングするためのコマンド

コマンド	目的
debug ptp bmc	PTP ベスト マスター クロック アルゴリズムのデバッグをイネーブルにします。
debug ptp clock-correction	PTP クロック修正のデバッグをイネーブルにします。
debug ptp collision	PTP ソースの衝突のデバッグをイネーブルにします。
debug ptp error	PTP エラーのデバッグをイネーブルにします。
debug ptp event	PTP ステート イベントのデバッグをイネーブルにします。
debug ptp messages	PTP メッセージのデバッグをイネーブルにします。
debug ptp transparent-clock	PTP トランスペアレント クロックのデバッグをイネーブルにします。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 9

PROFINET の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

PROFINET の設定に関する制約事項

このスイッチでは、等時間隔のリアルタイム通信チャネルはサポートされていません。

PROFINET の設定に関する情報

PROFINET は PROFIBUS International（PI）のオープンな工業イーサネット標準であり、オートメーション コントロール用に TCP/IP および IT 標準を使用しています。PROFINET は、装置およびテスト機器の動きや精度の制御が重要である工業オートメーション システムやプロセス制御ネットワークに特に有用です。PROFINET はデータ交換を重視しており、速度要件に合った通信パスを定義しています。PROFINET 通信は、次の 3 つの点でスケーラブルです。

- 標準の非リアルタイム通信では TCP/IP を使用し、約 100 ms のバス サイクル タイムが実現されます。
- リアルタイム通信では、約 10 ms のサイクル タイムが実現されます。
- 等時間隔のリアルタイム通信では、約 1 ms のサイクル タイムが実現されます。

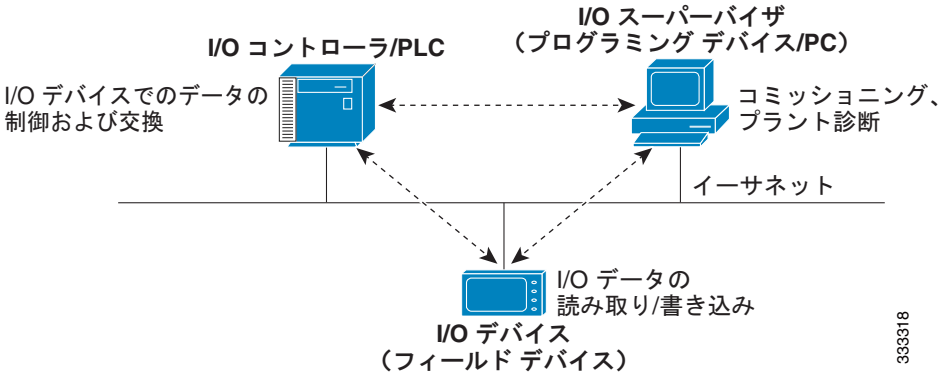
PROFINET I/O は、分散型オートメーション アプリケーション用のモジュラ通信フレームワークです。PROFINET I/O は巡回型のデータ転送を使用して、プログラマブル コントローラ、入力/出力（I/O）装置、およびその他のオートメーション コントローラ（モーション コントローラなど）とデータ、アラーム、診断情報を交換します。

PROFINET I/O は、次の 3 つのクラスの装置を認識します。

- I/O デバイス
- I/O コントローラ
- I/O スーパーバイザ

PROFINET 装置の役割

図 9-1　PROFINET 装置の役割



I/O コントローラは I/O 装置を制御するプログラマブル ロジック コントローラ（PLC）であり、オートメーション プログラムを通して設定、アラーム、I/O データなどのデータを交換します。I/O コントローラと I/O のスーパーバイザは診断情報を交換します。I/O コントローラは I/O 装置と設定や入力/出力情報を共有し、I/O 装置からアラームを受信します。

PROFINET は、唯一またはプライマリの管理システムとして使用するよう設計されています。I/O コントローラが Discovery and Configuration Protocol（DCP）でスイッチを検出し、デバイス名と IP アドレスを設定するため、基本的な設定に Cisco IOS コマンドを入力する必要はありません。拡張設定（QoS や DHCP などの機能）を行うには、スイッチ上で Cisco IOS コマンドを使用する必要があります。PROFINET を使用して、これらの機能の設定はできません。

I/O スーパーバイザはヒューマン マシン インターフェイス（HMI）や PC などのエンジニアリング ステーションであり、コミッショニング、モニタリング、診断分析に使用されます。I/O スーパーバイザは I/O 装置と診断情報、ステータス情報、制御情報、パラメータ情報を交換します。

I/O 装置は、センサー、アクチュエータ、モーション コントローラなどの分散型入力/出力装置です。

（注）　スイッチは I/O 装置として動作し、I/O コントローラへの PROFINET 管理接続を行います。

PROFINET I/O システムでは、バス サイクル タイム 100 ms 未満のオートメーション産業要件を満たすため、すべての I/O 装置がイーサネット通信ネットワークを介して通信します。このネットワークでは、データの衝突を避けるため、スイッチと全二重データ交換が使用されます。

PROFINET 装置のデータ交換

PROFINET が DCP を使用してスイッチなどの装置を検出すると、アプリケーション関係（AR）および通信関係（CR）が確立されます。接続が確立され、装置パラメータに関する情報が交換されたら、入力データと出力データが交換されます。スイッチは非リアルタイム CR を使用して、表 9-1 および表 9-2 に示すデータ属性を交換します。

表 9-1　PROFINET I/O スイッチ属性

PROFINET I/O スイッチ設定属性	値またはアクション
デバイス名	デバイス名を設定します。
TCP/IP	IP アドレス、サブネット マスク、デフォルト ゲートウェイ、SVI。
プライマリ温度アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
セカンダリ温度アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
RPS 障害アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
リレー メジャー アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
出荷時デフォルトへのリセット	PROFINET I/O コントローラを使用して、スイッチを出荷時デフォルトにリセットします。このアクションにより、スタートアップ コンフィギュレーションが削除され、スイッチがリロードされます。
リレー メジャー設定	メジャー リレーをトリガーするポート アラーム（リンク障害など）のタイプを指定します。指定したアラーム タイプで設定された任意のポートがメジャー リレーをトリガーできます。

表 9-2　PROFINET I/O ポート属性

PROFINET I/O ポート設定属性	値またはアクション
速度	10、100、1000、自動。
二重	半二重 / 全二重 / 自動。
ポート モード	アクセス / トランク。
リンク ステータス	シャットダウン / シャットダウンなし。
設定レートの制限	ブロードキャスト、ユニキャスト、マルチキャストのしきい値が設定されたレベルを超えています。
ポート リンク障害アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
Port not forwarding アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
Port not operating アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。
ポート FCS しきい値アラーム	指定したアラームのモニタリングをイネーブルまたはディセーブルにします。

PROFINET 装置は General Station Description（GSD）ファイルを使用して統合されます。このファイルには、エンジニアリング用のデータや、I/O コントローラ、I/O スーパーバイザ、および I/O 装置（スイッチなど）間のデータ交換用のデータが含まれています。各 PROFINET I/O フィールド装置には、装置のプロパティが記述され、設定に必要な次の情報がすべて含まれた GSD ファイルが関連付けられている必要があります。

- 装置 ID 情報（装置 ID、ベンダー ID およびベンダー名、製品ファミリ、ポート数）。
- 着脱可能モジュールの数およびタイプ。

- Cisco IE 2000 8 ポート拡張モジュールはホットスワップ可能ではありません。拡張モジュールの接続や切断を行う前に、スイッチをオフにしてください。
- 診断情報のエラー テキスト。
- I/O 装置の通信パラメータ（最小サイクル タイム、リダクション比率、ウォッチ ドッグ タイムなど）。

（注）　Cisco IE 2000 スイッチのデフォルトのリダクション比率は 128 ms ですが、スイッチに複雑な設定を使用する場合は、スイッチの CPU に対する負荷を減らすため、リダクション比率を 256 ms または 512 ms にすることを推奨します。

- I/O 装置モジュールに関する設定データ（速度、デュプレックス、VLAN、ポート セキュリティ情報、アラーム、ブロードキャスト レート制限のしきい値など）。
- 表 9-2 にリストされた属性に対して設定された、I/O 装置モジュールのパラメータ。

GSD ファイルはスイッチに関するものですが、I/O スーパーバイザはこのファイルを使用します。

（注）　PROFINET ネットワークを管理するには、スイッチ上の Cisco IOS Release と関連付けられた GSD ファイルを使用する必要があります。I/O スーパーバイザと Cisco IOS ソフトウェアはどちらも、GSD ファイルとスイッチの Cisco IOS ソフトウェア バージョン間の不一致を通知します。

PROFINET の設定方法

PROFINET の設定

基本的なスイッチ設定には、I/O スーパーバイザ上の PROFINET ソフトウェアか Cisco IOS ソフトウェアのいずれかを使用できます。

デフォルト コンフィギュレーション

PROFINET はすべてのベース スイッチ モジュールおよび拡張ユニットのイーサネット ポート上で、デフォルトでイネーブルになっています。PROFINET がディセーブルになっている場合は、「PROFINET のイネーブル化」（P.9-4）の手順に従ってください。

PROFINET のイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**profinet**	スイッチ上で PROFINET をイネーブルにします。

	コマンド	目的
ステップ 3	**profinet id** *line*	（任意）Cisco IOS ソフトウェアを使用して PROFINET 装置 ID を設定します。 最大長は 240 文字です。使用可能な特殊文字はピリオド（.）とハイフン（-）のみです。これらの文字は ID 文字列内の特定のオプションでのみ使用可能です。文字列内には複数のラベルを含めることができます。各ラベルに使用できる文字数は 1 ～ 63 文字です。複数のラベルはピリオド（.）で区切る必要があります。文字列内の末尾文字はゼロ（0）にしないでください。 PROFINET ID の設定の詳細については、PROFINET の仕様、文書番号 TC2-06-0007a、ファイル名 PN-AL-protocol_2722_V22_Oct07 を参照してください（PROFIBUS から入手できます）。
ステップ 4	**profinet vlan** *vlan id*	（任意）VLAN 番号を変更します。デフォルトの VLAN 番号は 1 です。指定できる VLAN ID の範囲は 1 ～ 4096 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PROFINET のモニタリングおよびメンテナンス

表 9-3　PROFINET の設定を表示するためのコマンド

コマンド	目的
show profinet sessions	現在接続されている PROFINET セッションを表示します。
show profinet status	PROFINET サブシステムのステータスを表示します。

PROFINET のトラブルシューティング

PLC の LED はアラームが発生すると赤になり、I/O スーパーバイザのソフトウェアはこれらのアラームをモニタします。

PROFINET のトラブルシューティングを行うには、**debug profinet** 特権 EXEC コマンドを使用し、表 9-4 に示すキーワードを指定します。**debug** コマンドの出力により、シリアル リンクにエラーが発生する可能性があるので注意してください。これらのコマンドを使用する際には、必ずシスコのテクニカル サポートのエンジニアの指示に従ってください。このコマンドの使用時には、シリアル ポートではなくイーサネットを使用して、Telnet で Cisco IOS のコマンドライン インターフェイス（CLI）にアクセスしてください。

表 9-4　PROFINET の設定をトラブルシューティングするためのコマンド

コマンド	目的
debug profinet alarm	アラーム ステータス（オンまたはオフ）と PROFINET アラームの内容を表示します。
debug profinet cyclic	タイム サイクル ベースの PROFINET イーサネット フレームに関する情報を表示します。
debug profinet error	PROFINET セッション エラーを表示します。

表 9-4　PROFINET の設定をトラブルシューティングするためのコマンド （続き）

コマンド	目的
debug profinet packet ethernet	PROFINET イーサネット パケットに関する情報を表示します。
debug profinet packet udp	PROFINET Upper Layer Data Protocol（UDP）パケットに関する情報を表示します。
debug profinet platform	Cisco IOS と PROFINET 間の連携に関する情報を表示します。
debug profinet topology	受信した PROFINET トポロジ パケットを表示します。
debug profinet trace	トレースした一連のデバッグ出力ログを表示します。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 10

CIP の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

CIP の設定に関する制約事項

CIP はスイッチの VLAN で 1 つのみイネーブルにできます。

CIP の設定に関する情報

Common Industrial Protocol（CIP）は、産業オートメーション アプリケーション用の産業プロトコルです。DeviceNet、EtherNet/IP、CIP Safety および CIP sync などの CIP に基づいたネットワーク テクノロジーをサポートする組織である、Open DeviceNet Vendors Association（ODVA）によってサポートされます。

これまで制御および情報プロトコルとして知られていましたが、CIP は、制御、安全、時間同期、モーション、設定、情報、といった産業オートメーション アプリケーション向けのメッセージとサービスを包括的に網羅しています。これらの産業用アプリケーションは CIP によって、エンタープライズレベルのイーサネットやインターネットに統合することができます。

CIP の設定方法

デフォルト コンフィギュレーション

デフォルトでは、CIP はディセーブルになります。

CIP のイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cip security** {**password** *password* | **window timeout** *value*}	スイッチに CIP セキュリティ オプションを設定します。
ステップ 3	**interface vlan 20**	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cip enable**	VLAN 上で CIP をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

CIP のモニタリング

表 10-1　CIP 設定を表示するためのコマンド

コマンド	目的
show cip {**connection** | **faults** | **file** | **miscellaneous** | **object** | **security**| **session** | **status**}	CIP サブシステムに関する情報を表示します。

CIP のトラブルシューティング

表 10-2　CIP の設定をトラブルシューティングするためのコマンド

コマンド	目的
debug cip {**assembly** | **connection manager** | **errors** | **event** | **file** | **io** | **packet** | **request response** | **security** | **session** | **socket**}	CIP サブシステムのデバッグをイネーブルにします。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Express Setup による CIP 設定	『*Cisco IE 2000 Switch Getting Started Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 11

SDM テンプレートの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SDM テンプレートの設定の前提条件

設定された SDM テンプレートを適用でするには、**reload** 特権 EXEC コマンドを入力する必要があります。

SDM テンプレートの設定に関する制約事項

- IPv6 ルーティングをサポートするには、スイッチで LAN Base イメージを実行している必要があります。
- SDM テンプレートの選択と設定を行う際、設定を有効にするため、スイッチをリロードする必要があります。
- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 機能を設定しようとすると、警告メッセージが生成されます。
- デュアル スタック テンプレートを使用すると、リソースごとに使用可能な TCAM 容量が少なくなるため、IPv4 トラフィックだけを転送する場合は、このテンプレートを使用しないでください。

SDM テンプレートの設定に関する情報

SDM テンプレート

ネットワークでのスイッチの使用状況に応じて、SDM テンプレートを使用して、特定の機能に対するサポートを最適化するようにスイッチのシステム リソースを設定できます。

一部の機能にシステムを最大限に利用させるようにテンプレートを選択したり、デフォルト テンプレートを使用してリソースを均衡化することができます。

Ternary CAM（TCAM）リソースをさまざまな用途に割り当てるために、スイッチ SDM テンプレートはシステム リソースにプライオリティを設定して、特定の機能のサポートを最適化します。LAN Base イメージを実行すると、次の機能を最適化するために SDM テンプレートを選択することができます。

- デフォルト：デフォルト テンプレートでは、レイヤ 2 のすべての機能に対してリソースを均衡化します。
- デュアル IPv6 および IPv6：デュアル スタック環境でスイッチを使用できるようになります（IPv4 と IPv6 の両方をサポート）。
- LAN Base ルーティング：ルーティング テンプレートは、一般的に、ネットワークの中心にあるルータまたはアグリゲータで必要となります。IPv4 ユニキャスト ルーティングに対して、システム リソースを最大化します。

「デュアル IPv4/IPv6 SDM デフォルト テンプレート」（P.11-3）を参照してください。

（注）　LAN Lite イメージを実行するスイッチはデフォルト SDM テンプレートだけをサポートします。

表 11-1　IPv4 テンプレートによって許容される機能リソースの概算

リソース	デフォルト
ユニキャスト MAC アドレス	12 K
インターネット グループ管理プロトコル（IGMP）グループおよびマルチキャスト ルート	1 K
IPv4 ユニキャスト ルート	0
ポリシーベース ルーティング アクセス コントロール エントリ（ACE）	0
IPv4 または MAC QoS ACE	0.75 K
IPv4 または MAC セキュリティ ACE	1 K

表 11-2　各テンプレートに割り当てられた機能のリソースの概算

リソース	デフォルト	QoS	ルーティング
ユニキャスト MAC アドレス	8 K	8 K	2 K
IGMP グループとマルチキャスト ルート	256	256	1 K
ユニキャスト ルート	0		4 K
• ホストに直接接続	0		2 K
• 間接ルート	0		2 K
ポリシーベース ルーティング ACE	0		512
QoS 分類 ACE	375	625	625
セキュリティの ACE	375	125	375 K
Layer 2 VLANs	1 K	1 K	1 K

表の最初の 8 行（ユニキャスト MAC アドレスからセキュリティ ACE まで）は、各テンプレートが選択されたときに設定されるハードウェアのおおよその限度を表します。ハードウェア リソースのある部分がいっぱいの場合は、処理のオーバーフローはすべて CPU に送られ、スイッチのパフォーマンスに重大な影響が出ます。最後の行は、スイッチのレイヤ 2 VLAN の数に関連するハードウェア リソース消費量を計算するための目安です。

デュアル IPv4/IPv6 SDM デフォルト テンプレート

IP バージョン 6（IPv6）スイッチングをサポートするために SDM テンプレートを選択できます。IPv6 の詳細および IPv6 ルーティングの設定手順については、第 41 章「スタティック IP ユニキャスト ルーティングの設定」を参照してください。

このソフトウェア リリースは、IPv6 トラフィック転送時に Policy-Based Routing（PBR）をサポートしません。**dual-ipv4-and-ipv6 routing** テンプレートが設定されている場合に限り、このソフトウェアは IPv4 PBR をサポートします。

デュアル IPv4/IPv6 テンプレートを使用することにより、（IPv4 と IPv6 の両方をサポートする）デュアル スタック環境でスイッチを使用できるようになります。デュアルスタック テンプレートを使用すると、各リソースで使用可能な TCAM 容量が少なくなります。IPv4 トラフィックだけを転送する場合は、このテンプレートを使用すべきではありません。

次に示す SDM テンプレートは、IPv4 および IPv6 環境をサポートしています。

- デュアル IPv4/IPv6 デフォルト テンプレート：IPv4 の場合はレイヤ 2、QoS、および ACL をサポートし、IPv6 の場合は、レイヤ 2、IPv6 ホスト、および ACL をサポートします。
- デュアル IPv4/IPv6 ルーティング テンプレート：IPv4 の場合は、レイヤ 2、マルチキャスト、ルーティング（ポリシーベース ルーティングを含む）、QoS、および ACL をサポートし、IPv6 の場合はレイヤ 2、ルーティング、および ACL をサポートします。

（注）　IPv4 ルートに必要なのは、1 つの TCAM エントリだけです。IPv6 ではハードウェア圧縮方式が使用されるため、IPv6 ルートは複数の TCAM エントリを使用することができ、ハードウェアで転送されるエントリ数が削減されます。たとえば、IPv6 によって直接接続された IP アドレスの場合、デスクトップ テンプレートで使用可能なエントリ数は 2000 未満になります。

表 11-3　デュアル IPv6/IPv6 テンプレートによって許容される機能リソースの概算[1]

リソース	IPv4 および IPv6 のデフォルト	IPv4 および IPv6 のルーティング
ユニキャスト MAC アドレス	8 K	1 K
IPv4 IGMP グループおよびマルチキャスト ルート	0.25 K	0. 5 K
IPv4 ユニキャスト ルートの合計：	0	2 K
• IPv4 ホストに直接接続	0	1 K
• 間接 IPv4 ルート	0	1 K
IPv6 マルチキャスト グループ	0.375 K	0.625 K
IPv6 ユニキャスト ルートの合計：	0	1.375 K
• 直接接続された IPv6 アドレス	0	1 K
• 間接 IPv6 ユニキャスト ルート	0	0.375 K

表 11-3　デュアル IPv6/IPv6 テンプレートによって許容される機能リソースの概算[1]（続き）

リソース	IPv4 および IPv6 のデフォルト	IPv4 および IPv6 のルーティング
IPv4 ポリシー ベース ルーティング ACE	0	0.125 K
IPv4 または MAC QoS ACE（合計）	0.375 K	0.375 K
IPv4 または MAC セキュリティの ACE（合計）	0.375 K	0.125 K
IPv6 ポリシー ベース ルーティング ACE[2]	0	0.125 K
IPv6 QoS ACE	0	0.125 K
IPv6 セキュリティの ACE	0.125 K	0.125 K

1. この見積もりには、8 つのルーテッド インターフェイス、約 1000 個の VLAN が設定されたスイッチを使用しています。
2. IPv6 ポリシーベース ルーティングはサポートされません。

スイッチ SDM テンプレート機能の設定方法

SDM テンプレートの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer** {**default** | **dual-ipv4-and-ipv6** {**default**} | **lanbase-routing**}	スイッチで使用する SDM テンプレートを指定します。 • **default**：すべての機能に均等にリソースを割り当てます。 • **dual-ipv4-and-ipv6**：IPv4/IPv6 ルーティングの両方をサポートするテンプレートを選択します。 – **default**：IPv4/IPv6 のレイヤ 2 機能を均衡化します。 • **lanbase-routing**：スイッチでの IPv4 ルーティングを最大化します。 スイッチをデフォルト テンプレートに設定するには、**no sdm prefer** コマンドを使用します。デフォルト テンプレートは、システム リソースを均等に割り当てます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**reload**	オペレーティング システムをリロードします。

SDM テンプレートのモニタリングおよびメンテナンス

次に、**show sdm prefer default** コマンドの出力例を示します。

```
Switch# show sdm prefer default
 "default" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  8K
  number of IPv4 IGMP groups:                       0.25K
  number of IPv4/MAC qos aces:                      0.375k
  number of IPv4/MAC security aces:                 0.375k
```

次に、**show sdm prefer dual-ipv4-and-ipv6 default** コマンドの出力例を示します。

```
Switch# show sdm prefer dual-ipv4-and-ipv6 default
 "dual-ipv4-and-ipv6 default" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  7.5K
  number of IPv4 IGMP groups + multicast routes:    0.25K
  number of IPv4 unicast routes:                    0
  number of IPv6 multicast groups:                  0.375k
  number of directly-connected IPv6 addresses:      0
  number of indirect IPv6 unicast routes:           0
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.375k
  number of IPv4/MAC security aces:                 0.375k
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0
  number of IPv6 security aces:                     0.125k
```

次に、**show sdm prefer lanbase-routing** コマンドの出力例を示します。

```
Switch# show sdm prefer lanbase-routing
 "lanbase-routing" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1005 VLANs.

  number of unicast mac addresses:                  4K
  number of IPv4 IGMP groups + multicast routes:    0.25K
  number of IPv4 unicast routes:                    4.25K
    number of directly-connected IPv4 hosts:        4K
    number of indirect IPv4 routes:                 0.25K
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.375k
  number of IPv4/MAC security aces:                 0.375k
```

SDM テンプレートの設定例

デュアル IPv4/IPv6 デフォルト テンプレート設定：例

次に、デスクトップ スイッチに IPv4/IPv6 デフォルト テンプレートを設定する例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
Proceed with reload? [confirm]
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 12

スイッチ ベース認証の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

スイッチ ベース認証設定の前提条件

- SDM テンプレートを設定してから、**show sdm prefer** コマンドを実行すると、現在使用中のテンプレートが表示されます。
- 設定された SDM テンプレートを適用でするには、**reload** 特権 EXEC コマンドを入力する必要があります。
- スイッチ上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。
- 最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウンティングの方式リストを定義できます。

スイッチ ベース認証の設定に関する制約事項

- RADIUS CoA インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定されたセッションにだけ作用します。
- セキュア シェルを使用するには、暗号（暗号化）ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

スイッチ ベース認証の設定に関する情報

スイッチへの無許可アクセスの防止

不正ユーザによる、スイッチの再設定や設定情報の閲覧を防止できます。一般的には、ネットワーク管理者からスイッチへのアクセスを許可する一方、非同期ポートを用いてネットワーク外からダイヤルアップ接続するユーザや、シリアル ポートを通じてネットワーク外から接続するユーザ、またはローカル ネットワーク内の端末またはワークステーションから接続するユーザによるアクセスを制限します。

スイッチへの不正アクセスを防止するには、次のセキュリティ機能を 1 つまたは複数設定します。

- 最低限のセキュリティとして、各スイッチ ポートでパスワードおよび権限を設定します。このパスワードは、スイッチにローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。
- 追加のセキュリティ レイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。
- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティ サーバ上のデータベースに保存できます。これにより、複数のネットワーキング デバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。
- また、失敗したログイン試行をログに記録するログイン拡張機能もイネーブルにすることもできます。ログイン拡張は、設定した回数のログインが失敗したあとに、それ以降のログイン試行をブロックするために設定することもできます。

パスワード保護

ネットワークで端末のアクセス コントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワーク デバイスへのアクセスが制限されます。権限レベルによって、ネットワーク デバイスにログイン後、ユーザがどのようなコマンドを使用できるかが定義されます。

デフォルトのパスワードおよび権限レベル設定

表 12-1　デフォルトのパスワードおよび権限レベル設定

機能	デフォルト設定
イネーブル パスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、コンフィギュレーション ファイル内では暗号化されていない状態です。

表 12-1　デフォルトのパスワードおよび権限レベル設定 （続き）

機能	デフォルト設定
イネーブル シークレット パスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、暗号化されてからコンフィギュレーション ファイルに書き込まれます。
回線パスワード	パスワードは定義されていません。

シークレット パスワード暗号化のイネーブル

追加のセキュリティ レイヤを、特にネットワークを越えるパスワードや TFTP サーバに保存されているパスワードに対して設定する場合には、**enable password** または **enable secret** グローバル コンフィギュレーション コマンドを使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード（デフォルト設定）または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

特定の権限レベルのパスワードを定義する場合は、**level** キーワードを使用します。レベルを指定してパスワードを設定したあと、特権レベルにアクセスする必要のあるユーザだけに、パスワードを通知してください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、**privilege level** グローバル コンフィギュレーション コマンドを使用します。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブル コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

パスワードとレベルを削除するには、**no enable password** [**level** *level*] または **no enable secret** [**level** *level*] グローバル コンフィギュレーション コマンドを使用します。パスワードの暗号化をディセーブルにするには、**no service password-encryption** グローバル コンフィギュレーション コマンドを使用します。

パスワード回復

スイッチに物理的にアクセスできるエンド ユーザは、デフォルトで、スイッチの電源投入時にブート プロセスに割り込み、新しいパスワードを入力することによって、失われたパスワードを回復できます。

パスワード回復ディセーブル化機能では、この機能の一部をディセーブルにすることによりスイッチのパスワードへのアクセスを保護できます。この機能がイネーブルの場合、エンド ユーザは、システムをデフォルト設定に戻すことに同意した場合に限り、ブート プロセスに割り込むことができます。パスワード回復をディセーブルにしても、ブート プロセスに割り込んでパスワードを変更できますが、コンフィギュレーション ファイル（config.text）および VLAN データベース ファイル（vlan.dat）は削除されます。

（注）　パスワード回復をディセーブルにする場合は、エンド ユーザがブート プロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コ

ピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。詳細については、「パスワードを忘れた場合の回復」（P.47-9）を参照してください。

（注）　パスワード回復のディセーブル化は、**boot manual** グローバル コンフィギュレーション コマンドを使用して手動でブートするようにスイッチを設定している場合は無効です。このコマンドは、スイッチの電源の再投入後、ブートローダ プロンプト（*switch:*）を表示させます。

端末回線に対する Telnet パスワード

初めてスイッチに電源を投入すると、自動セットアップ プログラムが起動して IP 情報を割り当て、この後続けて使用できるようにデフォルト設定を作成します。さらに、セットアップ プログラムは、パスワードによる Telnet アクセス用にスイッチを設定することを要求します。セットアップ プログラムの実行中にこのパスワードを設定しなかった場合は、この時点でコマンドライン インターフェイス（CLI）を使用して設定できます。

ユーザ名とパスワードのペア

ユーザ名とパスワードのペアを設定できます。このペアはスイッチ上でローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

複数の特権レベル

Cisco IOS ソフトウェアはデフォルトで、2 種類のパスワード セキュリティ モードを使用します。ユーザ EXEC および特権 EXEC です。各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセス制限を強化する場合は、レベル 3 のセキュリティを割り当て、そのパスワードを限られたユーザ グループに配布することもできます。

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip traffic** コマンドをレベル 15 に設定すると、**show** コマンドおよび **show ip** コマンドは、それぞれ別のレベルに設定しない限り、自動的にレベル 15 に設定されます。

特定のコマンドについて、デフォルトの権限に戻すには、**no privilege** *mode* **level** *level command* グローバル コンフィギュレーション コマンドを使用します。

ユーザは、回線にログインし、別の権限レベルをイネーブルに設定することにより、**privilege level** ライン コンフィギュレーション コマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

回線をデフォルトの権限レベルに戻すには、**no privilege level** ライン コンフィギュレーション コマンドを使用します。

TACACS+ のスイッチ アクセス

ここでは、Terminal Access Controller Access Control System Plus（TACACS+）をイネーブルにして設定する方法について説明します。TACACS+ は、詳細なアカウンティング情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。TACACS+ は、認証、許可、アカウンティング（AAA）機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

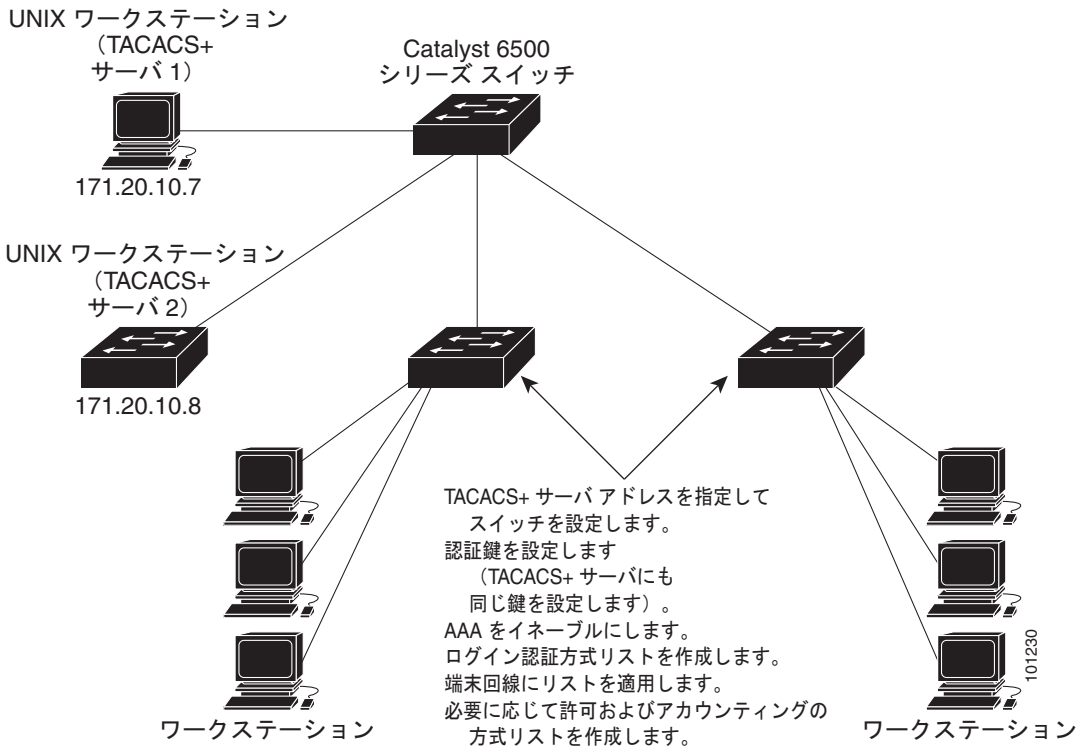
TACACS+

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。スイッチに TACACS+ 機能を設定するには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。ネットワーク アクセス サーバは、個々のユーザ、ネットワークまたはサブネットワーク、および相互接続されたネットワークとの接続を実現します（図 12-1 を参照）。

図 12-1　　一般的な TACACS+ ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の完全制御を行います。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力された後、自宅の住所、母親の旧姓、サービス タイプ、社会保険番号などのいくつかの質問をすることによりユーザを確認します）。TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード エージング ポリシーのため、パスワードを変更する必要があることをメッセージでユーザに通知することができます。

- 許可：autocommand、アクセス コントロール、セッション期間、プロトコル サポートの設定といった、ユーザ セッション時のユーザ機能についてきめ細かく制御します。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。

- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワード プロンプトを取得します。スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

   TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。

   - ACCEPT：ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
   - REJECT：ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するように求められます。
   - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
   - CONTINUE：ユーザは、さらに認証情報の入力を求められます。

   認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての属性の形式でデータが含まれています。

- Telnet、セキュア シェル（SSH）、rlogin、または特権 EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

（注）　TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ サーバ ホストと認証キー

認証用に 1 つのサーバを使用することも、また、既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するように設定することもできます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

TACACS+ ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可

AAA 認証によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルの場合、スイッチはローカル ユーザ データベースまたはセキュリティ サーバ上にあるユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

aaa authorization グローバル コンフィギュレーション コマンドに **tacacs+** キーワードを付けて使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec tacacs+ local コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

（注）　許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

TACACS+ Accounting

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

RADIUS によるスイッチ アクセス

ここでは、RADIUS をイネーブルにして設定する方法について説明します。RADIUS は、詳細なアカウンティング情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

RADIUS

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアが稼働しているマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

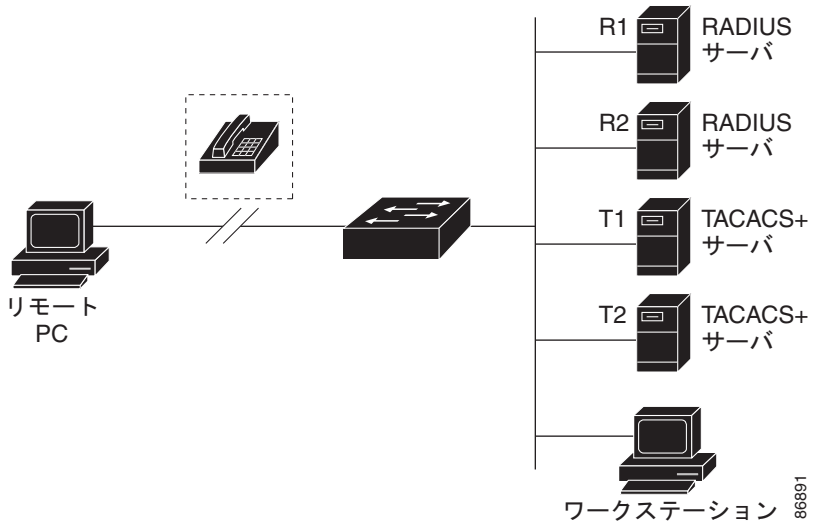
- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、*スマート カード*アクセス コントロール システムを使用するアクセス環境。あるケースでは、RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リソースへのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備の Cisco スイッチをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。

- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、第 13 章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

図 12-2　　RADIUS サービスから TACACS+ サービスへの移行



RADIUS の動作

RADIUS サーバによってアクセス コントロールされるスイッチに、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは RADIUS サーバから、次のいずれかの応答を受信します。
   a. ACCEPT：ユーザが認証されたことを表します。

b. REJECT：ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が要求されるか、またはアクセスが拒否されます。

c. CHALLENGE：ユーザに追加データを要求します。

d. CHALLENGE PASSWORD：ユーザは新しいパスワードを選択するように要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります（イネーブルに設定されている場合）。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

RADIUS 許可の変更

ここでは、使用可能なプリミティブおよびそれらの Change of Authorization（CoA）での使用方法を含む、RADIUS インターフェイスの概要について説明します。

RADIUS CoA の概要

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。Catalyst スイッチは、通常プッシュ モデルで使用される RFC 5176 で規定された RADIUS Change of Authorization（CoA）拡張機能をサポートし、外部の認証、許可、アカウンティング（AAA）またはポリシーサーバからのセッションのダイナミック再設定ができるようにします。

スイッチは、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッション終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

Change-of-Authorization 要求

Change of Authorization（CoA）要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。このモデルは、1 つの要求（CoA-Request）と 2 つの可能な応答コードで構成されています。

- CoA acknowledgement（ACK）[CoA-ACK]
- CoA non-acknowledgement（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から発信されて、リスナーとして動作するスイッチに送信されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してスイッチでサポートされています。

表 12-2　サポートされている IETF 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

表 12-3　Error-Cause の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチ セッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。サポートされているコマンドを表 12-4（P.12-12）に示します。

CoA セッション ID

特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Calling-Station-Id（ホストの MAC アドレスを含む IETF 属性 31）

- Audit-Session-Id VSA（シスコの VSA）
- Acct-Session-Id（IETF 属性 44）

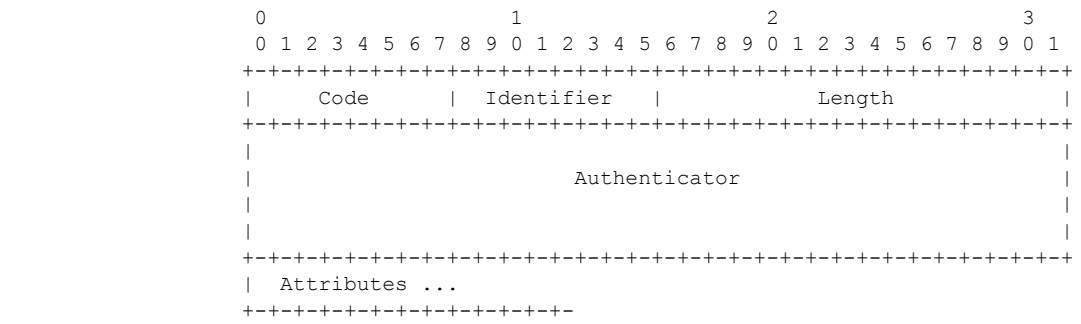
CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しないかぎり、スイッチは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

特定のセッションに対する接続解除および CoA 要求の場合、次のいずれかのセッション ID を使用できます。

- Calling-Station-ID（MAC アドレスを含む IETF 属性 31）
- Audit-Session-ID（シスコのベンダー固有属性）
- Accounting-Session-ID（IETF 属性 44）

メッセージに複数のセッション ID 属性が含まれる場合、すべての属性がセッションと一致する必要があります。一致しない場合は、スイッチが「*Invalid Attribute Value*」エラー コードを含む Disconnect-否定確認応答（NAK）または CoA-NAK を返します。

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。



属性フィールドは、Cisco VSA を送信するために使用します。

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

CoA NAK 応答コード

否定確認応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。CoA が成功したかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

表 12-4　スイッチでサポートされる CoA コマンド

コマンド[1]	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。

表 12-4　スイッチでサポートされる CoA コマンド （続き）

コマンド[1]	シスコの VSA
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

1. すべての CoA コマンドには、スイッチと CoA クライアント間のセッション識別情報が含まれている必要があります。

CoA セッションの再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバは通常、セッション再認証要求を生成します。再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバは *Cisco:Avpair="subscriber:command=reauthenticate"* の形式でシスコのベンダー固有属性（VSA）と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッション ステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは LAN 経由の拡張認証プロトコル（EAPOL）RequestId メッセージをサーバに送信することで応答します。

現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、スイッチはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッション認証が実行中である場合は、スイッチはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されてない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

CoA セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。このコマンドを使用すると、指定されたホストのオーセンティケータ ステート マシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワーク アクセスをただちにブロックする必要があります。ポートへのネットワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサプリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポート バウンスでホスト ポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。このコマンドはセッション指向であるため、「CoA セッション ID」（P.12-11）で示される 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは Disconnect-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。セッションがある場合は、スイッチはセッションを終了します。セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラー コード属性が送信されます。

CoA 要求：ホスト ポートのディセーブル化

このコマンドは、次の新しい VSA が含まれている標準 CoA 要求メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「CoA セッション ID」（P.12-11）で示される 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合は、CoA-NAK メッセージと「Session Context Not Found」エラー コード属性が返されます。このセッションがある場合は、スイッチはホスト ポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

（注）　再送信コマンドの後に接続解除要求が失敗すると、（接続解除 ACK が送信されてない場合に）チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイ スイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

CoA 要求：バウンス ポート

このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。
Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、「CoA セッション ID」（P.12-11）で示される 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合は、CoA-NAK メッセージと「Session Context Not Found」エラー コード属性が返されます。このセッションがある場合は、スイッチはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

RADIUS サーバ ホスト

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。この例では、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、スイッチは「%RADIUS-4-RADIUS_DEAD」メッセージを表示し、その後、同じデバイス上で 2 番めに設定されたホスト エントリでアカウンティング サービスを試みます（RADIUS ホスト エントリは、設定した順序に従って試行されます）。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デーモンが稼働するホストと、そのホストがスイッチと共有するシークレット テキスト（キー）ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。スイッチと通信するすべての RADIUS サーバに対して、これらの設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** の 3 つの固有のグローバル コンフィギュレーション コマンドを使用します。これらの設定を特定の RADIUS サーバに適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。

（注） スイッチ上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、およびキーコマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。すべての RADIUS サーバに対してこれらの値を設定する方法については、「すべての RADIUS サーバの設定」（P.12-38）を参照してください。

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。詳細については、「AAA サーバ グループの定義」（P.12-36）を参照してください。

RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

RADIUS 方式リスト

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティ プロトコル（TACACS+、ローカル ユーザ名検索など）を 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合は、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

AAA Server Groups

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。

定義したグループ サーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可

AAA 認証によってユーザが使用できるサービスが制限されます。AAA 認証がイネーブルの場合、ローカル ユーザ データベースまたはセキュリティ サーバ内のユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

グローバル コンフィギュレーション コマンド **aaa authorization** と **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

（注）　許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

RADIUS アカウンティング

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

AAA サーバが到達不能な場合のルータとのセッションの確立

aaa accounting system guarantee-first コマンドは、システム アカウンティングが最初のレコードになることを保証します。これはデフォルトの状態です。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

ベンダー固有の RADIUS 属性

Internet Engineering Task Force（IETF）ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダー タイプ 1（名前は *cisco-avpair*）です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

protocol は、特定の許可タイプに使用するシスコのプロトコル属性の値です。*attribute* および *value* は、シスコの TACACS+ 仕様で定義されている適切な属性値（AV）ペアです。*sep* は、必須の属性の場合は =、任意指定の属性の場合は * です。TACACS+ 許可で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアを指定すると、IP 許可時（PPP の IPCP アドレスの割り当て時）に、シスコの *複数の名前付き IP アドレス プール*機能が有効になります。

```
cisco-avpair= "ip:addr-pool=first"
```

ベンダー独自仕様の RADIUS サーバ通信

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず）を設定するには、RADIUS サーバ デーモンが稼働しているホストと、そのホストがスイッチと共有するシークレット テキスト ストリングを指定する必要があります。RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

Kerberos によるスイッチ アクセス

ここでは、Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。この機能を使用するには、スイッチにスイッチ ソフトウェアの暗号化バージョンをインストールする必要があります。

この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

Kerberos の概要

Kerberos はマサチューセッツ工科大学（MIT）が開発した秘密キーによるネットワーク認証プロトコルです。データ暗号規格（DES）という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティをキー発行局（KDC）と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC（つまり信頼できる Kerberos サーバ）がユーザにチケットを発行します。これらのチケットには有効期限があり、ユーザ クレデンシャルのキャッシュに保存されます。Kerberos サーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。

（注）　Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるスイッチを使用できます。

Kerberos のクレデンシャル発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを 1 回認証すると、ユーザ クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、（UNIX サーバや PC などの）他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

このソフトウェア リリースでは、Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh（リモート シェル プロトコル）

表 12-5 に、一般的な Kerberos 関連用語とその定義を示します。

表 12-5　Kerberos の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ユーザがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段
クレデンシャル	認証チケット（TGT[1] やサービス クレデンシャルなど）を表す総称。Kerberos クレデンシャルで、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。クレデンシャルの有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、*user@REALM* という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスのある Kerberos プリンシパルは、*user/instance@REALM* という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 **（注）**　Kerberos プリンシパル名およびインスタンス名はすべて小文字*でなければなりません。* **（注）**　Kerberos レルム名はすべて大文字で*なければなりません。*
KDC[2]	ネットワーク ホストで稼働する Kerberos サーバおよびデータベース プログラムで構成されるキー発行局
Kerberos 対応	Kerberos クレデンシャルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。 **（注）**　Kerberos レルム名はすべて大文字で*なければなりません。*
Kerberos サーバ	ネットワーク ホストで稼働しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。
KEYTAB[3]	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシャルを暗号解除して認証します。KEYTAB は Kerberos 5 よりも前のバージョンでは、SRVTAB[4] と呼ばれています。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。 **（注）**　Kerberos プリンシパル名はすべて小文字で*なければなりません。*

表 12-5　Kerberos の用語 （続き）

用語	定義
サービス クレデンシャル	ネットワーク サービスのクレデンシャル。KDC からクレデンシャルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザ TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のことで、KDC が認証済みユーザに発行するクレデンシャル。TGT を受け取ったユーザは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

1. TGT = Ticket Granting Ticket（身分証明書）
2. KDC = Key Distribution Center（キー発行局）
3. KEYTAB = key table（キー テーブル）
4. SRVTAB = server table（サーバ テーブル）

Kerberos の動作

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてリモート ユーザを認証できるスイッチを使用できます。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモート ユーザは、3 つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

Kerberos サーバとしてスイッチを使用し、リモート ユーザがネットワーク サービスに対して認証を得る手順は、次のとおりです。

1. 「境界スイッチに対する認証の取得」（P.12-20）
2. 「KDC からの TGT の取得」（P.12-21）
3. 「ネットワーク サービスに対する認証の取得」（P.12-21）

境界スイッチに対する認証の取得

ここでは、リモート ユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。リモート ユーザが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザ名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使って TGT の暗号解除を試行します。
   - 暗号解除に成功した場合は、ユーザはスイッチに対して認証を得ます。
   - 暗号解除に成功しない場合は、ユーザ名とパスワードを再入力（Caps Lock または Num Lock のオン/オフに注意）するか、別のユーザ名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモート ユーザはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過しなければならない 2 番めのセキュリティ レイヤについて説明します。ユーザは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番めのセキュリティ レイヤについて説明します。TGT を取得したユーザは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

Kerberos の設定

リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。

ホストおよびユーザのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字で*なければなりません*。
- Kerberos インスタンス名はすべて小文字で*なければなりません*。
- Kerberos レルム名はすべて大文字で*なければなりません*。

（注） Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるスイッチを使用できます。

Kerberos 認証済みサーバ/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

ローカル認証および許可

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウンティング機能は使用できません。

セキュア シェル

この機能を使用するには、暗号（暗号化）ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

SSH の設定例については、『*Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*』の「Configuring Secure Shell」の章にある「SSH Configuration Examples」の項を参照してください。

IPv6 における SSH は、IPv4 における SSH と同じように機能し、同じ利点があります。SSH への IPv6 の機能拡張により、IPv6 アドレスがサポートされるため、Cisco ルータは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。

（注）　ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。

SSH

SSH は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

SSH サーバ、統合クライアント、およびサポートされているバージョン

SSH 機能には SSH サーバおよび SSH 統合クライアントがあり、これらはスイッチ上で実行されるアプリケーションです。SSH クライアントを使用すると、SSH サーバが稼働するスイッチに接続できます。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。また、SSH クライアントは、このリリースでサポートされている SSH サーバおよび他社製の SSH サーバと使用します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートしています。

SSH は、データ暗号規格（DES）暗号化アルゴリズム、Triple DES（3DES）暗号化アルゴリズム、およびパスワードベースの認証をサポートしています。

SSH は次のユーザ認証方式をサポートしています。

- TACACS+（詳細については、「TACACS+ の設定」（P.12-31）を参照してください）
- RADIUS（詳細については、「RADIUS サーバ通信の設定」（P.12-34）を参照してください）
- ローカル認証および許可（詳細については、「スイッチのローカル認証および許可の設定」（P.12-40）を参照）

（注）　このソフトウェア リリースは、IP Security（IPSec）をサポートしていません。

制限事項

SSH には、次の制限事項が適用されます。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、DES（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。
- スイッチは、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。

SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます（逆の場合も同様です）。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力した後、CLI エラー メッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。詳細については、「スイッチで SSH を実行するためのセットアップ」（P.12-41）を参照してください。
- RSA キーのペアを生成する場合に、メッセージ「`No host name specified`」が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「`No domain specified`」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

SSL HTTP のためのスイッチ

Secure Socket Layer（SSL）バージョン 3.0 では、HTTP 1.1 のサーバおよびクライアントをサポートします。SSL は、セキュア HTTP 通信を実現するために、HTTP クライアント認証だけでなく、サーバ認証、暗号化、およびメッセージの完全性も提供します。この機能を使用するには、スイッチに暗号化ソフトウェア イメージをインストールする必要があります。この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。暗号化イメージの詳細については、このリリースのリリース ノートを参照してください。

セキュア HTTP サーバおよびクライアント

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。HTTP over SSL は、HTTPS と省略されます（セキュアな接続の場合、URL が http:// の代わりに https:// で始まります）。

セキュア HTTP サーバ（スイッチ）の主な役割は、指定のポート（デフォルトの HTTPS ポートは 443）で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。HTTP 1.1 サーバはその要求を処理して、セキュア HTTP サーバへ応答（呼び出す）します。セキュア HTTP サーバは HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント（Web ブラウザ）の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を（そのアプリケーションに）返すことです。

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンダで終了します。クラスタ メンバのスイッチは標準の HTTP で動作させる必要があります。

セキュア HTTP 接続には、CA のトラストポイントを正式に設定することを推奨します。CA のトラストポイントは、自己署名証明書より高いセキュリティがあります。

CA のトラストポイントを設定する前に、システム クロックが設定されていることを確認してください。クロックが設定されていないと、不正な日付により証明書が拒否されます。

SSL のデフォルト設定

表 12-6　　SSL のデフォルト設定

デフォルト設定
標準の HTTP サーバはイネーブルに設定されています。
SSL はイネーブルに設定されています。
CA のトラストポイントは設定されていません。
自己署名証明書は生成されていません。

CA のトラストポイント

認証局（CA）は、要求を認可して参加するネットワーク デバイスに証明書を発行します。これらのサービスは、参加するデバイスに対する中央集中的なセキュリティ キーおよび証明書の管理を提供します。特定の CA サーバは *トラストポイント*と呼ばれます。

接続が実行されると、HTTPS サーバは、トラストポイントとなる特定の CA から得た X.509v3 の証明書を発行することで、セキュアな接続をクライアントに提供します。クライアント（通常、Web ブラウザ）は、その証明書の認証に必要な公開キーを保有しています。

セキュア HTTP 接続には、CA のトラストポイントを設定することを強く推奨します。HTTPS サーバを実行しているデバイスに CA のトラストポイントが設定されていないと、サーバは自身を認証して必要な RSA のキーのペアを生成します。自身で認証した（自己署名）証明書は適切なセキュリティではないので、接続するクライアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択（確立または拒否）をさせる必要があります。この選択肢は内部ネットワーク トポロジ（テスト用など）に役立ちます。

CA のトラストポイントを設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ（またはクライアント）に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されてない場合、生成される自己署名証明書は一時的なものです。スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書（一時的に）が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。

（注） 認証局およびトラストポイントは、個々のデバイスで設定する必要があります。他のデバイスからコピーすると、それらはスイッチ上で無効になります。

（注） *TP self-signed* の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド（**ip http secure-client-auth**）を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェスト アルゴリズムを指定して、SSL 接続に使用します。HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで最適なものをリストから選択してネゴシエートします。たとえば、Netscape Communicator 4.76 は、米国の セキュリティ（RSA 公開キー暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC）をサポートしています。

最適な暗号化には、128 ビット暗号化をサポートするクライアント ブラウザ（Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など）が必要です。SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要になります。次に、スイッチでサポートされる CipherSuite およびルータの処理負荷（速さ）による CipherSuite のランク（速い順）を定義します。

1. SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）
2. SSL_RSA_WITH_RC4_128_MD5：RC4 128 ビット暗号化、およびメッセージ ダイジェストに MD5 を使用した RSA のキー交換
3. SSL_RSA_WITH_RC4_128_SHA：RC4 128 ビット暗号化、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）

（暗号化およびダイジェスト アルゴリズムをそれぞれ指定して組み合わせた）RSA は、SSL 接続においてキーの生成および認証の両方に使用されます。これは、CA のトラストポイントが設定されているかどうかにかかわりません。

Secure Copy Protocol（SCP）

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。SCP には、Berkeley r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルであるセキュア シェル（SSH）が必要です。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、スイッチには RSA キーのペアが必要です。

（注）　SCP を使用する場合、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。また、SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。

適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。

（注）　SCP の設定および検証方法の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4*』の「Secure Copy Protocol」を参照してください。
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_copy_ps6350_TSD_Products_Configuration_Guide_Chapter.html

スイッチ ベース認証の設定方法

パスワード保護の設定

スタティック イネーブル パスワードの設定または変更

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** *password*	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトでは、パスワードは定義されません。 *password* : 1 ～ 25 文字の英数字のストリングを入力します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符（?）は、パスワードを作成する場合に、疑問符の前に Ctrl+v を入力すれば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。 **abc** を入力します。 **Ctrl+V** キーを押します。 **?123** を入力します。 enable パスワードの入力を求められたら、疑問符の前で Ctrl+V キーを押す必要はありません。パスワード プロンプトで **abc?123** と入力するだけです。
ステップ 3	**end**	特権 EXEC モードに戻ります。

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted*-password} または **enable secret** [**level** *level*] {*password* | *encryption-type encrypted*-password}	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 または シークレット パスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。 • （任意）*level* : 指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です（特権 EXEC モード権限）。 • *password* : 1 ～ 25 文字の英数字のストリングを入力します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 • （任意）*encryption-type* : シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチの設定からコピーします。 **（注）** 暗号化タイプを指定し、クリア テキスト パスワードを入力した場合は特権 EXEC モードを再開できません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。
ステップ 3	**service password-encryption**	（任意）パスワードの定義時または設定の書き込み時に、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。

パスワード回復のディセーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no service password-recovery**	パスワード回復をディセーブルにします。 この設定は、フラッシュ メモリの中で、ブートローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイル システムには含まれません。また、ユーザがアクセスすることはできません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show version**	コマンド出力の最後の数行をチェックすることによって、設定を確認します。

端末回線に対する Telnet パスワードの設定

	コマンド	目的
ステップ 1		エミュレーション ソフトウェアを備えた PC またはワークステーションとスイッチのコンソール ポートを接続します。 コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなしです。コマンドライン プロンプトが表示されるまで、Return キーを何回か押す必要があります。
ステップ 2	**enable password** *password*	特権 EXEC モードを開始します。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**line vty 0 15**	Telnet セッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。 コマンド対応スイッチでは、最大 16 のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。
ステップ 5	**password** ***password***	1 つまたは複数の回線に対応する Telnet パスワードを入力します。 *password* : 1 ～ 25 文字の英数字のストリングを入力します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ 6	**end**	特権 EXEC モードに戻ります。

ユーザ名とパスワードのペアの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	各ユーザのユーザ名、特権レベル、およびパスワードを入力します。 • *name* : 1 語でユーザ ID を指定します。スペースと引用符は使用できません。 • （任意）*level* : アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* : 暗号化されていないパスワードが続くことを指定する場合は 0 を入力します。暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password* : ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 • 特定ユーザのユーザ名認証をディセーブルにするには、**no username** *name* グローバル コンフィギュレーション コマンドを使用します。

	コマンド	目的
ステップ 3	**line console 0** または **line vty 0 15**	ライン コンフィギュレーション モードを開始し、コンソール ポート（回線 0）または VTY 回線（回線 0 ～ 15）を設定します。
ステップ 4	**login local**	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。 パスワード チェックをディセーブルにし、パスワードなしでの接続を可能にするには、**no login** ライン コンフィギュレーション コマンドを使用します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

コマンドの特権レベルの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**privilege** *mode* **level** *level command*	コマンドの特権レベルを設定します。 • *mode*：グローバル コンフィギュレーション モードの場合は **configure**、EXEC モードの場合は **exec**、インターフェイス コンフィギュレーション モードの場合は **interface**、ライン コンフィギュレーション モードの場合は **line** と入力します。 • *level*：指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。 • *command*：アクセスを制限したいコマンドを指定します。
ステップ 3	**enable password level** *level password*	特権レベルの enable パスワードを指定します。 • *level*：指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。 • *password*：1 ～ 25 文字の英数字のストリングを入力します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show privilege**	パスワードおよびアクセス レベルの設定を確認します。

回線のデフォルト特権レベルの変更

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line vty** *line*	アクセスを制限する仮想端末回線を選択します。

	コマンド	目的
ステップ 3	**privilege level** *level*	回線のデフォルト特権レベルを変更します。 *level* : 指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show privilege**	パスワードおよびアクセス レベルの設定を確認します。

特権レベルへのログインと終了

コマンド	目的
enable *level*	指定された特権レベルにログインします。 *level* : 指定できる範囲は 0 ～ 15 です。
disable*level*	指定した特権レベルを終了します。 *level* : 指定できる範囲は 0 ～ 15 です。

TACACS+ の設定

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウンティングの方式リストを定義できます。方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティ プロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

TACACS+ サーバ ホストの特定および認証キーの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	TACACS+ サーバを維持する IP ホストを特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 • *hostname*：ホストの名前または IP アドレスを指定します。 • （任意）**port** *integer*：サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は 1 ～ 65535 です。 • （任意）**timeout** *integer*：スイッチがデーモンからの応答を待つ時間を秒数で指定します。これを過ぎるとスイッチはタイムアウトしてエラーを宣言します。デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 秒です。 • （任意）**key** *string*：スイッチと TACACS+ デーモン間のすべてのトラフィックを暗号化および暗号解除するための暗号キーを指定します。暗号化が成功するには、TACACS+ デーモンに同じキーを設定する必要があります。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa group server tacacs+** *group-name*	（任意）グループ名で AAA サーバグループを定義します。 このコマンドによって、スイッチはサーバ グループ サブコンフィギュレーション モードになります。
ステップ 5	**server** *ip-address*	（任意）特定の TACACS+ サーバを定義済みサーバ グループに関連付けます。AAA サーバ グループの TACACS+ サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show tacacs**	入力を確認します。

TACACS+ ログイン認証の設定

はじめる前に

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name*：作成するリストの名前として使用する文字列を指定します。 • *method1...*：認証アルゴリズムが試みる実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 • **group tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。詳細については、「TACACS+ サーバ ホストの特定および認証キーの設定」（P.12-32）を参照してください。 • **line**：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカルのユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **local-case**：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name*：**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network tacacs+**	ネットワーク関連のすべてのサービス要求に対してユーザ TACACS+ 許可を行うことを設定します。
ステップ 3	**aaa authorization exec tacacs+**	ユーザの特権 EXEC アクセスに対してユーザ TACACS+ 許可を行うことを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

TACACS+ アカウンティングの起動

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa accounting network start-stop tacacs+**	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop tacacs+**	TACACS+ アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

RADIUS サーバ通信の設定

はじめる前に

スイッチ上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。

最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウンティングの方式リストを定義できます。

いくつかの設定は、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングを含む RADIUS サーバ上で設定する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number*：認証要求のための UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number*：アカウンティング要求のための UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds*：スイッチが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries*：サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string*：RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。

AAA サーバ グループの定義

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number*：認証要求のための UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number*：アカウンティング要求のための UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds*：スイッチが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries*：サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • **key** *string* には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa group server radius** *group-name*	グループ名を使用して、AAA サーバ グループを定義します。 このコマンドを使用すると、スイッチはサーバ グループ コンフィギュレーション モードになります。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義済みのサーバ グループと関連付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7		RADIUS ログイン認証をイネーブルにします。「AAA サーバ グループの定義」（P.12-36）を参照してください。

RADIUS ログイン認証の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name*：作成するリストの名前として使用する文字列を指定します。 • *method1...*：認証アルゴリズムが試みる実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 – **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 – **group radius**：RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。詳細については、「RADIUS サーバ ホスト」（P.12-15）を参照してください。 – **line**：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 – **local**：ローカルのユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用します。 – **local-case**：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *password* グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 – **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name*：**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network radius**	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可を、スイッチに設定します。
ステップ 3	**aaa authorization exec radius**	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ RADIUS 許可を、スイッチに設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

RADIUS アカウンティングの起動

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa accounting network start-stop radius**	ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop radius**	RADIUS アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

すべての RADIUS サーバの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server key** *string*	スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト ストリングを指定します。 （注）　キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 3	**radius-server retransmit** *retries*	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout** *seconds*	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間（秒）を指定します。デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 です。
ステップ 5	**radius-server deadtime** *minutes*	認証要求に応答しない RADIUS サーバをスキップする時間（分）を指定し、要求がタイムアウトするまで待機することなく、次に設定されているサーバを試行できるようにします。デフォルトは 0 です。指定できる範囲は 0 ～ 1440 分です。

	コマンド	目的
ステップ 6	**radius-server vsa send** [**accounting** | **authentication**]	スイッチが VSA（RADIUS IETF 属性 26 で定義）を認識して使用できるようにします。 • （任意）**accounting**：認識されるベンダー固有属性の集合をアカウンティング属性だけに限定します。 • （任意）**authentication**：認識されるベンダー固有属性の集合を認証属性だけに限定します。 キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 7	**end**	特権 EXEC モードに戻ります。

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **non-standard**	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、RADIUS のベンダー独自仕様の実装を使用することを指定します。
ステップ 3	**radius-server key** *string*	スイッチとベンダー独自仕様の RADIUS サーバとの間で共有されるシークレット テキスト ストリングを指定します。スイッチおよび RADIUS サーバは、このテキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ上での CoA の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa server radius dynamic-author**	スイッチを認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシー サーバとの相互作用を実行します。

	コマンド	目的
ステップ 4	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*]	ダイナミック許可ローカル サーバ コンフィギュレーション モードを開始し、デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
ステップ 5	**server-key** [**0** | **7**] *string*	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 6	**port** *port-number*	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 7	**auth-type** {**any** | **all** | **session-key**}	スイッチが RADIUS クライアントに使用する許可のタイプを指定します。 クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 8	**ignore session-key**	（任意）セッション キーを無視するようにスイッチを設定します。
ステップ 9	**ignore server-key**	（任意）サーバキーを無視するようにスイッチを設定します。
ステップ 10	**authentication command bounce-port ignore**	（任意）CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするようにスイッチを設定します。ポートを一時的にディセーブルにする目的は、VLAN の変更が発生しても、その変更を検出するサプリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。
ステップ 11	**authentication command disable-port ignore**	（任意）セッションをホスティングしているポートを管理上のシャットダウン状態にすることを要求する非標準コマンドを無視するようにスイッチを設定します。ポートをシャットダウンすると、セッションが終了します。 ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。
ステップ 12	**end**	特権 EXEC モードに戻ります。

スイッチのローカル認証および許可の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login default local**	ローカル ユーザ名データベースを使用するログイン認証を設定します。**default** キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 4	**aaa authorization exec local**	ユーザの AAA 許可を設定し、ローカル データベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 5	**aaa authorization network local**	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。

	コマンド	目的
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 • *name*：1 語でユーザ ID を指定します。スペースと引用符は使用できません。 • （任意）*level*：アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type*：暗号化されていないパスワードが続くことを指定する場合は 0 を入力します。暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password*：ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

セキュア シェルの設定

スイッチで SSH を実行するためのセットアップ

	作業	目的
ステップ 1	暗号化ソフトウェア イメージを Cisco.com からダウンロードします。	（必須）詳細については、このリリースのリリース ノートを参照してください。
ステップ 2	スイッチのホスト名および IP ドメイン名を設定します。	この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
ステップ 3	スイッチが SSH を自動的にイネーブルにするための RSA キーのペアを生成します。	この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
ステップ 4	ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。	（必須）詳細については、「スイッチのローカル認証および許可の設定」（P.12-40）を参照してください。

SSH サーバの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *hostname*	スイッチのホスト名を設定します。
ステップ 3	**ip domain-name** *domain_name*	スイッチのホスト ドメインを設定します。

	コマンド	目的
ステップ 4	**crypto key generate rsa**	スイッチ上でローカルおよびリモート認証用に SSH サーバをイネーブルにし、RSA キーのペアを生成します。 最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。
ステップ 5	**ip ssh version** [**1** | **2**]	（任意）SSHv1 または SSHv2 を実行するようにスイッチを設定します。 • **1**：SSHv1 を実行するようにスイッチを設定します。 • **2**：SSHv2 を実行するようにスイッチを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 6	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}	SSH 制御パラメータを設定します。 • タイムアウト値は秒単位で指定します（デフォルト値は 120 秒）。指定できる範囲は 0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されると、スイッチは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。
ステップ 7	**line vty** *line_number* [*ending_line_number*] **transport input ssh**	（任意）仮想端末回線設定を設定します。 • ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。*line_number* および *ending_line_number* に対して、1 回線ペアを指定します。指定できる範囲は 0 ～ 15 です。 • スイッチで非 SSH Telnet 接続を回避するように設定します。これにより、ルータは SSH 接続に限定されます。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバのステータスを表示します。

セキュア HTTP サーバおよびクライアントの設定

CA のトラストポイントの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *hostname*	スイッチのホスト名を指定します（以前ホスト名を設定していない場合のみ必須）。
ステップ 3	**ip domain-name** *domain-name*	スイッチの IP ドメイン名を指定します（以前 IP ドメイン名を設定していない場合のみ必須）。
ステップ 4	**crypto key generate rsa**	（任意）RSA キー ペアを生成します。RSA キーのペアは、スイッチの証明書を入手する前に必要です。RSA キーのペアは自動的に生成されます。必要であれば、このコマンドを使用してキーを再生成できます。
ステップ 5	**crypto ca trustpoint** *name*	CA のトラストポイントにローカルの設定名を指定して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	**enrollment url** *url*	スイッチによる証明書要求の送信先の URL を指定します。
ステップ 7	**enrollment http-proxy** *host-name port-number*	（任意）HTTP プロキシ サーバを経由して CA から証明書を入手するようにスイッチを設定します。
ステップ 8	**crl query** *url*	ピアの証明書が取り消されていないかを確認するために、証明書失効リスト（CRL）を要求するようにスイッチを設定します。
ステップ 9	**primary**	（任意）トラストポイントが CA 要求に対してプライマリ（デフォルト）トラストポイントとして使用されるように指定します。
ステップ 10	**exit**	CA トラストポイント コンフィギュレーションモードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto ca authentication** *name*	CA の公開キーを取得して CA を認証します。ステップ 5 で使用した名前と同じものを使用します。
ステップ 12	**crypto ca enroll** *name*	指定した CA トラストポイントから証明書を取得します。このコマンドは、各 RSA キーのペアに対して 1 つの署名入りの証明書を要求します。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show crypto ca trustpoints**	設定を確認します。

セキュア HTTP サーバの設定

はじめる前に

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA トラストポイントを設定してから、HTTP サーバを有効にする必要があります。CA のトラストポイントを設定していない場合、セキュア HTTP サーバを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定した後、標準およびセキュア HTTP サーバ両方に適用するオプション（パス、適用するアクセス リスト、最大接続数、またはタイムアウト ポリシー）を設定できます。

	コマンド	目的

ステップ 1	**show ip http server status**	（任意）HTTP サーバのステータスを表示して、セキュア HTTP サーバの機能がソフトウェアでサポートされているかどうかを判断します。出力で、次のラインのどちらかを確認してください。
		`HTTP secure server capability: Present`
		または
		`HTTP secure server capability: Not present`

ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http secure-server**	HTTPS サーバがディセーブルの場合、イネーブルにします。HTTPS サーバは、デフォルトでイネーブルに設定されています。
ステップ 4	**ip http secure-port** *port-number*	（任意）HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。443 または 1025 ～ 65535 の範囲で指定できます。
ステップ 5	**ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これはデフォルトです。
ステップ 6	**ip http secure-client-auth**	（任意）HTTP サーバを設定して、接続処理の間、認証のために、クライアントからの X.509v3 証明書を要求します。デフォルトでは、クライアントがサーバからの証明書を要求する設定になっていますが、サーバはクライアントを認証しないようになっています。
ステップ 7	**ip http secure-trustpoint** *name*	X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA のトラストポイントを指定します。 **（注）** このコマンドの使用は、前の手順に従って CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。
ステップ 8	**ip http path** *path-name*	（任意）HTML ファイルのベースとなる HTTP パスを設定します。パスは、ローカル システムにある HTTP サーバ ファイルの場所を指定します（通常、システムのフラッシュ メモリを指定します）。
ステップ 9	**ip http access-class** *access-list-number*	（任意）HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 10	**ip http max-connections** *value*	（任意）HTTP サーバへの同時最大接続数を指定します。指定できる範囲は 1 ～ 16 です。デフォルトは 5 です。
ステップ 11	**ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value*	（任意）指定の状況下における、HTTP サーバへの接続最大時間を指定します。 • **idle**：データの受信がないか、応答データが送信できない場合の最大時間。指定できる範囲は 1 ～ 600 秒です。デフォルト値は 180 秒（3 分）です。 • **life**：接続を確立している最大時間を指定します。指定できる範囲は 1 ～ 86400 秒（24 時間）です。デフォルト値は 180 秒です。 • **requests**：永続的な接続で処理される要求の最大数を指定します。最大値は 86400 です。デフォルトは 1 です。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip http server secure status**	セキュア HTTP サーバのステータスを表示して、設定を確認します。

セキュア HTTP クライアントの設定

はじめる前に

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。証明書の認証にはセキュア HTTP クライアントの証明書が必要です。次の手順では、前の手順で CA のトラストポイントをスイッチに設定していることを前提にしています。CA のトラストポイントが設定されておらず、リモートの HTTPS サーバがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip http client secure-trustpoint** *name*	（任意）リモートの HTTP サーバがクライアント認証を要求した場合に使用する、CA のトラストポイントを指定します。このコマンドの使用は、前の手順を使用して CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。クライアント認証が必要ない場合、またはプライマリのトラストポイントがすでに設定されている場合は、このコマンドは任意です。
ステップ 3	**ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これはデフォルトです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip http client secure status**	セキュア HTTP サーバのステータスを表示して、設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ ベース認証のモニタリングおよびメンテナンス

コマンド	目的
show running-config	設定されたエントリを確認します。
copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。
show tacacs	TACACS+ サーバの統計情報を表示します。
debug radius	RADIUS 関連の情報を表示します。
debug aaa coa	CoA 処理のデバッグ情報を表示します。
debug cmdhd	コマンド ハンドラのデバッグ情報を表示します。
show aaa attributes protocol radius	RADIUS 属性を表示します。
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。
show ip http client secure status	セキュア HTTP クライアントの設定を表示します。
show ip http server secure status	セキュア HTTP サーバの設定を表示します。

スイッチ ベース認証の設定例

イネーブル パスワードの変更：例

次に、イネーブル パスワードを *l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
Switch(config)# enable password l1u2c3k4y5
```

暗号化パスワードの設定：例

次に、権限レベル 2 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

端末回線に対する Telnet パスワードの設定：例

次に、Telnet パスワードを *let45me67in89* に設定する例を示します。

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

コマンドの権限レベルの設定：例

configure コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

RADIUS サーバの設定：例

次に、1 つの RADIUS サーバを認証用に、もう 1 つの RADIUS サーバをアカウンティング用に設定する例を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次に、*host1* を RADIUS サーバとして設定し、認証およびアカウンティングの両方にデフォルトのポートを使用するように設定する例を示します。

```
Switch(config)# radius-server host host1
```

AAA サーバ グループの定義：例

次の例では、2 つの異なる RADIUS グループ サーバ（*group1* および *group2*）を認識するようにスイッチを設定しています。group1 では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。2 番目のホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

ベンダー固有 RADIUS 属性の設定：例

次に、スイッチから特権 EXEC コマンドへの即時アクセスが可能となるユーザ ログインを提供する例を示します。

```
cisco-avpair= "shell:priv-lvl=15"
```

次に、RADIUS サーバ データベース内の許可 VLAN を指定する例を示します。

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-id(#81)=vlanid"
```

次に、この接続中に ASCII 形式の入力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

次に、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

ベンダー固有 RADIUS ホストの設定：例

次に、ベンダー独自仕様の RADIUS ホストを指定し、スイッチとサーバの間で *rad124* という秘密キーを使用する例を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

自己署名証明書の出力：例

自己署名証明書が生成された場合、その情報は **show running-config** 特権 EXEC コマンドで出力できます。自己署名証明書を表示するコマンドの出力（show running-config コマンド）を例として一部示します。

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

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3080755072
 revocation-check none
 rsakeypair TP-self-signed-3080755072
!
```

```
!
crypto ca certificate chain TP-self-signed-3080755072
 certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109

<output truncated>
```

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。

セキュア HTTP 接続の確認：例

Web ブラウザを使用してセキュア HTTP 接続を確認するには、https://*URL* を入力します（*URL* は IP アドレス、またはサーバ スイッチのホスト名）。デフォルト ポート以外のポートを設定している場合、URL の後ろにポート番号も指定する必要があります。次に例を示します。

https://209.165.129:1026
または
https://host.domain.com:1026

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	*『Cisco IOS Configuration Fundamentals Command Reference』*
セキュア コピー プロトコルの設定	*『Cisco IOS Security Configuration Guide: Securing User Services』*
RADIUS サーバ ロード バランシングの設定	*『Cisco IOS Security Configuration Guide』*
Kerberos 設定例	*『Cisco IOS Security Configuration Guide: Security Server Protocols』*
ネットワーク サービスの認証	*『Cisco IOS Security Configuration Guide: Security Server Protocols』*
KDC の認証	*『Cisco IOS Security Configuration Guide: Security Server Protocols』*
Kerberos の設定作業リスト	*『Cisco IOS Security Configuration Guide: Security Server Protocols』*
Login enhancement の設定	*『Cisco IOS User Security Configuration Guide』*
パスワード保護コマンド	*『Cisco IOS Security Command Reference』*
Kerberos コマンド	*『Cisco IOS Security Command Reference』*
セキュア シェル コマンド	*『Cisco IOS Security Command Reference』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

その他の関連資料

CHAPTER 13

IEEE 802.1x ポートベース認証の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IEEE 802.1x ポートベースの認証の設定に関する制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

IEEE 802.1x ポート ベースの認証の設定に関する情報

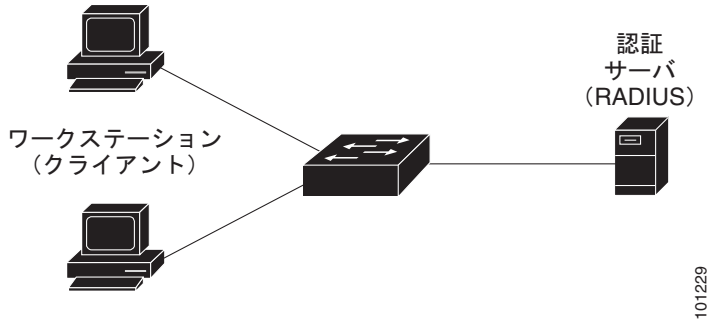
IEEE 802.1x ポートベースの認証

標準では、クライアント サーバ ベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを介して LAN に接続するの防ぎます。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN サービスを利用できるようにします。

IEEE 802.1x アクセス コントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、およびスパニングツリー プロトコル（STP）トラフィックしか許可されません。認証後、通常のトラフィックをポート経由で送受信できます。

デバイスの役割

図 13-1　802.1x におけるデバイスの役割



- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP OS（オペレーティング システム）に付属しているような 802.1x 準拠のクライアント ソフトウェアを実行する必要があります （クライアントは、802.1x 標準では*サプリカント*といいます）。

（注）　Windows XP のネットワーク接続と 802.1x 認証の問題を解決するには、次の URL にある「Microsoft Knowledge Base」を参照してください。
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ*：実際にクライアントの認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対して透過的に行われます。今回のリリースでサポートされる認証サーバは、Extensible Authentication Protocol（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムだけです。これは Cisco Secure Access Control Server バージョン 3.0 以降で利用できます。RADIUS はクライアント/サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- *スイッチ*（エッジ スイッチまたはワイヤレス アクセス ポイント）：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する RADIUS クライアントが含まれています （スイッチは、802.1x 標準では*オーセンティケータ*といいます）。

  スイッチが EAPOL フレームを受信して認証サーバにリレーすると、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS 形式で再度カプセル化されます。カプセル化では EAP フレームの変更は行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

  仲介装置として動作できる装置は、Cisco ESS-2020、IE 2000、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940 の各スイッチや、ワイヤレス アクセス ポイントなどです。これらのデバイスでは、RADIUS クライアントおよび 802.1x 認証をサポートするソフトウェアが稼働している必要があります。

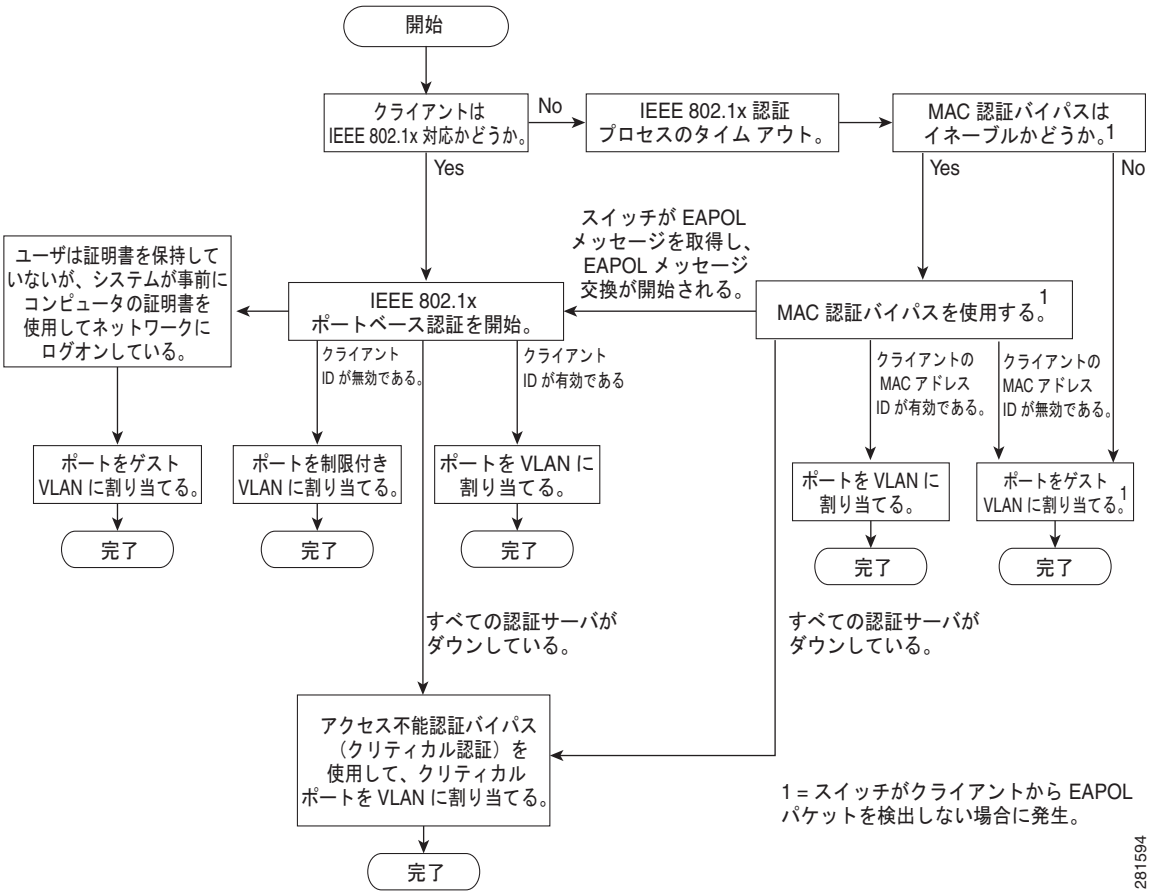
認証プロセス

802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

（注） アクセスできない認証バイパスは、クリティカル認証、または AAA 失敗ポリシーとも呼ばれます。

図 13-2　認証フローチャート



スイッチは、次のいずれかの状況が発生するとクライアントを再認証します。

- 定期再認証がイネーブルで、再認証タイマーが満了した場合。

  スイッチ固有の値を使用するか、または RADIUS サーバの値に基づくように再認証タイマーを設定できます。

  RADIUS サーバを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS 属性（属性 [27]）は、再認証が発生するまでの時間を指定します。

  Termination-Action RADIUS 属性（属性 [29]）は、再認証中に実行するアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。*Initialize* アクションが設定されている場合は（属性値は *DEFAULT*）、802.1x セッションが終了し、再認証中に接続は失われます。*ReAuthenticate* アクションが設定されている場合（属性値は RADIUS-Request）、再認証中にセッションは影響を受けません。

- **dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力して、クライアントを手動で再認証した場合。

マルチドメイン認証（MDA）がポートでイネーブルにされている場合、このフローが使用されます。ただし、音声許可の場合はいくつかの例外があります。MDA の詳細については、「マルチドメイン認証」（P.13-10）を参照してください。

スイッチおよび RADIUS サーバ間の通信

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。1 台の RADIUS サーバ上の異なる 2 つのホスト エントリが 1 つのサービス（認証など）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

認証の開始およびメッセージ交換

802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンク ステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

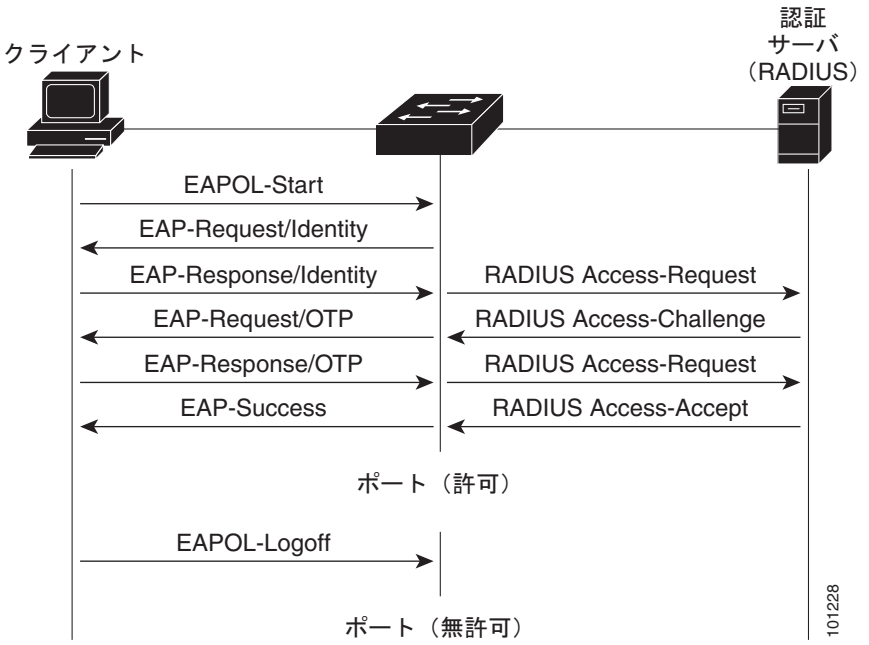
ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）　ネットワーク アクセス デバイスで 802.1x 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステートおよび無許可ステートのポート」（P.13-9）を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。詳細については、「許可ステートおよび無許可ステートのポート」（P.13-9）を参照してください。

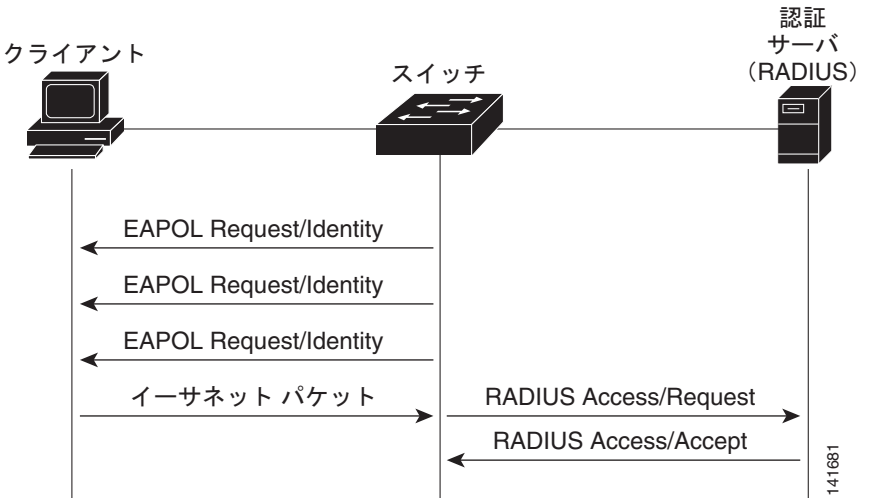
実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 13-3 に、クライアントが RADIUS サーバとの間で OTP（ワンタイム パスワード）認証方式を使用する際に行われるメッセージ交換を示します。

図 13-3　メッセージ交換



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS Access/Request フレームにこの情報を保存します。サーバがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1x 認証を停止します。

図 13-4　MAC 認証バイパス中のメッセージ交換



認証マネージャ

ポートベース認証方法

表 13-1 に、これらのホスト モードでサポートされている認証方法を示します。

- シングル ホスト：ポートで認証できるデータまたは音声ホスト（クライアント）は 1 つだけです。
- マルチ ホスト：同じポートで複数のデータ ホストを認証できます。（ポートがマルチ ホスト モードで無許可になると、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します）。
- マルチドメイン認証（MDA）：同じスイッチ ポートでデータ デバイスと音声デバイスの両方を認証できます。ポートはデータ ドメインと音声ドメインに分割されます。
- 複数認証：複数のホストがデータ VLAN で認証できます。このモードでは、音声 VLAN が設定されている場合、VLAN で 1 クライアントだけ使用できます。

表 13-1　802.1x の機能

	モード			
認証方式	**シングル ホスト**	**マルチ ホスト**	**MDA[1]**	**複数認証[2]**
802.1x	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[4] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]	ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]	ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
スタンドアロン Web 認証[4]	プロキシ ACL、Filter-Id 属性、ダウンロード可能な ACL[2]			
NAC レイヤ 2 IP 検証	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
フォールバック メソッドとしての Web 認証[5]	Proxy ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	Proxy ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	Proxy ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	Proxy ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3]

1. MDA = マルチドメイン認証。
2. *multiauth* とも呼ばれます。

3. Cisco IOS Release 12.2(50)SE 以降でサポートされています。
4. Cisco IOS Release 12.2(50)SE 以降でサポートされています。
5. 802.1x 認証をサポートしていないクライアントの場合。

ユーザ単位 ACL および Filter-Id

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、ユーザ単位 ACL および Filter-Id がサポートされているのは、シングル ホスト モードだけでした。Cisco IOS Release 12.2(50) では、MDA および複数認証（multiauth）をイネーブルにしたポートのサポートが追加されました。12.2(52)SE 以降では、マルチホスト モードのポートのサポートが追加されました。

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、スイッチで設定された ACL は、Catalyst 6500 スイッチなど、Cisco IOS ソフトウェアを実行する別のデバイスで設定された ACL と互換性がありませんでした。

Cisco IOS Release 12.2(50)SE 以降では、スイッチで設定された ACL は、Cisco IOS リリースを実行する他のデバイスで設定された ACL と互換性があります。

（注）　**any** は、ACL の発信元としてだけ設定できます。

（注）　マルチ ホスト モードで設定された ACL では、ステートメントの発信元部分は *any* でなければなりません （たとえば、**permit icmp** *any* **host 10.10.1.1**）。

定義された ACL の発信元ポートには *any* を指定する必要があります。指定しない場合、ACL は適用できず、認証は失敗します。シングル ホストは唯一例外的に後方互換性をサポートします。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。

マルチ ホスト ポートで認証されるホストが 1 つだけで、他のホストが認証なしでネットワーク アクセスを取得する場合、発信元アドレスに *any* を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドは、802.1x、MAC 認証バイパスおよび Web 認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。一般的な認証コマンドには、**authentication host-mode**、**authentication violation** および **authentication timer** インターフェイス コンフィギュレーション コマンドがあります。

802.1x 専用コマンドは、頭に **dot1x** または **authentication** キーワードが付きます。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。ただし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは常にグローバルに 802.1x 認証をイネーブルまたはディセーブルにします。

（注）　802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

認証マネージャで生成された冗長なシステム メッセージをフィルタリングできます。通常、フィルタリングされた内容は、認証の成功と関係しています。802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの冗長なメッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の冗長なメッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC 認証バイパス（MAB）の冗長なメッセージをフィルタリングします。

詳細については、このリリースのコマンド リファレンスを参照してください。

許可ステートおよび無許可ステートのポート

802.1x 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、*無許可*ステートです。このステートでは、音声 VLAN（仮想 LAN）ポートとして設定されていないポートは 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは*許可*ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコル パケットが許可された後クライアントが正常に認証されます。

802.1x をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized**：ポートを無許可ステートのままにして、クライアントが認証を試みてもすべて無視します。スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto**：802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

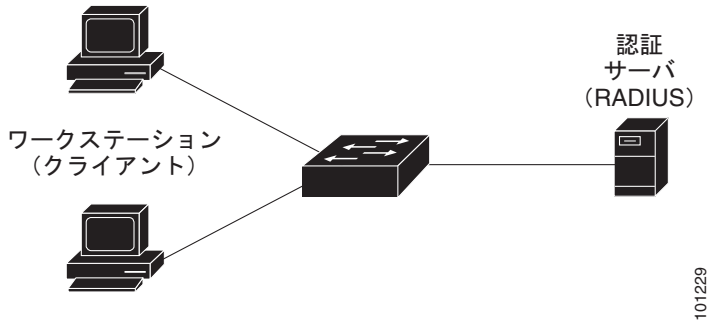
ポートのリンク ステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

802.1x のホスト モード

802.1x ポートは、シングル ホスト モードまたはマルチ ホスト モードで設定できます。シングル ホスト モード（図 13-1（P.13-2）を参照）では、802.1x 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチ ホスト モードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。図 13-5（P.13-10）に、ワイヤレス LAN における 802.1x ポートベース認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、スイッチは接続されたすべてのクライアントのネットワーク アクセスを拒否します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

図 13-5　　マルチ ホスト モードの例



スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポートに接続できます。詳細については、「マルチドメイン認証」（P.13-10）を参照してください。

マルチドメイン認証

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポート上で認証できます。ポートはデータ ドメインと音声ドメインに分割されます。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定するには、「ホスト モードの設定」（P.13-38）を参照してください。
- ホスト モードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細については、第 17 章「VLAN の設定」を参照してください。

- 音声デバイスを許可するには、値 `device-traffic-class=voice` の Cisco 属性値（AV）ペア属性を送信するように AAA サーバを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、errordisable になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC アドレス制限にカウントされません。
- MDA は、フォールバック方法として MAC 認証バイパスを使用して、IEEE 802.1x 認証をサポートしていないデバイスにスイッチポートを接続できます。詳細については、「MAC 認証バイパスの注意事項」（P.13-34）を参照してください。
- *データ*または*音声*デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスが*データ* VLAN で検出された場合や、複数の音声デバイスが*音声* VLAN で検出された場合、ポートは errdisable になります。
- ポートのホスト モードがシングル ホストまたはマルチホストからマルチドメイン モードに変更される場合、許可済みのデータ デバイスはポートで許可済みのままになります。ただし、ポート音声 VLAN の Cisco IP Phone は自動的に削除され、そのポートで再認証される必要があります。
- ポートがシングルまたはマルチ ホスト モードからマルチドメイン モードに変更された後に、ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック方法は設定されたままになります。
- マルチドメイン モードからシングル ホストまたはマルチ ホスト モードにポートを切り替えると、ポートからすべての認証済みデバイスが削除されます。
- データ ドメインがまず許可されてゲスト VLAN に配置された場合、IEEE 802.1x 非対応音声デバイスは認証をトリガーするために音声 VLAN 上のパケットにタグを付ける必要があります。電話機はタグ付きトラフィックを送信する必要はありません （802.1x 対応電話の場合も同様です）。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーがある許可済みデバイスは、ポートの音声およびデータ VLAN の両方のトラフィックに影響を与える可能性があります。使用する場合、ポート上の 1 デバイスだけでユーザ単位 ACL が実行されます。

詳細については、「ホスト モードの設定」（P.13-38）を参照してください。

802.1x 複数認証モード

複数認証（multiauth）モードでは、データ VLAN で複数のクライアントを認証できます。各ホストは個別に認証されます。音声 VLAN が設定されている場合、このモードでは、VLAN で 1 クライアントだけ認証できます （ポートが他の音声クライアントを検出すると、これらはポートから廃棄されますが、違反エラーは発生しません）。

ハブまたはアクセス ポイントが 802.1x 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。

802.1x 以外のデバイスでは、MAC 認証バイパスまたは Web 認証をホスト単位認証フォールバック メソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

複数認証ポートで認証できるデータ ホストの数には制限はありません。ただし、音声 VLAN が設定されている場合、許可される音声デバイスは 1 台だけです。ホスト制限がないため、定義された違反はトリガーされません。たとえば、別の音声デバイスが検出された場合、これは通知なしで廃棄され、違反はトリガーされません。

音声 VLAN の MDA 機能の場合、複数認証モードでは、認証サーバから受け取った VSA に応じて、認証されたデバイスがデータまたは音声のいずれかの VLAN に割り当てられます。

（注）　ポートがマルチ認証モードの場合、ゲスト VLAN、および認証失敗 VLAN 機能はアクティブになりません。

クリティカル認証モードおよびクリティカル VLAN の詳細については、「アクセス不能認証バイパスを使用した 802.1x 認証」（P.13-22）を参照してください。

ポートでのマルチ認証モードの設定の詳細については、「ホスト モードの設定」（P.13-38）を参照してください。

MAC 移動

あるスイッチ ポートで MAC アドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MAC アドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチ ポート間に別のデバイス（ハブまたは IP Phone など）がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC 移動をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。

MAC 移動はすべてのホスト モードでサポートされます （認証ホストは、ポートでイネーブルにされているホスト モードに関係なく、スイッチの任意のポートに移動できます）。

MAC アドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。

MAC 移動の機能は、音声およびデータ ホストの両方に適用されます。

（注）　オープン認証モードでは、MAC アドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

詳細については、「任意の 802.1x 認証機能の設定」（P.13-40）を参照してください。

MAC 置換

MAC 置換機能は、ホストが、別のホストがすでに認証済みであるポートに接続しようとすると発生する違反に対処するように設定できます。

（注）　違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホスト モードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 既存の認証済み MAC アドレスを使用するポートで新しい MAC アドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ ホストの MAC アドレスを、新しい MAC アドレスで置き換えます。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MAC アドレスはただちに MAC アドレス テーブルに追加されます。

詳細については、「任意の 802.1x 認証機能の設定」（P.13-40）を参照してください。

802.1x アカウンティング

802.1x 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1x アカウンティングは、デフォルトでディセーブルです。802.1x アカウンティングをイネーブルにすると、次の処理を 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証の正常な発生
- 再認証の失敗

スイッチは 802.1x アカウンティング情報を記録しません。その代わり、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定する必要があります。

802.1x アカウンティング属性値ペア

RADIUS サーバに送信された情報は、属性値（AV）ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます （たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です）。

AV ペアは、802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START：新規ユーザ セッションの開始時に送信されます。
- INTERIM：既存のセッション中にアップデートのために送信されます。
- STOP：セッション終了時に送信されます。

表 13-2　アカウンティング AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常時送信	常時送信	常時送信
属性 [4]	NAS-IP-Address	常時送信	常時送信	常時送信
属性 [5]	NAS-Port	常時送信	常時送信	常時送信
属性 [8]	Framed-IP-Address	非送信	条件に応じて送信[1]	条件に応じて送信[1]
属性 [25]	Class	常時送信	常時送信	常時送信
属性 [30]	Called-Station-ID	常時送信	常時送信	常時送信
属性 [31]	Calling-Station-ID	常時送信	常時送信	常時送信
属性 [40]	Acct-Status-Type	常時送信	常時送信	常時送信
属性 [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
属性 [42]	Acct-Input-Octets	非送信	常時送信	常時送信
属性 [43]	Acct-Output-Octets	非送信	常時送信	常時送信
属性 [44]	Acct-Session-ID	常時送信	常時送信	常時送信
属性 [45]	Acct-Authentic	常時送信	常時送信	常時送信
属性 [46]	Acct-Session-Time	非送信	常時送信	常時送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
属性 [61]	NAS-Port-Type	常時送信	常時送信	常時送信

1. ホストに対して有効な Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在している場合にのみ、Framed-IP-Address の AV ペアは送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。

AV ペアの詳細については、RFC 3580『802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサプリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりません。

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- 802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタックのすべてのポートがテストされます。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x に対応していません。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホスト（たとえば、IP Phone に接続される PC）を扱うポートに送信できます。Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアントに生成されます。

802.1x 準備状態チェックのスイッチの設定については、「802.1x 準備状態チェックの設定」（P.13-36）を参照してください。

VLAN 割り当てを使用した 802.1x 認証

RADIUS サーバは、VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバ データベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声デバイスが許可されているときに、RADIUS サーバから許可された VLAN が返される場合、このポートの音声 VLAN は、割り当てられた音声 VLAN でパケットを送受信するように設定されています。音声 VLAN 割り当ては、マルチドメイン認証（MDA）対応のポートでのデータ VLAN 割り当てと同じように機能します。詳細については、「マルチドメイン認証」（P.13-10）を参照してください。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

  設定エラーには、ルーテッド ポートへの VLAN の指定、誤った VLAN ID、存在しないまたは内部（ルーテッド ポートの）VLAN ID、リモート SPAN（RSPAN）VLAN、シャットダウンまたは一時停止された VLAN があります。マルチドメイン ホスト ポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。
- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバにより指定）に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。

- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
  - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
  - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

トランク ポート、ダイナミック ポート、または VLAN メンバーシップ ポリシー サーバ（VMPS）によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。（アクセス ポートで 802.1x 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN 名、VLAN ID または VLAN-Group
  - [83] Tunnel-Preference

  属性 [64] は、値 *VLAN*（タイプ 13）でなければなりません。属性 [65] は、値 *802*（タイプ 6）でなければなりません。属性 [81] は、802.1x 認証ユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

トンネル属性の例については、「ベンダー固有 RADIUS 属性の設定：例」（P.12-47）を参照してください。

音声対応 802.1x セキュリティ

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

スイッチで音声認識 802.1x 音声セキュリティを設定する場合、次の注意事項に従ってください。

- **errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力して、音声認識 802.1x セキュリティをイネーブルにします。音声認識 802.1x セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。このコマンドは、スイッチの 802.1x 設定ポートのすべてに適用されます。

（注）　**shutdown vlan** キーワードを指定しない場合、errdisable ステートになったときにポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して、errordisable リカバリを設定すると、ポートは自動的に再びイネーブルにされます。errordisable リカバリがポートで設定されていない場合、**shutdown** および **no-shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface** *interface-id* **vlan** [*vlan-list*] 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

ユーザ単位 ACL を使用した 802.1x 認証

ユーザ単位アクセス コントロール リスト（ACL）をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザに提供できます。RADIUS サーバは、802.1x ポートに接続されるユーザを認証する場合、ユーザ ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザ セッションの期間中、その属性を 802.1x ポートに適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド パケットは、ルータ ACL によってフィルタリングされます。発信するルーテッド パケットには、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛盾を回避するには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。ベンダー固有属性（VSA）は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限りサポートされます。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。詳細については、第 37 章「ACL によるネットワーク セキュリティの設定」を参照してください。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位コンフィギュレーションを定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。スイッチでの Cisco IOS のアクセス リストに関するサポートが制限されているため、Filter-ID 属性は 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してだけサポートされます。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズにより制限されます。

ベンダー固有属性の例については、「ベンダー固有 RADIUS 属性の設定：例」（P.12-47）を参照してください。ACL の設定の詳細については、第 37 章「ACL によるネットワーク セキュリティの設定」を参照してください。

（注）　ユーザ単位 ACL がサポートされるのはシングル ホスト モードだけです。

ユーザ単位 ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- 802.1x ポートをシングル ホスト モードに設定します。

設定の詳細については、「認証マネージャ」（P.13-7）を参照してください。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもできます。

（注）　ダウンロード可能な ACL は *dACL* とも呼ばれます。

複数のホストが認証され、それらのホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

（注）　認証デフォルト ACL は、実行コンフィギュレーションでは表示されません。

認証デフォルト ACL は、ポートで許可ポリシーを持つホストが 1 つ以上検出されると作成されます。認証デフォルト ACL は、最後の認証セッションが終了すると削除されます。認証デフォルト ACL は、**ip access-list extended auth-default-acl** グローバル コンフィギュレーション コマンドを使用して作成できます。

（注）　認証デフォルト ACL は、シングル ホスト モードの Cisco Discovery Protocol（CDP）バイパスをサポートしていません。CDP バイパスをサポートするには、インターフェイス上のスタティック ACL を設定する必要があります。

802.1x および MAB 認証方式では、*オープン*および*クローズ*の 2 つの認証方式がサポートされます。*クローズ*認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL が作成されます。
- 認証デフォルト ACL は、ポリシーが実施されるまで DHCP トラフィックのみを許可します。

- 最初のホスト認証では、許可ポリシーは IP アドレスを挿入せずに適用されます。
- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、最初のセッションと後続セッションのポリシーが IP アドレスを挿入して実施されます。

*オープン*認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL-OPEN が作成され、すべてのトラフィックが許可されます。
- セキュリティ違反を防ぐために、IP アドレスを挿入してポリシーが実施されます。
- Web 認証は、認証デフォルト ACL-OPEN に従います。

許可ポリシーのないホストへのアクセスを制御するために、ディレクティブを設定することができます。サポートされているディレクティブの値は、*open* と *default* です。*open* ディレクティブを設定すると、すべてのトラフィックが許可されます。*default* ディレクティブは、ポートから提供されるアクセスにトラフィックを従わせます。ディレクティブは、AAA サーバ上のユーザ プロファイル、またはスイッチ上のいずれかで設定できます。AAA サーバ上でディレクティブを設定するには、**authz-directive =** *open*/*default* グローバル コマンドを使用します。スイッチ上でディレクティブを設定するには、**epm access-control open** グローバル コンフィギュレーション コマンドを使用します。

（注） ディレクティブのデフォルト値は *default* です。

設定された ACL なしでポート上の Web 認証にホストがフォールバックする場合は、次のようになります。

- ポートがオープン認証モードの場合、認証デフォルト ACL-OPEN が作成されます。
- ポートがクローズ認証モードの場合、認証デフォルト ACL が作成されます。

フォールバック ACL のアクセス コントロール エントリ（ACE）は、ユーザ単位のエントリに変換されます。設定されたフォールバック プロファイルにフォールバック ACL が含まれていない場合、ホストはポートに関連付けられた認証デフォルト ACL に従います。

（注） Web 認証でカスタム ロゴを使用し、それを外部サーバに格納する場合、認証の前にポートの ACL で外部サーバへのアクセスを許可する必要があります。外部サーバに適切なアクセスを提供するには、スタティック ポート ACL を設定するか、認証デフォルト ACL を変更する必要があります。

Cisco Secure ACS およびリダイレクト URL の属性と値のペア

スイッチはこれらの *cisco-av-pair* VSA を使用します。

- url-redirect は HTTP to HTTPS URL です。
- url-redirect-acl はスイッチ ACL 名または番号です。

スイッチは、CiscoSecure-Defined-ACL 属性値ペアを使用して、エンド ポイント デバイスからの HTTP または HTTPS リクエストを代行受信します。スイッチは、クライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure ACS の url-redirect 属性値ペアには、Web ブラウザがリダイレクトされる URL が含まれます。url-redirect-acl 属性値ペアには、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。ACL の permit ACE と一致するトラフィックがリダイレクトされます。

（注） スイッチの URL リダイレクト ACL およびデフォルト ポート ACL を定義します。

リダイレクト URL が認証サーバのクライアントに設定される場合、接続されるクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア

RADIUS の cisco-av-pair ベンダー固有属性（VSA）を使用すると、Cisco Secure ACS で CiscoSecure-Defined-ACL 属性値（AV）ペアを設定できます。このペアは、#ACL#-IP-*name-number* 属性を使って、Cisco Secure ACS でダウンロード可能な ACL の名前を指定します。

- *name* は ACL の名前です。
- *number* はバージョン番号（たとえば 3f783768）です。

ダウンロード可能な ACL が認証サーバのクライアントに設定される場合、接続されるクライアント スイッチ ポートのデフォルト ポート ACL も設定する必要があります。

デフォルト ACL がスイッチで設定されている場合、Cisco Secure ACS がホスト アクセス ポリシーをスイッチに送信すると、スイッチは、スイッチ ポートに接続されるホストからのトラフィックにこのポリシーを適用します。ポリシーが適用されない場合、デフォルト ACL が適用されます。Cisco Secure ACS がダウンロード可能な ACL をスイッチに送信する場合、この ACL は、スイッチ ポートに設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信し、デフォルト ACL が設定されていない場合、許可失敗が宣言されます。

設定の詳細については、および「ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定」（P.13-48）を参照してください。

VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID ベース MAC 認証を使用できます。スタティック VLAN ポリシーがスイッチで設定されている場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS（Microsoft）RADIUS サーバに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバで使用することで、ネットワークで一定数の VLAN を使用できます。

機能は、STP によってモニタおよび処理される VLAN の数も制限します。ネットワークは固定 VLAN として管理できます。

（注）　この機能は Cisco ACS Server ではサポートされていません（ACS サーバは、新しいホストに送信される VLAN-ID を無視して、MAC アドレスに基づいた認証だけを行います）。

設定については、「任意の 802.1x 認証機能の設定」（P.13-40）を参照してください。追加設定は、同様の MAC 認証バイパスです（「802.1x ユーザ ディストリビューションの設定」（P.13-46）を参照してください）。

ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます（802.1x クライアントのダウンロードなど）。これらのクライアントは 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト（Windows 98 システムなど）は 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。ポートはマルチホスト モードに自動的に設定されます。

スイッチは EAPOL パケット履歴を保持します。EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバが使用できない場合、許可は失敗します。ただし、EAPOL パケットの検出は EAPOL 履歴に保存されます。この音声デバイスは、AAA サーバが使用可能になると許可されます。ただし、他のデバイスによるゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンド シーケンスを使用します。

- **authentication event no-response action authorize vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

（注）　インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、単一のホスト、複数のホスト、またはマルチドメイン モードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

スイッチは *MAC 認証バイパス*をサポートします。MAC 認証バイパスが 802.1x ポートでイネーブルの場合、スイッチは、802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。802.1X ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。詳細については、「MAC 認証バイパスによる 802.1x 認証」（P.13-25）を参照してください。

詳細については、「ゲスト VLAN の設定」（P.13-42）を参照してください。

制限付き VLAN を使用した 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチの各 802.1X ポートに対して制限付き VLAN（*認証失敗 VLAN* と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできな

い 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効なクレデンシャルを持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。

（注）　両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがスパニングツリーのブロッキング ステートから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザは、次の再認証の試行まで制限付き VLAN 内に残ります。制限 VLAN のポートは、設定された間隔（デフォルトで 60 秒）で再認証を試行します。再認証に失敗した場合、ポートは制限 VLAN に残ります。再認証に成功した場合、ポートは設定された VLAN または RADIUS サーバによって送信される VLAN に移動します。再認証はディセーブルにすることができます。ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続される可能性がある場合、再認証をイネーブルのままにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼働しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、レイヤ 2 ポートにある 802.1x ポート上でシングル ホスト モードの場合だけサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

ダイナミック ARP インスペクション、DHCP スヌーピング、および IP 送信元ガードのような他のセキュリティ機能は、制限付き VLAN に対して個別に設定できます。

詳細については、「制限付き VLAN の設定」（P.13-43）を参照してください。

アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、*クリティカル認証*または *AAA 失敗ポリシー*とも呼ばれます。これらのホストを*クリティカル ポート*に接続するようにスイッチを設定できます。

新しいホストがクリティカル ポートに接続しようとすると、そのホストはユーザ指定のアクセス VLAN、*クリティカル VLAN* に移動されます。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、クリティカル ポートに接続されているホストを認証しようとする場合、設定されている RADIUS サーバのステータスをチェックします。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースである*クリティカル認証*ステートにします。

複数認証ポートのサポート

ポートが任意のホスト モードで設定されていて、AAA サーバを使用できない場合、ポートはマルチホスト モードに設定され、クリティカル VLAN に移動されます。マルチ認証（multiauth）ポートで、このアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan *vlan-id*** コマンドを使用します。新しいホストがクリティカル ポートに接続しようとすると、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

このコマンドは、すべてのホスト モードでサポートされます。

認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカル ポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、スイッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動するように、クリティカル ポートを設定できます。このように設定した場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。詳細については、このリリースのコマンド リファレンスおよび「アクセス不能認証バイパスの設定」（P.13-44）を参照してください。

機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN：アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 8021.x ポートでイネーブルの場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN：ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1x アカウンティング：RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。

- プライベート VLAN : プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN : アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）: アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

音声 VLAN ポートを使用した 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は 802.1x 認証とは独立して動作できます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチ ホスト モードでは、サプリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチ ホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。

（注）　音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

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

ポート セキュリティを使用した 802.1x 認証

通常、IEEE 802.1x がイネーブルの場合に、ポート セキュリティをイネーブルにすることは推奨されません。IEEE 802.1x がポートごとに（または IP テレフォニーに MDA が設定されている場合は VLAN ごとに）単一の MAC アドレスを強制するため、ポート セキュリティが冗長になり、正常な IEEE 802.1x 操作が妨害される場合もあります。

Wake-on-LAN を使用した 802.1x 認証

802.1x 認証の Wake-on-LAN（WoL）機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが 802.1x ポートを通じて接続され、ホストの電源がオフになると、802.1x ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした 802.1x 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の 802.1x ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注）　PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパニングツリー フォワーディング ステートに変わります。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスによる 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレス（図 13-2（P.13-4）を参照）に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。802.1X ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが 802.1x 対応サプリカントであることを確認し、（MAC 認証バイパス機能ではなく）802.1x 認証を使用してインターフェイスを認証します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、802.1x サプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が実行されるとき、Termination-Action RADIUS 属性値が DEFAULT であるために以前のセッションが終了した場合、スイッチは優先再認証プロセスとして 802.1x 認証を使用します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。再認証プロセスは、802.1x で認証されたクライアントの場合と同じです。再認証中に、ポートは前に割り当てられた VLAN に残ります。再認証に成功した場合、スイッチはポートを同じ VLAN 内に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていればポートにゲスト VLAN を割り当てます。

再認証が Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）に基づいており、Termination-Action RADIUS 属性（属性 [29]）アクションが *Initialize* である場合は（属性値は *DEFAULT*）、MAC 認証バイパス セッションが終了し、再認証中に接続は失われます。MAC 認証バイパスがイネーブルになって 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再許可を開始します。AV ペアの詳細については、RFC 3580『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- 802.1x 認証：802.1x 認証がポートでイネーブルの場合にだけ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ：「ポート セキュリティを使用した 802.1x 認証」（P.13-24）を参照してください。
- 音声 VLAN：「音声 VLAN ポートを使用した 802.1x 認証」（P.13-24）を参照してください。
- VLAN メンバーシップ ポリシー サーバ（VMPS）：802.1x および VMPS は相互に排他的です。
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- Network Admission Control（NAC）レイヤ 2 IP 検証：この機能は、802.1X ポートが例外リスト内のホストを含む MAC 認証バイパスを使用して認証されると有効になります。
- ネットワーク エッジ アクセス トポロジ（NEAT）：MAB と NEAT は相互排他的です。インターフェイス上で NEAT がイネーブルの場合は、MAB をイネーブルにできません。また、インターフェイス上で MAB がイネーブルの場合は、NEAT をイネーブルにできません。

設定の詳細については、「認証マネージャ」（P.13-7）を参照してください。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。「認証マネージャ CLI コマンド」（P.13-8）を参照してください。

802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。

- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロードバランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。

（注）　RADIUS サーバは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合わせて VLAN 情報を送信できます。

802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされることを確認してください。
- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

詳細については、「802.1x ユーザ ディストリビューションの設定」（P.13-46）を参照してください。

Network Admission Control レイヤ 2 802.1x 検証

スイッチは、デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウイルス対策の状態または*ポスチャ*をチェックする Network Admission Control（NAC）レイヤ 2 802.1x 検証をサポートしています。NAC レイヤ 2 802.1x 検証を使用すると、次の作業を実行できます。

- Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）を認証サーバからダウンロードします。
- Session-Timeout RADIUS 属性（属性 [27]）の値として再認証試行の間隔（秒）を設定し、RADIUS サーバからクライアントに対するアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS 属性（属性 [29]）を使用してクライアントを再認証しようとするときに実行されるアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。この値が RADIUS-Request である場合は、再認証プロセスが開始されます。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから選択されます。
- **show authentication** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、802.1x ポートベース認証と似ています。NAC レイヤ 2 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 802.1x 検証の設定」（P.13-46）および「定期的な再認証の設定」（P.13-39）を参照してください。

NAC の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

設定の詳細については、「認証マネージャ」（P.13-7）を参照してください。

柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときに使用する方法の順序を設定できます。MAC 認証バイパスおよび 802.1x は、プライマリまたはセカンダリ認証方法として使用し、Web 認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。コンフィギュレーション コマンドについては、「任意の 802.1x 認証機能の設定」（P.13-40）を参照してください。

Open1x 認証

Open1x 認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。オープン認証が設定されている場合、新しいホストはポートに定義されているアクセス コントロール リスト（ACL）に基づいてトラフィックを渡します。ホストが認証されると、RADIUS サーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングル ホスト モードでのオープン認証：1 人のユーザだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの 1 人のユーザだけ、およびデータ ドメインの 1 人のユーザだけが許可されます。
- マルチ ホスト モードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDA の場合と似ていますが、複数のホストを認証できます。

詳細については、「ホスト モードの設定」（P.13-38）を参照してください。

（注）　オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイス コンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ

Network Edge Access Topology（NEAT）機能は、ワイヤリング クローゼット（会議室など）外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x サプリカント機能を使用することで、別のスイッチのサプリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランク ポートを介してアップストリーム スイッチに接続される場合に役に立ちます。802.1x スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。

  サプリカント スイッチが認証に成功すると、ポート モードがアクセスからトランクに変更されます。

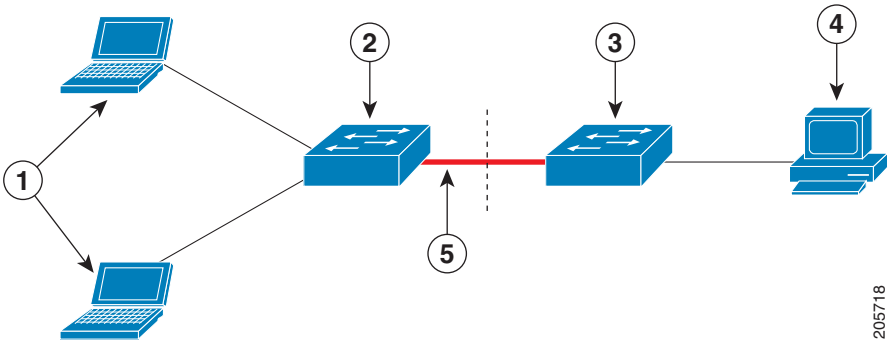
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または multiauth モードをイネーブルにできます。マルチホスト モードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

すべてのホスト モードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを Network Edge Access Topology（NEAT）のサプリカント スイッチで使用します。

- ホスト許可：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol（CISP）を使用して、サプリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します（図 13-6 を参照してください）。
- 自動イネーブル化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的にイネーブル化します。これにより、サプリカント スイッチから着信する複数の VLAN のユーザ トラフィックが許可されます。ACS で cisco-av-pair を *device-traffic-class=switch* として設定します （この設定は *group* または *user* 設定で行うことができます）。

図 13-6　CISP を使用したオーセンティケータまたはサプリカント スイッチ



1	ワークステーション（クライアント）	**2**	サプリカント スイッチ（ワイヤリング クローゼット外）
3	オーセンティケータ スイッチ	**4**	Access Control Server（ACS）
5	トランク ポート		

802.1x サプリカントおよびオーセンティケータ スイッチの注意事項

- NEAT ポートは、他の認証ポートと同じコンフィギュレーションで設定できます。サプリカント スイッチが認証すると、ポート モードはベンダー固有属性（VSA）に基づいてアクセスからトランクに変更されます （device-traffic-class=switch）。

- VSA はオーセンティケータ スイッチ ポート モードをアクセスからトランクに変更し、802.1x トランク カプセル化およびアクセス VLAN をイネーブルにします（任意の VLAN がネイティブ トランク VLAN に変換される場合）。VSA はサプリカントのポート コンフィギュレーションは変更しません。
- ホスト モードを変更して、オーセンティケータ スイッチ ポートの標準ポート コンフィギュレーションを適用するには、スイッチ VSA ではなく、Auto Smartport ユーザ定義マクロを使用することもできます。これにより、オーセンティケータ スイッチ ポートでサポートされていないコンフィギュレーションを削除して、ポート モードを *アクセス*から *トランク*に変更できます。詳細については、『*AutoSmartports Configuration Guide*』を参照してください。

詳細については、「オーセンティケータの設定」（P.13-47）を参照してください。

ACL および RADIUS Filter-Id 属性を使用した IEEE 802.1x 認証の使用

スイッチは、入力ポートの IP 標準および IP 拡張ポートのアクセス コントロール リスト（ACL）の両方をサポートします。

- 設定する ACL
- Access Control Server（ACS）からの ACL

シングル ホスト モードでの IEEE 802.1x ポートは、ACS からの ACL を使用して、異なるレベルのサービスを IEEE 802.1x 認証ユーザに提供します。RADIUS サーバは、このタイプのユーザおよびポートを認証する場合、ユーザ ID に基づいた ACL 属性をスイッチに送信します。送信された属性は、ユーザ セッション期間中、ポートに適用されます。セッションが終了、認証が失敗、またはリンクで故障が発生した場合、ポートは無許可になり、スイッチは ACL をポートから削除します。

ACS からの IP 標準および IP 拡張ポート ACL だけが Filter-Id 属性をサポートします。これは ACL の名前または番号を指定します。Filter-id 属性は、方向（インバウンドまたはアウトバウンド）、およびユーザまたはユーザが属するグループも指定できます。

- ユーザの Filter-Id 属性は、グループの Filter-Id 属性よりも優先されます。
- ACS からの Filter-Id 属性が、すでに設定されている ACL を指定する場合、これは、ユーザ設定 ACL よりも優先されます。
- RADIUS サーバが複数の Filter-Id 属性を送信する場合、最後の属性だけが適用されます。

Filter-Id 属性がスイッチで定義されていない場合、認証が失敗し、ポートが無許可ステートに戻ります。

認証マネージャの共通セッション ID

認証マネージャは、使用する認証方式に関係なく、クライアント用にただ 1 つのセッション ID（共通セッション ID と呼ばれます）を使用します。この ID は、**表示**コマンドや MIB などのすべてのレポートに使用されます。セッション ID は、セッション単位のすべての Syslog メッセージに表示されます。

セッション ID には、次の情報が含まれます。

- ネットワーク アクセス デバイス（NAD）の IP アドレス
- 一意の 32 ビット整数（機械的に増加します）
- セッション開始タイム スタンプ（32 ビット整数）

802.1x 認証のデフォルト設定

表 13-3 に、802.1x 認証のデフォルト設定を示します。

表 13-3　802.1x 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1x イネーブル ステート	ディセーブル
ポート単位の 802.1x イネーブル ステート	ディセーブル（force-authorized） ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし • 1812 • 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
再認証の回数	2 回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数）
待機時間	60 秒（スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数）
再送信時間	30 秒（スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数）
クライアント タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間）
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間） **authentication timer server** インターフェイス コンフィギュレーション コマンドを使用すると、このタイムアウト時間を変更できます。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ（スイッチ）モード	指定なし
MAC 認証バイパス	ディセーブル
音声認識セキュリティ	ディセーブル

802.1X アカウンティング

802.1x アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1x セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

802.1x 認証の注意事項

- 802.1x 認証をイネーブルにすると、他のレイヤ 2 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、RADIUS サーバが割り当てた VLAN に割り当てられているポートが、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 のスタティックアクセス ポートおよび音声 VLAN ポート上ではサポートされますが、次のポート タイプではサポートされません。
  - トランク ポート：トランク ポート上で 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。

  - EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。
  - スイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- 802.1x 認証に関連するシステム メッセージをフィルタリングすることができます。「認証マネージャ CLI コマンド」（P.13-8）を参照してください。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパスの注意事項

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。
- 802.1X 認証をプライベート VLAN ポートに設定できますが、ポート セキュリティ、音声 VLAN、ゲスト VLAN、制限付き VLAN、またはユーザ単位 ACL が付いた 802.1X 認証をプライベート VLAN ポートに設定できません。
- RSPAN VLAN、プライベート VLAN、音声 VLAN を除くあらゆる VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を軽減します（**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド）。設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - この機能はシングル ホスト モードおよびマルチホスト モードの 802.1x ポートでサポートされます。
  - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Widows XP クライアントが DHCP 用に設定されていて、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP-Success メッセージを受信しても DHCP 設定プロセスが再開されない場合があります。
  - アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとしたときにすべての RADIUS サーバが使用不可の場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制限付き VLAN 内に残ります。

- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

MAC 認証バイパスの注意事項

- 特に明記していない限り、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。詳細については、「802.1x 認証の注意事項」（P.13-32）を参照してください。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加された場合、スイッチは MAC 認証バイパスを使用してポートを再許可できます。
- ポートが許可ステートの場合、再許可が発生するまでポートはこのステートのままになります。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は 1 ～ 65535 秒です。

ポートあたりの最大デバイス数の注意事項

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングル ホスト モードの場合、アクセス VLAN で接続できるデバイスは 1 台だけです。ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限はありません。
- マルチドメイン認証（MDA）モードの場合、アクセス VLAN で 1 台のデバイス、音声 VLAN で 1 台の IP Phone が許可されます。
- マルチ ホスト モードの場合、1 台の 802.1x サプリカントだけがポートで許可されます。ただし、アクセス VLAN で許可される 802.1x 非対応ホストの数には制限はありません。音声 VLAN で許可されるデバイスの数には制限はありません。

802.1x ポートベース認証の設定方法

802.1x 認証の設定プロセス

802.1x ポートベース認証を設定するには、認証、許可、アカウンティング（AAA）をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1x の AAA の設定プロセスを示します。

ステップ 1　ユーザがスイッチのポートに接続します。

ステップ 2　認証が実行されます。

ステップ 3　RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。

ステップ 4　スイッチが開始メッセージをアカウンティング サーバに送信します。

ステップ 5　必要に応じて再認証が実行されます。

ステップ 6　スイッチが、再認証の結果に基づく中間アカウンティング アップデートをアカウンティング サーバに送信します。

ステップ 7　ユーザがポートから切断します。

ステップ 8　スイッチが停止メッセージをアカウンティング サーバに送信します。

802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用することになっている方法に続いて **default** キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 （注）　**group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**dot1x system-auth-control**	スイッチで 802.1x 認証をグローバルにイネーブルにします。
ステップ 5	**aaa authorization network** {**default**} **group radius**	（任意）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。 ユーザ単位 ACL を設定するには、シングルホスト モードを設定する必要があります。この設定は、デフォルトです。
ステップ 6	**radius-server host** *ip-address*	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 7	**radius-server key** *string*	（任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 8	**interface** *interface-id*	802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode access**	（任意）ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセス モードに設定します。
ステップ 10	**authentication port-control auto**	ポートでの 802.1x 認証をイネーブルにします。
ステップ 11	**dot1x pae authenticator**	インターフェイスのポート アクセス エンティティを、オーセンティケータとしてのみ動作し、サプリカント用のメッセージは無視するように設定します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show authentication**	入力を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチおよび RADIUS サーバ間の通信の設定

radius-server host グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号化キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバの設定」（P.12-38）を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	RADIUS サーバ パラメータを設定します。 *hostname* | *ip-address*：リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **auth-port** *port-number*：認証要求のための UDP 宛先ポートを指定します。デフォルトは 1812 です。指定できる範囲は 0 ～ 65536 です。 **key** *string*：スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 **（注）** キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず **radius-server host** コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x 準備状態チェックの設定

	コマンド	目的
ステップ 1	**dot1x test eapol-capable** [**interface** *interface-id*]	スイッチ上で 802.1x 準備状態チェックをイネーブルにします。 *interface-id*：802.1x 準備状態チェックを実行するポートを指定します。 **（注）** オプションの **interface** キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。
ステップ 2	**configure terminal**	（任意）グローバル コンフィギュレーション モードを開始します。
ステップ 3	**dot1x test timeout** *timeout*	（任意）EAPOL 応答の待機に使用するタイムアウトを設定します。範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。
ステップ 4	**end**	（任意）特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	（任意）変更したタイムアウト値を確認します。

音声認識 802.1x セキュリティのイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause security-violation shutdown vlan**	セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。 （注）　**shutdown vlan** キーワードを指定しない場合、すべてのポートが errdisable ステートになり、シャットダウンされます。
ステップ 3	**errdisable recovery cause security-violation**	（任意）自動 VLAN 単位エラー リカバリをイネーブルにします。
ステップ 4	**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]	（任意）errdisable になっている個々の VLAN を再びイネーブルにします。 • *interface-id* : 個々の VLAN を再びイネーブルにするポートを指定します。 • （任意）*vlan-list* : 再びイネーブルにする VLAN のリストを指定します。*vlan-list* を指定しない場合は、すべての VLAN が再びイネーブルになります。
ステップ 5	**shutdown** **no-shutdown**	（任意）errdisable の VLAN を再びイネーブルにして、すべての errdisable 指示をクリアします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show errdisable detect**	入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットを廃棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用することになっている方法に続いて **default** キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* : 認証用にすべての RADIUS サーバのリストを使用するには、**group radius** キーワードを入力します。 （注）　**group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

	コマンド	目的
ステップ 4	**interface** *interface-id*	802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access**	ポートをアクセス モードに設定します。
ステップ 6	**authentication violation** {**shutdown** | **restrict** | **protect** | **replace**}	違反モードを設定します。 • **shutdown**：ポートを errdisable にします。 • **restrict**：syslog エラーを生成します。 • **protect**：トラフィックをポートに送信するすべての新しいデバイスからパケットをドロップします。 • **replace**：現在のセッションを削除し、新しいホストで認証します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show authentication**	入力を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ホスト モードの設定

この作業では、802.1x 許可ポートで単一のホスト（クライアント）または複数のホストの接続を設定する方法について説明します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server vsa send authentication**	ネットワーク アクセス サーバが、ベンダー固有属性（VSA）を認識して使用するように設定します。
ステップ 3	**interface** *interface-id*	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	キーワードの意味は次のとおりです。 • **multi-auth**：音声 VLAN で 1 クライアント、データ VLAN で複数の認証クライアントを許可します。各ホストは個別に認証されます。 （注）　**multi-auth** キーワードを使用できるのは、**authentication host-mode** コマンドだけです。 • **multi-host**：シングル ホストの認証後に 802.1x 許可ポートで複数のホスト（クライアント）の接続を許可します。 • **multi-domain**：IP Phone（シスコ製または他社製）など、ホストおよび音声の両方のデバイスを 802.1x 許可ポートで認証できるようにします。 （注）　ホスト モードが **multi-domain** に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細については、第 19 章「音声 VLAN の設定」を参照してください。 • **single-host**：802.1x 許可ポートでシングル ホスト（クライアント）の接続を許可します。 指定するインターフェイスで、**authentication port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。
ステップ 5	**switchport voice vlan** *vlan-id*	（任意）音声 VLAN を設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication interface** *interface-id*	入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

定期的な再認証の設定

定期的な 802.1x クライアント再認証を有効にして、再認証の頻度を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。クライアントの定期的な再認証をイネーブルにし、再認証試行の間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication periodic**	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルに設定されています。 （注）　デフォルト値は 3600 秒です。再認証タイマーの値を変更するか、スイッチで RADIUS-provided セッション タイムアウトを使用するようにするには、**authentication timer reauthenticate** コマンドを入力します。

	コマンド	目的
ステップ 4	**authentication timer** {{[**inactivity** | **reauthenticate**]} {**restart** *value*}}	再認証の間隔（秒）を設定します。 • **inactivity**：クライアントからのアクティビティがなくなり無許可になるまでの間隔（秒単位）。 • **reauthenticate**：自動的な再認証の試行が開始されるまでの秒数。 • **restart** *value*：無許可ポートの認証を試行するまでの間隔（秒単位）。 このコマンドがスイッチの動作に影響を与えるのは、定期的再認証がイネーブルに設定されている場合だけです。
ステップ 5	**authentication timer reauthenticate** *seconds*	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 5 秒です。 （注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication interface** *interface-id*	入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

任意の 802.1x 認証機能の設定

	コマンド	目的
ステップ 1	**dot1x reauthenticate interface** *interface-id*	（任意）手動で指定の IEEE 802.1x 対応ポートの再認証を開始します。
ステップ 2	**authentication mac-move permit**	（任意）スイッチで MAC 移動をイネーブルにします。
ステップ 3	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**}	（任意）**replace**：インターフェイスで MAC を置き換えます。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。 他のキーワードは、次のような機能があります。 • **protect**：システム メッセージを生成せずに、予期しない MAC アドレスを使用するポートのパケットをドロップします。 • **restrict**：違反パケットが CPU によってドロップされ、システム メッセージが生成されます。 • **shutdown**：ポートは予期しない MAC アドレスを受信すると、errdisable になります。
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mab request format attribute 32 vlan access-vlan**	（任意）VLAN ID ベースの MAC 認証をイネーブルにします。
ステップ 3	**interface** *interface-id*	（任意）設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**authentication timer inactivity** *seconds*	（任意）スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 5	**authentication timer reauthenticate** *seconds*	（任意）スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 5 秒です。 **（注）** このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。
ステップ 6	**dot1x max-reauth-req** *count*	（任意）スイッチが認証処理を再開するまでに、クライアントへ EAP-request/identity フレームを送信する回数を変更できます。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。 **（注）** このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。
ステップ 7	**dot1x max-req** *count*	（任意）ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。
ステップ 8	**authentication control-direction {both | in}**	（任意）ポートでの WoL を使った 802.1x 認証をイネーブルにし、以下のキーワードを使用してポートを双方向または単一方向に設定します。 • **both**：ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。 • **in**：ポートを単方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。
ステップ 9	**authentication order** [**mab**] {**webauth**}	（任意）認証方式の順序を設定します。 • **mab**：認証方式の順序に MAC 認証バイパス（MAB）を追加します。 • **webauth**：認証方式の順序に Web 認証を追加します。
ステップ 10	**authentication order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポート上で使用される認証方式の順序を設定します。
ステップ 11	**authentication priority** [**dot1x** | **mab**] | {**webauth**}	（任意）認証方式をポート プライオリティ リストに追加します。
ステップ 12	**dot1x default**	設定可能な 802.1x のパラメータをデフォルト値へ戻します。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show authentication interface** *interface-id*	入力を確認します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1X アカウンティングの設定

はじめる前に

スイッチで AAA がイネーブルに設定されている必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting dot1x default start-stop group radius**	すべての RADIUS サーバのリストを使用して 802.1x アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting system default start-stop group radius**	（任意）システム アカウンティングをイネーブルにし（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1x 対応でないクライアントはゲスト VLAN に配置されます。802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングル ホスト モードまたはマルチ ホスト モードでゲスト VLAN をサポートします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access**	ポートをアクセス モードに設定します。
	または	または
	switchport mode private-vlan host	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto**	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	**authentication event no-response action authorize vlan** *vlan-id*	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4096 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication interface** *interface-id*	入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

制限付き VLAN の設定

スイッチ上に制限付き VLAN を設定している、認証サーバが有効なユーザ名またはパスワードを受信できない場合と、802.1X に準拠した場合クライアントは制限付き VLAN に移されます。スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access**	ポートをアクセス モードに設定します。
	または	または
	switchport mode private-vlan host	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto**	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize** *vlan-id*	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4096 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限付き VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication interface** *interface-id*	（任意）入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

認証試行回数の最大値の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access**	ポートをアクセス モードに設定します。
	または	または
	switchport mode private-vlan host	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto**	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize** *vlan-id*	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4096 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限付き VLAN として設定できます。
ステップ 6	**authentication event retry** *retry count*	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ～ 3 です。デフォルトは 3 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	**show authentication interface** *interface-id*	（任意）入力を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス不能認証バイパスの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server dead-criteria time** *time* **tries** *tries*	（任意）RADIUS サーバが利用不能または*停止*と見なされるときを判別するのに使用される条件を設定します。 指定できる *time* の範囲は 1 ～ 120 秒です。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 秒の間で動的に決定します。 指定できる *tries* の範囲は 1 ～ 100 です。スイッチは、デフォルトの *tries* パラメータを 10 ～ 100 の間で動的に決定します。
ステップ 3	**radius-server deadtime** *minutes*	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。デフォルト値は 0 分です。

	コマンド	目的
ステップ 4	**radius-server host** *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]	（任意）以下のキーワードを使用して RADIUS サーバのパラメータを設定します。 • **acct-port** *udp-port* : RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルト値は 1646 です。 • **auth-port** *udp-port* : RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルト値は 1645 です。 （注） RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。 • **test username** *name* : RADIUS サーバ ステータスの自動化テストをイネーブルにして、使用されるユーザ名を指定します。 • **idle-time** *time* : スイッチがテスト パケットをサーバに送信した後の間隔を分数で設定します。指定できる範囲は 1 ～ 35791 分です。デフォルトは 60 分（1 時間）です。 • **ignore-acct-port** : RADIUS サーバのアカウンティング ポートでのテストをディセーブルにします。 • **ignore-auth-port** : RADIUS サーバの認証ポートでのテストをディセーブルにします。 • **key** *string* : スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号キーを指定します。 （注） キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず **radius-server host** コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 **radius-server key** {**0** *string* | **7** *string* | *string*} グローバル コンフィギュレーション コマンドを使用しても認証および暗号キーを設定できます。
ステップ 5	**dot1x critical** {**eapol** | **recovery delay** *milliseconds*}	（任意）アクセス不能認証バイパスのパラメータを設定します。 • **eapol** : スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。 • **recovery delay** *milliseconds* : 使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカル ポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポートが毎秒再初期化可能になります）。
ステップ 6	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**authentication event server dead action [authorize | reinitialize] vlan** *vlan-id*	これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。 • **authorize** : 認証しようとする新しいホストをユーザ指定のクリティカル VLAN に移動します。 • **reinitialize** : ポートのすべての許可済みホストをユーザ指定のクリティカル VLAN に移動します。

	コマンド	目的
ステップ 8	**authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*]	アクセス不能認証バイパス機能をイネーブルにして、次のキーワードを使用して機能を設定します。 • **authorize**：ポートを認証します。 • **reinitialize**：すべての許可済みのクライアントを再初期化します。
ステップ 9	**authentication server dead action authorize** [**vlan**]	ACS サーバがダウンしているときに、アクセス VLAN または設定された VLAN のスイッチを許可します（VLAN が指定されている場合）。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show authentication interface** *interface-id*	（任意）入力を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x ユーザ ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**vlan group** *vlan-group-name* ***vlan-list*** *vlan-list*	VLAN グループを設定し、単一の VLAN または VLAN の範囲をそのグループにマッピングします。
ステップ 2	**show vlan group all** *vlan-group-name*	設定を確認します。
ステップ 3	**no vlan group** ***vlan-group-name*** **vlan-list** *vlan-list*	VLAN グループ コンフィギュレーションまたは VLAN グループ コンフィギュレーションの要素をクリアします。

NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバを使用した 802.1x 認証とも呼ばれます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication event no-response action authorize vlan** *vlan-id*	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4096 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。
ステップ 4	**authentication periodic**	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルに設定されています。

	コマンド	目的
ステップ 5	**authentication timer reauthenticate**	クライアントに対する再認証の試行を設定します（1 時間に設定）。 このコマンドがスイッチの動作に影響を与えるのは、定期的再認証がイネーブルに設定されている場合だけです。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication interface** *interface-id*	802.1x 認証設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

オーセンティケータとサプリカントの設定

スイッチ VSA ではなく Auto Smartport ユーザ定義マクロを使用して、オーセンティケータ スイッチを設定することもできます。詳細については、「SmartPort マクロの設定」の章を参照してください。

オーセンティケータの設定

はじめる前に

ワイヤリング クローゼットの外に 1 台のスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。

（注）　*cisco-av-pairs* は、ACS で *device-traffic-class=switch* として設定されている必要があります。これは、サプリカントが正常に認証された後でトランクとしてインターフェイスを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	ポート モードを **access** に設定します。
ステップ 5	**authentication port-control auto**	ポート認証モードを auto に設定します。
ステップ 6	**dot1x pae authenticator**	インターフェイスをポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 7	**spanning-tree portfast**	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で Port Fast をイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id*	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

NEAT を使用したサプリカント スイッチの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile*	802.1x クレデンシャル プロファイルを作成します。これは、サプリカントとして設定されるポートに接続する必要があります。
ステップ 4	**username** *suppswitch*	ユーザ名を作成します。
ステップ 5	**password** *password*	新しいユーザ名のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast**	ユニキャストまたはマルチキャスト パケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL *だけ*を送信させます。 これにより、NEAT がすべてのホスト モードでのサプリカント スイッチで機能できるようにもなります。
ステップ 7	**interface** ***interface-id***	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport trunk encapsulation dot1q**	ポートをトランク モードに設定します。
ステップ 9	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant**	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name*	802.1x クレデンシャル プロファイルをインターフェイスに対応付けます。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show running-config interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定

スイッチで 802.1x 認証を設定するほか、ACS を設定する必要があります。詳細については、Cisco Secure ACS コンフィギュレーション ガイドを参照してください。

（注） スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイス トラッキング テーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに適用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking**	IP デバイス トラッキング テーブルを設定します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa authorization network default group radius**	許可の方法をローカルに設定します。許可の方法を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 5	**radius-server vsa send authentication**	RADIUS VSA 送信認証を設定します。
ステップ 6	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip access-group** *acl-id* **in**	ポートの入力方向のデフォルト ACL を設定します。 **（注）**　*acl-id* はアクセス リストの名前または番号です。
ステップ 8	**show running-config interface** *interface-id*	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ダウンロード ポリシーの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **deny** *source* [*source-wildcard* **log**]	送信元アドレスおよびワイルドカードを使用してデフォルト ポート ACL を定義します。 access-list-number には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 **deny** または **permit**：条件が一致した場合にアクセスを拒否する場合は deny、許可する場合は permit を指定します。 *source*：パケットを送信するネットワークまたはホストの送信元アドレスを指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • **source**、および *source-wildcard* 値 0.0.0.0 255.255.255.255 の略を意味するキーワード **any**。*source-wildcard* 値を入力する必要はありません。 • **source** および *source-wildcard* の値 source 0.0.0.0 の省略形を意味するキーワード host。 （任意）*source-wildcard*：ワイルドカード ビットを送信元アドレスに適用します。 （任意）**log**：コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip access-group** *acl-id* **in**	ポートの入力方向のデフォルト ACL を設定します。 **（注）**　*acl-id* はアクセス リストの名前または番号です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**aaa new-model**	AAA をイネーブルにします。
ステップ 7	**aaa authorization network default group radius**	許可の方法をローカルに設定します。許可の方法を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 8	**ip device tracking**	IP デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング テーブルをディセーブルにするには、**no ip device tracking** グローバル コンフィギュレーション コマンドを使用します。
ステップ 9	**ip device tracking probe** [**count** | **interval** | **use-svi**]	（任意）IP デバイス トラッキング テーブルを設定します。 • **count** *count*：スイッチが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 5 です。デフォルトは 3 です。 • **interval** *interval*：スイッチが ARP プローブを再送信するまでに応答を待機する時間（秒単位）を設定します。指定できる範囲は 30 ～ 300 秒です。デフォルトは 30 秒です。 • **use-svi**：スイッチ仮想インターフェイス（SVI）の IP アドレスを ARP プローブの送信元として使用します。
ステップ 10	**radius-server vsa send authentication**	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。 **（注）**　ダウンロード可能な ACL が機能する必要があります。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip device tracking all**	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Open1x の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication control-direction {both | in}**	（任意）ポート制御を単一方向モードまたは双方向モードに設定します。
ステップ 4	**authentication fallback** ***name***	（任意）802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
ステップ 5	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	（任意）ポート上で認証マネージャ モードを設定します。
ステップ 6	**authentication open**	（任意）ポート上でオープン アクセスをイネーブルまたはディセーブルにします。
ステップ 7	**authentication order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポート上で使用される認証方式の順序を設定します。
ステップ 8	**authentication periodic**	（任意）ポート上で再認証をイネーブルまたはディセーブルにします。

	コマンド	目的
ステップ 9	**authentication port-control** {**auto** | **force-authorized** | **force-un authorized**}	（任意）ポートの許可ステートの手動制御をイネーブルにします。
ステップ 10	**show authentication**	（任意）入力を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x 認証設定のデフォルト値へのリセット

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	**dot1x default**	設定可能な 802.1x のパラメータをデフォルト値へ戻します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id*	入力を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IEEE 802.1x ポート ベース認証 のモニタリングとメンテナンス

コマンド	目的
show dot1x all statistics	すべてのポートの 802.1x 統計情報を表示します。
show dot1x statistics interface *interface-id*	指定されたポートの 802.1x 統計情報を表示します。
show dot1x all [**details** | **statistics** | **summary**]	スイッチの 802.1x 管理ステータスおよび動作ステータスを表示します。
show dot1x interface *interface-id*	指定されたポートの 802.1x 管理および動作ステータスを表示します。

IEEE 802.1x ポート ベースの認証 に関する設定例

準備状態チェックのイネーブル化：例

次の例では、スイッチ上の準備状態チェックをイネーブルにして、ポートを照会する方法を示します。また、照会済みポートから受信した応答も示し、接続しているデバイスが 802.1x 対応であることを確認します。

```
switch# dot1x test eapol-capable interface gigabitethernet1/2

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/2 is EAPOL
capable
```

802.1x 認証のイネーブル化：例

次に、802.1x 認証をイネーブルにして、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)# end
```

MDA のイネーブル化：例

次に、MDA をイネーブルにして、ポートでホストおよび音声デバイスの両方を許可する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

スイッチで違反した VLAN のディセーブル化 : 例

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次の例では、errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet1/2 vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

RADIUS サーバ パラメータの設定：例

次に、IP アドレス 172.120.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポートとして使用し、暗号キーを RADIUS サーバ上のキーと同じ *rad123* に設定する例を示します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

802.1x アカウンティング設定：例

次に、802.1x アカウンティングを設定する例を示します。最初のコマンドは、アカウンティングの UDP ポートとして 1813 を指定して、RADIUS サーバを設定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

802.1x ゲスト VLAN のイネーブル化：例

次に、VLAN 2 を 802.1x ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# authentication event no-response action authorize vlan 2
```

次の例では、スイッチの待機時間を 3 秒に設定し、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を 15 に設定する方法、および IEEE 802.1x ポートが DHCP クライアントに接続されているときに VLAN 2 を 802.1x ゲスト VLAN としてイネーブルにする方法を示します。

```
Switch(config-if)# authentication timer inactivity 3
Switch(config-if)# authentication timer reauthenticate 15
Switch(config-if)# authentication event no-response action authorize vlan 2
```

認証マネージャの共通セッション ID の表示：例

次に、**show authentication** コマンドの出力にセッション ID が表示される例を示します。この例では、セッション ID は 160000050000000B288508E5 です。

```
Switch# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

次に、Syslog 出力にセッション ID が表示される例を示します。この例でも、セッション ID は 160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッション ID は、NAD、AAA サーバ、その他のレポート分析アプリケーションでクライアントを識別するために使用されます。ID は自動的に表示されます。設定は必要ありません。

アクセス不能認証バイパスの設定：例

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 1/1
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

VLAN グループの設定：例

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 10

switch(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
switch# show dot1x vlan-group all
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
hr-dept                         20
```

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10,30
```

次に、VLAN を VLAN グループから削除する例を示します。

```
switch# no vlan group eng-dept vlan-list 10
```

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

switch(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

NAC レイヤ 2 802.1x 検証の設定：例

次に、NAC レイヤ 2 IEEE 802.1x 検証を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate
```

802.1x オーセンティケータ スイッチの設定：例

次に、スイッチを 802.1x オーセンティケータとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet1/1
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

802.1x サプリカント スイッチの設定：例

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

ダウンロード ポリシーの設定：例

次に、ダウンロード ポリシーのスイッチを設定する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

ポートの open1x の設定：例

次の例では、ポートの open1x を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config)# authentication control-direction both
Switch(config)# au ten tic at ion fallback profile1
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
RADIUS コマンド	『*Cisco IOS Security Command Reference*』
スイッチの認証設定	第 12 章「スイッチ ベース認証の設定」
オーセンティケータ スイッチ情報	第 16 章「SmartPort マクロの設定」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 14

Web ベース認証の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Web ベース認証設定の前提条件

- デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルに設定されています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。
- スイッチ HTTP サーバを実行するには、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要もあります。HTTP サーバは、ホストに HTTP ログイン ページを送信します。
- Web ベース認証を設定する前に、インターフェイスでデフォルトの ACL を設定する必要があります。レイヤ 2 インターフェイスのポート ACL を設定します。

Web ベース認証の設定に関する制約事項

- Web ベース認証は入力だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランク ポート、EtherChannel メンバ ポート、またはダイナミック トランク ポートではサポートされていません。
- スタティックな ARP キャッシュが割り当てられているレイヤ 2 インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検出されません。
- 2 ホップ以上離れたところにあるホストでは、STP トポロジの変更により、ホスト トラフィックの到着するポートが変わってしまった場合、トラフィックが停止する可能性があります。これは、レイヤ 2（STP）トポロジの変更後に、ARP および DHCP の更新が送信されていない場合に発生します。

- Web ベース認証は、ダウンロード可能なホスト ポリシーとして、VLAN 割り当てをサポートしていません。
- IPv6 トラフィックについては、Web ベース認証はサポートされていません。
- Web ベース認証および Network Edge Access Topology（NEAT）は、相互に排他的です。インターフェイス上で NEAT がイネーブルの場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- Web ベース認証は、RADIUS 許可サーバだけをサポートします。TACACS+ サーバまたはローカル許可を使用できません。

Web ベース認証 の設定に関する情報

Web ベース認証

IEEE 802.1x サプリカントが実行されていないホスト システムのエンド ユーザを認証するには、*Web 認証プロキシ*と呼ばれる Web ベース認証機能を使用します。

（注）　レイヤ 2 インターフェイスで Web ベース認証を設定できます。

HTTP セッションを開始すると、Web ベース認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザに HTML ログイン ページを送信します。ユーザはクレデンシャルを入力します。このクレデンシャルは、Web ベース認証機能により、認証のために認証、許可、アカウンティング（AAA）サーバに送信されます。

認証に成功した場合、Web ベース認証は、ログインの成功を示す HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザにプロンプトを表示します。最大試行回数を超過した場合、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは待機期間中、ウォッチ リストに載せられます。

ここでは、AAA の一部としての Web ベース認証の役割について説明します。

- 「デバイスの役割」（P.14-2）
- 「ホストの検出」（P.14-3）
- 「セッションの作成」（P.14-3）
- 「認証プロセス」（P.14-4）
- 「Web 認証カスタマイズ可能な Web ページ」（P.14-6）
- 「その他の機能と Web ベース認証の相互作用」（P.14-8）

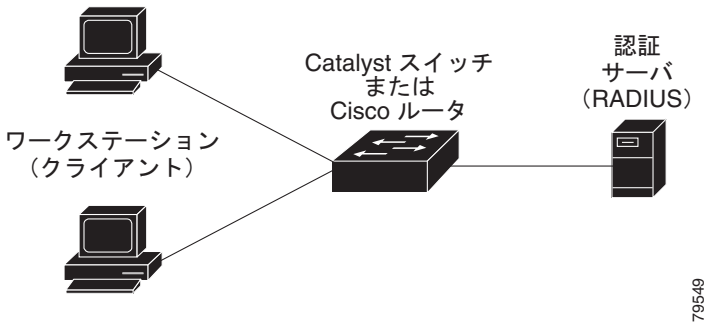
デバイスの役割

Web ベース認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script がイネーブルに設定された HTML ブラウザが実行されている必要があります。

- 認証サーバ：クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可するか、拒否するかをスイッチに通知します。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介装置（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

図 14-1　Web ベース認証デバイスの役割



ホストの検出

スイッチ は、検出されたホストに関する情報を格納するために、IP デバイス トラッキング テーブルを維持します。

（注）　デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルに設定されています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスでは、Web ベース認証は、これらのメカニズムを使用して、IP ホストを検出します。

- ARP ベースのトリガー：ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション
- DHCP スヌーピング：スイッチにより、このホストに対する DHCP バインディング エントリが作成されると、Web ベース認証に通知が送られます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをレビューします。

  ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、セッションが確立されます。
- 認証バイパスをレビューします。

  ホスト IP が例外リストに含まれていない場合、Web ベース認証は応答しないホスト（NRH）要求をサーバに送信します。

サーバの応答が *access accepted* であった場合、認証はこのホストにバイパスされます。セッションが確立されます。

- HTTP インターセプト ACL を設定します。

  NRH 要求に対するサーバの応答が *access rejected* であった場合、HTTP インターセプト ACL がアクティブ化され、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証をイネーブルにすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログイン ページを送信します。ユーザはユーザ名とパスワードを入力します。スイッチはこのエントリを認証サーバに送信します。
- 認証に成功した場合、スイッチは、認証サーバからこのユーザのアクセス ポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチは、ログイン期限切れページを送信します。このホストはウォッチ リストに入れられます。ウォッチ リストのタイム アウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答しない場合、AAA 失敗ポリシーが設定されていれば、スイッチは失敗アクセス ポリシーにホストを適用します。ログインの成功ページがユーザに送信されます（「ローカル Web 認証バナー」（P.14-4）を参照）。
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドル タイムアウト内にトラフィックを送信しなかった場合、スイッチ はクライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッション タイムアウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

ローカル Web 認証バナー

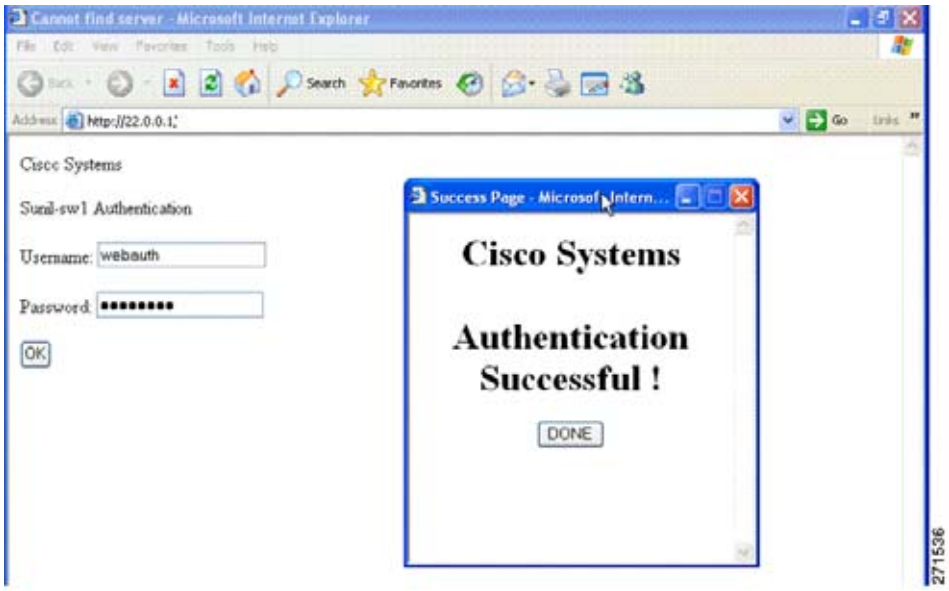
Web 認証を使用してスイッチにログインしたときに表示されるバナーを作成できます。

このバナーは、ログイン ページと認証結果ポップアップ ページの両方に表示されます。

- 認証成功
- 認証失敗
- 認証期限切れ

ip admission auth-proxy-banner http グローバル コンフィギュレーション コマンドを使用して、バナーを作成できます。ログイン ページには、デフォルトのバナー、Cisco Systems、および Switch host-name Authentication が表示されます。認証ポップアップ ページには、Cisco System と表示されます（図 14-2 を参照）。

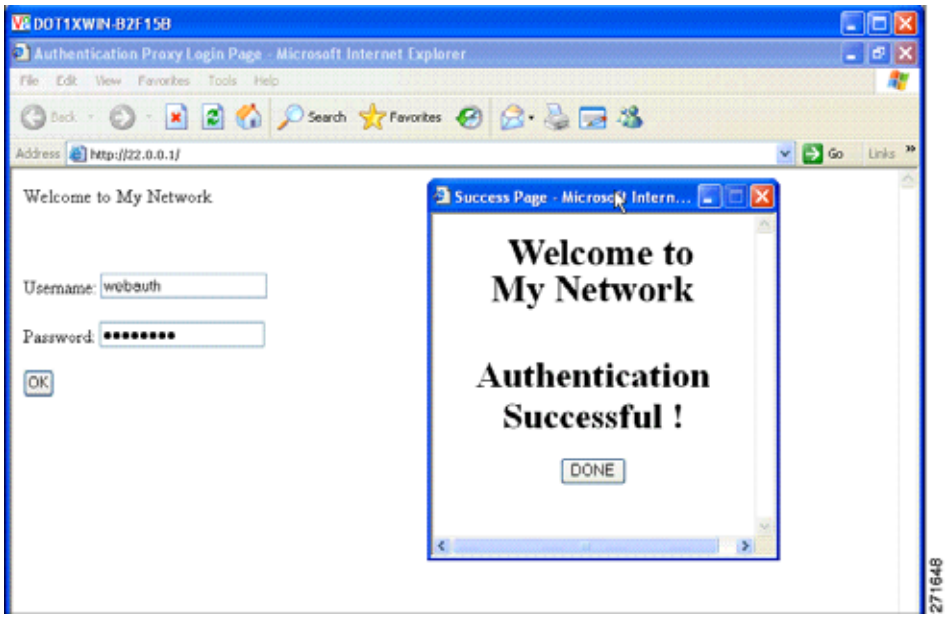
図 14-2　認証成功バナー



また、図 14-3 に示すように、バナーをカスタマイズすることもできます。

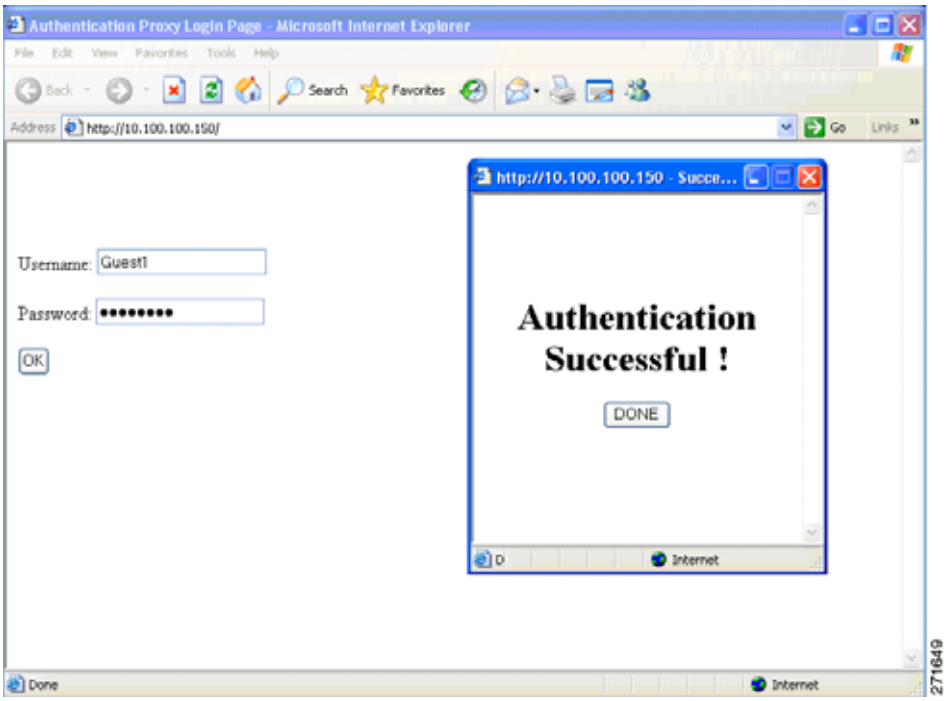
- スイッチ、ルータ、または企業名をバナーに追加するには、**ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用します。
- ロゴ、またはテキスト ファイルをバナーに追加するには、**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。

図 14-3　カスタマイズされた Web バナー



バナーがイネーブルにされていない場合、図 14-4 に示すように、Web 認証ログイン画面にはユーザ名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 14-4　　バナーが表示されていないログイン画面



詳細については、『*Cisco IOS Security Command Reference*』および「Web 認証ローカル バナーの設定」（P.14-14）を参照してください。

Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。サーバはこれらのページを使用して、ユーザに次の 4 種類の認証プロセス ステートを通知します。

- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログイン セッションが期限切れになりました。

Web 認証時の注意事項

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。

- この URL 文字列は有効な URL（例：http://www.cisco.com）でなければなりません。不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイム アウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります.
- 設定されたログイン フォームがイネーブルにされている場合、特定の URL にユーザをリダイレクトする CLI コマンドは使用できません。管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- 設定されたページには、スタック マスターまたはメンバ上のフラッシュからアクセスできます。
- ログイン ページを 1 つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。
- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システム ディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログイン ページに表示する必要のあるロゴ ファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、*web_auth_filename* の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

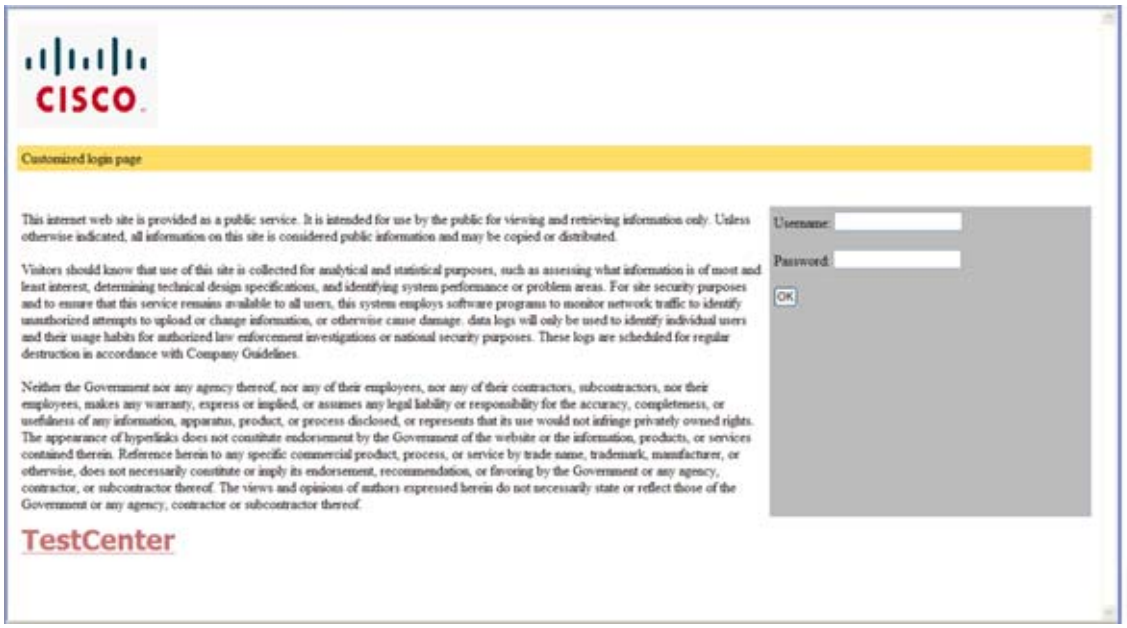
- カスタム Web ページ機能をイネーブルにするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個の HTML ファイルは、スイッチのフラッシュ メモリ内に存在しなければなりません。各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のイメージはすべて、アクセス可能は HTTP サーバ上に存在しなければなりません。インターセプト ACL は、管理ルール内で設定します。
- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL の設定を必要とします。
- 有効な DNS サーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理ルール内にインターセプト ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルに設定されている場合、設定された auth-proxy-banner は使用されません。
- カスタム Web ページ機能がイネーブルに設定されている場合、ログインの成功に対するリダイレクション URL は使用できません。
- カスタム ファイルの指定を解除するには、このコマンドの **no** 形式を使用します。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事項に従ってください。

- ログイン フォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

図 14-5 に示すように、デフォルトの内部 HTML ページを独自の HTML ページで置き換えることができます。認証後のユーザのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

図 14-5　　カスタマイズ可能な認証ページ



その他の機能と Web ベース認証の相互作用

- 「ポート セキュリティ」（P.14-8）
- 「LAN ポート IP」（P.14-9）
- 「ゲートウェイ IP」（P.14-9）
- 「ACL」（P.14-9）
- 「コンテキストベース アクセス コントロール」（P.14-9）
- 「802.1X 認証」（P.14-9）
- 「EtherChannel」（P.14-9）

ポート セキュリティ

Web ベース認証とポート セキュリティは、同じポートに設定できます。Web ベース認証はポートを認証し、ポート セキュリティは、クライアントの MAC アドレスを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

ポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定」（P.29-12）を参照してください。

LAN ポート IP

LAN ポート IP（LPIP）とレイヤ 2 Web ベース認証は、同じポートに設定できます。ホストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。LPIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。ホストが認証され、ポスチャが再度検証されます。

ゲートウェイ IP

VLAN のいずれかのスイッチ ポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP（GWIP）を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホスト ポリシーが適用されます。GWIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証のホスト ポリシーが適用された後だけ、ホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、ポート ACL（PACL）をデフォルトのアクセス ポリシーとして設定する必要があります。認証後、Web ベース認証のホスト ポリシーは、PACL に優先されます。

（注）　プロキシ ACL が Web ベース認証クライアントに設定されると、プロキシ ACL はダウンロードされて、許可プロセスの一部として適用されます。したがって、PACL はプロキシ ACL のアクセス コントロール エントリ（ACE）を表示します。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

コンテキストベース アクセス コントロール

コンテキストベース アクセス コントロール（CBAC）が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証は設定できません。

802.1X 認証

フォールバック認証メソッドとして設定する場合を除き、Web ベース認証は 802.1x 認証と同じポート上には設定できません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバ チャネルに適用されます。

デフォルトの Web ベース認証の設定

表 14-1　デフォルトの Web ベース認証の設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし • 1812 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

スイッチと RADIUS サーバ間の通信設定

RADIUS セキュリティ サーバの識別情報は次のとおりです。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。

Web ベース認証の設定方法

認証ルールとインターフェイスの設定

	コマンド	目的
ステップ 1	**ip admission name** *name* **proxy http**	Web ベース許可の認証ルールを設定します。
ステップ 2	**interface** *type slot/port*	インターフェイス コンフィギュレーション モードを開始し、Web ベースの認証をイネーブルにする入力レイヤ 2 インターフェイスを指定します。 *type* は、Fast Ethernet、Gigabit Ethernet、10-Gigabit Ethernet があります。
ステップ 3	**ip access-group** *name*	デフォルト ACL を適用します。
ステップ 4	**ip admission** *name*	指定されたインターフェイスに Web ベース認証を設定します。
ステップ 5	**exit**	コンフィギュレーション モードに戻ります。
ステップ 6	**ip device tracking**	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip admission configuration**	設定を表示します。

AAA 認証の設定

	コマンド	目的
ステップ 1	**aaa new-model**	AAA 機能をイネーブルにします。
ステップ 2	**aaa authentication login default group** {*tacacs+* | *radius*}	ログイン時の認証方法のリストを定義します。
ステップ 3	**aaa authorization auth-proxy default group** {*tacacs+* | *radius*}	Web ベース許可の許可方式リストを作成します。
ステップ 4	**radius-server host** {*hostname* | *ip-address*} **test username** *username*	AAA サーバを指定します。 リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username** *username* は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された username は有効なユーザ名である必要はありません。
ステップ 5	**radius-server key** *string*	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。複数の RADIUS サーバを使用するには、それぞれのサーバでこのコマンドを入力してください。

および RADIUS サーバ間の通信の設定

	コマンド	目的
ステップ 1	**ip radius source-interface** *interface_name*	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **test username** *username*	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username** *username* は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された *username* は有効なユーザ名である必要はありません。 **key** オプションは、スイッチと RADIUS サーバの間で使用される認証と暗号キーを指定します。 複数の RADIUS サーバを使用するには、それぞれのサーバでこのコマンドを入力してください。
ステップ 3	**radius-server key** *string*	スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する、認証キーおよび暗号化キーを設定します。
ステップ 4	**radius-server vsa send authentication**	RADIUS サーバからの ACL のダウンロードをイネーブルにします。この機能は、Cisco IOS Release 12.2(50)SG でサポートされています。
ステップ 5	**radius-server dead-criteria tries** *num-tries*	RADIUS サーバに送信されたメッセージへの応答がない場合に、このサーバが非アクティブであると見なすまでの送信回数を指定します。指定できる *num-tries* の範囲は 1 ～ 100 です。

HTTP サーバの設定

	コマンド	目的
ステップ 1	**ip http server**	HTTP サーバをイネーブルにします。Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
ステップ 2	**ip http secure-server**	HTTPS をイネーブルにします。

認証プロキシ Web ページのカスタマイズ

はじめる前に

Web ベースの認証中、スイッチのデフォルト HTML ページではなく、代わりの HTML ページがユーザに表示されるように、Web 認証を設定できます。

カスタム認証プロキシ Web ページの使用を指定するには、まず、カスタム HTML ファイルをスイッチのフラッシュ メモリに保存し、次にグローバル コンフィギュレーション モードでこのタスクを実行します。

	コマンド	目的
ステップ 1	**ip admission proxy http login page file** *device:login-filename*	スイッチのメモリ ファイル システム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。*device:* はフラッシュ メモリです。
ステップ 2	**ip admission proxy http success page file** *device:success-filename*	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 3	**ip admission proxy http failure page file** *device:fail-filename*	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 4	**ip admission proxy http login expired page file** *device:expired-filename*	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。

成功ログインに対するリダイレクション URL の指定

認証後に、内部*成功* HTML ページを効果的に置き換え、ユーザのリダイレクト先となる URL を指定することができます。

コマンド	目的
ip admission proxy http success redirect *url-string*	デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。

Web ベース認証パラメータの設定

失敗できるログイン試行回数の最大値を設定します。失敗した試行回数がこの値を超えると、クライアントは待機期間中、ウォッチ リストに載せられます。

	コマンド	目的
ステップ 1	**ip admission max-login-attempts** *number*	失敗ログイン試行の最大回数を設定します。指定できる範囲は 1 ～ 2147483647 回です。デフォルトは 5 です。
ステップ 2	**end**	特権 EXEC モードに戻ります。
ステップ 3	**show ip admission configuration**	認証プロキシの設定を表示します。
ステップ 4	**show ip admission cache**	認証エントリのリストを表示します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Web 認証ローカル バナーの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*]	ローカル バナーをイネーブルにします。 （任意）*C banner-text C* と入力して、カスタム バナーを作成します。ここで、*C* は区切り文字、またはバナーに表示されるファイル（例：ロゴ、またはテキスト ファイル）を示すファイル パスです。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Web ベース認証キャッシュ エントリの削除

シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。

コマンド	目的
clear ip auth-proxy cache {* | *host ip address*}	スイッチから認証プロキシ エントリを消去します。
clear ip admission cache {* | *host ip address*}	スイッチから IP アドミッション キャッシュ エントリを消去します。

Web ベース認証のモニタリングおよびメンテナンス

コマンド	目的
show authentication sessions	Web ベース認証設定を表示します。
show ip admission configuration	認証プロキシの設定を表示します。
show ip admission cache	認証エントリのリストを表示します。

Web ベース認証の設定例

Web ベース認証のイネーブル化と表示：例

次に、Fast Ethernet ポート 5/1 で Web ベース認証をイネーブルにする例を示します。

```
Switch(config)# ip admission name webauth1 proxy http
Switch(config)# interface fastethernet 5/1
Switch(config-if)# ip admission webauth1
Switch(config-if)# exit
Switch(config)# ip device tracking
```

次に、設定を確認する例を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name webauth1
    http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA のイネーブル化：例

次の例では、AAA をイネーブルにする方法を示します。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# aaa authorization auth-proxy default group radius
```

RADIUS サーバ パラメータの設定：例

次の例では、スイッチで RADIUS サーバ パラメータを設定する方法を示します。

```
Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.l20.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(config)# radius-server dead-criteria tries 2
```

カスタム認証プロキシ Web ページの設定：例

次の例では、カスタム認証プロキシ Web ページを設定する方法を示します。

```
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
```

カスタム認証プロキシ Web ページの確認：例

次の例では、カスタム認証プロキシ Web ページの設定を確認する方法を示します。

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
 Success page         : flash:success.htm
 Fail Page            : flash:fail.htm
 Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
```

```
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

リダイレクト URL の設定：例

次の例では、成功したログインに対するリダイレクション URL を設定する方法を示します。

```
Switch(config)# ip admission proxy http success redirect www.cisco.com
```

リダイレクト URL の確認：例

次の例では、成功したログインに対するリダイレクション URL を確認する方法を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

ローカル バナーの設定：例

次の例では、「*My Switch*」というカスタム メッセージが表示されているローカル バナーを設定する方法を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
```

Web ベース認証セッションの削除：例

次に、IP アドレス 209.165.201.1 のクライアントに対する Web ベース認証セッションを削除する例を示します。

```
Switch# clear ip auth-proxy cache 209.165.201.1
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
認証プロキシ コマンド RADIUS サーバ コマンド	『*Cisco IOS Security Command Reference*』
認証プロキシ設定 RADIUS サーバ設定	『*Cisco IOS Security Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 15

インターフェイス特性の設定

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能が一部サポートされていない場合があります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

インターフェイス特性の設定の制約事項

- EtherChannel ポート グループ インターフェイスは、LAN Base イメージを実行するスイッチでサポートされます。

インターフェイス特性に関する情報

インターフェイス タイプ

ここでは、スイッチによってサポートされる各種インターフェイス タイプについて説明するとともに、これらのインターフェイス タイプの設定に関する詳細情報が記載された章についても言及します。

ポートベースの VLAN

VLAN は、ユーザの物理的な位置に関係なく、機能、チーム、またはアプリケーションなどで論理的に分割された、スイッチによるネットワークです。VLAN の詳細については、第 17 章「VLAN の設定」を参照してください。ポートで受信したパケットが転送されるのは、その受信ポートと同じ VLAN に属するポートに限られます。異なる VLAN 上のネットワーク デバイスは、VLAN 間でトラフィックをルーティングするレイヤ 3 デバイスがなければ、互いに通信できません。

VLAN に分割することにより、VLAN 内でトラフィック用の堅固なファイアウォールを実現します。また、各 VLAN には固有の MAC アドレス テーブルがあります。VLAN が認識されるのは、ローカル ポートが VLAN に対応するように設定されたとき、VLAN トランキング プロトコル（VTP）トランク上のネイバーからその存在を学習したとき、またはユーザが VLAN を作成したときです。

VLAN を設定するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して、VLAN コンフィギュレーション モードを開始します。標準範囲 VLAN（VLAN ID 1 ～ 1005）の VLAN 設定は、VLAN データベースに保存されます。VTP がバージョン 1 または 2 の場合に、拡張範囲 VLAN（VLAN ID が 1006 ～ 4096）を設定するには、最初に VTP モードをトランスペアレントに設定する必要があります。トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースには追加されませんが、スイッチの実行コンフィギュレーションに保存されます。VTP バージョン 3 では、クライアントまたはサーバ モードで拡張範囲 VLAN を作成できます。これらの VLAN は VLAN データベースに格納されます。

switchport インターフェイス コンフィギュレーション コマンドを使用すると、VLAN にポートが追加されます。

- インターフェイスを特定します。
- トランク ポートには、トランク特性を設定し、必要に応じて、所属できる VLAN を定義します。
- アクセス ポートには、所属する VLAN を設定して定義します。

スイッチ ポート

スイッチ ポートは、物理ポートに対応付けられたレイヤ 2 専用インターフェイスです。ポートは、アクセス ポートまたはトランク ポートに設定できます。また、ポート単位で Dynamic Trunking Protocol（DTP）を稼働させ、リンクのもう一端のポートとネゴシエートすることで、スイッチ ポート モードも設定できます。スイッチ ポートは、物理インターフェイスおよび対応するレイヤ 2 プロトコルの管理に使用されます。

スイッチ ポートの設定には、**switchport** インターフェイス コンフィギュレーション コマンドを使用します。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにするには、**switchport** コマンドと no キーワードを使用します。

（注） レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

アクセス ポート特性およびトランク ポート特性の設定についての詳細については、第 17 章「VLAN の設定」を参照してください。

（注）　LAN Base イメージでは、スタティック ルーティングがサポートされます。

アクセス ポート

アクセス ポートは（音声 VLAN ポートとして設定されている場合を除き）1 つの VLAN だけに所属し、その VLAN のトラフィックだけを伝送します。トラフィックは、VLAN タグが付いていないネイティブ形式で送受信されます。アクセス ポートに着信したトラフィックは、ポートに割り当てられている VLAN に所属すると見なされます。

2 種類のアクセス ポートがサポートされています。

- スタティック アクセス ポートは、手動で VLAN に割り当てます。
- ダイナミック アクセス ポートの VLAN メンバーシップは、着信パケットを通じて学習されます。デフォルトでは、ダイナミック アクセス ポートはどの VLAN のメンバーでもなく、ポートとの伝送はポートの VLAN メンバーシップが検出されたときにだけイネーブルになります。スイッチ上のダイナミック アクセス ポートは、VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）によって VLAN に割り当てられます。Catalyst 6500 シリーズ スイッチを VMPS にできます。このスイッチを VMPS サーバにすることはできません。

また、Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。音声 VLAN ポートの詳細については、第 19 章「音声 VLAN の設定」を参照してください。

トランク ポート

トランク ポートは複数の VLAN のトラフィックを伝送し、デフォルトで VLAN データベース内のすべての VLAN のメンバとなります。

スイッチは IEEE 802.1Q トランク ポートだけをサポートします。IEEE 802.1Q トランク ポートは、タグ付きとタグなしの両方のトラフィックを同時にサポートします。IEEE 802.1Q トランク ポートは、デフォルトの Port VLAN ID（PVID; ポート VLAN ID）に割り当てられ、すべてのタグなしトラフィックはポートのデフォルト PVID 上を流れます。NULL VLAN ID を備えたすべてのタグなしおよびタグ付きトラフィックは、ポートのデフォルト PVID に所属するものと見なされます。発信ポートのデフォルト PVID と等しい VLAN ID を持つパケットは、タグなしで送信されます。残りのトラフィックはすべて、VLAN タグ付きで送信されます。

デフォルトでは、トランク ポートは、VTP に認識されているすべての VLAN のメンバですが、トランク ポートごとに VLAN の許可リストを設定して、VLAN メンバーシップを制限できます。許可 VLAN のリストは、その他のポートには影響を与えませんが、対応トランク ポートには影響を与えます。デフォルトでは、使用可能なすべての VLAN（VLAN ID 1 ～ 4096）が許可リストに含まれます。トランク ポートは、VTP が VLAN を認識し、VLAN がイネーブル状態にある場合に限り、VLAN のメンバーになることができます。VTP が新しいイネーブル VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバになり、トラフィックはその VLAN のトランク ポート間で転送されます。VTP が、VLAN のトランク ポートの許可リストに登録されていない、新しいイネーブル VLAN を認識した場合、ポートはその VLAN のメンバーにはならず、その VLAN のトラフィックはそのポート間で転送されません。

トランク ポートの詳細については、第 17 章「VLAN の設定」を参照してください。

EtherChannel ポート グループ

（注）　LAN Base イメージでは、EtherChannel ポート グループがサポートされます。

EtherChannel ポート グループは、複数のスイッチ ポートを 1 つのスイッチ ポートとして扱います。このようなポート グループは、スイッチ間、またはスイッチおよびサーバ間で高帯域接続を行う単一論理ポートとして動作します。EtherChannel は、チャネルのリンク全体でトラフィックの負荷を分散させます。EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが残りのリンクに切り替えられます。複数のトランク ポートを 1 つの論理トランク ポートに、複数のアクセス ポートを 1 つの論理アクセス ポートに、複数のトンネル ポートを 1 つの論理トンネル ポートに、または複数のルーテッド ポートを 1 つの論理ルーテッド ポートにグループ化できます。

ほとんどのプロトコルは単一のまたは集約スイッチ ポートで動作し、ポート グループ内の物理ポートを認識しません。例外は、DTP、Cisco Discovery Protocol（CDP）、およびポート集約プロトコル（PAgP）で、物理ポート上でしか動作しません。

EtherChannel を設定するとき、ポートチャネル論理インターフェイスを作成し、EtherChannel にインターフェイスを割り当てます。**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ダイナミックにポート チャネル論理インターフェイスを作成します。このコマンドは物理および論理ポートをバインドします。

レイヤ 3 インターフェイスの場合は、**interface port-channel** グローバル コンフィギュレーション コマンドを使用して手動で論理インターフェイスを作成します。そのあと、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

詳細については、第 40 章「EtherChannel の設定」を参照してください。

デュアルパーパス アップリンク ポート

一部の 2960 スイッチでは、デュアルパーパス アップリンク ポートがサポートされています。各アップリンク ポートはデュアル フロント エンド（RJ-45 コネクタおよび Small Form-factor Pluggable モジュール コネクタ）を持つ 1 つのインターフェイスと見なされます。デュアル フロント エンドは冗長インターフェイスではありません。スイッチはペアのうちの 1 つのコネクタのみをアクティブにします。

デフォルトでは、スイッチは最初にリンクするインターフェイス タイプを動的に選択します。ただし、**media-type** インターフェイス コンフィギュレーション コマンドを使用して、手動で RJ-45 コネクタまたは SFP モジュール コネクタを選択できます。デフォルトの設定に戻すには、**media-type auto interface** または **no media-type** インターフェイス コンフィギュレーション コマンドを使用します。

各アップリンク ポートには、2 つの LED が付いています。1 つは RJ-45 ポートのステータスを示すもので、もう 1 つは SFP モジュール ポートのステータスを示すものです。ポート LED は、いずれかのコネクタがアクティブのときに点灯します。LED の詳細については、*ハードウェア インストレーション ガイド*を参照してください。

スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます（デフォルト）。**auto-select** を設定した場合、**speed** および **duplex** インターフェイス コンフィギュレーション コマンドによる設定は行えません。

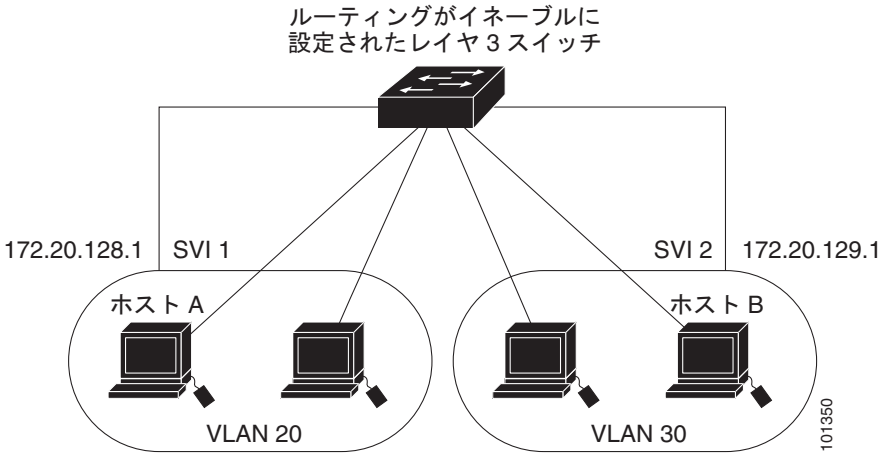
スイッチの電源を ON にした場合、または **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドでデュアルパーパス アップリンク ポートをイネーブル化した場合、SFP モジュール インターフェイスが選択されます。これ以外の場合、最初にアップの状態になったリンクのタイプに基づいて、アクティブなリンクが選択されます。

インターフェイスの接続

単一 VLAN 内のデバイスは、スイッチを通じて直接通信できます。異なる VLAN に属すポート間では、ルーティングデバイスを介さなければデータを交換できません。

標準のレイヤ 2 スイッチを使用すると、異なる VLAN のポートは、ルータを通じて情報を交換する必要があります。ルーティングがイネーブルに設定されたスイッチを使用することにより、IP アドレスを割り当てた SVI で VLAN 20 および VLAN 30 の両方を設定すると、外部ルータを使用せずに、スイッチを介してパケットをホスト A からホスト B に直接送信できます（図 15-1 を参照）。

図 15-1　　レイヤ 3 スイッチによる VLAN の接続



LAN Base イメージでは、基本的なルーティング（スタティック ルーティングと RIP）がサポートされます。高いパフォーマンスを維持するため、可能な場合は常にスイッチ ハードウェアによって転送を行います。ただし、ハードウェア内をルーティングできるのは、イーサネット II カプセル化機能を備えた IP バージョン 4 パケットだけです。*非 IP トラフィックと、他のカプセル化方式を使用しているトラフィックは、ハードウェアによってフォールバック ブリッジングできます。*

ルーティング機能は、すべての SVI およびルーテッド ポートでイネーブルにできます。スイッチは、IP トラフィックだけをルーティングします。IP ルーティング プロトコル パラメータとアドレス設定が SVI またはルーテッド ポートに追加されると、このポートで受信した IP トラフィックはルーティングされます。詳細については、第 41 章「スタティック IP ユニキャスト ルーティングの設定」を参照してください。

- *フォールバック ブリッジングを行うと、スイッチでルーティングされないトラフィックや、DECnet などのルーティングできないプロトコルに属するトラフィックが転送されます。また、フォールバック ブリッジングは、2 つ以上の SVI またはルーテッド ポート間のブリッジングによって、複数の VLAN を 1 つのブリッジ ドメインに接続します。フォールバック ブリッジングを設定する場合は、ブリッジ グループに SVI またはルーテッド ポートを割り当てます。各 SVI またはルーテッド ポートにはそれぞれ 1 つしかブリッジ グループが割り当てられません。同じグループ内のすべてのインターフェイスは、同じブリッジ ドメインに属します。*

インターフェイス コンフィギュレーション モードの使用方法

スイッチは、次のインターフェイス タイプをサポートします。

- 物理ポート：スイッチ ポートおよびルーテッド ポート
- VLAN：スイッチ仮想インターフェイス

- ポート チャネル：EtherChannel インターフェイス

インターフェイス範囲も設定できます（「インターフェイス範囲の設定」（P.15-12）を参照）。

物理インターフェイス（ポート）を設定するには、インターフェイス タイプ、およびスイッチ ポート番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

- タイプ：スイッチでのサポートに応じたポート タイプ。 予想されるタイプには、10/100 Mb/s イーサネット対応のファスト イーサネット（fastethernet または fa）、10/100/1000 Mb/s イーサネット ポート対応のギガビット イーサネット（gigabitethernet または gi）、または Small Form-Factor Pluggable（SFP）モジュール ギガビット イーサネット インターフェイスがあります。
- ポート番号：スイッチ上の物理インターフェイスの番号。ファスト イーサネット ポートでの IE-2000-4TC スイッチ モデルのポート数は 1 ～ 4 であり、ギガビット イーサネット ポートの場合は 1 ～ 2 です。ファスト イーサネット ポートでの IE-2000-8TC スイッチ モデルのポート数は 1 ～ 8 であり、ギガビット イーサネット ポートの場合は 1 ～ 2 です。表 15-1 に、スイッチとモジュールの組み合わせおよびインターフェイス番号を示します。

表 15-1　スイッチ インターフェイス番号

スイッチ モデル	インターフェイスの番号付け方式
IE-2000-4TS-L スイッチ	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2
IE-2000-4TS-B スイッチ	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2
IE-2000-4T-L スイッチ	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2
IE-2000-4T-B スイッチ	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2
IE-2000-4TS-G--L スイッチ	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2
IE-2000-4TS-G-B スイッチ	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2
IE-2000-8TC-L スイッチ	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ファスト イーサネット 1/5、ファスト イーサネット 1/6、ファスト イーサネット 1/7、ファスト イーサネット 1/8、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2

表 15-1　スイッチ インターフェイス番号 （続き）

IE-2000-8TC-B スイッチ	ファスト イーサネット 1/1、ファスト イーサネット 1/2、ファスト イーサネット 1/3、ファスト イーサネット 1/4、ファスト イーサネット 1/5、ファスト イーサネット 1/6、ファスト イーサネット 1/7、ファスト イーサネット 1/8、ギガビット イーサネット 1/1、およびギガビット イーサネット 1/2
	ファスト イーサネット 2/1、ファスト イーサネット 2/2、ファスト イーサネット 2/3、ファスト イーサネット 2/4、ファスト イーサネット 2/5、ファスト イーサネット 2/6、ファスト イーサネット 2/7、およびファスト イーサネット 2/8
	ファスト イーサネット 3/1、ファスト イーサネット 3/2、ファスト イーサネット 3/3、ファスト イーサネット 3/4、ファスト イーサネット 3/5、ファスト イーサネット 3/6、ファスト イーサネット 3/7、およびファスト イーサネット 3/8

スイッチを確認することで物理インターフェイスを識別できます。**show** 特権 EXEC コマンドを使用して、スイッチ上の特定のインターフェイスまたはすべてのインターフェイスに関する情報を表示することもできます。

イーサネット インターフェイスのデフォルト設定

表に示されている VLAN パラメータの詳細については、第 17 章「VLAN の設定」を参照してください。また、ポートへのトラフィック制御の詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。

（注）　インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

表 15-2　レイヤ 2 イーサネット インターフェイスのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ 2 またはスイッチング モード（**switchport** コマンド）
VLAN 許容範囲	VLAN 1 ～ 4096
デフォルト VLAN（アクセス ポート用）	VLAN 1（レイヤ 2 インターフェイスだけ）
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1（レイヤ 2 インターフェイスだけ）
VLAN トランキング	switchport mode dynamic auto（DTP をサポート）（レイヤ 2 インターフェイスだけ）

表 15-2　レイヤ 2 イーサネット インターフェイスのデフォルト設定 （続き）

機能	デフォルト設定
ポート イネーブル ステート	すべてのポートがイネーブル
ポートの説明	未定義
速度	自動ネゴシエーション
デュプレックス モード	自動ネゴシエーション
フロー制御	フロー制御は **receive**: **off** に設定されます。送信パケットでは常にオフです。
EtherChannel（PAgP）	すべてのイーサネット ポートでディセーブル。第 40 章「EtherChannel の設定」を参照してください。
ポート ブロッキング（不明マルチキャストおよび不明ユニキャスト トラフィック）	ディセーブル（ブロッキングされない）（レイヤ 2 インターフェイス限定）。
ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御	ディセーブル
保護ポート	ディセーブル（レイヤ 2 インターフェイス限定）。
ポート セキュリティ	ディセーブル（レイヤ 2 インターフェイス限定）。
PortFast	ディセーブル
Auto-MDIX	イネーブル。 **（注）** 受電デバイスがクロス ケーブルでスイッチに接続されている場合、スイッチは、IEEE 802.3af に完全には準拠していない、Cisco IP Phone やアクセス ポイントなどの準規格の受電をサポートしていない場合があります。これは、スイッチ ポート上で Automatic Medium-Dependent Interface Crossover（Auto-MIDX）がイネーブルかどうかは関係ありません。
キープアライブ メッセージ	SFP モジュールでディセーブル。他のすべてのポートでイネーブル。

インターフェイス速度およびデュプレックス モード

サポートされるポート タイプに応じて、スイッチのイーサネット インターフェイスは、10、100、または 1000 Mb/s、または全二重または半二重モードで動作します。全二重モードの場合、2 つのステーションが同時にトラフィックを送受信できます。通常、10 Mbps ポートは半二重モードで動作します。これは、各ステーションがトラフィックを受信するか、送信するかのどちらか一方しかできないことを意味します。

スイッチ モデルには、ファスト イーサネット（10/100 Mb/s）ポート、ギガビット イーサネット（10/100/1000 Mb/s）ポート、および Small Form-Factor Pluggable（SFP）モジュールをサポートする SFP モジュール スロットの組み合わせが含まれます。

速度とデュプレックス モードの設定時の注意事項

インターフェイス速度およびデュプレックス モードを設定するときには、次の注意事項に留意してください。

- ファスト イーサネット（10/100 Mbps）ポートは、すべての速度およびデュプレックス オプションをサポートします。
- ギガビット イーサネット（10/100/1000 Mbps）ポートは、すべての速度オプションとデュプレックス オプション（自動、半二重、全二重）をサポートします。ただし、1000 Mbps で稼働させているギガビット イーサネット ポートは、半二重モードをサポートしません。
- SFP モジュール ポートの場合、次の SFP モジュール タイプによって速度とデュプレックスの CLI（コマンドライン インターフェイス）オプションが変わります。
  - 1000 BASE-*x*（*x* には、BX、CWDM、LX、SX、ZX が適宜入ります）SFP モジュール ポートは、**speed** インターフェイス コンフィギュレーション コマンドで **nonegotiate** キーワードをサポートします。デュプレックス オプションはサポートされません。
  - 1000BASE-T SFP モジュール ポートは、10/100/1000 Mbps ポートと同一の速度とデュプレックス オプションをサポートします。
  - 100BASE-*x*（*x* には、BX、CWDM、LX、SX、ZX が適宜入ります）SFP モジュール ポートは、100 Mbps のみサポートします。これらのモジュールは、全二重および半二重オプションをサポートしますが、自動ネゴシエーションをサポートしません。

  スイッチでサポートされる SFP モジュールについては、各製品のリリース ノートを参照してください。
- 回線の両側で自動ネゴシエーションがサポートされる場合は、できるだけデフォルトの **auto** ネゴシエーションを使用してください。
- 一方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしない場合は、両方のインターフェイス上でデュプレックスと速度を設定します。サポートする側で **auto** 設定を使用しないでください。
- STP がイネーブルの場合にポートを再設定すると、スイッチがループの有無を調べるために最大で 30 秒かかる可能性があります。STP の再設定が行われている間、ポート LED はオレンジに点灯します。

注意　インターフェイス速度およびデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

IEEE 802.3x フロー制御

フロー制御により、接続しているイーサネット ポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。あるポートで輻輳が生じ、それ以上はトラフィックを受信できなくなった場合、ポーズ フレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。

（注）　スイッチのポートは、ポーズ フレームを受信できますが、送信はできません。

flowcontrol インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスのポーズ フレームを受信（**receive**）する能力を **on**、**off**、または **desired** に設定します。デフォルトの状態は **off** です。

desired に設定した場合、インターフェイスはフロー制御パケットの送信を必要とする接続デバイス、または必要ではないがフロー制御パケットを送信できる接続デバイスに対して動作できます。

デバイスのフロー制御設定には、次のルールが適用されます。

- **receive on**（または **desired**）：ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要のある、または送信できる接続デバイスと組み合わせて使用できます。ポーズ フレームの受信は可能です。
- **receive off**：フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

インターフェイスでの Auto-MDIX

インターフェイス上の Auto-MDIX がイネーブルに設定されている場合、インターフェイスが必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定します。Auto-MDIX 機能を使用せずにスイッチを接続する場合、サーバ、ワークステーション、またはルータなどのデバイスの接続にはストレート ケーブルを使用し、他のスイッチやリピータの接続にはクロス ケーブルを使用する必要があります。Auto-MDIX がイネーブルの場合、他のデバイスとの接続にはどちらのケーブルでも使用でき、ケーブルが正しくない場合はインターフェイスが自動的に修正を行います。ケーブル接続の詳細については、*ハードウェア インストレーション ガイド*を参照してください。

Auto-MDIX はデフォルトでイネーブルです。Auto-MDIX をイネーブルに設定する場合、Auto-MDIX 機能が正しく動作するようにインターフェイスの速度およびデュプレックスを **auto** に設定する必要があります。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mb/s インターフェイスでサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

SVI 自動ステート除外

SVI のアクセスまたはトランク ポートに SVI 自動ステート除外を設定すると、同じ VLAN に属していた場合でも、SVI ステータスの計算（アップまたはダウン ライン ステート）からポートを除外できます。除外されたポートがアップ状態でも、VLAN 内の他のポートがすべてダウン状態であれば、SVI ステートはダウンに変更されます。

SVI ライン ステート アップを保持するには、VLAN で少なくとも 1 つのポートがアップで除外されていない必要があります。このコマンドを使用して、SVI のステータスを決定する際にモニタリング ポートのステータスを除外できます。

システム MTU

すべてのインターフェイスで送受信されるフレームのデフォルト最大伝送単位（MTU）サイズは、1500 バイトです。10 または 100 Mbps で動作するすべてのインターフェイスで MTU サイズを増やすには、**system mtu** グローバル コンフィギュレーション コマンドを使用します。また、**system mtu jumbo** グローバル コンフィギュレーション コマンドを使用すると、すべてのギガビット イーサネット インターフェイス上でジャンボ フレームをサポートするように MTU サイズを増やすことができます。

system mtu routing グローバル コンフィギュレーション コマンドを使用すると、ルーテッド ポートの MTU サイズを変更できます。

（注）　システム MTU サイズを超えるルーティング MTU サイズは設定できません。システム MTU サイズを現在設定されているルーティング MTU サイズより小さい値に変更すると、設定変更は受け入れられますが、次にスイッチをリセットするまで適用されません。設定変更が有効になると、ルーティング MTU サイズは自動的にデフォルトの新しいシステム MTU サイズになります。

system mtu コマンドはギガビット イーサネット ポートには影響せず、**system mtu jumbo** コマンドは 10/100 ポートには影響しません。**system mtu jumbo** コマンドを設定していない場合、**system mtu** コマンドの設定はすべてのギガビット イーサネット インターフェイスに適用されます。

個々のインターフェイスに MTU サイズを設定することはできません。すべての 10/100 インターフェイスまたはすべてのギガビット イーサネット インターフェイスに対して設定されます。システムまたはジャンボ MTU サイズを変更する場合、新規設定を有効にするにはスイッチをリセットする必要があります。**system mtu routing** コマンドは、スイッチをリセットしなくても有効になります。

スイッチの CPU が受信できるフレーム サイズは、**system mtu** または **system mtu jumbo** コマンドで入力した値に関係なく、1998 バイトに制限されています。通常、転送またはルーティングされたフレームは CPU によって受信されませんが、場合によっては、制御トラフィック、SNMP、Telnet、またはルーティング プロトコルへ送信されたトラフィックなどのパケットが CPU へ送信されることがあります。

ルーテッド パケットは、出力ポートで MTU チェックの対象となります。ルーテッド ポートで使用される MTU 値は（**system mtu jumbo** 値ではなく）適用された **system mtu** 値から抽出されます。つまり、ルーテッド MTU はどの VLAN のシステム MTU よりも大きくなりません。ルーティング プロトコルは、隣接関係とリンクの MTU をネゴシエーションする場合にシステム MTU 値を使用します。たとえば、Open Shortest Path First（OSPF）プロトコルは、ピア ルータとの隣接関係を設定する前にこの MTU 値を使用します。特定の VLAN のルーテッド パケットの MTU 値を表示するには、**show platform port-asic mvid** 特権 EXEC コマンドを使用します。

（注）　レイヤ 2 ギガビット イーサネット インターフェイスが、10/100 インターフェイスより大きいサイズのフレームを受け取るように設定されている場合、レイヤ 2 ギガビット イーサネット インターフェイスに着信するジャンボ フレームとレイヤ 2 10/100 インターフェイスで発信されるジャンボ フレームはドロップされます。

インターフェイスの特性の設定方法

レイヤ 3 インターフェイスの設定

インターフェイスの設定

次の一般的な手順は、すべてのインターフェイス設定プロセスに当てはまります。

ステップ 1　特権 EXEC プロンプトに **configure terminal** コマンドを入力します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

ステップ 2　**interface** グローバル コンフィギュレーション コマンドを入力します。

ギガビット イーサネット ポート 1 でのインターフェイス タイプおよびインターフェイス番号の識別方法の例は、次のとおりです。

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

（注）　インターフェイス タイプとインターフェイス番号の間に入れるスペースはオプションです。

ステップ 3　各 **interface** コマンドの後ろに、インターフェイスに必要なインターフェイス コンフィギュレーション コマンドを続けて入力します。入力するコマンドによって、そのインターフェイスで稼働するプロトコルとアプリケーションが定義されます。別のインターフェイス コマンドまたは **end** を入力して特権 EXEC モードに戻ると、コマンドが収集されてインターフェイスに適用されます。

また、**interface range** または **interface range macro** グローバル コンフィギュレーション コマンドを使用すると、一定範囲のインターフェイスを設定することもできます。ある範囲内で設定したインターフェイスは、同じタイプである必要があります。また、同じ機能オプションを指定して設定しなければなりません。

ステップ 4　インターフェイスを設定してから、「インターフェイス特性のモニタリングとメンテナンス」（P.15-18）に示した **show** 特権 EXEC コマンドで、そのステータスを確認してください。

show interfaces 特権 EXEC コマンドを使用して、スイッチ上のまたはスイッチ用に設定されたすべてのインターフェイスのリストを表示します。デバイスがサポートする各インターフェイスまたは指定したインターフェイスのレポートが出力されます。

インターフェイス範囲の設定

interface range グローバル コンフィギュレーション コマンドを使用して、同じコンフィギュレーション パラメータを持つ複数のインターフェイスを設定できます。インターフェイス レンジ コンフィギュレーション モードを開始すると、このモードを終了するまで、入力されたすべてのコマンド パラメータはその範囲内のすべてのインターフェイスに対するものと見なされます。

インターフェイス範囲の制限

- ポート チャネルを指定して **interface range** コマンドを使用する場合は、先頭および最後のチャネル番号をアクティブなポート チャネルにする必要があります。
- **interface range** コマンドが機能するのは、**interface vlan** コマンドで設定された VLAN インターフェイスに限られます。**show running-config** 特権 EXEC コマンドを使用すると、設定されている VLAN インターフェイスが表示されます。**show running-config** コマンドで表示されない VLAN インターフェイスに **interface range** コマンドを使用することはできません。
- ある範囲内のすべてのインターフェイスは、同じタイプ（すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN）でなければなりません。ただし、1 つのマクロ内で複数のインターフェイス タイプを組み合わせることができます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** {*port-range* | **macro** *macro_name*}	設定するインターフェイス範囲（VLAN または物理ポート）を指定し、インターフェイス コンフィギュレーション モードを開始します。 • **interface range**：最大 5 つのポート範囲または定義済みマクロを 1 つ設定できます。 • **macro** *macro_name*：最大 32 文字の文字列を指定します。 • カンマで区切った *port-range* では、各エントリに対応するインターフェイス タイプを入力し、カンマの前後にスペースを含めます。 • ハイフンで区切った *port-range* では、インターフェイス タイプの再入力は不要ですが、ハイフンの前後にスペースを入力する必要があります。
ステップ 3		この時点で、通常のコンフィギュレーション コマンドを使用して、範囲内のすべてのインターフェイスにコンフィギュレーション パラメータを適用します。各コマンドは、入力されたとおりに実行されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** [*interface-id*]	指定した範囲内のインターフェイスの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイス レンジ マクロの設定および使用方法

はじめる前に

インターフェイス レンジ マクロを作成すると、設定するインターフェイスの範囲を自動的に選択できます。**interface range macro** グローバル コンフィギュレーション コマンドで **macro** キーワードを使用するには、まず **define interface-range** グローバル コンフィギュレーション コマンドでマクロを定義する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**define interface-range** *macro_name interface-range*	インターフェイス範囲マクロを定義して、NVRAM に保存します。 • **macro** *macro_name*：最大 32 文字の文字列を指定します。 • マクロには、カンマで区切ったインターフェイスを 5 つまで指定できます。 • *interface-range*：同じポート タイプで構成されます。
ステップ 3	**interface range macro** *macro_name*	*macro_name* の名前でインターフェイス範囲マクロに保存された値を使用することによって、設定するインターフェイスの範囲を選択します。 ここで、通常のコンフィギュレーション コマンドを使用して、定義したマクロ内のすべてのインターフェイスに設定を適用できます。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config | include define**	定義済みのインターフェイス範囲マクロの設定を表示します。

イーサネット インターフェイスの設定

デュアルパーパス アップリンク ポートのタイプの設定

速度およびデュプレックスを設定できるようにアクティブにするするデュアルパーパス アップリンクを選択するには、この作業を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するデュアルパーパス アップリンク ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**media-type** {**auto-select** | **rj45** | **sfp**}	インターフェイスとデュアルパーパス アップリンク ポートのタイプを選択します。キーワードの意味は次のとおりです。 • **auto-select**：スイッチが動的にタイプを選択します。リンクがアップの状態になると、アクティブなリンクがダウンの状態になるまで、スイッチによりその他のタイプがディセーブル化されます。アクティブなリンクがダウンの状態になると、いずれかのリンクがアップの状態になるまで、スイッチにより両方のタイプがイネーブル化されます。auto-select モードでは、スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます（デフォルト）。インストールされている SFP モジュールのタイプによって、スイッチで自動的に選択が行えない場合もあります。 • **rj45**：スイッチが SFP モジュール インターフェイスをディセーブル化します。このポートに SFP モジュールを接続する場合、RJ-45 側がダウンしている、または接続していない場合でも、リンクを確立することはできません。このモードでは、デュアルパーパス ポートは 10/100/1000BASE-TX インターフェイスと同様の動作をします。このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。 • **sfp**：スイッチが RJ-45 インターフェイスをディセーブル化します。この RJ-45 ポートにケーブルを接続している場合、SFP モジュール側がダウンしている、または SFP モジュールが接続していない場合でも、リンクを確立することはできません。インストールされている SFP モジュールのタイプに基づいて、このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **transceiver properties**	設定を確認します。

インターフェイス速度およびデュプレックス パラメータの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**speed** {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}	インターフェイスに対する適切な速度パラメータを入力します。 • **10**、**100**、または **1000**：インターフェイスの速度を設定します。**1000** キーワードを使用できるのは、10/100/1000 Mbps ポートに対してだけです。 • **auto**：インターフェイスが接続されたデバイスと速度の自動ネゴシエーションを行うようにします。**auto** キーワードと一緒に **10**、**100**、または **1000** キーワードを使用した場合、ポートは指定の速度でのみ自動ネゴシエートします。 • **nonegotiate**：SFP モジュール ポートに対してのみ使用できます。SFP モジュール ポートは 1000 Mbps だけで動作しますが、自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、ネゴシエートしないように設定できます。
ステップ 4	**duplex** {**auto** | **full** | **half**}	インターフェイスのデュプレックス パラメータを入力します。 半二重モードをイネーブルにします（10 または 100 Mbps のみで動作するインターフェイスの場合）。1000 Mbps で動作するインターフェイスには半二重モードを設定できません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id*	インターフェイス速度およびデュプレックス モードの設定を表示します。

IEEE 802.3x フロー制御の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**flowcontrol** {**receive**} {**on** | **off** | **desired**}	ポートのフロー制御モードを設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id*	インターフェイス フロー制御の設定を確認します。

インターフェイスでの Auto-MDIX の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**speed auto**	接続されたデバイスと速度の自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 4	**duplex auto**	接続されたデバイスとデュプレックス モードの自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 5	**mdix auto**	インターフェイスの Auto-MDIX をイネーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show controllers ethernet-controller** *interface-id* **phy**	インターフェイスの Auto-MDIX 動作ステートを確認します。

インターフェイスに関する記述の追加

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	記述を追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**description** *string*	インターフェイスに関する説明を追加します（最大 240 文字）。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **description** または **show running-config**	入力を確認します。

SVI 自動ステート除外の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レイヤ 2 インターフェイス（物理ポートまたはポート チャネル）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport autostate exclude**	SVI ライン ステート（アップまたはダウン）のステータスを定義する際、アクセスまたはトランク ポートを除外します。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running config interface** *interface-id*	（任意）実行コンフィギュレーションを表示します。
	show interface *interface-id* **switchport**	設定を確認します。

システム MTU の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**system mtu** *bytes*	（任意）10 または 100 Mb/s で動作するスイッチのすべてのインターフェイスに対して MTU サイズを変更します。 指定できる範囲は、1500 ～ 1998 バイトです。デフォルトは 1500 バイトです。
ステップ 3	**system mtu jumbo** *bytes*	（任意）スイッチのすべてのギガビット イーサネット インターフェイスに対して MTU サイズを変更します。 指定できる範囲は 1500 ～ 9000 バイトです。デフォルトは 1500 バイトです。
ステップ 4	**system mtu routing** *bytes*	（任意）ルーテッド ポートのシステム MTU を変更します。指定できる範囲は 1500 ～システム MTU 値で、すべてのポートにルーティング可能な最大 MTU 値です。 これより大きなパケットは受け入れられますが、ルーティングされません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	コンフィギュレーション ファイルに設定を保存します。
ステップ 7	**reload**	オペレーティング システムをリロードします。
ステップ 8	**show system mtu**	（任意）設定を確認します。

インターフェイス特性のモニタリングとメンテナンス

インターフェイス ステータスのモニタ

表 15-3　インターフェイス用の show コマンド

コマンド	目的
show interfaces [*interface-id*]	（任意）すべてのインターフェイスまたは特定のインターフェイスのステータスおよび設定を表示します。 **（注）** ディセーブルになっているインターフェイスは、出力に *administratively down* と表示されます。
show interfaces *interface-id* **status** [**err-disabled**]	（任意）インターフェイスのステータス、または errdisable ステートにあるインターフェイスの一覧を表示します。
show interfaces [*interface-id*] **switchport**	（任意）スイッチング ポートの管理上および動作上のステータスを表示します。このコマンドを使用すると、ポートがルーティングまたはスイッチングのどちらのモードにあるかが判別できます。
show interfaces [*interface-id*] **description**	（任意）1 つのインターフェイスまたはすべてのインターフェイスに関する記述とインターフェイスのステータスを表示します。
show ip interface [*interface-id*]	（任意）IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。
show interface [*interface-id*] **stats**	（任意）インターフェイスのスイッチング パスによる入出力パケットを表示します。
show interfaces transceiver properties	（任意）インターフェイスの速度およびデュプレックス設定を表示します。
show interfaces transceiver detail	（任意）インターフェイスの温度、電圧、電流量を表示します。
show interfaces [*interface-id*] [{**transceiver properties** | **detail**}] *module number*]	SFP モジュールに関する物理および動作ステータスを表示します。
show running-config interface [*interface-id*]	インターフェイスに対応する RAM 上の実行コンフィギュレーションを表示します。
show version	ハードウェア設定、ソフトウェア バージョン、コンフィギュレーション ファイルの名前と送信元、およびブート イメージを表示します。
show controllers ethernet-controller *interface-id* **phy**	インターフェイスの Auto-MDIX 動作ステートを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 15-4　インターフェイス用の clear コマンド

コマンド	目的
clear counters [*interface-id*]	インターフェイス カウンタをクリアします。 （注）　このコマンドは、簡易ネットワーク管理プロトコル（SNMP）を使用して取得されたカウンタをクリアしません。**show interface** 特権 EXEC コマンドで表示されるカウンタのみをクリアします。
clear interface *interface-id*	インターフェイスのハードウェア ロジックをリセットします。
clear line [*number* | **console 0** | **vty** *number*]	非同期シリアル回線に関するハードウェア ロジックをリセットします。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定されたインターフェイスのすべての機能がディセーブルになり、使用不可能であることがすべてのモニタ コマンドの出力に表示されます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。ルーティング アップデートには、インターフェイス情報は含まれません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** {**vlan** *vlan-id*} | {{**fastethernet** | **gigabitethernet**} *interface-id*} | {**port-channel** *port-channel-number*}	設定するインターフェイスを選択します。
ステップ 3	**shutdown**	インターフェイスをシャットダウンします。 （注）　インターフェイスを再起動するには、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力を確認します。

インターフェイス特性の設定例

インターフェイス範囲の設定：例

次の例では、**interface range** グローバル コンフィギュレーション コマンドを使用して、ポート 1 ～ 2 の速度を 100 Mb/s に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 - 2
Switch(config-if-range)# speed 100
```

この例では、カンマを使用して別のインターフェイス タイプ ストリングを追加し、ファスト イーサネット ポート 1 ～ 3 と、ギガビット イーサネット ポート 1 および 2 の両方をイネーブルにし、フロー制御ポーズ フレームを受信できるようにします。

```
Switch# configure terminal
Switch(config)# interface range fastethernet1/1 - 3, gigabitethernet1/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

インターフェイス レンジ モードで複数のコンフィギュレーション コマンドを入力した場合、各コマンドは入力した時点で実行されます。インターフェイス レンジ モードを終了した後で、コマンドがバッチ処理されるわけではありません。コマンドの実行中にインターフェイス レンジ コンフィギュレーション モードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスに対して実行されない場合もあります。コマンド プロンプトが再表示されるのを待ってから、インターフェイス範囲コンフィギュレーション モードを終了してください。

インターフェイス範囲マクロの設定：例

次に、*enet_list* という名前のインターフェイス範囲マクロを定義して、ポート 1 および 2 を含め、マクロ設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet1/1 - 2
Switch(config)# end
Switch# show running-config | include define
Switch# define interface-range enet_list gigabitethernet1/1 - 2
```

次に、複数のタイプのインターフェイスを含むマクロ *macro1* を作成する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range macro1 fastethernet1/1 - 2, gigabitethernet1/1 - 2
Switch(config)# end
```

次に、インターフェイス レンジ マクロ *enet_list* に対するインターフェイス レンジ コンフィギュレーション モードを開始する例を示します。

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

次に、インターフェイス レンジ マクロ *enet_list* を削除し、処理を確認する例を示します。

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

速度およびデュプレックス パラメータの設定：例

次に、10/100Mbps ポートでインターフェイスの速度を 10 Mbps に、デュプレックス モードを半二重に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fasttethernet1/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

次に、10/100/1000 Mbps ポートで、インターフェイスの速度を 100 Mbps に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# speed 100
```

Auto-MDIX のイネーブル化：例

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

ポートの説明の追加：例

次に、ポートに記述を追加して、その説明を確認する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/2 description
Interface Status         Protocol Description
Gi1/2   admin down     down     Connects to Marketing
```

SVI 自動ステート除外の設定：例

次に、SVI のアクセスまたはトランク ポートを設定して、ステータス計算から除外する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport autostate exclude
Switch(config-if)# exit
```

その他の関連資料

ここでは、スイッチの管理に関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS インターフェイス コマンド	『*Cisco IOS Interface Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 16

SmartPort マクロの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SmartPort マクロの設定に関する情報

SmartPort マクロは、共通の設定を保存および共有するのに便利です。SmartPort マクロを使用すると、ネットワークでのスイッチの場所に基づいて機能および設定をイネーブルにしたり、ネットワークを通じて大規模な設定を配置したりできます。

各 SmartPort マクロは、定義する一連の CLI コマンドです。SmartPort マクロは、既存の CLI コマンドの集まりであり、新しい CLI コマンドは含まれていません。

SmartPort マクロをインターフェイスに適用すると、マクロ内の CLI コマンドがインターフェイスに設定されます。インターフェイスに SmartPort マクロを適用しても、インターフェイスの既存の設定は失われません。新しいコマンドがインターフェイスに追加され、実行コンフィギュレーション ファイルに保存されます。

SmartPort マクロの設定方法

SmartPort のデフォルト設定

スイッチで SmartPort マクロはイネーブルになっていません。

表 16-1　デフォルト SmartPort マクロ

マクロ名[1]	説明
cisco-ie-global	このグローバル コンフィギュレーション マクロを使用して、スイッチの設定を工業用イーサネットの環境に合わせてスイッチの設定を行います。このマクロは、Express Setup を使用してスイッチを初期設定するときに自動的に適用されます。 （注）　**cisco-ethernetip** マクロが適切に動作するために、まず **cisco-ie-global** マクロを適用する必要があります。
cisco-desktop	PC のようなデスクトップ デバイスをスイッチ ポートに接続する場合、ネットワーク セキュリティと信頼性を高めるために、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-phone	Cisco IP Phone を搭載した PC などのデスクトップ デバイスをスイッチ ポートに接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは、**cisco-ie-desktop** マクロの拡張で、同じセキュリティと復元力機能を備えていますが、遅延に影響されやすい音声トラフィックを正しく処理できるように専用の音声 VLAN が追加されています。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-switch	このインターフェイス コンフィギュレーション マクロは、アクセス スイッチとディストリビューション スイッチを接続している場合や、Small Form-Factor Pluggable（SFP）モジュールを使用して接続されているアクセス スイッチ間で接続している場合に使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-router	スイッチと WAN ルータを接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ethernetip	このインターフェイス コンフィギュレーション マクロは、スイッチを EtherNet IP 装置に接続しているときに使用します。 （注）　**cisco-ethernetip** マクロが適切に動作するために、まず **cisco-ie-global** マクロを適用する必要があります。
cisco-ie-qos-map-setup	このグローバル コンフィギュレーション マクロを使用して、QoS ポリシー マップを産業用イーサネットの環境に合わせてスイッチの設定を行います。
cisco-ie-qos-queue-setup	このグローバル コンフィギュレーション マクロを使用して、QoS ポリシー マップを産業用イーサネットの環境に合わせてスイッチの設定を行います。

1. シスコ デフォルト SmartPort マクロは、スイッチで実行されているソフトウェア バージョンによって異なります。

SmartPort 設定時の注意事項

- マクロがスイッチまたはスイッチ インターフェイスにグローバルに適用されている場合、インターフェイス上の既存のすべての設定が保持されます。これは、差分設定に適用する場合に役立ちます。
- 構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドを適用します。マクロを適用およびデバッグして、構文エラーまたは設定エラーを検出するには、**macro global trace** *macro-name* グローバル コンフィギュレーション コマンド、または **macro trace** *macro-name* インターフェイス コンフィギュレーション コマンドを使用できます。
- 特定のインターフェイス タイプ固有の CLI コマンドもあります。設定を受け入れないインターフェイスにマクロを適用すると、マクロが構文または設定のチェックに失敗し、スイッチはエラーメッセージを返します。

- インターフェイス範囲へのマクロの適用は、単一インターフェイスへのマクロの適用と同じです。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。1 つのインターフェイスでマクロ コマンドの実行に失敗しても、マクロは残りのインターフェイス上に適用されます。
- スイッチまたはスイッチ インターフェイスにマクロを適用すると、マクロ名が自動的にスイッチまたはインターフェイスに追加されます。**show running-config** ユーザ EXEC コマンドを使用して、適用されたコマンドおよびマクロ名を表示できます。

SmartPort マクロの適用

	コマンド	目的
ステップ 1	**show parser macro**	スイッチ ソフトウェアに埋め込まれているシスコ デフォルト SmartPort マクロを表示します。
ステップ 2	**show parser macro name** *macro-name*	適用する特定のマクロを表示します。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**macro global** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	マクロで定義された各コマンドをスイッチに適用するには、**macro global apply** *macro-name* を入力します。**macro global trace** *macro-name* を指定して、構文または設定エラーを判別するためにマクロを適用およびデバッグします。 **parameter** *value* キーワードを使用して、必要な値をマクロに追加します。**$** で始まるキーワードには、一意のパラメータ値が必要です。 **macro global apply** *macro-name* **?** コマンドを使用すると、マクロに必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。 （任意）そのスイッチに限定された一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。
ステップ 5	**interface** *interface-id*	（任意）インターフェイス コンフィギュレーション モードを開始して、マクロを適用するインターフェイスを指定します。
ステップ 6	**default interface** *interface-id*	（任意）指定したインターフェイスからすべての設定を消去します。
ステップ 7	**macro** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	マクロで定義された各コマンドをポートに適用するには、**macro global apply** *macro-name* を入力します。**macro global trace** *macro-name* を指定して、構文または設定エラーを判別するためにマクロを適用およびデバッグします。 **parameter** *value* キーワードを使用して、必要な値をマクロに追加します。**$** で始まるキーワードには、一意のパラメータ値が必要です。 **macro global apply** *macro-name* **?** コマンドを使用すると、マクロに必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。 （任意）そのスイッチに限定された一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**show running-config interface** *interface-id*	マクロがインターフェイスに適用されたことを確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SmartPort マクロのモニタリングおよびメンテナンス

表 16-2　SmartPort マクロを表示するコマンド

コマンド	目的
show parser macro	すべての SmartPort マクロを表示します。
show parser macro name *macro-name*	特定の SmartPort マクロを表示します。
show parser macro brief	SmartPort マクロの名前を表示します。
show parser macro description [**interface** *interface-id*]	すべてのインターフェイスまたは特定のインターフェイスに関する SmartPort マクロの説明を表示します。

SmartPort マクロの設定例

SmartPort マクロの適用：例

次に、**cisco-ie-desktop** マクロを表示する例、およびインターフェイス上でマクロを適用し、アクセス VLAN ID を 25 に設定する例を示します。

```
Switch# show parser macro name cisco-ie-desktop
-------------------------------------------------------------
Macro name : cisco-ie-desktop
Macro type : default interface
# macro keywords ACCESS_VLAN
#macro name cisco-ie-desktop
switchport mode access
switchport access vlan ACCESS_VLAN
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
spanning-tree bpduguard enable
no macro description
macro description cisco-ie-desktop
-------------------------------------------------------------
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet1/4
Switch(config-if)# macro apply cisco-ie-desktop $AVID 25
```

次に、cisco-ethernetip マクロを表示する例と、このマクロをインターフェイスに適用する例を示します。

```
Switch# show parser macro name cisco-ethernetip
Macro name : cisco-ie-global
```

```
Macro type : default interface
#macro name cisco-ethernetip
#macro keywords ACCESS_VLAN
#macro description cisco-ethernetip
switchport host
switchport access vlan ACCESS-VLAN
storm-control broadcast level 3.00 1.00
service-policy input CIP-Traffic
#service-policy input 1588

Switch# configure terminal
Switch(config)# interface fastethernet 1/1
Switch(config-if)# macro apply cisco-ethernetip ACCESS_VLAN 1
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 17

VLAN の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

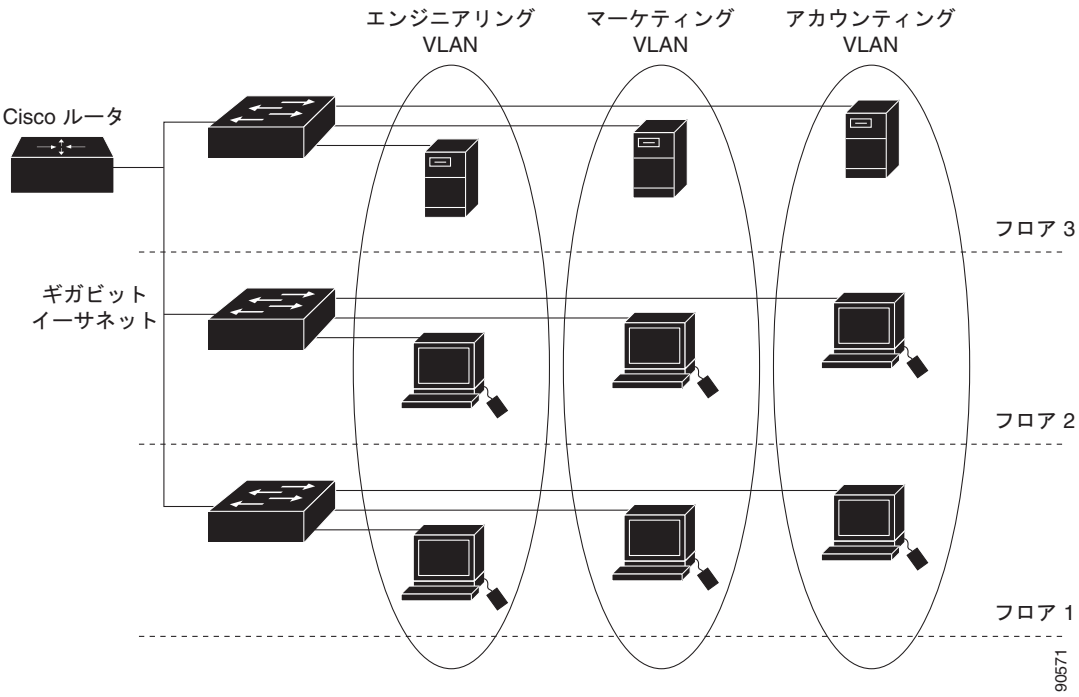
VLAN の設定に関する情報

VLAN

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのスイッチ ポートも VLAN に割り当てることができます。ユニキャスト、ブロードキャスト、およびマルチキャスト パケットは、VLAN 内のエンド ステーションだけに転送およびフラッディングが行われます。各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に割り当てられていないステーション宛てのパケットは、ルータまたはフォールバック ブリッジングをサポートするスイッチを経由して転送しなければなりません（図 17-1 を参照）。VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLAN ごとに独自のブリッジ管理情報ベース（MIB）情報があり、スパニングツリーの独自の実装をサポートできます。第 20 章「STP の設定」を参照してください。

（注） VLAN を作成する前に、VLAN トランキング プロトコル（VTP）を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。VTP の詳細については、第 18 章「VTP の設定」を参照してください。

図 17-1　論理的に定義されたネットワークとしての VLAN



VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるエンド ステーションはすべて同じ VLAN に属します。スイッチ上のインターフェイスの VLAN メンバーシップは、インターフェイスごとに手動で割り当てます。この方法でスイッチ インターフェイスを VLAN に割り当てた場合、これをインターフェイス ベース（またはスタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングまたはフォールバック ブリッジングする必要があります。スイッチは、スイッチ仮想インターフェイス（SVI）を使用して、VLAN 間でトラフィックをルーティングできます。VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。

（注）　スイッチに多数の VLAN を設定し、ルーティングをイネーブル化しない予定の場合は、**sdm prefer vlan** グローバル コンフィギュレーション コマンドを使用してスイッチ データベース管理（SDM）機能を VLAN テンプレートに設定できます。このテンプレートは、最大数のユニキャスト MAC アドレスをサポートするようにシステム リソースを設定します。SDM テンプレートの詳細については、第 11 章「SDM テンプレートの設定」、またはこのリリースのコマンド リファレンスの **sdm prefer** コマンドを参照してください。

サポートされる VLAN

スイッチは、VTP クライアント、サーバ、およびトランスペアレントの各モードで VLAN をサポートしています。VLAN は、1 ～ 4096 の番号で識別します。VLAN ID 1002 ～ 1005 は、トークンリングおよびファイバ分散データ インターフェイス（FDDI）VLAN 専用です。

VTP バージョン 1 およびバージョン 2 は、標準範囲の VLAN（VLAN ID 1 ～ 1005）だけをサポートします。これらのバージョンで 1006 ～ 4096 の VLAN ID を作成する場合は、スイッチを VTP トランスペアレント モードにする必要があります。

このリリースでは、VTP バージョン 3 をサポートします。VTP バージョン 3 は、VLAN 範囲全体（VLAN 1 ～ 4096）をサポートします。拡張範囲 VLAN（VLAN 1006 ～ 4096）は、VTP バージョン 3 でだけサポートされます。拡張 VLAN がドメインに設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

スイッチは合計 1005 の VLAN をサポートしますが、ルーテッド ポート、SVI、その他の設定済み機能の個数によって、スイッチのハードウェアの使用状況は左右されます。

スイッチは、最大 128 のスパニングツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus（PVST+）または Rapid PVST+ をサポートします。VLAN ごとに 1 つずつスパニングツリー インスタンスを使用できます。スパニングツリー インスタンス数および VLAN 数の詳細については、「標準範囲 VLAN 設定時の注意事項」（P.17-6）を参照してください。

VLAN ポート メンバーシップ モード

VLAN に所属するポートは、メンバーシップ モードを割り当てることで設定します。メンバーシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。表 17-1 に、各種メンバーシップ モード、およびそれぞれのメンバーシップと VTP の特性を示します。

表 17-1　ポートのメンバーシップ モードとその特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1 つの VLAN だけに所属します。 詳細については、「VLAN へのスタティック アクセス ポートの割り当て」（P.17-18）を参照してください。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードをトランスペアレント モードに設定します。VTP に加入するには、あるスイッチのトランク ポートに接続した別のスイッチ上に 1 つまたは複数のトランク ポートがなければなりません。
トランク（ISL または IEEE 802.1Q）	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバです。ただし、メンバーシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッディング トラフィックを阻止することもできます。 トランク ポートの設定については、「トランク ポートとしてのイーサネット インターフェイスの設定」（P.17-19）を参照してください。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランク リンクを通じて他のスイッチと VLAN コンフィギュレーション メッセージを交換します。

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
ダイナミック アクセス	ダイナミック アクセス ポートは VLAN に属すことができ、VMPS（VLAN メンバーシップ ポリシー サーバ）によって動的に割り当てられます。VMPS には Catalyst 5000 または Catalyst 6500 シリーズ スイッチを使用できますが、IE 2000 スイッチは使用できません。この IE 2000 スイッチは VMPS クライアントです。 同一スイッチ上でダイナミックアクセス ポートとトランク ポートを使用できますが、ダイナミックアクセス ポートは別のスイッチではなく、エンド ステーションまたはハブに接続する必要があります。 設定については、「VMPS クライアント上のダイナミック アクセス ポートの設定」（P.17-23）を参照してください。	VTP は必須です。 VMPS およびクライアントを同じ VTP ドメイン名で設定してください。 VTP に加入するには、あるスイッチのトランク ポートが別のスイッチのトランク ポートに接続していなければなりません。
音声 VLAN	音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データ トラフィックに別の VLAN を使用するように設定されたアクセス ポートです。 音声 VLAN ポートの詳細については、第 19 章「音声 VLAN の設定」を参照してください。	VTP は不要です。VTP は音声 VLAN に対して無効です。

アクセス モードとトランク モード、および機能の定義の詳細については、表 17-3（P.17-10）を参照してください。

ポートが VLAN に所属すると、スイッチは VLAN 単位で、ポートに対応するアドレスを学習して管理します。詳細については、「アドレス エージング タイムの変更」（P.7-13）を参照してください。

標準範囲 VLAN

標準範囲 VLAN は、VLAN ID が 1 ～ 1005 の VLAN です。スイッチが VTP サーバ モードまたは VTP トランスペアレント モードにある場合は、VLAN データベース内の VLAN 2 ～ 1001 について設定を追加、変更、または削除できます（VLAN ID 1 および 1002 ～ 1005 は自動作成され、削除できません）。

VLAN ID 1 ～ 1005 の設定は *vlan.dat*（VLAN データベース）ファイルに書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。*vlan.dat* ファイルはフラッシュ メモリに格納されます。

注意　*vlan.dat* ファイルを手動で削除しようとすると、VLAN データベースの不整合が生じる可能性があります。VLAN 設定を変更する場合は、ここに記載されたコマンド、およびこのリリースに対応するコマンド リファレンスに記載されたコマンドを使用します。VTP 設定の変更手順については、第 18 章「VTP の設定」を参照してください。

さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバーシップ モードの定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

VLAN データベースに新しい標準範囲 VLAN を作成したり、VLAN データベース内の既存の VLAN を変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ（イーサネット、FDDI、FDDI Network Entity Title（NET）、TrBRF または TrCRF、トークンリング、トークンリング Net）
- VLAN ステート（アクティブまたは中断）
- VLAN の最大伝送単位（MTU）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN のスパニングツリー プロトコル（STP）タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号

VLAN を **vlan** グローバル コンフィギュレーション コマンドで設定するには、VLAN ID を入力します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。デフォルトの VLAN 設定を使用するか（表 17-2 を参照）、複数のコマンドを入力して VLAN を設定できます。このモードで使用できるコマンドの詳細については、このリリースのコマンド リファレンスに記載されている **vlan** グローバル コンフィギュレーション コマンドを参照してください。設定を終了したら、VLAN コンフィギュレーション モードを終了して、設定を有効にする必要があります。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN ID 1 ～ 1005 の設定は、常に VLAN データベースに保存されます（vlan.dat ファイル）。VTP モードがトランスペアレント モードの場合、それらの設定もスイッチの実行コンフィギュレーション ファイルに保存されます。**copy running-config startup-config** 特権 EXEC コマンドを使用して、スタートアップ コンフィギュレーション ファイルに設定を保存できます。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 の VLAN のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバの場合、最初の 1005 の VLAN だけのドメイン名および VLAN 設定には VLAN データベース情報が使用されます。VTP バージョン 3 は、VLAN 1006 ～ 4096 もサポートします。

トークンリング VLAN

このスイッチはトークンリング接続をサポートしていませんが、トークンリング接続を行っている Catalyst 6500 シリーズ スイッチなどのリモート デバイスを、サポート対象スイッチのうちの 1 台から管理できます。VTP バージョン 2 が稼働しているスイッチは、次のトークンリング VLAN に関する情報をアドバタイズします。

- トークンリング TrBRF VLAN
- トークンリング TrCRF VLAN

トークンリング VLAN の詳しい設定手順については、『*Catalyst 6500 Series Software Configuration Guide*』を参照してください。

標準範囲 VLAN 設定時の注意事項

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- スイッチは、VTP クライアント、サーバ、およびトランスペアレントの各モードで 1005 の VLAN をサポートしています。
- 標準範囲 VLAN は、1 ～ 1001 の番号で識別します。VLAN 番号 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレント モードの場合、VTP と VLAN の設定もスイッチの実行コンフィギュレーション ファイルに保存されます。
- VTP バージョン 1 および 2 では、スイッチは VTP トランスペアレント モード（VTP はディセーブル）の場合だけ、VLAN ID 1006 ～ 4096 をサポートします。これらは拡張範囲 VLAN であり、設定オプションには制限があります。VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されません。VTP バージョン 3 は、拡張範囲 VLAN（VLAN 1006 ～ 4096）データベース伝播をサポートします。拡張 VLAN を設定している場合は、VTP バージョン 3 からバージョン 1 または 2 に変換できません。「拡張範囲 VLAN の作成」（P.17-18）を参照してください。
- VLAN を作成する前に、スイッチを VTP サーバ モードまたは VTP トランスペアレント モードにしておく必要があります。スイッチが VTP サーバである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを伝送しませんが、VTP を介して VLAN 設定を伝播します。
- スイッチは 128 のスパニングツリー インスタンスをサポートします。スイッチのアクティブな VLAN 数が、サポートされているスパニングツリー インスタンス数よりも多い場合、スパニングツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニングツリーはディセーブルになります。スイッチ上の使用可能なスパニングツリー インスタンスをすべて使い切ってしまった後に、VTP ドメインの中にさらに別の VLAN を追加すると、そのスイッチ上にスパニングツリーが稼働しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リスト（すべての VLAN を許可するリスト）が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパニングツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

スイッチ上の VLAN の数がサポートされているスパニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s Multiple STP（MSTP）を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 21 章「MSTP の設定」を参照してください。

イーサネット VLAN のデフォルト設定

（注）　スイッチがサポートするのは、イーサネット インターフェイスだけです。FDDI およびトークンリング VLAN は、ローカルではサポートされないので、FDDI およびトークンリング メディア固有の特性は、他のスイッチに対する VTP グローバル アドバタイズにのみ設定します。

表 17-2　イーサネット VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1	1 ～ 4096 （注）　拡張範囲 VLAN（VLAN ID 1006 ～ 4096）は、VTP バージョン 3 の場合だけ VLAN データベースに保存されます。
VLAN 名	*VLANxxxx*。*xxxx* は VLAN ID 番号に等しい 4 桁の数字（先行ゼロを含む）です。	範囲なし
IEEE 802.10 SAID	100001（100000 と VLAN ID の和）	1 ～ 4294967294
MTU サイズ	1500	1500 ～ 18190
トランスレーショナル ブリッジ 1	0	0 ～ 1005
トランスレーショナル ブリッジ 2	0	0 ～ 1005
VLAN ステート	アクティブ	アクティブ、中断
リモート SPAN	ディセーブル	イネーブル、ディセーブル

イーサネット VLAN

VLAN データベース内の各イーサネット VLAN には、1 ～ 1001 の 4 桁の一意の ID が設定されています。VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 用に予約されています。標準範囲 VLAN を作成して VLAN データベースに追加するには、VLAN に番号および名前を割り当てます。

（注）　VTP バージョン 1 および 2 でスイッチが VTP トランスペアレント モードの場合は、1006 を超える VLAN ID を割り当てることができますが、それらを VLAN データベースに追加できません。「拡張範囲 VLAN の作成」（P.17-18）を参照してください。

VLAN の追加時に指定されるデフォルト パラメータの一覧は、「標準範囲 VLAN」（P.17-4）を参照してください。

VLAN の削除

VTP サーバ モードのスイッチから VLAN を削除すると、VTP ドメイン内のすべてのスイッチの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレント モードのスイッチから VLAN を削除した場合、そのスイッチ上に限り VLAN が削除されます。

イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ～ 1005 の、メディア タイプ別のデフォルト VLAN は削除できません。

注意　VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブで）対応付けられたままです。

VLAN へのスタティック アクセス ポート

VTP をディセーブルにすることによって（VTP トランスペアレント モード）、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

クラスタ メンバ スイッチのポートを VLAN に割り当てる場合、最初に **rcommand** 特権 EXEC コマンドを使用して、そのクラスタ メンバ スイッチにログインします。

（注）　存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます（「イーサネット VLAN の作成または変更」（P.17-17）を参照）。

拡張範囲 VLAN

VTP バージョン 1 およびバージョン 2 でスイッチが VTP トランスペアレント モード（VTP がディセーブル）の場合、拡張範囲 VLAN（1006 ～ 4096）を作成できます。VTP バージョンは、拡張範囲 VLAN をサーバ モードおよびトランスペアレント モードでサポートします。サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID が許可されている任意の switchport コマンドで使用できます。

VTP バージョン 1 または 2 での拡張範囲 VLAN の設定は VLAN データベースに格納されません。ただし、VTP モードがトランスペアレントであるため、スイッチの実行コンフィギュレーション ファイルにストアされます。設定をスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。VTP バージョン 3 で作成された拡張範囲 VLAN は、VLAN データベースに保存されます。

VLAN のデフォルト設定

表 17-2（P.17-7）にイーサネット VLAN のデフォルト設定を示します。拡張範囲 VLAN については MTU サイズ、プライベート VLAN、およびリモート SPAN 設定ステートしか変更できません。残りのすべての特性はデフォルト ステートのままでなければなりません。

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、スイッチが VTP バージョン 3 を実行していない場合は VLAN データベースに保存されず、VTP で認識されません。

- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN を作成する場合は、スイッチを VTP トランスペアレント モードにする必要があります。VTP モードがサーバまたはクライアントの場合、エラー メッセージが生成され、拡張範囲 VLAN が拒否されます。VTP バージョン 3 は、拡張範囲 VLAN をサーバ モードおよびトランスペアレント モードでサポートします。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで、VTP モードをトランスペアレントに設定できます。「VTP ドメインへの VTP クライアント スイッチの追加」（P.18-11）を参照してください。VTP トランスペアレント モードでスイッチが始動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、スイッチをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。
- 拡張範囲 VLAN では、STP はデフォルトでイネーブルになりますが、**no spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用してディセーブルにできます。スイッチ上に最大数のスパニングツリー インスタンスが存在している場合に、VLAN を新規作成すると、この VLAN 上でスパニングツリーはディセーブルになります。スイッチ上の VLAN の数がスパニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s MSTP を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 21 章「MSTP の設定」を参照してください。
- スイッチ上の各ルーテッド ポートは、内部 VLAN を使用するために作成します。この内部 VLAN は拡張範囲 VLAN 番号を使用し、その内部 VLAN ID は拡張範囲 VLAN には使用できません。内部 VLAN として割り当て済みの VLAN ID を指定して拡張範囲 VLAN を作成すると、エラー メッセージが生成され、コマンドは拒否されます。
  - 内部 VLAN ID は拡張範囲の下部の方なので、拡張範囲 VLAN を作成するには最大の番号（4096）から始めて最小値（1006）へと動いて、内部 VLAN ID を使用する可能性を減らすことを推奨します。
  - 拡張範囲 VLAN を設定する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、どの VLAN が内部 VLAN として割り当てられているかを確認します。
  - 必要に応じて、内部 VLAN に割り当てられたルーテッド ポートをシャットダウンできます。これにより、内部 VLAN が解放され、拡張範囲 VLAN を作成してポートを再度イネーブルにし、別の VLAN を内部 VLAN として使用します。「内部 VLAN ID を指定した拡張範囲 VLAN の作成」（P.17-19）を参照してください。
- スイッチは合計 1005（標準範囲および拡張範囲）の VLAN をサポートしますが、ルーテッド ポート、SVI、その他の設定済み機能の個数によって、スイッチのハードウェアの使用状況は左右されます。拡張範囲 VLAN を作成するときに、使用できるハードウェア リソースが不足していると、エラー メッセージが生成され、拡張範囲 VLAN が拒否されます。

VLAN トランク

トランキングの概要

トランクとは、1 つまたは複数のイーサネット スイッチ インターフェイスと他のネットワーキング デバイス（ルータ、スイッチなど）の間のポイントツーポイント リンクです。イーサネット トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張できます。

トランクを設定できるのは、1 つのイーサネット インターフェイスまたは EtherChannel バンドルに対してです。EtherChannel の詳細については、第 40 章「EtherChannel の設定」を参照してください。

イーサネット トランク インターフェイスは、表 17-3 に示すトランキング モードをサポートしています。インターフェイスをトランキングまたは非トランキングとして設定したり、ネイバー インターフェイスとトランキングのネゴシエーションを行ったりするように設定できます。トランキングを自動ネゴシエーションするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、PPP（ポイントツーポイント プロトコル）であるダイナミック トランキング プロトコル（DTP）によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

この事態を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

表 17-3　レイヤ 2 インターフェイス モード

モード	機能
switchport mode access	インターフェイス（アクセス ポート）を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。
switchport mode dynamic auto	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェイスは、ネイバー インターフェイスが *trunk* または *desirable* モードに設定されている場合、トランク インターフェイスになります。すべてのイーサネット インターフェイスのデフォルトのスイッチポート モードは dynamic auto です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、ネイバー インターフェイスが *trunk*、*desirable*、または *auto* モードに設定されている場合、トランク インターフェイスになります。
switchport mode trunk	インターフェイスを永続的なトランキング モードにして、ネイバー リンクのトランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スイッチポート モードが access または trunk の場合だけ使用できます。トランク リンクを確立するには、手動でネイバー インターフェイスをトランク インターフェイスとして設定する必要があります。

IEEE 802.1Q の設定時の注意事項

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制限があります。

- IEEE 802.1Q トランクを使用して接続している Cisco スイッチのネットワークでは、スイッチはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。他社製のデバイスは、すべての VLAN でスパニングツリー インスタンスを 1 つサポートする場合があります。

  IEEE 802.1Q トランクを使用して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは、トランクの VLAN のスパニングツリー インスタンスを、他社製の IEEE 802.1Q スイッチのスパニングツリー インスタンスと結合します。ただし、各 VLAN のスパニングツリー情報

は、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。Cisco スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

- IEEE 802.1Q トランクに対応するネイティブ VLAN が、トランク リンクの両側で一致していなければなりません。トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニングツリー ループが発生する可能性があります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせずに、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。IEEE 802.1Q トランクのネイティブ VLAN 上でスパニングツリーをイネーブルのままにしておくか、またはネットワーク上のすべての VLAN でスパニングツリーをディセーブルにすることを推奨します。また、ネットワークにループがないことを確認してから、スパニングツリーをディセーブルにしてください。

レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

表 17-4　レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
インターフェイス モード	switchport mode dynamic auto
VLAN 許容範囲	VLAN 1 ～ 4096
プルーニングに適格な VLAN 範囲	VLAN 2 ～ 1001
デフォルト VLAN（アクセス ポート用）	VLAN 1
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1

トランク ポートとしてのイーサネット インターフェイス

トランク ポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、スイッチ上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。

（注） デフォルトでは、インターフェイスはレイヤ 2 モードです。レイヤ 2 インターフェイスのデフォルト モードは、**switchport mode dynamic auto** です。隣接インターフェイスがトランキングをサポートし、トランキングを許可するように設定されている場合、リンクはレイヤ 2 トランクです。また、インターフェイスがレイヤ 3 モードの場合は、**switchport** インターフェイス コンフィギュレーション コマンドを入力するとレイヤ 2 トランクになります。

トランキングと他の機能との相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートは、トンネル ポートにできません。

- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかについて、設定を変更すると、入力した設定値がスイッチによってグループ内のすべてのポートに伝播されます。
  - 許可 VLAN リスト。
  - 各 VLAN の STP ポート プライオリティ。
  - STP PortFast の設定値。
  - トランク ステータス。ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- PVST モードで設定するトランク ポートの数は 24 まで、MST モードで設定するトランク ポートの数は 40 までにすることを推奨します。
- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

トランクでの許可 VLAN

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランクですべての VLAN ID（1 ～ 4096）が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。トランクが伝送するトラフィックを制限するには、**switchport trunk allowed vlan remove** *vlan-list* インターフェイス コンフィギュレーション コマンドを使用して、許可リストから特定の VLAN を削除します。

（注） VLAN 1 は、すべての Cisco スイッチのすべてのトランク ポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を必ずイネーブルにする必要がありました。VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザ トラフィック（スパニングツリー アドバタイズなど）は VLAN 1 で送受信されなくなります。

スパニングツリー ループまたはストームのリスクを軽減するには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートで VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol（CDP）、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、DTP、および VTP などの管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、**switchport trunk allowed** の設定には関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている任意の VLAN について同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバになることができます。VTP が新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されて

いる場合、トランク ポートは自動的にその VLAN のメンバになります。VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバにはなりません。

タグなしトラフィック用ネイティブ VLAN

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、タグなしトラフィックは、ポートに設定されたネイティブ VLAN に転送されます。ネイティブ VLAN は、デフォルトでは VLAN 1 です。

（注）　ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

IEEE 802.1Q 設定についての詳細は、「IEEE 802.1Q の設定時の注意事項」（P.17-10）を参照してください。

トランク ポートを使用した負荷分散

負荷分散により、スイッチに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、スイッチ間で 1 つのパラレル リンク以外のすべてのリンクをブロックします。負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

トランク ポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使用します。STP ポート プライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リンクを同じスイッチに接続する必要があります。STP パス コストを使用して負荷分散を設定する場合には、それぞれの負荷分散リンクを同一のスイッチにも、2 台の異なるスイッチにも接続できます。STP の詳細については、第 20 章「STP の設定」を参照してください。

STP ポート プライオリティによる負荷分散

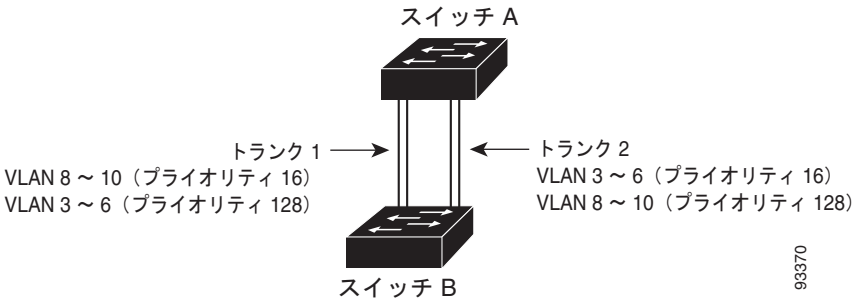
同一スイッチ上の 2 つのポートがループを形成すると、スイッチは STP ポート プライオリティを使用して、どのポートをイネーブルとし、どのポートをブロッキング ステートとするかを判断します。パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送します。同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロッキング ステートのままです。1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

図 17-2 に、サポート対象スイッチを接続する 2 つのトランクを示します。この例では、スイッチは次のように設定されています。

- VLAN 8 ～ 10 は、トランク 1 で 16 というポート プライオリティが割り当てられています。
- VLAN 3 ～ 6 は、トランク 1 でデフォルトのポート プライオリティである 128 のままです。
- VLAN 3 ～ 6 は、トランク 2 で 16 というポート プライオリティが割り当てられています。
- VLAN 8 ～ 10 は、トランク 2 でデフォルトのポート プライオリティである 128 のままです。

このように設定すると、トランク 1 が VLAN 8 ～ 10 のトラフィックを伝送し、トランク 2 が VLAN 3 ～ 6 のトラフィックを伝送します。アクティブ トランクで障害が起きた場合には、プライオリティの低いトランクが引き継ぎ、それらすべての VLAN のトラフィックを伝送します。いずれのトランク ポート上でも、トラフィックの重複は発生しません。

図 17-2　STP ポート プライオリティによる負荷分散



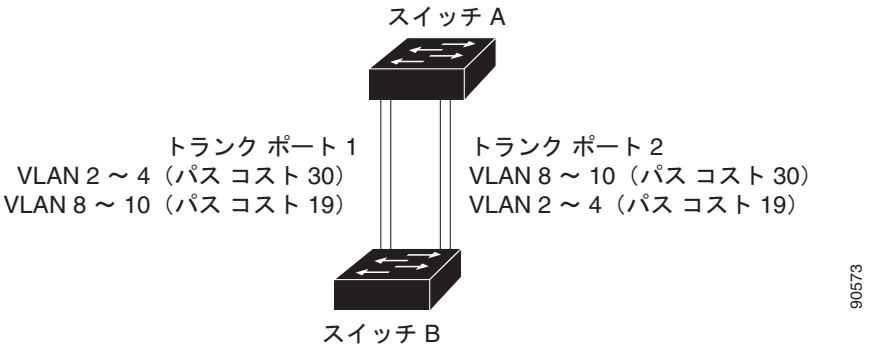
STP パス コストによる負荷分散

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トランクを設定できます。VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持します。

図 17-3 で、トランク ポート 1 および 2 は 100BASE-T ポートとして設定されています。次の VLAN パス コストが割り当てられています。

- VLAN 2 ～ 4 は、トランク ポート 1 で 30 というパス コストが割り当てられています。
- VLAN 8 ～ 10 は、トランク ポート 1 で 100BASE-T のデフォルトのパス コストである 19 のままです。
- VLAN 8 ～ 10 は、トランク ポート 2 で 30 というパス コストが割り当てられています。
- VLAN 2 ～ 4 は、トランク ポート 2 で 100BASE-T のデフォルトのパス コストである 19 のままです。

図 17-3　パス コストによってトラフィックが分散される負荷分散トランク



「STP パス コストによる負荷分散の設定」（P.17-22）を参照してください。

VMPS

VLAN Query Protocol（VQP）は、ダイナミックアクセス ポートをサポートする場合に使用します。ダイナミックアクセス ポートは VLAN に永続的に割り当てられるのではなく、ポートで認識された MAC（メディア アクセス コントロール）送信元アドレスに基づいて VLAN を割り当てます。未知の

MAC アドレスが検出されるたびに、スイッチはリモート VMPS に VQP クエリーを送信します。クエリーには新たに検出された MAC アドレスとそのアドレスを検出したポートが含まれます。VMPS はそのポートの VLAN 割り当てで応答します。このスイッチを VMPS サーバにすることはできませんが、VMPS のクライアントとして機能させ、VQP を介して通信できます。

クライアント スイッチは新しいホストの MAC アドレスを受信するたびに、VMPS に VQP クエリーを送信します。このクエリーを受信した VMPS は、データベースで MAC アドレスと VLAN のマッピングを検索します。サーバの応答は、このマッピングと、サーバがオープン モードかセキュア モードかに基づいて行われます。セキュア モードの場合、サーバは不正なホストが検出されると、ポートをシャットダウンします。オープン モードでは、サーバはホストに対してポート アクセスを拒否するだけです。

ポートが*未割り当て*の場合（つまり、VLAN 割り当てがまだ設定されていない場合）、VMPS は次のいずれかの応答を行います。

- そのポートでホストが許可されている場合、VMPS は割り当てられた VLAN 名を指定し、ホストへのアクセスを許可する *VLAN 割り当て*応答をクライアントに送信します。
- そのポートでホストが許可されておらず、なおかつ VMPS がオープン モードの場合、VMPS は*アクセス拒否*応答を送信します。
- そのポートで VLAN が許可されておらず、なおかつ VMPS がセキュア モードの場合、VMPS は*ポートシャットダウン*応答を送信します。

ポートに VLAN 割り当てがすでに設定されている場合、VMPS は次のいずれかの応答を行います。

- データベース内の VLAN がポート上の現在の VLAN と一致した場合、VMPS は*成功*応答を送信し、ホストへのアクセスを許可します。
- データベース内の VLAN がポート上の現在の VLAN と一致せず、なおかつポート上にアクティブ ホストが存在する場合、VMPS は VMPS のセキュア モードに応じて、*アクセス拒否*または*ポートシャットダウン*応答を送信します。

VMPS から*アクセス拒否*応答を受信した場合、スイッチはそのホスト MAC アドレスのトラフィックを双方向で引き続きブロックします。スイッチはポート宛てのパケットを引き続きモニタし、新しいホスト アドレスを検出すると VMPS にクエリーを送信します。VMPS から*ポートシャットダウン*応答を受信した場合、スイッチはそのポートをディセーブルにします。Network Assistant、CLI（コマンドライン インターフェイス）、または SNMP（簡易ネットワーク管理プロトコル）を使用して、ポートを手動で再びイネーブルにする必要があります。

ダイナミックアクセス ポート VLAN メンバーシップ

ダイナミックアクセス ポートが所属できるのは、VLAN ID が 1 ～ 4096 の 1 つの VLAN だけです。リンクがアップになっても、VMPS によって VLAN が割り当てられるまで、このポートとの間でトラフィック転送は行われません。VMPS は、ダイナミックアクセス ポートに接続した新しいホストの最初のパケットから送信元 MAC アドレスを受信し、VMPS データベースの VLAN とその MAC アドレスを照合します。

一致した場合、VMPS はそのポートの VLAN 番号を送信します。クライアント スイッチがまだ設定されていない場合は、スイッチは VMPS からトランク ポートで受信した最初の VTP パケットからのドメイン名を使用します。クライアント スイッチがすでに設定されている場合は、クエリー パケットにスイッチのドメイン名を含めて VMPS に送信し、VLAN 番号を取得します。VMPS はパケット内のドメイン名が自身のドメイン名と一致することを確認した後、要求を受け入れ、クライアントに割り当てられた VLAN 番号を応答します。一致しない場合、（VMPS セキュア モードの設定に応じて）VMPS は要求を拒否するか、ポートをシャットダウンします。

ダイナミックアクセス ポート上で複数のホスト（MAC アドレス）をアクティブにできますが、それらのホストはすべて同じ VLAN に存在する必要があります。ただし、ポート上でアクティブなホスト数が 20 を超えると、VMPS はダイナミックアクセス ポートをシャットダウンします。

ダイナミックアクセス ポート上でリンクがダウンになると、ポートは切り離された状態に戻り、VLAN の所属から外れます。ポート経由でオンラインになるホストは VMPS によって VQP 経由で再チェックされてから、ポートが VLAN に割り当てられます。

ダイナミックアクセス ポートは、直接ホスト接続に使用したり、ネットワークに接続したりできます。スイッチ上のポートごとに、最大 20 の MAC アドレスを使用できます。ダイナミックアクセス ポートが一度に所属できる VLAN は 1 つだけですが、VLAN は検出された MAC アドレスに基づいて後で変更されることがあります。

VMPS クライアントのデフォルト設定

表 17-5　VMPS クライアントおよびダイナミックアクセス ポートのデフォルト設定

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認インターバル	60 分
VMPS サーバ再試行回数	3
ダイナミックアクセス ポート	未設定

VMPS 設定時の注意事項

ダイナミックアクセス ポート VLAN メンバーシップには、次の注意事項および制限事項があります。

- VMPS を設定してから、ポートをダイナミックアクセス ポートとして設定する必要があります。
- ポートをダイナミックアクセス ポートとして設定すると、そのポートに対してスパニングツリーの PortFast 機能が自動的にイネーブルになります。PortFast モードにより、ポートをフォワーディング ステートに移行させるプロセスが短縮されます。
- IEEE 802.1x ポートをダイナミックアクセス ポートとして設定することはできません。ダイナミックアクセス（VQP）ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- トランク ポートをダイナミックアクセス ポートにすることはできませんが、トランク ポートに対して **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力することは可能です。その場合、スイッチの設定は維持され、後にアクセス ポートとして設定された場合には、その設定が適用されます。

  ダイナミックアクセス設定を有効にするには、ポート上でトランキングをオフにしておく必要があります。
- ダイナミックアクセス ポートをモニタ ポートにすることはできません。
- セキュア ポートをダイナミックアクセス ポートにすることはできません。ポートをダイナミックにするには、ポート上でポート セキュリティをディセーブルにしておく必要があります。
- プライベート VLAN ポートは、ダイナミックアクセス ポートにできません。
- ダイナミックアクセス ポートを EtherChannel グループのメンバにすることはできません。
- ポート チャネルをダイナミックアクセス ポートとして設定することはできません。
- ダイナミックアクセス ポートは、フォールバック ブリッジングに加入できます。
- VMPS クライアントと VMPS サーバの VTP 管理ドメインは、同じでなければなりません。

- VMPS サーバ上に設定された VLAN を音声 VLAN にしないでください。

VMPS 再確認インターバル

VMPS クライアントは、VMPS から受信する VLAN メンバーシップの情報を定期的に再確認します。再確認を実行する間隔は数字を使用して分単位で設定できます。

クラスタのメンバ スイッチを設定する場合、このパラメータはコマンド スイッチの再確認インターバルの設定値以上でなければなりません。メンバ スイッチにログインするには、最初に **rcommand** 特権 EXEC コマンドを使用する必要があります。

ダイナミックアクセス ポート VLAN メンバーシップ

VMPS は次の状況でダイナミックアクセス ポートをシャットダウンします。

- VMPS がセキュア モードであり、なおかつホストのポートへの接続を許可しない場合。VMPS はポートをシャットダウンして、ホストがネットワークに接続できないようにします。
- ダイナミックアクセス ポート上のアクティブ ホストが 20 を超えた場合。

ディセーブルにされているダイナミックアクセス ポートを再びイネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドに続けて、**no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

VLAN の設定方法

イーサネット VLAN の作成または変更

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。 **（注）** このコマンドで指定できる VLAN ID 範囲は 1 ～ 4096 です。1005 を超える VLAN ID（拡張範囲 VLAN）を追加する手順については、「拡張範囲 VLAN の作成」（P.17-18）を参照してください。
ステップ 3	**name** *vlan-name*	（任意）VLAN の名前を入力します。VLAN 名を指定しなかった場合には、デフォルトとして、VLAN という語の後ろに先行ゼロを含めた *vlan-id* が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。
ステップ 4	**mtu** *mtu-size*	（任意）MTU サイズ（または他の VLAN 特性）を変更します。
ステップ 5	**remote-span**	（任意）リモート スイッチド ポート アナライザ（SPAN）セッションに対する RSPAN VLAN として、VLAN を設定します。 **（注）** リモート SPAN の詳細は、第 30 章「SPAN および RSPAN の設定」を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。

VLAN の削除

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no vlan** *vlan-id*	VLAN ID を入力して、VLAN を削除します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

VLAN へのスタティック アクセス ポートの割り当て

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	VLAN に追加するインターフェイスを入力します。
ステップ 3	**switchport mode access**	ポート（レイヤ 2 アクセス ポート）の VLAN メンバーシップ モードを定義します。
ステップ 4	**switchport access vlan** *vlan-id*	VLAN にポートを割り当てます。指定できる VLAN ID の範囲は 1 ～ 4096 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。

拡張範囲 VLAN の作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp mode transparent**	スイッチを VTP トランスペアレント モードに設定し、VTP をディセーブルにします。 **（注）**　この手順は、VTP バージョン 3 では不要です。
ステップ 3	**vlan** *vlan-id*	拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ～ 4096 です。
ステップ 4	**mtu** *mtu-size*	（任意）MTU サイズを変更して、VLAN を変更します。 **（注）**　CLI ヘルプにすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされているのは、**mtu** *mtu-size* コマンド、**private-vlan** コマンド、**remote-span** コマンドだけです。
ステップ 5	**remote-span**	（任意）RSPAN VLAN として VLAN を設定します。「RSPAN VLAN としての VLAN の設定」（P.30-15）を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。

内部 VLAN ID を指定した拡張範囲 VLAN の作成

	コマンド	目的
ステップ 1	**show vlan internal usage**	スイッチが内部的に使用している VLAN ID を表示します。使用したい VLAN ID が内部 VLAN である場合は、その VLAN ID を使用しているルーテッド ポートが表示されます。そのポート番号をステップ 3 で入力してください。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	その VLAN ID を使用しているルーテッド ポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**shutdown**	ポートをシャットダウンして内部 VLAN ID を解放します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**vtp mode transparent**	VTP モードをトランスペアレントに設定して拡張範囲 VLAN を作成します。 **（注）**　この手順は、VTP バージョン 3 では不要です。
ステップ 7	**vlan** *vlan-id*	新しい拡張範囲 VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。
ステップ 8	**exit**	VLAN コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *interface-id*	ステップ 4 でシャットダウンしたルーテッド ポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**no shutdown**	ルーテッド ポートを再度イネーブルにします。新しい内部 VLAN ID が割り当てられます。
ステップ 11	**end**	特権 EXEC モードに戻ります。

トランク ポートとしてのイーサネット インターフェイスの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。 • **dynamic auto**：ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これはデフォルトです。 • **dynamic desirable**：ネイバー インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • **trunk**：ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。
ステップ 4	**switchport access vlan** *vlan-id*	（任意）インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。
ステップ 5	**switchport trunk native vlan** *vlan-id*	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

トランクでの許可 VLAN の定義

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 4	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*	（任意）トランク上で許容される VLAN のリストを設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

プルーニング適格リストの変更

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	VLAN プルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan*[,*vlan*[,,,]]	トランクからのプルーニングを許可する VLAN のリストを設定します。（「VTP プルーニング」（P.18-8）を参照）。
ステップ 4	**end**	特権 EXEC モードに戻ります。

タグなしトラフィック用ネイティブ VLAN の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport trunk native vlan** *vlan-id*	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

STP ポート プライオリティによる負荷分散

	コマンド	目的
ステップ 1	**configure terminal**	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp domain** *domain-name*	VTP 管理ドメインを設定します。 1 ～ 32 文字のドメイン名を使用できます。
ステップ 3	**vtp mode server**	スイッチ A を VTP サーバとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status**	スイッチ A および B の両方で、VTP 設定を確認します。
ステップ 6	**show vlan**	スイッチ A のデータベースに VLAN が存在していることを確認します。
ステップ 7	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**interface** *interface-id_1*	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show interfaces** *interface-id_1* **switchport**	VLAN の設定を確認します。
ステップ 12	スイッチの 2 番めのポートについて、スイッチ A 上でステップ 7 ～ 10 を繰り返します。	
ステップ 13	スイッチ B でステップ 7 ～10 を繰り返し、スイッチ A で設定されたトランク ポートに接続するトランク ポートを設定します。	
ステップ 14	**show vlan**	トランク リンクがアクティブになると、VTP がスイッチ B に VTP および VLAN 情報を渡します。スイッチ B が VLAN 設定を学習したことを確認します。
ステップ 15	**configure terminal**	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 16	**interface** *interface-id_1*	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 17	**spanning-tree vlan 8-10 port-priority 16**	VLAN 8 ～ 10 にポート プライオリティ 16 を割り当てます。

	コマンド	目的
ステップ 18	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 19	**interface** *interface-id_2*	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 20	**spanning-tree vlan 3-6 port-priority 16**	VLAN 3 ～ 6 にポート プライオリティ 16 を割り当てます。
ステップ 21	**end**	特権 EXEC モードに戻ります。

STP パス コストによる負荷分散の設定

	コマンド	目的
ステップ 1	**configure terminal**	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id_1*	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5		スイッチ A の 2 番めのインターフェイスでステップ 2 ～ 4 を繰り返します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力を確認します。画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。
ステップ 8	**show vlan**	トランク リンクがアクティブになると、スイッチ A がもう一方のスイッチから VTP 情報を受信します。スイッチ A が VLAN 設定を学習したことを確認します。
ステップ 9	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface** *interface-id_1*	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**spanning-tree vlan 2-4 cost 30**	VLAN 2 ～ 4 のスパニングツリー パス コストを 30 に設定します。
ステップ 12	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	スイッチ A に設定したもう一方のトランク インターフェイスで、ステップ 9 ～ 12 を繰り返し、VLAN 8、9、および 10 のスパニングツリー パス コストを 30 に設定します。	
ステップ 14	**exit**	特権 EXEC モードに戻ります。
ステップ 15	**show running-config**	入力を確認します。両方のトランク インターフェイスに対してパス コストが正しく設定されていることを表示で確認します。

VMPS クライアントの設定

ダイナミック VLAN を設定するには、VMPS（VLAN メンバーシップ ポリシー サーバ）を使用します。スイッチを VMPS クライアントにすることはできますが、VMPS サーバにすることはできません。

VMPS の IP アドレスの入力

はじめる前に

- スイッチをクライアントとして設定するには、サーバの IP アドレスを最初に入力する必要があります。
- ダイナミックアクセス ポートを動作させるには、VMPS に IP 接続できなければなりません。IP 接続が可能かどうかをテストするには、VMPS の IP アドレスに ping を実行し、応答が得られるかどうかを確認します。
- スイッチ クラスタに対して VMPS を定義する場合は、コマンド スイッチにこのアドレスを入力する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vmps server** *ipaddress* **primary**	プライマリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。
ステップ 3	**vmps server** *ipaddress*	（任意）セカンダリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。 セカンダリ サーバのアドレスは、3 つまで入力できます。
ステップ 4	**vmps reconfirm**	（任意）ダイナミックアクセス ポート VLAN メンバーシップを再確認します。
ステップ 5	**vmps retry** *count*	（任意）再試行の回数を変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

VMPS クライアント上のダイナミックアクセス ポートの設定

はじめる前に

クラスタ メンバ スイッチのポートをダイナミックアクセス ポートとして設定するには、最初に **rcommand** 特権 EXEC コマンドを使用して、そのクラスタ メンバ スイッチにログインします。

注意　ダイナミックアクセス ポート VLAN メンバーシップはエンド ステーション用、またはエンド ステーションに接続されたハブ用です。他のスイッチにダイナミックアクセス ポートを接続すると、接続が切断されることがあります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	エンド ステーションに接続するスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access**	ポートをアクセス モードに設定します。
ステップ 4	**switchport access vlan dynamic**	ポートをダイナミック VLAN メンバーシップ適格として設定します。 ダイナミックアクセス ポートは、エンド ステーションに接続されている必要があります。
ステップ 5	**end**	特権 EXEC モードに戻ります。

VLAN のモニタリングおよびメンテナンス

コマンド	目的
copy running-config startup config	コンフィギュレーション ファイルに設定を保存します。 • 拡張範囲 VLAN 設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP トランスペアレント モード設定と拡張範囲 VLAN 設定を保存する必要があります。これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバ モードになり、拡張範囲 VLAN ID は保存されません。 • VTP バージョン 3 では、VLAN が VLAN データベースに保存されるため、この手順は必要ありません。
show interfaces *interface-id* **switchport**	インターフェイスのスイッチ ポートの設定を表示します。
show interfaces *interface-id* **trunk**	インターフェイスのトランクの設定を表示します。
show running-config interface *interface-id*	インターフェイスの VLAN メンバーシップ モードを確認します。
show vmps	VMPS エントリを確認します。
show vlan	VLAN エントリを確認します。

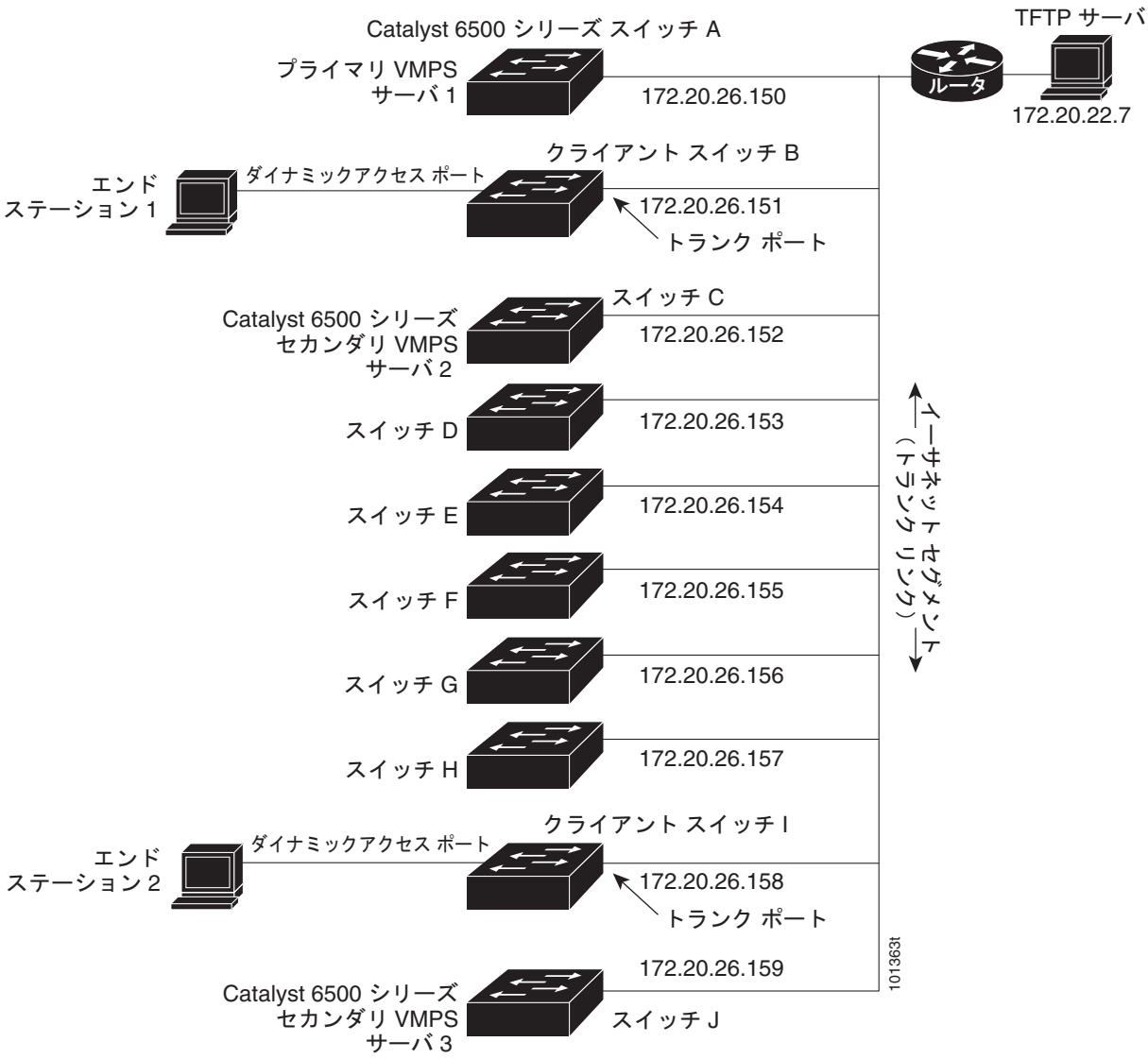
VLAN の設定例

VMPS ネットワーク：例

図 17-4 に、VMPS サーバ スイッチと、ダイナミック アクセス ポートを備えた VMPS クライアント スイッチが含まれるネットワークの例を示します。この例の前提条件は次のとおりです。

- VMPS サーバと VMPS クライアントは、それぞれ別のスイッチです。
- Catalyst 6500 シリーズのスイッチ A が、プライマリ VMPS サーバです。
- Catalyst 6500 シリーズのスイッチ C およびスイッチ J が、セカンダリ VMPS サーバです。
- エンド ステーションはクライアント（スイッチ B、スイッチ I）に接続されています。
- データベース コンフィギュレーション ファイルは、IP アドレス 172.20.22.7 の TFTP サーバに保存されています。

図 17-4　ダイナミック ポート VLAN メンバーシップの構成例



VLAN の設定：例

次に、イーサネット VLAN 20 を作成し、*test20* という名前を付け、VLAN データベースに追加する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

VLAN アクセス ポートの設定：例

次に、VLAN 2 のアクセス ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

拡張範囲 VLAN の設定：例

次の例では、すべての特性をデフォルトで持つ新しい拡張範囲 VLAN を作成する方法を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

トランク ポートの設定：例

次に、IEEE 802.1Q トランクとしてポートを設定する例を示します。この例では、ネイバー インターフェイスが IEEE 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```

VLAN の削除：例

次に、ポートの許可 VLAN リストから VLAN 2 を削除する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

VMPS 出力を表示：例

次に、**show vmps** 特権 EXEC コマンドの出力例を示します。

```
Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         other
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
VTP プルーニングの設定	*第 18 章「VTP の設定」*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 18

VTP の設定

VTP 機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VTP の設定の前提条件

- VTP を設定する場合は、スイッチがドメイン内の他のスイッチと VTP アドバタイズメントを送受信できるように、トランク ポートを設定する必要があります。詳細については、「トランク ポートとしてのイーサネット インターフェイスの設定」（P.17-19）を参照してください。
- VTP クライアント スイッチを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP コンフィギュレーション リビジョン番号の確認手順およびリセット手順については、「VTP ドメインへの VTP クライアント スイッチの追加」（P.18-14）を参照してください。

VTP の設定に関する制約事項

- VTP バージョン 3 では、スイッチが LAN Base イメージを実行している必要があります。
- 同一 VTP ドメイン内のスイッチ上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。VTP ドメイン内のすべてのスイッチが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにはしないでください。
- VTP バージョン 1 および 2 では、そのスイッチで拡張範囲 VLAN を設定するとき、スイッチは VTP トランスペアレント モードでなければなりません。VTP バージョン 3 でも、クライアント モードまたはサーバ モードでの拡張範囲 VLAN の作成をサポートしています。

VTP の設定に関する情報

VTP

VLAN Trunking Protocol（(VTP) は、レイヤ 2 のメッセージ プロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のスイッチ上で中央集約的に設定変更を行い、その変更を自動的にネットワーク上の他のスイッチに伝達できます。VTP を使用しない場合、VLAN 情報を他のスイッチに送信することはできません。

VTP は、1 台のスイッチで行われた更新が VTP を介してドメイン内の他のスイッチに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のスイッチ上で同時に発生する環境の場合、VTP は適していません。VLAN データベースの不整合が生じます。

スイッチは 1005 の VLAN をサポートしますが、設定済み機能の個数によって、スイッチ ハードウェアの使用が左右されます。VTP が新しい VLAN をスイッチに通知し、スイッチが使用可能な最大限のハードウェア リソースをすでに使用している場合、スイッチはハードウェア リソース不足を伝えるメッセージを送信して、VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。

VTP バージョン 1 およびバージョン 2 は、標準範囲の VLAN（VLAN ID 1 ～ 1005）だけをサポートします。VTP バージョン 3 は、VLAN 範囲全体（VLAN 1 ～ 4096）をサポートします。拡張範囲 VLAN（VLAN 1006 ～ 4096）は、VTP バージョン 3 でだけサポートされます。拡張 VLAN がドメインに設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

VTP ドメイン

VTP ドメイン（別名 VLAN 管理ドメイン）は、1 つのスイッチ、または同じ VTP ドメイン名を共有して同一管理下にある相互接続された複数のスイッチで構成されます。スイッチは、1 つの VTP ドメインにだけ所属できます。そのドメインに対してグローバル VLAN の設定を変更します。

デフォルトの設定では、トランク リンク（複数 VLAN のトラフィックを伝送するリンク）を介してドメインについてのアドバタイズを受信しない限り、またはユーザがドメイン名を設定しない限り、スイッチは VTP 非管理ドメイン ステートです。管理ドメイン名を指定するか学習するまでは、VTP サーバ上で VLAN を作成または変更できません。また、VLAN 情報はネットワークを介して伝播されません。

スイッチがトランク リンクを介して VTP アドバタイズを受信すると、スイッチは管理ドメイン名および VTP コンフィギュレーション リビジョン番号を継承します。その後スイッチは、別のドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズについては、すべて無視します。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのスイッチに伝播されます。VTP アドバタイズは、IEEE 802.1Q を含め、すべての IEEE トランク接続に送信されます。VTP は、複数の LAN タイプにわたり、固有の名前と内部インデックスの対応によって VLAN を動的にマッピングします。このマッピングにより、ネットワーク管理者がデバイスを管理するための作業負担が大幅に軽減されます。

VTP トランスペアレント モードでスイッチを設定した場合、VLAN の作成および変更は可能ですが、その変更はドメイン内の他のスイッチには送信されません。また、変更が作用するのは、個々のスイッチに限られます。ただし、スイッチがこのモードのときに設定を変更すると、変更内容がスイッチの実行コンフィギュレーションに保存されます。この変更はスイッチのスタートアップ コンフィギュレーション ファイルに保存することもできます。

ドメイン名およびパスワードの設定時の注意事項については、「VTP 設定時の注意事項」（P.18-10）を参照してください。

VTP モード

表 18-1　VTP モード

VTP モード	説明
VTP サーバ	VTP サーバ モードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ（VTP バージョンなど）を指定できます。VTP サーバは、同一 VTP ドメイン内の他のスイッチに自身の VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて、自身の VLAN 設定を他のスイッチと同期させます。 VTP サーバがデフォルトのモードです。 **（注）** VTP サーバ モードでは、VLAN 設定は NVRAM に保存されます。スイッチがコンフィギュレーションを NVRAM に書き込んでいる間に障害を検出すると、VTP モードはサーバ モードからクライアント モードに自動的に移行します。この場合、スイッチは NVRAM が動作するまで VTP サーバ モードに戻ることができません。
VTP クライアント	VTP クライアントは VTP サーバと同様に動作し、対応するトランクで VTP アップデートを送受信しますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。VLAN は、ドメインに含まれる、他のサーバ モードのスイッチで設定します。 VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM に保存されません。VTP バージョン 3 では、VLAN 設定はクライアント モードで NVRAM に保存されます。
VTP トランスペアレント	VTP トランスペアレント スイッチは、VTP に参加しません。VTP トランスペアレント スイッチは自身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設定を同期させることもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレント スイッチは、トランク インターフェイスを介して他のスイッチから受信した VTP アドバタイズを転送します。VTP トランスペアレント モードでは、スイッチ上の VLAN を作成、変更、削除できます。 VTP バージョン 1 および 2 では、拡張範囲 VLAN を作成するときはスイッチを VTP トランスペアレント モードにする必要があります。VTP バージョン 3 でも、クライアント モードまたはサーバ モードでの拡張範囲 VLAN の作成をサポートしています。「拡張範囲 VLAN の作成」（P.17-18）を参照してください。 スイッチが VTP トランスペアレント モードの場合、VTP および VLAN の設定は NVRAM に保存されますが、他のスイッチにはアドバタイズされません。このモードでは、VTP モードおよびドメイン名はスイッチの実行コンフィギュレーションに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。
VTP オフ	VTP オフ モードでのスイッチの機能は、トランクを介して VTP アドバタイズを転送しないことを除くと VTP トランスペアレント スイッチとしての機能と同じです。

VTP モードのガイドライン

- VTP バージョン 1 およびバージョン 2 では、拡張範囲 VLAN がスイッチ上に設定されている場合、VTP モードをクライアントまたはサーバに変更できません。エラー メッセージが表示され、設定が許可されません。VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4096）の設定情報を伝播しません。これらの VLAN を各装置上に手動で設定する必要があります。

（注）　VTP バージョン 1 およびバージョン 2 の場合、拡張範囲 VLAN（VLAN ID 1006 ～ 4096）を作成するには、事前に **vtp mode transparent** グローバル コンフィギュレーション コマンドを使用して、VTP モードをトランスペアレントに設定する必要があります。VTP トランスペアレント モードでスイッチが開始するように、この設定をスタートアップ コンフィギュレーションに保存してください。このようにしないと、スイッチのリセット時に拡張範囲 VLAN 設定が失われ、VTP サーバ モード（デフォルト）で起動します。

- VTP バージョン 3 は拡張範囲 VLAN をサポートします。拡張 VLAN が設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。
- スイッチを VTP クライアント モードに設定した場合、VLAN データベース ファイル（vlan.dat）は作成されません。そのままスイッチの電源をオフにすると、VTP 設定はデフォルトにリセットされます。スイッチが再起動された後も VTP 設定を VTP クライアント モードに維持するには、VTP モードを設定する前に、VTP ドメイン名を設定する必要があります。
- スイッチが VTP サーバ モードの場合には、VLAN 設定を変更し、その変更をネットワーク全体に伝播できます。
- スイッチが VTP クライアント モードの場合には、そのスイッチの VLAN 設定を変更できません。クライアント スイッチは、VTP ドメイン内の VTP サーバから VTP アップデート情報を受信し、それに基づいて設定を変更します。
- スイッチを VTP トランスペアレント モードに設定すると、スイッチの VTP はディセーブルになります。VTP トランスペアレント スイッチは VTP アップデートを送信せず、他のスイッチから受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 を実行する VTP トランスペアレント モードのスイッチは、対応するトランク リンクで、受信した VTP アドバタイズを転送します。
- VTP オフ モードは、VTP アドバタイズが転送されない以外は、VTP トランスペアレント モードと同じです。

注意　すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメイン名を設定しないでください。ドメイン名を設定すると、そのドメインの VLAN 設定を変更できなくなります。したがって、少なくとも 1 台のスイッチを VTP サーバとして設定してください。

VTP アドバタイズ

VTP ドメイン内の各スイッチは、専用のマルチキャスト アドレスに対して、それぞれのトランク ポートからグローバル コンフィギュレーション アドバタイズを定期的に送信します。このようなアドバタイズを受信したネイバー スイッチは、必要に応じて各自の VTP および VLAN 設定をアップデートします。

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP 設定のリビジョン番号
- アップデート ID およびアップデート タイムスタンプ
- 各 VLAN の最大伝送単位（MTU）サイズを含む MD5 ダイジェスト VLAN コンフィギュレーション
- フレーム形式

VTP アドバタイズではさらに、設定されている各 VLAN について、次の VLAN 情報が配信されます。

- VLAN ID（ISL および IEEE 802.1Q）
- VLAN 名
- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、VTP アドバタイズにはプライマリ サーバ ID、インスタンス番号、および開始インデックスも含まれます。

VTP バージョン 2

ネットワークで VTP を使用する場合、VTP のどのバージョンを使用するかを決定する必要があります。デフォルトでは、バージョン 1 の VTP が動作します。

VTP バージョン 1 でサポートされず、バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリング サポート：VTP バージョン 2 は、トークンリング ブリッジ リレー機能（TrBRF）およびトークンリング コンセントレータ リレー機能（TrCRF）VLAN をサポートします。トークンリング VLAN の詳細については、「標準範囲 VLAN」（P.17-4）を参照してください。
- 認識不能な Type-Length-Value（TLV）のサポート：VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、スイッチが VTP サーバ モードで動作している場合、NVRAM に保存されます。
- バージョン依存型トランスペアレント モード：VTP バージョン 1 の場合、VTP トランスペアレント スイッチが VTP メッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。VTP バージョン 2 がサポートするドメインは 1 つだけですが、VTP バージョン 2 トランスペアレント スイッチは、ドメイン名が一致した場合のみメッセージを転送します。
- 整合性検査：VTP バージョン 2 の場合、CLI（コマンドライン インターフェイス）、または SNMP（簡易ネットワーク管理プロトコル）を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

VTP バージョン 3

VTP バージョン 1 または 2 でサポートされず、バージョン 3 でサポートされる機能は、次のとおりです。

- 拡張認証：認証を **hidden** または **secret** として設定できます。設定を **hidden** にしている場合、パスワード文字列からの秘密キーは VLAN のデータベース ファイルに保存されますが、設定においてプレーン テキストで表示されることはありません。代わりに、パスワードに関連付けられているキーが 16 進表記で実行コンフィギュレーションに保存されます。ドメインにテイクオーバー コマンドを入力するときは、パスワードを再入力する必要があります。キーワード **secret** を入力する場合、パスワードに秘密キーを直接設定できます。
- 拡張範囲 VLAN（VLAN 1006 ～ 4096）のデータベース伝播をサポートします。VTP バージョン 1 および 2 で伝播する範囲は、VLAN 1 ～ 1005 だけです。拡張 VLAN を設定している場合は、VTP バージョン 3 からバージョン 1 または 2 に変換できません。

  （注） VTP プルーニングは引き続き VLAN 1 ～ 1005 にだけ適用され、VLAN 1002 ～ 1005 は予約されたままで変更できません。

- ドメインの任意のデータベースをサポートします。VTP 情報の伝播に加えて、バージョン 3 は Multiple Spanning Tree Protocol（MSTP）データベース情報を伝播できます。VTP プロトコルの個別インスタンスが VTP を使用する各アプリケーションで実行されます。
- VTP プライマリ サーバと VTP セカンダリ サーバ。VTP プライマリ サーバはデータベース情報をアップデートし、システム内のすべてのデバイスによって行われるアップデートを送信します。VTP セカンダリ サーバで実行できるのは、プライマリ サーバから NVRAM に受け取ったアップデート済み VTP コンフィギュレーションのバックアップだけです。

  デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。**vtp primary** 特権 EXEC コマンドを入力してプライマリ サーバを指定することができます。プライマリ サーバのステータスは、管理者がドメインでテイクオーバー メッセージを発行する場合、データベースのアップデート用に必要となるだけです。プライマリ サーバなしで実用 VTP ドメインを持つことができます。プライマリ サーバのステータスは、スイッチにパスワードが設定されている場合でも、装置がリロードしたり、ドメインのパラメータが変更したりすると失われます。
- トランク（ポート）単位で VTP をオンまたはオフにするオプション。[**no**] **vtp** インタフェイス コンフィギュレーション コマンドを使用すると、ポート単位で VTP をイネーブルまたはディセーブルにできます。トランク ポート上で VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。VTP の設定を、MST データベースには *off* にする一方で、同じポートの VLAN データベースには *on* にすることはできません。

  グローバルに VTP モードをオフに設定すると、システムのすべてのトランク ポートにこの設定が適用されます。ただし、VTP インスタンス ベースでこのモードのオンまたはオフを指定することはできます。たとえば、VLAN データベースには、スイッチを VTP サーバとして設定する一方で、MST データベースには VTP を *off* に設定することができます。

VTP バージョンの注意事項

実装する VTP バージョンを決定する場合は、次の注意事項に従ってください。

- VTP ドメイン内のすべてのスイッチは同じドメイン名を使用する必要がありますが、すべてが同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のスイッチ上で VTP バージョン 2 がディセーブルに設定されている場合、VTP バージョン 2 対応スイッチは、VTP バージョン 1 を実行しているスイッチと同じ VTP ドメインで動作できます（デフォルトでは VTP バージョン 2 はディセーブルになっています）。

- VTP バージョン 1 を実行しているものの、VTP バージョン 2 に対応可能なスイッチが VTP バージョン 3 アドバタイズを受信すると、このスイッチは VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 を実行しているスイッチが VTP バージョン 1 を実行しているスイッチに接続すると、VTP バージョン 1 のスイッチは VTP バージョン 2 に移行し、VTP バージョン 3 のスイッチは、スケールダウンしたバージョンの VTP パケットを送信するため、VTP バージョン 2 スイッチは自身のデータベースをアップデートできます。
- VTP バージョン 3 を実行するスイッチは、拡張 VLAN を持つ場合はバージョン 1 または 2 に移行できません。
- 同一 VTP ドメイン内のすべてのスイッチがバージョン 2 に対応可能な場合を除いて、スイッチ上で VTP バージョン 2 をイネーブルにしないでください。あるスイッチでバージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応スイッチでバージョン 2 がイネーブルになります。バージョン 1 専用のスイッチがドメインに含まれている場合、そのスイッチはバージョン 2 対応スイッチとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 のスイッチは VTP バージョン 3 のアドバタイズを転送しないため、これらをネットワーク エッジに配置することを推奨します。
- 使用環境に TrBRF および TrCRF トークンリング ネットワークが含まれている場合に、トークンリング VLAN スイッチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4096）の設定情報を伝播しません。これらの VLAN は各装置で手動によって設定する必要があります。VTP バージョン 3 は拡張範囲 VLAN をサポートします。拡張 VLAN を設定している場合、VTP バージョン 3 から VTP バージョン 2 に変換できません。
- VTP バージョン 3 装置のトランク ポートが VTP バージョン 2 装置からのメッセージを受信した場合、この装置は、VLAN データベースをスケールダウンし、その特定のトランク上で VTP バージョン 2 フォーマットを使用して送信します。VTP バージョン 3 装置は、最初にそのトランク ポートで VTP バージョン 2 パケットを受信しない限り、VTP バージョン 2 フォーマットのパケットを送信しません。
- VTP バージョン 3 装置が、あるトランク ポートで VTP バージョン 2 装置を検出した場合、両方のネイバーが同一トランク上で共存できるように、VTP バージョン 2 パケットだけでなく VTP バージョン 3 パケットの送信も継続します。
- VTP バージョン 3 装置は、VTP バージョン 2 またはバージョン 1 の装置からの設定情報は受け入れません。
- 2 つの VTP バージョン 3 リージョンは、VTP バージョン 1 リージョンまたはバージョン 2 リージョンでは、トランスペアレント モードでだけ通信できます。
- VTP バージョン 1 にだけ対応する装置は、VTP バージョン 3 装置との相互運用はできません。
- デフォルトで VTP バージョン 2 およびバージョン 3 はディセーブルになっています。
- あるスイッチ上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内の VTP バージョン 2 に対応可能なすべてのスイッチでバージョン 2 がイネーブルになります。VTP バージョン 3 をイネーブルにするには、各スイッチ上で手動によって設定する必要があります。
- VTP バージョン 1 および 2 では、VTP サーバ モードまたはトランスペアレント モードのスイッチでだけバージョンを設定できます。VTP バージョン 3 を実行するスイッチがクライアント モードの場合、既存の拡張 VLAN や既存のプライベート VLAN がなく、パスワードが非表示に設定されていないときであれば、バージョン 2 に変更できます。

注意　VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのインスタンスに存在できます。

VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能なネットワーク帯域幅が増えます。VTP プルーニングを使用しない場合、スイッチは受信側のスイッチで廃棄される可能性があっても、VTP ドメイン内のすべてのトランク リンクに、ブロードキャスト、マルチキャスト、および不明のユニキャスト トラフィックをフラッディングします。VTP プルーニングはデフォルトでディセーブルです。

VTP プルーニングは、プルーニング適格リストに指定された VLAN トランク ポートへの不要なフラッディング トラフィックを阻止します。プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、スイッチのトランク ポート上で VLAN 2 ～ 1001 がプルーニング適格です。プルーニング不適格として設定した VLAN については、引き続きフラッディングが行われます。VTP プルーニングはすべてのバージョンの VTP でサポートされます。

図 18-1 に、VTP プルーニングを使用しない場合のスイッチド ネットワークを示します。スイッチ A のポート 1 およびスイッチ D のポート 2 は、Red という VLAN に割り当てられています。スイッチ A に接続されたホストからブロードキャストが送信された場合、スイッチ A は、このブロードキャストをフラッディングします。Red VLAN にポートを持たないスイッチ C、E、F も含めて、ネットワーク内のすべてのスイッチがこのブロードキャストを受信します。

図 18-1　VTP プルーニングを使用しない場合のフラッディング トラフィック

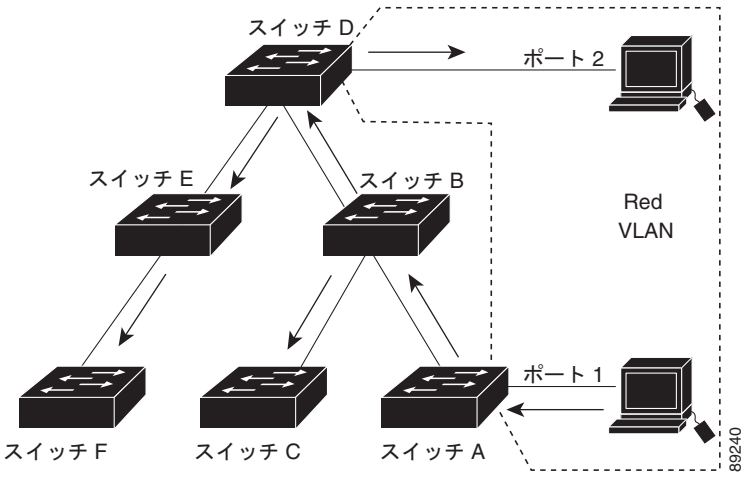
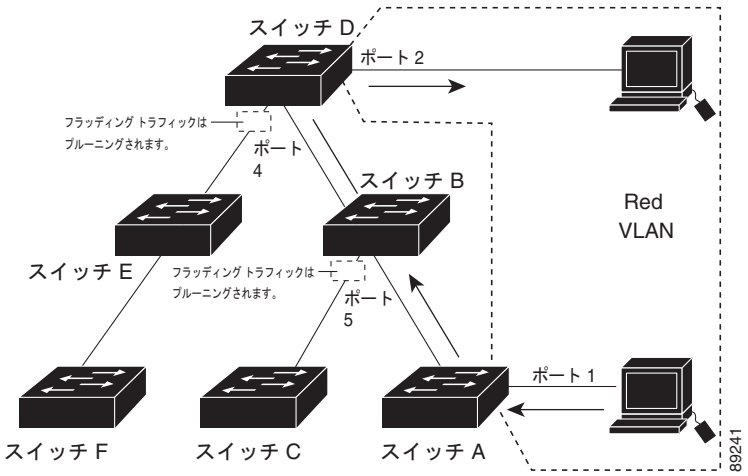


図 18-2 に、VTP プルーニングをイネーブルに設定したスイッチド ネットワークを示します。スイッチ A からのブロードキャスト トラフィックは、スイッチ C、E、F には転送されません。図に示されているリンク ポート（スイッチ B のポート 5、およびスイッチ D のポート 4）で、Red VLAN のトラフィックがプルーニングされるからです。

図 18-2　VTP プルーニングによるフラッディング トラフィックの最適化



VTP バージョン 1 および 2 では、VTP サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体でプルーニングがイネーブルになります。VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのトランク上の VLAN のプルーニングだけです（VTP ドメイン内のすべてのスイッチに影響するわけではありません）。VTP バージョン 3 では、ドメイン内の各スイッチ上で手動によってプルーニングをイネーブルにする必要があります。

「VTP プルーニングのイネーブル化」（P.18-13）を参照してください。VTP プルーニングは、イネーブルにしてから数秒後に有効になります。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 および VLAN 1002 ～ 1005 は常にプルーニング不適格です。これらの VLAN からのトラフィックはプルーニングできません。拡張範囲 VLAN（1005 を超える VLAN ID）もプルーニング不適格です。

VTP プルーニングは VTP トランスペアレント モードでは機能しないように設計されています。ネットワーク内に VTP トランスペアレント モードのスイッチが 1 台または複数存在する場合は、次のいずれかを実行する必要があります。

- ネットワーク全体の VTP プルーニングをオフにします。
- VTP トランスペアレント スイッチのアップストリーム側にあるスイッチのトランク上で、すべての VLAN をプルーニング不適格にすることによって、VTP プルーニングをオフにします。

インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します。VTP プルーニングは、インターフェイスがトランキングを実行している場合に作用します。VLAN プルーニングの適格性は、VTP ドメインで VTP プルーニングがイネーブルであるかどうか、特定の VLAN が存在するかどうか、およびインターフェイスが現在トランキングを実行しているかどうかにかかわらず、設定できます。

VTP のデフォルト設定

表 18-2　VTP のデフォルト設定

機能	デフォルト設定
VTP ドメイン名	ヌル
VTP モード（VTP バージョン 1 およびバージョン 2）	サーバ

表 18-2　VTP のデフォルト設定 （続き）

機能	デフォルト設定
VTP モード（VTP バージョン 3）	このモードは、VTP バージョン 3 に変換する前のバージョン 1 または 2 のモードと同じです。
VTP バージョン	バージョン 1
MST データベース モード	トランスペアレント
VTP バージョン 3 のサーバ タイプ	セカンダリ
VTP パスワード	なし。
VTP プルーニング	ディセーブル

VTP 設定時の注意事項

VTP パスワード、バージョン、VTP ファイル名、最新の VTP 情報を提供するインターフェイス、ドメイン名、およびモードを設定する場合、さらにプルーニングをディセーブルまたはイネーブルに設定する場合には、**vtp** グローバル コンフィギュレーション コマンドを使用します。使用できるキーワードの詳細については、このリリースに対応するコマンド リファレンスに記載されているコマンドの説明を参照してください。VTP 情報は VTP VLAN データベースに保存されます。VTP モードがトランスペアレントである場合、VTP ドメイン名およびモードはスイッチの実行コンフィギュレーション ファイルにも保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。スイッチをリセットした場合、VTP モードをトランスペアレントとして保存するには、このコマンドを使用する必要があります。

スイッチのスタートアップ コンフィギュレーション ファイルに VTP 情報を保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）ます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 個の VLAN のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

ドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。また、VTP ドメイン内のすべてのスイッチを、同じドメイン名で設定しなければなりません。VTP トランスペアレント モードのスイッチは、他のスイッチと VTP メッセージを交換しません。これらのスイッチについては VTP ドメイン名を設定する必要はありません。

（注）　NVRAM および DRAM の記憶域が十分にある場合は、VTP ドメイン内のすべてのスイッチを VTP サーバ モードにする必要があります。

注意　すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメインを設定しないでください。ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の少なくとも 1 台のスイッチを VTP サーバ モードに設定してください。

パスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。ドメイン パスワードを設定する場合は、すべてのドメイン スイッチで同じパスワードを共有し、管理ドメイン内のスイッチごとにパスワードを設定する必要があります。パスワードのないスイッチ、またはパスワードが不正なスイッチは、VTP アドバタイズを拒否します。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したスイッチは、正しいパスワードを使用して設定しない限り、VTP アドバタイズを受信しません。設定後、スイッチは同じパスワードおよびドメイン名を使用した VTP アドバタイズを受信します。

VTP 機能を持つ既存のネットワークに新しいスイッチを追加した場合、その新しいスイッチに適切なパスワードを設定して初めて、スイッチはドメイン名を学習します。

注意　VTP ドメイン パスワードを設定したにもかかわらず、ドメイン内の各スイッチに管理ドメイン パスワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

VTP ドメインへの VTP クライアント スイッチの追加

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP バージョン 3 では、VLAN 情報が消去されることはありません。

VTP の設定方法

VTP ドメインとパラメータの設定

はじめる前に

他の VTP パラメータを設定する前に、VTP ドメインを設定する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp domain** *domain-name*	VTP 管理ドメイン名を設定します。1 ～ 32 文字の名前を使用できます。同一管理下にある VTP サーバ モードまたはクライアント モードのスイッチは、すべて同じドメイン名に設定する必要があります。 サーバ モード以外にはこのコマンドは任意です。VTP サーバ モードではドメイン名が必要です。スイッチで VTP ドメインにトランクを接続している場合、スイッチはドメインの VTP サーバからドメイン名を学習します。
ステップ 3	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}	VTP モード（クライアント、サーバ、トランスペアレントまたはオフ）のスイッチの設定。 任意のデータベース パラメータ： • **vlan**：何も設定されていない場合は VLAN データベースがデフォルトです。 • **mst**：マルチ スパニングツリー（MST）データベース。 • **unknown**：データベース タイプは不明。
ステップ 4	**vtp password** *password*	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。VTP パスワードを設定したにもかかわらず、ドメイン内の各スイッチに同じパスワードを割り当てなかった場合には、VTP ドメインが正常に動作しません。 VTP バージョン 3 で使用可能なオプションについては、「VTP バージョン 3 のパスワードの設定」（P.18-13）を参照してください。
ステップ 5	**vtp primary-server** [**vlan** | **mst**] [**force**]	（任意）スイッチの動作ステートをセカンダリ サーバ（デフォルト）からプライマリ サーバに変更し、その設定をドメインにアドバタイズします。スイッチのパスワードが **hidden** に設定されている場合は、パスワードの再入力を要求されます。 • **vlan**：テイク オーバー機能として VLAN データベースを選択します。これはデフォルトです。 • **mst**：テイク オーバー機能としてマルチ スパニングツリー（MST）データベースを選択します。 • **force**：競合するサーバの設定が上書きされます。**force** を入力しない場合、テイクオーバーの実行前に確認を求められます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show vtp status**	表示された *VTP Operating Mode* および *VTP Domain Name* フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）スタートアップ コンフィギュレーション ファイルに設定を保存します。 **（注）** スイッチの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

VTP バージョン 3 のパスワードの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp password** *password* [**hidden** | **secret**]	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。 • （任意）**hidden**：パスワード文字列から生成された秘密キーが nvam:vlan.dat ファイルに保存されます。VTP プライマリ サーバを設定してテイクオーバーを設定しようとすると、パスワードの再入力を要求されます。 • （任意）**secret**：パスワードを直接設定します。シークレット パスワードには 16 進数文字を 32 個含める必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vtp password**	入力を確認します。

VTP バージョンのイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp version** {**1** | **2** | **3**}	スイッチで VTP バージョンをイネーブルにします。デフォルトは VTP バージョン 1 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vtp status**	設定された VTP バージョンがイネーブルであることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）スタートアップ コンフィギュレーション ファイルに設定を保存します。

VTP プルーニングのイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp pruning**	VTP 管理ドメインでプルーニングをイネーブルにします。 プルーニングは、デフォルトではディセーブルに設定されています。VTP サーバ モードの 1 台のスイッチ上に限ってプルーニングをイネーブルにする必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vtp status**	表示された *VTP Pruning Mode* フィールドの設定を確認します。

ポート単位の VTP の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**vtp**	指定したポートの VTP をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config interface** *interface-id*	ポートの変更を確認します。
ステップ 6	**show vtp status**	設定を確認します。

VTP ドメインへの VTP クライアント スイッチの追加

はじめる前に

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より *小さい*ことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP バージョン 3 では、VLAN 情報が消去されることはありません。

	コマンド	目的
ステップ 1	**show vtp status**	VTP コンフィギュレーション リビジョン番号をチェックします。 番号が 0 の場合は、スイッチを VTP ドメインに追加します。 番号が 0 より大きい場合は、次の手順に従います。 **a.** ドメイン名を書き留めます。 **b.** コンフィギュレーション リビジョン番号を書き留めます。 **c.** 次のステップに進んで、スイッチのコンフィギュレーション リビジョン番号をリセットします。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain** *domain-name*	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。
ステップ 4	**end**	スイッチの VLAN 情報を更新し、コンフィギュレーション リビジョン番号が 0 にリセットされます。
ステップ 5	**show vtp status**	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認します。
ステップ 6	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**vtp domain** *domain-name*	スイッチの元のドメイン名を入力します。
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**show vtp status**	（任意）ドメイン名がステップ 1 のものと同じであり、コンフィギュレーション リビジョン番号が 0 であることを確認します。
ステップ 10	コンフィギュレーション リビジョン番号をリセットした後に、スイッチを VTP ドメインに追加します。	

VTP のモニタリングおよびメンテナンス

コマンド	目的
show vtp counters	送受信された VTP メッセージに関するカウンタを表示します。
show vtp devices [**conflict**]	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。プライマリ サーバと競合する VTP バージョン 3 の装置が表示されます。**show vtp devices** コマンドは、スイッチがトランスペアレント モードまたはオフ モードのときは情報を表示しません。
show vtp interface [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
show vtp password	VTP パスワードを表示します。表示されるパスワードの形式は、**hidden** キーワードが入力されているか、または、暗号化がスイッチでイネーブル化されているかどうかによって異なります。
show vtp status	VTP スイッチの設定情報を表示します。

VTP の設定例

VTP サーバの設定：例

次に、ドメイン名が *eng_group*、パスワードが *mypassword* という VTP サーバとしてスイッチを設定する例を示します。

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end
```

VTP パスワード非表示の設定：例

次に、非表示のパスワードの設定方法とその表示方法の例を示します。

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

VTP バージョン 3 のプライマリ サーバの設定：例

次に、パスワードが非表示またはシークレットに設定されている場合に、VLAN データベースのプライマリ サーバ（デフォルト）としてスイッチを設定する方法の例を示します。

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- --------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

VTP の設定に関する追加情報

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
VLAN コンフィギュレーション	「VLAN の設定」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 19

音声 VLAN の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

音声 VLAN の設定に関する情報

音声 VLAN

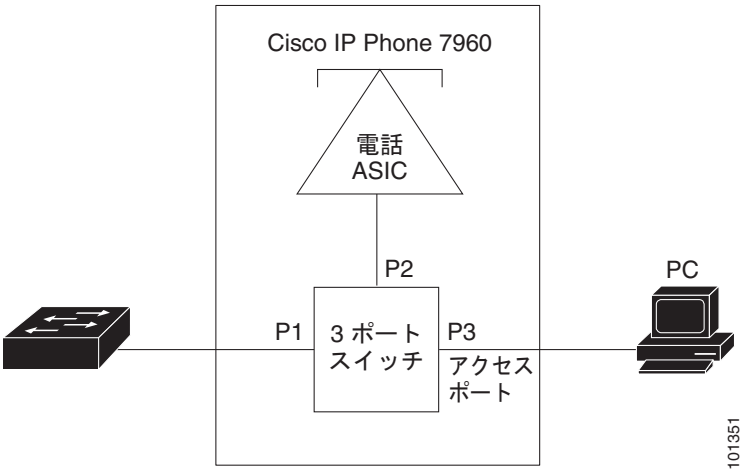
音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。スイッチを Cisco 7960 IP Phone に接続すると、IP Phone はレイヤ 3 IP precedence およびレイヤ 2 サービス クラス（CoS）値を使用して、音声トラフィックを送信します。どちらの値もデフォルトでは 5 に設定されます。データ送信が均質性に欠ける場合、Cisco IP Phone の音質が低下することがあります。そのため、このスイッチでは、IEEE 802.1p CoS に基づく Quality of Service（QoS）をサポートしています。QoS は、分類およびスケジューリングを使用して、スイッチからのネットワーク トラフィックを予測可能な方法で送信します。Catalyst 6500 ファミリ スイッチの一部のマニュアルでは、音声 VLAN を *補助 VLAN* と表しています。

Cisco7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィック プライオリティを信頼するように、または上書きするようにスイッチを設定できます。

Cisco IP Phone には、3 ポートの 10/100 スイッチが統合されています。図 19-1 を参照してください。これらのポートは、次のデバイスへの接続専用です。

- ポート 1 は、スイッチまたは他の Voice over IP（VoIP）デバイスに接続します。
- ポート 2 は、IP Phone のトラフィックを伝送する内部 10/100 インターフェイスです。
- ポート 3（アクセス ポート）は、PC または他のデバイスに接続します。

図 19-1　スイッチに接続された Cisco7960 IP Phone



Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。スイッチ上のアクセス ポートを設定して、Cisco Discovery Protocol（CDP）パケットを送信させることができます。CDP には、接続する IP Phone に対して、次のいずれかの方法でスイッチに音声トラフィックを送信するように指定します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし（レイヤ 2 CoS プライオリティ値なし）のアクセス VLAN による送信

（注）　いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（音声トラフィックはデフォルトで 5、音声制御トラフィックは 3）を伝送します。

Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。IEEE 802.1p のプライオリティ タグを使用すると、音声トラフィックにさらに高いプライオリティを与え、すべての音声トラフィックをネイティブ（アクセス）VLAN 経由で転送できます。Cisco IP Phone はタグなしの音声トラフィックを送信する、または独自の設定を使用してアクセス VLAN で音声トラフィックを送信することもできます。いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（デフォルトは 5）を伝送します。

Cisco IP Phone のデータ トラフィック

スイッチは、Cisco IP Phone のアクセス ポートに接続されたデバイス（図 19-1 を参照）から送られた、タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム タイプのトラフィック）を処理することもできます。スイッチ上のレイヤ 2 アクセス ポートが、CDP パケットを送信するように設定できます。CDP は、接続する IP Phone に、次のいずれかのモードで IP Phone 上のアクセス ポートを設定するように指定します。

- trusted（信頼性がある）モードでは、Cisco IP Phone のアクセス ポート経由で受信したすべてのトラフィックがそのまま IP Phone を通過します。
- untrusted（信頼性がない）モードでは、Cisco IP Phone のアクセス ポート経由で受信した IEEE 802.1Q および IEEE 802.1p フレームのすべてのトラフィックに、設定されたレイヤ 2 CoS 値を与えます。デフォルトのレイヤ 2 CoS 値は 0 です。信頼できないモードがデフォルト設定です。

（注）　Cisco IP Phone に接続されたデバイスからのタグなしトラフィックは、IP Phone のアクセス ポートの信頼状態に関係なく、そのまま IP Phone を通過します。

音声 VLAN のデフォルト設定

音声 VLAN 機能は、デフォルトではディセーブルに設定されています。

音声 VLAN 機能がイネーブルの場合、すべてのタグなしトラフィックはポートのデフォルトの CoS プライオリティに従って送信されます。

IEEE 802.1p または IEEE 802.1Q のタグ付きトラフィックでは、CoS 値が信頼されません。

音声 VLAN 設定時の注意事項

- 音声 VLAN 設定はスイッチのアクセス ポートだけでサポートされており、トランク ポートではサポートされていません。

（注）　トランク ポートは、標準 VLAN と同様に、任意の数の音声 VLAN を伝送できます。音声 VLAN の設定は、トランク ポートでは不要です。

- IP Phone での通信が適切に行えるように、音声 VLAN はスイッチ上でアクティブになっている必要があります。VLAN が存在しているかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します（リストで表示されます）。VLAN がリストになかった場合、音声 VLAN の作成方法について、第 17 章「VLAN の設定」を参照してください。
- 音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチ上で QoS をイネーブルに設定し、さらに **mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力してポートの信頼状態を trust に設定しておくことを推奨します。Auto-QoS 機能を使用すると、これらは自動的に設定されます。詳細については、第 38 章「標準 QoS の設定」を参照してください。
- IP Phone にコンフィギュレーションを送信するために、Cisco IP Phone に接続するスイッチ ポート上で CDP をイネーブルにする必要があります。（デフォルト設定では、CDP がすべてのスイッチ インターフェイスでグローバルにイネーブルです）。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上にあります。
  - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
  - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
  - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
  - Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。
- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上でルーティングされないからです（ルーティングによってフレーム タイプの相違が排除されます）。
- 音声 VLAN には、スタティック セキュア MAC アドレスを設定できません。
- 音声 VLAN ポートには次のポート タイプがあります。
  - ダイナミック アクセス ポート。詳細については、「VMPS クライアント上のダイナミックアクセス ポートの設定」（P.17-23）を参照してください。
  - IEEE 802.1x 認証ポート。詳細については、「802.1x 準備状態チェックの設定」（P.13-36）を参照してください。

    （注）　音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x をイネーブルにした場合、その IP Phone のスイッチへの接続が最大 30 秒間失われます。

  - 保護ポート。詳細については、「保護ポートの設定」（P.29-11）を参照してください。
  - SPAN または RSPAN セッションの送信元ポートまたは宛先ポート。
  - セキュア ポート。詳細については、「ポート セキュリティの設定」（P.29-12）を参照してください。

    （注）　音声 VLAN も設定しているインターフェイス上でポート セキュリティをイネーブルにする場合、ポートで許容されるセキュア アドレスの最大数を、アクセス VLAN におけるセキュア アドレスの最大数に 2 を足した数に設定する必要があります。ポートを Cisco IP Phone に接続している場合、IP Phone に最大で 2 つの MAC アドレスが必要になります。IP Phone のアドレスは、音声 VLAN で学習され、アクセス VLAN でも学習される場合があります。PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

Cisco 7960 IP Phone ポートへの接続

Cisco7960 IP Phone は、PC または他のデバイスとの接続もサポートしているので、スイッチを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。ポートを設定することによって、Cisco IP Phone による音声トラフィックおよびデータ トラフィックの伝送方法を決定できます。

着信データ フレームのプライオリティ

PC またはその他のデータ デバイスを Cisco IP Phone ポートに接続できます。タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム）を処理するために、スイッチが CDP パケットを送信するように設定できます。CDP は、Cisco IP Phone に、IP Phone 上のアクセス ポートに接続されたデバイスからのデータ パケットをどのように送信するかを指定します。PC は、CoS 値が割り当てられたパケットを生成できます。接続デバイスから IP Phone のポートに届いたフレームのプライオリティを変更しない（信頼する）または変更する（信頼しない）ように、IP Phone を設定できます。

VTP の設定方法

Cisco IP Phone の音声トラフィックの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**mls qos trust cos**	パケットの CoS 値を使用して着信するトラフィック パケットを分類するように、インターフェイスを設定します。タグなしパケットの場合、ポートのデフォルト CoS 値が使用されます。 **（注）** ポートの信頼状態を設定する前に、**mls qos** グローバル コンフィギュレーション コマンドを使用することによって、QoS をグローバルでイネーブルに設定しておく必要があります。
ステップ 4	**switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}}	Cisco IP Phone による音声トラフィックの伝送方法を設定します。 • *vlan-id* : すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。指定できる VLAN ID の範囲は 1 ～ 4096 です。 • **dot1p** : 音声トラフィック用に IEEE 802.1p プライオリティ タギングを使用し、デフォルトのネイティブ VLAN（VLAN 0）を使用してすべてのトラフィックを搬送するように、Cisco IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。 • **none** : IP Phone が独自の設定を使用してタグなしの音声トラフィックを送信するようにします。 • **untagged** : タグなしの音声トラフィックを送信するように IP Phone を設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

着信データ フレームのプライオリティ設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport priority extend** {**cos** *value* | **trust**}	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを設定します。 • **cos** *value* : PC または接続しているデバイスから受信したプライオリティを指定の CoS 値に変更するように、IP Phone を設定します。値は 0 ～ 7 です。7 が最高のプライオリティです。デフォルトのプライオリティは **cos** 0 です。 • **trust** : PC または接続しているデバイスから受信したプライオリティを信頼するように IP Phone のアクセス ポートを設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

音声 VLAN のモニタリングとメンテナンス

コマンド	目的
show interfaces *interface-id* **switchport**	入力を確認します。
copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

音声 VLAN の設定例

Cisco IP Phone の音声トラフィックの設定：例

次に、Cisco IP Phone に接続されたポートが、CoS 値を使用して着信トラフィックを分類し、音声トラフィックに IEEE 802.1p プライオリティ タギングを使用し、デフォルトのネイティブ VLAN（VLAN0）を使用してすべてのトラフィックを搬送するように設定する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

Cisco IP Phone の着信データ フレームのプライオリティ設定：例

次に、Cisco IP Phone に接続しているポートを設定して、PC または接続しているデバイスから受信するフレームのプライオリティを変更しないようにする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport priority extend trust
Switch(config-if)# end
```

音声 VLAN の設定に関する追加情報

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
QoS の設定	*第 38 章「標準 QoS の設定」*
VLAN コンフィギュレーション	*第 17 章「VLAN の設定」*
ダイナミック アクセス ポートの設定	「VMPS クライアント上のダイナミックアクセス ポートの設定」（P.17-23）
IEEE 802.1x 認証ポートの設定	「802.1x 準備状態チェックの設定」（P.13-36）
保護ポートの設定	「保護ポートの設定」（P.29-11）
セキュア ポートの設定	「ポート セキュリティの設定」（P.29-12）

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 20

STP の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

STP の設定の前提条件

VTP を設定する場合は、スイッチがドメイン内の他のスイッチと VTP アドバタイズメントを送受信できるように、トランク ポートを設定する必要があります。

詳細については、「トランク ポートとしてのイーサネット インターフェイスの設定」（P.17-19）を参照してください。

STP の設定に関する制約事項

- クラスタ メンバ スイッチの VTP を VLAN に設定する場合、**rcommand** 特権 EXEC コマンドを使用して、そのメンバ スイッチにログインします。
- VTP バージョン 1 および 2 では、そのスイッチで拡張範囲 VLAN を設定するとき、スイッチは VTP トランスペアレント モードでなければなりません。VTP バージョン 3 でも、クライアント モードまたはサーバ モードでの拡張範囲 VLAN の作成をサポートしています。

STP の設定に関する情報

この章では、スイッチのポートベースの VLAN にスパニングツリー プロトコル（STP）を設定する方法について説明します。このスイッチは、IEEE 802.1D 標準に準拠した Per-VLAN Spanning-Tree plus（PVST+）とシスコ独自の拡張機能の組み合わせか、もしくは IEEE 802.1w 標準に準拠した Rapid Per-VLAN Spanning-Tree plus（Rapid PVST+）プロトコルのいずれかを使用できます。

STP

STP は、ネットワーク上でループを防止しながら、パスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正常に動作するには、任意の 2 つのステーション間で存在できるアクティブ パスは 1 つだけです。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンド ステーションにメッセージが重複して到着する可能性があります。また、スイッチも複数のレイヤ 2 インターフェイスのエンド ステーション MAC アドレスを学習する可能性が出てきます。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンド ステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STP は、スパニングツリー アルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。スパニングツリー アルゴリズムは、アクティブ トポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッチはルート スイッチです。少なくとも *1* つのポートに役割が指定されているスイッチは、指定スイッチを意味します。

冗長データ パスはスパニングツリーによって、強制的にスタンバイ（ブロックされた）ステートにされます。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリー アルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、定期的に Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）と呼ばれるスパニングツリー フレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。BPDU には、送信側スイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

スイッチの 2 つのポートがループの一部になっている場合、スパニングツリー ポート プライオリティとパス コストの設定値によって、どちらのポートをフォワーディング ステートにするか、どちらをブロッキング ステートにするかが制御されます。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。パス コストの値は、メディアの速度を表します。

（注） デフォルトでは、Small Form-Factor Pluggable（SFP）を搭載していないインターフェイスにだけ、スイッチがキープアライブ メッセージを（接続が有効か確認するために）送信します。**[no] keepalive** インターフェイス コンフィギュレーション コマンドを使用してインターフェイスのデフォルトを変更することができます。

スパニングツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパニングツリー トポロジは、次の要素によって制御されます。

- 各スイッチのそれぞれの VLAN に対応付けられた一意のブリッジ ID（スイッチ プライオリティおよび MAC アドレス）。
- ルート スイッチに対するスパニングツリー パス コスト。
- 各レイヤ 2 インターフェイスに対応付けられたポート ID（ポート プライオリティおよび MAC アドレス）。

ネットワーク内のスイッチに電源が投入されると、それぞれがルート スイッチとして機能します。各スイッチは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパニングツリー トポロジが計算されます。各コンフィギュレーション BPDU には、次の情報が含まれます。

- 送信側スイッチがルート スイッチと見なしたスイッチの固有ブリッジ ID
- ルートに対するスパニングツリー パス コスト
- 送信側スイッチのブリッジ ID
- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および最大エージングプロトコル タイマーの値

スイッチは、*優位の*情報（より小さいブリッジ ID、より低いパス コストなど）を格納したコンフィギュレーション BPDU を受信すると、そのポートのためにこの情報を保存します。スイッチは、この BPDU をルート ポートで受信した場合は、更新されたメッセージ付きで、自身が指定スイッチであるすべての接続 LAN に対して BPDU を転送します。

そのポートに対して現在保存されているものより *下位*の情報を格納したコンフィギュレーション BPDU を受信した場合は、BPDU は廃棄されます。スイッチが、下位 BPDU の送信元の LAN の指定スイッチである場合は、そのポート用に保存された最新情報を格納した BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の 1 台のスイッチがルート スイッチ（スイッチド ネットワークのスパニングツリー トポロジの論理的な中心）として選択されます。

  各 VLAN で、スイッチのプライオリティが最も高い（プライオリティ値が数値的に最も小さい）スイッチがルート スイッチとして選定されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合は、VLAN 内で最小の MAC アドレスを持つスイッチがルート スイッチになります。スイッチのプライオリティ値は、ブリッジ ID の最上位ビットを占めます（表 20-1（P.20-4）を参照）。
- 各スイッチ（ルート スイッチを除く）に対して 1 つのルート ポートが選択されます。このポートは、スイッチによってパケットがルート スイッチに転送されるときに、最適なパス（最小コスト）を提供します。
- スイッチごとに、パス コストに基づいてルート スイッチまでの最短距離が計算されます。
- 各 LAN セグメントの指定スイッチが選定されます。指定スイッチでは、LAN からルート スイッチへのパケット転送の場合、パス コストが最小となります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。

スイッチド ネットワーク上のすべての地点からルート スイッチに到達する場合に必要のないパスはすべて、スパニングツリー ブロッキング モードになります。

ブリッジ ID、スイッチ プライオリティ、および拡張システム ID

IEEE 802.1D 規格では、各スイッチに一意のブリッジ識別子（ブリッジ ID）を設定する必要があります。この ID によってルート スイッチの選択が制御されます。各 VLAN は PVST+ と Rapid PVST+ によって異なる*論理ブリッジ*と見なされるので、同一のスイッチは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。スイッチ上の各 VLAN には一意の 8 バイト ブリッジ ID が設定されます。上位の 2 バイトはスイッチ プライオリティに使用され、残りの 6 バイトがスイッチの MAC アドレスから取得されます。

スイッチでは IEEE 802.1t スパニングツリー拡張機能がサポートされ、従来はスイッチ プライオリティに使用されていたビットの一部が VLAN ID として使用されるようになりました。その結果、スイッチに割り当てられる MAC アドレスが少なくなり、より広い範囲の VLAN ID をサポートできるようになり、しかもブリッジ ID の一意性を損なうこともありません。表 20-1 に示すように、従来はスイッチ プライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張システム ID 値（VLAN ID と同じ）に割り当てられています。

表 20-1　スイッチ プライオリティ値および拡張システム ID

スイッチ プライオリティ値				拡張システム ID（VLAN ID と同設定）											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニングツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用します。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティの手動での設定方法に影響が生じます。たとえば、スイッチのプライオリティ値を変更すると、ルート スイッチとして選定される可能性も変更されることになります。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。詳細については、「ルート スイッチの設定」（P.20-16）、「セカンダリ ルート スイッチの設定」（P.20-16）、および「STP オプション パラメータの設定」（P.20-17）を参照してください。

スパニングツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジの変化が発生します。インターフェイスがスパニングツリー トポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インターフェイスは新しいトポロジ情報がスイッチド LAN 上で伝播されるまで待機し、フレーム転送を開始する必要があります。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパニングツリーを使用しているスイッチの各レイヤ 2 インターフェイスは、次のいずれかのステートになります。

- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニングツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。

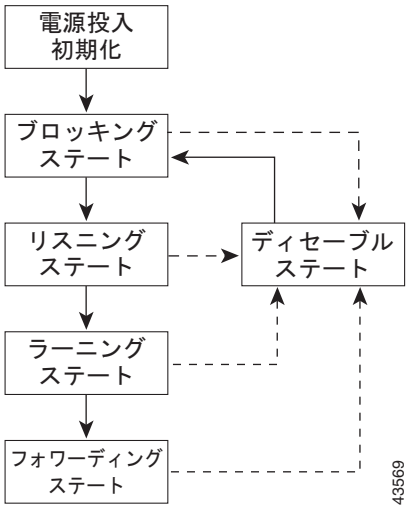
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリー インスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 20-1 に、インターフェイスがステートをどのように移行するかを示します。

図 20-1　スパニングツリー インターフェイス ステート



デフォルト設定では、スイッチを起動するとスパニングツリーがイネーブルになります。その後、スイッチの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニングツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートで、スイッチがデータベース転送のためにエンド ステーションの位置情報を学習している間、インターフェイスはフレーム転送を引き続きブロックします。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスはフレームの転送に関与しません。初期化後、スイッチの各インターフェイスに BPDU が送信されます。スイッチは最初、他のスイッチと BPDU を交換するまで、ルートとして動作します。この BPDU 交換によって、ネットワーク上のどのスイッチがルート、つまりルート スイッチであるかが確立されます。ネットワークにスイッチが 1 台しかない場合は、交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。インターフェイスはスイッチの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ 2 インターフェイスが最初に移行するステートです。インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレームの転送に関与できるように準備します。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。

- BPDU を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ 2 インターフェイスは、フレームの転送やスパニングツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

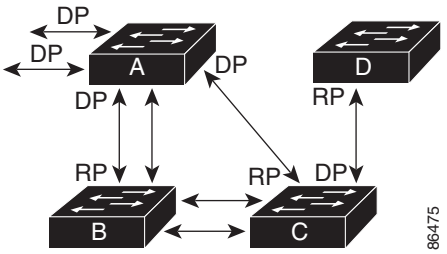
ディセーブル インターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

スイッチまたはポートがルート スイッチまたはルート ポートになる仕組み

ネットワーク上のすべてのスイッチがデフォルトのスパニングツリー設定でイネーブルになっている場合、最小の MAC アドレスを持つスイッチがルート スイッチになります。図 20-2 では、スイッチ A がルート スイッチとして選定されます（すべてのスイッチのスイッチ プライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるため）。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチとは限りません。ルート スイッチになるように、最適なスイッチのプライオリティを引き上げる（数値を引き下げる）と、スパニングツリーの再計算が強制的に行われ、最適なスイッチをルートとした新しいトポロジが形成されます。

図 20-2　　スパニングツリー トポロジ



RP = ルート ポート
DP = 指定ポート

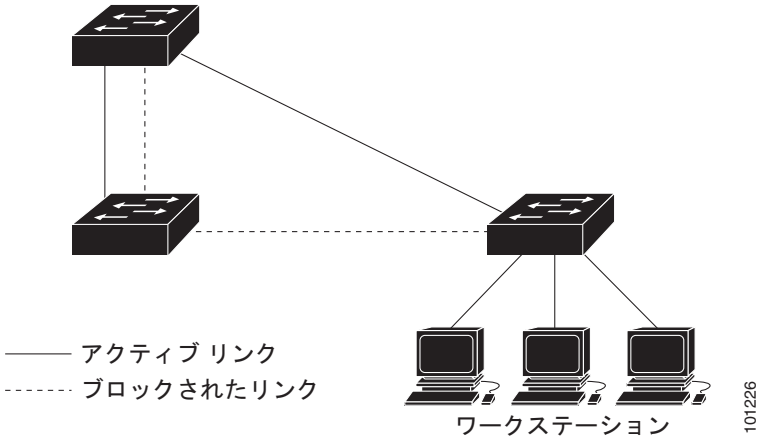
スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチド ネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルート ポートが変更される可能性があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B のあるポートがギガビット イーサネット リンクで、別のポート（10/100 リンク）がルート ポートであると仮定します。ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

スパニングツリーおよび冗長接続

2 つのスイッチ インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます（図 20-3 を参照）。スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート プライオリティとポート ID が加算され、値の小さいリンクがスパニングツリーによってディセーブルにされます。

図 20-3　スパニングツリーおよび冗長接続



EtherChannel グループを使用して、スイッチ間に冗長リンクを設定することもできます。詳細については、第 40 章「EtherChannel の設定」を参照してください。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ～ 0x0180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、各スイッチは 0x0180C2000000 ～ 0x0180C200000F のアドレス宛のパケットを受信しますが、転送は行いません。

スパニングツリーがイネーブルな場合、スイッチの CPU は 0x0180C2000000 および 0x0180C2000010 宛のパケットを受信します。スパニングツリーがディセーブルな場合は、スイッチは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、**mac address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルト値です。ただし、スパニングツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5 分以上にわたって到達できないことがあるので、アドレス テーブルからステーション アドレスを削除し、改めて学習できるように、アドレス エージング タイムが短縮されます。スパニングツリー再構成時に短縮されるエージング タイムは、転送遅延パラメータ値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN はそれぞれ独立したスパニングツリー インスタンスなので、スイッチは VLAN 単位でエージング タイムを短縮します。ある VLAN でスパニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、スイッチで設定されたエージング タイムがそのまま適用されます。

スパニングツリー モードおよびプロトコル

このスイッチでサポートされるモードおよびプロトコルは、次のとおりです。

- PVST+：このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。すべてのイーサネット ポートベースの VLAN で使用されるスパニングツリーのデフォルト モードです。PVST+ はスイッチ上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

  PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルート スイッチがあります。このルート スイッチは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのスイッチに伝送します。このプロセスにより、各スイッチがネットワークに関する共通の情報を持つようになるので、ネットワーク トポロジが確実に維持されます。

- Rapid PVST+：このスパニングツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

  Rapid PVST+ は PVST+ と同じ設定を使用しているので（特に明記する場合を除く）、必要なことは最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行するのに、複雑な MSTP 設定の学習やネットワーク再設定の必要がないことです。Rapid PVST+ モードでは、各 VLAN は独自のスパニングツリー インスタンスを最大数実行します。

- MSTP：このスパニングツリー モードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同一のスパニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニングツリー インスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree Protocol（RSTP）（IEEE 802.1w 準拠）上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行することにより、スパニングツリーの高速コンバージェンスを可能にします。RSTP を使用しない場合、MSTP は稼働できません。

  MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの配備です。詳細については、第 21 章「MSTP の設定」を参照してください。

サポートされるスパニングツリー インスタンス数については、次の項を参照してください。

サポートされるスパニングツリー インスタンス

PVST+ または Rapid PVST+ モードでは、スイッチは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、スイッチは最大 65 MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

スパニングツリーと VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）の相互作用については、「スパニングツリー モードの変更」（P.20-15）を参照してください。

スパニングツリーの相互運用性と下位互換性

表 20-2 に、ネットワークでサポートされるスパニングツリー モード間の相互運用性と下位互換性を示します。

表 20-2　PVST+、MSTP、および Rapid PVST+ の相互運用性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり（制限あり）	あり（PVST+ に戻る）
MSTP	あり（制限あり）	あり	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	あり

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree（CST）のルートは MST バックボーンの内側に配置する必要があり、PVST+ スイッチを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ が稼働しているスイッチと PVST+ が稼働しているスイッチが存在する場合、Rapid PVST+ スイッチと PVST+ スイッチを別のスパニングツリー インスタンスにすることを推奨します。Rapid PVST+ スパニングツリー インスタンスでは、ルート スイッチは Rapid PVST+ スイッチでなければなりません。PVST+ インスタンスでは、ルート スイッチは PVST+ スイッチでなければなりません。PVST+ スイッチはネットワークのエッジに配置する必要があります。

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー ストラテジに一定の制限を設けています。この規格では、トランク上で使用できる *すべての* VLAN に対して、1 つのスパニングツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクによって接続された Cisco スイッチのネットワークでは、スイッチはトランク上で使用できる *各* VLAN に 1 つずつ、スパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを使用して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは PVST+ を使用してスパニングツリーの相互運用性を実現します。Rapid PVST+ がイネーブルの場合、スイッチは PVST+ ではなく Rapid PVST+ を使用します。スイッチは、トランクの IEEE 802.1Q VLAN のスパニングツリー インスタンスと他社の IEEE 802.1Q スイッチのスパニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。Cisco スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的にイネーブルになるので、ユーザ側で設定する必要はありません。アクセス ポートでの外部スパニングツリーの動作は、PVST+ の影響を受けません。

VLAN ブリッジ スパニングツリー

シスコ VLAN ブリッジ スパニングツリーは、フォールバック ブリッジング機能（ブリッジ グループ）で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッド ポート間で伝送します。VLAN ブリッジ スパニングツリーにより、ブリッジ グループは個々の VLAN スパニングツリーの上部にスパニングツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。また、ブリッジングされている VLAN からの個々のスパニングツリーが単一のスパニングツリーに縮小しないようにする働きもします。

VLAN ブリッジ スパニングツリーをサポートするには、一部のスパニングツリー タイマーを増やします。

スパニングツリーのデフォルト設定

表 20-3　スパニングツリーのデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
スパニングツリー モード	PVST+ （Rapid PVST+ と MSTP はディセーブル）
スイッチ プライオリティ	32768
スパニングツリー ポート プライオリティ（インターフェイス単位で設定可能）	128
スパニングツリー ポート コスト（インターフェイス単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー VLAN ポート プライオリティ（VLAN 単位で設定可能）	128
スパニングツリー VLAN ポート コスト（VLAN 単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー タイマー	hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒 転送保留カウント：6 BPDU

スパニングツリーのディセーブル化

スパニングツリーはデフォルトで、VLAN 1 および「サポートされるスパニングツリー インスタンス」（P.20-9）のスパニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

注意　スパニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

ルート スイッチ

スイッチは、スイッチ上で設定されているアクティブ VLAN ごとに 1 つずつ、個別のスパニングツリー インスタンスを維持します。各インスタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるブリッジ ID が対応付けられます。VLAN ごとに、ブリッジ ID が最小のスイッチがその VLAN のルート スイッチになります。

特定の VLAN でスイッチがルートになるように設定するには、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値（32768）からかなり小さい値に変更します。このコマンドを入力すると、ソフトウェアが各 VLAN について、ルート スイッチのスイッチ プライオリティをチェックします。拡張システム ID をサポートするため、スイッチは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このスイッチを指定された VLAN のルートに設定できます。

指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です。表 20-1（P.20-4）を参照）。

（注）　ルート スイッチとして設定する必要のある値が 1 未満の場合、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドは失敗します。

（注）　ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼働する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

（注）　各スパニングツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリビューション スイッチにする必要があります。アクセス スイッチをスパニングツリーのプライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ カウント）を指定するには、**diameter** キーワードを指定します。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

（注）　ルート スイッチとして設定した後で、**spanning-tree vlan** *vlan-id* **hello-time**、**spanning-tree vlan** *vlan-id* **forward-time**、および **spanning-tree vlan** *vlan-id* **max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、および最大エージング タイムを手動で設定することは推奨できません。

セカンダリ ルート スイッチ

スイッチをセカンダリ ルートとして設定すると、スイッチ プライオリティがデフォルト値（32768）から 28672 に変更されます。したがって、プライマリ ルート スイッチで障害が発生した場合に、このスイッチが指定された VLAN のルート スイッチになる可能性が高くなります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート スイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。**spanning-tree vlan** *vlan-id* **root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

ポートのプライオリティ

ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

パス コスト

スパニングツリー パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スパニングツリー タイマー

表 20-4　スパニングツリー タイマー

変数	説明
hello タイマー	スイッチから他のスイッチへ hello メッセージをブロードキャストする頻度を制御します。
転送遅延タイマー	インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を制御します。
最大エージング タイマー	インターフェイスが受信したプロトコル情報をスイッチに保存させておく時間を制御します。
転送保留カウント	1 秒間停止する前に送信できる BPDU 数を制御します。

スパニングツリー設定時の注意事項

VTP にスパニングツリー インスタンスよりも多くの VLAN が定義されている場合、PVST+ または Rapid PVST+ をイネーブルにできるのは、スイッチ上の 128 の VLAN に限られます。残りの VLAN は、スパニングツリーがディセーブルの状態で動作します。ただし、MSTP を使用して複数の VLAN を同一のスパニングツリー インスタンスにマッピングすることが可能です。詳細については、第 21 章「MSTP の設定」を参照してください。

128 のスパニングツリー インスタンスがすでに使用されている場合、VLAN の 1 つでスパニングツリーをディセーブルにして、STP を稼働させたい別の VLAN でイネーブルにできます。**no spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して、特定の VLAN でスパニングツリーをディセーブルにし、**spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して、所定の VLAN でスパニングツリーをイネーブルにします。

注意　スパニングツリーが稼働していないスイッチは、スパニングツリー インスタンスが稼働している VLAN 上の他のスイッチがループを切断できるように、受信した BPDU を引き続き転送します。したがって、スパニングツリーは、ネットワーク上のすべてのループを切断できるように十分な数

のスイッチ上で稼働している必要があります。たとえば、VLAN の各ループで少なくとも 1 台のスイッチがスパニングツリーを稼働している必要があります。VLAN 内のすべてのスイッチでスパニングツリーを稼働させる必要はありません。ただし、最小限の数のスイッチだけでスパニングツリーが稼働している状況では、不注意なネットワーク変更によって VLAN に別のループが発生し、ブロードキャスト ストームを引き起こす可能性があります。

（注）　スイッチ上の使用可能なスパニングツリー インスタンスをすべて使い切ってしまった後に、VTP ドメイン内にさらに別の VLAN を追加すると、そのスイッチ上にスパニングツリーが稼働しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リストが設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパニングツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。ただし、ネットワークに VLAN を追加するときより多くの作業を伴うことになるので、通常、許可リストの設定は必要ありません。

VLAN スパニングツリー インスタンスの設定はスパニングツリー コマンドによって制御されます。スパニングツリー インスタンスは、VLAN にインターフェイスを割り当てるときに作成します。スパニングツリー インスタンスは最終インターフェイスが別の VLAN に移されたときに削除されます。スパニングツリー インスタンスの作成前に、スイッチとポートのパラメータを設定できます。設定されたパラメータは、スパニングツリー インスタンスを作成するときに適用されます。

スイッチは、PVST+、Rapid PVST+、および MSTP をサポートしますが、アクティブにできるバージョンは常に 1 つだけです（たとえば、すべての VLAN で PVST+ を使用するか、すべての VLAN で Rapid PVST+ を使用するか、またはすべての VLAN で MSTP を使用することになります）。さまざまなスパニングツリー モードおよび相互運用性については、「スパニングツリーの相互運用性と下位互換性」（P.20-10）を参照してください。

UplinkFast および BackboneFast 設定時の注意事項については、「オプションのスパニングツリー機能の設定に関する情報」（P.22-1）を参照してください。

注意　ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

STP の設定方法

スパニングツリー モードの変更

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}	スパニングツリー モードを設定します。 • **pvst**：PVST+ をイネーブルにします（デフォルト設定）。 • **mst**：MSTP（および RSTP）をイネーブルにします。設定手順の詳細については、第 21 章「MSTP の設定」を参照してください。 • **rapid-pvst**：Rapid PVST+ をイネーブルにします。
ステップ 3	**interface** *interface-id*	（Rapid PVST+ モードの場合のみ推奨）設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。
ステップ 4	**spanning-tree link-type point-to-point**	（Rapid PVST+ モードの場合のみ推奨）このポートのリンク タイプをポイントツーポイントに指定します。 このポート（ローカル ポート）をポイントツーポイント リンクでリモート ポートと接続し、ローカル ポートが指定ポートになると、スイッチはリモート ポートとネゴシエーションし、ローカル ポートをフォワーディング ステートに高速変更します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**clear spanning-tree detected-protocols**	（Rapid PVST+ モードの場合のみ推奨）スイッチ上のすべてのポートが IEEE 802.1D レガシー スイッチ上のポートに接続されている場合、スイッチ全体でプロトコル移行プロセスを再開します。 このステップは、このスイッチで Rapid PVST+ が稼働していることを指定スイッチが検出する場合のオプションです。

ルート スイッチの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定された VLAN のルートになるように、スイッチを設定します。 • *vlan-id*：VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 •（任意）**diameter** *net-diameter*：任意の 2 つのエンド ステーション間のスイッチの最大数を指定します。 •（任意）**hello-time** *seconds*：ルート スイッチがコンフィギュレーション メッセージを生成する間隔を秒数で指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

セカンダリ ルート スイッチの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定された VLAN のセカンダリ ルートになるように、スイッチを設定します。 • *vlan-id*：VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4096 です。 •（任意）**diameter** *net-diameter*：任意の 2 つのエンド ステーション間のスイッチの最大数を指定します。指定できる範囲は 2 ～ 7 です。 •（任意）**hello-time** *seconds*：ルート スイッチがコンフィギュレーション メッセージを生成する間隔を秒数で指定します。指定できる範囲は 1 ～ 10 です。デフォルト値は 2 です。 プライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。「ルート スイッチの設定」（P.20-16）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。

ポート プライオリティの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 3	**spanning-tree port-priority** *priority*	インターフェイスのポート プライオリティを設定します。
ステップ 4	**spanning-tree vlan** *vlan-id* **port-priority** *priority*	VLAN にポート プライオリティを設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

パス コストの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 3	**spanning-tree cost** *cost*	インターフェイスのコストを設定します。
ステップ 4	**spanning-tree vlan** *vlan-id* **cost** *cost*	VLAN にコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

STP オプション パラメータの設定

はじめる前に

STP のプライオリティ、hello タイムを設定する場合は、注意が必要です。

スイッチ プライオリティの変更には、通常は、**spanning-tree vlan** *vlan-id* **root primary** および **spanning-tree vlan** *vlan-id* **root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **priority** *priority*	VLAN のスイッチ プライオリティを設定します。
ステップ 3	**spanning-tree vlan** *vlan-id* **hello-time** *seconds*	VLAN の hello タイムを設定します。

	コマンド	目的
ステップ 4	**spanning-tree vlan** *vlan-id* **max-age** *seconds*	VLAN の最大エージング タイムを設定します。
ステップ 5	**spanning-tree vlan** *vlan-id* **forward-time** *seconds*	VLAN の転送時間を設定します。
ステップ 6	**spanning-tree vlan** *vlan-id* **max-age** *seconds*	VLAN の最大エージング タイムを設定します。
ステップ 7	**spanning-tree transmit hold-count** *value*	1 秒間停止する前に送信できる BPDU 数を設定します。 **（注）** このパラメータをより高い値に変更すると、CPU の使用率が非常に大きくなります（Rapid PVST モード時に特に顕著に変化します）。逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。
ステップ 8	**end**	特権 EXEC モードに戻ります。

STP のモニタリングおよびメンテナンス

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree summary	インターフェイス ステートのサマリーを表示します。
show spanning-tree vlan *vlan-id*	スパニングツリー VLAN エントリを表示します。
copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
VLAN コンフィギュレーション	*第 17 章「VLAN の設定」*
マルチ スパニングツリー プロトコルの設定	*第 21 章「MSTP の設定」*
オプションのスパニングツリー設定	*第 22 章「オプションのスパニングツリー機能の設定」*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 21

MSTP の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MSTP の設定に関する情報

この章では、スイッチにシスコが実装した IEEE 802.1s Multiple STP（MSTP）を設定する方法について説明します。

（注） マルチ スパニングツリー（MST）実装は IEEE 802.1s 標準に準拠しています。

MSTP は複数の VLAN を同一のスパニングツリー インスタンスにマッピングできるようにして、多数の VLAN をサポートする場合に必要となるスパニングツリー インスタンスの数を減らします。MSTP は、データ トラフィック用に複数の転送パスを提供し、ロード バランシングを可能にします。MSTP を使用すると、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）は影響を受けないので、ネットワークのフォールトトレランスが向上します。MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

スイッチが MST モードの場合、IEEE 802.1w 準拠の高速スパニングツリー プロトコル（RSTP）が自動的にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

RSTP と MSTP は、（オリジナル）IEEE 802.1D スパニングツリー準拠デバイス、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存のシスコ Per-VLAN Spanning-Tree plus（PVST+）との下位互換性を保ちながら、スパニングツリーの動作を向上させます。

MSTP

MSTP は、高速コンバージェンスが可能な RSTP を使用し、複数の VLAN を 1 つのスパニングツリー インスタンスにまとめます。各インスタンスのスパニングツリー トポロジは、他のスパニングツリー インスタンスの影響を受けません。このアーキテクチャによって、データ トラフィックに複数の転送パスが提供され、ロード バランシングが可能になり、また多数の VLAN をサポートするのに必要なスパニングツリー インスタンスの数を減らすことができます。

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。同じ MST コンフィギュレーションを持ち、相互接続されたスイッチの集合を MST リージョンといいます（図 21-1（P.21-4）を参照）。

各スイッチがどの MST リージョンに属しているかは、MST コンフィギュレーションによって制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。スイッチにリージョンを設定するには、そのスイッチで **spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用して、MST コンフィギュレーション モードを開始します。このモードでは、**instance** MST コンフィギュレーション コマンドを使用して VLAN を MST インスタンスにマッピングし、**name** MST コンフィギュレーション コマンドを使用してリージョン名を指定し、**revision** MST コンフィギュレーション コマンドを使用してリビジョン番号を設定できます。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。さらに、各メンバは、RSTP ブリッジ プロトコル データ ユニット（BPDU）を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。インスタンスは 0 ～ 4096 の数字で識別されます。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

IST、CIST、CST

すべてのスパニングツリー インスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 種類のスパニングツリーを確立して維持します。

- Internal Spanning-Tree（IST）は、1 つの MST リージョン内で稼働するスパニングツリーです。

  各 MST リージョン内の MSTP は複数のスパニングツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他の MST インスタンスはすべて 1 ～ 4096 まで番号が付けられます。

  IST は、BPDU を送受信する唯一のスパニングツリー インスタンスです。他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリー インスタンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

  同一リージョン内の MST インスタンスはすべて、同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ（ルート スイッチ ID、ルート パス コストなど）を持っています。デフォルトでは、すべての VLAN が IST に割り当てられます。

  MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- Common and Internal Spanning-Tree（CIST）は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニングツリーを相互接続する Common Spanning-Tree（CST）の集合です。

  1 つのリージョン内で計算されたスパニングツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニングツリー アルゴリズムによって形成されます。MST リージョン内の CIST は、リージョン外の CST と同じです。

詳細については、「MST リージョン内の動作」（P.21-3）および「MST リージョン間の動作」（P.21-3）を参照してください。

（注）　IEEE 802.1s 標準を実装すると、一部の MST 実装関連の用語が変更されます。これらの変更の要約については、表 20-1（P.20-4）を参照してください。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは、図 21-1（P.21-4）のように、CIST リージョナル ルート（IEEE 802.1s 標準が実装される以前は *IST マスター*）になります。CIST ルートに対してリージョン内で最も低いスイッチ ID とパス コストを持つスイッチがルートになります。ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MSTP スイッチは初期化時に、自身が CIST のルートおよび CIST リージョナル ルートであることを主張するため、CIST ルートと CIST リージョナル ルートへのパス コストがいずれもゼロに設定された BPDU を送信します。スイッチはさらに MST インスタンスをすべて初期化し、自身がこれらすべてのインスタンスのルートであると主張します。スイッチは、ポートに現在保存されているルート情報よりも優位の MST ルート情報（小さいスイッチ ID、パス コストなど）を受信すると、CIST リージョナル ルートとしての主張を撤回します。

リージョンには、初期化中に多くのサブ リージョンが含まれて、それぞれに独自の CIST リージョナル ルートが含まれることがあります。スイッチは、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真の CIST リージョナル ルートが含まれている新しいサブリージョンに加入します。真の CIST リージョナル ルートが含まれているサブリージョン以外のサブリージョンはすべて縮小させます。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。共通の CIST リージョナル ルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

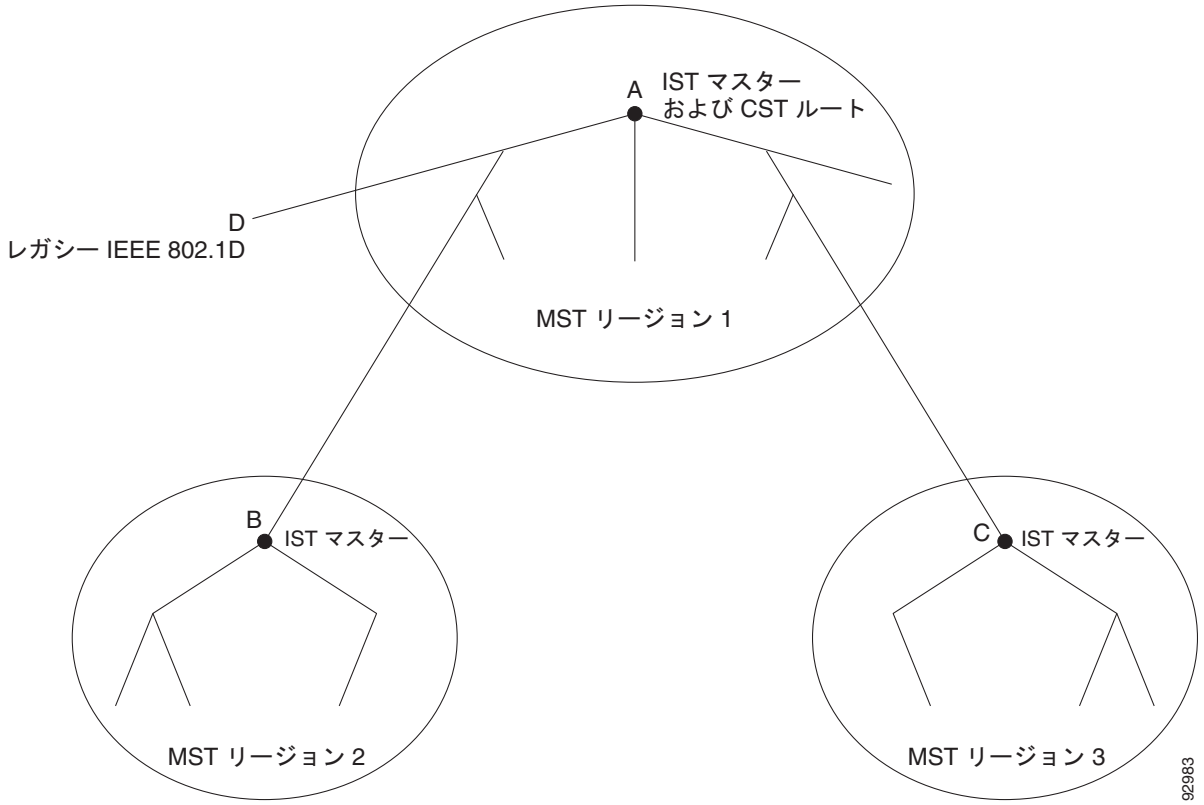
MST リージョン間の動作

ネットワーク内に複数のリージョンまたは IEEE 802.1D 準拠のレガシー スイッチが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP スイッチからなる CST を構築して維持します。MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST は、リージョン内のすべての MSTP スイッチに接続し、スイッチド ドメイン全体を網羅する CIST のサブツリーとして見なされます。サブツリーのルートは CIST リージョナル ルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

図 21-1 は、3 つの MST リージョンと IEEE 802.1D 準拠のレガシー スイッチ（D）からなるネットワークを示しています。リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。リージョン 2 の CIST リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。RSTP はすべてのリージョンで稼働しています。

図 21-1　MST リージョン、CIST マスター、および CST ルート



BPDU を送受信するのは、CST インスタンスだけです。MST インスタンスは自身のスパニングツリー情報を BPDU に追加して、ネイバー スイッチと通信し、最終的なスパニングツリー トポロジを計算します。そのため、BPDU 送信に関連したスパニングツリー パラメータ（たとえば hello タイム、転送時間、最大エージング タイム、最大ホップ数など）は、CST インスタンスのみで設定されますが、すべての MST インスタンスに影響します。スパニングツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、IEEE 802.1D 準拠のレガシー スイッチと通信します。MSTP スイッチ同士の通信には、MSTP BPDU が使用されます。

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の*内部*パラメータまたは*リージョン*パラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体を網羅するスパニングツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート スイッチです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。CIST では、MST リージョンが単一のスイッチのように見えるので注意してください。CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。
- CIST リージョナル ルートは、準規格の実装で IST マスターと呼ばれていました。CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。CIST リージョナル ルートは IST のルート スイッチとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

表 21-1（P.21-5）に、IEEE 規格とシスコ準規格の用語の比較を示します。

表 21-1　準規格と規格の用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

ホップ カウント

IST および MST インスタンスは、スパニングツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。その代わりに、IP Time To Live（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用すると、領域内の最大ホップ数を設定し、IST およびその領域のすべての MSTI に適用できます。ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート スイッチは、常にコストを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。この BPDU を受信したスイッチは、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼働する単一のスパニングツリー リージョン、PVST+ または Rapid PVST+ が稼働する単一のスパニングツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。また、境界ポートは、指定スイッチが単一のスパニングツリー スイッチ、または異なる MST コンフィギュレーションを持つスイッチである LAN に接続されます。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートで受信可能な内部（同一リージョンからの）および外部の 2 種類のメッセージを識別します。メッセージが外部である場合、CIST だけが受信します。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードだけを受信します。シスコ先行標準の実装では、ポートが境界ポートとして外部メッセージを受信します。つまり、ポートは内部メッセージと外部メッセージを混在させたものは受信できません。

MST リージョンには、スイッチと LAN の両方が含まれています。セグメントは、DP のリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。この定義では、リージョン内部の 2 つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。

（注）　レガシー STP スイッチがセグメントに存在する場合、メッセージは常に外部と見なされます。

先行標準の実装から他に変更された点は、送信スイッチ ID を持つ RSTP またはレガシー IEEE 802.1Q スイッチの部分に、CIST リージョナル ルート スイッチ ID フィールドが加えられたことです。一貫した送信スイッチ ID をネイバー スイッチに送信することで、リージョン全体で 1 つの仮想スイッチのように動作します。この例では、スイッチ A または B がそのセグメントで指定されているかどうかにかかわらず、スイッチ C が、ルートの一貫した送信スイッチ ID を持つ BPDU を受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんでしたが、境界の概念自体はシスコの実装に投影されています。ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステートに必ずしも従うわけではありません。現状、次の 2 通りの事例が考えられます。

- 境界ポートが CIST リージョナル ルートのルート ポートである場合：CIST インスタンス ポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。MSTI ポートには、特別なマスターの役割があります。

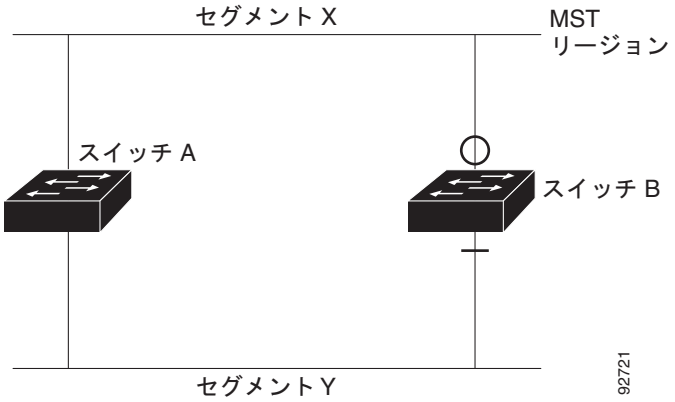
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU（M レコード）を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

レガシー スイッチと標準スイッチの相互運用

先行標準のスイッチでは先行標準のポートを自動検出ができないため、インターフェイス コンフィギュレーション コマンドを使用して認識させます。標準と先行標準の間にあるリージョンは形成できませんが、CIST を使用することで相互運用できます。このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロード バランシングのみです。ポートが先行標準の BPDU を受信すると、CLI（コマンドライン インターフェイス）にはポートの設定に応じて異なるフラグが表示されます。また、スイッチが、先行標準の BPDU 転送の設定がされてないポートで先行標準の BPDU を初めて受信すると、Syslog メッセージにも表示されます。

図 21-2 に、このシナリオを示します。A を標準スイッチ、B を先行標準のスイッチと仮定してください。両方とも同じリージョンに設定されています。A が CIST のルート スイッチのため、B にセグメント X のルート ポート（BX）とセグメント Y の代替ポート（BY）があります。セグメント Y がフラップして、先行標準の単一の BPDU を送信する前に BY のポートが代替ポートになった場合、AY は Y に接続している先行標準のスイッチを検出できないため、標準の BPDU を送信し続けます。ポート BY は境界に固定され、A と B の間でのロードバランスは不可能になります。セグメント X にも同じ問題がありますが、B は TC を送信することがあります。

図 21-2　標準スイッチおよび先行標準のスイッチでの相互運用



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

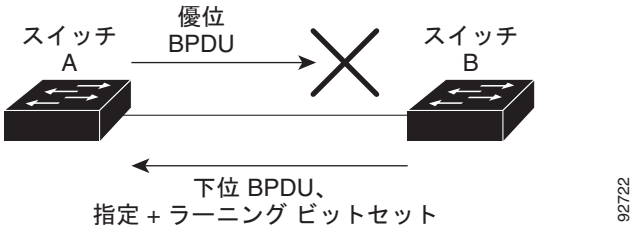
単一方向リンクの失敗の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートで矛盾が検出された場合、役割には従いますが、ブリッジ処理のループを引き起こすよりは、矛盾による接続中断の方が望ましい状態のため、廃棄ステートへ戻ります。

図 21-3 に、一般的にブリッジング ループになる単一方向リンク障害を示します。スイッチ A はルート スイッチです。スイッチ B へ向かうリンク上で、BPDU が紛失しています。RSTP および MST BPDU には、送信側ポートの役割とステートが含まれます。この情報があれば、スイッチ A は、送信した優位 BPDU にスイッチ B が反応しないこと、さらにスイッチ B はルート スイッチではなく指定スイッチであることを検出できます。結果として、スイッチ A は自身のポートをブロックし（またはブロックを維持して）、ブリッジ処理のループを回避します。

図 21-3　　単一方向リンク障害の検出



IEEE 802.1D STP との相互運用性

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、レガシー スイッチが指定スイッチでない場合、レガシー スイッチがリンクから削除されているかどうか検出できないので、スイッチは IEEE 802.1D BPDU を受け取らなくなった場合でも、自動的に MSTP モードには戻りません。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、引き続きポートに境界の役割を指定する可能性があります。プロトコル移行プロセスを再起動する（ネイバー スイッチとの再ネゴシエーションを強制する）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー スイッチが RSTP スイッチであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP スイッチは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境界ポートは、指定スイッチがシングル スパニングツリー スイッチまたは異なる MST コンフィギュレーションを持つスイッチのいずれかである LAN に接続されます。

RSTP

RSTP は、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパニングツリーを再構成できます（IEEE 802.1D スパニングツリーのデフォルトに設定されている 50 秒とは異なります）。

ポートの役割およびアクティブ トポロジー

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。「スパニングツリー トポロジと BPDU」（P.20-3）で説明したように、RSTP は、IEEE 802.1D STP に基づき、スイッチ プライオリティが最も高い（プライオリティの値が最も小さい）スイッチをルート スイッチに選択します。RSTP はさらに、各ポートに次のいずれか 1 つの役割を割り当てます。

- ルート ポート：スイッチからルート スイッチへパケットを転送する場合の最適パス（最も低コストなパス）を提供します。
- 指定ポート：指定スイッチに接続します。これにより、LAN からルート スイッチへパケットを転送するときのパス コストが最小になります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート スイッチへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンクによってループバックで接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合です。
- ディセーブル ポート：スパニングツリーの動作において何も役割が与えられていません。

ルート ポートまたは DP の役割があるポートは、アクティブ トポロジーに組み込まれます。代替ポートまたはバックアップ ポートのロールがあるポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルート ポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート（IEEE 802.1D のブロッキング ステートと同じ）になるように保証します。ポートのステートにより、転送処理および学習処理の動作が制御されます。表 21-2 に、IEEE 802.1D と RSTP のポート ステートの比較を示します。

表 21-2　ポート ステートの比較

動作ステータス	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	廃棄	No
イネーブル	リスニング	廃棄	No
イネーブル	ラーニング	ラーニング	Yes
イネーブル	フォワーディング	フォワーディング	Yes
ディセーブル	ディセーブル	廃棄	No

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを*廃棄*ではなく*ブロッキング*として定義します。DP はリスニング ステートから開始します。

高速コンバージェンス

RSTP を使用すると、スイッチ、スイッチ ポート、または LAN に障害が発生しても、ただちに接続を回復できます。エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジ ポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して、RSTP スイッチ上の 1 つのポートをエッジ ポートに設定すると、そのエッジ ポートはただちにフォワーディング ステートになります。エッジ ポートは Port Fast 対応ポートと同じであり、単一エンド ステーションに接続しているポートだけでイネーブルにする必要があります。
- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクで別のポートにポートを接続し、ローカル ポートが DP になると、提案と合意のハンドシェークを使用して別のポートと高速移行がネゴシエーションされ、ループがないトポロジーが確保されます。

  図 21-4 では、スイッチ A とスイッチ B はポイントツーポイント リンクを通じて接続され、すべてのポートがブロッキング ステートになっています。スイッチ A のプライオリティ値がスイッチ B のプライオリティ値より小さい数値である場合、スイッチ A はスイッチ B に提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）を送信し、スイッチ A 自身が指定スイッチになることを提案します。

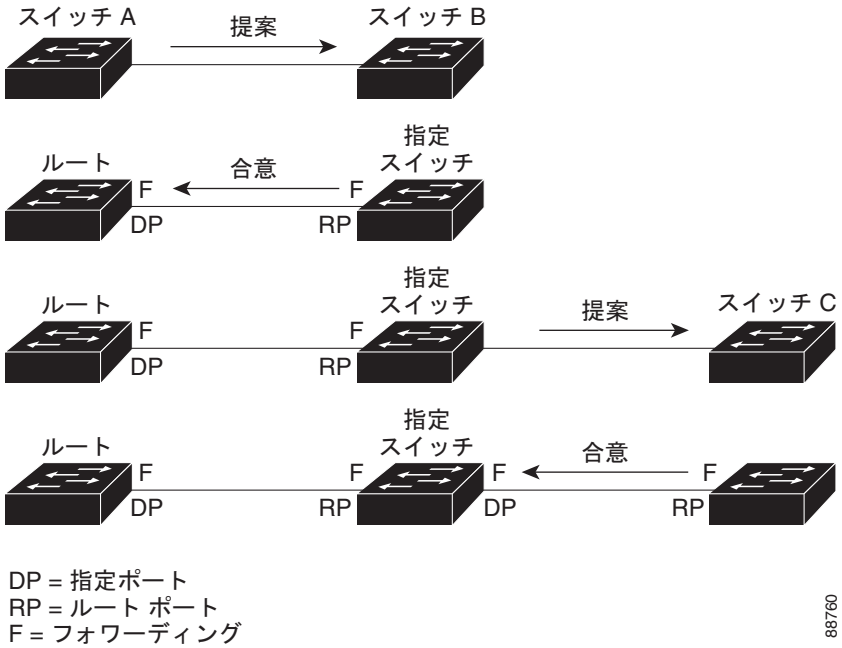
  スイッチ B は、提案メッセージを受信すると、提案メッセージを受信したポートを新しいルート ポートとして選択し、すべての非エッジ ポートをブロッキング ステートにします。さらに、新しいルート ポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

  スイッチ A は、スイッチ B の合意メッセージを受信すると、ただちに自身の指定ポートをフォワーディング ステートにします。スイッチ B はその非エッジ ポートをすべてブロックし、またスイッチ A とスイッチ B はポイントツーポイント リンクで接続されているので、ネットワークにループは形成されません。

  スイッチ C がスイッチ B に接続された場合も、同様のハンドシェイク メッセージが交換されます。スイッチ C はスイッチ B に接続されたポートをルート ポートとして選択し、両端のポートはただちにフォワーディング ステートに移行します。アクティブ トポロジにスイッチが追加されるたびに、このハンドシェイク プロセスが実行されます。ネットワークが収束すると、この提案 / 合意ハンドシェイクがルートからスパニングツリーのリーフへと進みます。

  スイッチはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。

図 21-4　高速コンバージェンスの提案と合意のハンドシェーク



DP = 指定ポート
RP = ルート ポート
F = フォワーディング

ポートの役割の同期

スイッチのポートの 1 つで提案メッセージが受信され、そのポートが新しいルート ポートに選択されると、RSTP は他のすべてのポートを新しいルートの情報に同期させます。

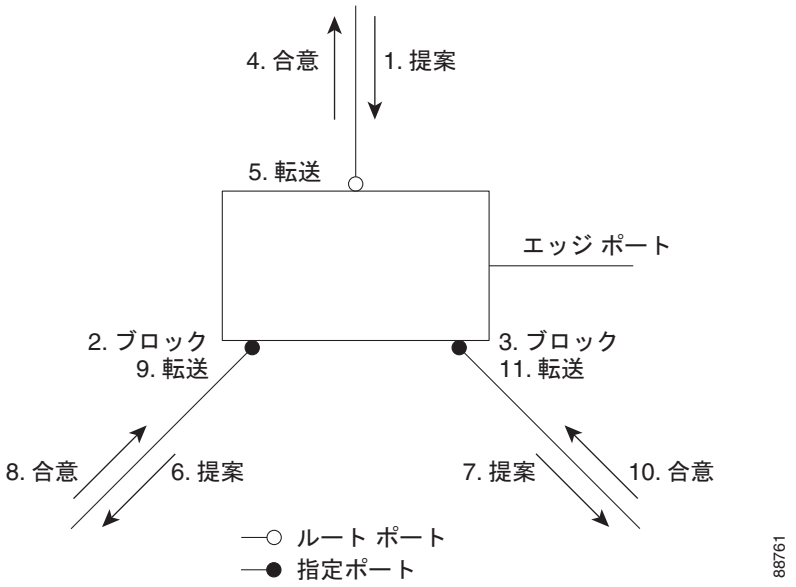
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。スイッチ上の個々のポートは次の場合に同期化された状態となります。

- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

DP は、フォワーディング ステートになっていてエッジ ポートとして設定されていない場合、RSTP によって DP が強制的に新しいルート情報で同期化すると、DP がブロッキング ステートに移行します。一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

スイッチは、すべてのポートが同期化されたことを確認すると、そのルート ポートに対応する指定スイッチに合意メッセージを送信します。ポイントツーポイント リンクで接続されたスイッチがポートの役割について互いに合意すると、RSTP はポート ステートをただちにフォワーディング ステートに移行させます。イベントのシーケンスについては、図 21-5 を参照してください。

図 21-5　高速コンバージェンス中のイベントのシーケンス



ブリッジ プロトコル データ ユニットの形式および処理

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。表 21-3 に、RSTP のフラグ フィールドを示します。

表 21-3　RSTP BPDU フラグ

ビット	機能
0	トポロジーの変化（TC）
1	提案
2 ～ 3:	ポートの役割：
00	不明
01	代替ポート
10	ルート ポート
11	指定ポート
4	ラーニング
5	フォワーディング
6	合意
7	トポロジー変更確認応答（TCA）

送信スイッチは、自身を LAN 上の指定スイッチにするために、RSTP BPDU に提案フラグを設定します。提案メッセージのポートの役割は、常に DP に設定されます。

送信スイッチは、提案を受け入れる場合、RSTP BPDU に合意フラグを設定します。合意メッセージのポートの役割は、常にルート ポートに設定されます。

RSTP には個別のトポロジ変更通知（TCN）BPDU はありません。TC フラグが使用されて、TC が示されます。ただし、IEEE 802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 BPDU 情報の処理

現在保存されているルート情報よりも優位のルート情報（小さいスイッチ ID、低パス コストなど）をポートが受信すると、RSTP は再構成を開始します。ポートが新しいルート ポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が提案フラグの設定された RSTP BPDU である場合、スイッチは他のすべてのポートを同期化した後、合意メッセージを送信します。BPDU が IEEE 802.1D BPDU である場合、スイッチは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

ポートで優位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる場合、RSTP はそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

指定ポートの役割フラグが設定された下位 BPDU（そのポートに現在保存されている値より大きいスイッチ ID、高いパス コストなど）を指定ポートが受信した場合、その指定ポートは、ただちに現在の自身の情報を応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出：IEEE 802.1D ではブロッキングとフォワーディング ステート間での すべての移行によってトポロジの変更が生じますが、RSTP ではトポロジの変更が生じるのは、ブロッキングからフォワーディングにステートが移行する場合のみです（トポロジの変更と見なされるのは、相互接続性が向上する場合だけです）。エッジ ポートにおけるステート変更は、TC の原因になりません。RSTP スイッチは、トポロジの変更を検出すると、そのスイッチのすべての非エッジ ポート（TC 通知を受信したポートを除く）で学習した情報を削除します。
- 通知：IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D との相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。
- 確認：RSTP スイッチは、指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D スイッチに接続されたルート ポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

  この処理は、IEEE 802.1D スイッチをサポートする目的でのみ必要とされます。RSTP BPDU は TCA ビットが設定されていません。

- 伝播：RSTP スイッチは、指定ポートまたはルート ポートを介して別のスイッチから TC メッセージを受信すると、自身のすべての非エッジ ポート、指定ポート、およびルート ポート（この TC メッセージを受信したポートを除く）に変更を伝播します。スイッチは、これらのすべてのポートの TC 時間タイマーを起動し、これらのポート上で学習した情報を削除します。
- プロトコルの移行：IEEE 802.1D スイッチとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU が送信される最低時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

  スイッチはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D スイッチに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP スイッチが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

MSTP のデフォルト設定

表 21-4　MSTP のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	PVST+（Rapid PVST+ と MSTP はディセーブル）
スイッチ プライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	1000 Mbps：4 100 Mbps：19 10 Mbps：100
hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

MSTP 設定時の注意事項

ここでは、MSTP の設定時の注意事項を説明します。

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- 2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- スイッチは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです（たとえば、すべての VLAN で PVST+ を使用するか、すべての VLAN で Rapid PVST+ を使用するか、またはすべての VLAN で MSTP を使用することになります）。詳細については、「スパニングツリーの相互運用性と下位互換性」（P.20-10）を参照してください。
- MST コンフィギュレーションの VTP 伝播機能はサポートされません。ただし、コマンドライン インターフェイス（CLI）または SNMP（簡易ネットワーク管理プロトコル）サポートを通じて、MST リージョン内の各スイッチで MST コンフィギュレーション（リージョン名、リビジョン番号、および VLAN とインスタンスのマッピング）を手動で設定することは可能です。
- ネットワークの冗長パスでロードバランスを実現するには、すべての VLAN とインスタンスのマッピング割り当てが一致する必要があります。一致しない場合、すべてのトラフィックは単一リンクを流れます。
- すべての MST 境界ポートは、PVST+ と MST クラウドの間、または高速 PVST+ および MST クラウドの間におけるロードバランスのために転送する必要があります。そのためには、MST クラウドの IST マスターが CST のルートを兼ねている必要があります。MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があり、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。クラウド内のスイッチを手動で設定しなければならない場合もあります。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。
- UplinkFast および BackboneFast の設定時情報については、「オプションのスパニングツリー機能の設定に関する情報」（P.22-1）を参照してください。

ルート スイッチ

スイッチは、スパニングツリー インスタンスを VLAN グループとマッピングして維持します。各インスタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるスイッチ ID が対応付けられます。最小のスイッチ ID を持つスイッチがその VLAN グループのルート スイッチになります。

特定のスイッチがルートになるように設定するには、**spanning-tree mst** *instance-id* **root** グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値（32768）からきわめて小さい値に変更します。これにより、そのスイッチが指定されたスパニングツリー インスタンスのルート スイッチになることができます。このコマンドを入力すると、スイッチは、ルート スイッチのスイッチ プライオリティを確認します。拡張システム ID のサポートのため、スイッチは指定されたインスタンスについて、自身のプライオリティを 24576 に設定します（この値によって、このスイッチが指定されたスパニングツリー インスタンスのルートになる場合）。

指定されたインスタンスのルート スイッチに、24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です。表 20-1（P.20-4）を参照）。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼働する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

各スパニングツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリビューション スイッチにする必要があります。アクセス スイッチをスパニングツリーのプライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ カウント）を指定するには、**diameter** キーワードを指定します（MST インスタンス 0 の場合のみ使用可）。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

セカンダリ ルート スイッチ

拡張システム ID をサポートするスイッチをセカンダリルートとして設定すると、スイッチ プライオリティはデフォルト値（32768）から 28672 に変更されます。その結果、プライマリ ルート スイッチに障害が発生した場合に、このスイッチが、指定されたインスタンスのルート スイッチになる可能性が高くなります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート スイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。**spanning-tree mst** *instance-id* **root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

ポートのプライオリティ

ループが発生した場合、MSTP はポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

パス コスト

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

高速移行を保障するリンク タイプ

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、「高速コンバージェンス」（P.21-10）で説明したようなループがないトポロジーを保証します。

デフォルトの場合、リンク タイプはインターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続、半二重ポートは共有接続と見なされます。MSTP が稼働しているリモート スイッチ上の 1 つのポートと物理的にポイントツーポイントで接続されている半二重リンクが存在する場合は、リンク タイプのデフォルト設定値を変更して、フォワーディング ステートへの高速移行をイネーブルにできます。

ネイバー タイプ

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。先行標準のフラグは、ポートが STP 互換モードにある場合でも、すべての show コマンドで表示されます。

プロトコル移行プロセスの再開

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MST BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、レガシー スイッチが指定スイッチでない場合、レガシー スイッチがリンクから削除されているかどうか検出できないので、スイッチは IEEE 802.1D BPDU を受け取らなくなった場合でも、自動的に MSTP モードには戻りません。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、ポートに対して引き続き、境界の役割を割り当てる可能性もあります。

MSTP の設定方法

MST リージョンの設定および MSTP のイネーブル化

このタスクは必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst configuration**	MST コンフィギュレーション モードを開始します。
ステップ 3	**instance** *instance-id* **vlan** *vlan-range*	VLAN を MSTI にマップします。 • *instance-id*：指定できる範囲は 0 ～ 4096 です。 • **vlan** *vlan-range*：指定できる範囲は 1 ～ 4096 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MSTI 1 にマップされます。 一連の VLAN を指定するには、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MSTI 1 にマップされます。

	コマンド	目的
ステップ 4	**name** *name*	コンフィギュレーション名を指定します。*name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 5	**revision** *version*	設定リビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
ステップ 6	**show pending**	保留中の設定を表示し、設定を確認します。
ステップ 7	**exit**	すべての変更を適用し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**spanning-tree mode mst**	MSTP をイネーブルにします。RSTP もイネーブルになります。 **注意** スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスは以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 9	**end**	特権 EXEC モードに戻ります。

ルート スイッチの設定

はじめる前に

スイッチをルート スイッチとして設定した後に、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

このタスクはオプションです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst** *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	スイッチをルート ブリッジとして設定します。 • *instance-id*：単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定します。範囲は 0 ～ 4096 です。 • （任意）**diameter** *net-diameter*：任意の 2 つのエンド ステーション間のスイッチの最大数を指定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • （任意）**hello-time** *seconds*：ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。

	コマンド	目的
ステップ 3	**spanning-tree mst** *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	スイッチをセカンダリ ルート スイッチとして設定します。 • *instance-id*：単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定します。範囲は 0 ～ 4096 です。 • （任意）**diameter** *net-diameter*：任意の 2 つのエンド ステーション間のスイッチの最大数を指定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • （任意）**hello-time** *seconds*：ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。 プライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

オプションの MSTP パラメータの設定

はじめる前に

スイッチ プライオリティを設定する場合は、注意が必要です。スイッチ プライオリティの変更には、通常は、**spanning-tree vlan** *vlan-id* **root primary** および **spanning-tree vlan** *vlan-id* **root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst** *instance-id* **priority** *priority*	スイッチ プライオリティを設定します。 • *instance-id*：単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定します。範囲は 0 ～ 4096 です。 • *priority*：指定できる範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。数値が小さいほど、スイッチがルート スイッチとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他の値はすべて拒否されます。
ステップ 3	**spanning-tree mst hello-time** *seconds*	すべての MST インスタンスについて、hello タイムを設定します。hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。これらのメッセージは、スイッチがアクティブであることを意味します。 *seconds*：指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。

	コマンド	目的
ステップ 4	**spanning-tree mst forward-time** *seconds*	すべての MST インスタンスについて、転送時間を設定します。転送遅延は、ポートがスパニングツリー ラーニングおよびリスニング ステートからフォワーディング ステートに変更するまでに待機する秒数です。 *seconds*：指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 5	**spanning-tree mst max-age** *seconds*	すべての MST インスタンスについて、最大経過時間を設定します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニングツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 *seconds*：指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 6	**spanning-tree mst max-hops** *hop-count*	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。 *hop-count*：指定できる範囲は 1 ～ 255 です。デフォルトは 20 です。
ステップ 7	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートとポート チャネル論理インターフェイスがあります。
ステップ 8	**spanning-tree mst** *instance-id* **port-priority** *priority*	ポート プライオリティを設定します。 • *instance-id*：単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定します。範囲は 0 ～ 4096 です。 • *priority*：指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。値が小さいほど、プライオリティが高くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。その他の値はすべて拒否されます。
ステップ 9	**spanning-tree mst** *instance-id* **cost** *cost*	コストを設定します。 ループが発生した場合、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 • *instance-id*：単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定します。範囲は 0 ～ 4096 です。 • *cost*：指定できる範囲は 1 ～ 200000000 です。デフォルト値は、インターフェイスのメディア速度に基づきます。
ステップ 10	**spanning-tree link-type point-to-point**	ポートのリンク タイプがポイントツーポイントであることを指定します。
ステップ 11	**spanning-tree mst pre-standard**	ポートが準規格 BPDU だけを送信できることを指定します。
ステップ 12	**end**	特権 EXEC モードに戻ります。

MSTP のモニタリングおよびメンテナンス

コマンド	目的
show spanning-tree mst configuration	MST リージョンの設定を表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれる MD5 ダイジェストを表示します。
show spanning-tree mst *instance-id*	指定インスタンスの MST 情報を表示します。
show spanning-tree mst interface *interface-id*	指定インターフェイスの MST 情報を表示します。
clear spanning-tree detected-protocols	スイッチでプロトコル移行プロセスを再開（強制的にネイバー スイッチと再びネゴシエートさせる）します。
clear spanning-tree detected-protocols interface *interface-id*	指定されたインターフェイスでプロトコル移行プロセスを再開します。
show running-config	入力を確認します。
copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

MSTP の設定例

MST リージョンの設定：例

次の例は、MST コンフィギュレーション モードを開始し、VLAN 10 ～ 20 を MSTI 1 にマッピングし、リージョンに *region1* という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4096
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
PVST+ および Rapid PVST+ の設定	*第 17 章「VLAN の設定」*
オプションのスパニングツリー設定	*第 22 章「オプションのスパニングツリー機能の設定」*
サポートされるスパニングツリー インスタンス数	*第 20 章「サポートされるスパニングツリー インスタンス」*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 22

オプションのスパニングツリー機能の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

オプションのスパニングツリー機能の前提条件

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）を実行している場合、これらのすべての機能を設定できます。スイッチが Multiple Spanning-Tree Protocol（MSTP）または Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルを稼働している場合は、明記した機能だけを設定できます。

オプションのスパニングツリー機能の制約事項

Rapid PVST+ または MSTP 用に、UplinkFast または BackboneFast 機能を設定できます。ただし、スパニングツリー モードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

オプションのスパニングツリー機能の設定に関する情報

PortFast

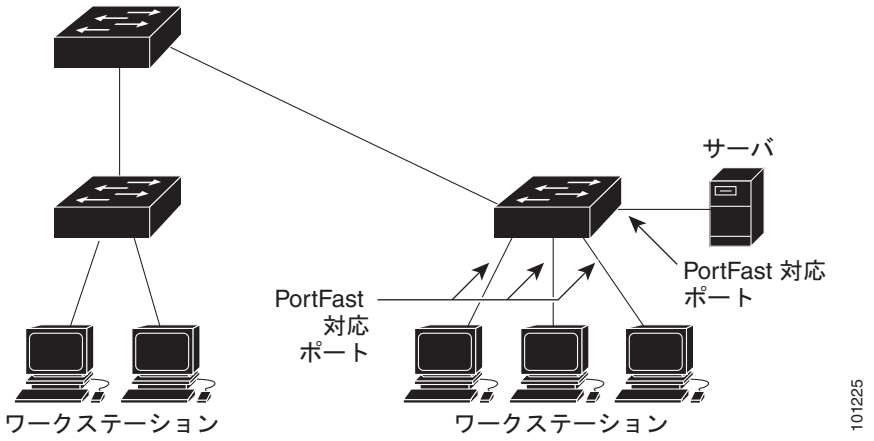
PortFast 機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。単一のワークステーションまたはサーバに接続されたインターフェイス上で PortFast を使用すると、スパニングツリーが収束するのを待たずにデバイスをただちにネットワークに接続できます（図 22-1 を参照）。

1 台のワークステーションまたはサーバに接続されたインターフェイスがブリッジ プロトコル データ ユニット（BPDU）を受信しないようにする必要があります。スイッチを再起動すると、PortFast がイネーブルに設定されているインターフェイスは通常のスパニングツリー ステータスの遷移をたどります。

（注）　PortFast の目的は、インターフェイスがスパニングツリーのコンバージェンスを待機する時間を最小限に抑えることです。したがって、PortFast はエンド ステーションに接続されたインターフェイス上で使用する場合にのみ有効です。他のスイッチに接続するインターフェイスで PortFast をイネーブルにすると、スパニングツリーのループが生じるおそれがあります。

この機能をイネーブルにするには、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンド、または **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用します。

図 22-1　PortFast 対応インターフェイス



BPDU ガード

BPDU ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルの場合は、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、PortFast 対応ポート上で BPDU ガードをイネーブルにできます。これらのポート上で BPDU が受信されると、スパニングツリーは、PortFast で動作しているポートをシャットダウンします。設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合は、許可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは errdisable ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

ポートをシャットダウンしないようにするには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用して、違反が発生したポート上の原因となっている VLAN だけをシャットダウンします。

インターフェイス レベルの場合は、PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポート上で BPDU ガードをイネーブルにできます。BPDU を受信したポートは、errdisable ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

BPDU フィルタリング

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルの場合は、**spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用して、PortFast 対応インターフェイス上で BPDU フィルタリングをイネーブルにできます。このコマンドを使用すると、PortFast 動作ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

インターフェイス レベルの場合は、PortFast 機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイス上で BPDU フィルタリングをイネーブルにできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

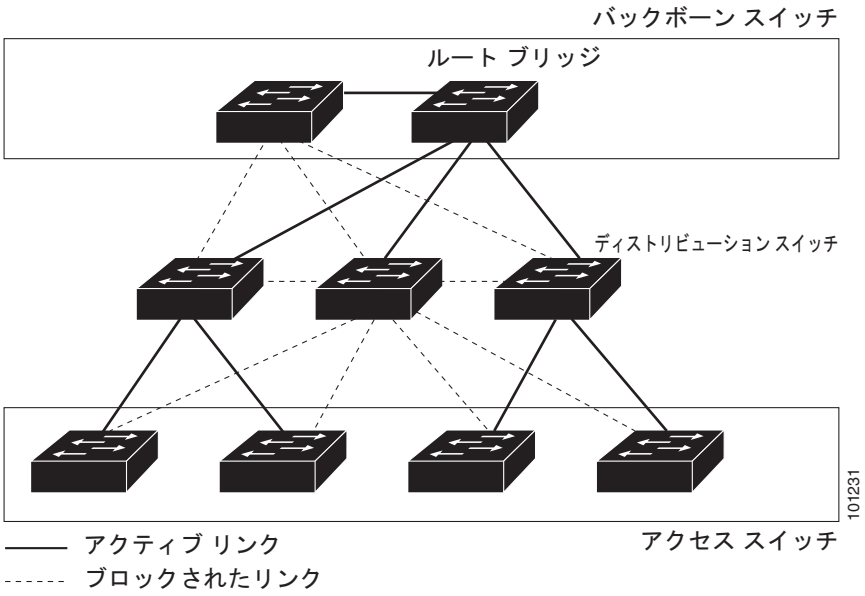
注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

スイッチ全体または 1 つのインターフェイスで BPDU フィルタリング機能をイネーブルにできます。

UplinkFast

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。図 22-2 に、ディストリビューション スイッチおよびアクセス スイッチに少なくとも 1 つの冗長リンクが確保されている複雑なネットワークの例を示します。冗長リンクは、ループを防止するために、スパニングツリーによってブロックされています。

図 22-2　　階層型ネットワークのスイッチ



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニングツリーが再設定された場合は、**spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用して UplinkFast をイネーブルにすることにより、新しいルート ポートを短時間で選択できます。ルート ポートは、通常のスパニングツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

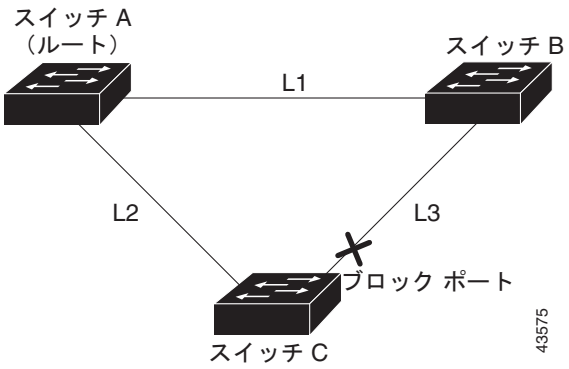
スパニングツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒 150 パケットです）。ただし、0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。

（注）　UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実行します。アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。つまり、アップリンク グループは、（転送を行う）ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

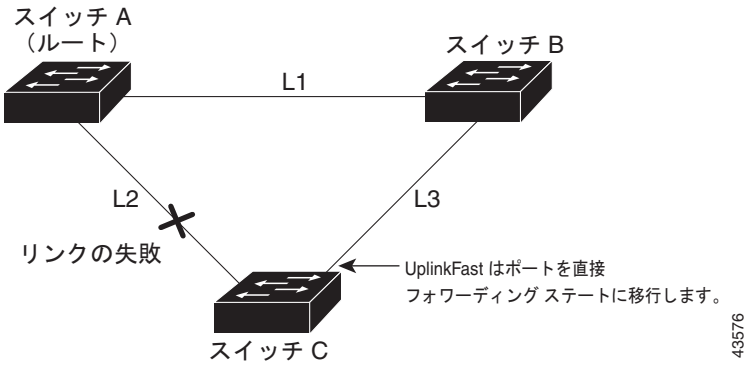
図 22-3 は、リンク障害が発生していないときのトポロジー例です。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 22-3　直接リンク障害が発生する前の UplinkFast の例



C が、ルート ポートの現在アクティブ リンクである L2 でリンク障害（*直接*リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワーディング ステートに移行させます（図 22-4 を参照）。この切り替えに必要な時間は、約 1 ～ 5 秒です。

図 22-4　直接リンク障害が発生したあとの UplinkFast の例



BackboneFast

BackboneFast は、バックボーンのコアにおける間接障害を検出します。BackboneFast は、UplinkFast 機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害に対応します。BackboneFast は、最大エージング タイマーを最適化します。最大エージング タイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。スイッチが別のスイッチの指定ポートから下位 BPDU を受信した場合、BPDU は他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFast はルートまでの別のパスを見つけようとします。

BackboneFast をイネーブルにするには、**spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。スイッチ上のルート ポートまたはブロック インターフェイスが指定スイッチから下位 BPDU を受信すると、BackboneFast が開始します。下位 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（*間接*リンク）で障害が発生したことを意味します（指定スイッチとルート スイッチ間の接続が切断されています）。スパニングツリーのルールとして、**spanning-tree vlan** *vlan-id max-age* グローバル コンフィギュレーション コマンドによって設定された最大エージング タイムの間、スイッチは下位 BPDU を無視します。

スイッチは、ルート スイッチへの代替パスの有無を判別します。下位 BPDU がブロック インターフェイスに到達した場合、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート スイッチへの代替パスになります （セルフループ ポートは、ルート スイッチへの代替パスとは見なされません）。下位 BPDU がルート ポートに到達した場合、すべてのブロック インターフェイスがルート スイッチへの代替パスになります。下位 BPDU がルート ポートに到達し、しかもブロック インターフェイスがない場合、スイッチはルート スイッチへの接続が切断されたものと見なし、ルート ポートの最大エージング タイムが経過するまで待ち、通常のスパニングツリー ルールに従ってルート スイッチになります。

スイッチが代替パスでルート スイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query（RLQ）要求を送信します。スイッチは、すべての代替パスに RLQ 要求を送信し、ネットワーク内の他のスイッチからの RLQ 応答を待機します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージング タイムが経過するまで待ちます。ルート スイッチへのすべての代替パスが、スイッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルート スイッチへ引き続き接続できる場合、スイッチは下位 BPDU を受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

図 22-5 は、リンク障害が発生していないときのトポロジー例です。ルート スイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 22-5　　間接リンク障害が発生する前の BackboneFast の例

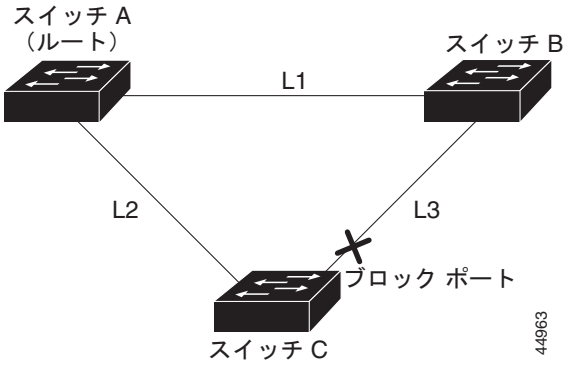


図 22-6 のリンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、その障害を検出できません。一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。BackboneFast は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを設定します。ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。図 22-6 に、BackboneFast がリンク L1 で発生した障害に応じてどのようにトポロジーを再設定するかを示します。

図 22-6　間接リンク障害が発生したあとの BackboneFast の例

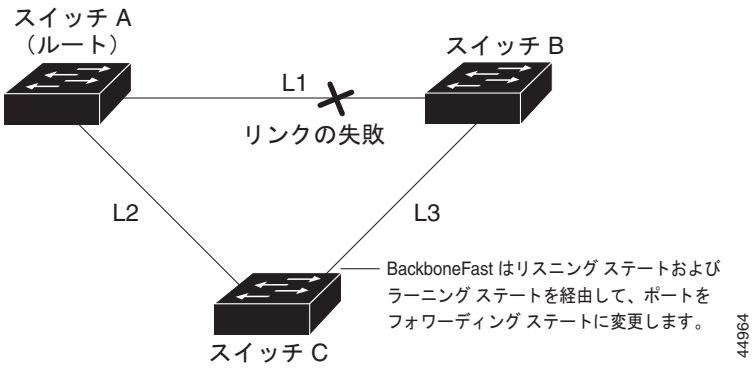
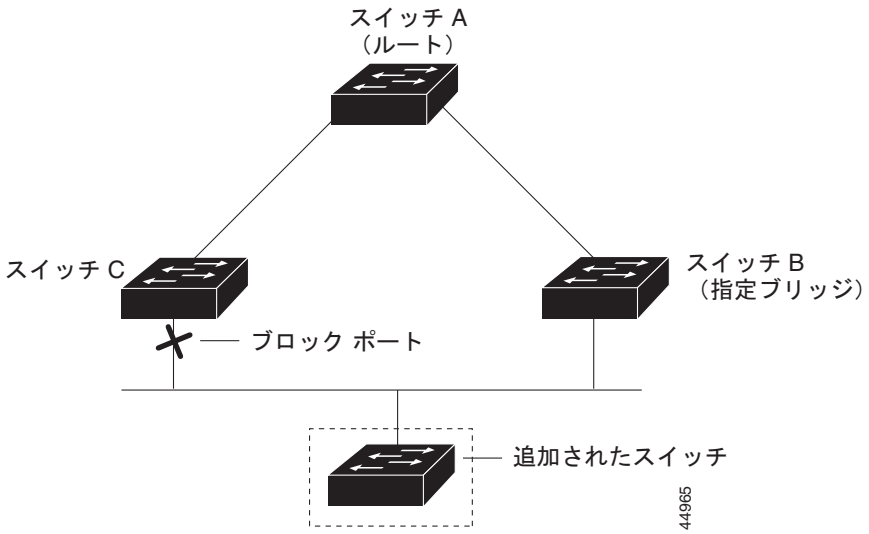


図 22-7 のように、新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。

図 22-7　メディア共有型トポロジにおけるスイッチの追加



EtherChannel ガード

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。EtherChannel 設定時の注意事項については、「EtherChannel 設定時の注意事項」（P.40-11）を参照してください。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

spanning-tree etherchannel guard misconfig グローバル コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

ルート ガード

サービス プロバイダー（SP）のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。このようなトポロジでは、スパニングツリーが再構成され、*カスタマー スイッチ*をルート スイッチとして選択する可能性があります（図 22-8）。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能をイネーブルに設定します。スパニングツリーの計算によってカスタマー ネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを root-inconsistent（ブロッキング）ステートにして、カスタマーのスイッチがルート スイッチにならないように、またはルートへのパスに組み込まれないようにします。

SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ（root-inconsistent ステートになり）、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはなく、ルートへのパスに組み込まれることもありません。

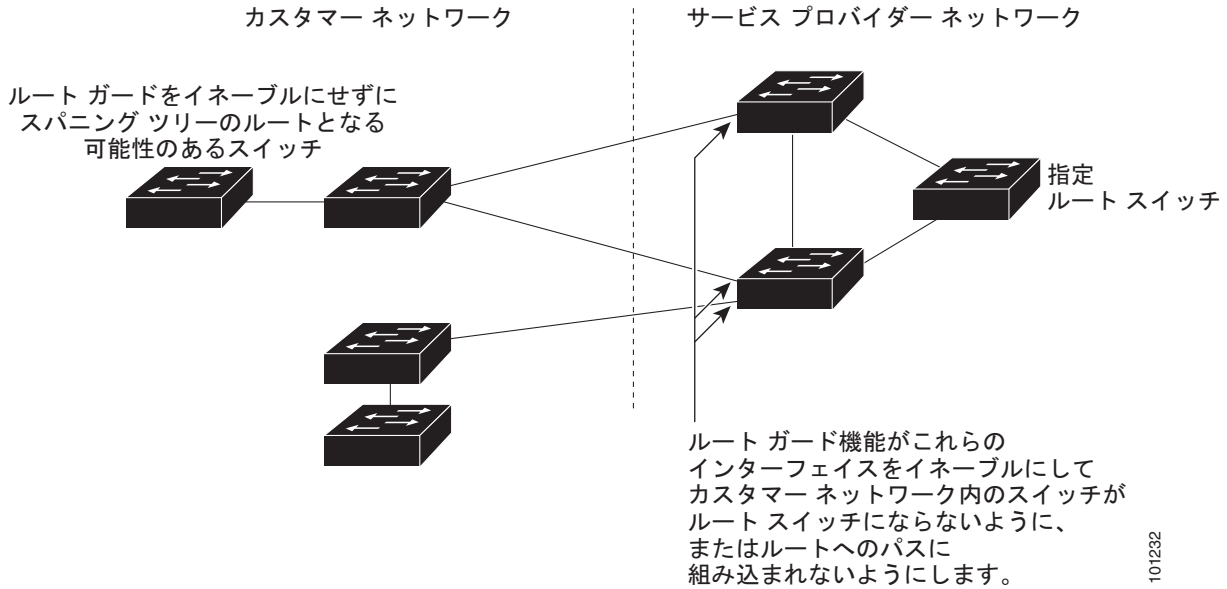
スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがルート ガードによって Internal Spanning-Tree（IST）インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロックされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。

spanning-tree guard root インターフェイス コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

注意　ルート ガード機能は使い方を誤ると、接続が切断されることがあります。

図 22-8　サービス プロバイダー ネットワークのルート ガード



ループ ガード

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体でイネーブルにした場合に最も効果があります。ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

オプションのスパニングツリーのデフォルト設定

表 22-1　オプションのスパニングツリーのデフォルト設定

機能	デフォルト設定
PortFast、BPDU フィルタリング、BPDU ガード	グローバルにディセーブル（インターフェイス単位で個別に設定する場合を除く）
UplinkFast	グローバルにディセーブル
BackboneFast	グローバルにディセーブル
EtherChannel ガード	グローバルにイネーブル

表 22-1　オプションのスパニングツリーのデフォルト設定 （続き）

機能	デフォルト設定
ルート ガード	すべてのインターフェイスでディセーブル
ループ ガード	すべてのインターフェイスでディセーブル

オプションのスパニングツリー機能の設定方法

オプションの SPT 機能のイネーブル化

はじめる前に

- トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。
- PortFast を使用するのは、単一エンド ステーションをアクセス ポートまたはトランク ポートに接続する場合に*限定*してください。スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニングツリーがネットワーク ループを検出または阻止できなくなり、その結果、ブロードキャスト ストームおよびアドレス ラーニングの障害が起きる可能性があります。
- PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、ただちにスパニングツリー フォワーディング ステートに移行されます。
- ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。
- UplinkFast をイネーブルにすると、スイッチのすべての VLAN に影響します。個々の VLAN について UplinkFast を設定することはできません。
- 音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

	コマンド	目的
ステップ 1	**show spanning-tree active** または **show spanning-tree mst**	どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default**	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**spanning-tree portfast bpduguard default**	BPDU ガードをイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 5	**spanning-tree portfast bpdufilter default**	BPDU フィルタリングをイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。

	コマンド	目的
ステップ 6	**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*]	UplinkFast をイネーブルにします。 （任意）*pkts-per-second*：指定できる範囲は毎秒 0 ～ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。
ステップ 7	**spanning-tree backbonefast**	BackboneFast をイネーブルにします。
ステップ 8	**spanning-tree etherchannel guard misconfig**	EtherChannel ガードをイネーブルにします。
ステップ 9	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**spanning-tree portfast** [**trunk**]	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。**trunk** キーワードを指定すると、トランク ポート上で PortFast をイネーブルにできます。 **（注）** トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポート上では機能しないためです。 デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。
ステップ 11	**spanning-tree guard root**	インターフェイス上でルート ガードをイネーブルにします。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルです。
ステップ 12	**end**	特権 EXEC モードに戻ります。

オプションのスパニングツリー機能のモニタリングおよびメンテナンス

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface *interface-id*	指定インターフェイスの MST 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはスパニングツリー ステート セクションのすべての行を表示します。
show interfaces status err-disabled	どのスイッチ ポートが EtherChannel の誤設定によってディセーブルにされているかを表示します。

コマンド	目的
show etherchannel summary	EtherChannel 設定を表示します。スイッチ ポートがディセーブルにされた後、リモート デバイスで利用すると便利です。
[**no**] **shutdown**	インターフェイスをディセーブルにします。**no** オプションを選択すると、インターフェイスがイネーブルになります。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
VLAN コンフィギュレーション	*第 17 章「VLAN の設定」*
音声 VLAN の設定	*第 19 章「音声 VLAN の設定」*
PVST+ および Rapid PVST+ の設定	*第 20 章「STP の設定」*
マルチ スパニングツリー プロトコルの設定	*第 21 章「MSTP の設定」*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 23

Resilient Ethernet Protocol の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

REP の前提条件

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）を実行している場合、これらのすべての機能を設定できます。スイッチが Multiple Spanning-Tree Protocol (MSTP) または Rapid PVST+（RPVST+）プロトコルを実行している場合は、明記した機能だけを設定できます。

REP の制約事項

Rapid PVST+ または MSTP 用に、UplinkFast または BackboneFast 機能を設定できます。ただし、スパニングツリー モードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

REP の設定に関する情報

REP

Resilient Ethernet Protocol（REP）はシスコ独自のプロトコルで、スパニングツリー プロトコル（STP）に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジング ループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

1 REP セグメントは、相互接続しているポートのチェーンで、セグメント ID が設定されています。各セグメントは、標準（非エッジ）セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。1 スイッチに、同じセグメントに属することができるポートは 2 つまでで、各セグメント ポートにある外部ネイバーは 1 つだけです。セグメントは共有メディアを通過できますが、どのリンクであっても同じセグメントに属することができるのは 2 ポートだけです。REP は、レイヤ 2 トランク インターフェイスだけでサポートされます。

図 23-1 に、4 つのスイッチにまたがる 6 つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジ ポートとして設定されています。（左側のセグメントのように）すべてのポートが動作可能の場合、斜線で表しているように単一ポートがブロックされます。右側の図のようにネットワークに障害が発生すると、ブロックされたポートがフォワーディング ステートに復帰して、ネットワークの中断を最小限にします。

図 23-1　REP オープン セグメント

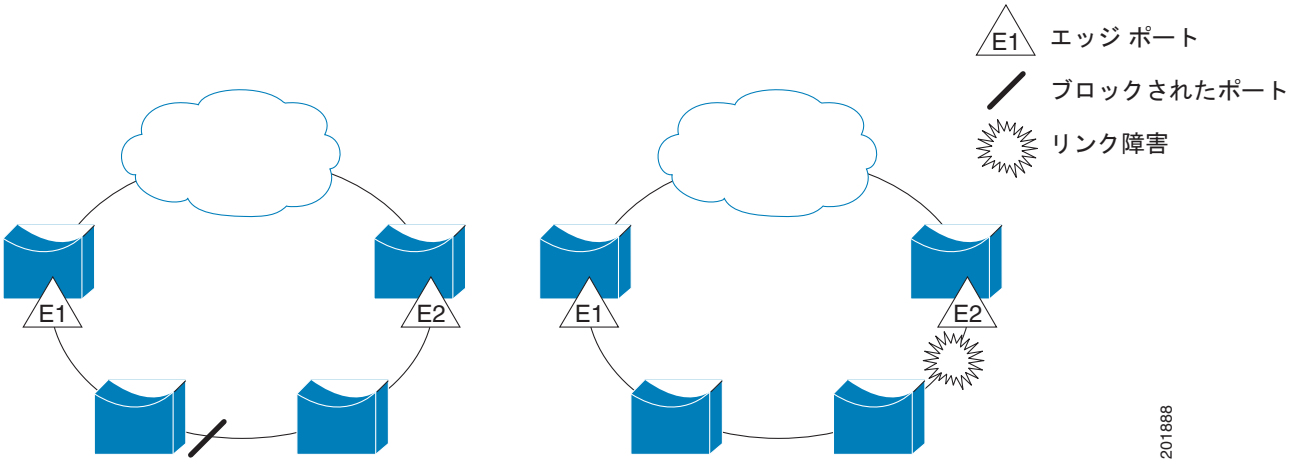
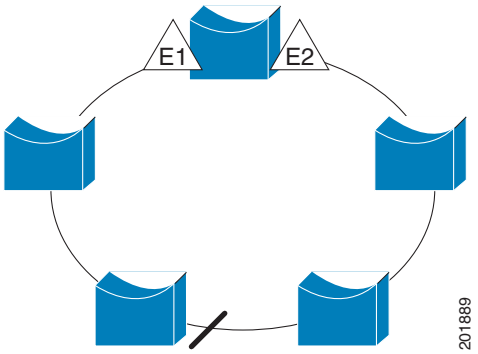


図 23-1 に示されたセグメントは、オープン セグメントで、2 つのエッジ ポート間は接続されていません。REP セグメントは、ブリッジング ループとなる可能性がなく、セグメント エッジが安全に任意のネットワークに接続されます。セグメント内のスイッチに接続されているすべてのホストには、エッジ ポートを通じて残りのネットワークに接続する方法が 2 つありますが、いつでもアクセス可能なのは 1 つだけです。障害により、ホストが通常のゲートウェイにアクセスできない場合、REP がすべてのポートのブロックを解除して、他のゲートウェイを通じた接続を確保します。

図 23-2 で示しているセグメントは、両方のエッジ ポートが同じスイッチ内にあるリング セグメントです。この設定では、セグメントを通じてエッジ ポートと接続します。この設定を使用すると、セグメント内の任意の 2 スイッチ間で冗長接続を形成することができます。

図 23-2　REP リング セグメント



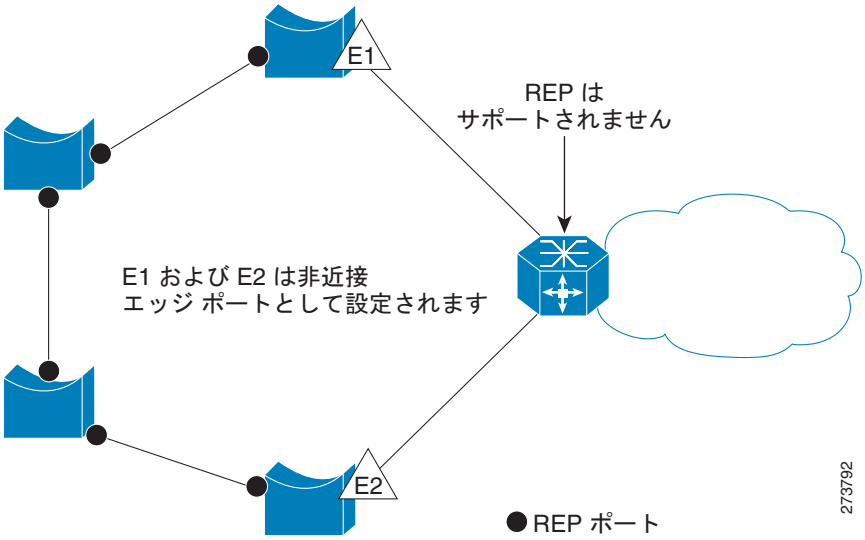
REP セグメントには次のような特徴があります。

- セグメント内の全ポートが動作可能な場合、1 ポート（*代替*ポートと呼ばれる）が各 VLAN でブロック ステートとなります。VLAN ロード バランシングが設定されている場合は、セグメント内の 2 つのポートが VLAN のブロック ステートを制御します。
- セグメント内の 1 つまたは複数のポートが動作不能になると、リンク障害が発生して、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えながら論理的にブロックされるポートが VLAN ごとに選択されます。

REP セグメントに基づいて、ほとんどのネットワーク タイプを構成することができます。また REP は、プライマリ エッジ ポートで制御されているが、セグメント内の任意のポートで発生する、VLAN ロード バランシングをサポートしています。

アクセス リング トポロジでは、ネイバー スイッチで REP がサポートされていない場合があります（図 23-3 を参照）。この場合、そのスイッチ側のポート（E1 と E2）を非ネイバー エッジ ポートとして設定できます。これらのポートは、エッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。たとえば、STP や REP のトポロジ変更通知を集約スイッチに送信するように設定することもできます。その場合、送信される STP トポロジ変更通知（TCN）は、マルチ スパニングツリー（MST）STP メッセージになります。

図 23-3　非ネイバー エッジ ポート



REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディング ループが発生します。
- REP はセグメント内の単一障害ポートだけを管理できます。REP セグメント内の複数ポート障害の場合、ネットワークの接続が中断します。
- 冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性を確認するためにエッジ ポート間でエンドツーエンド ポーリング メカニズムを使用していません。ローカル リンク障害検出を実装しています。REP リンク ステータス レイヤ（LSL）が REP 対応ネイバーを検出して、セグメント内の接続性を確立します。すべての VLAN は、ネイバーが検出されるまでインターフェイス上でブロックされます。ネイバーが特定されたあと、REP が代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID フォーマットは、スパニングツリー アルゴリズムで使用されるものと類似しており、ポート番号（ブリッジ上で一意）と、関連 MAC アドレス（ネットワーク内で一意）から構成されます。セグメント ポートが起動すると、ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。ポートは、同じセグメント内のネイバーとのスリーウェイ ハンドシェイクを実行したあとで、動作可能と宣言されます。

次のような場合、セグメント ポートは動作可能になりません。

- ネイバーに同じセグメント ID がない
- 複数のネイバーに同じセグメント ID がある
- ネイバーがピアとして、ローカル ポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。ネイバー関係が確立されると、ポートがセグメントの 1 つのブロックされたポート（代替ポート）を決定するようにネゴシエートします。その他のポートのブロックは解除されます。デフォルトで、REP パケットは BPDU クラス MAC アドレスに送

信されます。パケットは、シスコ マルチキャスト アドレスにも送信できますが、セグメントに障害が発生した場合にブロックされたポートのアドバタイズ（BPA）メッセージの送信だけに使用されます。パケットは、REP が動作していない装置によって廃棄されます。

短時間でのコンバージェンス

REP が物理リンク ベースで動作し、VLAN 単位ベースで動作しないため、必要なのは全 VLAN で 1 Hello メッセージだけなので、プロトコルの負荷が低減します。指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッディングすることも可能です。これらのメッセージはハードウェア フラッド レイヤ（HFL）で動作し、REP セグメントだけではなくネットワーク全体にフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体で専用の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

ファイバ インターフェイスのコンバージェンス復旧時間の推定値は、200 の VLAN が設定されたローカル セグメントで 200 ミリ秒未満です。VLAN ロード バランシングのコンバージェンスは 300 ミリ秒以下です。

VLAN ロード バランシング

REP セグメント内の 1 エッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジ ポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックすることで実行されます。VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

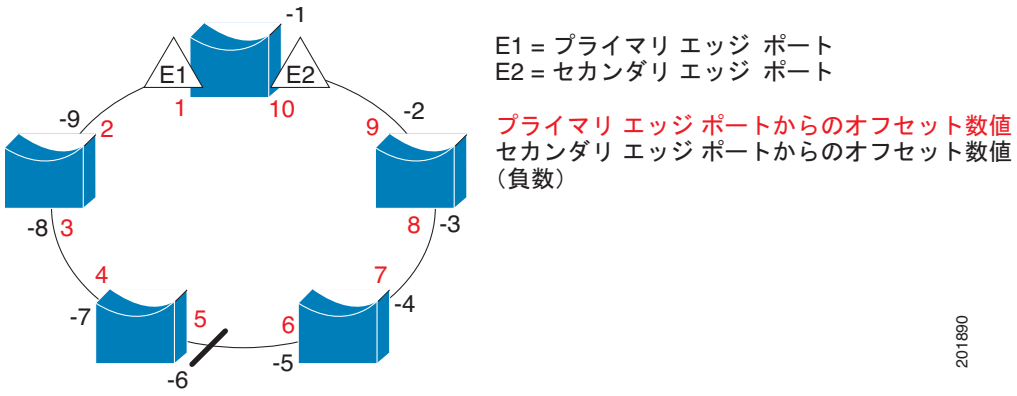
- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep detail** インターフェイス コンフィギュレーション コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ～ +256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

（注） プライマリ（またはセカンダリ）エッジ ポートからポートのダウンストリーム位置を識別することで、プライマリ エッジ ポートのオフセット番号を設定します。番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

図 23-4 に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートの場合の、セグメントのネイバー オフセット番号を示します。リングの内側にある赤い番号は、プライマリ エッジ ポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリ エッジ ポートからのオフセット番号です。正のオフセット番号（プライマリ エッジ ポートからのダウンストリーム位置）または負のオフセット番号（セカンダリ エッジ ポートからのダウンストリーム位置）のいずれかにより、（プライマリ エッジ ポートを除く）全ポートを識別することができます。E2 がプライマリ エッジ ポートになるとオフセット番号 1 となり、E1 のオフセット番号が -1 になります。

- **preferred** キーワードを入力します。これにより、**rep segment** *segment-id* **preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。

図 23-4　　セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN ロード バランシングを設定する際には、次の 2 種類の方法のいずれかを使用してトリガーを設定する必要もあります。

- プライマリ エッジ ポートのあるスイッチ上で **rep preempt segment** *segment-id* 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- **rep preempt delay** *seconds* インターフェイス コンフィギュレーション コマンドを入力すると、プリエンプション遅延時間を設定できます。リンク障害が発生して回復すると、設定されたプリエンプション期間の経過後に VLAN ロード バランシングが開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。

（注） VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および回復によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリ ポートで受信されると、これがネットワークに反映され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジ ポートだけによって VLAN ロード バランシングが開始され、セグメントが各エンドでエッジ ポートによって終端されていない場合開始することができません。プライマリ エッジ ポートは、ローカル VLAN ロード バランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。ロード バランシング設定を変更すると、プライマリ エッジ ポートでは、再び **rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済プリエンプト遅延期間が経過してから、新規設定が実行されます。エッジ ポートを通常セグメント ポートに変更しても、既存の VLAN ロード バランシング ステータスは変更されません。新規エッジ ポートを設定すると、新規トポロジ設定になる可能性があります。

スパニングツリー インタラクション

REP は、STP とも FlexLink 機能とも対話しませんが、どちらとも共存できます。セグメントに属しているポートはスパニングツリーの制御から削除されるため、セグメント ポートでは STP BPDU の送受信は行われません。したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジ ポートの場所まで両方向に設定されたら、次にエッジ ポートを設定します。

REP ポート

REP セグメント内のポートは、障害、オープン、代替のいずれかになります。

- 標準セグメント ポートとして設定されたポートは、障害ポートとして起動します。
- ネイバーとの隣接関係が確立されると、ポートは代替ポート ステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが発生して、セグメントが安定すると、ブロックされたポートのうちの 1 つが代替ロールのままになって他のすべてのポートがオープン ポートになります。
- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。代替ポートは、障害通知を受信すると、すべての VLAN を転送するオープン ステートに遷移します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジ ポートを通常セグメント ポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングの場合、セグメント内に 2 つのエッジ ポートを設定する必要があります。

スパニングツリー ポートとして再設定されたセグメント ポートは、スパニングツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキング ポートです。PortFast が設定されていたり、STP がディセーブルの場合、ポートはフォワーディング ステートになります。

REP セグメント

セグメントは、チェーンで相互接続しているポートの集合で、セグメント ID が設定されています。REP セグメントを設定するには、REP 管理 VLAN を設定し（またはデフォルト VLAN 1 を使用し）、次にインターフェイス コンフィギュレーション モードを使用してセグメントにポートを追加します。2 つのエッジ ポートをセグメント内に設定して、1 つをプライマリ エッジ ポート、もう 1 つをデフォルトでセカンダリ エッジ ポートにします。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。オプションで、セグメント トポロジ変更通知（STCN）および VLAN ロード バランシングを送信する場所を設定することもできます。

REP のデフォルト設定

REP はすべてのインターフェイス上でディセーブルです。イネーブルにする際に、エッジ ポートとして設定されていなければインターフェイスは通常セグメント ポートになります。

REP をイネーブルにする際に、STCN の送信はディセーブルで、すべての VLAN はブロックされ、管理 VLAN は VLAN 1 になります。

VLAN ロード バランシングがイネーブルの場合、デフォルトは手動でのプリエンプションで、遅延タイマーはディセーブルになっています。VLAN ロード バランシングが設定されていない場合、手動でのプリエンプション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

- まず 1 ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接するポートを設定することを推奨します。
- 外部ネイバーが設定されておらずセグメント内では 3 つ以上のポートに障害が発生した場合、1 ポートがデータ パス用のフォワーディング ステートになり、設定中の接続性の維持に役立ちます。show rep interface 特権 EXEC コマンド出力では、このポートのポート ロールは *Fail Logical Open* と表示され、他の障害ポートのポート ロールは *Fail No Ext Neighbor* と表示されます。障害ポートの外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行して、代替ポート選定メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままになります。
- REP ポートは、レイヤ 2 トランク ポートである必要があります。
- Telnet 接続を通じて REP を設定する際には注意してください。別の REP インターフェイスがメッセージを送信してブロック解除するまで REP はすべての VLAN をブロックするため、同じインターフェイスを通じてスイッチにアクセスする Telnet セッションで REP をイネーブルにすると、スイッチへの接続が失われる可能性があります。
- REP と STP または REP と Flex Link を同じセグメントやインターフェイスで実行できません。
- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを確認してください。エッジで実行されていない STP 接続は、REP セグメントでは STP が実行されないため、ブリッジング ループが発生する可能性があります。すべての STP BPDU は、REP インターフェイスで廃棄されます。
- 同じ許容 VLAN セットでセグメント内のすべてのトランク ポートを設定する必要があります。そうでない場合、設定ミスが発生します。
- REP ポートは以下の規則に従います。
  - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
  - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。
  - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジ ポートであるか、両方のポートが通常セグメント ポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。
  - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメント ポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われます。
- REP インターフェイスがブロック ステートになり、ブロック解除しても安全であると通知されるまでブロック ステートのままになります。突然の接続切断を避けるために、これを意識しておく必要があります。

- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコ マルチキャスト アドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままどのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。**rep lsl-age-timer** *value* インターフェイス コンフィギュレーション コマンドを使用して、120 ～ 10000 ミリ秒の時間を設定します。LSL hello タイマーは、このエージング タイマーの値を 3 で割った値に設定されます。通常の動作では、ピア スイッチのエージング タイマーが満了になって hello メッセージが確認されるまでに LSL hello が 3 回送信されます。
  - Cisco IOS Release 12.2(52)SE では、LSL エージング タイマーの範囲が 3000 ～ 10000 ミリ秒（500 ミリ秒単位）から 120 ～ 10000 ミリ秒（40 ミリ秒単位）に変更されています。REP ネイバー装置で Cisco IOS release 12.2(52)SE 以降が実行されていない場合は、タイマーの値を 3000 ミリ秒未満に設定しないでください。3000 ミリ秒未満の値を設定すると、要求されている時間内にネイバー スイッチが応答しないため、ポートがシャットダウンします。
  - EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。
- REP LSL エージング タイマーを設定するときには、リンクの両端で同じ値を設定するようにしてください。リンクの両端で同じ値が設定されていないと、REP リンク フラップが発生します。
- REP ポートは、これらのポート タイプのいずれかに設定できません。
  - SPAN 宛先ポート
  - トンネル ポート
  - Access port
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。
- スイッチごとに最大で 64 REP セグメントです。

REP 管理 VLAN

ロード バランシング時のリンク障害や VLAN ブロッキングの通知のメッセージをソフトウェアでリレーすることによって発生する遅延を回避するために、REP は HFL で通常のマルチキャスト アドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。ドメイン全体の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- スイッチとセグメントで 1 つの管理 VLAN だけが可能です。ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN は RSPAN VLAN になりません。

REP の設定方法

REP 管理 VLAN の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rep admin vlan** *vlan-id*	管理 VLAN を指定します。指定できる範囲は 2 ～ 4096 です。デフォルトは VLAN 1 です。管理 VLAN を 1 に設定するには、**no rep admin vlan** グローバル コンフィギュレーション コマンドを実行します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

REP インターフェイスの設定

はじめる前に

REP 動作の場合、各セグメント インターフェイスでこれをイネーブルにして、セグメント ID を指定します。このステップは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**switchport mode trunk**	インターフェイスをレイヤ 2 トランク ポートとして設定します。

	コマンド	目的
ステップ 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]	インターフェイス上で REP をイネーブルにして、セグメント番号を特定します。指定できるセグメント ID の範囲は 1 ～ 1024 です。これらの任意のキーワードは利用可能です。 **（注）** 各セグメントに 1 つのプライマリ エッジ ポートを含めて、2 つのエッジ ポートを設定する必要があります。 • **edge**：エッジ ポートとしてポートを設定します。**primary** キーワードなしで **edge** を入力すると、ポートがセカンダリ エッジ ポートとして設定されます。各セグメントにあるエッジ ポートは 2 つだけです。 • （任意）**primary**：プライマリ エッジ ポート（VLAN ロード バランシングを設定できるポート）としてポートを設定します。 • （任意）**no-neighbor**：エッジ ポートとして外部 REP ネイバーを使用せずにポートを設定します。そのポートはエッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。 **（注）** 各セグメントにあるプライマリ エッジ ポートは 1 つだけですが、2 つの異なるスイッチにエッジ ポートを設定して **primary** キーワードを両方のスイッチに入力しても、その設定は許容されます。ただし、REP ではセグメント プライマリ エッジ ポートとして 1 つのポートだけが選択されます。**show rep topology** 特権 EXEC コマンドを入力すると、セグメントのプライマリ エッジ ポートを指定することができます。 • （任意）**preferred**：ポートが優先代替ポートであるか、VLAN ロード バランシングの優先ポートであるかを示します。 **（注）** ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。
ステップ 5	**rep stcn** {**interface** *interface-id* | **segment** *id-list* | **stp**}	（任意）STCN を送信するようにエッジ ポートを設定します。 • **interface** *interface-id*：物理インターフェイスまたはポート チャネルを指定して、STCN を受け取ります。 • **segment** *id-list*：STCN を受け取る 1 つ以上のセグメントを指定します。有効範囲は 1 ～ 1024 です。 • **stp**：STCN を STP ネットワークに送信します。

	コマンド	目的
ステップ 6	**rep block port** {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**}	（任意）プライマリ エッジ ポートに VLAN ロード バランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。 • **id** *port-id*：ポート ID で代替ポートを特定します。セグメント内の各ポートにポート ID が自動的に生成されます。**show interface** *interface-id* **rep** [**detail**] 特権 EXEC コマンドを入力して、インターフェイス ポート ID を表示できます。 • *neighbor_offset* 番号：エッジ ポートからのダウンストリーム ネイバーとして代替ポートを指定します。有効範囲は -256 ～ 256 で、負数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。値 **0** は無効です。**-1** を入力して、セカンダリ エッジ ポートを代替ポートとして識別します。ネイバー オフセット番号付けの例については、図 23-4（P.23-6）を参照してください。 **（注）** プライマリ エッジ ポート（オフセット番号 1）にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力しません。 • **preferred**：すでに VLAN ロード バランシングの優先代替ポートとして指定されている通常セグメント ポートを選択します。 • **vlan** *vlan-list*：1 つの VLAN または VLAN の範囲をブロックします。 • **vlan all**：すべての VLAN をブロックします。 **（注）** REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 7	**rep preempt delay** *seconds*	（任意）リンク障害および回復後に自動的に VLAN ロード バランシングをトリガーする場合、このコマンドを入力して、プリエンプション遅延時間を設定する必要があります。遅延時間の範囲は 15 ～ 300 秒です。デフォルトは、遅延時間のない手動によるプリエンプションです。 **（注）** REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 8	**rep lsl-age-timer** *value*	（任意）ネイバーからの hello が受信されないままどのくらいの時間（ミリ秒）が経過すると REP インターフェイスがダウンするかを設定します。 指定できる範囲は 120 ～ 10000 ミリ秒（40 ミリ秒単位）です。デフォルト値は 5000 ミリ秒（5 秒）です。 **（注）** ネイバー装置で Cisco IOS Release 12.2(52)SE 以降が実行されていない場合は、指定できる範囲が 3000 ～ 10000 ミリ秒（500 ミリ秒単位）になります。EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。
ステップ 9	**end**	特権 EXEC モードに戻ります。

VLAN ロード バランシングの手動によるプリエンプションの設定

はじめる前に

プライマリ エッジ ポートでプリエンプション遅延時間を設定する **rep preempt delay** *seconds* インターフェイス コンフィギュレーション コマンドを入力しない場合、デフォルトでは、セグメントでの VLAN ロード バランシングのトリガーは手動になっています。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。**rep preempt segment** *segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

	コマンド	目的
ステップ 1	**rep preempt segment** *segment-id*	手動により、セグメント上の VLAN ロード バランシングをトリガーします。 実行前にコマンドを確認する必要があります。
ステップ 2	**show rep topology**	REP トポロジ情報を表示します。

REP の SNMP トラップ設定

リンク動作ステータス変更およびポート ロール変更について SNMP サーバに通知するために、REP 固有のトラップの送信をスイッチに設定できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp mib rep trap-rate** *value*	ルータで REP トラップの送信をイネーブルにして、1 秒あたりのトラップの送信数を設定します。指定できる範囲は 0 ～ 1000 です。デフォルトは 0（制限なし、発生するたびにトラップが送信される）です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

REP のモニタリングおよびメンテナンス

コマンド	目的
show interface [*interface-id*] **rep** [**detail**]	特定のインターフェイスまたはすべてのインターフェイスの REP の設定とステータスを表示します。
show rep topology [**segment** *segment_id*] [**archive**] [**detail**]	セグメント内のプライマリおよびセカンダリ エッジ ポートを含む、1 セグメントまたは全セグメントの REP トポロジ情報を表示します。
copy running-config startup config	スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

REP の設定例

管理 VLAN の設定：例

次に、管理 VLAN を VLAN 100 として設定して、REP インターフェイスの 1 つに **show interface rep detail** コマンドを入力して設定を確認する例を示します。

```
Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end
Switch# show interface gigabitethernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

プライマリ エッジ ポートの設定：例

次に、インターフェイスをセグメント 1 のプライマリ エッジ ポートに設定し、STCN をセグメント 2 ～ 5 に送信し、代替ポートをポート ID 0009001818D68700 のポートとして設定して、セグメント ポート障害および回復後の 60 秒のプリエンプション遅延後にすべての VLAN をブロックする例を示します。このインターフェイスは、ネイバーからの hello が受信されないまま 6000 ミリ秒が経過するとダウンするように設定されています。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end
```

インターフェイスに外部 REP ネイバーがない場合にプライマリ エッジ ポートとしてインターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
```

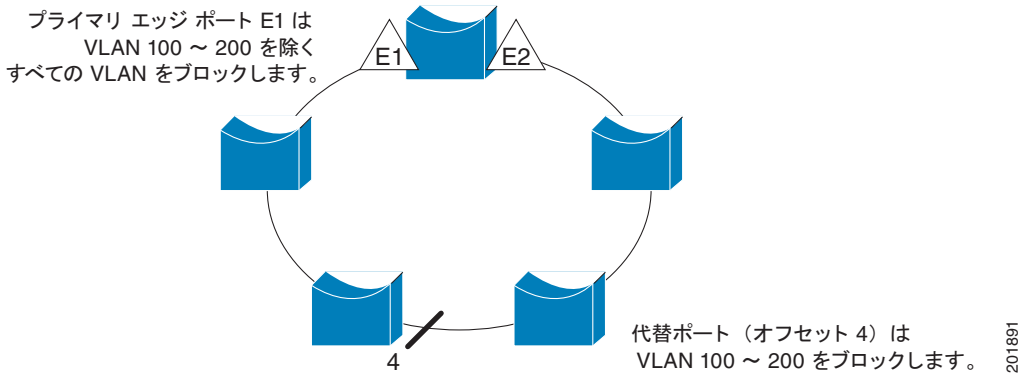
```
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
```

VLAN ブロッキング：設定例

次に、図 23-5 の、VLAN ブロッキング コンフィギュレーションを設定する例を示します。代替ポートは、ネイバー オフセット番号 4 のネイバーです。手動によるプリエンプションのあとに、VLAN 100 ～ 200 がこのポートでブロックされ、その他のすべての VLAN がプライマリ エッジ ポート E1（ギガビット イーサネット ポート 1/0/1）でブロックされます。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

図 23-5　VLAN ブロッキングの例



その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 24

FlexLink および MAC アドレス テーブル移動更新の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

FlexLink および MAC アドレス テーブル移動更新の制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

FlexLink と MAC アドレス テーブル移動更新の設定に関する情報

FlexLink

FlexLink は、レイヤ 2 インターフェイス（スイッチ ポートまたはポート チャネル）のペアで、1 つのインターフェイスがもう一方のバックアップとして機能するように設定されています。この機能は、スパニングツリー プロトコル（STP）の代替ソリューションです。ユーザは、STP をディセーブルにしても、基本的リンク冗長性を保つことができます。FlexLink は、通常、お客様がスイッチで STP を実行しない場合のサービス プロバイダーまたは企業ネットワークに設定されます。スイッチが STP を実行中の場合は、STP がすでにリンクレベルの冗長性またはバックアップを提供しているため、FlexLink は不要です。

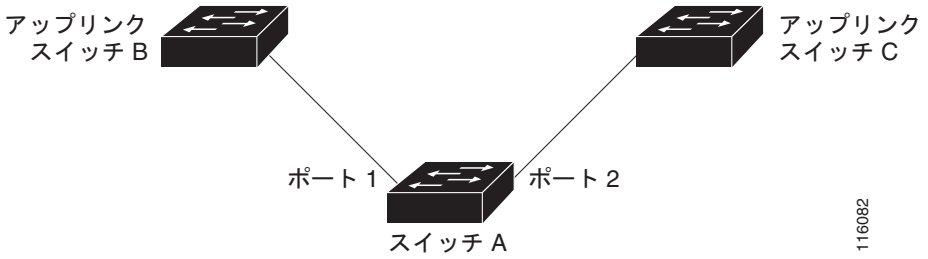
別のレイヤ 2 インターフェイスを FlexLink またはバックアップ リンクとして割り当てることで、1 つのレイヤ 2 インターフェイス（アクティブ リンク）に FlexLink を設定します。リンクの 1 つがアップでトラフィックを転送しているときは、もう一方のリンクがスタンバイ モードで、このリンクがシャット ダウンした場合にトラフィックの転送を開始できるように準備しています。どの時点でも、1

つのインターフェイスのみがリンクアップ ステートでトラフィックを転送しています。プライマリ リンクがシャットダウンされると、スタンバイ リンクがトラフィックの転送を始めます。アクティブ リンクがアップに戻った場合はスタンバイ モードになり、トラフィックが転送されません。STP は FlexLink インターフェイス上でディセーブルです。

図 24-1 では、スイッチ A のポート 1 およびポート 2 がアップリンク スイッチ B およびアップリンク スイッチ C に接続されています。これらのスイッチは FlexLink として設定されているので、どちらかのインターフェイスがトラフィックを転送し、もう一方のインターフェイスはスタンバイ モードになります。ポート 1 がアクティブ リンクになる場合、ポート 1 とスイッチ B との間でトラフィックの転送を開始し、ポート 2（バックアップ リンク）とスイッチ C との間のリンクでは、トラフィックは転送されません。ポート 1 がダウンした場合はポート 2 がアップし、トラフィックをスイッチ C に転送し始めます。ポート 1 は、再び動作を開始するとスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィック転送を続けます。

また、優先してトラフィックの転送に使用するポートを指定して、プリエンプション メカニズムを設定することもできます。たとえば、図 24-1 では、FlexLink ペアをプリエンプション モードで設定することにより、ポート 2 より帯域幅の大きいポート 1 が再び動作を開始した後、ポート 1 が 60 秒後にトラフィックの転送を開始し、ポート 2 がスタンバイとなります。これを行うには、**switchport backup interface preemption mode bandwidth** および **switchport backup interface preemption delay** インターフェイス コンフィギュレーション コマンドを入力します。

図 24-1　　FlexLink の設定例



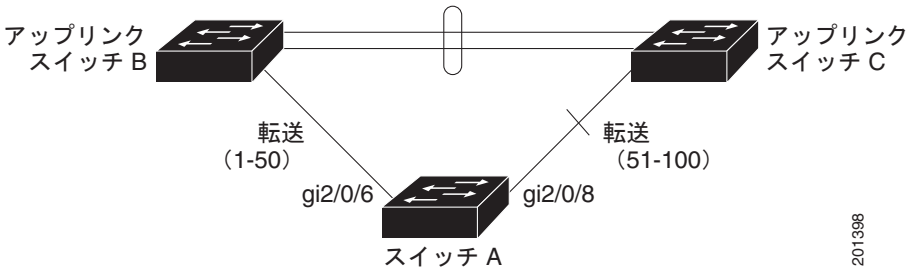
プライマリ（転送）リンクがダウンすると、トラップによってネットワーク管理ステーションが通知を受けます。スタンバイ リンクがダウンすると、トラップによってユーザが通知を受けます。

FlexLink はレイヤ 2 ポートおよびポート チャネルだけでサポートされ、VLAN またはレイヤ 3 ポートではサポートされません。

VLAN FlexLink ロード バランシングおよびサポート

VLAN FlexLink ロード バランシングにより、ユーザは相互に排他的な VLAN のトラフィックを両方のポートで同時に転送するように FlexLink ペアを設定できます。たとえば、FlexLink ポートが 1 ～ 100 の VLAN に対して設定されている場合、最初の 50 の VLAN のトラフィックを 1 つのポートで転送し、残りの VLAN のトラフィックをもう一方のポートで転送できます。どちらかのポートで障害が発生した場合には、もう一方のアクティブ ポートがすべてのトラフィックを転送します。障害が発生したポートが元に戻ると、優先 VLAN のトラフィックの転送を再開します。このように、FlexLink のペアは冗長性を提供するだけでなく、ロード バランシングの用途に使用できます。FlexLink VLAN ロード バランシングによってアップリンク スイッチが制約を受けることはありません。

図 24-2　VLAN FlexLink ロード バランシングの設定例



FlexLink マルチキャスト高速コンバージェンス

FlexLink マルチキャスト高速コンバージェンスにより、FlexLink の障害発生後のマルチキャスト トラフィック コンバージェンス時間が短縮されます。

その他の FlexLink ポートを mrouter ポートとして学習

通常のマルチキャスト ネットワークでは、個々の VLAN について 1 つのクエリアが選定されます。ネットワーク エッジに展開されたスイッチには、クエリーを受信するいずれかの FlexLink ポートが存在します。FlexLink ポートは常に、転送状態になります。

クエリーを受信するポートが、スイッチの *mrouter* ポートとして追加されます。mrouter ポートは、スイッチが学習したすべてのマルチキャスト グループの 1 つとして認識されます。切り替えの後、クエリーは別の FlexLink ポートによって受信されます。この別の FlexLink ポートは mrouter ポートとして認識されるようになります。切り替えの後、マルチキャスト トラフィックは別の FlexLink ポートを介して流れます。トラフィック コンバージェンスを高速化するために、いずれか一方の FlexLink ポートが mrouter ポートとして学習されると、両方の FlexLink ポートが mrouter ポートとして認識されます。いずれの FlexLink ポートも常に、マルチキャスト グループの一部として扱われます。

通常の動作モードではいずれの FlexLink ポートもグループの一部として認識されますが、バックアップ ポートを通過するトラフィックはすべてブロックされます。したがって、mrouter ポートとしてバックアップ ポートを追加しても、通常のマルチキャスト データ フローが影響を受けることはありません。切り替えが生じると、バックアップ ポートのブロックが解除され、トラフィックが流れるようになります。この場合、バックアップ ポートのブロックが解除されるとただちに、アップストリーム データが流れ始めます。

IGMP レポートの生成

切り替えの後、バックアップ リンクがアップ状態になると、アップストリームでの新しいディストリビューション スイッチでのマルチキャスト データの転送は開始されません。これは、ブロックされた FlexLink ポートに接続されているアップストリーム ルータのポートが、いずれのマルチキャスト グループの一部としても認識されないからです。マルチキャスト グループのレポートは、バックアップ リンクがブロックされているため、ダウンストリーム スイッチでは転送されません。このポートのデータは、マルチキャスト グループが学習されるまで流れません。マルチキャスト グループの学習は、レポートを受信した後にだけ行われます。

レポートは、一般クエリーが受信されると、ホストより送信されます。一般クエリーは、通常のシナリオであれば 60 秒以内に送信されます。バックアップ リンクが転送を開始し、マルチキャスト データを高速で収束できるようになると、ダウンストリーム スイッチが一般クエリーを待つことなく、ただちにこのポート上のすべての学習済みグループに対し、プロキシ レポートを送信します。

IGMP レポートのリーク

マルチキャスト トラフィックを最小限の損失で収束させるために、FlexLink のアクティブ リンクがダウンする前に冗長データ パスを設定しておく必要があります。マルチキャスト トラフィックのコンバージェンスは、FlexLink バックアップ リンクに IGMP レポート パケットだけをリークさせれば行えます。こうしてリークさせた IGMP レポート メッセージがアップストリームのディストリビューション ルータで処理されるため、マルチキャスト データのトラフィックはバックアップ インターフェイスに転送されます。バックアップ インターフェイスの着信トラフィックはすべてアクセス スイッチの入り口部分でドロップされるため、ホストが重複したマルチキャスト トラフィックを受信することはありません。FlexLink のアクティブ リンクに障害が発生した場合、ただちにアクセス スイッチがバックアップ リンクからのトラフィックを受け入れ始めます。このスキームの唯一の欠点は、ディストリビューション スイッチ間のリンク、およびディストリビューション スイッチとアクセス スイッチの間のバックアップ リンクで帯域幅が大幅に消費される点です。この機能はデフォルトでディセーブルになっています。**switchport backup interface *interface-id* multicast fast-convergence** コマンドを使用して、設定を変更できます。

切り替え時にこの機能がイネーブルになっている場合、スイッチでは転送ポートに設定されたバックアップ ポート上でプロキシ レポートは生成されません。

MAC アドレス テーブル移動更新

MAC アドレス テーブル移動更新機能により、プライマリ（転送）リンクがダウンしてスタンバイ リンクがトラフィックの転送を開始したときに、スイッチで高速双方向コンバージェンスが提供されます。

図 24-3 では、スイッチ A がアクセス スイッチで、スイッチ A のポート 1 および 2 が FlexLink ペア経由でアップリンク スイッチの B と D に接続されます。ポート 1 はトラフィックの転送中で、ポート 2 はバックアップ ステートです。PC からサーバへのトラフィックはポート 1 からポート 3 に転送されます。PC の MAC アドレスが、スイッチ C のポート 3 で学習されています。サーバから PC へのトラフィックはポート 3 からポート 1 に転送されます。

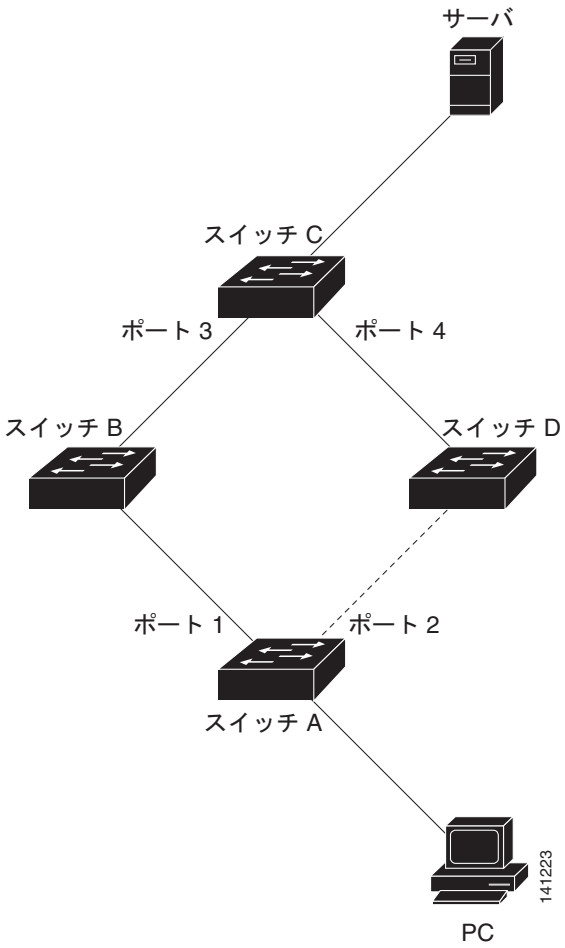
MAC アドレス テーブル移動更新機能が設定されておらず、ポート 1 がダウンした場合は、ポート 2 がトラフィックの転送を開始します。しかし、少しの間、スイッチ C がポート 3 経由でサーバから PC にトラフィックを転送し続けるため、ポート 1 がダウンしていることにより、PC へのトラフィックが途切れます。スイッチ C がポート 3 で PC の MAC アドレスを削除し、ポート 4 で再度学習した場合は、トラフィックはポート 2 経由でサーバから PC へ転送される可能性があります。

図 24-3 で MAC アドレス テーブル移動更新機能が設定され、各スイッチでイネーブルになっていて、ポート 1 がダウンした場合は、ポート 2 が PC からサーバへのトラフィックの転送を開始します。スイッチは、ポート 2 から MAC アドレス テーブル移動更新パケットを送出します。スイッチ C はこのパケットをポート 4 で受信し、ただちに PC の MAC アドレスをポート 4 で学習します。これにより、再収束時間が短縮されます。

アクセススイッチであるスイッチ A を設定し、MAC アドレス テーブル移動更新メッセージを送信（*send*）することができます。また、アップリンク スイッチ B、C、および D を設定して、MAC アドレス テーブル移動更新メッセージの取得（*get*）および処理を行うこともできます。スイッチ C がスイッチ A から MAC アドレス テーブル移動更新メッセージを受信すると、スイッチ C はポート 4 で PC の MAC アドレスを学習します。スイッチ C は、PC の転送テーブル エントリを含め、MAC アドレス テーブルをアップデートします。

スイッチ A が、MAC アドレス テーブル移動更新を待機する必要はありません。スイッチはポート 1 上の障害を検出すると、ただちに、新しい転送ポートであるポート 2 からのサーバ トラフィックの転送を開始します。この変更は、100 ミリ秒（ms）以内に行われます。PC はスイッチ A に直接接続され、その接続状態に変更はありません。スイッチ A による、MAC アドレス テーブルでの PC エントリの更新は必要ありません。

図 24-3　MAC アドレス テーブル移動更新の例



FlexLink および MAC アドレス テーブル移動更新のデフォルト設定

デフォルト設定
FlexLink は設定されておらず、バックアップ インターフェイスは定義されていません。
プリエンプション モードはオフです。
プリエンプション遅延は 35 秒です。
MAC アドレス テーブル移動更新は、スイッチで設定されていません。

FlexLink および MAC アドレス テーブル移動更新設定時の注意事項

FlexLink の設定時には、次の注意事項に従ってください。

- 最大 16 のバックアップ リンクを設定できます。
- アクティブ リンクには、FlexLink バックアップ リンクを 1 つだけ設定できます。バックアップ リンクは、アクティブ インターフェイスとは異なるインターフェイスにする必要があります。
- インターフェイスは 1 つの FlexLink ペアだけに属します。インターフェイスは、1 つだけのアクティブ リンクのバックアップ リンクにすることができます。アクティブ リンクは、別の FlexLink ペアに属することができません。
- どちらのリンクも、EtherChannel に属するポートには設定できません。ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を FlexLink として設定でき、ポート チャネルおよび物理インターフェイスを FlexLink として設定して、ポート チャネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。
- バックアップ リンクはアクティブ リンクと同じタイプ（ファスト イーサネット、ギガビット イーサネット、またはポート チャネル）にする必要はありません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の FlexLink を同様の特性で設定する必要があります。
- FlexLink ポートでは STP がディセーブルになります。ポート上にある VLAN が STP 用に設定されている場合でも、FlexLink ポートは STP に参加しません。STP がイネーブルでない場合は、設定されているトポロジでループが発生しないようにしてください。FlexLink 設定が削除されると、そのポートの STP は再びイネーブルになります。

FlexLink 機能による VLAN ロード バランシングを設定するときには、次の注意事項に従ってください。

- FlexLink VLAN ロード バランシングでは、バックアップ インターフェイス上で優先される VLAN を選択する必要があります。
- 同じ FlexLink ペアに対して、プリエンプション メカニズムと VLAN ロード バランシングを設定することはできません。

MAC アドレス テーブル移動更新機能の設定時には、次の注意事項に従ってください。

- アクセス スイッチでこの機能のイネーブル化と設定を行うと、MAC アドレス テーブル移動更新を送信（*send*）することができます。
- アップリンク スイッチでこの機能のイネーブル化と設定を行うと、MAC アドレス テーブル移動更新を受信（*receive*）することができます。

FlexLink および MAC アドレス テーブル移動更新の設定方法

FlexLink の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネルの範囲は 1 ～ 6 です。
ステップ 3	**switchport backup interface** *interface-id*	物理レイヤ 2 インターフェイス（ポート チャネル）をインターフェイスを装備した FlexLink ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**end**	特権 EXEC モードに戻ります。

FlexLink のプリエンプト方式の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネルの範囲は 1 ～ 6 です。
ステップ 3	**switchport backup interface** *interface-id*	物理レイヤ 2 インターフェイス（ポート チャネル）をインターフェイスを装備した FlexLink ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。

	コマンド	目的
ステップ 4	**switchport backup interface** *interface-id* **preemption mode** [**forced** | **bandwidth** | **off**]	FlexLink インターフェイス ペアのプリエンプション メカニズムおよび遅延を設定します。次のプリエンプション モードを設定することができます。 • **forced**：アクティブ インターフェイスが常にバックアップに対してプリエンプションを行います。 • **bandwidth**：より広い帯域幅のインターフェイスが常にアクティブ インターフェイスとして動作します。 • **off**：アクティブからバックアップへのプリエンプションは発生しません。
ステップ 5	**switchport backup interface** *interface-id* **preemption delay** *delay-time*	ポートが他のポートより先に使用されるまでの遅延時間を設定します。 **（注）** 遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
ステップ 6	**end**	特権 EXEC モードに戻ります。

FlexLink の VLAN ロード バランシングの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネルの範囲は 1 ～ 6 です。
ステップ 3	**switchport backup interface** *interface-id* ***prefer vlan*** *vlan-range*	物理レイヤ 2 インターフェイス（またはポート チャネル）を、インターフェイスを装備した FlexLink ペアの一部として設定し、インターフェイス上の VLAN を指定します。VLAN ID の範囲は 1 ～ 4096 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

MAC アドレス テーブル移動更新機能の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネルの範囲は 1 ～ 6 です。

	コマンド	目的
ステップ 3	**switchport backup interface** *interface-id* または **switchport backup interface** *interface-id* **mmu primary vlan** *vlan-id*	物理レイヤ 2 インターフェイス（またはポート チャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定します。MAC アドレス テーブル移動更新 VLAN はインターフェイスで最も低い VLAN ID です。 物理レイヤ 2 インターフェイス（またはポート チャネル）を設定し、MAC アドレステーブル移動更新の送信に使用される、インターフェイス上の VLAN ID を指定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**mac address-table move update transmit**	プライマリ リンクがダウンし、スイッチがスタンバイ リンク経由でトラフィックの転送を開始した場合は、アクセス スイッチをイネーブルにして、MAC アドレス テーブル移動更新をネットワーク上の他のスイッチに送信します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

MAC アドレス テーブル移動更新メッセージの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table move update receive**	スイッチをイネーブルにして、MAC アドレス テーブル移動更新の受信および処理を行います。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table move update**	設定を確認します。
ステップ 5	**copy running-config startup config**	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

FlexLink および MAC アドレス テーブル移動更新のモニタリングおよびメンテナンス

コマンド	目的
show interfaces [*interface-id*] **switchport backup**	あるインターフェイス用に設定された FlexLink バックアップ インターフェイス、または設定されたすべての FlexLink と、各アクティブ インターフェイスおよびバックアップ インターフェイスの状態（アップまたはスタンバイ モード）を表示します。VLAN ロード バランシングがイネーブルであると、出力には、アクティブ インターフェイスおよびバックアップ インターフェイスの優先 VLAN が表示されます。
show mac address-table move update	設定を確認します。

FlexLink および MAC アドレス テーブル移動更新の設定例

FlexLink ポートの設定：例

次に、FlexLink ポートを設定したときに他の FlexLink ポートを mrouter ポートとして学習する例と、**show interfaces switchport backup** コマンドの出力を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface GigabitEthernet1/2
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
Preemption Mode : off
Multicast Fast Convergence : Off
Mac Address Move Update Vlan : auto
```

次の出力は、特定のポートを介してスイッチに到達するクエリーを持つ、VLAN 1 および VLAN 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier
Vlan    IP Address      IGMP Version       Port
------------------------------------------------------------
1       1.1.1.1         v2                 Gi0/1
401     41.41.41.1      v2                 Gi0/1
```

次に、VLAN 1 および VLAN 401 用の **show ip igmp snooping mrouter** コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter
```

```
Vlan    ports
----    -----
1       Gi1/1(dynamic), Gi1/2(dynamic)
401     Gi1/1(dynamic), Gi1/2(dynamic)
```

同様に、両方の FlexLink ポートは学習されたグループに属しています。この例では、GigabitEthernet1/1 は VLAN 1 のレシーバ/ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups
Vlan    Group       Type    Version     Port List
------------------------------------------------------------------------
1       228.1.5.1   igmp    v2          Gi1/1, Gi1/2, Fa2/1
1       228.1.5.2   igmp    v2          Gi1/1, Gi1/2, Fa2/1
```

ホストが一般クエリーに応答するときに、スイッチはすべてのマルチキャスト ルータ ポートに関するこのレポートを転送します。この例では、ホストがグループ 228.1.5.1 のレポートを送信するとき、バックアップ ポート GigabitEthernet1/2 はブロックされているので、レポートは GigabitEthernet1/1 でだけ送信されます。アクティブ リンクの GigabitEthernet1/1 がダウンすると、バックアップ ポートの GigabitEthernet1/2 が転送を開始します。

このポートが転送を開始すると、ただちにホストに代わり、228.1.5.1 と 228.1.5.2 のグループにプロキシ レポートを送信します。アップストリーム ルータはグループを学習し、マルチキャスト データの転送を開始します。これは、FlexLink のデフォルトの動作です。この動作は、ユーザが **switchport backup interface GigabitEthernet**1/2 **multicast fast-convergence** コマンドを使用して高速コンバージェンスを設定すると、変更されます。次に、この機能を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# switchport backup interface GigabitEthernet1/2 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:
Active                Interface             Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/1  GigabitEthernet1/2  Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Mac Address Move Update Vlan : auto
```

次の出力は、設定されたポートを介してスイッチに到達するクエリーを持つ、VLAN 1 および VLAN 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier
Vlan       IP Address     IGMP Version   Port
-----------------------------------------------------------
1          1.1.1.1        v2             Gi1/1
401        41.41.41.1     v2             Gi1/1
```

次に VLAN 1 と 401 に対する **show ip igmp snooping mrouter** コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter
Vlan       ports
----       -----
1          Gi1/1(dynamic), Gi1/2(dynamic)
401        Gi1/1(dynamic), Gi1/2(dynamic)
```

同様に、両方の FlexLink ポートは学習されたグループに属しています。この例では、ポートは VLAN 1 のレシーバ/ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups
Vlan    Group       Type    Version     Port List
------------------------------------------------------------------------
1       228.1.5.1   igmp    v2          Gi1/1, Gi1/2, Gi1/1
1       228.1.5.2   igmp    v2          Gi1/1, Gi1/2, Gi1/1
```

一般クエリーに対してあるホストが応答すると必ず、スイッチがすべての mrouter ポートに関するこのレポートを転送します。コマンドライン ポートを介してこの機能をオンにし、設定された GigabitEthernet1/1 上のスイッチによってレポートが転送されると、レポートはバックアップ ポート GigabitEthernet1/2 にもリークされます。アップストリーム ルータはグループを学習し、マルチキャスト データの転送を開始します。GigabitEthernet1/2 はブロックされているので、このデータは入力で廃棄されます。アクティブ リンクの GigabitEthernet1/1 がダウンすると、バックアップ ポートの GigabitEthernet1/2 が転送を開始します。マルチキャスト データはすでにアップストリーム ルータにより転送されているため、いずれのプロキシ レポートも送信する必要はありません。バックアップ ポートにレポートをリークさせることにより、冗長マルチキャスト パスが設定されるため、マルチキャスト トラフィック コンバージェンスに要する時間が最小限に抑えられます。

バックアップ インターフェイスの設定：例

次に、インターフェイスをバックアップ インターフェイスに設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)# switchport backup interface gigabitethernet1/2
Switch(conf-if)# end

Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Vlans Preferred on Active Interface: 1-3,5-4096
        Vlans Preferred on Backup Interface: 4
```

プリエンプト方式の設定：例

次に、バックアップ インターフェイスのペアに対してプリエンプション モードを *forced* に設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)#switchport backup interface gigabitethernet1/2 preemption mode forced
Switch(conf-if)#switchport backup interface gigabitethernet1/2 preemption delay 50
Switch(conf-if)# end

Switch# show interfaces switchport backup detail
Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/1 GigabitEthernet1/2 Active Up/Backup Standby
Interface Pair : Gi1/1, Gi1/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi1/1), 100000 Kbit (Gi1/2)
Mac Address Move Update Vlan : auto
```

FlexLink の VLAN ロード バランシングの設定：例

次に、スイッチに VLAN 1 ～ 50、60、および 100 ～ 120 を設定する例を示します。

```
Switch(config)# interface gigabitEthernet 1/2
Switch(config-if)# switchport backup interface gigabitEthernet 1/2 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合、GigabitEthernet1/1 は VLAN 60 および 100 ～ 120 のトラフィックを転送し、GigabitEthernet1/2 は VLAN 1 ～ 50 のトラフィックを転送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/1    GigabitEthernet1/2    Active Up/Backup Standby
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

FlexLink インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は、FlexLink ペアのピア インターフェイスに移動します。この例では、インターフェイス Gigabit Ethernet1/1 がダウンした場合、Gigabit Ethernet1/2 が FlexLink ペアのすべての VLAN を引き継ぎます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/1    GigabitEthernet1/2    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

FlexLink インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gigabit Ethernet1/1 がアップになって、このインターフェイスに指定されていた VLAN がピア インターフェイス Gigabit Ethernet1/2 上でブロックされ、Gigabit Ethernet1/1 に転送されます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/1    GigabitEthernet1/2    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet1/3       FastEthernet1/4       Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4096
Vlans Preferred on Backup Interface: 3-4
Preemption Mode  : off
Bandwidth : 10000 Kbit (Fa1/3), 100000 Kbit (Fa1/4)
Mac Address Move Update Vlan : auto
```

MAC アドレス テーブル移動更新の設定：例

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)# switchport backup interface gigabitethernet1/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次に、設定を確認する例を示します。

```
Switch# show mac-address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 25

DHCP の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

DHCP の設定に関する情報

この章では、スイッチに Dynamic Host Configuration Protocol（DHCP）スヌーピング機能、Option 82 データ挿入機能、および DHCP サーバのポートベースのアドレス割り当て機能を設定する方法について説明します。また、IP ソース ガード機能の設定方法についても説明します。

DHCP スヌーピング

DHCP は、中央のサーバからホスト IP アドレスを動的に割り当てるために LAN 環境で広く使用されており、それによって IP アドレス管理のオーバーヘッドが大幅に軽減されます。DHCP では、ネットワークに接続されたホストだけが IP アドレスを使用し、IP アドレスを永続的にホストに割り当てる必要がなくなるため、限られた IP アドレス空間を節約できます。

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するレイヤ 3 デバイスです。リレー エージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バインディング データベース（DHCP スヌーピング バインディング テーブルとも呼ばれる）の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンド ユーザに接続された信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。

（注）　DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、ネットワークまたはファイアウォールの外側から送信されたメッセージのことです。サービス プロバイダー環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービス プロバイダー ネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカル インターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスは、信頼できないインターフェイスとなります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。

- スイッチが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP Option 82 情報を挿入するエッジ スイッチに接続されているスイッチは、Option 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジ スイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スイッチによって挿入された Option 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチ インターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで、ダイナミック ARP インスペクションや IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジ スイッチとの接続ポートは、信頼できるインターフェイスとして設定する必要があります。

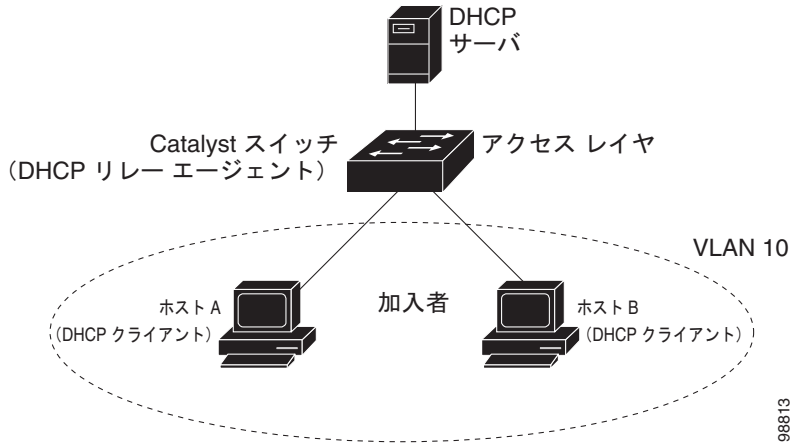
Option 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチ ポートによっても識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。

（注）　DHCP Option 82 機能は、DHCP スヌーピングがグローバルにイネーブルであり、この機能を使用する加入者装置が割り当てられた VLAN でもイネーブルである場合に限りサポートされます。

図 25-1 に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタン イーサネット ネットワークの例を示します。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント（Catalyst スイッチ）にヘルパー アドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 25-1　メトロポリタン イーサネット ネットワークにおける DHCP リレー エージェント



スイッチで DHCP スヌーピング情報オプション Option 82 をイネーブルにすると、次のイベントがこの順序で発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションはスイッチの MAC アドレスであり、回線 ID サブオプションは、パケットの受信ポートの ID である **vlan-mod-port** です。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。次に DHCP サーバは、DHCP 応答内に Option 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、図 25-2 にある次のフィールドの値は変化しません。

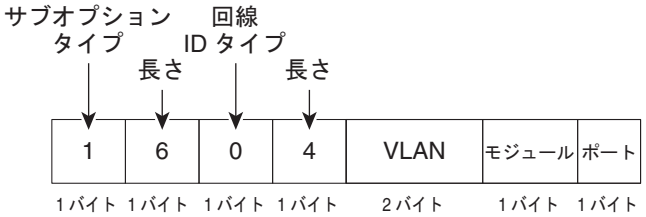
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります。たとえば、8 つの 10/100 ポートと Small Form-Factor Pluggable（SFP）モジュール スロットを備えたスイッチでは、ポート 3 がファスト イーサネット 1/1 ポート、ポート 4 がファスト イーサネット 1/2 ポートなどのようになります。ポート 11 は SFP モジュール スロット 1/1 などになります。

図 25-2 に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット フォーマットを示します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力した場合です。

図 25-2　サブオプションのパケット形式

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット

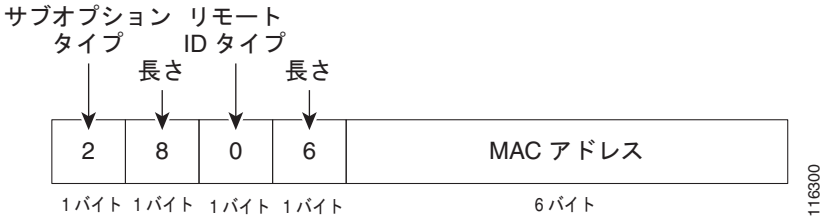


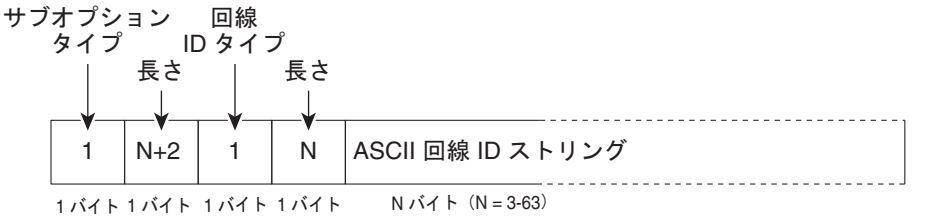
図 25-3 は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらのパケットが使用されます。

パケットでは、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

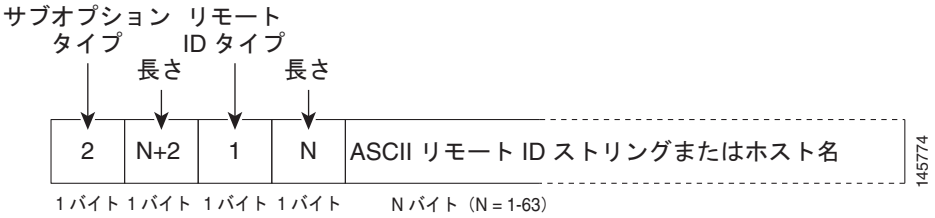
- 回線 ID サブオプション フィールド
  - 回線 ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
  - リモート ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。

図 25-3　ユーザ設定のサブオプションのパケット形式

回線 ID サブオプション フレーム フォーマット（ユーザ設定のストリング）



リモート ID サブオプション フレーム フォーマット（ユーザ設定のストリング）



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、*アドレス バインディング*、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることが可能です。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。データベースには、8192 のバインディングを含めることができます。

各データベース エントリ（*バインディング*）は、IP アドレス、それに関連付けられた MAC アドレス、リース期間（16 進形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。データベース エージェントは、設定された場所のファイルにバインディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトのデータがあり、その後に 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディング データベースがダイナミックバインディングされている場合、スイッチは接続を切断されます。このエージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディング データベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。スイッチはバインディング ファイル内のエントリも更新します。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内（書き込み遅延および中断タイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E interface-id 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB interface-id 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB interface-id 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スイッチがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッド インターフェイスまたは DHCP スヌーピングにおける信頼できるインターフェイスである。

DHCP スヌーピングのデフォルト設定

表 25-1　DHCP スヌーピングのデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要。[1]
DHCP リレー エージェント	イネーブル[2]
DHCP パケット転送アドレス	未設定
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄）。[2]
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。[2]
DHCP スヌーピングをグローバルにイネーブル	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション[3]	ディセーブル
DHCP スヌーピング レート制限	未設定
DHCP スヌーピング信頼状態	信頼できない
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル、設定が必要。 **（注）** スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。

1. スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
2. スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
3. この機能は、スイッチがエッジ スイッチによって Option 82 が挿入されたパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN で DHCP スヌーピングがイネーブルになるまでアクティブになりません。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレー エージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- スイッチで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- スイッチ上で文字数の多いサーキット ID を設定する場合、NVRAM またはフラッシュ メモリに長い文字列が与える影響を考慮してください。サーキット ID 設定がその他のデータと組み合わされた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、エラー メッセージが表示されます。
- スイッチで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントをセットアップする必要があります。
- DHCP リレー エージェントがイネーブルで、DHCP スヌーピングがディセーブルである場合、DHCP Option 82 データ挿入機能はサポートされません。
- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチ ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。
- 信頼できないデバイスが接続されたアグリゲーション スイッチに **ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。
- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。

（注） RSPAN VLAN で DHCP スヌーピングをイネーブルにしないでください。RSPAN VLAN で DHCP スヌーピングをイネーブルにすると、DHCP パケットが RSPAN 宛先ポートに届かない可能性があります。

DHCP スヌーピング バインディング データベースの注意事項

- NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することを推奨します。

- ネットワーク ベースの URL（TFTP や FTP など）については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。空のファイルをサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
- データベースに正しいリース期間が記録されるように、NTP をイネーブルにし、設定することを推奨します。詳細については、「手動での日時の設定」（P.7-9）を参照してください。
- NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。

パケット転送アドレス

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address** *address* インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的なルールは、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

DHCP サーバ ポート ベースのアドレス割り当て

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネット スイッチは、直接接続されたデバイスに接続を提供します。工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代わりのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この代わりのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

DHCP の設定方法

DHCP リレー エージェントの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service dhcp**	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。
ステップ 3	**end**	特権 EXEC モードに戻ります。

パケット転送アドレスの指定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id*	VLAN ID を入力してスイッチの仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** *ip-address subnet-mask*	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 4	**ip helper-address** *address*	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバ アドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface range** *port-range* または **interface** *interface-id*	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**switchport mode access**	ポートの VLAN メンバーシップ モードを定義します。

	コマンド	目的
ステップ 8	**switchport access vlan** *vlan-id*	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
ステップ 9	**end**	特権 EXEC モードに戻ります。

DHCP スヌーピングおよび Option 82 のイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp snooping**	DHCP スヌーピングをグローバルにイネーブル化します。
ステップ 3	**ip dhcp snooping vlan** *vlan-range*	VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 4096 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。
ステップ 4	**ip dhcp snooping information option**	スイッチが DHCP サーバへの DHCP 要求メッセージにおいて DHCP リレー情報（Option 82 フィールド）を挿入および削除できるようにします。これがデフォルト設定です。
ステップ 5	**ip dhcp snooping information option format remote-id [string** *ASCII-string* **|** *hostname*]	（任意）リモート ID サブオプションを設定します。 次のようにリモート ID を設定できます。 • 63 文字までの ASCII 文字列（スペースなし） • スイッチのホスト名 **（注）** ホスト名が 64 文字以上の場合、リモート ID 設定で 63 文字に切り捨てられます。 デフォルトのリモート ID はスイッチ MAC アドレスです。
ステップ 6	**ip dhcp snooping information option allow-untrusted**	（任意）スイッチがエッジ スイッチに接続された集約スイッチである場合、スイッチがエッジ スイッチによって Option 82 情報が挿入された着信 DHCP スヌーピング パケットを受け入れるようにします。 デフォルト設定では無効になっています。 **（注）** このコマンドは、信頼できるデバイスに接続された集約スイッチだけで入力してください。
ステップ 7	**interface** *interface-id*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id** [**override**] **string** *ASCII-string*	（任意）指定したインターフェイスの回線 ID サブオプションを設定します。 1 ～ 4096 の範囲の VLAN ID を使用して、VLAN およびポート ID を指定します。デフォルトの回線 ID はポート ID で、フォーマットは **vlan-mod-port** です。 回線 ID は 3 ～ 63 の ASCII 文字列（スペースなし）を設定できます。 （任意）**override** キーワードは、加入者情報を定義するための TLV 形式に回線 ID サブオプションを挿入したくない場合に使用します。

	コマンド	目的
ステップ 9	**ip dhcp snooping trust**	（任意）インターフェイスを信頼できるインターフェイスまたは信頼できないインターフェイスとして設定します。信頼できないクライアントからのメッセージを受信するようにインターフェイスを設定するには、**no** キーワードを使用します。デフォルト設定は untrusted です。
ステップ 10	**ip dhcp snooping limit rate** *rate*	（任意）インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。指定できる範囲は 1 ～ 2048 です。デフォルトでは、レート制限は設定されません。 **（注）** 信頼できないインターフェイスのレート制限を 1 秒あたり 100 パケット以下に設定することを推奨します。信頼できるインターフェイスのレート制限を設定する場合、DHCP スヌーピングを使った複数の VLAN に割り当てられたトランク ポートでは、レート制限の値を大きくすることが必要になることがあります。
ステップ 11	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**ip dhcp snooping verify mac-address**	（任意）信頼できないポートに着信した DHCP パケットの送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
ステップ 13	**end**	特権 EXEC モードに戻ります。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp snooping database** {**flash:**/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** | **rcp:**//*user*@*host*/*filename*}| **tftp:**//*host*/*filename*	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。 • **flash:**/*filename* • **ftp:**//*user*:*password*@*host*/*filename* • **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** • **rcp:**//*user*@*host*/*filename* • **tftp:**//*host*/*filename*
ステップ 3	**ip dhcp snooping database timeout** *seconds*	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。 デフォルトは 300 秒です。指定できる範囲は 0 ～ 86400 です 無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。
ステップ 4	**ip dhcp snooping database write-delay** *seconds*	バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は 15 ～ 86400 秒です。デフォルトは 300 秒（5 分）です。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*	（任意）DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。*vlan-id* の範囲は 1 ～ 4904 です。*seconds* の範囲は 1 ～ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。 **（注）** このコマンドは、スイッチをテストまたはデバッグするときに使用します。

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp use subscriber-id client-id**	すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。
ステップ 3	**ip dhcp subscriber-id interface-name**	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。
ステップ 4	**interface** *interface-id*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip dhcp server use subscriber-id client-id**	インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

IP アドレスの事前割り当て

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *poolname*	DHCP プール コンフィギュレーション モードを開始し、DHCP プールの名前を定義します。プール名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。
ステップ 3	**network** *network-number* [*mask* | */prefix-length*]	DHCP アドレス プールのサブネット ネットワーク番号およびマスクを指定します。

	コマンド	目的
ステップ 4	**address** *ip-address* **client-id** *string* [**ascii**]	インターフェイス名で指定された DHCP クライアントの IP アドレスを予約します。 *string* : ASCII 値、または 16 進数値のいずれかです。
ステップ 5	**reserved-only**	（任意）DHCP アドレス プールでは、予約されたアドレスだけを使用します。デフォルトでは、プール アドレスは制限されません。
ステップ 6	**end**	特権 EXEC モードに戻ります。

DHCP のモニタリングおよびメンテナンス

コマンド	目的
show interface *interface id*	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバのアドレス バインディングを表示します。
ip dhcp snooping database timeout *seconds*	データベース転送プロセスを打ち切るまでの時間（秒）を指定します。
ip dhcp snooping database write-delay *seconds*	バインディング データベースが変更された後に、転送を遅らせる期間（秒）を指定します。
clear ip dhcp snooping database statistics	DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアします。
renew ip dhcp snooping database	DHCP スヌーピング バインディング データベースを更新します。
show ip dhcp snooping database [**detail**]	DHCP スヌーピング バインディング データベース エージェントのステータスおよび統計情報を表示します。
show ip dhcp snooping	スイッチの DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp pool	DHCP プール設定を確認します。
copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

DHCP の設定例

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化：例

次の例では、加入者 ID が自動的に生成され、DHCP サーバは DHCP メッセージ内のクライアント ID フィールドを一切無視して、その代わりに、加入者の ID を使用しています。加入者 ID はインターフェイスのショート名に基づきます。また、クライアントの事前割り当てされた IP アドレスは 10.1.1.7 です。

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id “Et1/0” ascii
<output truncated>
```

次に、事前割り当てされたアドレスが DHCP プールに正常に予約された例を示します。

```
switch# show ip dhcp pool dhcppool
Pool dhcp pool:
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 0
 Excluded addresses : 4
 Pending event : none
 1 subnet is currently in the pool:
 Current index   IP address range         Leased/Excluded/Total
 10.1.1.1        10.1.1.1 - 10.1.1.254     0     / 4 / 254
 1 reserved address is currently in the pool
 Address         Client
 10.1.1.7 Et1/0
```

DHCP スヌーピングのイネーブル化：例

次に、DHCP スヌーピングをグローバルおよび VLAN 10 でイネーブルにし、ポートのレート制限を 1 秒あたり 100 パケットに設定する例を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS DHCP コマンド	『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』
Cisco IOS DHCP 設定 Cisco IOS DHCP サーバ ポート ベースのアドレス割り当て	『*Cisco IOS IP Configuration Guide*』の「IP Addressing and Services」の章
Cisco IOS DHCP 設定作業リスト	『Cisco IOS IP Configuration Guide』の「*Configuring DHCP*」の章

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

その他の関連資料

CHAPTER 26

ダイナミック ARP インスペクションの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ダイナミック ARP インスペクションの前提条件

- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP（Dynamic Address Resolution Protocol）インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARP インスペクションの制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

ダイナミック ARP インスペクションに関する情報

ダイナミック ARP インスペクション

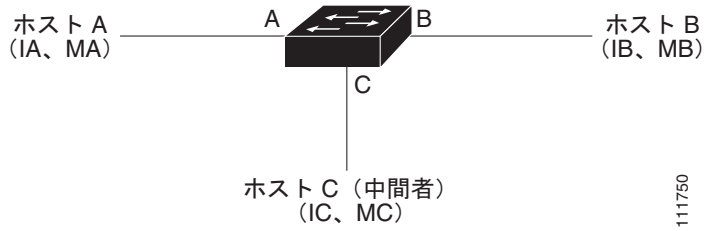
ダイナミック ARP インスペクション（DAI）により、同じ VLAN（仮想 LAN）内の他のポートの無効な ARP 要求や応答を信頼しないようにして、スイッチでの悪意のある攻撃を回避できます。

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。しかし、ARP は、

ARP 要求が受信されなった場合でも、ホストからの余分な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生することがあります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図 26-1 は、ARP キャッシュ ポイズニングの例を示します。

図 26-1　　ARP キャッシュ ポイズニング



ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらの IP アドレス、および MAC アドレスです。たとえば、ホスト A が使用する IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA（または IB）で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。おなじみの *中間者*攻撃です。

DAI は、ネットワーク内の ARP パケットを検証するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の中間者攻撃から保護することができます。

DAI を使用することで、有効な ARP 要求および応答だけがリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

DAI は信頼できるデータベースに保存された IP アドレスと MAC アドレスとの有効なバインディングに基づき、ARP パケットの有効性を判断します。このデータベースを、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースと呼びます。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピン

グにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

インターフェイスの信頼状態とネットワーク セキュリティ

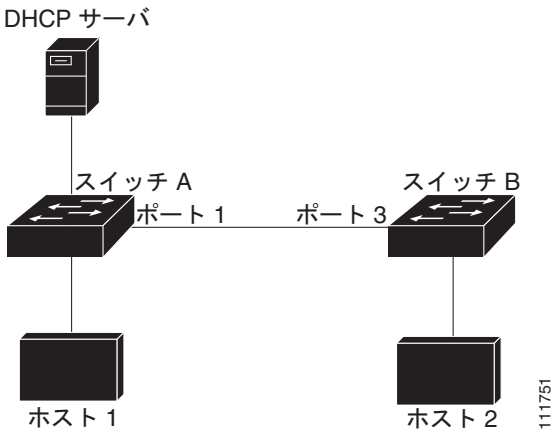
DAI は、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチ ポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティ チェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、**ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

注意　信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

図 26-2 では、スイッチ A とスイッチ B の両方が VLAN に対して DAI を実行しているとします。この VLAN には、ホスト 1 とホスト 2 が含まれています。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B の間のインターフェイスが信頼できない場合、ホスト 1 からの ARP パケットは、スイッチ B によりドロップされます。こうして、ホスト 1 とホスト 2 の間の接続が失われます。

図 26-2　DAI をイネーブルにした VLAN での ARP パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A で DAI が実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、スイッチ B が DAI を実行している場合でも起こりえます。

DAI は、DAI を実行するスイッチに接続された（信頼できないインターフェイス上の）ホストが、ネットワークのその他のホストの ARP キャッシュをポイズニングしないようにします。ただし、ネットワークのその他の場所にあるホストが、DAI を実行するスイッチに接続されたホストのキャッシュをポイズニングする可能性は防止できません。

VLAN のスイッチの一部が DAI を実行し、残りのスイッチは実行していない場合、これらのスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、DAI 非対応スイッチからパケットのバインディングを検証するには、ARP ACL を使用して、DAI を実行するスイッチを設定します。バインディングが判断できない場合は、レイヤ 3 で、DAI スイッチを実行していないスイッチから、DAI を実行しているスイッチを分離します。

（注）　DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチの CPU によって DAI 違反チェックが実行されます。したがって、DoS 攻撃を防ぐために着信 ARP パケット数がレート制限されています。デフォルトでは、信頼できないインターフェイスのレートは 15 パケット/秒（pps）です。信頼できるインターフェイスはレート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。ユーザが介入するまで、ポートはこの状態を維持します。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用すると、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

（注）　インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

DAI では DHCP スヌーピング バインディング データベースを使用して、IP アドレスと MAC アドレスとの有効なバインディングのリストを維持します。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が **ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

廃棄パケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。記録されるパケットの種類を指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。

1 つのログ バッファ エントリで複数のパケットを表すことができます。たとえば、インターフェイスが同じ ARP パラメータを使用して同じ VLAN 上で多数のパケットを受信した場合、スイッチはこれらのパケットを組み合わせて 1 つのエントリとしてログ バッファに格納し、エントリとして 1 つのシステム メッセージを生成します。

ログ バッファでオーバーフローが生じた場合は、1 つのログ イベントがログ バッファ内に収まらなかったことを意味し、**show ip arp inspection log** 特権 EXEC コマンドによる出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに -- が表示されます。このエントリに対しては、その他の統計情報は表示されません。このようなエントリが表示された場合は、ログ バッファ内のエントリ数を増やすか、またはログ レートを高くしてください。

ダイナミック ARP インスペクションのデフォルト設定

表 26-1　ダイナミック ARP インスペクションのデフォルト設定

機能	デフォルト設定
DAI	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチド ネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	DAI をイネーブルにした場合は、拒否または廃棄されたすべての ARP パケットが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギングレート インターバルは、1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

ダイナミック ARP インスペクション設定時の注意事項

- DAI は入力セキュリティ機能であり、出力検査は行いません。
- DAI は、DAI をサポートしないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されているホストに対しては、効果がありません。man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI 検査が有効なドメインを、DAI 検査の行われないドメインから切り離します。これにより、DAI をイネーブルにしたドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- DAI では、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。コンフィギュレーションについては、第 25 章「DHCP の設定」を参照してください。

  DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。
- DAI は、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポートでサポートされます。

（注）　RSPAN VLAN で DAI をイネーブルにしないでください。RSPAN VLAN で DAI をイネーブルにすると、DAI パケットが RSPAN 宛先ポートに届かない可能性があります。

- 物理ポートを EtherChannel ポート チャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポート チャネル内で中断状態のままとなります。ポート チャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポート チャネルで信頼状態を変更すると、スイッチは、チャネルを構成するすべての物理ポートで新しい信頼状態を設定します。
- ポート チャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポート チャネルの設定に照合して検査されます。ポート チャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。
- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートは、各ポートのアグリゲーションを考慮し、DAI をイネーブルにした複数の VLAN でパケットを処理できるように、高い値に設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用して、レートを無制限に設定することもできます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。
- スイッチで DAI をイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラフィックは CPU に送信されます。

ダイナミック ARP インスペクションの設定方法

DHCP 環境でのダイナミック ARP インスペクションの設定

2 つのスイッチがこの機能をサポートする場合の DAI の設定手順を示します。図 26-2（P.26-3）に示すとおり、ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B に接続されています。両方のスイッチは、これらのホストが置かれている VLAN 1 上で DAI を実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。したがって、スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。

はじめる前に

この処理は、両方のスイッチで行う必要があります。この手順は必須です。

	コマンド	目的
ステップ 1	**show cdp neighbors**	スイッチ間の接続を確認します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip arp inspection vlan** vlan-range	VLAN 単位で DAI をイネーブルにします。デフォルトでは、すべての VLAN で DAI はディセーブルです。 *vlan-range*：VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4096 です。 両方のスイッチに同じ VLAN ID を指定します。
ステップ 4	**interface** *interface-id*	他のスイッチに接続されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip arp inspection trust**	スイッチ間の接続を trusted に設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。 スイッチは、信頼できるインターフェイス上の他のスイッチから受信した ARP パケットを確認せず、単純にパケットを転送します。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

非 DHCP 環境での ARP ACL の設定

ここでは、図 26-2（P.26-3）のように、スイッチ B が、DAI も DHCP スヌーピングもサポートしていない場合の DAI の設定方法を示します。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**arp access-list** *acl-name*	ARP ACL を定義し、ARP アクセス リスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセス リストは定義されません。 **（注）** ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 3	**permit ip host** *sender-ip* **mac host** *sender-mac* [**log**]	指定されたホスト（ホスト 2）からの ARP パケットを許可します。 • *sender-ip*：ホスト 2 の IP アドレスを入力します。 • *sender-mac*：ホスト 2 の MAC アドレスを入力します。 • （任意）**log**：パケットがアクセス コントロール エントリ（ACE）に一致すると、ログ バッファにパケットを記録します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで **matchlog** キーワードを設定している場合も、一致したパケットがログ記録されます。詳細については、「ログ バッファの設定」（P.26-12）を参照してください。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 5	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]	VLAN に ARP ACL を適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。 • *arp-acl-name*：ステップ 2 で作成した ACL の名前を指定します。 • *vlan-range*：スイッチとホストが存在する VLAN を指定します。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4096 です。 • （任意）**static**：ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。 IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセス リストで許可された場合だけに許可されます。
ステップ 6	**interface** *interface-id*	スイッチ B に接続されたスイッチ A のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**no ip arp inspection trust**	スイッチ B に接続されたスイッチ A のインターフェイスを untrusted として設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。
ステップ 8	**end**	特権 EXEC モードに戻ります。

着信 ARP パケットのレート制限

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] | **none**}	インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。 デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒です。 • **rate** *pps*：1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ～ 2048 pps です。 • （任意）**burst interval** *seconds*：高レートの ARP パケットの有無についてインターフェイスがモニタリングされる間隔（秒）を指定します。指定できる範囲は 1 ～ 15 です。 • **rate none**：処理できる着信 ARP パケットのレートに上限を設定しません。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**errdisable recovery cause arp-inspection interval** *interval*	（任意）DAI の errdisable ステートからのエラー回復をイネーブルにします。 デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。 **interval** *interval*：errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。
ステップ 6	**exit**	特権 EXEC モードに戻ります。

確認検査の実行

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}	着信 ARP パケットで特定の検査を実行します。デフォルトでは、検証は実行されません。 • **src-mac**：イーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信元 MAC アドレスと比較して検査します。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **dst-mac**：イーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **ip**：ARP 本体を検査し、無効かつ予期されない IP アドレスの有無を確認します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。 少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが **src** および **dst mac** の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって **src** および **dst mac** の検証がディセーブルになります。
ステップ 3	**exit**	特権 EXEC モードに戻ります。

ログ バッファの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip arp inspection log-buffer** {**entries** *number* | **logs** *number* **interval** *seconds*}	DAI のログ バッファを設定します。 デフォルトでは、DAI がイネーブル化されると、拒否またはドロップされた ARP パケットが記録されます。ログ エントリ数は、32 です。システム メッセージ数は、毎秒 5 つに制限されます。ロギング レート インターバルは、1 秒です。 • **entries** *number*：バッファに記録するエントリ数を指定します。指定できる範囲は 0 ～ 1024 です • **logs** *number* **interval** *seconds*：指定されたインターバルでシステム メッセージを生成するエントリの数を表します。 **logs** *number*：指定できる範囲は 0 ～ 1024 です。0 は、エントリはログ バッファ内に入力されますが、システム メッセージが生成されないことを意味します。 **interval** *seconds*：指定できる範囲は 0 ～ 86400 秒（1 日）です。0 は、システム メッセージがただちに生成されることを意味します。この場合、ログ バッファは常に空となります。 インターバル値を 0 に設定すると、ログ値 0 は上書きされます。 **logs** および **interval** の設定は、相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合、X 割る Y（X/Y）のシステム メッセージが毎秒送信されます。そうでない場合、1 つのシステム メッセージが Y 割る X（Y/X）秒ごとに送信されます。
ステップ 3	**ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	VLAN 単位で記録するパケットのタイプを制御します。デフォルトでは、拒否またはドロップされたパケットは、すべて記録されます。*ログに記録される*という表現は、エントリがログ バッファに格納され、システム メッセージが生成されることを意味しています。 • *vlan-range*：VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4096 です。 • **acl-match matchlog**：ACE ロギング設定に基づいてログ パケットを指定します。このコマンドに **matchlog** キーワードを指定して、さらに **permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドに **log** キーワードを指定すると、ACL によって許可または拒否された ARP パケットが記録されます。 • **acl-match none**：ACL と一致したパケットを記録しません。 • **dhcp-bindings all**：DHCP バインディングと一致したすべてのパケットが記録されます。 • **dhcp-bindings none**：DHCP バインディングと一致したパケットは記録されません。 • **dhcp-bindings permit**：DHCP バインディングによって許可されたパケットが記録されます。
ステップ 4	**exit**	特権 EXEC モードに戻ります。

ダイナミック ARP インスペクションのモニタリングおよびメンテナンス

コマンド	説明
clear ip arp inspection log	DAI のログ バッファを消去します。
clear ip arp inspection statistics	DAI 統計情報をクリアします。
show arp access-list [*acl-name*]	ARP ACL についての詳細情報を表示します。
show errdisable recovery	errdisable 回復タイマー情報を表示します。
show ip arp inspection interfaces [*interface-id*]	指定のインターフェイス、またはすべてのインターフェイスに対して、ARP パケットの信頼状態およびレート制限を表示します。
show ip arp inspection log	DAI ログ バッファの設定および内容を表示します。
show ip arp inspection vlan *vlan-range*	指定の VLAN に対し、DAI の設定内容および動作状態を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN だけの情報が表示されます。
show ip arp inspection statistics [**vlan** *vlan-range*]	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN だけの情報が表示されます。
show ip dhcp snooping binding	DHCP バインディングを確認します。

ダイナミック ARP インスペクションの設定例

DHCP 環境でのダイナミック ARP インスペクションの設定：例

次の例では、VLAN 1 のスイッチ A で DAI を設定する方法を示します。スイッチ B でも同様の手順を実行します。

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境での ARP ACL の設定：例

次に、スイッチ A で ARP ACL host2 を設定して、ホスト 2（IP アドレス 1.1.1.1、および MAC アドレス 0001.0001.0001）からの ARP パケットを許可し、この ACL を VLAN 1 に適用してから、スイッチ A のポート 1 を信頼できないものに設定する例を示します。

```
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet0/1
```

```
Switch(config-if)# no ip arp inspection trust
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
DHCP の設定	『Configuring DHCP on the IE 2000 Switch』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

その他の関連資料

CHAPTER 27

IP ソース ガードの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IP ソース ガードの前提条件

- スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。この要件は、スタティック ホストの IPSG がレイヤ 2 アクセス ポート上で使用される場合にも適用されます。

IP ソース ガードの制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- IP ソース ガード（IPSG）は、アクセス ポートおよびトランク ポートを含むレイヤ 2 ポートだけでサポートされます。
- スタティック ホストの IPSG は、アップリンク ポートまたはトランク ポートでは使用しないでください。

IP ソース ガードの概要

IP ソース ガード

IPSG は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることにより、非ルーテッド レイヤ 2 インターフェイスでの IP トラフィックを制限するセキュリティ機能です。IPSG を使用して、ホストが、そのネイバーの IP アドレスの使用を試みた場合のトラフィック攻撃を防ぐことができます。

信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合は、IPSG をイネーブルにできます。インターフェイス上で IPSG をイネーブルにすると、スイッチは、DHCP スヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。ポート アクセス コントロール リスト（ACL）は、このインターフェイスに適用されます。ポート ACL は、IP ソース バインディング テーブルに送信元 IP アドレスを持つ IP トラフィックだけを許可し、その他のトラフィックはすべて拒否します。

（注）　ポート ACL は、同じインターフェイスに影響を与えるその他のルータ ACL や VLAN マップよりも優先されます。

IP ソース バインディング テーブル バインディングは、DHCP スヌーピングにより学習されるか、または手動で設定されます（スタティック IP ソース バインディング）。このテーブルのエントリはすべて、MAC アドレスと VLAN 番号が関連付けられた IP アドレスを持ちます。スイッチは、IPSG がイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

送信元 IP アドレスと送信元 IP および MAC アドレス フィルタリングで IPSG を設定できます。

送信元 IP アドレスのフィルタリング

IPSG でこのオプションがイネーブルにされている場合、IP トラフィックは、送信元 IP アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP が DHCP スヌーピング バインディング データベースのエントリ、または IP ソース バインディング テーブルのバインディングと一致する場合に、IP トラフィックを転送します。

インターフェイス上で、DHCP スヌーピング バインディング、またはスタティック IP ソース バインディングが追加、変更、または削除された場合、スイッチは IP ソース バインディングの変更を使用して、ポート ACL を変更し、このポート ACL をインターフェイスに再度適用します。

IP ソース バインディング（DHCP スヌーピングにより動的に学習された、または手動で設定されたもの）が設定されていないインターフェイス上で IPSG をイネーブルにした場合、スイッチはこのインターフェイス上で IP トラフィックすべてを拒否するポート ACL を作成し、適用します。IPSG をディセーブルにした場合、スイッチはインターフェイスからポート ACL を削除します。

送信元 IP および MAC アドレス フィルタリング

IP トラフィックは、送信元 IP アドレスおよび MAC アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP アドレスと MAC アドレスが IP ソース バインディング テーブルのエントリと一致する場合だけ、トラフィックを転送します。

アドレス フィルタリングがイネーブルの場合、スイッチは IP トラフィックと非 IP トラフィックをフィルタリングします。IP パケット、または非 IP パケットの送信元 MAC アドレスが有効な IP ソース バインディングと一致する場合、スイッチはこのパケットを転送します。DHCP パケットを除き、その他の種類のパケットはすべて、スイッチによりドロップされます。

スイッチは、送信元 MAC アドレスのフィルタリングにポート セキュリティを使用します。ポート セキュリティ違反が発生した場合、インターフェイスはシャットダウンします。

スタティック ホスト用 IP ソース ガード

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングします。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エントリに依存しています。このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティック エントリを作成します。また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイヤ 3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、IP DHCP スヌーピング テーブルで使用できる DHCP によって割り当てられた IP アドレスを受信すると、同じエントリが IP デバイス トラッキング テーブルで学習されます。**show ip device tracking all** EXEC コマンドを入力する場合、IP デバイス トラッキング テーブルでエントリが ACTIVE として表示されます。

（注） 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。この無効なパケットには、ソース アドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティング システムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これらはデバイス トラッキング データベースに保存されます。指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングとともに使用できます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガード設定時の注意事項

- IP ソース ガードは、デフォルトではディセーブルに設定されています。
- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッド インターフェイスで **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを入力すると、次のエラー メッセージが表示されます。

  ```
  Static IP source binding can only be configured on switch port.
  ```

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。
- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。

  （注）　IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、インターフェイスの DHCP スヌーピングとポート セキュリティをイネーブルにする必要があります。また、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力して、DHCP サーバに確実に Option 82 をサポートさせる必要もあります。MAC アドレス フィルタリングとともに IP ソース ガードをイネーブルにした場合、DHCP ホストによりリースが認可されるまで、このホストの MAC アドレスは学習されません。サーバからホストにパケットを転送する場合、DHCP スヌーピングは Option 82 データを使用して、ホスト ポートを識別します。
- プライベート VLAN が設定されているインターフェイスに IP ソース ガードを設定した場合、ポート セキュリティはサポートされません。
- EtherChannels では、IP ソース ガードはサポートされません。
- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。
- Ternary Content Addressable Memory（TCAM）エントリの数が最大値を超えた場合、CPU の使用率は増加します。

IP ソース ガードの設定方法

IP ソース ガードのイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ip verify source** または **ip verify source port-security**	送信元 IP アドレスのフィルタリングによる IPSG をイネーブルにします。 送信元 IP アドレスと MAC アドレスのフィルタリングによる IPSG をイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して IPSG とポート セキュリティの両方をイネーブルにする場合は、次の 2 つの警告があります。 • DHCP サーバは Option 82 をサポートする必要があります。サポートしていない場合、クライアントには IP アドレスを割り当てることができません。 • DHCP パケットの MAC アドレスが、セキュア アドレスとして学習されることはありません。DHCP クライアントの MAC アドレスがセキュア アドレスとして学習されるには、スイッチが非 DHCP データ トラフィックを受信した場合だけです。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **inteface** *interface-id*	スタティック IP ソース バインディングを追加します。 スタティック バインディングごとにこのコマンドを入力します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking**	IP ホスト テーブルを開き、IP デバイス トラッキングをグローバルにイネーブルにします。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	アクセスとしてポートを設定します。
ステップ 5	**switchport access vlan** *vlan-id*	このポートに VLAN を設定します。

	コマンド	目的
ステップ 6	**ip verify source tracking port-security**	MAC アドレス フィルタリングとともにスタティック ホスト用 IPSG をイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して、IPSG とポート セキュリティの両方をイネーブルにする場合、 • DHCP サーバは Option 82 をサポートする必要があります。サポートしていない場合、クライアントには IP アドレスを割り当てることができません。 • DHCP パケットの MAC アドレスが、セキュア アドレスとして学習されることはありません。DHCP クライアントの MAC アドレスがセキュア アドレスとして学習されるには、スイッチが非 DHCP データ トラフィックを受信した場合だけです。
ステップ 7	**ip device tracking maximum** *number*	そのポートで、IP デバイス トラッキング テーブルにより許可されるスタティック IP 数の上限を設定します。指定できる範囲は 1 ～ 10 です。最大値は 10 です。 （注）　**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 8	**switchport port-security**	（任意）このポートのポート セキュリティをアクティブにします。
ステップ 9	**switchport port-security maximum** *value*	（任意）このポートに対する MAC アドレスの最大値を設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip verify source interface** *interface-id*	設定を確認し、スタティック ホストの IPSG の許可 ACL を表示します。
ステップ 12	**show ip device track all [active | inactive] count**	スイッチ インターフェイス上の指定ホストの IP/MAC バインディングを表示して、設定を確認します。 • **all active**：アクティブな IP または MAC バインディング エントリだけを表示します。 • **all inactive**：非アクティブな IP または MAC バインディング エントリだけを表示します。 • **all**：アクティブおよび非アクティブな IP または MAC バインディング エントリを表示します。

プライベート VLAN ホスト ポート上のスタティック ホストの IP ソース ガードの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2	**vlan** *vlan-id1*	VLAN コンフィギュレーション モードを開始します。
ステップ 3	**private-vlan primary**	プライマリ VLAN をプライベート VLAN ポート上に設定します。
ステップ 4	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 5	**vlan** *vlan-id2*	別の VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 6	**private-vlan isolated**	独立 VLAN をプライベート VLAN ポート上に設定します。
ステップ 7	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 8	**vlan** *vlan-id1*	コンフィギュレーション VLAN モードを開始します。
ステップ 9	**private-vlan association 201**	VLAN を独立プライベート VLAN ポートに関連付けます。
ステップ 10	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 11	**interface fastEthernet** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**switchport mode private-vlan host**	（任意）ポートをプライベート VLAN ホストとして設定します。
ステップ 13	**switchport private-vlan host-association** *vlan-id1 vlan-id2*	（任意）このポートに、対応するプライベート VLAN を関連付けます。
ステップ 14	**ip device tracking maximum** *number*	このポートに対して IP デバイス トラッキング テーブルに保持できるスタティック IP の数の最大値を設定します。 最大値は 10 です。 **（注）** スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *number* インターフェイス コマンドをグローバルに設定する必要があります。
ステップ 15	**ip verify source tracking [port-security]**	このポート上のスタティック ホストの IPSG と MAC アドレス フィルタリングをアクティブにします。
ステップ 16	**end**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 17	**show ip device tracking all**	設定を確認します。
ステップ 18	**show ip verify source interface** *interface-id*	IPSG の設定を確認し、スタティック ホストの IPSG の許可 ACL を表示します。

IP ソース ガードのモニタリングおよびメンテナンス

コマンド	目的
show ip device tracking	すべてのインターフェイスに対してアクティブな IP または MAC バインディング エントリを表示します。
show ip source binding	スイッチ上の IP ソース バインディングを表示します。
show ip verify source	スイッチ上の IP ソース ガード設定を表示します。
copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

IP ソース ガードの設定例

送信元 IP アドレスと MAC アドレスのフィルタリングによる IPSG のイネーブル化：例

次に、送信元 IP および MAC フィルタリングにより VLAN 10 および 11 で IPSG をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet1/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/1
Switch(config)# end
```

スタティック ホストによる IPSG のディセーブル化：例

次に、インターフェイス上でスタティック ホストを使って IPSG を停止する例を示します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

スタティック ホストの IPSG のイネーブル化：例

次に、ポート上でスタティック ホストを使って IPSG をイネーブルにする例を示します。

```
Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security
```

次に、レイヤ 2 アクセス ポートで IP フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、インターフェイス Gi0/3 で有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip trk       active       40.1.1.24                           10
Gi0/3      ip trk       active       40.1.1.20                           10
Gi0/3      ip trk       active       40.1.1.21                           10
```

次に、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、インターフェイス Gi0/3 で有効な IP-MAC バインディングを確認してから、このインターフェイス上で上限に達したバインディングの数を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Gi0/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Gi0/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Gi0/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Gi0/3      ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  1
```

IP または MAC バインディング エントリの表示：例

この例は、すべてのインターフェイスに対する IP または MAC バインディング エントリをすべて表示します。CLI はアクティブ エントリと非アクティブ エントリの両方を表示します。インターフェイスでホストが学習されると、この新しいエントリは、アクティブとマークされます。このホストをこのインターフェイスから切断し、別のインターフェイスに接続すると、ホストを検出すると同時に、新しい IP または MAC バインディング エントリがアクティブとして表示されます。以前のインターフェイスでは、このホストに対する古いエントリが非アクティブとマークされます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

```
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

この例は、すべてのインターフェイスに対するアクティブな IP または MAC バインディング エントリをすべて表示します。

```
Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
```

この例は、すべてのインターフェイスに対する非アクティブな IP または MAC バインディング エントリをすべて表示します。このホストはまず、GigabitEthernet 0/1 で学習され、次に GigabitEthernet 0/2 で移動されます。GigabitEthernet 0/1 で学習された IP または MAC バインディング エントリは非アクティブとマークされます。

```
Switch# show ip device tracking all inactive
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

この例は、すべてのインターフェイスに対するすべての IP デバイス トラッキング ホスト エントリの総数を表示します。

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
-----------------------------------------------------------------------
  Interface           Maximum Limit           Number of Entries
-----------------------------------------------------------------------
Gi0/3                  5
```

スタティック ホストの IPSG のイネーブル化：例

次に、プライベート VLAN ホスト ポート上でスタティック ホストの IPSG と IP フィルタをイネーブルにする例を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int fastEthernet 4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface               STATE
-----------------------------------------------------------------------
40.1.1.24       0000.0000.0304  200  FastEthernet0/3        ACTIVE
40.1.1.20       0000.0000.0305  200  FastEthernet0/3        ACTIVE
40.1.1.21       0000.0000.0306  200  FastEthernet0/3        ACTIVE
40.1.1.22       0000.0000.0307  200  FastEthernet0/3        ACTIVE
40.1.1.23       0000.0000.0308  200  FastEthernet0/3        ACTIVE
```

出力には、インターフェイス Fa0/3 上で学習された 5 つの有効な IP-MAC バインディングが表示されています。プライベート VLAN の場合は、バインディングにはプライマリ VLAN ID が関連付けられます。この例では、プライマリ VLAN ID である 200 が表に表示されています。

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/3      ip trk       active       40.1.1.23                           200
Fa0/3      ip trk       active       40.1.1.24                           200
Fa0/3      ip trk       active       40.1.1.20                           200
Fa0/3      ip trk       active       40.1.1.21                           200
Fa0/3      ip trk       active       40.1.1.22                           200
Fa0/3      ip trk       active       40.1.1.23                           201
Fa0/3      ip trk       active       40.1.1.24                           201
Fa0/3      ip trk       active       40.1.1.20                           201
Fa0/3      ip trk       active       40.1.1.21                           201
Fa0/30/3   ip trk       active       40.1.1.22                           201
```

この出力からは、5 つの有効な IP-MAC バインディングはプライマリとセカンダリの両方の VLAN 上にあることがわかります。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 28

IGMP スヌーピングおよび MVR の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IGMP スヌーピングおよび MVR の制約事項

- Multicast VLAN Registration（MVR）機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定するには、**ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。最大数をデフォルト設定（制限なし）に戻すには、このコマンドの **no** 形式を使用します。この制限が適用されるのはレイヤ 2 ポートだけです。ルーテッド ポートや SVI には IGMP グループの最大数を設定できません。このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

IGMP スヌーピングおよび MVR に関する情報

この章では、ローカル インターネット グループ管理プロトコル（IGMP）スヌーピングのアプリケーションであるマルチキャスト VLAN レジストレーション（MVR）など、スイッチに IGMP スヌーピングを設定する方法について説明します。また、IGMP フィルタリングを使用したマルチキャスト グループ メンバーシップの制御と、IGMP スロットリング アクションの設定手順についても説明します。

（注） IP Version 6（IPv6）トラフィックでは、Multicast Listener Discovery（MLD）スヌーピングが IPv4 トラフィックに対する IGMP スヌーピングと同じ機能を実行します。MLD スヌーピングの詳細については、第 44 章「IPv6 MLD スヌーピングの設定」を参照してください。

（注）　IGMP スヌーピング、MVR などの機能を使用して IP マルチキャスト グループ アドレスを管理することもできますし、スタティック IP アドレスを使用することもできます。

IGMP スヌーピング

レイヤ 2 スイッチは IGMP スヌーピングを使用して、レイヤ 2 インターフェイスを動的に設定し、マルチキャスト トラフィックが IP マルチキャスト デバイスと対応付けられたインターフェイスにだけ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを制限できます。名称が示すとおり、IGMP スヌーピングの場合は、LAN スイッチでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャスト グループとメンバ ポートを追跡する必要があります。特定のマルチキャスト グループについて、ホストから IGMP レポートを受信したスイッチは、ホストのポート番号を転送テーブル エントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブル エントリからホスト ポートを削除します。マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。

（注）　IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャスト ルータは、すべての VLAN に一般クエリーを定期的に送信します。このマルチキャスト トラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。スイッチは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

スイッチは、MAC アドレスに基づくグループではなく、IP マルチキャスト グループに基づくブリッジングをサポートしています。マルチキャスト MAC アドレスに基づくグループの場合、設定されている IP アドレスを設定済みの MAC アドレス（エイリアス）または予約済みのマルチキャスト MAC アドレス（224.0.0.xxx の範囲内）に変換すると、コマンドがエラーになります。スイッチでは IP マルチキャスト グループを使用するので、アドレス エイリアスの問題は発生しません。

IGMP スヌーピングによって、IP マルチキャスト グループは動的に学習されます。ただし、**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用すると、マルチキャスト グループを静的に設定できます。グループ メンバーシップをマルチキャスト グループ アドレスに静的に指定すると、その設定値は IGMP スヌーピングによる自動操作より優先されます。マルチキャスト グループ メンバーシップのリストは、ユーザが定義した設定値および IGMP スヌーピングによって学習された設定値の両方で構成できます。

マルチキャスト トラフィックはルーティングする必要がないのでマルチキャスト インターフェイスを使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピング クエリーを設定できます。IGMP スヌーピング クエリアの詳細については、「IGMP スヌーピング クエリアの設定」（P.28-17）を参照してください。

ポート スパニングツリー、ポート グループ、または VLAN ID が変更された場合、VLAN 上のこのポートから IGMP スヌーピングで学習されたマルチキャスト グループは削除されます。

IGMP 即時脱退をイネーブルに設定すると、スイッチはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。

IGMP のバージョン

スイッチは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。これら 3 つのバージョンは、スイッチ上でそれぞれ相互運用できます。たとえば、IGMPv2 スイッチ上で IGMP スヌーピングがイネーブルの場合、このスイッチが IGMPv3 レポートをホストから受信すると、この IGMPv3 レポートをマルチキャスト ルータへ転送できます。

（注）　スイッチは、宛先マルチキャスト MAC アドレスのみに基づいて IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。

IGMPv3 スイッチは、Basic IGMPv3 Snooping Support（BISS）をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバーシップ レポート メッセージをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャスト トラフィックのフラッディングは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。

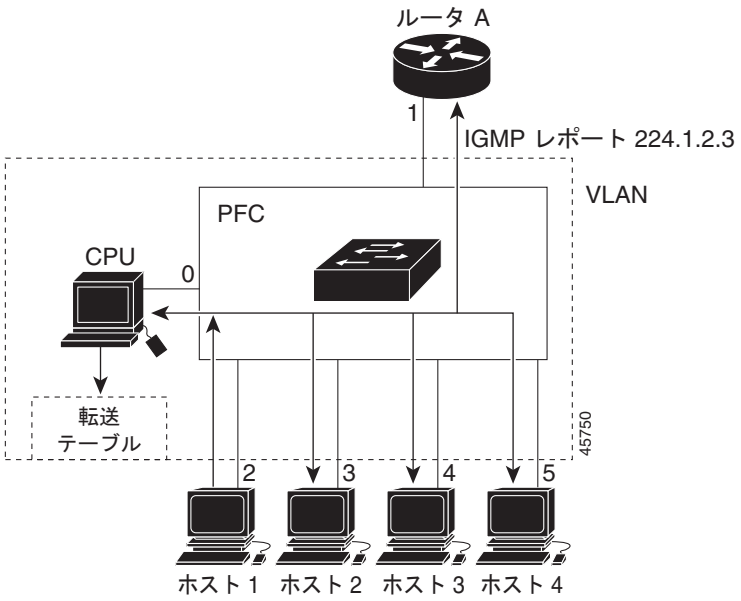
（注）　IGMP フィルタリングまたは MVR が実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行しているデバイスとメッセージの送受信を行うことができます。

マルチキャスト グループへの加入

スイッチに接続したホストが IP マルチキャスト グループに加入し、なおかつそのホストが IGMP バージョン 2 クライアントの場合、ホストは加入する IP マルチキャスト グループを指定した非送信請求 IGMP Join メッセージを送信します。別の方法として、ルータから一般クエリーを受信したスイッチは、そのクエリーを VLAN 内のすべてのポートに転送します。IGMP バージョン 1 またはバージョン 2 のホストがマルチキャスト グループに加入する場合、ホストはスイッチに Join メッセージを送信することによって応答します。スイッチの CPU は、そのグループのマルチキャスト転送テーブル エントリがまだ存在していないのであれば、エントリを作成します。CPU はさらに、Join メッセージを受信したインターフェイスを転送テーブル エントリに追加します。そのインターフェイスと対応付けられたホストが、そのマルチキャスト グループ用のマルチキャスト トラフィックを受信します。図 28-1 を参照してください。

図 28-1　最初の IGMP Join メッセージ



ルータ A がスイッチに一般クエリーを送り、スイッチはそのクエリーをポート 2 ～ 5、つまり同一 VLAN のすべてのメンバに転送します。ホスト 1 はマルチキャスト グループ 224.1.2.3 に加入するために、グループに IGMP メンバーシップ レポート（IGMP Join メッセージ）をマルチキャストします。スイッチの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します（表 28-1 を参照）。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 28-1　IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1、2

スイッチのハードウェアは、マルチキャスト グループの他のパケットと IGMP 情報パケットを区別できます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛ての、IGMP パケットではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジンに指示します。

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 IGMP Join メッセージを送信する場合（図 28-2 を参照）、CPU がそのメッセージを受け取り、ホスト 4 のポート番号を転送テーブルに追加します（表 28-2 を参照）。転送テーブルによって、CPU だけに IGMP メッセージが転送されるので、スイッチ上の他のポートにメッセージがフラッディングされることはありません。認識されているマルチキャスト トラフィックは、CPU 宛てではなくグループ宛てに転送されます。

図 28-2　2 番めのホストのマルチキャスト グループへの加入

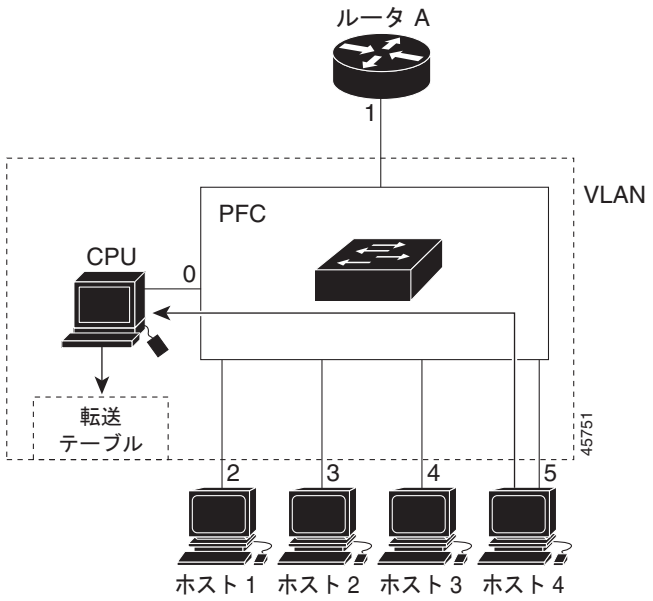


表 28-2　更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

マルチキャスト グループからの脱退

ルータはマルチキャスト一般クエリーを定期的に送信し、スイッチはそれらのクエリーを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくとも 1 つのホストがマルチキャスト トラフィックを受信しなければならない場合、ルータは VLAN に引き続き、マルチキャスト トラフィックを転送します。スイッチは、その IGMP スヌーピングによって維持された IP マルチキャスト グループの転送テーブルで指定されたホストに対してだけ、マルチキャスト グループ トラフィックを転送します。

ホストがマルチキャスト グループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。ホストから Leave メッセージを受信したスイッチは、グループ固有のクエリーを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャスト グループのトラフィックに関与しているかどうかを学習します。スイッチはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャスト トラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

即時脱退

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。

スイッチは IGMP スヌーピングの即時脱退を使用して、先にスイッチからインターフェイスにグループ固有のクエリーを送信しなくても、Leave メッセージを送信するインターフェイスを転送テーブルから削除できるようにします。VLAN インターフェイスは、最初の Leave メッセージで指定されたマル

チキャスト グループのマルチキャスト ツリーからプルーニングされます。即時脱退によって、複数のマルチキャスト グループが同時に使用されている場合でも、スイッチド ネットワークのすべてのホストに最適な帯域幅管理が保証されます。

（注）　即時脱退機能を使用するのは、各ポートに接続されているホストが 1 つだけの VLAN に限定してください。1 つのポートに複数のホストが接続されている VLAN で即時脱退機能をイネーブルにすると、一部のホストが誤って切断される可能性があります。

IGMP 即時脱退をイネーブルに設定すると、スイッチはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。

IGMP 脱退タイマーの設定

まだ指定のマルチキャスト グループに関心があるかどうかを確認するために、グループ固有のクエリーを送信した後のスイッチの待機時間を設定できます。IGMP 脱退応答時間は、100 ～ 5000 ミリ秒の間で設定できます。デフォルトの脱退時間は 1000 ミリ秒です。タイマーはグローバルにまたは VLAN 単位で設定できますが、VLAN に脱退時間を設定すると、グローバルに設定した脱退時間は上書きされます。

ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。

（注）　IGMP の脱退時間の設定は、IGMP バージョン 2 が稼働しているホストでのみサポートされます。

IGMP レポート抑制

（注）　IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは、IGMP レポート抑制を使用して、1 つのマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。

マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

IGMP レポート抑制をディセーブルにすると、すべての IGMP レポートはマルチキャスト ルータに転送されます。設定手順については、「IGMP レポート抑制のディセーブル化」（P.28-18）を参照してください。

IGMP スヌーピングのデフォルト設定

表 28-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 28-3　IGMP スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブル
マルチキャスト ルータ	未設定
マルチキャスト ルータの学習（スヌーピング）方式	PIM-DVMRP
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	未設定
TCN[1] フラッド クエリー カウント	2
TCN クエリー送信要求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	イネーブル

1. TCN = Topology Change Notification（トポロジ変更通知）

スヌーピング方式

マルチキャスト対応のルータ ポートは、レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。スイッチは、次のいずれかの方法でポートを学習します。

- IGMP クエリー、Protocol Independent Multicast（PIM）パケット、および Distance Vector Multicast Routing Protocol（DVMRP）パケットのスヌーピング
- 他のルータからの Cisco Group Management Protocol（CGMP）パケットの待ち受け
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャスト ルータ ポートへの静的な接続

IGMP クエリーおよび PIM パケットと DVMRP パケットのスヌーピング、または CGMP self-join パケットまたは proxy-join パケットのいずれかの待ち受けを行うように、スイッチを設定できます。デフォルトでは、スイッチはすべての VLAN 上の PIM パケットと DVMRP パケットをスヌーピングします。CGMP パケットだけでマルチキャスト ルータ ポートを学習するには、**ip igmp snooping vlan** *vlan-id* **mrouter learn cgmp** グローバル コンフィギュレーション コマンドを使用します。このコマンドを入力すると、ルータは CGMP self-join パケットおよび CGMP proxy-join パケットだけを待ち受け、その他の CGMP パケットは待ち受けません。PIM パケットと DVMRP パケットだけでマルチキャスト ルータ ポートを学習するには、**ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp** グローバル コンフィギュレーション コマンドを使用します。

（注）　学習方法として CGMP を使用する場合で、なおかつ VLAN に CGMP プロキシ対応のマルチキャスト ルータがない場合は、**ip cgmp router-only** コマンドを入力し、ルータに動的にアクセスする必要があります。

TCN イベント後のマルチキャスト フラッディング時間

ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知（TCN）イベント後にフラッディングするマルチキャスト トラフィックの時間を制御できます。このコマンドは、TCN イベント後にフラッディングするマルチキャスト データのトラフィックに対し、一般クエリー数を設定します。クライアントが場所を変更することで同ポートの受信者がブロックされた後、現在転送中の場合、またはポートが Leave メッセージを送信せずにダウンした場合などが、TCN イベントに該当します。

ip igmp snooping tcn flood query count コマンドを使用して TCN フラッド クエリー カウントを 1 に設定した場合、1 つの一般的クエリーの受信後にフラッディングが停止します。カウントを 7 に設定した場合、一般クエリーを 7 つ受信するまでフラッディングが続きます。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

TCN のフラッディング モード

トポロジの変更が発生した場合、スパニングツリーのルートは特別な IGMP Leave メッセージ（グローバル Leave メッセージ）をグループ マルチキャスト アドレス 0.0.0.0. に送信します。ただし、**ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドをイネーブルにしている場合、スイッチはスパニングツリーのルートであるかどうかにかかわらず、グローバル Leave メッセージを送信します。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを送信して、TCN 中のフラッディング モードからできるだけ早く回復するようにします。スイッチがスパニングツリーのルートであれば、このコンフィギュレーション コマンドに関係なく、Leave メッセージが常に送信されます。デフォルトでは、クエリー送信要求はディセーブルに設定されています。

TCN イベント中のマルチキャスト フラッディング

スイッチは TCN を受信すると、一般クエリーを 2 つ受信するまで、すべてのポートに対してマルチキャスト トラフィックをフラッディングします。異なるマルチキャスト グループのホストに接続しているポートが複数ある場合、リンク範囲を超えてスイッチによるフラッディングが行われ、パケット損失が発生する可能性があります。その場合、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用して、この状態を制御できます。

IGMP スヌーピング クエリアの注意事項

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN スイッチ仮想インターフェイス（SVI）IP アドレス（存在する場合）を使用しようとします。SVI IP アドレスが存在しない場合、スイッチはスイッチ上で設定された利用可能な最初の IP アドレスを使用します。利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピング クエリアはスイッチ上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアはネットワークにマルチキャスト ルータの存在を検出すると、非クエリア ステートになります。

- 管理上イネーブルである場合、IGMP スヌーピング クエリアは操作上、次の状況でディセーブル ステートになります。
  - IGMP スヌーピングが VLAN でディセーブルの場合
  - PIM が、VLAN に対応する SVI でイネーブルの場合

IGMP レポート抑制

IGMP レポート抑制はデフォルトでイネーブルです。IGMP レポート抑制がイネーブルの場合、スイッチは、マルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけ転送します。IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。

マルチキャスト VLAN レジストレーション

（注）　この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

MVR は、イーサネット リング ベースのサービス プロバイダー ネットワークにおいて、マルチキャスト トラフィックを大規模展開する用途（サービス プロバイダー ネットワークによる複数のテレビ チャネルのブロードキャストなど）を想定して開発されました。MVR によってポート上の加入者は、ネットワークワイドなマルチキャスト VLAN 上のマルチキャスト ストリームに加入し、脱退できます。加入者は別個の VLAN 上にありながら、ネットワークで単一マルチキャスト VLAN を共有できます。MVR によって、マルチキャスト VLAN でマルチキャスト ストリームを連続送信する能力が得られますが、ストリームと加入者の VLAN は、帯域幅およびセキュリティ上の理由で分離されます。

MVR では、加入者ポートが IGMP Join および Leave メッセージを送信することによって、マルチキャスト ストリームへの加入および脱退（Join および Leave）を行うことが前提です。これらのメッセージは、イーサネットで接続され、IGMP バージョン 2 に準拠しているホストから発信できます。MVR は IGMP スヌーピングの基本メカニズムで動作しますが、この 2 つの機能はそれぞれ単独で動作します。それぞれ他方の機能の動作に影響を与えずに、イネーブルまたはディセーブルにできます。ただし、IGMP スヌーピングと MVR が両方ともイネーブルの場合、MVR は MVR 環境で設定されたマルチキャスト グループが送信した Join および Leave メッセージだけに反応します。他のマルチキャスト グループから送信された Join および Leave メッセージはすべて、IGMP スヌーピングが管理します。

スイッチの CPU は、MVR IP マルチキャストストリームとそれに対応するスイッチ転送テーブル内の IP マルチキャスト グループを識別し、IGMP メッセージを代行受信し、転送テーブルを変更して、マルチキャスト ストリームの受信側としての加入者を追加または削除します。受信側が送信元と異なる VLAN 上に存在している場合でも同じです。この転送動作により、異なる VLAN の間でトラフィックを選択して伝送できます。

スイッチの MVR 動作は、互換モードまたはダイナミック モードに設定できます。

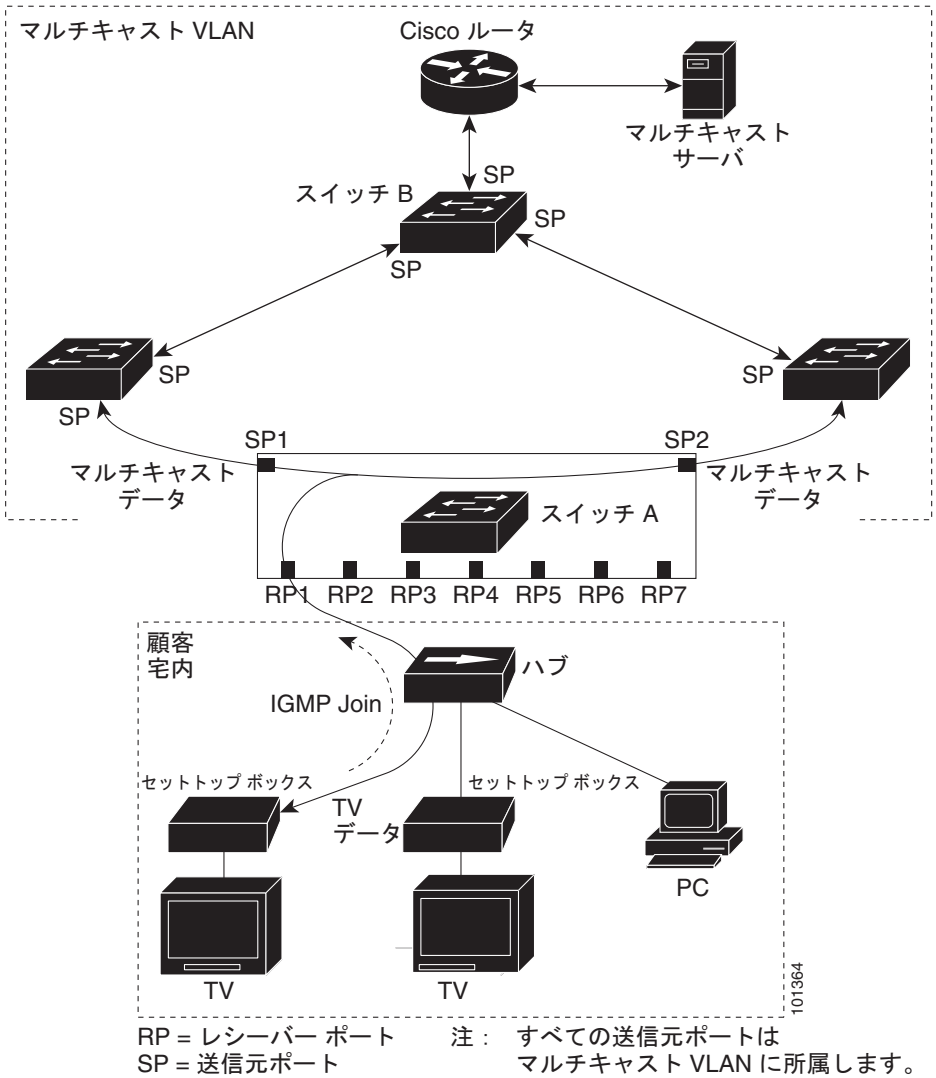
- 互換モードの場合、MVR ホストが受信したマルチキャスト データはすべての MVR データ ポートに転送されます。MVR データ ポートの MVR ホスト メンバーシップは無関係です。マルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入しているレシーバ ポートだけに転送されます。MVR ホストから受信した IGMP レポートが、スイッチに設定された MVR データ ポートから転送されることはありません。
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入している MVR データおよびクライアント ポートから転送されます。それ以外のポートからは転送されません。MVR ホストから受信した IGMP レポートも、スイッチのすべての MVR データ ポートから転送されます。したがって、互換モードでスイッチを稼働させた場合と異なり、MVR データ ポート リンクで不要な帯域幅を使用しなくてすみます。

MVR に関与するのはレイヤ 2 ポートだけです。ポートを MVR 受信ポートとして設定する必要があります。各スイッチでサポートされる MVR マルチキャスト VLAN は、1 つだけです。

マルチキャスト TV アプリケーションでの MVR

マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備したテレビでマルチキャスト ストリームを受信できます。1 つの加入者ポートに複数のセットトップ ボックスまたは PC を接続できます。加入者ポートは、MVR 受信ポートとして設定されたスイッチ ポートです。図 28-3 に構成例を示します。Dynamic Host Configuration Protocol（DHCP）によって、セットトップ ボックスまたは PC に IP アドレスが割り当てられます。加入者がチャネルを選択すると、適切なマルチキャストに加入するために、セットトップ ボックスまたは PC からスイッチ A に IGMP レポートが送信されます。IGMP レポートが、設定されている IP マルチキャスト グループ アドレスの 1 つと一致すると、スイッチの CPU がハードウェア アドレス テーブルを変更して、指定のマルチキャスト ストリームをマルチキャスト VLAN から受信したときの転送先として、レシーバ ポートと VLAN を追加します。マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを、MVR 送信元ポートと呼びます。

図 28-3　MVR の例



RP = レシーバー ポート
SP = 送信元ポート

注：　すべての送信元ポートは
マルチキャスト VLAN に所属します。

加入者がチャネルを切り替えた場合、またはテレビのスイッチを切った場合には、セットトップ ボックスからマルチキャスト ストリームに対する IGMP Leave メッセージが送信されます。スイッチの CPU は、レシーバ ポートの VLAN 経由で MAC ベースの一般クエリーを送信します。VLAN に、このグループに加入している別のセットトップ ボックスがある場合、そのセットトップ ボックスはクエリーに指定された最大応答時間内に応答しなければなりません。応答を受信しなかった場合、CPU はこのグループの転送先としての受信ポートを除外します。

即時脱退機能を使用しない場合、レシーバ ポートの加入者から IGMP Leave メッセージを受信したスイッチは、そのポートに IGMP クエリーを送信し、IGMP グループ メンバーシップ レポートを待ちます。設定された時間内にレポートを受信しなかった場合は、受信ポートがマルチキャスト グループ メンバーシップから削除されます。即時脱退機能がイネーブルの場合、IGMP Leave を受信したレシーバ ポートから IGMP クエリーが送信されません。Leave メッセージの受信後ただちに、受信ポートがマルチキャスト グループ メンバーシップから削除されるので、脱退遅延時間が短縮されます。即時脱退機能は、1 つの受信デバイスが接続された受信ポートでのみイネーブルにしてください。

MVR を使用すると、各 VLAN の加入者に対してテレビ チャネルのマルチキャスト トラフィックを重複して送信する必要がなくなります。すべてのチャネル用のマルチキャスト トラフィックは、マルチキャスト VLAN 上でのみ、VLAN トランクに 1 回だけ送信されます。IGMP Leave および Join メッセージは、加入者ポートが割り当てられている VLAN で送信されます。これらのメッセージは、レイヤ 3 デバイス上のマルチキャスト VLAN のマルチキャスト トラフィック ストリームに対して動的に登録されます。スイッチ B アクセス レイヤ スイッチ（スイッチ A）は、2 つの VLAN 間でのトラフィック伝送を選択的に許可し、マルチキャスト VLAN から別の VLAN 上の加入者ポートにトラフィックが転送されるように転送動作を変更します。

IGMP レポートは、マルチキャスト データと同じ IP マルチキャスト グループ アドレスに送信されます。スイッチ A の CPU は、レシーバ ポートから送られたすべての IGMP Join および Leave メッセージを取り込み、MVR モードに基づいて、送信元（アップリンク）ポートのマルチキャスト VLAN に転送しなければなりません。

デフォルトの MVR 設定

表 28-4　デフォルトの MVR 設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位でディセーブル
マルチキャスト アドレス	未設定
クエリーの応答時間	0.5 秒
マルチキャスト VLAN	VLAN 1
モード	互換性
インターフェイスのデフォルト（ポート単位）	受信ポートでも送信元ポートでもない
即時脱退	すべてのポートでディセーブル

MVR 設定時の注意事項および制限事項

- 受信ポートはアクセス ポートでなければなりません。トランク ポートにはできません。スイッチのレシーバ ポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。
- スイッチ上で設定できるマルチキャスト エントリ（MVR グループ アドレス）の最大数（受信できるテレビ チャネルの最大数）は 256 です。
- 送信元 VLAN で受信され、レシーバ ポートから脱退する MVR マルチキャスト データは、スイッチで存続可能時間（TTL）が 1 だけ少なくなります。
- スイッチ上の MVR は、MAC マルチキャスト アドレスではなく IP マルチキャスト アドレスを使用するので、スイッチ上でエイリアスの IP マルチキャスト アドレスを使用できます。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス（224.0.0.xxx 範囲内）を設定する必要はありません。
- プライベート VLAN ポートに MVR を設定しないでください。
- スイッチ上でマルチキャスト ルーティングがイネーブルの場合、MVR はサポートされません。MVR がイネーブルの場合に、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにすると、MVR がディセーブルになり、警告メッセージが表示されま

す。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの場合に、MVR をイネーブルにしようとすると、MVR をイネーブルにする操作が取り消され、エラー メッセージが表示されます。

- MVR はスイッチで IGMP スヌーピングと共存できます。
- MVR 受信ポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- MVR は IGMPv3 メッセージをサポートしていません。

IGMP フィルタリングおよび IGMP スロットリング

都市部や Multiple-Dwelling Unit（MDU）などの環境では、スイッチ ポート上のユーザが属する一連のマルチキャスト グループを制御する必要があります。この機能を使用することにより、IP/TV などのマルチキャスト サービスの配信を、特定タイプの契約またはサービス計画に基づいて制御できます。また、マルチキャスト グループの数を、スイッチ ポート上でユーザが所属できる数に制限することもできます。

IGMP フィルタリング機能を使用すると、IP マルチキャスト プロファイルを設定し、それらを各スイッチ ポートに関連付けて、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プロファイルにはマルチキャスト グループを 1 つまたは複数格納して、グループへのアクセスを許可するか拒否するかを指定できます。マルチキャスト グループへのアクセスを拒否する IGMP プロファイルがスイッチ ポートに適用されると、IP マルチキャスト トラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループからの IP マルチキャスト トラフィックを受信できなくなります。マルチキャスト グループへのアクセスがフィルタリング アクションで許可されている場合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバーシップ レポート（Join および Leave レポートを含む）だけです。一般 IGMP クエリーは制御されません。IGMP フィルタリングは、IP マルチキャスト トラフィックの転送を指示する機能とは無関係です。フィルタリング機能は、マルチキャスト トラフィックの転送に CGMP が使用されているか、または MVR が使用されているかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャスト グループ アドレスを動的に学習する場合だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インターフェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートでランダムに選択されたマルチキャスト エントリを上書きします。

（注）　IGMP フィルタリングが実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

表 28-5 に、IGMP フィルタリングのデフォルト設定を示します。

表 28-5　IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用されない
IGMP グループの最大数	最大数は設定されない
IGMP プロファイル	未設定
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

転送テーブルに登録されているグループが最大数に達していると、デフォルトの IGMP スロットリング アクションは IGMP レポートを拒否します。

IGMP プロファイル

IGMP プロファイルを設定するには、**ip igmp profile** グローバル コンフィギュレーション コマンドおよびプロファイル番号を使用して、IGMP プロファイルを作成し、IGMP プロファイル コンフィギュレーション モードを開始します。ポートから送信される IGMP Join 要求をフィルタリングするために使用される IGMP プロファイルのパラメータは、このモードから指定できます。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- **deny**：一致するアドレスを拒否します。デフォルトで設定されています。
- **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。
- **no**：コマンドを否定するか、または設定をデフォルトに戻します。
- **permit**：一致するアドレスを許可します。
- **range**：プロファイルに対する IP アドレスの範囲を指定します。単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。

デフォルトでは、スイッチには IGMP プロファイルが設定されていません。プロファイルが設定されており、**permit** および **deny** キーワードがいずれも指定されていない場合、デフォルトでは、IP アドレス範囲へのアクセスが拒否されます。

IGMP プロファイルの定義に従ってアクセスを制御するには、**ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用して、プロファイルを該当するインターフェイスに適用します。IGMP プロファイルを適用できるのは、レイヤ 2 アクセス ポートだけです。ルーテッド ポートや SVI には適用できません。EtherChannel ポート グループに所属するポートに、プロファイルを適用することはできません。1 つのプロファイルを複数のインターフェイスに適用できますが、1 つのインターフェイスに適用できるプロファイルは 1 つだけです。

IGMP スロットリング アクション

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定した後、**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドを使用して受信した IGMP レポートの新しいグループで、既存のグループを上書きします。IGMP Join レポートを廃棄するデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

IGMP スロットリング アクションを設定する場合には、次の注意事項に従ってください。

- この制限事項は、レイヤ 2 ポートにだけ適用されます。このコマンドは、論理 EtherChannel インターフェイスでは使用できますが、EtherChannel ポート グループに属するポートでは使用できません。
- グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action** {**deny** | **replace**} コマンドを入力しても効果はありません。
- インターフェイスによりマルチキャスト エントリが転送テーブルに追加されてから、スロットリング アクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリング アクションに応じて期限切れになるか削除されます。
  - スロットリング アクションを **deny** に設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、スイッチは、インターフェイスで受信した次の IGMP レポートを廃棄します。
  - スロットリング アクションを **replace** に設定すると、すでに転送テーブルに登録されていたエントリは削除されます。転送テーブルのエントリが最大数まで達したら、スイッチはランダムに選択したエントリを受信した IGMP レポートで上書きします。

  スイッチが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送テーブルにエントリが追加される前に、IGMP スロットリング アクションを設定します。

IGMP スヌーピングおよび MVR の設定方法

IGMP スヌーピングの設定

IGMP スヌーピングのイネーブル化およびディセーブル化

デフォルトでは、IGMP スヌーピングはスイッチ上でグローバルにイネーブルです。グローバルにイネーブルまたはディセーブルに設定されている場合、既存のすべての VLAN インターフェイスでもイネーブルまたはディセーブルです。デフォルトでは、IGMP スヌーピングはすべての VLAN でイネーブルですが、VLAN 単位で IGMP スヌーピングをイネーブルおよびディセーブルに設定できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping** **または** **ip igmp snooping vlan** *vlan-id*	既存のすべての VLAN インターフェイスでグローバルに IGMP スヌーピングを有効にします。 または VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。 VLAN スヌーピングをイネーブルにするには、IGMP スヌーピングをグローバルにイネーブルに設定しておく必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。

IGMP スヌーピング パラメータの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **mrouter learn** {**cgmp** | **pim-dvmrp**}	（任意）VLAN で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。 マルチキャスト ルータの学習方式を指定します。 • **cgmp** : CGMP パケットを待ち受けます。この方法は、制御トラフィックを減らす場合に有用です。 • **pim-dvmrp** : IGMP クエリーおよび PIM パケットと DVMRP パケットをスヌーピングします。これはデフォルトです。
ステップ 3	**ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	マルチキャスト ルータ ポートを追加します（マルチキャスト ルータにスタティック接続を追加します）。 （任意）マルチキャスト ルータの VLAN ID を指定して、マルチキャスト ルータにインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネルの範囲は 1 ～ 6 です。 • マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。
ステップ 4	**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id*	（任意）マルチキャスト グループのメンバとしてレイヤ 2 ポートをスタティックに設定します。 • *vlan-id* : マルチキャスト グループの VLAN ID。指定できる範囲は 1 ～ 1001 または 1006 ～ 4096 です。 • *ip-address* : グループの IP アドレス。 • *interface-id* : メンバ ポート。物理インターフェイスまたはポート チャネル（1 ～ 6）に設定できます。
ステップ 5	**ip igmp snooping vlan** *vlan-id* **immediate-leave**	（任意）VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。 **（注）** 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。
ステップ 6	**ip igmp snooping last-member-query-interval** *time*	（任意）IGMP 脱退タイマーをグローバルに設定します。指定できる範囲は 100 ～ 32768 ミリ秒です。デフォルト値は 1000 秒です。
ステップ 7	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time*	（任意）VLAN インターフェイス上で IGMP 脱退時間を設定します。指定できる範囲は 100 ～ 32768 ミリ秒です。 **（注）** VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。
ステップ 8	**end**	特権 EXEC モードに戻ります。

TCN の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping tcn flood query count** *count*	マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ～ 10 です。デフォルトのフラッディング クエリー カウントは 2 です。
ステップ 3	**ip igmp snooping tcn query solicit**	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。デフォルトでは、クエリー送信要求はディセーブルに設定されています。 **（注）** スイッチがスパニングツリーのルートであるかどうかにかかわらず、グローバル脱退メッセージを送信できるようにします。
ステップ 4	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**no ip igmp snooping tcn flood**	スパニングツリーの TCN イベント中に発生するマルチキャスト トラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャスト フラッディングはイネーブルです。
ステップ 6	**end**	特権 EXEC モードに戻ります。

IGMP スヌーピング クエリアの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping querier**	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 3	**ip igmp snooping querier address** *ip_address*	（任意）IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 **（注）** IGMP スヌーピング クエリアはスイッチ上で IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
ステップ 4	**ip igmp snooping querier query-interval** *interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
ステップ 5	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*]	（任意）トポロジ変更通知（TCN）クエリーの間隔を設定します。指定できる count の範囲は 1 ～ 10 です。指定できる interval の範囲は 1 ～ 255 秒です。
ステップ 6	**ip igmp snooping querier timer expiry** *timeout*	（任意）IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ～ 300 秒です。
ステップ 7	**ip igmp snooping querier version** *version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 8	**end**	特権 EXEC モードに戻ります。

IGMP レポート抑制のディセーブル化

はじめる前に

IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ip igmp snooping report-suppression**	IGMP レポート抑制をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

MVR の設定

MVR グローバル パラメータの設定

デフォルト値を使用する場合は、オプションの MVR パラメータを設定する必要はありません。デフォルトのパラメータを変更する場合には（MVR VLAN 以外）、最初に MVR をイネーブルにする必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルにします。
ステップ 3	**mvr group** *ip-address* [*count*]	スイッチ上で IP マルチキャスト アドレスを設定するか、または *count* パラメータを使用して、連続する MVR グループ アドレスを設定します（*count* の範囲は 1 ～ 256、デフォルトは 1）。このアドレスに送信されたマルチキャスト データは、スイッチ上のすべての送信元ポートおよびそのマルチキャスト アドレスのデータを受信するために選ばれた、すべてのレシーバ ポートに送信されます。マルチキャスト アドレスとテレビ チャネルは 1 対 1 の対応です。
ステップ 4	**mvr querytime** *value*	（任意）マルチキャスト グループ メンバーシップからポートを削除する前に、受信ポート上で IGMP レポート メンバーシップを待機する最大時間を定義します。この値は 10 分の 1 秒単位で設定します。範囲は 1 ～ 100、デフォルトは 10 分の 5 秒、つまり 0.5 秒です。
ステップ 5	**mvr vlan** *vlan-id*	（任意）マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートはこの VLAN に属する必要があります。VLAN の範囲は 1 ～ 1001 および 1006 ～ 4096 です。デフォルトは VLAN 1 です。

	コマンド	目的
ステップ 6	**mvr mode** {**dynamic** | **compatible**}	（任意）MVR の動作モードを指定します。 • **dynamic**：送信元ポートでダイナミック MVR メンバーシップを使用できます。 • **compatible**：Catalyst 3500 XL スイッチおよび Catalyst 2900 XL スイッチとの互換性が得られます。送信元ポートでのダイナミック IGMP Join はサポートされません。 デフォルトは **compatible** モードです。
ステップ 7	**end**	特権 EXEC モードに戻ります。

MVR インターフェイスの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルにします。
ステップ 3	**interface** *interface-id*	設定するレイヤ 2 ポートを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**mvr type** {**source** | **receiver**}	MVR ポートを次のいずれかに設定します。 • **source**：マルチキャスト データを送受信するアップリンク ポートを送信元ポートとして設定します。加入者が送信元ポートに直接接続することはできません。スイッチ上のすべての送信元ポートは、単一マルチキャスト VLAN に所属します。 • **receiver**：ポートが加入者ポートで、マルチキャスト データの受信だけを行う場合には、ポートを受信ポートとして設定します。受信ポートは、スタティックな設定、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバーになるまでは、データを受信しません。受信ポートをマルチキャスト VLAN に所属させることはできません。 デフォルトでは、非 MVR ポートとして設定されます。非 MVR ポートに MVR 特性を設定しようとしても、エラーになります。
ステップ 5	**mvr vlan** *vlan-id* **group** [*ip-address*]	（任意）マルチキャスト VLAN および IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するポートを静的に設定します。グループ メンバとして静的に設定されたポートは、静的に削除されない限り、グループ メンバのままです。 **（注）** 互換モードでは、このコマンドが適用されるのはレシーバ ポートだけです。ダイナミック モードでは、レシーバ ポートおよび送信元ポートに適用されます。 レシーバ ポートは、IGMP Join および Leave メッセージを使用することによって、マルチキャスト グループに動的に加入することもできます。
ステップ 6	**mvr immediate**	（任意）ポート上で MVR の即時脱退機能をイネーブルにします。 **（注）** このコマンドが適用されるのは、受信ポートだけです。また、イネーブルにするのは、単一の受信デバイスが接続されている受信ポートに限定してください。
ステップ 7	**end**	特権 EXEC モードに戻ります。

IGMP の設定

IGMP プロファイルの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp profile** *profile number*	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。指定できるプロファイル番号の範囲は 1 ～ 4294967295 です。
ステップ 3	**permit** | **deny**	（任意）IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。
ステップ 4	**range** *ip multicast address*	アクセスを制御する IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力する場合は、IP マルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。 **range** コマンドを複数回入力すると、複数のアドレスまたはアドレス範囲を入力できます。
ステップ 5	**end**	特権 EXEC モードに戻ります。

IGMP インターフェイスの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属していないレイヤ 2 ポートでなければなりません。
ステップ 3	**ip igmp filter** *profile number*	インターフェイスに指定された IGMP プロファイルを適用します。指定できる範囲は 1 ～ 4294967295 です。
ステップ 4	**ip igmp max-groups** *number*	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ～ 4294967294 です デフォルトでは最大数は設定されません。
ステップ 5	**ip igmp max-groups action** {**deny** | **replace**}	インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。 • **deny**：レポートを廃棄します。 • **replace**：既存のグループを、IGMP レポートを受信した新しいグループで上書きします。
ステップ 6	**end**	特権 EXEC モードに戻ります。

IGMP スヌーピングおよび MVR のモニタリングおよびメンテナンス

コマンド	目的
show ip igmp snooping [**vlan** *vlan-id*]	スイッチ上のすべての VLAN または特定の VLAN のスヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。
show ip igmp snooping groups [**count** |**dynamic** [**count**] | **user** [**count**]]	スイッチまたは特定のパラメータに関して、マルチキャスト テーブル情報を表示します。 • **count**：実際のエントリではなく、特定のコマンド オプションに対応するエントリの総数を表示します。 • **dynamic**：IGMP スヌーピングによって学習されたエントリを表示します。 • **user**：ユーザによって設定されたマルチキャスト エントリだけを表示します。
show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user**[**count**]]	マルチキャスト VLAN またはその VLAN の特定のパラメータについて、マルチキャスト テーブル情報を表示します。 • *vlan-id*：VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。 • **count**：実際のエントリではなく、特定のコマンド オプションに対応するエントリの総数を表示します。 • **dynamic**：IGMP スヌーピングによって学習されたエントリを表示します。 • *ip_address*：指定のグループ IP アドレスのマルチキャスト グループについて、特性を表示します。 • **user**：ユーザによって設定されたマルチキャスト エントリだけを表示します。
show ip igmp snooping mrouter [**vlan** *vlan-id*]	動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。 **（注）** IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。
show ip igmp snooping querier [**vlan** *vlan-id*]	IP アドレス、および VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。
show ip igmp snooping querier [**vlan** *vlan-id*] **detail**	IP アドレスおよび VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報、VLAN の IGMP スヌーピング クエリアの設定および動作ステートに関する情報を表示します。

コマンド	目的
show ip igmp profile [*profile number*]	特定の IGMP プロファイルまたはスイッチ上で定義されているすべての IGMP プロファイルを表示します。
show mvr	スイッチの MVR ステータスおよび値を表示します。これは、MVR のイネーブルまたはディセーブルの判別、マルチキャスト VLAN、マルチキャスト グループの最大数（256）および現在の数（0 ～ 256）、クエリーの応答時間、および MVR モードです。
show mvr interface [*interface-id*] [**members** [**vlan** *vlan*-**id**]]	すべての MVR インターフェイスおよびその MVR 設定を表示します。 特定のインターフェイスを指定すると、次の情報が表示されます。 • Type：Receiver または Source • Status：次のいずれか – ACTIVE は、ポートが VLAN に含まれていることを意味します。 – UP/DOWN は、ポートが転送中または転送中ではないことを示します。 – INACTIVE は、ポートが VLAN に含まれていないことを意味します。 • Immediate Leave：Enabled または Disabled **members** キーワードを入力すると、そのポート上のすべてのマルチキャスト グループ メンバが表示されます。VLAN ID を入力した場合は、VLAN 上のすべてのマルチキャスト グループ メンバが表示されます。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。
show mvr members [*ip-address*]	すべての IP マルチキャスト グループまたは指定した IP マルチキャスト グループ IP アドレスに含まれているレシーバ ポートおよび送信元ポートがすべて表示されます。
show ip igmp profile *profile number*	プロファイルの設定を確認します。
show ip igmp snooping mrouter [**vlan** *vlan-id*]	VLAN インターフェイス上で IGMP スヌーピングがイネーブルになっていることを確認します。

IGMP スヌーピングの設定例

IGMP スヌーピングの設定：例

次に、CGMP パケットを学習方式として使用するように IGMP スヌーピングを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
```

マルチキャスト ルータ ポートのディセーブル化：例

VLAN からマルチキャスト ルータ ポートを削除するには、**no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/2
Switch(config)# end
```

ポート上のホストの静的な設定：例

次に、ポート上のホストを静的に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/1
Switch(config)# end
```

IGMP 即時脱退のイネーブル化：例

次に、VLAN 130 上で IGMP 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

IGMP スヌーピング クエリアのパラメータ設定：例

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

MVR のイネーブル化：例

次に、MVR をイネーブルにして、MVR グループ アドレスを設定し、クエリー タイムを 1 秒（10 分の 10 秒）に設定し、MVR マルチキャスト VLAN を VLAN 22 として指定し、MVR モードをダイナミックに設定する例を示します。

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
```

```
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(config)# end
```

show mvr members 特権 EXEC コマンドを使用すると、スイッチ上の MVR マルチキャスト グループ アドレスを確認できます。

次に、ポートをレシーバ ポートとして設定し、マルチキャスト グループ アドレスに送信されたマルチキャスト トラフィックを受信するようにポートを静的に設定し、ポートに即時脱退機能を設定し、結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config)# end
Switch# show mvr interface
Port    Type        Status          Immediate Leave
----    ----        -------         ---------------
Gi1/2   RECEIVER    ACTIVE/DOWN     ENABLED
```

IGMP プロファイルの作成：例

次に、単一の IP マルチキャスト アドレスへのアクセスを許可する IGMP プロファイル 4 を作成して、設定を確認する例を示します。アクションが拒否（デフォルト）である場合は、**show ip igmp profile** の出力には表示されません。

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

IGMP プロファイルの適用：例

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

IGMP グループの制限：例

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS マルチキャスト コマンド	『*Cisco IOS IP Command Reference, Volume 3 of 3:Multicast*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 29

ポート単位のトラフィック制御の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ポート ベースのトラフィック制御の制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

ポート ベースのトラフィック制御に関する情報

ストーム制御

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム制御（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レートの秒単位のパケット数。

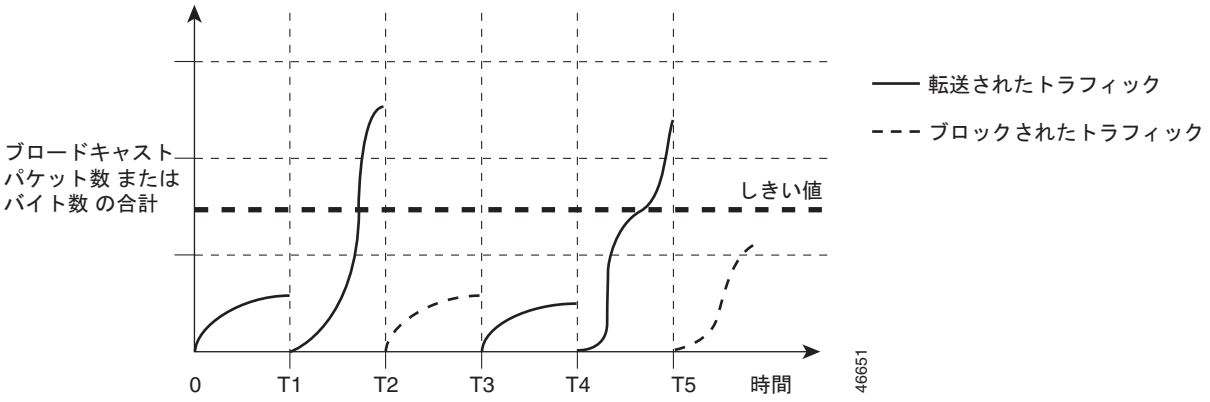
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レートの秒単位のビット数。
- 小さいフレームのトラフィック レートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注）　マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

図 29-1 のグラフは、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。この例は、マルチキャストおよびユニキャスト トラフィックにも当てはまります。この例では、T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

図 29-1　　ブロードキャスト ストーム制御の例



ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過できるパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注）　パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御のデフォルト設定

デフォルトでは、ユニキャスト、ブロードキャスト、およびマルチキャスト ストーム制御はスイッチ インターフェイス上でディセーブルになります。したがって、抑制レベルは 100% です。

ストーム制御およびしきい値レベル

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

小さいフレームの着信レート

67 バイト未満の着信 VLAN タグ付きパケットは、*小さいフレーム*と見なされます。このパケットはスイッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。Cisco IOS Release 12.2(44)SE 以降では、小さいフレームが指定されたレート（しきい値）で到着した場合は、ポートがディセーブルになるように設定できます。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

errdisable recovery cause small-frame グローバル コンフィギュレーション コマンドを入力すると、指定された時間後にポートが再びイネーブルになります。（**errdisable recovery** グローバル コンフィギュレーション コマンドを使用して、リカバリ時間を指定します）。

保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ 3 デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

保護ポート設定時の注意事項

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

プライベート VLAN ポートを保護ポートとして設定しないでください。保護ポートをプライベート VLAN ポートとして設定しないでください。プライベート VLAN の独立ポートは、他の独立ポートやコミュニティ ポートにトラフィックを転送しません。VLAN の詳細については、第 17 章「VLAN の設定」を参照してください。

ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注）　マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

ポート セキュリティ

ポート セキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュア ポートとして設定されたポートのセキュア MAC アドレスが最大数に達した場合に、ポートにアクセスしようとするステーションの MAC アドレスが、識別されたどのセキュア MAC アドレスとも異なるときは、セキュリティ違反が発生します。また、あるセキュア ポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュア ポートにアクセスしようとしたときにも、違反のフラグが立てられます。

セキュア MAC アドレス

ポートで許可されるセキュア アドレスの最大数を設定するには、**switchport port-security maximum** *value* インターフェイス コンフィギュレーション コマンドを使用します。

（注）　最大値をインターフェイス上ですでに設定されているセキュア アドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- スタティック セキュア MAC アドレス：**switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス：動的に設定されてアドレス テーブルにのみ保存され、スイッチの再起動時に削除されます。
- *スティッキー* セキュア MAC アドレス：動的に学習することも、手動で設定することもできます。アドレス テーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

*スティッキー ラーニング*をイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。スティッキー ラーニングをイネーブルにするには、**switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、インターフェイスはスティッキー ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的には反映されません。スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。

スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management（SDM）テンプレートによって決められます。第 11 章「SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同じスイッチ上の同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合のアクションに基づいて、次の 4 つの違反モードのいずれかにインターフェイスを設定できます。

- protect（保護）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。

  （注）　トランク ポートに protect 違反モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

- restict（制限）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- shutdown（シャットダウン）：ポート セキュリティ違反により、インターフェイスが errdisable になり、ただちにシャットダウンされます。その後、ポートの LED が消灯します。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが errdisable ステートの場合、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにしたりできます。これは、デフォルトのモードです。
- shutdown vlan（VLAN シャットダウン）：VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。

表 29-1　セキュリティ違反モードの処置

違反モード	トラフィックの転送[1]	SNMP トラップの送信	syslog メッセージの送信	エラー メッセージの表示[2]	違反カウンタの増加	ポートのシャットダウン
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	No	No	No	Yes	Yes
shutdown vlan	No	No	Yes	No	Yes	No[3]

1. 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。
2. セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラー メッセージを返します。
3. 違反が発生した VLAN のみシャットダウンします。

デフォルトのポート セキュリティ設定

表 29-2　ポート セキュリティのデフォルト設定

機能	デフォルト設定
ポート セキュリティ	ポート上でディセーブル
スティッキー アドレス ラーニング	ディセーブル

表 29-2　ポート セキュリティのデフォルト設定 （続き）

機能	デフォルト設定
ポートあたりのセキュア MAC アドレスの最大数	1
違反モード	shutdown。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポート セキュリティ エージング	ディセーブル エージング タイムは 0 スタティック エージングはディセーブル タイプは absolute

ポート セキュリティの設定時の注意事項

- ポート セキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートを Fast EtherChannel ポート グループに含めることはできません。

（注）　音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュア アドレスを設定する必要があります。
- トランク ポートがポート セキュリティで設定され、データ トラフィックのアクセス VLAN および音声トラフィックのアクセス VLAN に割り当てられている場合は、**switchport voice** および **switchport priority extend** インターフェイス コンフィギュレーション コマンドを入力しても効果はありません。

  接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。
- ポート セキュリティを設定する場合、**switchport port-security maximum** インターフェイス コンフィギュレーション コマンドを使用して、最初に許可する MAC アドレスの総数を指定します。次に、許可するアクセス VLAN の数（**switchport port-security vlan access** インターフェイス コンフィギュレーション コマンド）および音声 VLAN（**switchport port-security vlan voice** インターフェイス コンフィギュレーション コマンド）を設定します。最初に合計数を指定しなかった場合は、デフォルト設定（1 個の MAC アドレス）にシステムが戻ります。
- インターフェイスの最大セキュア アドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングをサポートしていません。

表 29-3　ポート セキュリティと他のポートベース機能との互換性

ポート タイプまたはポートの機能	ポート セキュリティとの互換性
DTP [1] ポート[2]	No
トランク ポート	Yes
ダイナミック アクセス ポート[3]	No
ルーテッド ポート	No
SPAN 送信元ポート	Yes
SPAN 宛先ポート	No
EtherChannel	No
トンネリング ポート	Yes
保護ポート	Yes
IEEE 802.1x ポート	Yes
音声 VLAN ポート[4]	Yes
プライベート VLAN ポート	Yes
IP ソース ガード	Yes
ダイナミック アドレス解決プロトコル（ARP）インスペクション	Yes
FlexLink	Yes

1. DTP = Dynamic Trunking Protocol
2. **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート。
3. **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定された VLAN Query Protocol（VQP）ポート。
4. ポートに最大限可能なセキュアなアドレスを設定します（アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数）。

ポート セキュリティ エージング

ポート上のすべてのセキュア アドレスにエージング タイムを設定するには、ポート セキュリティ エージングを使用します。ポートごとに 2 つのタイプのエージングがサポートされています。

- absolute：指定されたエージング タイムの経過後に、ポート上のセキュア アドレスが削除されます。
- inactivity：指定されたエージング タイムの間、セキュア アドレスが非アクティブであった場合に限り、ポート上のセキュア アドレスが削除されます。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュア ポート上のデバイスを削除および追加し、なおかつポート上のセキュア アドレス数を制限できます。セキュア アドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

ポート セキュリティおよびプライベート VLAN

ポート セキュリティとプライベート VLAN（PVLAN）の両方が設定されているポートには、セキュア PVLAN ポートのラベル付けが可能です。セキュア アドレスがセキュア PVLAN ポートで学習されるとき、同じセキュア アドレスは、同じプライマリ VLAN に属する別のセキュア PVLAN ポートでは学習できません。ただし、非セキュア PVLAN ポートで学習されたアドレスは、同じプライマリ VLAN に属するセキュア PVLAN ポートで学習できます。

ホスト ポートで学習されるセキュア アドレスは、関連プライマリ VLAN で自動的に複製され、また同様に、無差別ポートで学習されるセキュア アドレスは、すべての関連セカンダリ VLAN で自動的に複製されます。静的アドレス（**mac-address-table static** コマンドを使用）は、ユーザがセキュア ポートで設定することはできません。

プロトコル ストーム プロテクション

スイッチがアドレス解決プロトコル（ARP）または制御パケットでフラッドされると、CPU の高い使用率により CPU のオーバーロードが発生する可能性があります。これらの問題は、次のように発生します。

- プロトコル制御パケットが受信されず、ネイバーの隣接がドロップされるため、ルーティング プロトコルがフラップする場合があります。
- スパニングツリー プロトコル（STP）ブリッジ プロトコル データ ユニット（BPDU）が送受信されないため、STP が再収束します。
- CLI が遅くなるか応答しなくなります。

プロトコル ストーム プロテクションを使用すると、パケットのフロー レートの上限しきい値を指定して、制御パケットが送信されるレートを制御できます。サポートされるプロトコルは、ARP、ARP スヌーピング、Dynamic Host Configuration Protocol（DHCP）v4、DHCP スヌーピング、インターネット グループ管理プロトコル（IGMP）、および IGMP スヌーピングです。

パケットのレートが定義されたしきい値を超えると、スイッチは指定されたポートに着信したすべてのトラフィックを 30 秒間ドロップします。パケット レートが再度計測され、必要な場合はプロトコル ストーム プロテクションが再度適用されます。

より強力な保護が必要な場合は、仮想ポートを手動で errdisable にし、その仮想ポートのすべての着信トラフィックをブロックできます。また、手動で仮想ポートをイネーブルにしたり、仮想ポートの自動再イネーブル化の時間間隔を設定することもできます。

（注） 超過したパケットは、2 つ以下の仮想ポートにおいてドロップされます。
仮想ポートの errdisable は、EtherChannel および Flexlink インターフェイスではサポートされません。

プロトコル ストーム プロテクションはデフォルトでディセーブルです。これがイネーブルになると、仮想ポートの自動リカバリがデフォルトでディセーブルになります。

ポート ベースのトラフィック制御の設定方法

ストーム制御の設定

ストーム制御およびしきい値レベルの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。 • *level*：ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第 2 位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low*：下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第 2 位まで）。この値は上限抑制値より小さいか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ～ 100.00 です。 しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。 • **bps** *bps*：ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します（小数点第 1 位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low*：下限しきい値レベルをビット/秒で指定します（小数点第 1 位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ～ 10000000000.0 です。
		• **pps** *pps*：ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第 1 位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low*：下限しきい値レベルをパケット/秒で指定します（小数点第 1 位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は **0.0** ～ 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、g など）を使用できます。
ステップ 4	**storm-control action** {**shutdown** | **trap**}	ストーム検出時に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 • **shutdown**：ストームの間、ポートを errdisable にします。 • **trap**：ストームが検出された場合、SNMP トラップを生成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

小さいフレームの着信レートの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause small-frame**	スイッチ上の小さいフレームの着信レート機能をイネーブルにします。
ステップ 3	**errdisable recovery interval** *interval*	（任意）指定された errdisable ステートから回復する時間を指定します。
ステップ 4	**errdisable recovery cause small-frame**	（任意）小さいフレームの着信によりポートが errdisable になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。
ステップ 5	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインタフェースを指定します。
ステップ 6	**small violation-rate** *pps*	インターフェイスが着信パケットをドロップしてポートを errdisable にするようにしきい値レートを設定します。指定できる範囲は、1 ～ 10,000 pps（パケット/秒）です。
ステップ 7	**end**	特権 EXEC モードに戻ります。

保護ポートの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport protected**	インターフェイスを保護ポートとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

ポート ブロッキングの設定

インターフェイスでのフラッディング トラフィックのブロッキング

（注）　インターフェイスは物理インターフェイスまたは EtherChannel グループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**switchport block multicast**	ポートからの未知のマルチキャストの転送をブロックします。 **（注）** 純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
ステップ 4	**switchport block unicast**	ポートからの未知のユニキャストの転送をブロックします。
ステップ 5	**end**	特権 EXEC モードに戻ります。

ポート セキュリティの設定

ポート セキュリティのイネーブル化および設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode** {**access** | **trunk**}	アクセスまたはトランクとしてインターフェイス スイッチポート モードを設定します。デフォルト モード（dynamic auto）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 4	**switchport voice vlan** *vlan-id*	ポート上で音声 VLAN をイネーブルにします。 *vlan-id*：音声トラフィックに使用する VLAN を指定します。
ステップ 5	**switchport port-security**	インターフェイス上でポート セキュリティをイネーブルにします。

	コマンド	目的
ステップ 6	**switchport port-security** [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]	（任意）**maximum**：ポートでのセキュア MAC アドレスの最大数を指定します。デフォルトでは、1 個の MAC アドレスのみ使用できます。 スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、アクティブな SDM テンプレートによって決まります。第 11 章「SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-list*：トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定します。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注）　**voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。

	コマンド	目的
ステップ 7	**switchport port-security [violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}]	（任意）違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。 • **protect**（保護）：ポート セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。 （注）　トランク ポートに protect モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。 • **restrict**：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown**（シャットダウン）：違反が発生すると、インターフェイスが error-disabled になり、ポートの LED が消灯します。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown vlan**：VLAN 単位のセキュリティ違反モードを設定します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。 （注）　セキュア ポートが errdisable ステートになった場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力して、このステートを解除します。手動で再びイネーブルにするには、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface vlan** 特権 EXEC コマンドを入力します。

	コマンド	目的
ステップ 8	**switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]	（任意）インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。 **（注）** このコマンドの入力後にスティッキー ラーニングをイネーブルにすると、動的に学習されたセキュア アドレスがスティッキー セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。
ステップ 9	**switchport port-security mac-address sticky**	（任意）インターフェイス上でスティッキ ラーニングをイネーブルにします。
ステップ 10	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | ***voice***}}]	（任意）スティッキー セキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティッキー セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。 **（注）** このコマンドの入力前にスティッキー ラーニングをイネーブルにしないと、エラー メッセージが表示されてスティッキー セキュア MAC アドレスを入力できません。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。
ステップ 11	**end**	特権 EXEC モードに戻ります。

ポート セキュリティ エージングのイネーブル化および設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}	セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。 （注）　スイッチは、スティッキー セキュア アドレスのポート セキュリティ エージングをサポートしていません。 **static**：このポートに静的に設定されたセキュア アドレスのエージングをイネーブルにします。 **time**：このポートのエージング タイムを指定します。指定できる範囲は、0 ～ 1440 分です。 **type**：エージング タイプを absolute または inactivity に指定します。 • **absolute**：このポートのセキュア アドレスはすべて、指定した時間（分単位）が経過すると期限切れになり、セキュア アドレス リストから削除されます。 • **inactivity**：指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合に限り、このポートのセキュア アドレスが期限切れになります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

プロトコル ストーム プロテクションの設定

プロトコル ストーム プロテクションのイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**psp** {**arp** | **dhcp** | **igmp**} **pps** *value*	ARP、IGMP、または DHCP に対してプロトコル ストーム プロテクションを設定します。 *value*：秒あたりのパケット数のしきい値を指定します。トラフィックがこの値を超えると、プロトコル ストーム プロテクションが適用されます。範囲は毎秒 5 ～ 50 パケットです。
ステップ 3	**errdisable detect cause psp**	（任意）プロトコル ストーム プロテクションの errdisable 検出をイネーブルにします。この機能がイネーブルになると、仮想ポートが errdisable になります。この機能がディセーブルになると、そのポートは、ポートを errdisable にせずに超過したパケットをドロップします。

	コマンド	目的
ステップ 4	**errdisable recovery interval** *time*	（任意）errdisable の仮想ポートの自動リカバリ時間を秒単位で設定します。仮想ポートが errdisable の場合、この時間を過ぎるとスイッチは自動的にリカバリします。指定できる範囲は 30 ～ 86400 秒です。
ステップ 5	**end**	特権 EXEC モードに戻ります。

ポート ベースのトラフィック制御のモニタリングとメンテナンス

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。
show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**]	すべてのインターフェイスまたは指定されたインターフェイスに設定されているストーム制御抑制レベルを、指定されたトラフィック タイプについて、またはブロードキャスト トラフィック（トラフィック タイプが入力されていない場合）について表示します。
show port-security [**interface** *interface-id*]	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を、各インターフェイスで許容されるセキュア MAC アドレスの最大数、インターフェイスのセキュア MAC アドレスの数、発生したセキュリティ違反の数、違反モードを含めて表示します。
show port-security [**interface** *interface-id*] **address**	すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
show port-security interface *interface-id* **vlan**	指定されたインターフェイスに VLAN 単位で設定されているセキュア MAC アドレスの数を表示します。
show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**]	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを表示します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
show interfaces *interface-id*	インターフェイスの設定を表示します。
show interfaces *interface-id* **switchport**	スイッチ ポート情報を表示します。
show port-security	インターフェイスまたはスイッチのポート セキュリティ設定を表示します。
show psp config {**arp** | **dhcp** | **igmp**}	プロトコルの PSP 設定の詳細を表示します。

ポート ベースのトラフィック制御の設定例

ユニキャスト ストーム制御のイネーブル化：例

次に、ポート上で、上限抑制レベルを 87%、下限抑制レベルを 65% に設定し、ユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# storm-control unicast level 87 65
```

ポートのブロードキャスト アドレスのストーム制御のイネーブル化：例

次に、ポート上で、ブロードキャスト アドレスのストーム制御を 20% のレベルでイネーブルにする例を示します。ブロードキャスト トラフィックが、トラフィック ストーム制御インターバル内にポートで使用できる総帯域幅のうち、設定された 20% のレベルを超えた場合、トラフィック ストーム制御インターバルが終わるまで、スイッチはすべてのブロードキャスト トラフィックをドロップします。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# storm-control broadcast level 20
```

小さいフレームの着信レートのイネーブル化：例

次に、小さいフレームの着信レート機能をイネーブルにし、ポートのリカバリ時間を設定し、ポートを errdisable にするしきい値を設定する例を示します。

```
Switch# configure terminal
Switch# errdisable detect cause small-frame
Switch# errdisable recovery cause small-frame
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# small-frame violation rate 10000
Switch(config-if)# end
```

保護ポートの設定：例

次に、保護ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

ポートでのフラッディングのブロック：例

次に、ポート上のユニキャストおよびレイヤ 2 マルチキャスト フラッディングをブロックする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport block multicast
```

```
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

ポート セキュリティの設定：例

次に、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、ポートのスティッキー ポート セキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの総数を 20 に設定します（データ VLAN に 10、音声 VLAN に 10 を割り当てます）。

```
Switch(config)# interface FastEthernet1/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

ポート セキュリティ エージングの設定：例

次に、ポート上のセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport port-security aging time 120
```

次に、このインターフェイスに設定されたセキュア アドレスに対して、エージングをイネーブルにし、非アクティブ エージング タイプのエージング タイムを 2 分に設定する例を示します。

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

上記のコマンドを確認するには、**show port-security interface** *interface-id* 特権 EXEC コマンドを入力します。

プロトコル ストーム プロテクションの設定：例

次の例では、DHCP の着信 DHCP トラフィックが毎秒 35 パケットを超えた場合に、トラフィックをドロップするようプロトコル ストーム プロテクションを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# psp dhcp pps 35
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 30

SPAN および RSPAN の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SPAN および RSPAN の前提条件

- スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。この要件は、スタティック ホストの IPSG がレイヤ 2 アクセス ポート上で使用される場合にも適用されます。

SPAN および RSPAN の制約事項

- RSPAN 機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- 侵入検知のための SPAN は、LAN Lite イメージではサポートされません。
- スイッチが LAN Base イメージを実行中の場合は、2 つの SPAN セッションがサポートされます。
- スイッチが LAN Lite イメージを実行中の場合は、1 の SPAN セッションがサポートされます。

SPAN および RSPAN に関する情報

SPAN および RSPAN

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、スイッチド ポート アナライザ（SPAN）またはリモート SPAN（RSPAN）を使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

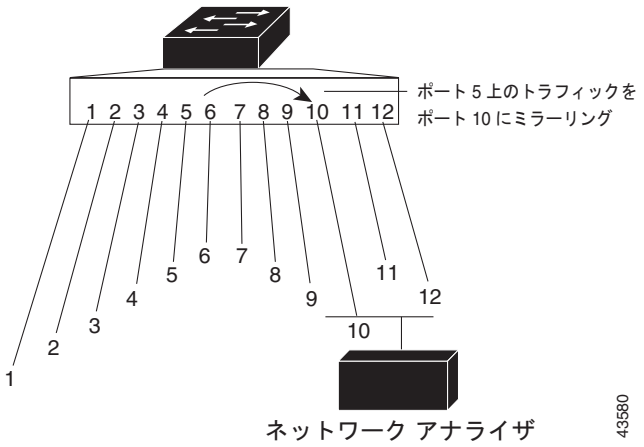
SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco 侵入検知システム（IDS）センサー装置を宛先ポートに接続すれば、IDS デバイスは TCP リセット パケットを送信して疑わしい攻撃者の TCP セッションを閉じることができます。

ローカル SPAN

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。たとえば、図 30-1 の場合、ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされます。ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。

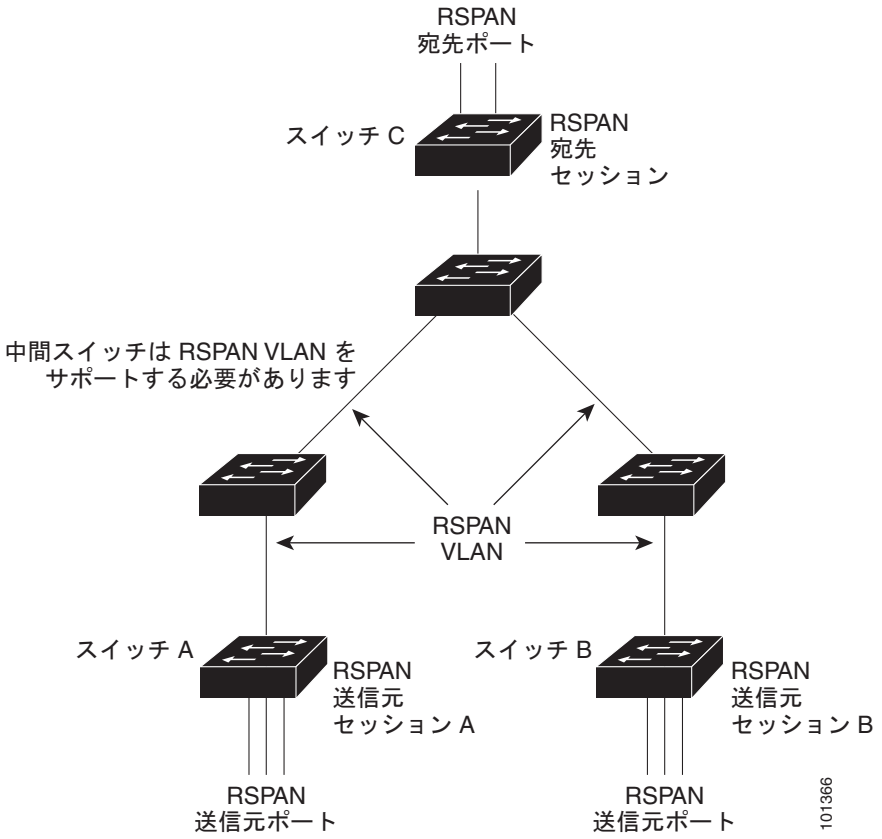
図 30-1　　単一スイッチでのローカル SPAN の設定例



リモート SPAN

RSPAN は異なるスイッチ上の送信元ポート、送信元 VLAN、および宛先ポートをサポートし、ネットワーク上にある複数のスイッチのリモート モニタリングを可能にします。図 30-2 に、スイッチ A およびスイッチ B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元スイッチでは、RSPAN 送信元としてポートまたは VLAN のいずれかを設定する必要があります。図中のスイッチ C のように、宛先は常に物理ポートになります。

図 30-2　　RSPAN の設定例



SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1 つまたは複数のポート上、あるいは 1 つまたは複数の VLAN 上でトラフィックをモニタし、そのモニタしたトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN（すべて単一のネットワーク デバイス上にある）を結び付けたものです。ローカル SPAN には、個別の送信元および宛先のセッションはありません。ローカル SPAN セッションはユーザが指定した入力および出力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも 1 つの RSPAN 送信元セッション、1 つの RSPAN VLAN、および少なくとも 1 つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームが転送される点を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを介して宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタギングを除去し、宛先ポートに送ります。RSPAN 宛先セッションの目的は、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットを解析のためにユーザにコピーすることです。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。RSPAN 送信元セッションと宛先セッションを分離する中間スイッチを配置することもできます。これらのスイッチには RSPAN の実行機能は不要ですが、RSPAN VLAN の要求に応答する必要があります（「RSPAN VLAN」（P.30-8）を参照）。

SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- スイッチは最大 2 つの送信元セッションをサポートします（ローカル SPAN および RSPAN 送信元セッション）。同じスイッチ内でローカル SPAN と RSPAN の送信元セッションの両方を実行できます。スイッチは合計 66 個の送信元および RSPAN 宛先セッションをサポートします。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、設定できる宛先ポート数は最大 64 です。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- RSPAN がイネーブルの場合、モニタ中の各パケットは 2 回伝送されます（1 回は標準トラフィックとして、もう 1 回はモニタされたパケットとして）。したがって、多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。つまり、RSPAN 送信元セッションにローカル宛先ポートを設定したり、RSPAN 宛先セッションにローカル送信元ポートを設定したり、同じスイッチ上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

SPAN セッションのモニタ対象トラフィック タイプ

- RX（受信）SPAN：受信（または入力）SPAN の役割は、送信元インターフェイスまたは VLAN が受信したすべてのパケットを、スイッチが変更または処理を行う前にできるだけ多くモニタすることです。送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。

  Diffserv コード ポイント（DSCP）の変更など、ルーティングや Quality of Service（QoS）が原因で変更されたパケットは、変更される前にコピーされます。

  受信処理中にパケットをドロップする可能性のある機能は、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットがドロップされた場合でも、パケットのコピーを受信します。パケットをドロップする可能性のある機能は、標準および拡張 IP 入力アクセス コントロール リスト（ACL）、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- TX（送信）SPAN：送信（または出力）SPAN の役割は、スイッチによる変更および処理がすべて完了した後で、送信元インターフェイスが送信したすべてのパケットをできるだけ多くモニタすることです。送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。

  ルーティングが原因で変更されたパケット（存続可能時間（TTL）、MAC アドレス、QoS 値の変更など）は、宛先ポートで（変更されて）コピーされます。

  送信処理中にパケットをドロップする可能性のある機能は、SPAN 用の複製コピーにも影響します。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

- 両方：SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニタすることもできます。これはデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。通常、SPAN は Cisco Discovery Protocol（CDP）、VLAN トランキング プロトコル（VTP）、Dynamic Trunking Protocol（DTP）、スパニングツリー プロトコル（STP）、ポート集約プロトコル（PAgP）などのブリッジ プロトコル データ ユニット（BPDU）パケットおよびレイヤ 2 プロトコルをモニタしません。ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

- 送信元ポートの場合と同じカプセル化設定（タグなし、または IEEE 802.1Q）を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットがモニタされます。

したがって、カプセル化レプリケーションがイネーブルにされたローカル SPAN セッションでは、タグなし、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

スイッチの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットがドロップされることがあります。一般に、これらの特性は互いに無関係です。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニタされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スイッチの輻輳が原因でドロップされた出力パケットは、出力 SPAN からもドロップされます。

SPAN の設定によっては、同一送信元のパケットのコピーが複数、SPAN 宛先ポートに送信されます。たとえば、ポート A での RX モニタ、ポート B での TX モニタ用に、双方向（RX と TX）SPAN セッションが設定されているとします。パケットがポート A を介してスイッチに着信し、ポート B にスイッチングされると、着信パケットと発信パケットの両方が宛先ポートに送信されます。このため、両方のパケットは同じものになります（レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります）。

ソース ポート

送信元ポート（別名*監視対象ポート*）は、ネットワーク トラフィック分析のために監視するスイッチド ポートまたはルーテッド ポートです。1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニタできます。スイッチは、任意の数の送信元ポート（スイッチで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートしています。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数は最大 2 つ（ローカルまたは RSPAN）であるため、単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニタできます。
- モニタする方向（入力、出力、または両方）を指定して、各送信元ポートを設定できます。
- すべてのポート タイプ（EtherChannel、ファスト イーサネット、ギガビット イーサネットなど）が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポート チャネルに含まれている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセス ポート、トランク ポート、ルーテッド ポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタすることが可能です。

送信元 VLAN

VLAN ベースの SPAN（VSPAN）では、1 つまたは複数の VLAN のネットワーク トラフィックをモニタできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニタされます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートのみです。
- VLAN フィルタリングはポートベース セッションにのみ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の該当 VLAN のみがモニタされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名 *モニタ側ポート*）が必要です。

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチに存在している必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションだけを実行するスイッチには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。
- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。削除されたポートがルーテッド ポートであった場合、このポートはルーテッド ポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。
- 送信元ポートにすることはできません。
- EtherChannel グループまたは VLAN にすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- スイッチの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化について次のとおり動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなし、または IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブルになっているローカル SPAN セッションの出力に、タグなしまたは IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN の送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には次の特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、**remote-span** VLAN コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VLAN トランキング プロトコル（VTP）に対して可視である VLAN 1 ～ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲（1006 ～ 4096）内の RSPAN VLAN ID を割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信したりできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN と他の機能の相互作用

- ルーティング：SPAN はルーテッド トラフィックを監視しません。VSPAN が監視するのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックは監視しません。たとえば、VLAN が受信モニタされ、スイッチが別の VLAN から監視対象 VLAN にトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP：VTP を使用すると、スイッチ間で RSPAN VLAN のプルーニングが可能です。

- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定値を、いつでも変更できます。ただし、宛先ポートの VLAN メンバーシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してからです。送信元ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。
- EtherChannel：EtherChannel グループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

  モニタ対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。モニタ対象の EtherChannel グループからポートを削除すると、送信元ポート リストからそのポートが自動的に削除されます。

  EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループ メンバのままですが、*inactive* または *suspended* ステートになります。

  EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよびモニタ対象ポート リストから削除されます。
- マルチキャスト トラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未編集のパケットが 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト パケットの送信回数は反映されません。
- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。
- セキュア ポートを SPAN 宛先ポートにすることはできません。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。
- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。

ローカル SPAN 設定時の注意事項

- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するトラフィックがモニタされるだけです。

- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなしまたは IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。RSPAN 宛先ポートの場合、発信パケットはタグなしです。
- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

RSPAN 設定時の注意事項

- 「ローカル SPAN 設定時の注意事項」（P.30-9）のすべての項目は RSPAN にも当てはまります。
- RSPAN VLAN には特殊なプロパティがあるので、RSPAN VLAN として使用する VLAN をネットワーク上に一部確保します。これらの VLAN にはアクセス ポートを割り当てないでください。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択的にフィルタリングまたはモニタできます。RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのスイッチで VLAN RSPAN 機能がサポートされていることを確認してください。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、スイッチはセッション間にわたるトラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
  - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
  - 参加するすべてのスイッチで RSPAN がサポートされている。
- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラッディングが防止されます。

SPAN および RSPAN のデフォルト設定

表 30-1　SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN のステート（SPAN および RSPAN）	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方（**both**）
カプセル化タイプ（宛先ポート）	ネイティブ形式（タグなしパケット）
入力転送（宛先ポート）	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。
RSPAN VLAN	未設定

SPAN および RSPAN の設定方法

ローカル SPAN セッションの作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number*：指定できる範囲は 1 ～ 66 です。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。

	コマンド	目的
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number*：指定できる範囲は 1 ～ 66 です。 *interface-id*：モニタする送信元ポートまたは送信元 VLAN を指定します。 • source *interface-id*：モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 6 です。 • *vlan-id*：モニタする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4096 です（RSPAN VLAN は除く）。 **（注）** 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。 （任意）[**,** | **-**]：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。 **（注）** **monitor session** *session_number* **source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**]}	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 *session_number*：ステップ 3 で入力したセッション番号を指定します。 **（注）** ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 • *interface-id*：宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）**[, | -]**：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**encapsulation replicate**：宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 **（注）** **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 5	**end**	特権 EXEC モードに戻ります。

ローカル SPAN セッションの作成および着信トラフィックの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} **[, | -]** [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 *session_number*：ステップ 3 で入力したセッション番号を指定します。 *interface-id*：宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマまたはハイフンの前後にスペースを 1 つずつ入力します。 （任意）**encapsulation replicate**：宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 **ingress**：宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 • **dot1q vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

フィルタリングする VLAN の指定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number*：指定できる範囲は 1 ～ 66 です。 **all**：すべての SPAN セッションを削除します。 **local**：すべてのローカル セッションを削除します。 **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id*	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 *session_number*：指定できる範囲は 1 ～ 66 です。 *interface-id*：モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number*：ステップ 3 で指定したセッション番号を入力します。 *vlan-id*：指定できる範囲は 1 ～ 4096 です。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**]}	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 *session_number*：ステップ 3 で入力したセッション番号を指定します。 *interface-id*：宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）**encapsulation replicate**：宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。
ステップ 6	**end**	特権 EXEC モードに戻ります。

RSPAN VLAN としての VLAN の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4096 です。 RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN 専用）にすることはできません。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RSPAN 送信元セッションの作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の RSPAN 設定を削除します。 *session_number*：指定できる範囲は 1 ～ 66 です。 **all**：すべての RSPAN セッションを削除します。 **local**：すべてのローカル セッションを削除します。 **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number*：指定できる範囲は 1 ～ 66 です。 RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 • *interface-id*：モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id*：モニタする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4096 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。 （任意）[**,** | **-**]：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。
ステップ 4	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションと宛先 RSPAN VLAN を指定します。 *session_number*：ステップ 3 で定義したセッション番号を入力します。 *vlan-id*：モニタする送信元 RSPAN VLAN を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RSPAN 宛先セッションの作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	送信元スイッチで作成された RSPAN VLAN の VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ～ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 2 ～ 4 は不要です。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として識別します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の RSPAN 設定を削除します。 *session_number*：指定できる範囲は 1 ～ 66 です。 **all**：すべての RSPAN セッションを削除します。 **local**：すべてのローカル セッションを削除します。 **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 6	**monitor session** *session_number* **source remote vlan** *vlan-id*	RSPAN セッションと送信元 RSPAN VLAN を指定します。 *session_number*：指定できる範囲は 1 ～ 66 です。 *vlan-id*：モニタする送信元 RSPAN VLAN を指定します。
ステップ 7	**monitor session** *session_number* **destination interface** *interface-id*	RSPAN セッションと宛先インターフェイスを指定します。 *session_number*：ステップ 6 で定義した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 *interface-id*：宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。
ステップ 8	**end**	特権 EXEC モードに戻ります。

RSPAN 宛先セッションの作成および着信トラフィックの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。
ステップ 3	**monitor session** *session_number* **source remote vlan** *vlan-id*	RSPAN セッションと送信元 RSPAN VLAN を指定します。 *session_number*：指定できる範囲は 1 ～ 66 です。 *vlan-id*：モニタする送信元 RSPAN VLAN を指定します。
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケットカプセル化、および着信 VLAN とカプセル化を指定します。 *session_number*：ステップ 4 で定義したセッション番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 *interface-id*：宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** を追加のキーワードと一緒に入力します。 • **dot1q vlan** *vlan-id*：VLAN をデフォルトの VLAN として指定し、IEEE 802.1Q カプセル化を使用して着信パケットを転送します。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

フィルタリングする VLAN の指定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number*：指定できる範囲は 1 ～ 66 です。 **all**：すべての SPAN セッションを削除します。 **local**：すべてのローカル セッションを削除します。 **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id*	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 *session_number*：指定できる範囲は 1 ～ 66 です。 *interface-id*：モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number*：ステップ 3 で指定したセッション番号を入力します。 *vlan-id*：指定できる範囲は 1 ～ 4096 です。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 *session_number*：ステップ 3 で指定したセッション番号を入力します。 *vlan-id*：モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

SPAN と RSPAN のモニタリングとメンテナンス

show monitor [**session** *session_number*]	SPAN または RSPAN 設定を確認します。

SPAN および RSPAN の設定例

ローカル SPAN セッションの設定：例

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 にミラーリングします。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/2
encapsulation replicate
Switch(config)# end
```

ローカル SPAN セッションの変更：例

次に、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/1
Switch(config)# end
```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/1 rx
```

ポート 1 で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ～ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation
replicate ingress dot1q vlan 6
Switch(config)# end
```

トランク ポート上のすべての VLAN をモニタするには、**no monitor session** *session_number* **filter** グローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/1
Switch(config)# end
```

RSPAN の設定：例

次に、RSPAN VLAN 901 を作成する例を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

SPAN セッションに関する VLAN の設定：例

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet1/1
Switch(config)# end
```

RSPAN セッションの変更：例

次に、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/2 rx

Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/2 ingress vlan 6
Switch(config)# end
```

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Switch(config)# no monitor session 2
(config)# monitor session 2 source interface gigabitethernet1/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
```

```
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 31

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの制約事項

- 次の機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
  - LLDP-MED ロケーション 802.lab
  - CoS/DSCP への LLDP-MED の統合
  - ネットワーク ポリシー TLV およびロケーション TLV
  - ワイヤード ロケーション サービス

LLDP、LLDP-MED、およびワイヤード ロケーション サービスに関する情報

Cisco Discovery Protocol（CDP）は、すべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データ リンク層）上で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、ネットワーク接続されている 他のシスコ デバイスを自動的に検出し、識別できます。

スイッチでは他社製のデバイスをサポートし他のデバイス間の相互運用性を確保するために、IEEE 802.1AB リンク層検出プロトコル（LLDP）をサポートしています。LLDP は、ネットワーク デバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用するネイバー探索プロトコルです。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP は一連の属性をサポートし、これらを使用してネイバー デバイスを検出します。属性には、Type、Length、および Value の説明が含まれていて、これらを TLV と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用できます。このプロトコルは、設定情報、デバイス機能、およびデバイス ID などの詳細情報をアドバタイズできます。

スイッチは、次の基本管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述 TLV
- システム名 TLV
- システム記述 TLV
- システム機能 TLV
- 管理アドレス TLV

次の IEEE 固有の LLDP TLV もアドバタイズに使用されて LLDP-MED をサポートします。

- ポート VLAN ID TLV（IEEE 802.1 に固有の TLV）
- MAC/PHY コンフィギュレーション / ステータス TLV（IEEE 802.3 に固有の TLV）

（注）　スイッチ スタックは、ネットワーク内で 1 つのスイッチと見なされます。したがって、LLDP は個々のスタック メンバではなく、スイッチ スタックを検出します。

LLDP-MED

LLDP for Media Endpoint Devices（LLDP-MED）は LLDP の拡張版で、IP 電話などのエンドポイント デバイスとスイッチなどのネットワーク デバイスの間で動作します。特に VoIP アプリケーションをサポートし、検出機能、ネットワーク ポリシー、Power over Ethernet（PoE）、インベントリ管理、およびロケーション情報に関する TLV を提供します。デフォルトで、すべての LLDP-MED TLV がイネーブルです。

LLDP-MED では、次の TLV がサポートされます。

- LLDP-MED 機能 TLV

  LLDP-MED エンドポイントは、接続装置がサポートする機能と現在イネーブルになっている機能を識別できます。

- ネットワーク ポリシー TLV

  ネットワーク接続デバイスとエンドポイントはともに、VLAN 設定、および関連するレイヤ 2 とレイヤ 3 属性をポート上の特定アプリケーションにアドバタイズできます。たとえば、スイッチは使用する VLAN 番号を IP 電話に通知できます。IP 電話は任意のスイッチに接続し、VLAN 番号を取得してから、コール制御の通信を開始できます。

  ネットワーク ポリシー プロファイル TLV を定義することによって、VLAN、サービス クラス（CoS）、Diffserv コード ポイント（DSCP）、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成できます。その後、これらのプロファイル属性は、スイッチで中央集約的に保守され、IP 電話に伝播されます。

- 電源管理 TLV

  LLDP-MED エンドポイントとネットワーク接続デバイスの間で拡張電源管理を可能にします。スイッチおよび IP 電話は、デバイスの受電方法、電源プライオリティ、デバイスの消費電力などの電源情報を通知することができます。

- インベントリ管理 TLV

  エンドポイントは、スイッチにエンドポイントの詳細なインベントリ情報を送信することが可能です。インベントリ情報には、ハードウェア リビジョン、ファームウェア バージョン、ソフトウェア バージョン、シリアル番号、メーカー名、モデル名、Asset ID TLV などがあります。

- ロケーション TLV

  スイッチからのロケーション情報をエンドポイント デバイスに提供します。ロケーション TLV はこの情報を送信することができます。

  - 都市ロケーション情報

    都市アドレス情報および郵便番号情報を提供します。都市ロケーション情報の例には、地名、番地、郵便番号などがあります。

  - ELIN ロケーション情報

    発信側のロケーション情報を提供します。ロケーションは、緊急ロケーション識別番号（ELIN）によって決定されます。これは、緊急通報を Public Safety Answering Point（PSAP）にルーティングする電話番号で、PSAP はこれを使用して緊急通報者にコールバックすることができます。

ワイヤード ロケーション サービス

スイッチはワイヤード ロケーション サービス機能を使用して、接続されたデバイスのロケーションおよび接続のトラッキング情報を Cisco Mobility Services Engine（MSE）に送信します。トラッキングされたデバイスは、ワイヤレス エンドポイント、ワイヤード エンドポイント、またはワイヤード スイッチやワイヤード コントローラになります。スイッチは、MSE にネットワーク モビリティ サービス プロトコル（NMSP）のロケーション通知および接続通知を介して、デバイスのリンク アップ イベントおよびリンク ダウン イベントを通知します。

MSE がスイッチに対して NMSP 接続を開始すると、サーバ ポートが開きます。MSE がスイッチに接続する場合は、バージョンの互換性を確保する 1 組のメッセージ交換およびサービス交換情報があり、その後にロケーション情報の同期が続きます。接続後、スイッチは定期的にロケーション通知および接続通知を MSE に送信します。インターバル中に検出されたリンク アップ イベントまたはリンク ダウン イベントは、集約されてインターバルの最後に送信されます。

スイッチがリンク アップ イベントまたはリンク ダウン イベントでデバイスの有無を確認した場合は、スイッチは、MAC アドレス、IP アドレス、およびユーザ名のようなクライアント固有情報を取得します。クライアントが LLDP-MED または CDP に対応している場合は、スイッチは LLDP-MED ロケーション TLV または CDP でシリアル番号および UDI を取得します。

デバイス機能に応じて、スイッチは次のクライアント情報をリンク アップ時に取得します。

- ポート接続で指定されたスロットおよびポート。
- クライアント MAC アドレスで指定された MAC アドレス。
- ポート接続で指定された IP アドレス。
- 802.1X ユーザ名（該当する場合）。
- デバイス カテゴリは、*wired station* として指定されます。
- ステートは *new* として指定されます。
- シリアル番号、UDI。
- モデル番号
- スイッチによる関連付け検出後の時間（秒）。

デバイス機能に応じて、スイッチは次のクライアント情報をリンク ダウン時に取得します。

- 切断されたスロットおよびポート。
- MAC アドレス
- IP アドレス
- 802.1X ユーザ名（該当する場合）。
- デバイス カテゴリは、*wired station* として指定されます。
- ステートは *delete* として指定されます。
- シリアル番号、UDI。
- スイッチによる関連付け解除の検出後の時間（秒）。

スイッチがシャットダウンする場合は、スイッチは、MSE との NMSP 接続を終了する前に、ステート *delete* および IP アドレスとともに接続情報通知を送信します。MSE は、この通知を、スイッチに関連付けられているすべてのワイヤード クライアントに対する関連付け解除として解釈します。

スイッチ上のロケーション アドレスを変更すると、スイッチは、影響を受けるポートを識別する NMSP ロケーション通知メッセージ、および変更されたアドレス情報を送信します。

デフォルトの LLDP 設定

表 31-1　デフォルトの LLDP 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム（廃棄までの時間）	120 秒。
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	ディセーブル（すべての TLV を送受信不可）
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	ディセーブル
LLDP 転送	ディセーブル
LLDP med-tlv-select	ディセーブル（すべての LLDP-MED TLV への送信）。LLDP がグローバルにイネーブルにされると、LLDP-MED-TLV もイネーブルになります。

LLDP、LLDP-MED、およびワイヤード ロケーション サービス設定時の注意事項

- インターフェイスがトンネル ポートに設定されていると、LLDP は自動的にディセーブルになります。

- 最初にインターフェイス上にネットワークポリシー プロファイルを設定した場合、インターフェイス上に **switchport voice vlan** コマンドを適用できません。**switchport voice vlan** *vlan-id* がすでに設定されているインターフェイスには、ネットワーク ポリシー プロファイルを適用できます。このように、そのインターフェイスには、音声または音声シグナリング VLAN ネットワーク ポリシー プロファイルが適用されます。
- ネットワーク ポリシー プロファイルを持つインターフェイス上では、スタティック セキュア MAC アドレスを設定できません。
- プライベート VLAN ポート上では、ネットワーク ポリシー プロファイルを設定できません。
- ワイヤード ロケーションが機能するためには、まず、**ip device tracking** グローバル コンフィギュレーション コマンドを入力する必要があります。

LLDP-MED TLV

デフォルトでは、スイッチはエンド デバイスから LLDP-MED パケットを受信するまで、LLDP パケットだけを送信します。スイッチは、MED TLV を持つ LLDP パケットを送信します。LLDP-MED エントリが期限切れになった場合は、スイッチは LLDP パケットだけを送信します。

lldp インターフェイス コンフィギュレーション コマンドを使用すれば、インターフェイスがこの表にリストされている TLV を送信しないように設定できます。

表 31-2　LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED インベントリ管理 TLV
location	LLDP-MED ロケーション TLV（LAN Base イメージ限定）
network-policy	LLDP-MED ネットワーク ポリシー TLV（LAN Base イメージ限定）
power-management	LLDP-MED 電源管理 TLV

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法

LLDP のイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lldp run**	スイッチの全体的で LLDP をイネーブルにします。
ステップ 3	**interface** *interface-id*	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lldp transmit**	LLDP パケットを送信するようにインターフェイスをイネーブルにします。

	コマンド	目的
ステップ 5	**lldp receive**	LLDP パケットを受信するようにインターフェイスをイネーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。

LLDP 特性の設定

LLDP 更新の頻度、情報を廃棄するまでの保持期間、および初期化遅延時間を設定できます。送受信する LLDP および LLDP-MED TLV も選択できます。

（注）　ステップ 2 ～ 5 は任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lldp holdtime** *seconds*	（任意）デバイスから送信された情報を受信側デバイスが廃棄するまで保持する必要がある期間を指定します。 指定できる範囲は 0 ～ 65535 秒です。デフォルトは 120 秒です。
ステップ 3	**lldp reinit** *delay*	（任意）任意のインターフェイス上で LLDP の初期化の遅延時間（秒）を指定します。 指定できる範囲は 2 ～ 5 秒です。デフォルトは 2 秒です。
ステップ 4	**lldp timer** *rate*	（任意）インターフェイス上で LLDP の更新の遅延時間（秒）を指定します。 指定できる範囲は 5 ～ 65534 秒です。デフォルトは 30 秒です。
ステップ 5	**lldp tlv-select**	（任意）送受信する LLDP TLV を指定します。
ステップ 6	**lldp med-tlv-select**	（任意）送受信する LLDP-MED TLV を指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

LLDP-MED TLV の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	LLDP-MED TLV を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**lldp med-tlv-select** *tlv*	イネーブルにする TLV を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

Network-Policy TLV の設定

この作業では、ネットワーク ポリシー プロファイルを作成して、ポリシー属性を設定し、それをインターフェイスに適用する方法について説明します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**network-policy profile** *profile number*	ネットワーク ポリシー プロファイル番号を指定し、ネットワーク ポリシー コンフィギュレーション モードを開始します。指定できる範囲は 1 ～ 4294967295 です。
ステップ 3	{**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos** *cvalue* | **dscp** *dvalue*}] | [[**dot1p** {**cos** *cvalue* | **dscp** *dvalue*}] | **none** | **untagged**]	ポリシー属性の設定: **voice**：音声アプリケーション タイプを指定します。 **voice-signaling**：音声シグナリング アプリケーション タイプを指定します。 **vlan**：音声トラフィックのネイティブ VLAN を指定します。 *vlan-id*：（任意）音声トラフィックの VLAN を指定します。指定できる範囲は 1 ～ 4096 です。 **cos** *cvalue*：（任意）設定された VLAN のレイヤ 2 プライオリティ サービス クラス（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルトは 0 です。 **dscp** *dvalue*：（任意）設定された VLAN の Differentiated Services Code Point（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルトは 0 です。 **dot1p**：（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話機を設定します。 **none**：（任意）音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。 **untagged**：（任意）タグなしの音声トラフィックを送信するように IP Phone を設定します。これが IP Phone のデフォルト設定になります。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	ネットワーク ポリシー プロファイルを設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**network-policy** *profile number*	ネットワーク ポリシー プロファイル番号を指定します。
ステップ 7	**lldp med-tlv-select network-policy**	ネットワーク ポリシー TLV を指定します。
ステップ 8	**end**	特権 EXEC モードに戻ります。

ロケーション TLV およびワイヤード ロケーション サービスの設定

この作業では、エンドポイントのロケーション情報を設定し、インターフェイスに適用する方法について説明します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location** {**admin-tag** *string* | **civic-location identifier** *id* | **elin-location** *string* **identifier** *id*}	エンドポイントにロケーション情報を指定します。 • **admin-tag**：管理タグまたはサイト情報を指定します。 • **civic-location**：都市ロケーション情報を指定します。 • **elin-location**：緊急ロケーション情報（ELIN）を指定します。 • **identifier** *id*：都市ロケーションの ID を指定します。 • *string*：サイト情報またはロケーション情報を英数字形式で指定します。
ステップ 3	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id*	ロケーション情報を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**location** {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}	インターフェイスのロケーション情報を入力します。 **additional-location-information**：ロケーション（位置）に関する追加情報を指定します。 **civic-location-id**：インターフェイスのグローバル都市ロケーション情報を指定します。 **elin-location-id**：インターフェイスの緊急ロケーション情報を指定します。 *id*：都市ロケーションまたは ELIN ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。 *word*：追加のロケーション情報を指定する語またはフレーズを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**nmsp enable**	スイッチで NMSP 機能をイネーブルにします。
ステップ 8	**nmsp notification interval** {**attachment** | **location**} *interval-seconds*	NMSP 通知間隔を指定します。 **attachment**：接続通知間隔を指定します。 **location**：位置通知間隔を指定します。 *interval-seconds*：スイッチから MSE にロケーション更新または接続更新が送信されるまでの期間（秒）。指定できる範囲は 1 ～ 30 です。デフォルト値は 30 です。
ステップ 9	**end**	特権 EXEC モードに戻ります。

LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス

コマンド	説明
clear lldp counters	トラフィック カウンタを 0 にリセットします。
clear lldp table	LLDP ネイバー情報テーブルを削除します。
clear nmsp statistics	NMSP 統計カウンタをクリアします。
show lldp	送信頻度、送信するパケットのホールドタイム、LLDP 初期化の遅延時間のような、インターフェイス上のグローバル情報を表示します。
show lldp entry *entry-name*	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力すると、すべてのネイバーの表示、またはネイバーの名前の入力が可能です。
show lldp interface [*interface-id*]	LLDP がイネーブルに設定されているインターフェイスに関する情報を表示します。 表示対象を特定のインターフェイスに限定できます。
show lldp neighbors [*interface-id*] [**detail**]	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show lldp traffic	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、LLDP カウンタを表示します。
show location admin-tag *string*	指定した管理タグまたはサイトのロケーション情報を表示します。
show location civic-location identifier *id*	特定のグローバル都市ロケーションのロケーション情報を表示します。
show location elin-location identifier *id*	緊急ロケーションのロケーション情報を表示します。
show network-policy profile	設定されたネットワークポリシー プロファイルを表示します。
show nmsp	NMSP 情報を表示します。

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例

LLDP のイネーブル化：例

次に、LLDP をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

次に、インターフェイス上で LLDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# lldp transmit
```

```
Switch(config-if)# lldp receive
Switch(config-if)# end
```

LDP パラメータの設定：例

次に、LLDP パラメータを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config)# lldp timer 30
Switch(config)# end
```

TLV の設定：例

次に、インターフェイス上で TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```

ポリシーネットワークの設定：例

次に、CoS を持つ音声アプリケーションの VLAN 100 を設定して、インターフェイス上のネットワーク ポリシー プロファイルおよびネットワーク ポリシー TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
Switch(config-network-policy)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# network-policy profile 1
Switch(config-if)# lldp med-tlv-select network-policy
```

音声アプリケーションの設定：例

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
Switch(config-network-policy)# voice vlan dot1p dscp 34
```

都市ロケーション情報の設定：例

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
```

```
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

NMSP のイネーブル化：例

次の例では、スイッチ上で NMSP をイネーブルにして、位置通知間隔を 10 秒に設定する方法を示します。

```
Switch(config)# nmsp enable
Switch(config)# nmsp notification interval location 10
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド Cisco IOS システム管理コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 32

CDP の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

CDP の概要

CDP

CDP はすべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスにネイバー シスコ デバイスを検出できます。また、下位レイヤのトランスペアレント プロトコルが稼働しているネイバー デバイスのデバイス タイプや、簡易ネットワーク管理プロトコル（SNMP）エージェント アドレスを学習することもできます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、サブネットワーク アクセス プロトコル（SNAP）をサポートしているすべてのメディアで動作します。CDP はデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャスト アドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

CDP はスイッチ上で Network Assistant をイネーブルにすることで、ネットワークをグラフィカルに表示できます。スイッチは CDP を使用してクラスタ候補を検出し、クラスタ メンバ、およびコマンド スイッチから最大 3 台（デフォルト）離れたクラスタ対応の他のデバイスについての情報を維持します。

スイッチおよび Cisco Medianet が稼働している接続されたエンドポイント デバイスの場合は、次のイベントが発生します。

- CDP は、スイッチと直接通信する接続されたエンドポイントを識別します。
- 隣接デバイスのレポートの重複を防ぐため、1 つの有線スイッチだけ報告します。
- 有線スイッチとエンドポイントは、ロケーションの送信と受信の両方を行います。

スイッチは CDP バージョン 2 をサポートします。

CDP のデフォルト設定

表 32-1　CDP のデフォルト設定

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー（パケット更新頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

CDP の設定方法

CDP パラメータの設定

CDP 更新の頻度、廃棄するまで情報を保持する期間、およびバージョン 2 アドバタイズを送信するかどうかを設定できます。

（注） ステップ 2 ～ 4 はすべて任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp timer** *seconds*	（任意）CDP 更新の送信頻度を秒単位で設定します。 指定できる範囲は 5 ～ 254 です。デフォルトは 60 秒です。
ステップ 3	**cdp holdtime** *seconds*	（任意）受信デバイスがこのデバイスから送信された情報を破棄せずに保持する時間を指定します。 指定できる範囲は 10 ～ 255 秒です。デフォルトは 180 秒です。
ステップ 4	**cdp advertise-v2**	（任意）バージョン 2 アドバタイズを送信するように CDP を設定します。 これは、デフォルトの状態です。
ステップ 5	**end**	特権 EXEC モードに戻ります。

CDP のディセーブル化

CDP はデフォルトで有効になっています。

（注）　スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no cdp run**	CDP をグローバルにディセーブルにします。
ステップ 3	**interface** *interface-id*	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no cdp enable**	インターフェイス上で CDP をディセーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。

CDP のモニタおよびメンテナンス

コマンド	説明
clear cdp counters	トラフィック カウンタを 0 にリセットします。
clear cdp table	ネイバー デバイスに関する情報を収めた CDP テーブルを削除します。
show cdp	送信間隔、送信したパケットの保持時間などのグローバル情報を表示します。
show cdp entry *entry-name* [**protocol** | **version**]	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力してすべての CDP ネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定されたネイバー上でイネーブルになっているプロトコルの情報や、デバイス上で稼働しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。
show cdp interface [*interface-id*]	CDP がイネーブルに設定されているインターフェイスの情報を表示します。 必要なインターフェイスの情報だけを表示できます。
show cdp neighbors [*interface-id*] [**detail**]	装置タイプ、インターフェイス タイプ、インターフェイス番号、保持時間の設定値、機能、プラットフォーム、ポート ID を含めたネイバー情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show cdp traffic	CDP カウンタ（送受信されたパケット数およびチェックサム エラーを含む）を表示します。

CDP の設定例

CDP パラメータの設定：例

次の例は、CDP パラメータを設定する方法を示しています。

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

CDP のイネーブル化：例

次に、特定のポート上で、ディセーブル化されている CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# cdp enable
Switch(config-if)# end
```

（注）　CDP がスイッチ インターフェイスでディセーブルの場合、音声 VLAN はポート セキュリティにはカウントされません。

次に、ディセーブル化されている CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド Cisco IOS システム管理コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
スイッチ クラスタの設定	第 6 章「スイッチ クラスタの設定」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

CHAPTER 33

UDLD の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

UDLD の前提条件

- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。

UDLD の制約事項

- UDLD は非同期転送モード（ATM）ポート上ではサポートされていません。
- UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。
- ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD について

UDLD

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタしたり、単一方向リンクの存在を検出したりできるようにするためのレイヤ 2 プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている

必要があります。UDLD は単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単一方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、ノーマル（デフォルト）とアグレッシブの 2 つの動作モードをサポートしています。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。アグレッシブ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラフィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤った接続を検出しません。ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ 1 メカニズムがリンクの物理的な問題を検出するため、リンクは稼働状態でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD hello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ 1 の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブ モードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

単一方向の検出方法

UDLD は、2 通りの方法を使用して動作します。

- ネイバー データベース メンテナンス

  UDLD は、アクティブな各ポート上で hello パケット（別名アドバタイズまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

  スイッチが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れる前に、スイッチが新しい hello メッセージを受信すると、古いエントリが新しいエントリで置き換えられます。

  UDLD の稼働中にポートがディセーブルになったり、ポート上で UDLD がディセーブルになったり、またはスイッチをリセットした場合、UDLD は設定変更の影響を受けるポートの既存のキャッシュ エントリをすべて消去します。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

- イベントドリブン検出およびエコー

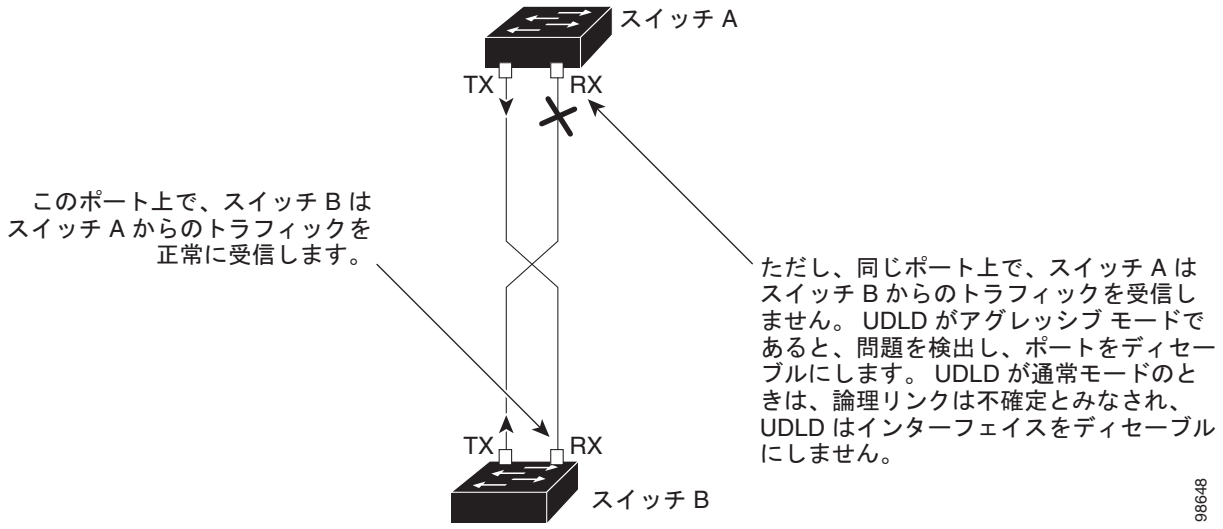
  UDLD は検出メカニズムとしてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作はすべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

  検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ モードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

通常モードにある UDLD が、アドバタイズまたは検出段階にあり、すべてのネイバーのキャッシュ エントリが期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。

アグレッシブ モードをイネーブルにしていて、ポートのすべてのネイバーがアドバタイズまたは検出段階で期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。高速な一連のメッセージの送受信後に、リンク ステートが不確定のままの場合、UDLD はポートをシャットダウンします。

図 33-1　UDLD による単一方向リンクの検出



UDLD のデフォルト設定

表 33-1　UDLD のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ ポート上でディセーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX ポート上でディセーブル
UDLD アグレッシブ モード	ディセーブル

UDLD の設定方法

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは通常モードで UDLD をイネーブルにし、スイッチ上のすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、次の手順に従ってください：

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*}	UDLD モードの動作を指定します。 • **aggressive**：すべての光ファイバ ポート上で、UDLD をアグレッシブ モードでイネーブルにします。 • **enable**：スイッチ上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。UDLD はデフォルトでディセーブルです。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定を上書きします。 アグレッシブおよび通常モードの詳細については、「動作モード」（P.33-2）を参照してください。 • **message time** *message-timer-interval*：アドバタイズ フェーズに存在し、双方向と検出されたポートにおける UDLD プローブ メッセージ間の間隔を設定します。指定できる範囲は 1 ～ 90 秒です。 **（注）** このコマンドが作用するのは、光ファイバ ポートだけです。他のポート タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。詳細については、「インターフェイス上での UDLD のイネーブル化」（P.33-5）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。

インターフェイス上での UDLD のイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	UDLD のためにイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**udld port** [**aggressive**]	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポート上で、UDLD を通常モードでイネーブルにします。 • **udld port aggressive**：指定されたポート上で、UDLD をアグレッシブ モードでイネーブルにします。 **（注）** 特定の光ファイバ ポート上で UDLD をディセーブルにする場合は、**no udld port** インターフェイス コンフィギュレーション コマンドを使用します。 アグレッシブおよび通常モードの詳細については、「動作モード」（P.33-2）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

UDLD パラメータの設定およびリセット

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld reset**	（任意）UDLD によってディセーブルにされたすべてのポートをリセットします。
ステップ 3	**no udld** {**aggressive** | **enable**}	（任意）UDLD ポートをディセーブルにします。
ステップ 4	**udld** {**aggressive** | **enable**}	（任意）ディセーブルにされたポートを再度イネーブルにします。
ステップ 5	**errdisable recovery cause udld**	（任意）UDLD errdisable ステートから自動的に回復するためのタイマーをイネーブルにします。
ステップ 6	**errdisable recovery interval** *interval*	（任意）UDLD errdisable ステートから回復する時間を指定します。
ステップ 7	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**no udld port**	（任意）UDLD 光ファイバ ポートをディセーブルにします。
ステップ 9	**udld port** [**aggressive**]	（任意）ディセーブルにされた光ファイバ ポートを再度イネーブルにします。
ステップ 10	**shutdown**	（任意）インターフェイス ポートをディセーブルにします。
ステップ 11	**no shutdown**	（任意）ディセーブルのポートを再起動します。
ステップ 12	**show udld**	（任意）入力を確認します。

UDLD のメンテナンスおよびモニタリング

コマンド	目的
show udld [*interface-id*]	UDLD のステータスを表示します。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 34

RMON の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

RMON の前提条件

- RMON MIB オブジェクトにアクセスするために、スイッチ上で SNMP を設定する必要があります。
- NMS 上で汎用 RMON コンソール アプリケーションを使用し、RMON のネットワーク管理機能を利用することを推奨します。

RMON の制約事項

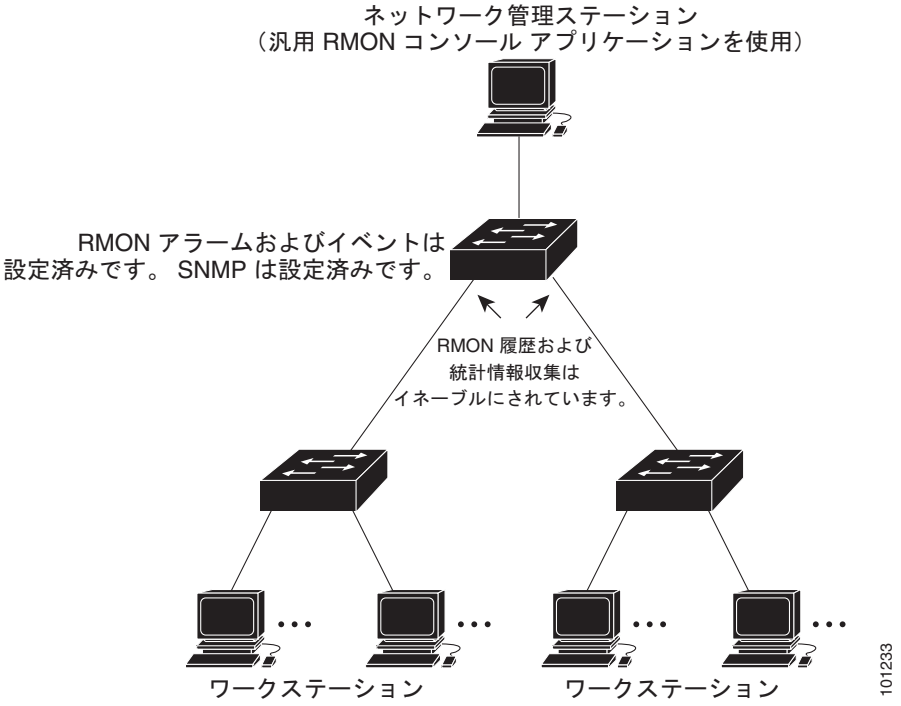
- 64 ビット カウンタは、RMON アラームではサポートされていません。

RMON について

RMON

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするためのインターネット技術特別調査委員会（IETF）標準モニタリング仕様です。図 34-1 のように、RMON 機能をスイッチの簡易ネットワーク管理プロトコル（SNMP）エージェントと組み合わせて使用することによって、接続されているすべての LAN セグメント上のスイッチ間で流れるすべてのトラフィックをモニタリングできます。

図 34-1　リモート モニタリングの例



スイッチは次の RMON グループ（RFC 1757 で規定）をサポートしています。

- 統計情報（RMON グループ 1）：インターフェイス上のイーサネットの統計情報（スイッチ タイプとサポートされているインターフェイスに応じた、ファスト イーサネットやギガビット イーサネット統計情報など）を収集します。
- 履歴（RMON グループ 2）：指定されたポーリング間隔で、イーサネット ポート上（スイッチ タイプおよびサポートされるインターフェイスに応じた、ファスト イーサネットおよびギガビット イーサネット統計情報を含む）の統計情報グループの履歴を収集します。
- アラーム（RMON グループ 3）：指定された期間、特定の管理情報ベース（MIB）オブジェクトをモニタリングし、指定された値（上限しきい値）でアラームを発生し、別の値（下限しきい値）でアラームをリセットします。アラームはイベントと組み合わせて使用できます。アラームがイベントを発生させ、イベントによってログ エントリまたは SNMP トラップが生成されるようにできます。
- イベント（RMON グループ 9）：アラームによってイベントが発生したときのアクションを指定します。アクションは、ログ エントリまたは SNMP トラップを生成できます。

このソフトウェア リリースがサポートするスイッチは、RMON データの処理にハードウェア カウンタを使用するので、モニタが効率的になり、処理能力はほとんど必要ありません。

（注）　64 ビット カウンタは、RMON アラームではサポートされていません。

RMON はデフォルトでディセーブルです。アラームまたはイベントは設定されていません。

RMON の設定方法

RMON アラームおよびイベントの設定

スイッチを RMON 対応として設定するには、コマンドライン インターフェイス（CLI）または SNMP 準拠のネットワーク管理ステーションを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rmon alarm** *number variable interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]	MIB オブジェクトにアラームを設定します。 • *number*：アラーム番号を指定します。指定できる範囲は 1 ～ 65535 です。 • *variable*：モニタ対象の MIB オブジェクトを指定します。 • *interval*：アラームが MIB 変数をモニタリングする時間を秒数で指定します。指定できる範囲は 1 ～ 4294967295 秒です。 • 各 MIB 変数を直接テストする場合は、**absolute** キーワードを指定します。MIB 変数のサンプル間の変動をテストする場合は、**delta** キーワードを指定します。 • *value*：アラームを発生させる値およびアラームがリセットされる値を指定します。上限および下限しきい値に指定できる範囲は -2147483648 ～ 2147483647 です。 • （任意）*event-number*：上限および下限しきい値が限度を超えた場合に発生させるイベントの番号を指定します。 • （任意）**owner** *string*：アラームの所有者を指定します。
ステップ 3	**rmon event** *number* [**description** *string*] [**log**] [**owner** *string*] [**trap** *community*]	RMON イベント テーブルで RMON イベント番号に関連付けられたイベントを追加します。 • *number*：イベント番号を割り当てます。指定できる範囲は 1 ～ 65535 です。 • （任意）**description** *string*：イベントの説明を指定します。 • （任意）**log**：イベント発生時に RMON ログ エントリを生成します。 • （任意）**owner** *string*：イベントの所有者を指定します。 • （任意）**trap** *community*：このトラップ用の SNMP コミュニティ ストリングを入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

インターフェイス上でのグループ履歴統計情報の収集

収集情報を表示するには、最初に RMON アラームおよびイベントを設定する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	履歴を収集するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**rmon collection history** *index* [**buckets** *bucket-number*] [**interval** *seconds*] [**owner** *ownername*]	指定したバケット数と期間での履歴収集をイネーブルにします。 • *index*：RMON 統計グループを指定します。指定できる範囲は 1 ～ 65535 です。 •（任意）**buckets** *bucket-number*：RMON 統計グループ履歴収集に必要な最大バケット数を指定します。指定できる範囲は 1 ～ 65535 です。デフォルトのバケット数は 50 です。 •（任意）**interval** *seconds*：ポーリング サイクルを秒数で指定します。指定できる範囲は 1 ～ 3600 です。デフォルトは 1,800 秒です。 •（任意）**owner** *ownername*：RMON 統計グループの所有者名を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

インターフェイス上でのイーサネット グループ統計情報の収集

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	統計情報を収集するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**rmon collection stats** *index* [**owner** *ownername*]	インターフェイスの RMON 統計情報収集をイネーブルにします。 • *index*：RMON 統計グループを指定します。指定できる範囲は 1 ～ 65535 です。 •（任意）**owner** *ownername*：RMON 統計グループの所有者名を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

RMON のモニタリングおよびメンテナンス

表 34-1　RMON ステータスを表示するコマンド

コマンド	目的
show rmon	汎用 RMON 統計情報を表示します。
show rmon alarms	RMON アラーム テーブルを表示します。
show rmon events	RMON イベント テーブルを表示します。
show rmon history	RMON 履歴テーブルを表示します。
show rmon statistics	RMON 統計情報テーブルを表示します。

RMON の設定例

RMON アラーム番号の設定：例

次に、RMON アラーム番号の設定例を示します。

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0 owner jjohnson
```

このアラームは、ディセーブルにされない限り、20 秒に 1 度 MIB 変数 *ifEntry.20.1* をモニタリングし、変数の上下の変動をチェックします。*ifEntry.20.1* 値で MIB カウンタが 100000 から 100015 になるなど、15 以上増加すると、アラームが発生します。そのアラームによってさらにイベント番号 1 が発生します。イベント番号 1 は、**rmon event** コマンドで設定されています。使用できるイベントは、ログ エントリまたは SNMP トラップです。*ifEntry.20.1* 値の変化が 0 の場合、アラームはリセットされ、再び発生が可能になります。

RMON イベント番号の作成：例

次に、RMON イベント番号 1 を作成する例を示します。

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones
```

このイベントは *High ifOutErrors* と定義され、アラームによってイベントが発生したときに、ログ エントリが生成されます。ユーザ *jjones* が、このコマンドによってイベント テーブルに作成される行を所有します。次の例の場合も、イベント発生時に SNMP トラップが生成されます。

RMON 統計情報の設定：例

次の例では、所有者 *root* の RMON 統計情報を収集する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# rmon collection stats 2 owner root
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド Cisco IOS システム管理コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
SNMP コンフィギュレーション	第 36 章「SNMP の設定」
アラームおよびイベントの相互作用	RFC 1757

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 35

システム メッセージ ロギングの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

システム メッセージ ロギングの制約事項

- 高レートでコンソールへのメッセージを記録すると、CPU の使用率が高くなり、スイッチの動作に悪影響を与える可能性があります。

システム メッセージ ロギングについて

システム メッセージ ロギング

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をロギング プロセスに送信します。ロギング プロセスはログ メッセージを各宛先（設定に応じて、ログ バッファ、端末回線、UNIX Syslog サーバなど）に配信する処理を制御します。ロギング プロセスは、コンソールにもメッセージを送信します。

（注） Syslog フォーマットは 4.3 Berkeley Standard Distribution（BSD）UNIX と互換性があります。

ロギング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

ロギングされたシステム メッセージにアクセスするには、スイッチのコマンドライン インターフェイス（CLI）を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチ ソフトウェアは Syslog メッセージを内部バッファに保存します。

システム メッセージをリモートでモニタするには、Syslog サーバ上でログを表示するか、または Telnet あるいはコンソール ポート経由でスイッチにアクセスします。

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字とパーセント記号（%）、およびその前に配置されるオプションのシーケンス番号やタイム スタンプ情報（設定されている場合）で構成されています。メッセージは、次のフォーマットで表示されます。

seq no:timestamp: %facility-severity-MNEMONIC:description

パーセント記号の前のメッセージ部分は、**service sequence-numbers**、**service timestamps log datetime**、**service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]、または **service timestamps log uptime** グローバル コンフィギュレーション コマンドの設定によって変わります。

表 35-1　システム ログ メッセージの要素

要素	説明
seq no:	**service sequence-numbers** グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。 詳細については、「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」（P.35-8）を参照してください。
timestamp のフォーマット： *mm/dd hh:mm:ss* または *hh:mm:ss*（短時間） または *d h*（長時間）	メッセージまたはイベントの日時です。**service timestamps log** [**datetime** | **log**] グローバル コンフィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。 詳細については、「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」（P.35-8）を参照してください。
facility	メッセージが参照する機能（SNMP、SYS など）です。サポートされる機能の一覧については、表 35-3（P.35-4）を参照してください。
severity	メッセージの重大度を示す 0 ～ 7 の 1 桁のコードです。重大度の詳細については、表 35-2（P.35-3）を参照してください。
MNEMONIC	メッセージを一意に示すテキスト ストリングです。
description	レポートされているイベントの詳細を示すテキスト ストリングです。

ログ メッセージ

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。重大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージが削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ロギングがイネーブルの場合、送信請求デバイス出力がコンソールに表示または印刷された後に、非送信請求デバイスからの出力が表示または印刷されます。非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力用プロンプトが返された後に、コンソールに表示されます。したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。非送信請求メッセージが表示された後に、コンソールはユーザ プロンプトを再表示します。

メッセージの重大度

（注） *level* を指定すると、このレベルのメッセージ、および数値的により低いレベルのメッセージが宛先に表示されます。

コンソールへのロギングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのロギングをディセーブルにするには、**no logging monitor** グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのロギングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを使用します。

表 35-2 に *level* キーワードを示します。また、対応する UNIX Syslog 定義を、重大度の最も高いものから順に示します。

表 35-2　メッセージ ロギング level キーワード

level キーワード	レベル	説明	syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	即時処理が必要	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
warnings	4	警告状態	LOG_WARNING
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	情報メッセージだけ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアは、これらのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ：**warnings** ～ **emergencies** の重大度で表示されます。このタイプのメッセージは、スイッチの機能に影響があることを示します。この誤動作からの回復手順については、このリリースに対応するシステム メッセージ ガイドを参照してください。
- **debug** コマンドの出力：**debugging** の重大度で表示されます。通常、デバッグ コマンドは Technical Assistance Center（TAC）でのみ使用されます。

- インターフェイスのアップまたはダウン トランジション メッセージおよびシステム再起動メッセージ：**notifications** の重大度で表示されます。このメッセージは単なる情報であり、スイッチの機能には影響がありません。

UNIX Syslog サーバの設定

次に、UNIX サーバの Syslog デーモンを設定し、UNIX システム ロギング機能を定義する手順について説明します。

UNIX Syslog デーモンへのメッセージのロギング

システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。この手順は任意です。

（注） 最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。このようなシステムの場合に、Syslog メッセージのリモート ロギングをイネーブルにするには、Syslog コマンド ラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

root としてログインし、次のステップを実行します。

ステップ 1　/etc/syslog.conf ファイルに次のような行を 1 行追加します。

```
local7.debug /usr/adm/logs/cisco.log
```

local7 キーワードは、使用するロギング機能を指定します。機能の詳細については、表 35-3（P.35-4）を参照してください。**debug** キーワードは、Syslog の重大度を指定します。重大度の詳細については、表 35-2（P.35-3）を参照してください。syslog デーモンは、次のフィールドで指定されたファイルに、このレベルまたはより重大なレベルのメッセージを送信します。このファイルは、syslog デーモンに書き込み権限がある既存ファイルである必要があります。

ステップ 2　UNIX シェル プロンプトに次のコマンドを入力して、ログ ファイルを作成します。

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

ステップ 3　Syslog デーモンに新しい設定を認識させます。

```
$ kill -HUP `cat /etc/syslog.pid`
```

詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

表 35-3 に、ソフトウェアでサポートされている UNIX システム機能を示します。これらの機能の詳細については、ご使用の UNIX オペレーティング システムの操作マニュアルを参照してください。

表 35-3　ロギング facility-type キーワード

facility-type キーワード	説明
auth	許可システム
cron	cron 機能

表 35-3　ロギング facility-type キーワード （続き）

facility-type キーワード	説明
daemon	システム デーモン
kern	カーネル
local0 ～ local7	ローカルに定義されたメッセージ
lpr	ライン プリンタ システム
mail	メール システム
news	USENET ニュース
sys9 ～ sys14	システムで使用
syslog	システム ログ
user	ユーザ プロセス
uucp	UNIX から UNIX へのコピー システム

システム メッセージ ロギングのデフォルト設定

表 35-4　システム メッセージ ロギングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル
コンソールの重大度	debugging（および数値的により低いレベル。 表 35-2（P.35-3）を参照）
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ
タイム スタンプ	ディセーブル
同期ロギング	ディセーブル
ロギング サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
設定変更ロガー	ディセーブル
サーバ機能	Local7（表 35-3（P.35-4）を参照）
サーバの重大度	informational（および数値的により低いレベル。 表 35-2（P.35-3）を参照）

システム メッセージ ロギングの設定方法

メッセージ ロギングのディセーブル化

メッセージ ロギングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ロギングをイネーブルにする必要があります。メッセージ ロギングがイネーブルの場合、ログ メッセージはロギング プロセスに送信されます。ロギング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

ロギング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ロギング プロセスがディセーブルの場合、メッセージは生成後すぐに（通常はコマンド出力に割り込む形で）コンソールに表示されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no logging console**	メッセージ ロギングをディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

メッセージ表示宛先デバイスの設定

メッセージ ロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。特権 EXEC モードから、次のコマンドの 1 つ以上を使用してメッセージを受信する場所を指定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging buffered** [*size*]	スイッチの内部バッファにメッセージを保存します。指定できる範囲は 4096 ～ 2147483647 バイトです。デフォルトのバッファ サイズは 4096 バイトです。 スイッチに障害が発生すると、フラッシュ メモリに保存されていないログは失われます。ステップ 4 を参照してください。 **（注）** バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、**show memory** 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定*しない*でください。
ステップ 3	**logging** *host*	UNIX Syslog サーバ ホストにメッセージを保存します。 *host* : Syslog サーバとして使用するホストの名前または IP アドレスを指定します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。

	コマンド	目的
ステップ 4	**logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]	フラッシュ メモリ内のファイルにログ メッセージを格納します。 • *filename*：ログ メッセージのファイル名を入力します。 • （任意）*max-file-size*：ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。デフォルトは 4096 バイトです。 • （任意）*min-file-size*：ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。デフォルトは 2048 バイトです。 • （任意）*severity-level-number* | *type*：ロギングの重大度またはロギング タイプを指定します。重大度に指定できる範囲は 0 ～ 7 です。ロギング タイプ キーワードの一覧については、表 35-2（P.35-3）を参照してください。デフォルトでは、デバッグ メッセージ、および数値的により低いレベルのメッセージがログ ファイルに送信されます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**terminal monitor**	現在のセッション間、非コンソール端末にメッセージを保存します。 端末パラメータ コンフィギュレーション コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。

ログ メッセージの同期化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number* [*ending-line-number*]	メッセージの同期ロギングに設定する回線を指定します。 • スイッチのコンソール ポートを介して行われる設定には、**console** キーワードを使用します。 • 同期ロギングをイネーブルにする vty 回線を指定するには、**line vty** *line-number* コマンドを使用します。Telnet セッションを介して行われる設定には、vty 接続を使用します。回線番号に指定できる範囲は 0 ～ 15 です。 16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。 **line vty 0 15** また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。 **line vty 2** このコマンドを入力すると、ライン コンフィギュレーション モードになります。

	コマンド	目的
ステップ 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*]	メッセージの同期ロギングをイネーブルにします。 • （任意）**level** *severity-level*：メッセージの重大度を指定します。重大度がこの値以上であるメッセージは、非同期に出力されます。値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。デフォルトは 2 です。 • （任意）**level all**：重大度に関係なく、すべてのメッセージが非同期に出力されます。 • （任意）**limit** *number-of-buffers*：キューイングされる端末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 20 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service timestamps log uptime** または **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	ログのタイムスタンプをイネーブルにします。 最初のコマンドを実行するとログ メッセージのタイム スタンプがイネーブルになり、システムを再起動した後の経過時間が表示されます。 2 番めのコマンドを実行すると、ログ メッセージのタイム スタンプがイネーブルになります。選択したオプションに応じて、ローカル タイム ゾーンを基準とした日付、時間（ミリ秒）、タイム ゾーン名をタイム スタンプとして表示できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージのタイム スタンプが同じになることがあるため、1 つのメッセージを正確に識別できるように、メッセージにシーケンス番号を表示できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service sequence-numbers**	シーケンス番号をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

メッセージ重大度の定義

選択したデバイスに表示されるメッセージを制限するには、メッセージの重大度を指定します（表 35-2 を参照）。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging console** *level*	コンソールに保存するメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 3	**logging monitor** *level*	端末回線に出力するメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的に低レベルのメッセージを受信します。
ステップ 4	**logging trap** *level*	Syslog サーバに保存するメッセージを制限します。 デフォルトでは、Syslog サーバは通知メッセージ、および数値的に低レベルのメッセージを受信します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP ネットワーク管理ステーションに送信されるように Syslog メッセージ トラップがイネーブルに設定されている場合は、スイッチの履歴テーブルに送信および格納されるメッセージの重大度を変更できます。また、履歴テーブルに格納されるメッセージの数を変更することもできます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、Syslog トラップがイネーブルでない場合も、重大度が **warnings** のメッセージ、および数値的により低いメッセージ（表 35-2（P.35-3）を参照）が、履歴テーブルに 1 つ格納されます。

履歴テーブルがいっぱいの場合（**logging history size** グローバル コンフィギュレーション コマンドで指定した最大メッセージ エントリ数が格納されている場合）は、新しいメッセージ エントリを格納できるように、最も古いエントリがテーブルから削除されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging history** *level*	履歴ファイルに保存され、SNMP サーバに送信される syslog メッセージのデフォルト レベルを変更します。 デフォルトでは、**warnings**、**errors**、**critical**、**alerts**、および **emergencies** のメッセージが送信されます。
ステップ 3	**logging history size** *number*	履歴テーブルに保存できる Syslog メッセージの数を指定します。 デフォルトでは 1 つのメッセージが格納されます。指定できる範囲は 0 ～ 500 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

設定変更ロガーのイネーブル化

コマンドライン インターフェイス（CLI）で行った設定変更をトラッキングするために設定ロガーをイネーブルにすることができます。**logging enable** 設定変更ロガー コンフィギュレーション コマンドを入力すると、設定変更用に入力されたセッション、ユーザおよびコマンドがログに記録されます。設定ログのサイズは 1 ～ 1000 エントリの間で設定することができます（デフォルトは 100）。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**archive**	アーカイブ コンフィギュレーション モードを開始します。
ステップ 3	**log config**	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ 4	**logging enable**	設定変更のロギングをイネーブルにします。
ステップ 5	**logging size** *entries*	（任意）設定ログで取得するエントリ数を設定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 100 です。 **（注）** 設定ログがいっぱいになると、新規エントリが入力されるたびに最も古いログ エントリが削除されます。
ステップ 6	**end**	特権 EXEC モードに戻ります。

UNIX システム ロギング機能の設定

システム ログ メッセージを外部デバイスに送信する場合は、メッセージを UNIX Syslog 機能から送信されたメッセージとして特定するようにシステムを設定できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging** *host*	IP アドレスを入力することにより、メッセージを UNIX Syslog サーバ ホストに保存するようにします。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。
ステップ 3	**logging trap** *level*	Syslog サーバに保存するメッセージを制限します。 デフォルトでは、Syslog サーバは通知メッセージおよびそれより下のレベルのメッセージを受信します。*level* キーワードについては、表 35-2（P.35-3）を参照してください。
ステップ 4	**logging facility** *facility-type*	Syslog ファシリティを設定します。*facility-type* キーワードについては、表 35-3（P.35-4）を参照してください。 デフォルトは **local7** です。
ステップ 5	**end**	特権 EXEC モードに戻ります。

システム メッセージ ログのモニタリングおよびメンテナンス

コマンド	目的
show logging	ロギング メッセージを表示します。
show archive log config	設定ログを表示します。

システム メッセージ ログの設定例

システム メッセージ：例

次に、スイッチ システム メッセージの一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

ロギング表示：例

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

次に、シーケンス番号をイネーブルにした場合のロギング表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

ロガーのイネーブル化：例

次に、設定変更ロガーをイネーブルにして、ログのエントリ数を 500 に設定する例を示します。

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

出力ログの設定：例

設定ログの出力例は次のとおりです。

```
Switch# show archive log config all
 idx   sess           user@line      Logged command
   38    11   unknown user@vty3     |no aaa authorization config-commands
   39    12   unknown user@vty3     |no aaa authorization network default group radius
   40    12   unknown user@vty3     |no aaa accounting dot1x default start-stop group
radius
   41    13   unknown user@vty3     |no aaa accounting system default
   42    14           temi@vty4     |interface GigabitEthernet4/0/1
   43    14           temi@vty4     | switchport mode trunk
   44    14           temi@vty4     | exit
   45    16           temi@vty5     |interface FastEthernet5/0/1
   46    16           temi@vty5     | switchport mode trunk
   47    16           temi@vty5     | exit
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド Cisco IOS システム管理コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Syslog サーバの設定手順	「UNIX システム ロギング機能の設定」（P.35-10）

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 36

SNMP の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SNMP の前提条件

SNMP *グループ*は、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP *ユーザ*は、SNMP グループのメンバです。SNMP *ホスト*は、SNMP トラップ動作の受信側です。SNMP *エンジン ID* は、ローカルまたはリモート SNMP エンジンの名前です。

- スイッチが起動し、スイッチのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェントはイネーブルになります。
- SNMP グループを設定するときは、通知ビューを指定しません。**snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザを対応するグループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。通知ビューの設定が必要な状況については、『*Cisco IOS Network Management Command Reference*』を参照してください。
- リモート ユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して認証およびプライバシー ダイジェストが算出されます。先にリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。

SNMP の制約事項

- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモート エージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。

- ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）の認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。（コマンド ラインで入力された）ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 または SHA セキュリティ ダイジェストに変換されます。コマンド ラインのパスワードは、RFC 2274 の規定に従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は SNMPv3 ユーザのセキュリティ ダイジェストが無効となり、**snmp-server user** *username* グローバル コンフィギュレーション コマンドを使用して、SNMP ユーザを再設定する必要がでてきます。エンジン ID を変更した場合は、同様の制限によってコミュニティ ストリングも再設定する必要があります。

SNMP に関する情報

SNMP

簡易ネットワーク管理プロトコル（SNMP）は、マネージャとエージェントの間の通信のメッセージ フォーマットを提供するアプリケーション層プロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および管理情報ベース（MIB）で構成されます。SNMP マネージャは、CiscoWorks などのネットワーク管理システム（NMS）に統合できます。エージェントおよび MIB は、スイッチに常駐します。スイッチに SNMP を設定するには、マネージャとエージェントの関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイス パラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1：RFC1157 に規定された SNMP（完全インターネット標準）。
- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティ ベースの管理およびセキュリティ フレームワークをコミュニティ ストリング ベースの管理フレームワークに置き換えたものです。次の機能があります。
  - SNMPv2：RFC 1902 ～ 1907 に規定された SNMP バージョン 2（ドラフト版インターネット標準）
  - SNMPv2C：RFC 1901 に規定された SNMPv2 のコミュニティ ストリング ベースの管理フレームワーク（試験版インターネット プロトコル）

- SNMPv3：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に規定されている相互運用可能な標準ベース プロトコルです。SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
  - メッセージの完全性：パケットが伝送中に改ざんされないようにします。
  - 認証：有効な送信元からのメッセージであるかどうかを判別します。
  - 暗号化：パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。

（注）　暗号化を選択するには、**priv** キーワードを入力します。このキーワードは、暗号化ソフトウェア イメージがインストールされている場合のみ使用可能です。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2C にはバルク検索メカニズムが組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索メカニズムは、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラー コードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されます。SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを扱うときに使用するセキュリティ メカニズムが決まります。使用可能なセキュリティ モデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

表 36-1 に、セキュリティ モデルとセキュリティ レベルのさまざまな組み合わせについて、その特性を示します。

表 36-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv （LAN Base イメージが必要）	ユーザ名	No	ユーザ名の照合を使用して認証します。

表 36-1　SNMP セキュリティ モデルおよびセキュリティ レベル （続き）

モデル	レベル	認証	暗号化	結果
SNMPv3	authNoPriv （LAN Base イメージが必要）	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	No	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。
SNMPv3	authPriv （LAN Base イメージが必要）	MD5 または SHA	データ暗号規格（DES）または Advanced Encryption Standard（AES）	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。次の暗号化アルゴリズムで、User-based Security Model（USM）を指定できます。 • CBC-DES（DES-56）規格に基づく認証に加えた DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 36-2 に示す動作を実行します。

表 36-2　SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[1]
get-bulk-request[2]	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

1. この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
2. **get-bulk** コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリー トポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするには、NMS のコミュニティ ストリング定義が、スイッチ上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致していなければなりません。

コミュニティ ストリングの属性は、次のいずれかです。

- Read-Only（RO）：許可された管理ステーションに、コミュニティ ストリングを除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- Read-Write（RW）：許可された管理ステーションに、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ ストリングに対するアクセスは許可しません。

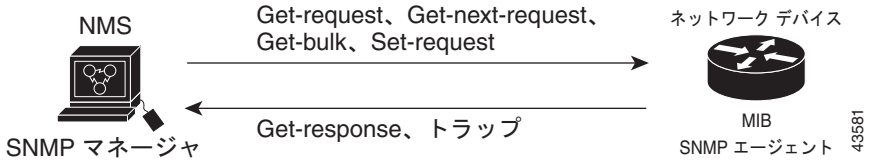
クラスタを作成すると、コマンド スイッチがメンバ スイッチと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンド スイッチ上で最初に設定された RW および RO コミュニティ ストリングにメンバ スイッチ番号（*@esN*、*N* はスイッチ番号）を追加し、これらのストリングをメンバ スイッチに伝播します。詳細は、第 6 章「スイッチ クラスタの設定」および Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。

SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、スイッチの MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスをポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 36-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリに応答します。

図 36-1　SNMP ネットワーク



SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード **traps** はトラップ、情報、またはその両方を表します。**snmp-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

（注）　SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうかが送信側にわからないからです。情報要求の場合、受信した SNMP マネージャは SNMP 応答プロトコル データ ユニット（PDU）でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはスイッチ メモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

NMS の IF-MIB は、物理インターフェイスまたは論理インターフェイスを識別する、ゼロより大きい一意の値である interface index（ifIndex）オブジェクト値の生成および割り当てを行います。スイッチの再起動またはスイッチのソフトウェアのアップグレード時に、スイッチは、インターフェイスにこれと同じ値を使用します。たとえば、スイッチのポート 2 に 10003 という ifIndex 値が割り当てられていると、スイッチの再起動後も同じ値が使用されます。

スイッチは、表 36-3 のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

表 36-3　ifIndex 値

インターフェイス タイプ	ifIndex 範囲
SVI	1 ～ 4999
EtherChannel	5001 ～ 5048
種類とポート番号に基づく物理（ギガビット イーサネットまたは SFP モジュール インターフェイスなど）	10000 ～ 14500
ヌル	10501
ループバックおよびトンネル	24567 +

（注） スイッチは、範囲内の連続した値を使用しない場合があります。

コミュニティ ストリング

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、スイッチ上のエージェントへのアクセスを許可するパスワードと同様に機能します。ストリングに対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

SNMP 通知

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにスイッチが生成するシステム アラートです。デフォルトでは、トラップ マネージャは定義されず、トラップは送信されません。この Cisco IOS Release が稼働しているスイッチでは、トラップ マネージャを無制限に設定できます。

（注） コマンド構文で *traps* というワードを使用するコマンドは多数あります。トラップまたは情報を選択するオプションがコマンドにない限り、キーワード **traps** はトラップ、情報のいずれか、またはその両方を表します。**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

次の表に、サポートされているスイッチのトラップ（通知タイプ）を示します。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr* **informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

表 36-4　スイッチの通知タイプ

通知タイプのキーワード	説明
bridge	STP ブリッジ MIB トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。
entity	SNMP エンティティが変更された場合に、トラップを生成します。
cpu threshold	CPU 関連トラップを許可します。
envmon	環境モニタ トラップを生成します。ファン（fan）、シャットダウン（shutdown）、ステータス（status）、電源（supply）、温度（temperature）の環境トラップのいずれかまたはすべてをイネーブルにできます。
errdisable	VLAN ポートが errdisable になった場合に、トラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 10000 です。デフォルトは 0 で、レート制限がないという意味です。
flash	SNMP FLASH 通知を生成します。
hsrp	ホットスタンバイ ルータ プロトコル（HSRP）が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャスト ルーティングが変更された場合に、トラップを生成します。
mac-notification	MAC アドレス通知のトラップを生成します。
msdp	Multicast Source Discovery Protocol（MSDP）が変更された場合に、トラップを生成します。
ospf	Open Shortest Path First（OSPF）が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステート アドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。
pim	Protocol-Independent Multicast（PIM）が変更された場合に、トラップを生成します。無効な PIM メッセージ、ネイバー変更、およびランデブー ポイント（RP）マッピングの変更に関するトラップを任意にイネーブルにできます。
port-security	SNMP ポート セキュリティ トラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 **（注）** 通知タイプ **port-security** を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate** *rate*
rtr	SNMP Response Time Reporter（RTR）のトラップを生成します。
snmp	認証、コールド スタート、ウォーム スタート、リンク アップ、またはリンク ダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 に設定されています（制限なしの状態では、発生ごとにトラップが送信されます）。
stpx	SNMP STP 拡張 MIB トラップを生成します。

表 36-4　スイッチの通知タイプ （続き）

通知タイプのキーワード	説明
syslog	SNMP の Syslog トラップを生成します。
tty	TCP 接続のトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバーシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN トランキング プロトコル（VTP）が変更された場合に、トラップを生成します。

（注）　**fru-ctrl**、**insertion**、および **removal** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

表 36-4 に示す通知タイプを受信するには、特定のホストに対して **snmp-server host** グローバル コンフィギュレーション コマンドを実行します。

SNMP のデフォルト設定

表 36-5　SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル[1]
SNMP トラップ レシーバ	未設定
SNMP トラップ	TCP 接続のトラップ（**tty**）以外は、イネーブルではありません。
SNMP バージョン	**version** キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで **noauth**（noAuthNoPriv）になります。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

1. これは、スイッチが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP の設定方法

SNMP エージェントのディセーブル化

no snmp-server グローバル コンフィギュレーション コマンドを使用すると、デバイスで稼働中のすべてのバージョン（バージョン 1、
バージョン 2C、バージョン 3）がディセーブルになります。SNMP をイネーブルにする特定の Cisco IOS コマンドは存在しません。最初に入力する **snmp-server** グローバル コンフィギュレーション コマンドによって、SNMP のすべてのバージョンがイネーブルになります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no snmp-server**	SNMP エージェント動作をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

コミュニティ ストリングの設定

（注）　SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します（コミュニティ ストリングに値を入力しないでください）。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*]	コミュニティ ストリングを設定します。 （注）　コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。 • *string*：パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 • （任意）**view**：コミュニティがアクセスできるビュー レコードを指定します。 • （任意）許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用（**ro**）、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き（**rw**）を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 • （任意）*access-list-number*：1 ～ 99 および 1300 ～ 1999 の標準 IP アクセス リスト番号を入力します。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	（任意）ステップ 2 で標準 IP アクセス リスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。 • *access-list-number*：ステップ 2 で指定したアクセスリスト番号を指定します。 • **deny**：条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source*：コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 • （任意）*source-wildcard*：source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}	SNMP のローカル コピーまたはリモート コピーに名前を設定します。 • *engineid-string* は、SNMP のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。たとえば、123400000000000000000000 というエンジン ID を設定する場合、**snmp-server engineID local 1234** のように入力できます。 • **remote** を指定した場合、SNMP のリモート コピーが置かれているデバイスの *ip-address* を指定し、任意でリモート デバイスのユーザ データグラム プロトコル（UDP）ポートを指定します。デフォルト値は 162 です。

	コマンド	目的
ステップ 3	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	リモート デバイス上で新しい SNMP グループを設定します。 • *groupname*：グループの名前を指定します。 • セキュリティ モデルを指定します。 – **v1** は、最も安全性の低いセキュリティ モデルです。 – **v2c** は、2 番めに安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を伝送できます。 – 最も安全な **v3** の場合、認証レベルを選択する必要があります。 **auth**：MD5 および SHA によるパケット認証が可能です。 **noauth**：noAuthNoPriv というセキュリティ レベルをイネーブルにします。キーワードを指定しなかった場合、これがデフォルトです。 **priv**：データ暗号規格（DES）によるパケット暗号化をイネーブルにします（*privacy* とも呼ばれます）。 （注）　**priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合のみ使用可能です。 • （任意）**read** *readview*：エージェントの内容を表示できるビューの名前を表すストリング（64 文字以下）を指定します。 • （任意）**write** *writeview*：データを入力し、エージェントの内容を表示できるビューの名前を表すストリング（64 文字以下）を指定します。 • （任意）**notify** *notifyview*：通知、情報、またはトラップを指定するビューの名前を表すストリング（64 文字以下）を指定します。 • （任意）**access** *access-list*：アクセス リスト名のストリング（64 文字以下）を指定します。

	コマンド	目的
ステップ 4	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]} [*priv* {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]	SNMP グループに対して新規ユーザを追加します。 • *username*：エージェントに接続するホストのユーザ名を指定します。 • *groupname*：ユーザが関連づけられているグループの名前を指定します。 • **remote** *:* ユーザが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルト値は 162 です。 • SNMP バージョン番号（**v1**、**v2c**、または **v3**）を入力します。**v3** を入力する場合は、次のオプションを追加します。 – **encrypted** *:* パスワードが暗号化形式で表示するように指定します。このキーワードは、**v3** キーワードが指定されている場合のみ使用可能です。 – **auth**：認証レベル設定セッションです。HMAC-MD5-96（**md5**）または HMAC-SHA-96（**sha**）のどちらかを指定でき、パスワード ストリング *auth-password*（64 文字以下）が必要です。 • **v3** を入力してスイッチが暗号化ソフトウェア イメージを実行中の場合は、プライベート（**priv**）暗号化およびパスワード ストリング *priv-password*（64 文字以下）の設定もできます。 – **priv**：User-based Security Model（USM）を指定します。 – **des**：56 ビット DES アルゴリズムの使用を指定します。 – **3des :** 168 ビット DES アルゴリズムの使用を指定します。 – **aes**：DES アルゴリズムの使用を指定します。128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化のいずれかを選択する必要があります。 •（任意）**access** *access-list* とともに、アクセス リスト名のストリング（64 文字以下）を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

SNMP 通知の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server engineID remote** *ip-address engineid-string*	リモート ホストのエンジン ID を指定します。

	コマンド	目的
ステップ 3	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]}	SNMP ユーザを設定し、ステップ 2 で作成したリモート ホストに関連付けます。 **（注）** アドレスに対応するリモート ユーザを設定するには、先にリモート ホストのエンジン ID を設定しておく必要があります。このようにしないと、エラー メッセージが表示され、コマンドが実行されません。
ステップ 4	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	SNMP グループを設定します。
ステップ 5	**snmp-server host** *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [*notification-type*]	SNMP トラップ動作の受信先を指定します。 • *host-addr*：ホスト（対象となる受信側）の名前またはインターネット アドレスを指定します。 • （任意）**informs**：ホストに送信される SNMP 情報を指定します。 • （任意）**traps**（デフォルト）：ホストに SNMP トラップを指定します。 • （任意）SNMP **version**（**1**、**2c**、または **3**）を指定します。SNMPv1 は informs をサポートしていません。 • （任意）Version 3：認証レベルとして **auth**、**noauth**、または **priv** を選択します。 **（注）** **priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合のみ使用可能です。 • *community-string*：**version 1** または **version 2c** が指定されている場合、通知動作で送信される、パスワードに類似したコミュニティ ストリングを入力します。**version 3** が指定されている場合、SNMPv3 ユーザ名を入力します。 **（注）** コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。 • （任意）*notification-type*：通知タイプを指定します。表 36-4（P.36-8）にリストされているキーワードを使用します。タイプが指定されていない場合、すべての通知が送信されます。

	コマンド	目的
ステップ 6	**snmp-server enable traps** *notification-types*	スイッチでのトラップまたはインフォームの送信をイネーブルにし、送信する通知の種類を指定します。通知タイプの一覧については、表 36-4（P.36-8）を参照するか、**snmp-server enable traps ?** と入力してください。 複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。 **（注）** 通知タイプ **port-security** を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate** *rate*
ステップ 7	**snmp-server trap-source** *interface-id*	（任意）送信元インターフェイスを指定します。このインターフェイスによってトラップ メッセージの IP アドレスが提供されます。情報の送信元 IP アドレスも、このコマンドで設定します。
ステップ 8	**snmp-server queue-length** *length*	（任意）各トラップ ホストのメッセージ キューの長さを指定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 10 です。
ステップ 9	**snmp-server trap-timeout** *seconds*	（任意）トラップ メッセージを再送信する頻度を指定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 30 秒です。
ステップ 10	**end**	特権 EXEC モードに戻ります。

CPU しきい値通知のタイプと値の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**process cpu threshold type** {**total** | **process** | **interrupt**} **rising** *percentage* **interval** *seconds* [**falling** *fall-percentage* **interval** *seconds*]	CPU しきい値通知のタイプと値を設定します。 • **total**：通知タイプを CPU 使用率の合計に設定します。 • **process**：通知タイプを CPU プロセス使用率に設定します。 • **interrupt**：通知タイプを CPU 割り込み使用率に設定します。 • **rising** *percentage*：CPU リソースのパーセンテージ（1 ～ 100）。設定された間隔を過ぎると CPU しきい値通知を送信します。 • **interval** *seconds*：CPU しきい値超過の秒単位の持続時間（5 ～ 86400）。この条件が満たされると CPU しきい値通知を送信します。 • **falling** *fall-percentage*：CPU リソースのパーセンテージ（1 ～ 100）。設定された間隔の間、使用率がこのレベルより低下すると、CPU しきい値通知を送信します。 この値は、**rising** *percentage* の値以下である必要があります。この値を指定しないと、**falling** *fall-percentage* の値は **rising** *percentage* の値と同じになります。
ステップ 3	**end**	特権 EXEC モードに戻ります。

エージェント コンタクトおよびロケーションの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server contact** *text*	システムの連絡先文字列を設定します。
ステップ 3	**snmp-server location** *text*	システムの場所を表す文字列を設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

SNMP を通して使用する TFTP サーバの制限

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server tftp-server-list** *access-list-number*	SNMP を介したコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リストのサーバに限定します。 *access-list-number* : 1 ～ 99 および 1300 ～ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* : ステップ 2 で指定したアクセスリスト番号を入力します。 • **deny** : 条件に合致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* : スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。 • （任意）*source-wildcard* : source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

SNMP のモニタリングおよびメンテナンス

コマンド	目的
show snmp	SNMP 統計情報を表示します。
show snmp engineID [**local** | **remote**]	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。

コマンド	目的
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 （注）　このコマンドは、**auth** | **noauth** | **priv** モードの SNMPv3 設定情報を表示するときに使用する必要があります。この情報は、**show running-config** の出力には表示されません。

SNMP の設定例

SNMP バージョンのイネーブル化：例

次に、SNMP の全バージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、スイッチはトラップを送信しません。

```
Switch(config)# snmp-server community public
```

SNMP マネージャ アクセスの許可：例

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。スイッチは、ホスト 192.180.1.111 および 192.180.1.33（SNMPv1 を使用）や、ホスト 192.180.1.27（SNMPv2C を使用）へ VTP トラップを送信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

読み取り専用アクセスの許可：例

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

SNMP トラップの設定：例

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されます。先頭行は、すでにイネーブルに設定されているトラップに加えて、エンティティ MIB トラップを送信するようにスイッチをイネーブルにします。2 行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の **snmp-server host** コマンドを無効にします。

```
Switch(config)# snmp-server enable traps entity
```

```
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

リモート ホストとユーザの関連付け：例

次に、ユーザとリモート ホストを関連付けて、ユーザがグローバル コンフィギュレーション モードのときに **auth**（authNoPriv）認証レベルで情報を送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

SNMP へのストリング割り当て：例

次に、ストリング *comaccess* を SNMP に割り当てて読み取り専用アクセスを許可し、IP アクセス リスト 4 がこのコミュニティ ストリングを使用してスイッチの SNMP エージェントにアクセスできるように指定する例を示します。

```
Switch(config)# snmp-server community comaccess ro 4
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS SNMP 構文と使用	『*Cisco IOS Network Management Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 37

ACL によるネットワーク セキュリティの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ACL によるネットワーク セキュリティの制約事項

このスイッチは、Cisco IOS ルータの ACL に関連する次の機能をサポートしていません。

- 非 IP プロトコル ACL（表 37-1（P.37-6）を参照）またはブリッジ グループ ACL
- IP アカウンティング
- 着信および発信レート制限（QoS ACL によるレート制限を除く）
- リフレクシブ ACL またはダイナミック ACL（スイッチ クラスタリング機能で使用される専用のダイナミック ACL を除く）
- ポート ACL および VLAN マップに関する ACL ロギング

ACL によるネットワーク セキュリティに関する情報

ACL

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN でパケットを許可、または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない

場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、VLAN 内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセス リストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。

ACL には、アクセス コントロール エントリ（ACE）の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートしています。

- IP ACL は、TCP、ユーザ データグラム プロトコル（UDP）、インターネット グループ管理プロトコル（IGMP）、およびインターネット制御メッセージ プロトコル（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このスイッチは、Quality of Service（QoS）分類 ACL もサポートしています。詳細については、「QoS ACL に基づく分類」（P.38-13）を参照してください。

ここでは、次の概要について説明します。

- 「サポートされる ACL」（P.37-2）
- 「フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理」（P.37-4）

サポートされる ACL

ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。スイッチでは、発信方向のポート ACL はサポートしません。1 つのレイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。詳細については、「ポート ACL」（P.37-2）を参照してください。

インターフェイスで IEEE 802.1Q トンネリングを設定している場合、トンネル ポートで受信した IEEE 802.1Q カプセル化 IP パケットは、MAC ACL によってフィルタリングされますが、IP ACL ではフィルタリングされません。これは、スイッチが IEEE 802.1Q ヘッダー内部のプロトコルを認識しないためです。この制限は、ルータ ACL およびポート ACL に適用されます。

ポート ACL

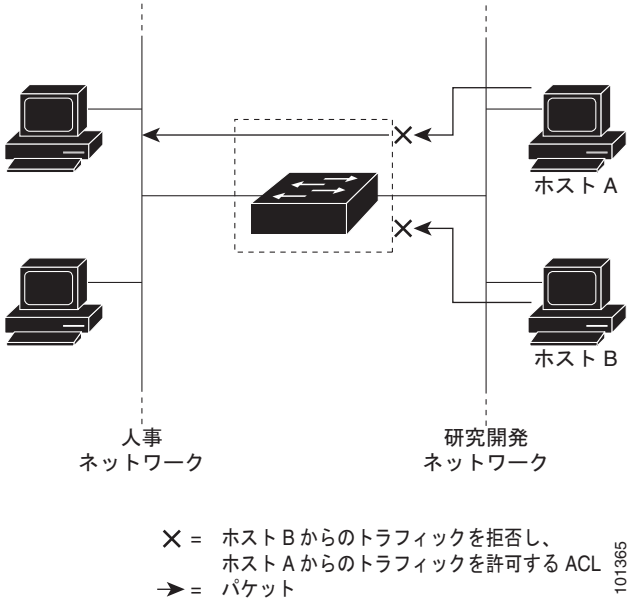
（注）　この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL がサポートされるのは物理インターフェイスだけで、EtherChannel インターフェイスではサポートされず、着信方向のインターフェイスだけに適用されます。次のアクセス リストがサポートされています。

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイスに設定されたすべての着信機能に関連付けられた ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。図 37-1 に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 入力に適用される ACL は、ホスト A に Human Resources ネットワークへのアクセスを許可しますが、ホスト B には同じネットワークへのアクセスを禁止します。ポート ACL は、着信方向のレイヤ 2 インターフェイスだけに適用できます。

図 37-1　ACL によるネットワークへのトラフィックの制御



ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。

（注）　レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに新しい IP アクセス リストまたは MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

ACE には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報（TCP や UDP などのプロトコル タイプを含む）をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

（注）　最初の 2 つの ACE には宛先アドレスの後に *eq* キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれシンプル メール転送プロトコル（SMTP）および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE（permit）と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが 2 つめの ACE（deny）と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。残りのフラグメントは 3 つめの ACE（permit）と一致します。

最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE（deny）と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

IPv4 ACL

このスイッチで IP v4ACL を設定する手順は、他の Cisco スイッチやルータで IP v4ACL を設定する手順と同じです。

ステップ 1　アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。

ステップ 2　その ACL をインターフェイスまたは端末回線に適用します。

標準 IPv4 ACL および拡張 IPv4 ACL

ここでは、IP ACL について説明します。ACL は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL（アクセス リスト）をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

スイッチは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号制標準 IPv4 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.37-18）を参照）、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.37-18）を参照）、または VLAN（「ACL によるネットワーク セキュリティのモニタリングとメンテナンス」（P.37-20）を参照）に適用できます。

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。表 37-1 に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト（1 ～ 199 および 1300 ～ 2699）をサポートします。

表 37-1　　アクセス リスト番号

アクセス リスト番号	タイプ	サポートあり
1 ～ 99	IP 標準アクセス リスト	Yes
100 ～ 199	IP 拡張アクセス リスト	Yes
200 ～ 299	プロトコル タイプコード アクセス リスト	No
300 ～ 399	DECnet アクセス リスト	No
400 ～ 499	XNS 標準アクセス リスト	No
500 ～ 599	XNS 拡張アクセス リスト	No
600 ～ 699	AppleTalk アクセス リスト	No
700 ～ 799	48 ビット MAC アドレス アクセス リスト	No
800 ～ 899	IPX 標準アクセス リスト	No
900 ～ 999	IPX 拡張アクセス リスト	No
1000 ～ 1099	IPX SAP アクセス リスト	No
1100 ～ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	No
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	No
1300 ～ 1999	IP 標準アクセス リスト（拡張範囲）	Yes
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	Yes

（注） 番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

ACL ロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、Syslog メッセージを制御するロギング コンソール コマンドで制御されます。

（注） ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可（*permit*）または拒否（*deny*）ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

番号付き拡張 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

次の IP プロトコルがサポートされます（プロトコル キーワードはカッコ内に太字で示してあります）。

- 認証ヘッダー プロトコル（**ahp**）
- 拡張内部ゲートウェイ ルーティング プロトコル（**eigrp**）
- カプセル化セキュリティ ペイロード（**esp**）
- 総称ルーティング カプセル化（**gre**）
- インターネット制御メッセージ プロトコル（**icmp**）
- インターネット グループ管理プロトコル（**igmp**）
- すべての内部プロトコル（**ip**）
- IP-in-IP トンネリング（**ipinip**）
- KA9Q NOS 互換 IP-over-IP トンネリング（**nos**）
- Open Shortest Path First ルーティング（**ospf**）
- ペイロード圧縮プロトコル（**pcp**）
- プロトコルに依存しないマルチキャスト（**pim**）
- 伝送制御プロトコル（**tcp**）
- ユーザ データグラム プロトコル（**udp**）

（注） ICMP エコー応答はフィルタリングできません。他の ICMP コードまたはタイプは、すべてフィルタリングできます。

（注） このスイッチは、ダイナミックまたはリフレクシブ アクセス リストをサポートしていません。また、タイプ オブ サービス（ToS）の minimize-monetary-cost ビットに基づくフィルタリングもサポートしていません。

サポートされているパラメータのカテゴリは、TCP、UDP、ICMP、IGMP、その他の IP です。

ACL の作成後に（端末からの入力などによって）追加したエントリは、リストの末尾に追加されます。番号付きアクセス リストの特定の場所にはアクセス リスト エントリを追加または削除できません。

（注）　ACL を作成するときには、アクセス リストの末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。

作成した番号制拡張 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.37-18）を参照）、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.37-18）を参照）、または VLAN（「ACL によるネットワーク セキュリティのモニタリングとメンテナンス」（P.37-20）を参照）に適用できます。

ACL 内の ACE の並べ替え

アクセス リスト内のエントリのシーケンス番号は、新しい ACL の作成時に自動的に生成されます。**ip access-list resequence** グローバル コンフィギュレーション コマンドを使用して、ACL のシーケンス番号を編集したり、ACE の適用順序を変更したりできます。たとえば、ACL に新しい ACE を追加すると、その ACE はリストの末尾に配置されます。この場合、シーケンス番号を変更することで、ACE を ACL 内の別の位置に移動できます。

名前付き標準 ACL および拡張 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。

（注）　標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項および制限事項に留意してください。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- 「番号制標準 ACL の作成」（P.37-12）で説明したとおり、番号付き ACL も使用できます。

標準 ACL または拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセス リスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

ACL の時間範囲

time-range グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。次に、ACL を適用してアクセス リストに制限を設定するときに時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内や指定曜日など）を定義できます。

時間範囲を使用する利点の一部を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザ アクセスをより厳密に許可または拒否できます。
- ログ メッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新しい設定を他の機能や TCAM にロードされた結合済みの設定とマージする必要があるためです。そのため、複数のアクセス リストが短期間に連続して（互いに数分以内に）有効となるような設定とならないように注意する必要があります。

（注）　時間範囲は、スイッチのシステム クロックに基づきます。したがって、信頼できるクロック ソースが必要です。ネットワーク タイム プロトコル（NTP）を使用してスイッチ クロックを同期させることを推奨します。詳細については、「システム日時の管理」（P.7-1）を参照してください。

ACL へのコメント

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは deny ステートメントの前後どちらにでも配置できます。コメントがどの permit ステートメントまたは deny ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する permit または deny ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招きます。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

端末回線への IPv4 ACL

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

ACL をインターフェイスに適用する手順については、「インターフェイスへの IPv4 ACL の適用」（P.37-18）を参照してください。VLAN への ACL の適用については、「ACL によるネットワーク セキュリティのモニタリングとメンテナンス」（P.37-20）を参照してください。

インターフェイスへの IPv4 ACL アプリケーション適用の注意事項

- ACL は着信レイヤ 2 ポートだけに適用してください。
- レイヤ 3 インターフェイスには、発信側または着信側のいずれかに ACL を適用してください。
- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- VLAN のメンバであるポートに ACL を適用すると、そのポートの ACL は VLAN インターフェイスに適用された ACL よりも優先されます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL よりも優先します。ポートの ACL は常にレイヤ 2 ポートで受信した着信パケットをフィルタリングします。
- レイヤ 3 インターフェイスに ACL が適用され、ルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。
- プライベート VLAN が設定されている場合、プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。

（注）　パケットがアクセス グループによって拒否された場合、デフォルトでは、ルータは ICMP 到達不能メッセージを送信します。アクセスグループによって拒否されたこれらのパケットはハードウェアでドロップされず、スイッチの CPU にブリッジングされて、ICMP 到達不能メッセージを生成します。ポート ACL は例外です。ポート ACL は ICMP 到達不能メッセージを生成しません。

ICMP 到達不能メッセージは、ルータ ACL で **no ip unreachables** インターフェイス コマンドを使用してディセーブルにできます。

着信 ACL の場合、スイッチはパケットの受信後に ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 ACL の場合、スイッチは、制御されたインターフェイスとの間でパケットを送受信した後に ACL とパケットを照合します。ACL がパケットを許可した場合は、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

IP ACL のハードウェアおよびソフトウェアの処理

ACL の処理は主にハードウェアで実行されますが、トラフィック フローの中には CPU に転送してソフトウェア処理を行う必要があるものもあります。ハードウェアで ACL の設定を保存する領域が不足すると、パケットは転送のために CPU に送られます。ソフトウェア転送トラフィックの転送レートは、ハードウェア転送トラフィックより大幅に低くなります。

（注）　スイッチのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受ける（ソフトウェアで転送される）のは、スイッチに着信した該当 VLAN 内のトラフィックだけです。パケットのソフトウェア転送が発生すると、消費される CPU サイクル数に応じて、スイッチのパフォーマンスが低下することがあります。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードを使用する。
- ICMP 到達不能メッセージを生成する。

トラフィック フローのロギングと転送の両方を行う場合、転送はハードウェアで処理されますが、ロギングはソフトウェアで処理する必要があります。ハードウェアとソフトウェアではパケット処理能力が異なるため、ロギング中であるすべてのフロー（許可フローと拒否フロー）の合計帯域幅が非常に大きい場合は、転送されたパケットの一部をロギングできません。

ルータ ACL の設定をハードウェアに適用できない場合、VLAN に着信したルーティング対象パケットはソフトウェアでルーティングされますが、ブリッジングはハードウェアで行われます。ACL により多数のパケットが CPU に送信されると、スイッチのパフォーマンスが低下する可能性があります。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチド パケットおよびルーテッド パケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、**show access-lists hardware counters** 特権 EXEC コマンドを使用します。

ACL のトラブルシューティング

[chars] がアクセスリスト名となる、次の ACL マネージャのメッセージが表示された場合、スイッチは ACL のハードウェア領域を確保するためのリソースが不足しています。

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

このリソースには、ハードウェア メモリおよびラベル スペースが含まれますが、CPU メモリは含まれません。この問題の原因は、使用可能な論理演算ユニットまたは専用のハードウェア リソースの不足です。論理演算ユニットは、TCP フラグの一致、または TCP、UDP、SCTP ポート番号での **eq** 以外（**ne**、**gt**、**lt**、**range**）のテストで必要です。

次のいずれかの回避策を使用します。

- ACL 設定を変更して使用するリソースを減らします。
- 他の ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します。

専用のハードウェア リソースを識別するには、**show platform layer4 acl map** 特権 EXEC コマンドを入力します。スイッチに使用可能なリソースがない場合は、出力に index 0 ～ index 15 が使用できないことが示されます。

十分なリソースがない ACL の設定の詳細については、Bug Toolkit の CSCsq63926 を参照してください。

名前付き MAC 拡張 ACL

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。

（注）　レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

（注）　**appletalk** は、コマンドラインのヘルプ ストリングに表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。

レイヤ 2 インターフェイスへの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL よりも優先します。レイヤ 2 ポートで受信する着信パケットは、常にポート ACL でフィルタリングされます。
- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

ACL によるネットワーク セキュリティの設定方法

番号制標準 ACL の作成

（注）　ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 *access-list-number*：1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 **deny** または **permit**：条件が一致した場合にアクセスを拒否する場合は deny、許可する場合は permit を指定します。 *source*：パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • *source* および *source-wildcard* の 0.0.0.0 255.255.255.255 の省略形を意味するキーワード **any**。source-wildcard を入力する必要はありません。 • source および source-wildcard の値 *source* 0.0.0.0 の省略形を意味するキーワード **host**。 （任意）*source-wildcard*：ワイルドカード ビットを送信元アドレスに適用します。 （任意）**log**：コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

番号付き拡張 ACL の作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2a	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] （注）　**dscp** 値を入力した場合、**tos** または **precedence** は入力できません。**dscp** を入力しない場合は、**tos** と **precedence** 値の両方を入力できます。	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number*：100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。 **deny** または **permit**：条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。 *protocol*：IP プロトコルの名前または番号を指定します。名前または番号は、**ahp eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、**udp**、および IP プロトコル番号を表す 0 ～ 255 の整数です。一致条件としてインターネット プロトコル（ICMP、TCP、UDP など）を指定するには、キーワード **ip** を使用します。 （注）　この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加のパラメータについては、ステップ 2b ～ 2e を参照してください。 *source*：パラメータの送信元であるネットワークまたはホストの番号を指定します。 *source-wildcard*：ワイルドカード ビットを送信元アドレスに適用します。 *destination*：パラメータの宛先であるネットワークまたはホストの番号を指定します。 *destination-wildcard*：ワイルドカード ビットを宛先アドレスに適用します。 *source*、*source-wildcard*、*destination*、および *destination-wildcard* の値は、次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。 • 単一のホスト 0.0.0.0 を表すキーワード **host**。 その他のキーワードはオプションであり、次の意味を持ちます。 • **precedence**：パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、**routine**（**0**）、***priority***（**1**）、**immediate**（**2**）、**flash**（**3**）、**flash-override**（**4**）、**critical**（**5**）、**internet**（6）、**network**（**7**）です。 • **fragments**：非初期フラグメントを検査します。 • **tos**：パケットを 0 ～ 15 の番号または名前で指定するサービス タイプ レベルと一致させます。指定できる値は、**normal**（**0**）、**max-reliability**（**2**）、**max-throughput**（**4**）、**min-delay**（**8**）です。 • **log**：エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。**log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。 • **time-range**：このキーワードの詳細については、「ACL での時間範囲の使用」（P.37-17）を参照してください。 • **dscp**：0 ～ 63 の番号で指定された DSCP 値を使用してパケットを照合します。疑問符（?）を使用すると、使用可能な値のリストが表示されます。

	コマンド	目的
または	**access-list** *access-list-number* {**deny** | permit} *protocol* any any [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	アクセス リスト コンフィギュレーション モードで、source および source wildcard の値 0.0.0.0 255.255.255.255 の省略形と destination および destination wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のアドレスおよびワイルドカードの代わりに **any** キーワードを使用できます。
または	**access-list** *access-list-number* {**deny** | **permit**} *protocol* **host** *source* **host** *destination* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	source および source wildcard の値 *source* 0.0.0.0 の省略形と destination および destination wildcard の値 *destination* 0.0.0.0 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のワイルドカードまたはマスクの代わりに **host** キーワードを使用できます。
ステップ 2b	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*]	（任意）拡張 TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。 次の例外を除き、ステップ 2a の説明にあるパラメータと同じパラメータを使用します。 （任意）*operator* および *port* では、送信元ポート（*source source-wildcard* の後に入力した場合）または宛先ポート（*destination destination-wildcard* の後に入力した場合）を比較します。使用可能な演算子は、**eq**（等しい）、**gt**（より大きい）、**lt**（より小さい）、**neq**（等しくない）、**range**（包含範囲）などです。演算子にはポート番号を指定する必要があります（**range** の場合は 2 つのポート番号をスペースで区切って指定する必要があります）。 *ポート*番号は、10 進数（0 ～ 65535）または TCP ポート名です。TCP ポート名を確認するには、? を使用するか、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。 他のオプションのキーワードの意味は次のとおりです。 • **established**：確立された接続を照合します。このキーワードは、**ack** または **rst** フラグでの照合と同じ機能を果たします。 • *flag*：指定された TCP ヘッダー ビットを基準にして照合します。使用できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）または **urg**（緊急）です。
ステップ 2c	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 **udp**：User Datagram Protocol（ユーザ データグラム プロトコル）。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[*operator* [*port*]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP では、**flag** および **established** パラメータは無効です。

	コマンド	目的
ステップ 2d	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 ICMP アクセス リストおよびアクセス条件を定義します。 **ICMP**：Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。 ICMP パラメータはステップ 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプでフィルタリングします。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングします。指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングします。ICMP メッセージ タイプ名と ICMP メッセージのタイプおよびコード名を表示する場合は、疑問符（?）を入力するか、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「Configuring IP Services」を参照してください。
ステップ 2e	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。 **IGMP**：Internet Group Management Protocol（インターネット グループ管理プロトコル）。 IGMP パラメータはステップ 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 *igmp-type*：IGMP メッセージ タイプと照合するには、0 ～ 15 の番号またはメッセージ名（**dvmrp**、**host-query**、**host-report**、**pim**、または **trace**）を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

名前付き標準 ACL および名前付き拡張 ACL の作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list standard** *name* または **ip access-list extended** *name*	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、1 ～ 99 の番号を使用できます。 または 名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、100 ～ 199 の番号を使用できます。

	コマンド	目的
ステップ 3	**{deny | permit}** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**] または {**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**] [**time-range** *time-range-name*]	アクセス リスト コンフィギュレーション モードで、パケットを転送するのかドロップするのかを決定する 1 つ以上の拒否条件または許可条件を指定します。 • **host** *source*：source および source wildcard の値 *source* 0.0.0.0 • **any**：source および source wildcard の値 0.0.0.0 255.255.255.255 または アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。**log** キーワードを使用すると、違反を含むアクセス リストのログ メッセージを取得できます。 プロトコルおよび他のキーワードの定義については、「番号付き拡張 ACL の作成」（P.37-13）を参照してください。 • **host** *source*：source および source wildcard の値 *source* 0.0.0.0 • ***host destination***：destination および destination wildcard の値 *destination* 0.0.0.0 • **any**：source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255
ステップ 4	**end**	特権 EXEC モードに戻ります。

ACL での時間範囲の使用

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**time-range** *time-range-name*	作成する時間範囲には意味のある名前（*workhours* など）を割り当て、時間範囲コンフィギュレーション モードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。
ステップ 3	**absolute** [**start** *time date*] [**end** *time date*] または **periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm* または **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*	適用対象の機能がいつ動作可能になるかを指定します。 • 時間範囲には、**absolute** ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。 • 複数の **periodic** ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。 設定例を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

端末回線への IPv4 ACL の適用

この作業では、仮想端末回線と ACL 内のアドレス間の着信および発信接続を制限します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number*	設定する回線を指定し、インライン コンフィギュレーション モードを開始します。 • **console**：コンソール端末回線を指定します。コンソール ポートは DCE です。 • **vty**：リモート コンソール アクセス用の仮想端末を指定します。 *line-number* は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ～ 16 です。
ステップ 3	**access-class** *access-list-number* {**in** | **out**}	（デバイスへの）特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

インターフェイスへの IPv4 ACL の適用

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定するインターフェイスはレイヤ 2 インターフェイス（ポート ACL）です。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**}	指定されたインターフェイスへのアクセスを制御します。 **out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 4	**end**	特権 EXEC モードに戻ります。

名前付き MAC 拡張 ACL の作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name*	名前を使用して MAC 拡張アクセス リストを定義します。

	コマンド	目的
ステップ 3	{**deny** | **permit**} {**any** | **host** *source MAC address* | *source MAC address mask*} {**any** | **host** *destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap** *lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp** | *0-65535*] [**cos** *cos*]	拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての（**any**）送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定のホスト（**host**）送信元 MAC アドレス、およびすべての（**any**）宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、**permit** または **deny** を指定します。 （任意）次のオプションを入力することもできます。 • *type mask*：Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号を指定します。10 進数、16 進数、または 8 進数で表記できます。一致検査の前に、任意で指定できる *don’t care* ビットのマスクが EtherType に適用されます。 • **lsap** *lsap mask*：IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で *don’t care* ビットのマスクを指定できます。 • **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**：IP 以外のプロトコルを指定します。 • **cos** *cos*：プライオリティを設定する 0 ～ 7 の IEEE 802.1Q CoS 番号を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

レイヤ 2 インターフェイスへの MAC ACL の適用

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** ***interface-id***	特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定するインターフェイスは物理レイヤ 2 インターフェイス（ポート ACL）でなければなりません。
ステップ 3	**mac access-group** {*name*} {**in**}	MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL は、着信方向に限りサポートされます。
ステップ 4	**end**	特権 EXEC モードに戻ります。

ACL によるネットワーク セキュリティのモニタリングとメンテナンス

コマンド	目的
show access-lists [*number* | *name*]	最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	最新の IP アクセス リスト全体、または特定の IP アクセス リスト（番号付きまたは名前付き）を表示します。
show ip interface *interface-id*	インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
show running-config [**interface** *interface-id*]	スイッチまたは指定されたインターフェイスのコンフィギュレーション ファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたかなど）を表示します。
show mac access-group [**interface** ***interface-i***d]	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リスト を表示します。
show access-lists [*number* | *name*]	アクセス リストの設定を表示します。
show time-range	時間範囲の設定を確認します。
show mac access-group [**interface** ***interface-i***d]	そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。

ACL によるネットワーク セキュリティの設定例

標準 ACL の作成：例

次に、IP ホスト 171.69.198.102 へのアクセスを拒否し、他のすべてのホストへのアクセスを許可し、結果を表示する標準 ACL の作成例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
    10 deny   171.69.198.102
    20 permit any
```

拡張 ACL の作成：例

次に、ネットワーク 171.69.198.0 のすべてのホストからネットワーク 172.20.52.0 のすべてのホストへの Telnet アクセスを拒否し、他のすべてのアクセスを許可する拡張アクセス リストを作成し、表示する例を示します（**eq** キーワードを宛先アドレスの後に指定すると、Telnet に対応する TCP 宛先ポート番号がチェックされます）。

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq
telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
    10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
    20 permit tcp any any
```

時間範囲の設定：例

次に、*workhours*（営業時間）の時間範囲および会社の休日（2006 年 1 月 1 日）を設定し、設定を確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

名前付き ACL の使用：例

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
```

```
Switch# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

ACL へのコメントの挿入：例

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセス リスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

ポートへの ACL の適用：例

次に、ポートにアクセス リスト 2 を適用して、ポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 2 in
```

インターフェイスへの ACL の適用：例

たとえば、次の ACL をインターフェイスに適用します。

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

なおかつ次のメッセージが表示される場合は次のようにします。

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

フラグ関連の演算子は使用できません。この問題を回避するには、

- **ip access-list resequence** グローバル コンフィギュレーション コマンドを使用することによって、4 つめの ACE を 1 つめの ACE の前に移動させます。

```
permit tcp source source-wildcard destination destination-wildcard
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
```

  または

- 他の ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します（たとえば、ACL *79* を ACL *1* に変更します）。

これで、ACL 内の 1 つめの ACE をインターフェイスに適用できます。スイッチは ACE を Opselect index 内の使用可能なマッピング ビットに割り当てた後、フラグ関連の演算子を割り当てて TCAM 内の同じビットを使用します。

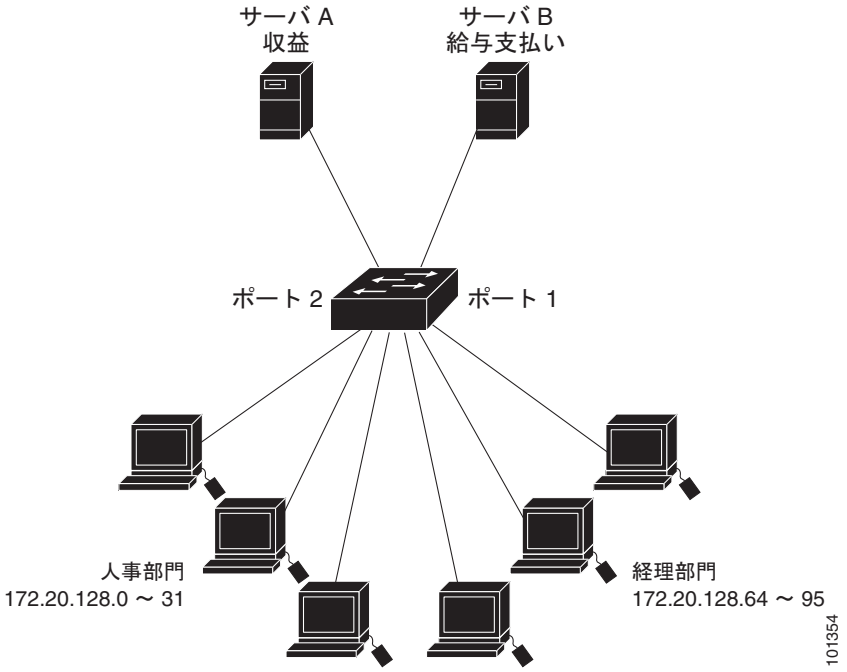
ルーテッド ACL：例

図 37-2 に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。

ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングします。

図 37-2　ルータ ACL によるトラフィックの制御



次に、標準 ACL を使用してポートからサーバ B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 6 out
```

次に、拡張 ACL を使用してサーバ B からポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。この ACL は、ルーテッド ポート 1 に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 106 in
```

番号付き ACL の設定：例

次の例のネットワーク 36.0.0.0 は、2 番めのオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク アドレス 36.0.0.0 の 3 番めおよび 4 番めのオクテットは、特定のホストを指定します。アクセス リスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL の設定：例

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番めの行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。3 番めの行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。発信パケットのポート番号は予約されています。安全なネットワーク システムでは常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できます。ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。**established** キーワードは、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。ギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 102 in
```

名前付き ACL の作成：例

次に、*Internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*Internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

IP ACL への時間範囲の適用：例

次に、月曜日から金曜日の午前 8 時～午後 6 時（18 時）の間に IP の HTTP トラフィックを拒否する例を示します。UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group strict in
```

コメント付き IP ACL エントリの作成：例

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

ACL ロギングの設定：例

log キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group ext1 in
```

レイヤ 2 インターフェイスへの MAC ACL の適用：例

次に、EtherType DECnet Phase IV トラフィックだけを拒否し、他のすべてのタイプのトラフィックを許可するアクセス リスト *mac1* を作成および表示する例を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    10 deny   any any decnet-iv
    20 permit any any
```

次に、アクセス リスト *mac1* をポートに適用してポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mac access-group mac1 in
```

（注）　**mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用された場合に限り有効となります。このコマンドは、EtherChannel ポート チャネルには使用できません。

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS マルチキャスト コマンド	『*Cisco IOS IP Command Reference, Volume 3 of 3:Multicast*』
Cisco IOS IP アドレッシングおよびサービス設定 Cisco IOS ACL 設定	『*Cisco IOS IP Configuration Guide*』 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』 『*Cisco IOS Security Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 38

標準 QoS の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

標準 QoS の前提条件

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン
- トラフィックの特性およびネットワークのニーズ。バースト性の高いトラフィックかどうかの判別。音声およびビデオ ストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

標準 QoS の制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- スイッチで受信された制御トラフィック（スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）やルーティング アップデート パケットなど）には、入力 QoS 処理がすべて行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。
- IPv6 QoS trust 機能はサポートされていません。

標準 QoS に関する情報

この章では、自動 Quality of Service（QoS）コマンドを使用して、またはスイッチで標準の QoS コマンドを使用して QoS を設定する方法について説明します。QoS を使用すると、特定のトラフィックを他のトラフィック タイプよりも優先的に処理できます。QoS を使用しなかった場合、スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。

QoS は物理ポートおよびスイッチ仮想インターフェイス（SVI）に設定できます。ポリシー マップを適用する他に、分類、キューイング、およびスケジューリングなどの QoS を同じ方法で物理ポートおよび SVI に設定します。物理ポートに QoS を設定した場合は、非階層型のポリシー マップをポートに適用します。SVI に QoS を設定すると、非階層型、または階層型のポリシー マップが適用されます。

スイッチは、モジュラ QoS CLI（MQC）コマンドの一部をサポートします。MQC コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Guide, Release 12.2*』の「Modular Quality of Service Command-Line Interface Overview」の章を参照してください。

ネットワークは通常、ベスト エフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、適度なタイミングで配信される可能性はどのトラフィックでも同等です。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。

QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのトラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS は、インターネット技術特別調査委員会（IETF）の新しい規格である Differentiated Services（DiffServ）アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類は IP パケット ヘッダーに格納され、推奨されない IP タイプ オブ サービス（ToS）フィールドの 6 ビットを使用して、分類（クラス）情報として伝達されます。分類情報をレイヤ 2 フレームでも伝達できます。レイヤ 2 フレームまたはレイヤ 3 パケット内のこれらの特殊ビットについて説明します（図 38-1 を参照）。

- レイヤ 2 フレームのプライオリティ ビット

  レイヤ 2 IEEE 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット（ユーザ プライオリティ ビット）で CoS 値が伝達されます。レイヤ 2 IEEE 802.1Q トランクとして設定されたポートでは、ネイティブ VLAN のトラフィックを除くすべてのトラフィックが IEEE 802.1Q フレームに収められます。

  他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

  レイヤ 2 CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

- レイヤ 3 パケットのプライオリティ ビット

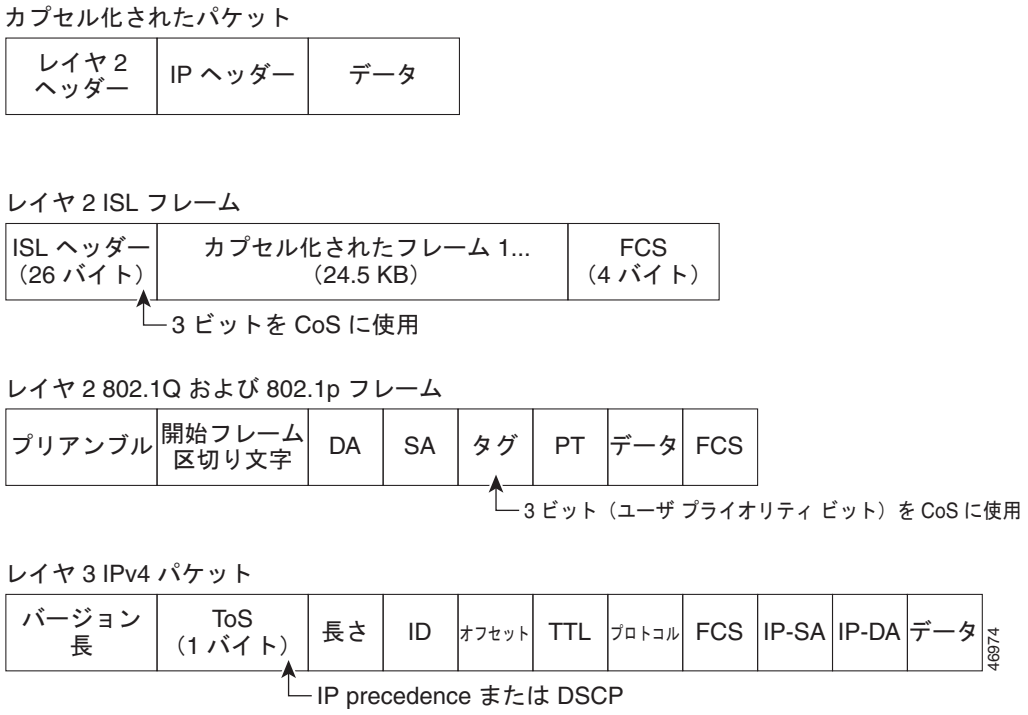
  レイヤ 3 IP パケットは、IP precedence 値または Diffserv コード ポイント（DSCP）値のいずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

  IP precedence 値の範囲は 0 ～ 7 です。

  DSCP 値の範囲は 0 ～ 63 です。

（注）　デュアル IPv4 および IPv6 Switch Database Management（SDM）テンプレートを持つ IPv6 ポートベースの信頼は、このスイッチでサポートされます。IPv6 が動作しているスイッチのデュアル IPv4/IPv6 テンプレートを持つスイッチをリロードする必要があります。詳細については、第 11 章「SDM テンプレートの設定」を参照してください。

図 38-1　　フレームおよびパケットにおける QoS 分類レイヤ



インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンド ホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コア スイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てるリソースの量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワーク上で QoS を実装する作業は、インターネットワーキング デバイスが提供する QoS 機能、ネットワークのトラフィック タイプおよびパターン、さらには着信および発信トラフィックに求める制御のきめ細かさによって、簡単にも複雑にもなります。

QoS の標準モデル

QoS を実装するには、スイッチ上でパケットまたはフローを相互に区別し（分類）、パケットがスイッチを通過するときに所定の QoS を指定するラベルを割り当て、設定されたリソース使用率制限にパケットを適合させ（ポリシングおよびマーキング）、リソース競合が発生する状況に応じて異なる処理（キューイングおよびスケジューリング）を行う必要があります。また、スイッチから送信されたトラフィックが特定のトラフィック プロファイルを満たすようにする必要もあります（シェーピング）。

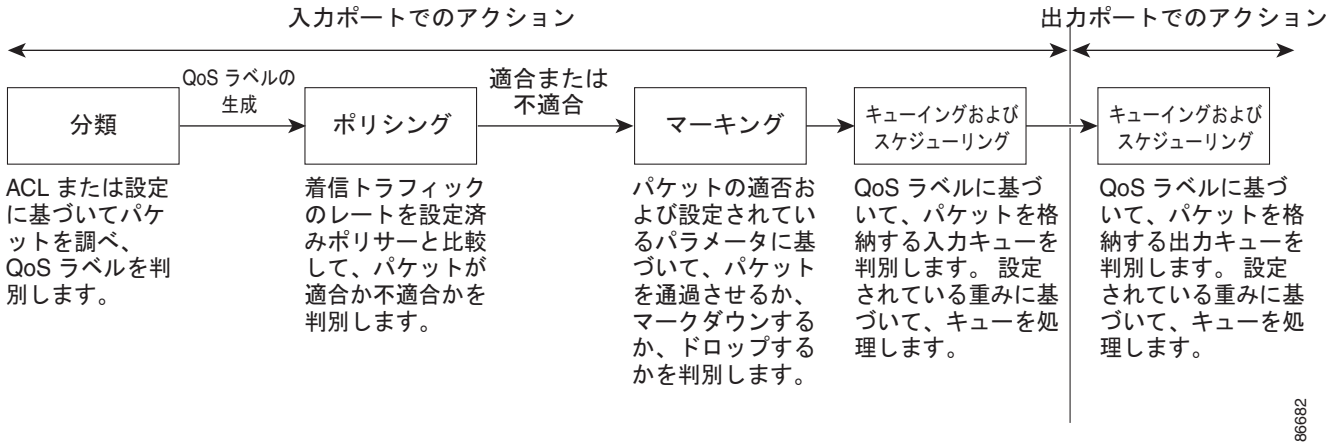
図 38-2 に、QoS の標準モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、キューイング、およびスケジューリングがあります。

- パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。スイッチはパケット内の CoS または DSCP を QoS ラベルにマッピングして、トラフィックの種類を区別します。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。詳細については、「分類」（P.38-10）を参照してください。
- ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。詳細については、「ポリシングおよびマーキング」（P.38-14）を参照してください。
- マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。詳細については、「ポリシングおよびマーキング」（P.38-14）を参照してください。
- キューイングでは、QoS ラベルおよび対応する DSCP または CoS 値を評価して、パケットを 2 つの入力キューのどちらに格納するかを選択します。キューイングは、輻輳回避メカニズムである Weighted Tail-Drop（WTD）アルゴリズムによって拡張されます。しきい値を超過している場合、パケットはドロップされます。詳細については、「キューイングおよびスケジューリングの概要」（P.38-19）を参照してください。
- スケジューリングでは、設定されているシェイプド ラウンド ロビン（SRR）の重みに基づいて、キューを処理します。入力キューの 1 つがプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから他のキューを処理します。詳細については、「SRR のシェーピングおよび共有」（P.38-20）を参照してください。

出力ポートでのアクションには、キューイングおよびスケジューリングがあります。

- 4 つの出力キューのどれを使用するかを選択する前に、キューイングでは、QoS パケット ラベルおよび対応する DSCP または CoS 値を評価します。複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、WTD を使用してトラフィック クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。しきい値を超過している場合、パケットはドロップされます。詳細については、「キューイングおよびスケジューリングの概要」（P.38-19）を参照してください。
- スケジューリングでは、設定されている SRR の共有重みまたはシェーピング重みに基づいて、4 つの出力キューを処理します。キューの 1 つ（キュー 1）は、他のキューの処理前に空になるまで処理される緊急キューにできます。

図 38-2　QoS の標準モデル



標準 QoS 設定時の注意事項

QoS ACL

ここでは、QoS アクセス コントロール リスト（ACL）の設定時の注意事項について説明します。

- IP フラグメントと設定されている IP 拡張 ACL を照合することによって、QoS を実施することはできません。IP フラグメントはベストエフォート型として送信されます。IP フラグメントは IP ヘッダーのフィールドで示されます。
- 1 つのクラス マップごとに使用できる ACL は 1 つだけ、使用できる **match** クラスマップ コンフィギュレーション コマンドは 1 つだけです。ACL には、フィールドとパケットの内容を照合する ACE を複数指定できます。
- ポリシー マップの信頼ステートメントには、ACL 行ごとに複数の TCAM エントリが必要です。入力サービス ポリシー マップに ACL の信頼ステートメントが含まれている場合、利用可能な QoS TCAM に収めるにはアクセス リストが大きすぎる可能性があり、ポリシー マップをポートに適用する際にエラーが発生する場合もあります。可能な限り、QoS ACL の行数を最小限に抑えてください。

インターフェイスでの QoS

ここでは、QoS 物理ポートの設定時の注意事項について説明します。また、この説明は SVI（レイヤ 3 インターフェイス）にも適用されます。

- QoS は物理ポートおよび SVI に設定できます。物理ポートに QoS を設定する場合は、非階層型のポリシー マップを作成し、適用してください。SVI に QoS を設定する場合は、非階層型および階層型のポリシー マップを作成し、適用できます。
- ブリッジング、ルーティング、または CPU への送信のどれを行うかに関係なく、着信トラフィックは分類、ポリシング、およびマークダウン（設定されている場合）されます。ブリッジングされたフレームをドロップしたり、DSCP および CoS 値を変更したりできます。
- 物理ポートまたは SVI でポリシー マップを設定する場合には、次の注意事項に従ってください。
  - 物理ポートと SVI に同じポリシー マップを適用できません。

- 物理ポートで VLAN ベースの QoS を設定した場合、スイッチはそのポートにあるすべてのポートベースのポリシー マップを削除します。そうすることで、物理ポートのトラフィックは、自身のポートの SVI に適用されているポリシー マップの適用を受け入れられます。
- SVI に適用された階層型のポリシー マップでは、物理ポートのインターフェイス レベルで個別にだけポリサーを作成でき、ポートのトラフィックの帯域幅制限を指定できます。入力ポートは、トランクまたはスタティック アクセス ポイントとして設定する必要があります。階層型のポリシー マップの VLAN レベルではポリサーを設定できません。
- スイッチは、階層型のポリシー マップで集約ポリサーをサポートしません。
- SVI に階層型のポリシー マップが適用されたあとは、インターフェイス レベルのポリシー マップを変更したり、削除したりできません。階層ポリシー マップに、新しいインターフェイス レベル ポリシー マップを追加することもできません。このような変更を行いたい場合は、まず階層ポリシー マップを SVI から削除する必要があります。また、階層型ポリシー マップで指定されたクラス マップを追加または削除できません。

ポリシング

- 複数の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個のシステムの内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。たとえば、ギガビット イーサネット ポートに 32 のポリサー、ファスト イーサネット ポートに 8 つのポリサーを設定したり、ギガビット イーサネット ポートに 64 のポリサー、ファスト イーサネット ポートに 5 つのポリサーを設定できます。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを確保することはできません。ポートがいずれかのポリサーに割り当てられる保証はありません。
- 入力ポートでは 1 つのパケットに適用できるポリサーは 1 つだけです。設定できるのは、平均レート パラメータおよび認定バースト パラメータだけです。
- 同じ非階層型のポリシー マップ内にある複数のトラフィック クラスで共有される集約ポリサーを作成できます。ただし、集約ポリサーを異なるポリシー マップにわたって使用できません。
- QoS 対応として設定されているポートを介して受信したすべてのトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。QoS 対応として設定されているトランク ポートの場合、ポートを介して受信した*すべての* VLAN のトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。
- スイッチ上で EtherChannel ポートが設定されている場合、EtherChannel を形成する個々の物理ポートに QoS の分類、ポリシング、マッピング、およびキューイングを設定する必要があります。また、QoS の設定を EtherChannel のすべてのポートで照合するかどうかを決定する必要があります。

標準 QoS のデフォルト設定

QoS はディセーブルです。パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念は存在しません。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

mls qos グローバル コンフィギュレーション コマンドを使用して QoS をイネーブルにし、その他のすべての QoS 設定がデフォルトである場合、トラフィックはポリシングを伴わないベストエフォート型として分類されます（DSCP および CoS 値は 0 に設定されます）。ポリシー マップは設定されません。

すべてのポート上のデフォルト ポートの信頼性は、信頼性なし（untrusted）の状態です。入力および出力キューのデフォルト設定については、「入力キューのデフォルト設定」（P.38-7）および「出力キューのデフォルト設定」（P.38-8）を参照してください。

入力キューのデフォルト設定

表 38-1 に、QoS がイネーブルの場合の入力キューのデフォルト設定を示します。

表 38-1　入力キューのデフォルト設定

機能	キュー 1	キュー 2
バッファ割り当て	90%	10%
帯域幅割り当て [1]	4	4
プライオリティ キューの帯域幅 [2]	0	10
WTD ドロップしきい値 1	100%	100%
WTD ドロップしきい値 2	100%	100%

1. 帯域幅は各キューで平等に共有されます。SRR は共有モードでのみパケットを送信します。
2. キュー 2 はプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

表 38-2 に、QoS がイネーブルの場合のデフォルトの CoS 入力キューしきい値マップを示します。

表 38-2　デフォルトの CoS 入力キューしきい値

CoS 値	キュー ID - しきい値 ID
0 ～ 4	1–1
5	2–1
6、7	1–1

表 38-3 に、QoS がイネーブルの場合のデフォルトの DSCP 入力キューしきい値マップを示します。

表 38-3　デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ～ 39	1–1
40 ～ 47	2–1
48 ～ 63	1–1

出力キューのデフォルト設定

表 38-4 に、QoS がイネーブルの場合、各キューセットの出力キューのデフォルト設定を示します。すべてのポートはキューセット 1 にマッピングされます。ポートの帯域幅限度は 100% に設定され、レートは制限されません。

表 38-4　出力キューのデフォルト設定

機能	キュー 1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
予約済みしきい値	50%	50%	50%	50%
最大しきい値	400%	400%	400%	400%
SRR シェーピング重み（絶対）[1]	25	0	0	0
SRR 共有重み [2]	25	25	25	25

1. シェーピング重みが 0 の場合、このキューはシェーピング モードで動作します。
2. 帯域幅の 4 分の 1 が各キューに割り当てられます。

表 38-5 に、QoS がイネーブルの場合のデフォルトの CoS 出力キューしきい値マップを示します。

表 38-5　デフォルトの CoS 出力キューしきい値マップ

CoS 値	キュー ID - しきい値 ID
0、1	2 - 1
2、3	3 - 1
4	4 - 1
5	1 - 1
6、7	4 - 1

表 38-6 に、QoS がイネーブルの場合のデフォルトの DSCP 出力キューしきい値マップを示します。

表 38-6　デフォルトの DSCP 出力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ～ 15	2 - 1
16 ～ 31	3 - 1
32 ～ 39	4 - 1
40 ～ 47	1 - 1
48 ～ 63	4 - 1

マッピング テーブルのデフォルト設定

（注）　これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 38-7 に、CoS 値を生成するための DSCP/CoS マップを示します。DSCP/CoS マップは 4 つの出力キューのうち 1 つを選択するために使用されます。

表 38-7　デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

表 38-8 に、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値に、着信パケットの IP precedence 値をマップするための、IP precedence/DSCP マップを示します。

表 38-8　デフォルトの IP Precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

表 38-9 に、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値に、着信パケットの CoS 値をマップするための、CoS/DSCP マップを示します。

表 38-9　CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24

表 38-9　CoS/DSCP マップ （続き）

CoS 値	DSCP 値
4	32
5	40
6	48
7	56

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

デフォルトのポリシング済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする（マークダウンしない）空のマップです。

分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。QoS がスイッチ上でグローバルにイネーブルになっている場合のみ、分類はイネーブルです。デフォルトでは、QoS はグローバルにディセーブルになっているため、分類は実行されません。

分類中に、スイッチは検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

QoS ラベルは、パケット内の DSCP または CoS 値に基づいて、パケットに実行されるキューイングおよびスケジューリング アクションを決定します。QoS ラベルは信頼設定およびパケット タイプに従ってマッピングされます（図 38-3（P.38-12）を参照）。

着信トラフィックの分類に、フレームまたはパケットのどのフィールドを使用するかは、ユーザ側で指定します。非 IP トラフィックには、次の分類オプションを使用できます（図 38-3 を参照）。

- 着信フレームの CoS 値を信頼します（ポートが CoS を信頼するように設定します）。次に、設定可能な CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。レイヤ 2 の ISL フレーム ヘッダーは、1 バイトのユーザ フィールドの下位 3 ビットで CoS 値を伝達します。レイヤ 2 IEEE 802.1Q フレームのヘッダーは、タグ制御情報フィールドの上位 3 ビットで CoS 値を伝達します。CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。
- 着信フレームの DSCP または IP precedence 値を信頼します。これらの設定は、非 IP トラフィックの場合は無意味です。これらのいずれかの方法で設定されているポートに非 IP トラフィックが着信した場合は、CoS 値が割り当てられ、CoS/DSCP マップから内部 DSCP 値が生成されます。スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表示する CoS 値を生成します。
- 設定されたレイヤ 2 の MAC アクセス コントロール リスト（ACL）に基づいて分類を実行します。レイヤ 2 の MAC ACL は、MAC 送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

IP トラフィックには、次の分類オプションを使用できます（図 38-3 を参照）。

- 着信パケットの DSCP 値を信頼し（DSCP を信頼するようにポートを設定し）、同じ DSCP 値をパケットに割り当てます。IETF は、1 バイトの ToS フィールドの上位 6 ビットを DSCP として定義しています。特定の DSCP 値が表すプライオリティは、設定可能です。DSCP 値の範囲は 0 ～ 63 です。

  2 つの QoS 管理ドメインの境界上にあるポートの場合は、設定可能な DSCP/DSCP 変換マップを使用して、DSCP を別の値に変更できます。

- 着信パケットの IP precedence 値を信頼し（IP precedence を信頼するようにポートを設定し）、設定可能な IP precedence/DSCP マップを使用してパケットの DSCP 値を生成します。IP バージョン 4 仕様では、1 バイトの ToS フィールドの上位 3 ビットが IP precedence として定義されています。IP precedence 値の範囲は 0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

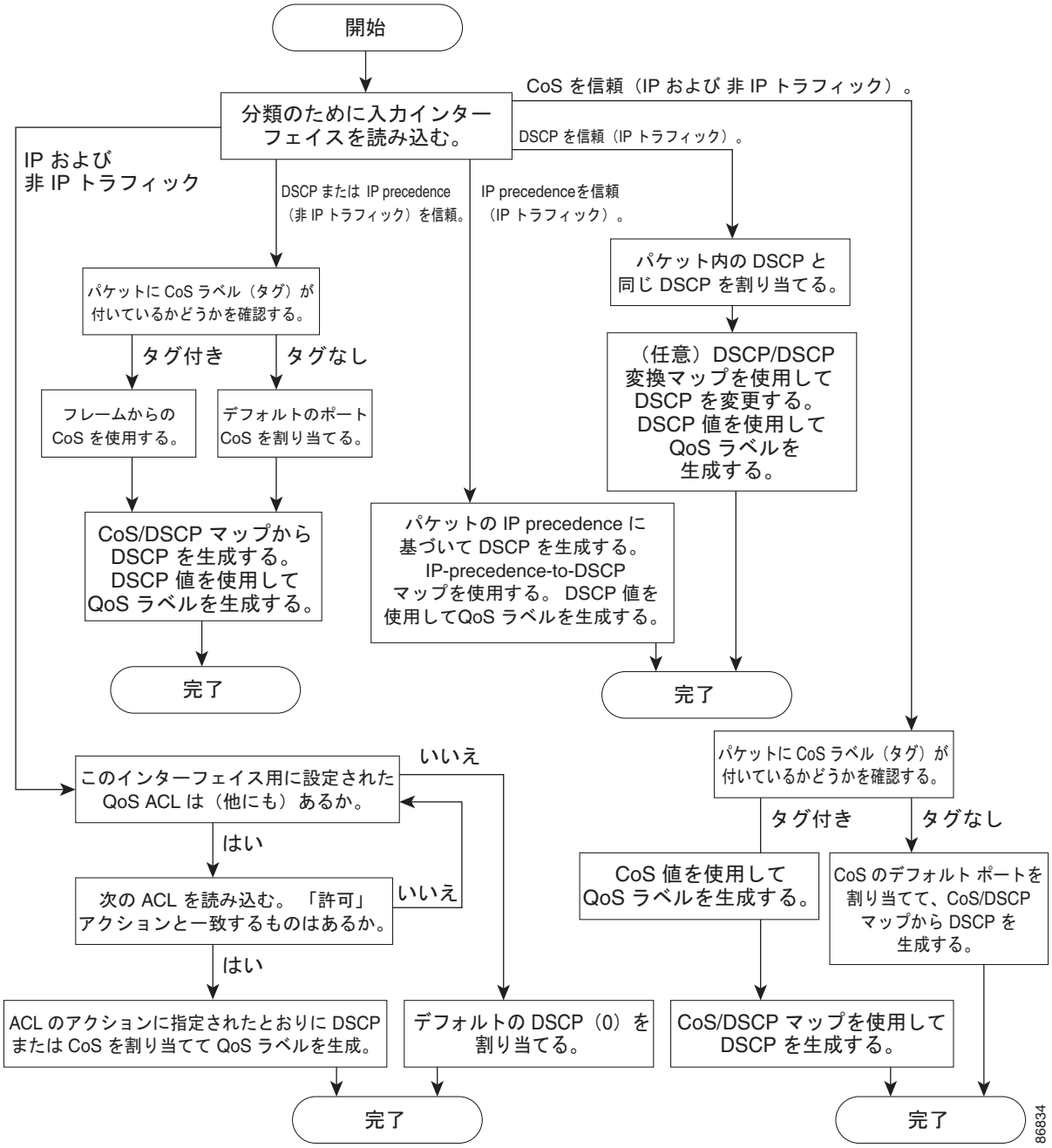
- 着信パケットに CoS 値がある場合には、その CoS 値を信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。

- 設定された IP 標準 ACL または IP 拡張 ACL（IP ヘッダーの各フィールドを調べる）に基づいて、分類を実行します。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

ここで説明されているマップの詳細については、「マッピング テーブル」（P.38-18）を参照してください。ポートの信頼状態の設定情報については、「ポートの信頼状態による分類の設定」（P.38-32）を参照してください。

分類されたパケットは、ポリシング、マーキング、および入力キューイングとスケジューリングの各段階に送られます。

図 38-3　分類フローチャート



QoS ACL に基づく分類

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケット グループ（クラス）を定義できます。QoS のコンテキストでは、アクセス コントロール エントリ（ACE）の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定の QoS 関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、ベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかると、それ以降の検索処理は中止され、QoS 処理が開始されます。

（注）　アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義した後で、そのトラフィック クラスにポリシーを結合できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、特定の集約としてクラスを分類する（DSCP を割り当てるなど）コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。設定については、「QoS ポリシーの設定」（P.38-36）を参照してください。

クラス マップおよびポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセス グループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。複数のトラフィック タイプを分類する場合は、別のクラス マップを作成し、異なる名前を使用できます。パケットをクラス マップ条件と照合した後で、ポリシー マップを使用してさらに分類します。

ポリシー マップでは、作用対象のトラフィック クラスを指定します。トラフィック クラスの CoS、DSCP、または IP precedence 値を信頼するアクションや、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、またはトラフィック帯域幅の制限やトラフィックが不適合な場合の対処法を指定するアクションなどを指定できます。ポリシー マップを効率的に機能させるには、ポートにポリシー マップを結合する必要があります。

クラス マップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。**class-map** コマンドを入力すると、クラス マップ コンフィギュレーション モードが開始されます。このモードで、**match** クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

ポリシー マップは、**policy-map** グローバル コンフィギュレーション コマンドを使用して作成し、名前を付けます。このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始されます。このモードでは、**class**、**trust**、または **set** ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシー マップには、ポリサー、トラフィックの帯域幅限度、および限度を超えた場合のアクションを定義する **police** および **police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを含めることもできます。

ポリシー マップをイネーブルにするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートにマップを結合します。

非階層型のポリシー マップは、物理ポートまたは SVI に対して適用できます。ただし、階層型のポリシー マップに関しては、SVI に対してだけしか適用できません。階層型のポリシー マップには 2 つのレベルがあります。1 番めは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。2 番めはインターフェイス レベルで、SVI の物理ポートのトラフィックに対して実行するアクションを指定します。インターフェイス レベルのアクションはインターフェイス レベルのポリシー マップで指定されます。

詳細については、「ポリシングおよびマーキング」（P.38-14）を参照してください。設定については、「QoS ポリシーの設定」（P.38-36）を参照してください。

ポリシングおよびマーキング

パケットを分類して、DSCP ベースまたは CoS ベースの QoS ラベルを割り当てた後で、ポリシングおよびマーキング プロセスを開始できます（図 38-4 を参照）。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「*アウト オブ プロファイル*」または「*不適合*」になります。各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられた DSCP 値を変更（マークダウン）してパケットの通過を許可するアクションなどがあります。設定可能なポリシング済み DSCP マップを使用すると、パケットに新しい DSCP ベース QoS ラベルが設定されます。ポリシング済み DSCP マップの詳細については、「マッピング テーブル」（P.38-18）を参照してください。マークダウンされたパケットは、元の QoS ラベルと同じキューを使用して、フロー内のパケットの順番が崩れないようにします。

（注）　すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を受けます（ポリサーが設定されている場合）。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときにドロップされたり、DSCP または CoS フィールドが変更されたりすることがあります。

物理ポートまたは SVI に対してポリシングを設定できます。物理ポートでは、信頼状態を設定したり、パケットに対して新規に DSCP または IP precedence 値を設定したり、個別にまたは集約的にポリサーを定義できます。物理ポートのポリシング設定の詳細については、「物理ポートのポリシング」（P.38-15）を参照してください。SVI にポリシー マップを設定する場合、階層型のポリシー マップを作成して、ポリシー マップの 2 番めのインターフェイス レベルにだけ個別にポリサーを定義します。詳細については、「SVI のポリシング」（P.38-16）を参照してください。

ポリシー マップおよびポリシング アクションを設定したあとで、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、入力ポートまたは SVI にポリシーを統合します。

物理ポートのポリシング

物理ポートのポリシー マップでは、次のポリサー タイプを作成できます。

- Individual：QoS はポリサーに指定された帯域幅限度を、一致したトラフィック クラスごとに別々に適用します。このタイプのポリサーは、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップの中で設定します。
- Aggregate：QoS はポリサーで指定された帯域幅限度を、一致したすべてのトラフィック フローに累積的に適用します。このタイプのポリサーは、**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップ内で集約ポリサー名を指定することにより設定します。ポリサーの帯域幅限度を指定するには、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。このようにして、集約ポリサーはポリシー マップ内にある複数のトラフィック クラスで共有されます。

（注）　SVI には個別のポリサーだけを設定します。

ポリシングは、トークン バケット アルゴリズムを使用します。各フレームがスイッチに着信すると、バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指定されたレート（ビット/秒）で送信されます。バケットにトークンが追加されるたびに、スイッチは、バケット内に十分なスペースがあるかを確認します。十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサー アクション（ドロップまたはマークダウン）が実行されます。

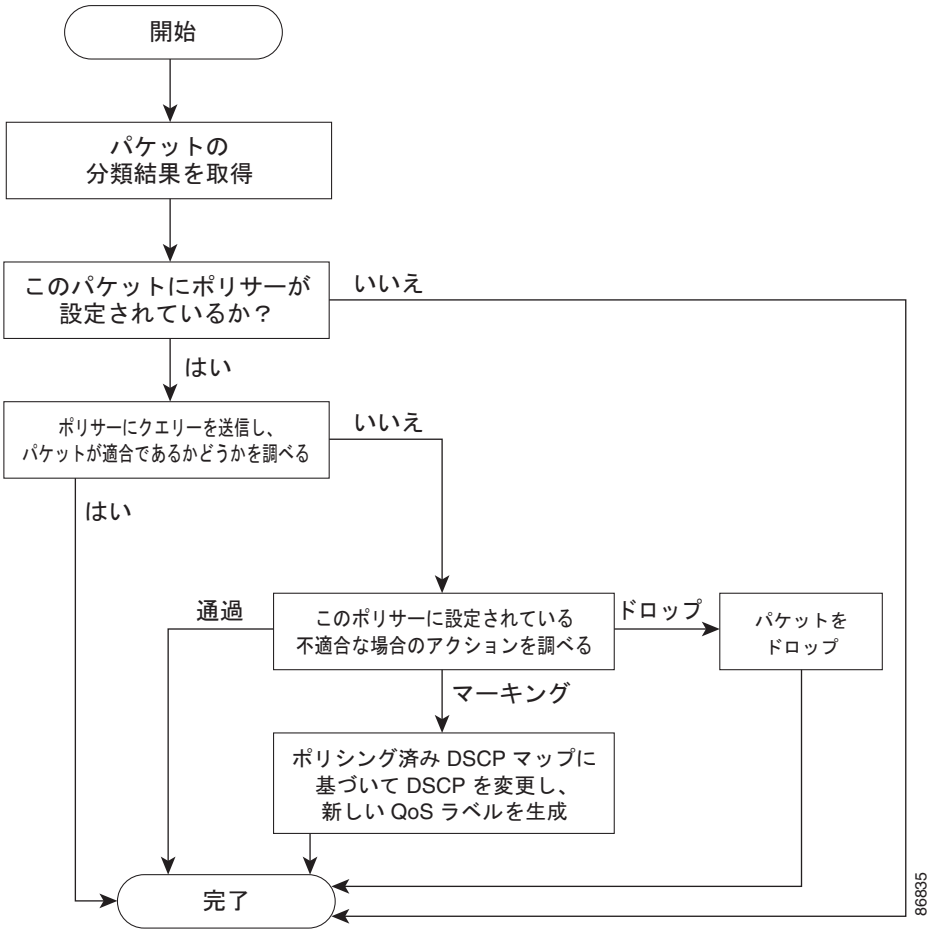
バケットが満たされる速度は、バケット深度（burst-byte）、トークンが削除されるレート（rate-bps）、および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。トークンがバケットから削除される速度（平均速度）を設定するには、*police* ポリシー マップ クラス コンフィギュレーション コマンドの **rate-bps** オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。

図 38-4 に、ポリシングおよびマーキングのプロセスを示します。次のタイプのポリシー マップを設定できます。

- 物理ポートの非階層型ポリシー マップ
- SVI に適用されたインターフェイス レベルの階層型ポリシー マップ。物理ポートは、このセカンダリ ポリシー マップに指定します。

図 38-4　物理ポートのポリシングおよびマーキング フローチャート



SVI のポリシング

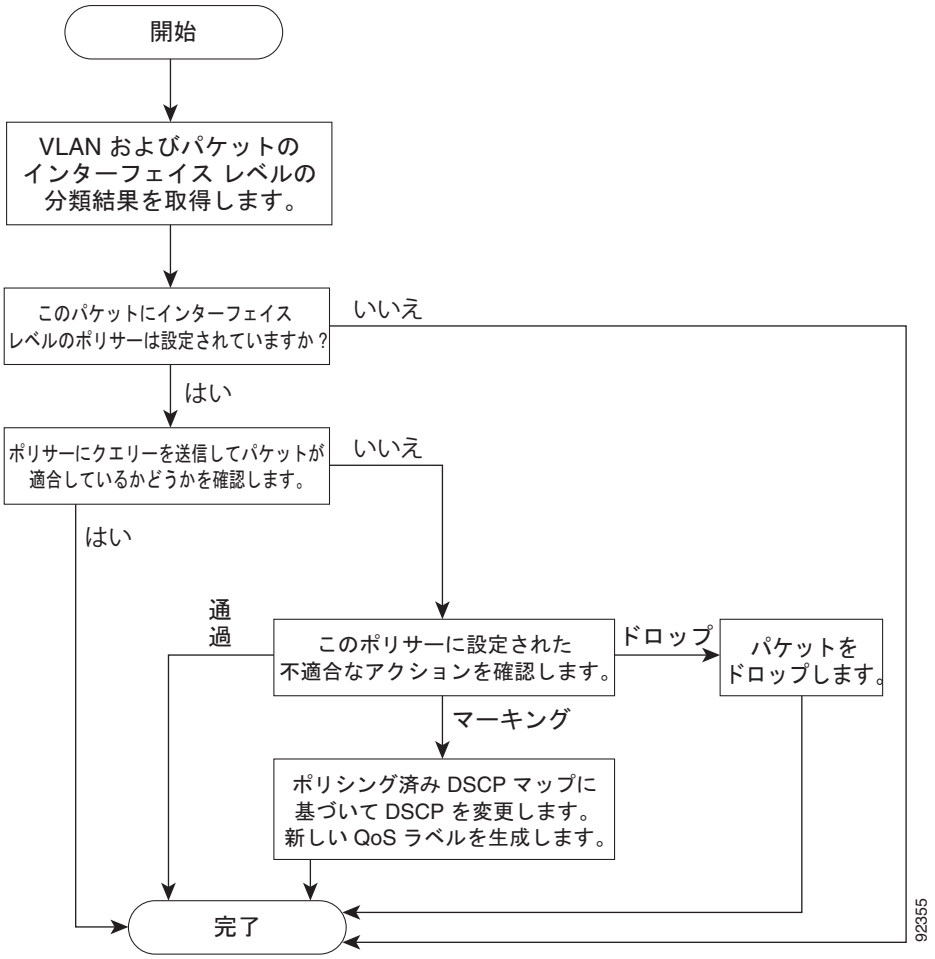
（注）　SVI に個別のポリサーで階層型のポリシー マップを設定する前に、SVI の物理ポートに対して VLAN ベースの QoS をイネーブルにする必要があります。ポリシー マップが SVI に適用されますが、個々のポリサーは、階層型のポリシー マップの 2 番めのインターフェイス レベルで指定した物理ポートのトラフィックに対してだけ影響します。

階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。もう 1 つはインターフェイス レベルで、インターフェイス レベルのポリシー マップに指定されていて、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。

SVI にポリシングを設定する場合、次の 2 つのレベルの階層型ポリシー マップを作成および設定できます。

- VLAN レベル：クラス マップおよびポートの信頼状態を指定するクラスを設定することで、またはパケットに新規に DSCP や IP precedence 値を設定することでプライマリ レベルを作成します。VLAN レベルのポリシー マップは SVI の VLAN に対してだけ適用可能で、ポリサーはサポートしません。
- インターフェイス レベル：クラス マップおよび SVI の物理ポートに個別にポリサーを指定するクラスを設定することで、セカンダリ レベルを作成します。インターフェイス レベルのポリシー マップは個別のポリサーだけサポートし、集約ポリサーをサポートしません。VLAN レベルのポリシー マップで定義された各クラスに対して、異なるインターフェイス レベル ポリシー マップを設定できます。

図 38-5　SVI のポリシングおよびマーキング フローチャート



マッピング テーブル

QoS を処理している間、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティは、分類段階で取得された DSCP または CoS 値に基づいて、QoS ラベルで表されます。

- 分類中に、QoS は設定可能なマッピング テーブルを使用して、受信された CoS、DSCP、または IP precedence 値から対応する DSCP または CoS 値を取得します。これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどがあります。これらのマップを設定するには、**mls qos map cos-dscp** および **mls qos map ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

  DSCP 信頼状態で設定された入力ポートの DSCP 値が QoS ドメイン間で異なる場合は、2 つの QoS ドメイン間の境界にあるポートに、設定可能な DSCP/DSCP 変換マップを適用できます。このマップを設定するには、**mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドを使用します。

- ポリシング中に、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます（パケットが不適合で、マークダウン値がポリサーによって指定されている場合）。この設定可能なマップは、ポリシング済み DSCP マップといいます。このマップを設定するには、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用します。

- トラフィックがスケジューリング段階に達する前に、QoS は QoS ラベルに従って、入力および出力キューにパケットを格納します。QoS ラベルはパケット内の DSCP または CoS 値に基づいており、DSCP 入力/出力キューしきい値マップまたは CoS 入力/出力キューしきい値マップを使用してキューを選択します。入力または出力のキューに加えて、QOS ラベルは WTD しきい値も識別します。これらのマップを設定するには、**mls qos srr-queue** {**input** | **output**} **dscp-map** および **mls qos srr-queue** {**input** | **output**} **cos-map** グローバル コンフィギュレーション コマンドを使用します。

CoS/DSCP、DSCP/CoS、および IP precedence/DSCP マップのデフォルト値は、使用しているネットワークに適する場合と適さない場合があります。

デフォルトの DSCP/DSCP 変換マップおよびデフォルトのポリシング済み DSCP マップは、空のマップです。これらのマップでは、着信した DSCP 値が同じ DSCP 値にマッピングされます。DSCP/DSCP 変換マップは、特定のポートに適用できる唯一のマップです。その他のすべてのマップはスイッチ全体に適用されます。

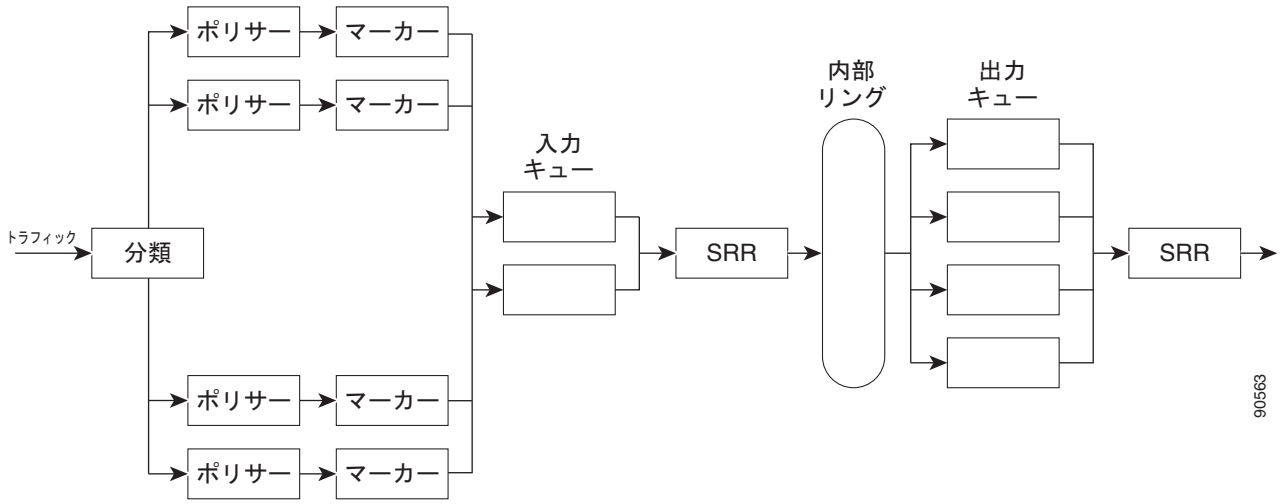
設定については、「DSCP マップの設定」（P.38-48）を参照してください。

DSCP および CoS 入力キューしきい値マップの詳細については、「入力キューでのキューイングおよびスケジューリング」（P.38-21）を参照してください。DSCP および CoS 出力キューしきい値マップの詳細については、「出力キューでのキューイングおよびスケジューリング」（P.38-22）を参照してください。

キューイングおよびスケジューリングの概要

スイッチは特定のポイントにキューを配置し、輻輳防止に役立てます（図 38-6 を参照）。

図 38-6　　入力および出力キューの位置



すべてのポートの入力帯域幅の合計が内部リングの帯域幅を超えることがあるため、入力キューはパケットの分類、ポリシング、およびマーキングの後、パケットがスイッチ ファブリックに転送される前の位置に配置されています。複数の入力ポートから 1 つの出力ポートに同時にパケットが送信されて、輻輳が発生することがあるため、出力キューは内部リングの後に配置されています。

WTD

入力および出力キューは両方とも、WTD と呼ばれるテールドロップ輻輳回避メカニズムの拡張バージョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとにドロップ優先順位を設定したりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると（宛先キューの空きスペースがフレーム サイズより小さくなると）、フレームはドロップされます。

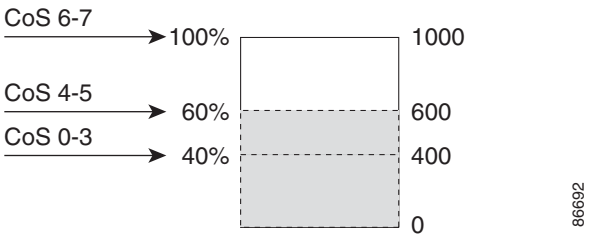
各キューには 3 つのしきい値があります。QOS ラベルは、3 つのしきい値のうちのどれがフレームの影響を受けるかを決定します。3 つのしきい値のうち、2 つは設定可能（明示的）で、1 つは設定不可能（暗示的）です。

図 38-7 に、サイズが 1000 フレームであるキューでの WTD の動作例を示します。ドロップ割合は次のように設定されています。40%（400 フレーム）、60%（600 フレーム）、および 100%（1000 フレーム）です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

この例では、CoS 値 6 および 7 は他の CoS 値よりも重要度が高く、100% ドロップしきい値に割り当てられます（キューフル ステート）。CoS 値 4 および 5 は 60% しきい値に、CoS 値 0 ～ 3 は 40% しきい値に割り当てられます。

600 個のフレームが格納されているキューに、新しいフレームが着信したとします。このフレームの CoS 値は 4 および 5 で、60% のしきい値が適用されます。このフレームがキューに追加されると、しきい値を超過するため、フレームは廃棄されます。

図 38-7　WTD およびキューの動作



詳細については、「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」（P.38-50）、「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」（P.38-54）、および「出力キューおよび ID への DSCP または CoS 値のマッピング」（P.38-55）を参照してください。

SRR のシェーピングおよび共有

入力および出力の両方のキューは SRR で処理され、SRR によってパケットの送信レートが制御されます。入力キューでは、SRR によってパケットが内部リングに送信されます。出力キューでは、SRR によってパケットが出力ポートに送信されます。

出力キューでは、SRR を共有またはシェーピング用に設定できます。ただし、入力キューでは共有がデフォルト モードであり、これ以外のモードはサポートされていません。

シェーピング モードでは、出力キューの帯域幅割合が保証され、この値にレートが制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を超えて使用できません。シェーピングを使用すると、時間あたりのトラフィック フローがより均一になり、バースト トラフィックの最高時と最低時を削減します。シェーピングの場合は、各重みの絶対値を使用して、キューに使用可能な帯域幅が計算されます。

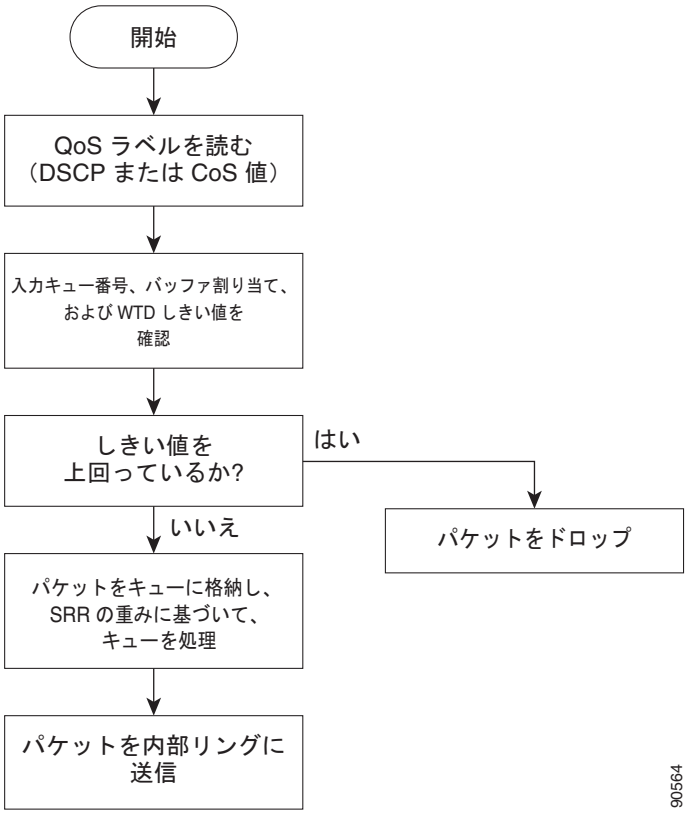
共有モードでは、各キューは設定された重みに従って帯域幅を共有します。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。シェーピングおよび共有は、インターフェイスごとに設定されます。各インターフェイスは、一意に設定できます。

詳細については、「入力キュー間の帯域幅の割り当て」（P.38-52）、「出力キューでの SRR シェーピング重みの設定」（P.38-55）、および「出力キューでの SRR 共有重みの設定」（P.38-56）を参照してください。

入力キューでのキューイングおよびスケジューリング

図 38-8 に、入力ポートのキューイングおよびスケジューリング フローチャートを示します。

図 38-8　　入力ポートのキューイングおよびスケジューリング フローチャート



（注）　共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

スイッチは、共有モードの SRR によってのみ処理される、設定可能な入力キューを 2 つサポートしています。表 38-10 にこれらのキューの説明を示します。

表 38-10　　入力キュー タイプ

キュー タイプ[1]	機能
Normal	標準プライオリティと見なされるユーザ トラフィック。各フローを区別するために、3 つの異なるしきい値を設定できます。**mls qos srr-queue input threshold**、**mls qos srr-queue input dscp-map**、および **mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用できます。
Expedite	Differentiated Services（DF）緊急転送または音声トラフィックなどのハイプライオリティ ユーザ トラフィック。このトラフィックに必要な帯域幅は、**mls qos srr-queue input priority-queue** グローバル コンフィギュレーション コマンドを使用して、合計トラフィックの割合として設定できます。緊急キューには帯域幅が保証されています。

1. スイッチでは、設定不可能なトラフィック用キューが 2 つ使用されます。これらのキューは、ネットワークを適切に動作させるために重要です。

キューおよびしきい値にスイッチを通過する各パケットを割り当てます。特に、入力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。**mls qos srr-queue input dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*}、または **mls** qos srr-queue input cos-map queue *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*} グローバル コンフィギュレーション コマンドを使用します。DSCP 入力キューしきい値マップおよび CoS 入力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

WTD しきい値

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（*明示的*）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（*暗示的*）なしきい値です。入力キューに 2 つの明示的 WTD しきい値の割合（しきい値 ID 1 および ID 2 用）を割り当てるには、**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2* グローバル コンフィギュレーション コマンドを使用します。各しきい値は、キューに割り当てられたバッファの合計値に対する割合です。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。WTD の仕組みの詳細については、「WTD」（P.38-19）を参照してください。

バッファおよび帯域幅の割り当て

2 つのキュー間の入力バッファを分割する比率を定義する（スペース量を割り当てる）には、**mls qos srr-queue input buffers** *percentage1 percentage2* グローバル コンフィギュレーション コマンドを使用します。バッファ割り当てと帯域幅割り当てを組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。帯域幅を割合として割り当てるには、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドを使用します。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

プライオリティ キューイング

特定の入力キューをプライオリティ キューとして設定するには、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューは内部リングの負荷にかかわらず帯域幅の一部が保証されているため、確実な配信を必要とするトラフィック（音声など）に使用する必要があります。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

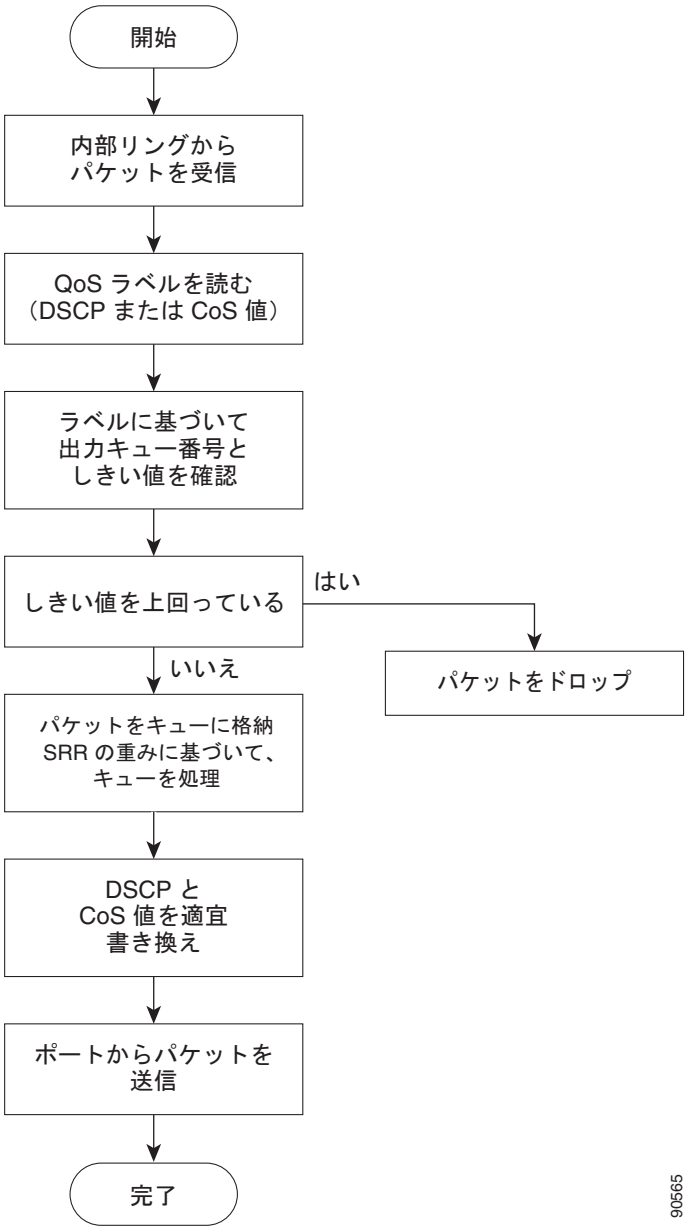
ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定については、「入力キューの特性の設定」（P.38-50）を参照してください。

出力キューでのキューイングおよびスケジューリング

図 38-9 に、出力ポートのキューイングおよびスケジューリング フローチャートを示します。

（注） 緊急キューがイネーブルの場合、SRR によって空になるまで処理されてから、他の 3 つのキューが処理されます。

図 38-9　出力ポートのキューイングおよびスケジューリング フローチャート

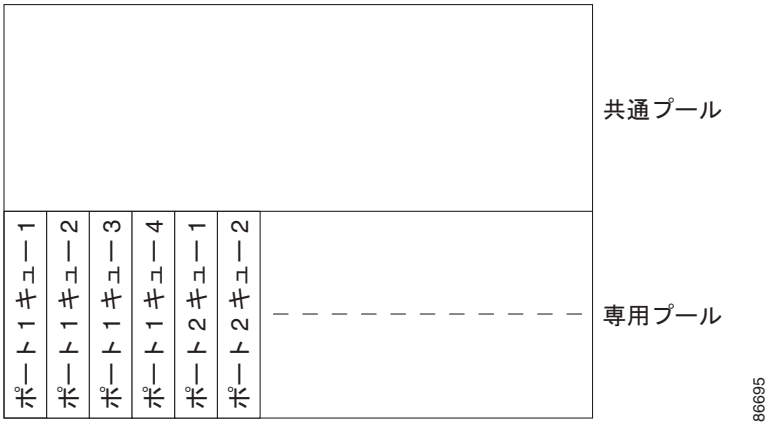


各ポートは、そのうち 1 つ（キュー 1）を出力緊急キューにできる、4 つの出力キューをサポートしています。これらのキューは、キューセットごとに設定されます。出力ポートから脱退するすべてのトラフィックは、パケットに割り当てられた QoS ラベルに基づいて、これらの 4 つのキューのいずれかを通過し、しきい値の影響を受けます。

図 38-10 に出力キュー バッファを示します。バッファ スペースは共通プールと専用プールで構成されます。スイッチはバッファ割り当て方式を使用して、出力キューごとに最小バッファ サイズを確保します。これにより、いずれかのキューまたはポートがすべてのバッファを消費して、その他のキューのバッファが不足することがなくなり、要求元のキューにバッファ スペースを割り当てるかどうかが制御されます。スイッチは、目的のキューが確保された量（限度内）を超えるバッファを消費していないかどうか、最大バッファ（限度超）をすべて消費しているかどうか、および共通プールが空である（空きバッファなし）か、または空でない（空きバッファあり）かを検出します。キューがオーバーリミッ

トでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファ スペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

図 38-10　出力キューのバッファ割り当て



バッファおよびメモリの割り当て

バッファのアベイラビリティの保証、ドロップしきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンドを使用します。各しきい値はキューに割り当てられたメモリの割合です。このパーセント値を指定するには、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* グローバル コンフィギュレーション コマンドを使用します。割り当てられたすべてのバッファの合計が専用プールになります。残りのバッファは共通プールの一部になります。

バッファ割り当てを行うと、ハイプライオリティ トラフィックを確実にバッファに格納できます。たとえば、バッファ スペースが 400 の場合、バッファ スペースの 70% をキュー 1 に割り当てて、10% をキュー 2 ～ 4 に割り当てることができます。キュー 1 には 280 のバッファが割り当てられ、キュー 2 ～ 4 にはそれぞれ 40 バッファが割り当てられます。

割り当てられたバッファをキューセット内の特定のキュー用に確保するよう保証できます。たとえば、キュー用として 100 バッファがある場合、50%（50 バッファ）を確保できます。残りの 50 バッファは共通プールに戻されます。また、最大しきい値を設定することにより、いっぱいになったキューが確保量を超えるバッファを取得できるようにすることもできます。共通プールが空でない場合、必要なバッファを共通プールから割り当てることができます。

WTD しきい値

スイッチを通過する各パケットをキューおよびしきい値に割り当てることができます。特に、出力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。**mls qos srr-queue output dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*}、または **mls** qos srr-queue output cos-map queue *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*} グローバル コンフィギュレーション コマンドを使用します。DSCP 出力キューしきい値マップおよび CoS 出力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（*明示的*）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（*暗示的*）なしきい値です。しきい値 ID 1 および ID 2 用の 2 つの WTD しきい値割合を割り当てます。しきい値 ID 3 のドロップしきい値

は、キューフル ステートに設定済みで、変更できません。キューセットにポートをマッピングするには、**queue-set qset-id** インターフェイス コンフィギュレーション コマンドを使用します。WTD しきい値の割合を変更するには、キューセット設定を変更します。WTD の仕組みの詳細については、「WTD」（P.38-19）を参照してください。

シェーピング モードまたは共有モード

SRR は、シェーピング モードまたは共有モードでキューセットを処理します。ポートに共有重みまたはシェーピング重みを割り当てるには、**srr-queue bandwidth share** *weight1 weight2 weight3 weight4* または **srr-queue bandwidth shape** *weight1 weight2 weight3 weight4* インターフェイス コンフィギュレーション コマンドを使用します。シェーピングと共有の違いについては、「SRR のシェーピングおよび共有」（P.38-20）を参照してください。

バッファ割り当てと SRR 重み比率を組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

緊急キューがイネーブルでない限り、4 つのキューはすべて SRR に参加し、この場合、1 番めの帯域幅重みは無視されて比率計算に使用されません。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。緊急キューをイネーブルにするには、**priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定については、「出力キューの特性の設定」（P.38-53）を参照してください。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

パケットの変更

QoS を設定するには、パケットの分類、ポリシング、キューイングを行います。このプロセス中に、次のようにパケットが変更されることがあります。

- IP パケットおよび非 IP パケットの分類では、受信パケットの DSCP または CoS に基づいて、パケットに QoS ラベルが割り当てられます。ただし、この段階ではパケットは変更されません。割り当てられた DSCP または CoS 値の指定のみがパケットとともに伝達されます。これは、QoS の分類および転送検索が並行して発生するためです。パケットを元の DSCP のまま CPU に転送し、CPU でソフトウェアによる再処理を行うことができます。
- ポリシング中は、IP および非 IP パケットに別の DSCP を割り当てることができます（これらのパケットが不適合で、ポリサーがマークダウン DSCP を指定している場合）。この場合も、パケット内の DSCP は変更されず、マークダウン値の指定がパケットとともに伝達されます。IP パケットの場合は、この後の段階でパケットが変更されます。非 IP パケットの場合は、DSCP が CoS に変換され、キューイングおよびスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベル、および選択された変換マップに応じて、フレームの DSCP および CoS 値が書き換えられます。変換マップが設定されておらず、着信フレームの DSCP を信頼するようにポートが設定されている場合、フレーム内の DSCP 値は変更されないで、

DSCP/CoS マップに従って CoS が書き換えられます。着信フレームの CoS を信頼するようにポートが設定されていて、着信フレームが IP パケットの場合、フレーム内の CoS 値は変更されないで、CoS/DSCP マップに従って DSCP が変更されることがあります。

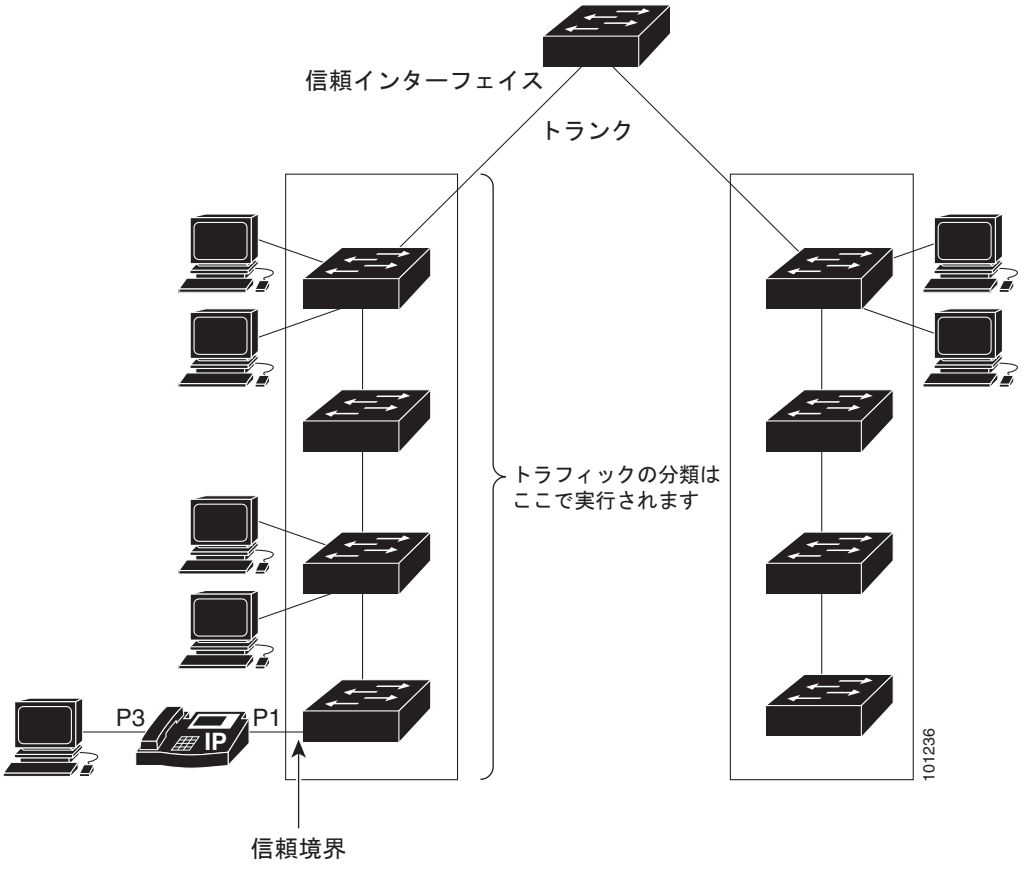
入力変換が行われると、選択された新しい DSCP 値に応じて DSCP が書き換えられます。ポリシー マップの設定アクションによっても、DSCP が書き換えられます。

ポートの信頼状態による分類

QoS ドメイン内のポートの信頼状態

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートをいずれか 1 つの信頼状態に設定できます。図 38-11 に、ネットワーク トポロジの例を示します。

図 38-11　QoS ドメイン内のポートの信頼状態



ポート セキュリティを確保するための信頼境界機能の設定

一般的なネットワークでは、Cisco IP Phone をスイッチ ポートに接続して（図 38-11 を参照）、電話の背後からデータ パケットを生成するデバイスをカスケードします。Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ（CoS = 5）にマーキングし、データ パケットをロー プライオリティ（CoS = 0）にマーキングすることで、共有データ リンクを通して音声品質を保証しています。電話からスイッチに送信されたトラフィックは通常 IEEE 802.1Q ヘッダーを使用するタグでマーキングされています。ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビット フィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からスイッチへ送信されるトラフィックは、音声トラフィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされていることを保証するように信頼されています。**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの CoS ラベルを信頼するように、電話が接続されているスイッチ ポートを設定します。**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの DSCP ラベルを信頼するように、電話が接続されているルーテッド ポートを設定します。

信頼設定により、ユーザが電話をバイパスして PC を直接スイッチに接続する場合に、ハイ プライオリティ キューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、（信頼性のある CoS 設定により）PC が生成した CoS ラベルがスイッチで信頼されてしまいます。それに対して、信頼境界機能は CDP を使用してスイッチ ポートにある Cisco IP Phone（Cisco IP Phone 7910、7935、7940、および 7960）の存在を検出します。電話が検出されない場合、信頼境界機能がハイ プライオリティ キューの誤使用を避けるためにスイッチ ポートの信頼設定をディセーブルにします。信頼境界機能は、PC および Cisco IP Phone がスイッチに接続されているハブに接続されている場合は機能しないことに注意してください。

Cisco IP Phone に接続した PC でハイ プライオリティのデータ キューを利用しないようにすることもできる場合があります。**switchport priority extend cos** インターフェイス コンフィギュレーション コマンドを使用して、PC から受信するトラフィックのプライオリティを上書きするようにスイッチ CLI を介して電話を設定できます。

DSCP トランスペアレントモード

スイッチは透過的な DSCP 機能をサポートします。この機能は発信パケットの DSCP フィールドのみに作用します。デフォルトでは、DSCP 透過性はディセーブルです。スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて Quality of Service（QoS）に基づきます。

no mls qos rewrite ip dscp コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

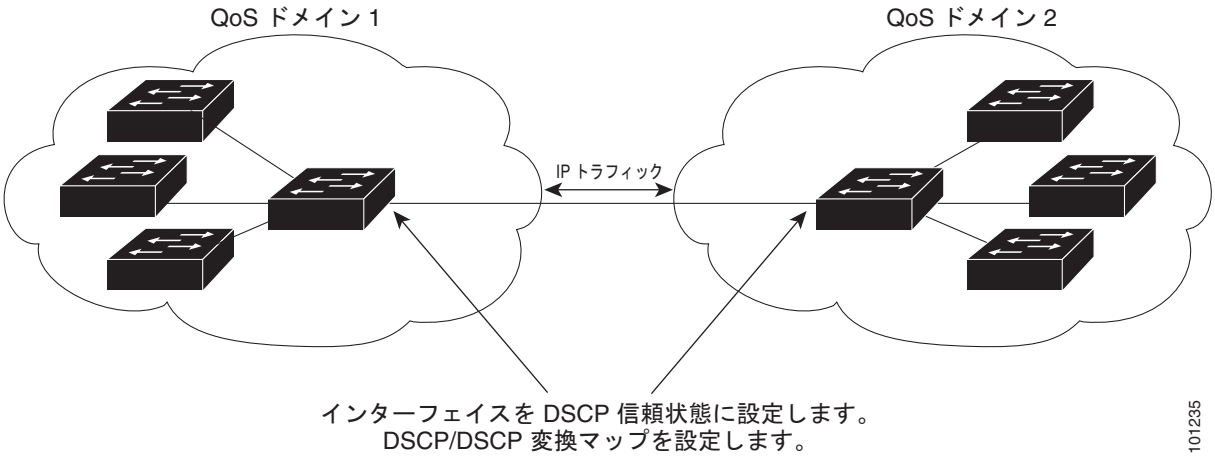
（注）　DSCP 透過性をイネーブルにしても、IEEE 802.1Q トンネリング ポート上のポート信頼性の設定には影響しません。

透過的な DSCP 設定にかかわらず、スイッチはパケット内部の DSCP 値を変更し、トラフィックのプライオリティを提示する CoS 値を生成します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

別の QoS ドメインとの境界ポートの DSCP 信頼状態

2 つの異なる QoS ドメインを管理しているときに、その QoS ドメイン間の IP トラフィックに QoS 機能を実装する場合は、ドメインの境界に位置するスイッチ ポートを DSCP trusted ステートに設定できます（図 38-12 を参照）。それにより、受信ポートでは DSCP trusted 値をそのまま使用し、QoS の分類手順が省略されます。2 つのドメインで異なる DSCP 値が使用されている場合は、他のドメイン内での定義に一致するように一連の DSCP 値を変換する DSCP/DSCP 変換マップを設定できます。

図 38-12　別の QoS ドメインとの境界ポートの DSCP 信頼状態



QoS ポリシー

ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング

実行対象となるトラフィック クラスを指定する非階層型ポリシー マップを、物理ポート上に設定できます。トラフィック クラスの CoS 値、DSCP 値、または IP precedence 値を信頼するアクション、トラフィック クラスに特定の DSCP 値または IP precedence 値を設定するアクション、および一致する各トラフィック クラスにトラフィック帯域幅限度を指定するアクション（ポリサー）や、トラフィックが不適合な場合の対処法を指定するアクション（マーキング）などを指定できます。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- 1 つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。
- ポリシー マップの信頼状態およびポートの信頼状態は互いに排他的であり、最後に設定された方が有効となります。

物理ポートでポリシー マップを設定する場合には、次の注意事項に従ってください。

- 入力ポートごとに付加できるポリシー マップは、1 つだけです。
- **mls qos map ip-prec-dscp** *dscp1...dscp8* グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにのみ影響を与えます。ポリシー マップでは、**set ip precedence** *new-precedence* ポリシー マップ クラス コンフィギュレーション コマンドを使用して

パケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp** *new-dscp* ポリシー マップ クラス コンフィギュレーション コマンドを使用します。

- **set ip dscp** コマンドを入力または使用すると、スイッチは設定内で、このコマンドを **set dscp** に変更します。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、パケット IP Precedence 値を変更できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- ポートに定義したクラスごとに第 2 レベル ポリシー マップを別々に設定できます。第 2 レベルのポリシー マップは、各トラフィック クラスで実行するポリシング作業を指定します。階層型のポリシー マップの設定については、「階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング」（P.38-29）を参照してください。
- ポリシー マップとポート信頼状態は、両方とも物理インターフェイス上で有効にすることができます。ポリシー マップは、ポート信頼状態の前に適用されます。

階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング

階層型ポリシー マップは SVI に設定できますが、他のタイプのインターフェイスには設定できません。階層型のポリシングは、VLAN レベルおよびインターフェイス レベルのポリシー マップで構成された、1 つのポリシー マップとして作成されます。

SVI では、VLAN レベルのポリシー マップに実行対象となるトラフィック クラスを指定します。アクションには、CoS、DSCP、IP precedence 値の信頼、またはトラフィック クラスの特定の DSCP、IP precedence 値の設定が含まれます。個々のポリサーで作用を受ける物理ポートを指定するには、インターフェイス レベルのポリシー マップを使用します。

階層型のポリシー マップを設定するときには、次の注意事項に従ってください。

- 階層型のポリシー マップを設定する前に、インターフェイス レベルのポリシー マップで指定した物理ポートの VLAN ベースの QoS をイネーブルにする必要があります。
- 入力ポートまたは SVI ごとに付加できるポリシー マップは、1 つだけです。
- 1 つのポリシー マップに、それぞれ異なる一致条件とアクションを指定した複数のクラス ステートメントを指定できます。
- SVI で受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。
- ポリシー マップとポート信頼状態は、両方とも物理インターフェイス上で有効にすることができます。ポリシー マップは、ポート信頼状態の前に適用されます。
- **mls qos map ip-prec-dscp** *dscp1...dscp8* グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにのみ影響を与えます。ポリシー マップでは、**set ip precedence** *new-precedence* ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp** *new-dscp* ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力または使用すると、スイッチは設定内で、このコマンドを **set dscp** に変更します。**set ip dscp** コマンドを入力した場合、スイッチ コンフィギュレーションでは **set dscp** の設定として表示されます。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、パケット IP Precedence 値を変更できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。

- VLAN ベースの QoS がイネーブルの場合、階層型のポリシー マップは直前に設定したポートベースのポリシー マップを優先します。
- 階層型のポリシー マップは SVI に適用され、VLAN に属するすべてのトラフィックに影響します。VLAN レベルのポリシー マップで指定されたアクションは、その SVI のトラフィックに影響します。ポート レベルのポリシー マップのポリシング アクションは、影響のある物理インターフェイスの入力トラフィックに影響します。
- トランク ポートの階層型のポリシー マップを設定する場合、VLAN の範囲と重ならないようにしてください。範囲が重なると、ポリシー マップで指定されたアクションは、重なっている VLAN の着信トラフィックおよび発信トラフィックにも作用します。
- 集約ポリサーは階層型のポリシー マップではサポートされません。
- VLAN ベースの QoS がイネーブルになると、スイッチは VLAN マップなどの VLAN ベースの機能をサポートします。
- 階層型のポリシー マップは、プライベート VLAN のプライマリ VLAN 上にだけ設定できます。

DSCP マップ

デフォルトの DSCP マッピングは、「マッピング テーブルのデフォルト設定」（P.38-9）を参照してください。

DSCP/DSCP 変換マップ

2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します（入力変換）。

入力変換により、パケットの DSCP 値が新しい DSCP 値で上書きされ、QoS はこの新しい値を使用してパケットを処理します。スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

入力キューの特性

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- 各キューに（DSCP 値または CoS 値によって）割り当てるパケット
- 各キューに適用されるドロップしきい値、および各しきい値にマッピングされる CoS または DSCP 値
- 各キュー間に割り当てられる空きバッファ スペースの量
- 各キュー間に割り当てられる使用可能な帯域幅の量
- ハイ プライオリティを設定する必要があるトラフィック（音声など）の有無

入力プライオリティ キュー

プライオリティ キューは、優先して進める必要があるトラフィックに限り使用してください（遅延とジッターを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューは、オーバーサブスクライブ リングに激しいネットワーク トラフィックが発生している状況で（バックプレーンが伝達できるトラフィックよりも多くのトラフィックが発生し、キューがいっぱいになって、フレームがドロップされている場合）、遅延およびジッターを軽減するように帯域幅の一部が保証されています。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

出力キューの特性

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- DSCP 値または CoS 値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューセット（ポートごとの 4 つの出力キュー）に適用されるドロップしきい値の割合、およびトラフィック タイプに必要なメモリの確保量および最大メモリ
- キュー セットに割り当てる固定バッファ スペースの量
- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）

出力キューの設定時の注意事項

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルで、SRR シェーピング重みが設定されていない場合、SRR はこのキューを共有モードで処理します。

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定

バッファのアベイラビリティの保証、WTD の設定、およびキューセットの最大割り当ての設定を行うには、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンドを使用します。

各しきい値はキューに割り当てられたバッファの割合です。このパーセント値を指定するには、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* グローバル コンフィギュレーション コマンドを使用します。キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

標準 QoS の設定方法

QoS のグローバルなイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	QoS をグローバルにイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

物理ポートで VLAN ベースの QoS をイネーブル化

デフォルトでは、VLAN ベースの QoS はスイッチにあるすべての物理ポートでディセーブルです。スイッチは、物理ポート ベースでだけ、クラス マップおよびポリシー マップ QoS を含む QoS を適用できます。スイッチ ポートで VLAN ベースの QoS をイネーブルにできます。

この手順には、SVI にインターフェイス レベルの階層型ポリシー マップが指定されている物理ポートが必要です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**mls qos vlan-based**	ポートで VLAN ベースの QoS をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。

ポートの信頼状態による分類の設定

ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネットワーク設定に応じて、次に示す作業または「QoS ポリシーの設定」（P.38-36）に記載されている作業を 1 つまたは複数実行する必要があります。

- 「QoS ドメイン内のポートの信頼状態の設定」（P.38-33）
- 「インターフェイスの CoS 値の設定」（P.38-33）
- 「ポート セキュリティを確保するための信頼境界機能の設定」（P.38-34）
- 「DSCP トランスペアレント モードのイネーブル化」（P.38-35）
- 「別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定」（P.38-35）

QoS ドメイン内のポートの信頼状態の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 3	**mls qos trust** [**cos** | **dscp** | **ip-precedence**]	ポートの信頼状態を設定します。 デフォルトでは、ポートは trusted ではありません。キーワードを指定しない場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：パケットの CoS 値を使用して入力パケットを分類します。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。デフォルトのポート CoS 値は 0 です。 • **dscp**：パケットの DSCP 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 • **ip-precedence**：パケットの IP precedence 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。
ステップ 4	**end**	特権 EXEC モードに戻ります。

インターフェイスの CoS 値の設定

QoS は、trusted ポートおよび untrusted ポートで受信したタグなしフレームに、**mls qos cos** インターフェイス コンフィギュレーション コマンドで指定された CoS 値を割り当てます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。

	コマンド	目的
ステップ 3	**mls qos cos** {*default-cos* | **override**}	ポートのデフォルトの CoS 値を設定します。 • *default-cos*：ポートに割り当てるデフォルトの CoS 値を指定します。パケットがタグなしの場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ～ 7 です。デフォルトは 0 です。 • **override**：着信パケットにすでに設定されている信頼状態を変更し、すべての着信パケットにデフォルトのポート CoS 値を適用します。デフォルトでは、CoS の上書きはディセーブルに設定されています。 特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合には、**override** キーワードを使用します。ポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されている場合でも、設定済みの信頼状態がこのコマンドによって上書き変更され、すべての着信 CoS 値にこのコマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、入力ポートで、ポートのデフォルト CoS を使用してパケットの CoS 値が変更されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。

ポート セキュリティを確保するための信頼境界機能の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp run**	CDP をグローバルにイネーブルにします。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 3	**interface** *interface-id*	Cisco IP Phone に接続するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**cdp enable**	ポート上で CDP をイネーブルにします。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 5	**mls qos trust cos** または **mls qos trust dscp**	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するようにスイッチ ポートを設定します。 または Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するようにルーテッド ポートを設定します。 デフォルトでは、ポートは trusted ではありません。
ステップ 6	**mls qos trust device cisco-phone**	Cisco IP Phone が信頼できるデバイスであることを指定します。 信頼境界機能と自動 QoS（**auto qos voip** インターフェイス コンフィギュレーション コマンド）を同時にイネーブルにはできません。両者は相互に排他的です。
ステップ 7	**end**	特権 EXEC モードに戻ります。

DSCP トランスペアレント モードのイネーブル化

透過的な DSCP 機能をディセーブルにして、信頼設定または ACL に基づいてスイッチに DSCP 値を変更させる設定にするには、**mls qos rewrite ip dscp** グローバル コンフィギュレーション コマンドを使用します。

no mls qos グローバル コンフィギュレーション コマンドで、QoS をディセーブルにした場合、CoS および DSCP 値は変更されません（デフォルトの QoS 設定）。

no mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを入力して DSCP 透過をイネーブルにしてから、**mls qos trust** [**cos** | **dscp**] インターフェイス コンフィギュレーション コマンドを入力した場合、DSCP 透過はイネーブルのままとなります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	QoS をグローバルにイネーブルにします。
ステップ 3	**no mls qos rewrite ip dscp**	DSCP 透過性をイネーブルにします。スイッチが IP パケットの DSCP フィールドを変更しないよう設定されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定

両方の QoS ドメインに一貫した方法でマッピングするには、両方のドメイン内のポート上で次の手順を実行する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを変更します。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。 • *dscp-mutation-name*：変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp*：最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *out-dscp*：1 つの DSCP 値を入力します。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id*	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**mls qos trust dscp**	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。

	コマンド	目的
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された DSCP trusted 入力ポートにマップを適用します。 • *dscp-mutation-name*：ステップ 2. で作成した変換マップ名を指定します。 • 1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。

QoS ポリシーの設定

QoS ポリシーを設定するには、通常、トラフィックをクラス別に分類し、各トラフィック クラスに適用するポリシーを設定し、ポリシーをポートに結合する必要があります。

ここでは、トラフィックを分類、ポリシング、マーキングする方法について説明します。ネットワーク設定に応じて、次の作業を 1 つまたは複数実行する必要があります。

- 「IP 標準 ACL の作成」（P.38-37）
- 「IP 拡張 ACL の作成」（P.38-38）
- 「非 IP トラフィック用のレイヤ 2 MAC ACL の作成」（P.38-38）
- 「クラス マップの作成」（P.38-39）
- 「非階層型ポリシー マップの作成」（P.38-41）
- 「階層型ポリシー マップの作成」（P.38-43）
- 「集約ポリサーの作成」（P.38-47）

IP 標準 ACL の作成

IP 標準 ACL または IP 拡張 ACL を使用することによって、IP トラフィックを分類できます。非 IP トラフィックは、レイヤ 2 MAC ACL を使用することによって分類できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* : アクセスリスト番号を入力します。有効範囲は 1 ～ 99 および 1300 ～ 1999 です。 • **permit** : 条件が一致した場合に特定のトラフィック タイプを許可します。**deny** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • *source* : パケットの送信元となるネットワークまたはホストを指定します。**any** キーワードは 0.0.0.0 255.255.255.255 の省略形として使用できます。 • （任意）*source-wildcard* : source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。

IP 拡張 ACL の作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number*：アクセスリスト番号を入力します。有効範囲は 100 ～ 199 および 2000 ～ 2699 です。 • **permit**：条件が一致した場合に特定のトラフィック タイプを許可します。**deny** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • *protocol*：IP プロトコルの名前または番号を入力します。疑問符（?）を使用すると、使用できるプロトコル キーワードのリストが表示されます。 • *source*：パケットの送信元となるネットワークまたはホストを指定します。ネットワークまたはホストを指定するには、ドット付き 10 進表記を使用したり、**source** 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として *any* キーワードを使用したり、**source** 0.0.0.0 を表す *host* キーワードを使用します。 • *source-wildcard*：無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。ワイルドカードを指定するには、ドット付き 10 進表記を使用したり、**source** 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として *any* キーワードを使用したり、**source** 0.0.0.0 を表す *host* キーワードを使用します。 • *destination*：パケットの送信元となるネットワークまたはホストを指定します。*destination および destination-wildcard* には、*source* および *source-wildcard* での説明と同じオプションを使用できます。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。

非 IP トラフィック用のレイヤ 2 MAC ACL の作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name*	リストの名前を指定することによって、レイヤ 2 MAC ACL を作成します。 このコマンドを入力すると、拡張 MAC ACL コンフィギュレーション モードに切り替わります。

	コマンド	目的
ステップ 3	{**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	条件が一致した場合に許可または拒否するトラフィック タイプを指定します。必要な回数だけコマンドを入力します。 • *src-MAC-addr* : パケットの送信元となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記（H.H.H）を使用したり、**source** 0.0.0、*source-wildcard* ffff.ffff.ffff の短縮形として *any* キーワードを使用したり、**source** 0.0.0 を表す *host* キーワードを使用します。 • *mask* : 無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。 • *dst-MAC-addr* : パケットの送信元となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記（H.H.H）を使用したり、**source** 0.0.0、*source-wildcard* ffff.ffff.ffff の短縮形として *any* キーワードを使用したり、**source** 0.0.0 を表す *host* キーワードを使用します。 • （任意）*type mask* : Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロトコルを識別します。*type* の範囲は 0 ～ 65535 です。通常は 16 進数で指定します。*mask* には、一致をテストする前に Ethertype に適用される*無視（don’t care）*ビットを入力します。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

クラス マップの作成

個々のトラフィック フロー（またはクラス）を他のすべてのトラフィックから分離して名前を付けるには、**class-map** グローバル コンフィギュレーション コマンドを使用します。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。match ステートメントには、ACL、IP precedence 値、DSCP 値などの条件を指定できます。一致条件は、クラス マップ コンフィギュレーション モードの中で match ステートメントを 1 つ入力することによって定義します。

（注） **class** ポリシー マップ コンフィギュレーション コマンドを使用することによって、ポリシー マップの作成時にクラス マップを作成することもできます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] または **access-list** *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] または **mac access-list extended** *name* {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	IP トラフィック用の IP 標準または IP 拡張 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「IP 標準 ACL の作成」（P.38-37）を参照してください。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）**match-all**：このクラス マップ内のすべての一致ステートメント論理積をとります。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）**match-any**：このクラス マップ内のすべての一致ステートメントの論理和をとります。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • *class-map-name*：クラス マップの名前を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとにサポートされる **match** コマンドは 1 つだけなので、**match-all** でも **match-any** でもキーワードの機能は変わりません。
ステップ 4	**match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。 • **access-group** *acl-index-or-name*：ステップ 2 で作成した ACL の番号または名前を指定します。 • **ip dscp** *dscp-list*：着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list*：着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。

非階層型ポリシー マップの作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）**match-all**：このクラス マップ内のすべての一致ステートメント論理積をとります。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）**match-any**：このクラス マップ内のすべての一致ステートメントの論理和をとります。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • *class-map-name*：クラス マップの名前を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとにサポートされる **match** コマンドは 1 つだけなので、**match-all** でも **match-any** でもキーワードの機能は変わりません。
ステップ 3	**policy-map** *policy-map-name*	ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 4	**class** *class-map-name*	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップ クラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。

	コマンド	目的
ステップ 5	**trust** [**cos** | **dscp** | **ip-precedence**]	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼ステートを設定します。 **（注）** このコマンドと **set** コマンドは、同じポリシー マップ内で相互に排他的になります。**trust** コマンドを入力する場合は、ステップ 6 へ進んでください。 デフォルトでは、ポートは trusted ではありません。キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • **dscp**：QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • **ip-precedence**：QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 詳細については、「CoS/DSCP マップの設定」（P.38-48）を参照してください。
ステップ 6	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp** *new-dscp*：分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *new-precedence*：分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ～ 7 です。

	コマンド	目的
ステップ 7	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類したトラフィックにポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」（P.38-5）を参照してください。 • *rate-bps*：平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • *burst-byte*：通常のバースト サイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」（P.38-49）を参照してください。
ステップ 8	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *interface-id*	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 10	**service-policy input** *policy-map-name*	ポリシーマップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 11	**end**	特権 EXEC モードに戻ります。

階層型ポリシー マップの作成

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	VLAN レベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）**match-all**：このクラス マップ内のすべての一致ステートメント論理積をとります。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）**match-any**：このクラス マップ内のすべての一致ステートメントの論理和をとります。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • *class-map-name*：クラス マップの名前を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとにサポートされる **match** コマンドは 1 つだけなので、**match-all** でも **match-any** でもキーワードの機能は変わりません。

	コマンド	目的
ステップ 3	**match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。 • **access-group** *acl-index-or-name*：ACL の番号または名前を指定します。 • **ip dscp** *dscp-list*：着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list*：着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 4	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**class-map** [**match-all** | **match-any**] *class-map-name*	インターフェイス レベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）**match-all**：このクラス マップ内のすべての一致ステートメント論理積をとります。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）**match-any**：このクラス マップ内のすべての一致ステートメントの論理和をとります。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • *class-map-name*：クラス マップの名前を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとにサポートされる **match** コマンドは 1 つだけなので、**match-all** でも **match-any** でもキーワードの機能は変わりません。
ステップ 6	**match input-interface** *interface-id-list*	インターフェイス レベルのクラス マップを実行する物理ポートを指定します。次の方法で、最大 6 つ指定できます。 • 単一のポート（1 つのエントリとしてカウントされます） • スペースで区切られたポートのリスト（各ポートが 1 つのエントリとしてカウントされます） • ハイフンで区切られたポートの範囲（2 つのエントリとしてカウントされます） このコマンドは、子レベルのポリシー マップでだけ使用でき、子レベルのポリシー マップ内での唯一の一致条件である必要があります。
ステップ 7	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**policy-map** *policy-map-name*	ポリシー マップ名を入力してインターフェイス レベルのポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されておらず、ポリサーも実行されていません。

	コマンド	目的
ステップ 9	**class-map** *class-map-name*	インターフェイス レベルのトラフィック分類を定義し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシーマップのクラスマップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。
ステップ 10	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類したトラフィックにそれぞれポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」（P.38-5）を参照してください。 • *rate-bps*：平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • *burst-byte*：通常のバースト サイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」（P.38-49）を参照してください。
ステップ 11	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**policy-map** *policy-map-name*	リシー マップ名を入力することによって VLAN レベルのポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 13	**class** *class-map-name*	VLAN レベルのトラフィック分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシーマップのクラスマップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。

	コマンド	目的
ステップ 14	**trust** [**cos** | **dscp** | **ip-precedence**]	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼ステートを設定します。 **（注）** このコマンドと **set** コマンドは、同じポリシー マップ内で相互に排他的になります。**trust** コマンドを入力する場合は、ステップ 18 を省略してください。 デフォルトでは、ポートは trusted ではありません。キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • **dscp**：QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • **ip-precedence**：QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 詳細については、「CoS/DSCP マップの設定」（P.38-48）を参照してください。
ステップ 15	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp** *new-dscp*：分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *new-precedence*：分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ～ 7 です。
ステップ 16	**service-policy** *policy-map-name*	インターフェイスレベルのポリシーマップ名を指定し（ステップ 10 を参照）、VLAN レベルのポリシー マップと連動させます。 VLAN レベルのポリシー マップで複数のクラスが指定されている場合、各クラスで別々の **service-policy** *policy-map-name* コマンドを使用できます。
ステップ 17	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 18	**interface** *interface-id*	階層型のポリシー マップを適用する SVI を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 19	**service-policy input** *policy-map-name*	VLAN レベルのポリシーマップ名を指定し、SVI にそれを適用します。前のステップとこのコマンドを使用して、他の SVI にポリシーマップを適用します。 階層型 VLAN レベルのポリシー マップに複数のインターフェイスレベルのポリシー マップがある場合、すべてのクラスが **service-policy** *policy-map-name* コマンドで指定されている同じ VLAN レベルのポリシー マップに設定されている必要があります。
ステップ 20	**end**	特権 EXEC モードに戻ります。

集約ポリサーの作成

集約ポリサーを使用すると、同じポリシー マップ内の複数のトラフィック クラスで共有されるポリサーを作成できます。ただし、集約ポリサーを複数の異なるポリシー マップまたはポートにわたって使用することはできません。

集約ポリサーは、物理ポートの非階層型ポリシー マップにだけ設定できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos aggregate-policer** *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**}	同じポリシー マップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。 デフォルトでは、集約ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」（P.38-5）を参照してください。 • *aggregate-policer-name*：集約ポリサー名を指定します。 • *rate-bps*：平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • *burst-byte*：通常のバースト サイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。 • レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name*	必要に応じて、トラフィックを分類するクラス マップを作成します。
ステップ 4	**policy-map** *policy-map-name*	ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 5	**class** *class-map-name*	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 6	**police aggregate** *aggregate-policer-name*	同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。 • *aggregate-policer-name*：ステップ 2 で指定した名前を入力します。

	コマンド	目的
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 9	**service-policy input** *policy-map-name*	ポリシーマップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 10	**end**	特権 EXEC モードに戻ります。

DSCP マップの設定

ここでは、次の設定について説明します。

- 「CoS/DSCP マップの設定」（P.38-48）（任意）
- 「IP precedence/DSCP マップの設定」（P.38-49）（任意）
- 「ポリシング済み DSCP マップの設定」（P.38-49）（任意、マップのヌル設定が不適切な場合以外）
- 「DSCP/CoS マップの設定」（P.38-49）（任意）
- 「DSCP/DSCP 変換マップの設定」（P.38-50）（任意、マップのヌル設定が不適切な場合以外）

デフォルトの DSCP のマッピングは、「マッピング テーブルのデフォルト設定」（P.38-9）を参照してください。

DSCP/DSCP 変換マップを除くすべてのマップはグローバルに定義され、すべてのポートに適用されます。

CoS/DSCP マップの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map cos-dscp** *dscp1...dscp8*	CoS/DSCP マップを変更します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

IP precedence/DSCP マップの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map ip-prec-dscp** *dscp1...dscp8*	IP precedence/DSCP マップを変更します。 • *dscp1...dscp8*：IP precedence 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

ポリシング済み DSCP マップの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map policed-dscp** *dscp-list* **to** *mark-down-dscp*	ポリシング済み DSCP マップを変更します。 • *dscp-list*：最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *mark-down-dscp*：対応するポリシング設定（マークダウンされた）DSCP 値を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

DSCP/CoS マップの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-cos** *dscp-list* **to** *cos*	DSCP/CoS マップを変更します。 • *dscp-list*：最大 8 つの DSCP 値をスペースで区切って入力し、**to** キーワードを入力します。 • *cos*：DSCP 値と対応する CoS 値を入力します。 DSCP の範囲は 0 ～ 63、CoS の範囲は 0 ～ 7 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

DSCP/DSCP 変換マップの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを変更します。 • *dscp-mutation-name*：変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp*：最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *out-dscp*：1 つの DSCP 値を入力します。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id*	マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**mls qos trust dscp**	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された DSCP trusted 入力ポートにマップを適用します。 • *dscp-mutation-name*：ステップ 2 で指定した変換マップ名を入力します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

入力キューの特性の設定

ここでは、次の設定について説明します。

- 「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」（P.38-50）（任意）
- 「入力キュー間のバッファ スペースの割り当て」（P.38-51）（任意）
- 「入力キュー間の帯域幅の割り当て」（P.38-52）（任意）
- 「入力プライオリティ キューの設定」（P.38-53）（任意）

入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* または **mls qos srr-queue input cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を入力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 39 および 48 ～ 63 はキュー 1 およびしきい値 1 にマッピングされます。DSCP 値 40 ～ 47 はキュー 2 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 ～ 4、6、および 7 はキュー 1 およびしきい値 1 にマッピングされます。CoS 値 5 はキュー 2 およびしきい値 1 にマッピングされます。 • *queue-id*：指定できる範囲は 1 ～ 2 です。 • *threshold-id*：指定できる範囲は 1 ～ 3 です。しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8*：最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 63 です。 • *cos1… cos8*：最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
ステップ 3	**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2*	入力キューに 2 つの WTD しきい値の割合（しきい値 1 および 2 用）を割り当てます。デフォルトでは、両方のしきい値が 100% に設定されています。 • *queue-id*：指定できる範囲は 1 ～ 2 です。 • *hreshold-percentage1 threshold-percentage2*：指定できる範囲は 1 ～ 100 です。各値はスペースで区切ります。 各しきい値は、キューに割り当てられたキュー記述子の総数に対する割合です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

入力キュー間のバッファ スペースの割り当て

2 つのキュー間で入力バッファを分割する比率を定義します（スペース量を割り当てます）。バッファ割り当てと帯域幅割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量が制御されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2	**mls qos srr-queue input buffers** *percentage1 percentage2*	入力キュー間のバッファを割り当てます。 デフォルトでは、バッファの 90% がキュー 1 に、残りの 10% がキュー 2 に割り当てられます。 *percentage1 percentage2*：指定できる範囲は 0 ～ 100 です。各値はスペースで区切ります。 キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。

入力キュー間の帯域幅の割り当て

入力キュー間に割り当てられる使用可能な帯域幅の量を指定する必要があります。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。帯域幅割り当てとバッファ割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量を制御できます。入力キューで SRR が動作するのは、共有モードの場合のみです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input bandwidth** *weight1 weight2*	入力キューに共有ラウンド ロビン重みを割り当てます。 *weight1 および* weight2 のデフォルト設定は 4 です（帯域幅の 1/2 が 2 つのキューで等しく共有されます）。 *weight1* および *weight2*：指定できる範囲は、1 ～ 100 です。各値はスペースで区切ります。 SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。詳細については、「入力プライオリティ キューの設定」（P.38-53）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。

入力プライオリティ キューの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight*	キューをプライオリティ キューとして割り当て、内部リングが輻輳している場合にリングの帯域幅を保証します。 デフォルトのプライオリティ キューはキュー 2 です。このキューには帯域幅の 10% が割り当てられています。 • *queue-id*：指定できる範囲は 1 ～ 2 です。 • **bandwidth** *weight*：内部リングの帯域幅に対する割合を割り当てます。指定できる範囲は 0 ～ 40 です。値が大きい場合はリング全体に影響が及び、パフォーマンスが低下することがあるため、保証できる帯域幅は制限されています。
ステップ 3	**end**	特権 EXEC モードに戻ります。

出力キューの特性の設定

ここでは、次の設定について説明します。

- 「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」（P.38-54）
- 「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」（P.38-54）（任意）
- 「出力キューおよび ID への DSCP または CoS 値のマッピング」（P.38-55）（任意）
- 「出力キューでの SRR シェーピング重みの設定」（P.38-55）（任意）
- 「出力キューでの SRR 共有重みの設定」（P.38-56）（任意）
- 「出力緊急キューの設定」（P.38-57）（任意）
- 「出力インターフェイスの帯域幅の制限」（P.38-57）（任意）

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4*	バッファをキューセットに割り当てます。 デフォルトでは、すべての割り当て値は 4 つのキューに均等にマッピングされます（25、25、25、25）。各キューがバッファ スペースの 1/4 を持ちます。 • *qset-id*：キュー セットの ID を入力します。指定できる範囲は 1 ～ 2 です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。 • *allocation1 ... allocation4*：キューセット内のキューごとに 1 つずつ、合計 4 つのパーセンテージを指定します。*allocation1*、*allocation3*、*allocation4* の場合、使用可能な範囲は 0 ～ 99 です。*allocation2* の場合、範囲は 1 ～ 100 です（CPU バッファを含める）。 トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。
ステップ 3	**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*	WTD しきい値を設定し、バッファのアベイラビリティを保証し、キューセット（ポートごとに 4 つの出力キュー）の最大メモリ割り当てを設定します。 デフォルトでは、キュー 1、3、および 4 の WTD は 100% に設定されています。キュー 2 の WTD は 200% に設定されています。キュー 1、2、3、および 4 の専用は 50% に設定されています。すべてのキューの最大は 400% に設定されています。 • *qset-id*：ステップ 2 で指定したキュー セットの ID を入力します。指定できる範囲は 1 ～ 2 です。 • *queue-id*：コマンドの実行対象となるキュー セット内の特定のキューを入力します。指定できる範囲は 1 ～ 4 です。 • *drop-threshold1 drop-threshold2*：キューの割り当てメモリの割合として表される 2 つの WTD を指定します。指定できる範囲は 1 ～ 3200% です。 • *reserved-threshold*：割り当てメモリの割合として表されるキューに保証（確保）されるメモリ サイズを入力します。指定できる範囲は 1 ～ 100% です。 • *maximum-threshold*：フル状態のキューが、予約量を超えるバッファを取得できるようにします。この値は、共通プールが空でない場合に、パケットがドロップされるまでキューが使用できるメモリの最大値です。指定できる範囲は 1 ～ 3200% です。
ステップ 4	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**queue-set** *qset-id*	キューセットにポートをマッピングします。 • *qset-id*：ステップ 2 で指定したキュー セットの ID を入力します。指定できる範囲は 1 ～ 2 です。デフォルトは 1 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。

出力キューおよび ID への DSCP または CoS 値のマッピング

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue output dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* または **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 15 はキュー 2 およびしきい値 1 に、DSCP 値 16 ～ 31 はキュー 3 およびしきい値 1 に、DSCP 値 32 ～ 39 および 48 ～ 63 はキュー 4 およびしきい値 1 に、DSCP 値 40 ～ 47 はキュー 1 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 に、CoS 値 2 および 3 はキュー 3 およびしきい値 1 に、CoS 値 4、6、および 7 はキュー 4 およびしきい値 1 に、CoS 値 5 はキュー 1 およびしきい値 1 にマッピングされます。 • *queue-id*：指定できる範囲は 1 ～ 4 です。 • *threshold-id*：指定できる範囲は 1 ～ 3 です。しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8*：最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 63 です。 • *cos1...cos8*：最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

出力キューでの SRR シェーピング重みの設定

各キューに割り当てられる使用可能な帯域幅の量を指定できます。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

出力キューにシェーピング重み、共有重み、またはその両方を設定できます。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。シェーピング重みの詳細については、「SRR のシェーピングおよび共有」（P.38-20）を参照してください。共有重みの詳細については、「出力キューでの SRR 共有重みの設定」（P.38-56）を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth shape** *weight1 weight2 weight3 weight4*	出力キューに SRR 重みを割り当てます。 デフォルトでは、weight1 は 25、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。 *weight1 weight2 weight3 weight4*：シェーピングされるポートの割合を制御する重みを入力します。このキューのシェーピング帯域幅は、インバース比率（1/*weight*）によって制御されます。各値はスペースで区切ります。指定できる範囲は 0 ～ 65535 です。 重み 0 を設定した場合は、対応するキューが共有モードで動作します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。シェーピングおよび共有の両方に対して同じキューセットのキューを設定した場合は、必ず番号が最も小さいキューにシェーピングを設定してください。 シェーピング モードは、共有モードを無効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。

出力キューでの SRR 共有重みの設定

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有ができます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth share** *weight1 weight2 weight3 weight4*	出力キューに SRR 重みを割り当てます。 デフォルトでは、4 つの重みがすべて 25 です（各キューに帯域幅の 1/4 が割り当てられています）。 • *weight1 weight2 weight3 weight4*：SRR スケジューラがパケットを送信する頻度の比率を制御する重みを入力します。各値はスペースで区切ります。指定できる範囲は 1 ～ 255 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

出力緊急キューの設定

出力緊急キューにパケットを入れることにより、特定のパケットのプライオリティを他のすべてのパケットより高く設定できます。SRR は、このキューが空になるまで処理してから他のキューを処理します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	スイッチの QoS をイネーブルにします。
ステップ 3	**interface** *interface-id*	出力ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**priority-queue out**	デフォルトでディセーブルに設定されている出力緊急キューをイネーブルにします。 このコマンドを設定すると、SRR に参加するキューは 1 つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。つまり、**srr-queue bandwidth shape** または **srr-queue bandwidth share** コマンドの *weight1* が無視されます（比率計算に使用されません）。
ステップ 5	**end**	特権 EXEC モードに戻ります。

出力インターフェイスの帯域幅の制限

出力ポートの帯域幅は制限できます。たとえば、カスタマーが高速リンクの一部しか費用を負担しない場合は、帯域幅をその量に制限できます。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レートを制限するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth limit** *weight1*	ポートの上限となるポート速度の割合を指定します。指定できる範囲は 10 ～ 90 です。 デフォルトでは、ポートのレートは制限されず、100% に設定されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。

標準 QoS のモニタリングおよびメンテナンス

コマンド	目的
show access-lists	入力を確認します。
show class-map [*class-map-name*]	トラフィックを分類するための一致基準を定義した QoS クラス マップを表示します。
show mls qos	グローバル QoS コンフィギュレーション情報を表示します。
show mls qos aggregate-policer [*aggregate-policer-name*]	集約ポリサーの設定を表示します。
show mls qos input-queue	入力キューの QoS 設定を表示します。
show mls qos interface [*interface-id*] [**buffers** | **policers** | **queueing** | **statistics**]	バッファ割り当て、ポリサーが設定されているポート、キューイング方式、入出力統計情報など、ポート レベルの QoS 情報が表示されます。
show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	QoS のマッピング情報を表示します。 DSCP 入力キューしきい値マップは、表形式で表示されます。d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1（02-01）のようになります。 CoS 入力キューしきい値マップでは、先頭行に CoS 値、2 番めの行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2（2-2）のようになります。
show mls qos maps dscp-to-cos	入力を確認します。
show mls qos queue-set [*qset-id*]	出力キューの QoS 設定を表示します。
show mls qos vlan *vlan-id*	指定の SVI に適用されたポリシー マップを表示します。
show policy-map [*policy-map-name* [**class** *class-map-name*]]	着信トラフィックの分類条件を定義した QoS ポリシー マップを表示します。 **（注）** 着信トラフィックの分類情報を表示する場合は、**show policy-map interface** 特権 EXEC コマンドを使用しないでください。**control-plane** および **interface** キーワードはサポートされていません。表示される統計情報は無視してください。
show running-config | include rewrite	DSCP 透過性設定を表示します。

標準 QoS の設定例

SRR スケジューラの設定：例

次の例では、出力ポートで稼働する SRR スケジューラの重み比を設定する方法を示します。4 つのキューが使用され、共有モードで各キューに割り当てられる帯域幅の比率は、キュー 1、2、3、および 4 に対して 1/(1 + 2 + 3 + 4)、2/(1 + 2 + 3 + 4)、3/(1 + 2 + 3 + 4)、および 4/(1 + 2 + 3 + 4) になります（それぞれ、10、20、30、および 40%）。キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

ポートでの DSCP 信頼状態の設定：例

次に、ポートが DSCP を信頼する状態に設定し、着信した DSCP 値 10 ～ 13 が DSCP 値 30 にマッピングされるように DSCP/DSCP 変換マップ（*gi0/2-mutation*）を変更する例を示します。

```
Switch(config)# mls qos map dscp-mutation gi1/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi1/2-mutation
Switch(config-if)# end
```

IP トラフィック用の ACL 権限の許可：例

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。ネットワーク アドレスのホスト部分にワイルドカード ビットが適用されます。アクセス リストのステートメントと一致しない送信元アドレスのホストはすべて拒否されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IP トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IP トラフィック（precedence 値は 5）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

次に、任意の送信元からアドレス 224.0.0.2 の宛先グループへの PIM トラフィック（DSCP 値は 32）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

クラス マップの設定：例

次に、*class1* というクラス マップの設定例を示します。*class1* にはアクセス リスト 103 という一致条件が 1 つ設定されています。このクラス マップによって、任意のホストから任意の宛先へのトラフィック（DSCP 値は 10）が許可されます。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
Switch#
```

次に、DSCP 値が 10、11、および 12 である着信トラフィックと照合する、*class2* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#
```

次に、IP precedence 値が 5、6、および 7 である着信トラフィックと照合する、*class3* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```

ポリシー マップの作成：例

次に、ポリシー マップを作成し、入力ポートに結合する例を示します。この設定では、IP 標準 ACL でネットワーク 10.1.0.0 からのトラフィックを許可します。この分類にトラフィックが一致した場合、着信パケットの DSCP 値が信頼されます。一致したトラフィックが平均トラフィック レート（48000 bps）、および標準バースト サイズ（8000 バイト）を超過している場合は、（ポリシング済み DSCP マップに基づいて）DSCP はマークダウンされて、送信されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map flow1t
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input flow1t
```

レイヤ 2 MAC ACL の作成：例

次に、2 つの許可ステートメントを指定してレイヤ 2 MAC ACL を作成し、入力ポートに結合する例を示します。最初の許可ステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番めの許可ステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

集約ポリサーの作成：例

次に、集約ポリサーを作成して、ポリシー マップ内の複数のクラスに結合する例を示します。この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。ネットワーク 10.1.0.0 から着信するトラフィックの場合は、着信パケットの DSCP が信頼されます。ホスト 11.3.1.1 から着信するトラフィックの場合、パケットの DSCP は 56 に変更されます。ネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィック レートには、ポリシングが設定されます。トラフィックが平均レート（48000 bps）、および標準バースト サイズ（8000 バイト）を超過している場合は、（ポリシング済み DSCP マップに基づいて）DSCP がマークダウンされて、送信されます。ポリシー マップは入力ポートに結合されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

CoS/DSCP マップの設定：例

次に、CoS/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

DSCP マップの設定：例

次に、IP precedence/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

次に、DSCP 50 ～ 57 を、マークダウンされる DSCP 値 0 にマッピングする例を示します。

```
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    00 00 00 00 00 00 00 00 58 59
      6 :    60 61 62 63
```

（注） このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点にある値が、マークダウンされる値です。たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

次に、DSCP 値 0、8、16、24、32、40、48、および 50 を CoS 値 0 にマッピングして、マップを表示する例を示します。

```
Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 00 01
      1 :    01 01 01 01 01 01 00 02 02 02
      2 :    02 02 02 02 00 03 03 03 03 03
      3 :    03 03 00 04 04 04 04 04 04 04
      4 :    00 05 05 05 05 05 05 05 00 06
      5 :    00 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

（注） 上記の DSCP/CoS マップでは、CoS 値が表形式で示されています。d1 列は DSCP の最上位桁、d2 行は DSCP の最下位桁を示します。d1 と d2 の交点にある値が CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。明示的に設定されていないすべてのエントリは変更されません（空のマップで指定された値のままです）。

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
   mutation1:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 10 10
      1 :    10 10 10 10 14 15 16 17 18 19
      2 :    20 20 20 23 24 25 26 27 28 29
      3 :    30 30 30 30 30 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

（注） 上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点の値が、変換される値です。たとえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。

次の例では、DSCP 値 0 ～ 6 を、入力キュー 1 とドロップしきい値 50% のしきい値 1 にマッピングする方法を示します。DSCP 値 20 ～ 26 は、入力キュー 1 とドロップしきい値 70% のしきい値 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

この例では、50% の WTD しきい値が DSCP 値（0 ～ 6）に割り当てられており、70% の WTD しきい値が割り当てられた DSCP 値（20 ～ 26）よりも先にドロップされます。

入力キューの設定：例

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

次に、キューに入力帯域幅を割り当てる例を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/（25+75）、キュー 2 が 75/（25+75）です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

デフォルト設定に戻すには、**no mls qos srr-queue input priority-queue** *queue-id* グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth 0** を入力します。

次に、キューに入力帯域幅を割り当てる例を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 および 2 に割り当てられている帯域幅比率は 4/(4 + 4) です。SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。その後、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

出力キューの設定：例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。出力キュー 1 にはバッファスペースの 40%、出力キュー 2、3、および 4 には 20% が割り当てられます。キュー 2 のドロップしきい値は割り当てメモリの 40 および 60% に設定され、割り当てメモリの 100% が保証（確保）され、パケットがドロップされるまでこのキューが使用できる最大メモリが 200% に設定されます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet1/1
lSwitch(config-if)# queue-set 2
```

次に、DSCP 値 10 および 11 を出力キュー 1 およびしきい値 2 にマッピングする例を示します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

次に、キュー 1 に帯域幅のシェーピングを設定する例を示します。キュー 2、3、4 の重み比が 0 に設定されているので、これらのキューは共有モードで動作します。キュー 1 の帯域幅の重みは 1/8（12.5%）です。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

次に、ポートの帯域幅を 80% に制限する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth limit 80
```

このコマンドを 80% に設定すると、ポートは該当期間の 20% はアイドルになります。回線レートは接続速度の 80%（800 Mbps）に低下します。ただし、ハードウェアはライン レートを 6% 単位で調整しているため、この値は厳密ではありません。

レイヤ 2 MAC ACL の作成：例

次に、2 つの許可（permit）ステートメントを指定したレイヤ 2 の MAC ACL を作成する例を示します。最初のステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番めのステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
```

```
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Auto-QoS コンフィギュレーション	*第 39 章「auto-QoS の設定」*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 39

auto-QoS の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

auto-QoS の前提条件

- ルーテッド ポートで Cisco IP Phone の自動 QoS をイネーブルにすると、スタティック IP アドレスを IP Phone に割り当てます。
- デフォルトでは、CDP 機能はすべてのポート上でイネーブルです。自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。

auto-QoS の制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- 接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。
- このリリースは、Cisco IP SoftPhone Version 1.3(3) 以降のみをサポートします。
- auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。必要に応じて QoS 設定を微調整できますが、自動 QoS が完了した後にのみ調整することを推奨します。詳細については、「コンフィギュレーションにおける自動 QoS の影響」（P.39-8）を参照してください。
- スイッチで受信された制御トラフィック（スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）やルーティング アップデート パケットなど）には、入力 QoS 処理がすべて行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。

- 自動 QoS は、非ルーテッド ポートおよびルーテッド ポートで Cisco IP Phone に VoIP のスイッチを設定します。また、自動 QoS は Cisco SoftPhone アプリケーションを稼働するデバイスの VoIP 用にスイッチを設定します。
- Cisco SoftPhone を稼働するデバイスが非ルーテッド ポートまたはルーテッド ポートに接続されている場合、スイッチはポート単位で Cisco SoftPhone アプリケーション 1 つのみをサポートします。
- auto-Qos VoIP では、**priority-queue** インターフェイス コンフィギュレーション コマンドを出力インターフェイスに使用します。ポリシー マップおよび信頼できるデバイスを Cisco IP Phone の同一インターフェイス上に設定することも可能です。
- auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシー マップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成したポリシー マップではなくこの新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除し、新しいポリシー マップをインターフェイスに適用します。
- 自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。

auto-QoS について

この章では、スイッチで自動 Quality of Service（auto-QoS）コマンドを使用して、QoS を設定する方法について説明します QoS を使用すると、特定のトラフィックを他のトラフィック タイプよりも優先的に処理できます。QoS を使用しなかった場合、スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。

QoS は物理ポートおよびスイッチ仮想インターフェイス（SVI）に設定できます。ポリシー マップを適用する他に、分類、キューイング、およびスケジューリングなどの QoS を同じ方法で物理ポートおよび SVI に設定します。物理ポートに QoS を設定した場合は、非階層型のポリシー マップをポートに適用します。SVI に QoS を設定すると、非階層型、または階層型のポリシー マップが適用されます。

スイッチは、モジュラ QoS CLI（MQC）コマンドの一部をサポートします。MQC コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Guide*』の「Modular Quality of Service Command-Line Interface Overview」の章を参照してください。

Auto-QoS

自動 QoS 機能を使用して、QoS 機能の配置を容易にできます。自動 QoS は、ネットワーク設計を確認し、スイッチがさまざまなトラフィック フローに優先度を指定できるように QoS 設定をイネーブルにします。自動 QoS は、デフォルト（ディセーブル）の QoS 動作を使用せずに、入力および出力キューを使用します。スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供し、単一キューからパケットを送信します。

自動 QoS をイネーブルにすると、トラフィック タイプおよび入力パケット ラベルに基づいてトラフィックを自動的に分類します。スイッチは分類した結果を使用して適切な出力キューを選択します。

sdm prefer dual ipv4-and-ipv6 グローバル コンフィギュレーション コマンドを使用してデュアル IPv4 および IPv6 SDM テンプレートを設定すると、自動 QoS で IPv4 と IPv6 の両方のトラフィックがサポートされます。

自動 QoS コマンドを使用して Cisco IP Phone、および Cisco SoftPhone アプリケーションを実行するデバイスに接続するポートを指定します。また、アップリンクを介して信頼のおけるトラフィックを受信するポートを指定します。自動 QoS は次の機能を実行します。

- Cisco IP Phone の有無を検知します。
- QoS 分類の設定
- 出力キューの設定

生成される自動 QoS 設定

デフォルトでは、自動 QoS はすべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、に示すように、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います（表 39-1 を参照）。

表 39-1　トラフィック タイプ、パケット ラベル、およびキュー

	VoIP[1] データ トラフィック	VoIP Control トラフィック	ルーティング プロトコル トラフィック	STP BPDU トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP	46	24、26	48	56	34	–	
CoS	5	3	6	7	4	–	
CoS/入力キュー マップ	2、3、4、5、6、7（キュー 2）					0、1（キュー 1）	
CoS/出力キュー マップ	5（キュー 1）	3、6、7（キュー 2）			4（キュー 3）	2（キュー 3）	0、1（キュー 4）

1. VoIP = Voice over IP

表 39-2 に、入力キューに対して生成された自動 QoS の設定を示します。

表 39-2　入力キューに対する Auto-QoS の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	キュー（バッファ）サイズ
SRR 共有	1	0、1	81 %	67 %
プライオリティ	2	2、3、4、5、6、7	19 %	33 %

表 39-3 に、出力キューに対して生成される auto-QoS の設定を示します。

表 39-3　出力キューに対する auto-QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ	1	5	最大 100%	16 %	10%
SRR 共有	2	3、6、7	10%	6 %	10%

表 39-3　出力キューに対する auto-QoS の設定 （続き）

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
SRR 共有	3	2、4	60%	17 %	26 %
SRR 共有	4	0、1	20%	61 %	54 %

最初のポートで auto-QoS 機能をイネーブルにすると、次の自動アクションが実行されます。

- QoS がグローバルにイネーブルになり（**mls qos** グローバル コンフィギュレーション コマンド）、そのあと、他のグローバル コンフィギュレーション コマンドが追加されます。
- Cisco IP Phone に接続されたネットワークの端にあるポート上で **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、スイッチは信頼境界機能をイネーブルにします。スイッチは、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone が存在するかしないかを検出します。Cisco IP Phone が検出されると、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼するように設定されます。また、スイッチはポリシングを使用してパケットがプロファイル内か、プロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。Cisco IP Phone が存在しない場合、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼しないように設定されます。スイッチは、表 39-2 および表 39-3 の設定に従ってポート上の入力および出力キューを設定します。ポリシングがポリシーマップ分類と一致したトラフィックに適用された後で、スイッチが信頼境界の機能をイネーブルにします。
- **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを、Cisco SoftPhone を稼働するデバイスに接続されたネットワークのエッジのポートに入力すると、スイッチはポリシングを使用して、パケットがプロファイルの内部または外部にいるかを判断し、パケット上のアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。スイッチは、表 39-2 および表 39-3 の設定に従ってポート上の入力および出力キューを設定します。
- ネットワーク内部に接続されたポート上で、**auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは、入力パケットでルーティングされないポートの CoS 値、またはルーテッド ポートの DSCP 値を信頼します（トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります）。スイッチは、表 39-2 および表 39-3 の設定値に従ってポートの入力キューと出力キューを設定します。

  信頼境界機能の詳細については、「ポート セキュリティを確保するための信頼境界機能の設定」（P.38-34）を参照してください。

auto qos voip cisco-phone、**auto qos voip cisco-softphone**、または **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを使用して自動 QoS をイネーブルにする場合、スイッチはトラフィック タイプおよび入力パケット ラベルに応じて自動的に QoS 設定を生成し、表 39-4 にリストされているコマンドをポートに適用します。

表 39-4　生成される自動 QoS 設定

説明	自動的に生成されるコマンド
スイッチが自動的に標準 QoS をイネーブルにして Cos/DSCP マップ（着信パケットの CoS 値の DSCP 値へのマッピング）を設定します。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**
スイッチが、自動的に CoS 値を入力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 0** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 1** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 3 3 5**
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**
スイッチが、自動的に DSCP 値を入力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 32** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47**

表 39-4　生成される自動 QoS 設定 （続き）

説明	自動的に生成されるコマンド
スイッチが、自動的に DSCP 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**
スイッチが自動的に入力キューを設定します。キュー 2 がプライオリティ キューでキュー 1 が共有モードです。また、スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 90 10** Switch(config)# **mls qos srr-queue input threshold 1 8 16** Switch(config)# **mls qos srr-queue input threshold 2 34 66** Switch(config)# **mls qos srr-queue input buffers 67 33**
スイッチが自動的に出力キューのバッファ サイズを設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード（シェーピングまたは共有）を設定します。	Switch(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Switch(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Switch(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Switch(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Switch(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Switch(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Switch(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Switch(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Switch(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Switch(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Switch(config-if)# **priority-que out** Switch(config-if)# **srr-queue bandwidth share 10 10 60 20**

表 39-4　生成される自動 QoS 設定 （続き）

説明	自動的に生成されるコマンド
auto qos voip trust コマンドを入力した場合、**mls qos trust cos** コマンドを使用することによって、スイッチは非ルーテッド ポートで受信したパケットの CoS 値を信頼するように、または **mls qos trust dscp** コマンドを使用することによって、ルーテッド ポートで受信したパケットの DSCP 値を信頼するように、自動的に入力分類を設定します。	Switch(config-if)# **mls qos trust cos** Switch(config-if)# **mls qos trust dscp**
auto qos voip cisco-phone コマンドを入力すると、スイッチは自動的に信頼境界機能をイネーブルにします。この機能は、CDP を使用して Cisco IP Phone の有無を検出するものです。	Switch(config-if)# **mls qos trust device cisco-phone**
auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。	Switch(config)# **mls qos map policed-dscp 24 26 46 to 0** Switch(config)# **class-map match-all AutoQoS-VoIP-RTP-Trust** Switch(config-cmap)# **match ip dscp ef** Switch(config)# **class-map match-all AutoQoS-VoIP-Control-Trust** Switch(config-cmap)# **match ip dscp cs3 af31** Switch(config)# **policy-map AutoQoS-Police-SoftPhone** Switch(config-pmap)# **class AutoQoS-VoIP-RTP-Trust** Switch(config-pmap-c)# **set dscp ef** Switch(config-pmap-c)# **police 320000 8000 exceed-action policed-dscp-transmit** Switch(config-pmap)# **class AutoQoS-VoIP-Control-Trust** Switch(config-pmap-c)# **set dscp cs3** Switch(config-pmap-c)# **police 32000 8000 exceed-action policed-dscp-transmit**
クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。	Switch(config-if)# **service-policy input AutoQoS-Police-SoftPhone**
auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。	witch(config)# **mls qos map policed-dscp 24 26 46 to 0** Switch(config)# **class-map match-all AutoQoS-VoIP-RTP-Trust** Switch(config-cmap)# **match ip dscp ef** Switch(config)# **class-map match-all AutoQoS-VoIP-Control-Trust** Switch(config-cmap)# **match ip dscp cs3 af31** Switch(config)# **policy-map AutoQoS-Police-CiscoPhone** Switch(config-pmap)# **class AutoQoS-VoIP-RTP-Trust** Switch(config-pmap-c)# **set dscp ef** Switch(config-pmap-c)# **police 320000 8000 exceed-action policed-dscp-transmit** Switch(config-pmap)# **class AutoQoS-VoIP-Control-Trust** Switch(config-pmap-c)# **set dscp cs3** Switch(config-pmap-c)# **police 32000 8000 exceed-action policed-dscp-transmit**
クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-CiscoPhone*）を、Cisco IP Phone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。	Switch(config-if)# **service-policy input AutoQoS-Police-CiscoPhone**

コンフィギュレーションにおける自動 QoS の影響

自動 QoS がイネーブルになっていると、**auto qos voip** インターフェイス コンフィギュレーション コマンドおよび生成された設定が、実行コンフィギュレーションに追加されます。

スイッチは、自動 QoS が生成したコマンドを、CLI から入力したように適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

自動 QoS がイネーブルまたはディセーブルの場合に自動生成される QoS コマンドを表示するには、**debug auto qos** 特権 EXEC コマンドを入力してから、自動 QoS をイネーブルにします。詳細については、このリリースに対応するコマンド リファレンスにある **debug** autoqos コマンドの項を参照してください。

ポートの auto-QoS をディセーブルにするには、**no auto qos voip** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

no mls qos グローバル コンフィギュレーション コマンドを使用して、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合は、パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念はありません。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

auto-QoS の設定方法

VoIP 用自動 QoS のイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	Cisco IP Phone に接続されたポート、Cisco SoftPhone 機能を実行する装置に接続されたポート、またはネットワーク内部の信頼性のある他のスイッチやルータに接続されたアップリンク ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**auto qos voip** {**cisco-phone** | **cisco-softphone** | **trust**}	Auto-QoS をイネーブルにします。 • **cisco-phone**：Cisco IP Phone に接続するポートを指定します。着信パケットの QoS ラベルは電話が検出された場合のみ信頼されます。 • **cisco-softphone**：Cisco SoftPhone 機能を実行するデバイスに接続するポートを指定します。 • **trust**：信頼性のあるスイッチまたはルータに接続するアップリンク ポートを指定します。入力パケットの VoIP トラフィック分類は信頼されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。

VoIP トラフィックに優先度を指定する QoS 設定

この作業では、QoS ドメインのエッジにあるスイッチで VoIP トラフィックを他のトラフィックより優先させるように設定する方法について説明します。

	コマンド	目的
ステップ 1	**debug auto qos**	Auto-QoS のデバッグをイネーブルにします。デバッグをイネーブルにすると、スイッチは、自動 QoS がイネーブルである場合に自動的に生成される QoS 設定を表示します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cdp enable**	CDP をグローバルにイネーブルにします。デフォルトでは有効に設定されています。
ステップ 4	**interface** *interface-id*	Cisco IP Phone に接続するスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**auto qos voip cisco-phone**	インターフェイス上で自動 QoS をイネーブルにし、インターフェイスが Cisco IP Phone に接続されるように指定します。 着信パケット内の QoS ラベルは、Cisco IP Phone が検出された場合だけ信頼されます。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7		Cisco IP Phone に接続されているポートの数だけ、ステップ 4 ～ 6 を繰り返します。
ステップ 8	**interface** *interface-id*	信頼できるスイッチまたはルータに接続されていると識別されたスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。図 39-1 を参照してください。
ステップ 9	**auto qos voip trust**	ポートで自動 QoS をイネーブルにし、そのポートが信頼できるルータまたはスイッチに接続されるように指定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

auto-QoS のモニタリングおよびメンテナンス

コマンド	目的
show auto qos [**interface** [*interface-id*]]	自動 QoS がイネーブルのインターフェイスで入力される QoS コマンドを表示します。
show mls qos	グローバル QoS コンフィギュレーション情報を表示します。
show mls qos interface [*interface-id*] [**buffers** | **queueing**]	ポート レベルで QoS 情報を表示します。
show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	QoS マッピング情報を表示します。分類では、QoS はマッピング テーブルを使用してトラフィックのプライオリティを表示し、受信した CoS、DSCP、または IP precedence 値から対応する CoS または DSCP 値を取得します。
show mls qos input-queue	入力キューの QoS 設定を表示します。
show running-config	定義されたマクロを含む現在の動作設定を表示します。

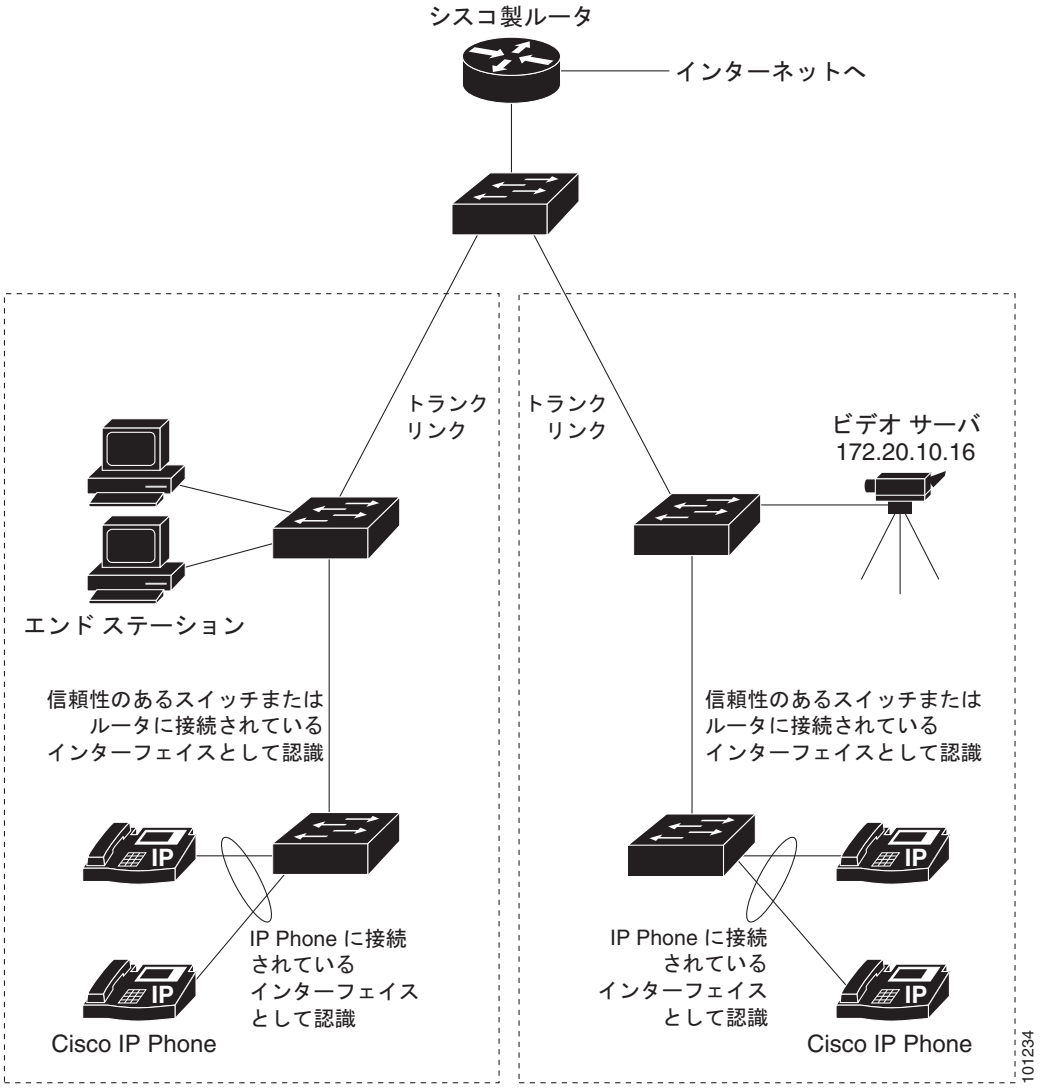
auto-QoS の設定例

auto-QoS ネットワーク：例

この例では、VoIP トラフィックが他のすべてのトラフィックよりも優先されるネットワーク上で、自動 QoS を実装する方法を示します。QoS ドメインのエッジにあるワイヤリング クローゼット内のスイッチ上で、自動 QoS はイネーブルです。

QoS パフォーマンスを最適にするには、ネットワーク内部の装置すべてで自動 QoS をイネーブルにします。

図 39-1　　ネットワークでの自動 QoS の設定例



自動 QoS VoIP の信頼のイネーブル化：例

次の例では、ポートに接続されているスイッチまたはルータが信頼できる装置である場合に、auto-QoS をイネーブルにし、着信パケットで受信した QoS ラベルを信頼する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
標準 QoS（Standard SIP）	*第 38 章「標準 QoS の設定」*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 40

EtherChannel の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

EtherChannel の設定に関する制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- ポート チャネルは LAN Base イメージでのみサポートされます。

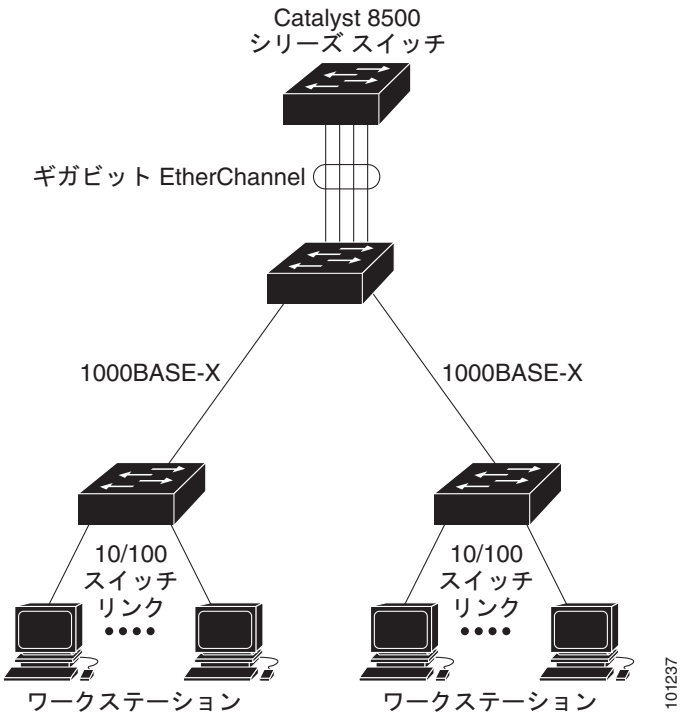
EtherChannel の設定に関する情報

この章では、スイッチで EtherChannel を設定する方法について説明します。EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用すると、ワイヤリング クローゼットおよびデータ センタ間の帯域幅を拡張できます。EtherChannel はネットワーク上でボトルネックの発生が見込まれるところに、任意に配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。この章では、リンクステート トラッキングを設定する方法についても説明します。

EtherChannel

EtherChannel は、単一の論理リンクにバンドルされた個々のファスト イーサネットまたはギガビット イーサネット リンクで構成されます（図 40-1 を参照）。

図 40-1　　一般的な EtherChannel 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 800Mbps（ファスト EtherChannel）または 2 Gbps（ギガビット EtherChannel）の全二重帯域幅を提供します。各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

EtherChannel の数は 6 に制限されています。詳細については、「EtherChannel 設定時の注意事項」（P.40-11）を参照してください。

EtherChannel は、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、または On のいずれかのモードに設定できます。EtherChannel の両端は同じモードで設定します。

- EtherChannel の一方の端を PAgP または LACP モードに設定すると、システムはもう一方の端とネゴシエーションし、アクティブにするポートを決定します。互換性のないポートは独立ステートになり、他の単一リンクのようにデータ トラフィックを伝送し続けます。ポート設定は変更されませんが、ポートは EtherChannel に参加しません。
- EtherChannel を **on** モードに設定すると、ネゴシエーションは実行されません。スイッチは EtherChannel 内で互換性のあるすべてのポートを強制的にアクティブにします。EtherChannel のもう一方の端（他のスイッチ上）も、同じように **on** モードに設定する必要があります。それ以外を設定した場合、パケットの損失が発生します。

EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。スイッチでトラップがイネーブルになっている場合、スイッチ、EtherChannel、および失敗したリンクを区別したトラップが送信されます。EtherChannel の 1 つのリンク上の着信ブロードキャストおよびマルチキャスト パケットは、EtherChannel の他のリンクに戻らないようにブロックされます。

ポートチャネル インターフェイス

EtherChannel を作成すると、ポート チャネル論理インターフェイスも作成されます。

- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを動的に作成します。

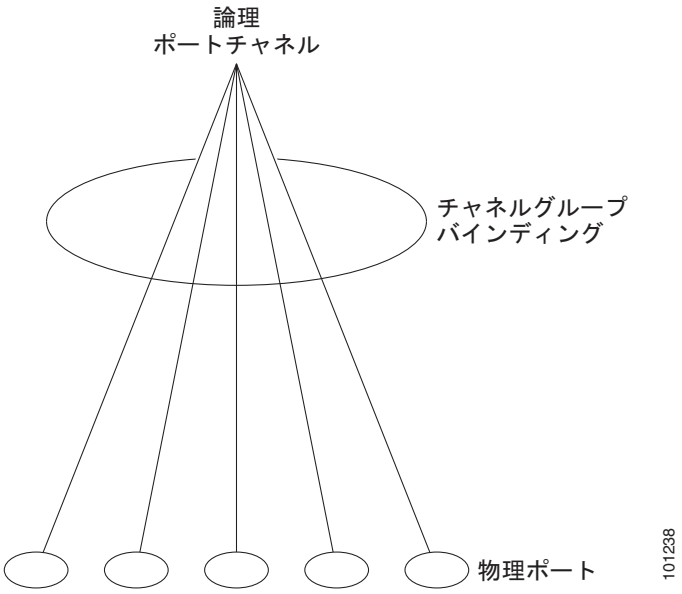
  また、**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。*channel-group-number* は *port-channel-number* と同じ値に設定することも、違う値を使用することもできます。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。そのあと、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

レイヤ 2 およびレイヤ 3 ポートのいずれの場合も、**channel-group** コマンドを実行すると、物理ポートと論理インターフェイスがバインドされます（図 40-2 を参照）。

各 EtherChannel には 1 ～ 6 番のポートチャネル論理インターフェイスがあります。ポートチャネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定した番号に対応しています。

図 40-2　物理ポート、論理ポートチャネル、およびチャネル グループの関係



EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャネル インターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、spanning-tree コマンドを使用して、レイヤ 2 EtherChannel をトランクとして設定します。

ポート集約プロトコル

ポート集約プロトコル（PAgP）はシスコ独自のプロトコルで、Cisco スイッチおよび PAgP をサポートするベンダーによってライセンス供与されたスイッチでのみ稼働します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の倫理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、PAgP は単一スイッチ ポートとして、スパニングツリーにそのグループを追加します。

PAgP モード

表 40-1 に、**channel-group** インターフェイス コンフィギュレーション コマンドでユーザが設定できる EtherChannel PAgP モードを示します。

表 40-1　EtherChannel PAgP モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。これにより、PAgP パケットの送信は最小限に抑えられます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードでは、どちらの場合も、ポートは相手ポートとのネゴシエーションにより、ポート速度、レイヤ 2 EtherChannel の場合はトランキング ステートおよび VLAN 番号などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

PAgP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートとともに EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、非サイレント動作としてスイッチ ポートを設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。ただし、サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

PAgP 学習方式およびプライオリティ

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャネル上のアドレスを学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。集約ポート ラーニングを使用している場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカル デバイスに手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるように、ポートを設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注） CLI（コマンドライン インターフェイス）で **physical-port** キーワードを指定した場合でも、スイッチがサポートするのは、集約ポート上でのアドレス ラーニングのみです。**pagp learn-method** コマンドおよび **pagp port-priority** コマンドはスイッチ ハードウェアに影響を及ぼしませんが、物理ポートによるアドレス ラーニングだけをサポートしているデバイスとの PAgP の相互運用性のために必要です。

スイッチのリンク パートナーが（Catalyst 1900 シリーズ スイッチなどのように）物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用してスイッチを物理ポート ラーナーに設定することを推奨します。送信元 MAC アドレスに基づいて負荷の分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。このように設定すると、送信元アドレスの学習元である EtherChannel 内の同じポートを使用して、パケットが Catalyst 1900 スイッチに送信されます。**pagp learn-method** コマンドは、このような場合のみ使用してください。

PAgP と仮想スイッチとの相互交流およびデュアルアクティブ検出

仮想スイッチは、仮想スイッチ リンク（VSL）により接続された複数の Catalyst 6500 コア スイッチであり、それらのスイッチ間で制御情報とデータ トラフィックを伝送します。スイッチのうちの 1 つはアクティブ モードです。その他のスイッチはスタンバイ モードです。冗長性のため、リモート スイッチはリモート サテライト リンク（RSL）によって仮想スイッチに接続されます。

2 つのスイッチ間の VSL に障害が発生すると、一方のスイッチは他方のスイッチのステータスを認識しません。両方のスイッチがアクティブ モードになり、ネットワークを、重複したコンフィギュレーション（IP アドレスおよびブリッジ ID の重複を含む）を伴う*デュアルアクティブの状態*にする可能性があります。ネットワークがダウンする場合もあります。

デュアルアクティブの状態を防止するために、コア スイッチは PAgP プロトコル データ ユニット（PDU）を RSL を介してリモート スイッチに送信します。PAgP PDU はアクティブ スイッチを識別し、リモート スイッチは、コア スイッチが同期化するように PDU をコア スイッチに転送します。ア

クティブ スイッチに障害が発生した場合、またはアクティブ スイッチがリセットされた場合は、スタンバイ スイッチがアクティブスイッチの役割を引き継ぎます。VSL がダウンした場合は、1 つのコア スイッチが他のコア スイッチのステータスを認識して状態を変更しません。

PAgP と他の機能との相互作用

ダイナミック トランキング プロトコル（DTP）および Cisco Discovery Protocol（CDP）は、EtherChannel の物理ポートを使用してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP プロトコル データ ユニット（PDU）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを渡します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

LACP

LACP は IEEE 802.3ad で定義されており、Cisco スイッチが IEEE 802.3ad プロトコルに適合したスイッチ間のイーサネット チャネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の倫理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、LACP は単一スイッチ ポートとして、スパニングツリーにそのグループを追加します。

LACP モード

表 40-2 に、**channel-group** インターフェイス コンフィギュレーション コマンドでユーザが設定できる EtherChannel LACP モードを示します。

表 40-2　EtherChannel LACP モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードでは、どちらの場合も、ポートは相手ポートとのネゴシエーションにより、ポート速度、レイヤ 2 EtherChannel の場合はトランキング ステートおよび VLAN 番号などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

LACP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートとともに EtherChannel を形成できます。
- どのポートも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートとは EtherChannel を形成できません。

LACP ホット スタンバイ ポート

イネーブルの場合、LACP はチャネル内の LACP 互換ポート数を最大に設定しようとします（最大 16 ポート）。同時にアクティブになれる LACP リンクは 8 つだけです。リンクが追加されるとソフトウェアによってホット スタンバイモードになります。アクティブ リンクの 1 つが非アクティブになると、ホット スタンバイ モードのリンクが代わりにアクティブになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホット スタンバイ ポートを決定します。ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID（スイッチの MAC アドレス）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイ モードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の（2 つの）手順を使用します。はじめに、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホット スタンバイ ポートを決定します。他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。

デフォルトでは、すべてのポートは同じポート プライオリティです。ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さい値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。ホット スタンバイ ポートは、番号が小さい方が先にチャネルでアクティブになります。**show etherchannel summary** 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが *H* になっています）。

LACP がすべての互換ポートを集約できない場合（たとえば、ハードウェアの制約が大きいリモート システム）、EtherChannel 中でアクティブにならないポートはすべてホット スタンバイ ステートになり、チャネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを渡します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。**on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。**on** モードでは、リンクの両端のスイッチが **on** モードに設定されている場合のみ EtherChannel を使用できます。

同じチャネル グループの **on** モードで設定されたポートは、速度やデュプレックスのようなポート特性に互換性を持たせる必要があります。**on** モードで設定されていたとしても、互換性のないポートは suspended ステートになります。

注意　**on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリー ループが発生することがあります。

ロード バランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に縮小することによって、チャネル内のリンク間でトラフィックのロード バランシングを行います。EtherChannel のロード バランシングには、MAC アドレスまたは IP アドレス、送信元アドレスや宛先アドレスのどちらか一方、またはその両方のアドレスを使用できます。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。ロード バランシングおよび転送方式を設定するには、**port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャネル ポートを使用しますが、送信元ホストが同じパケットは同じチャネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットに指定されている宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のスイッチに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

送信元 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、IP アドレスが異なるパケットはそれぞれ異なるチャネル ポートを使用しますが、IP アドレスが同じパケットは同じチャネル ポートを使用します。

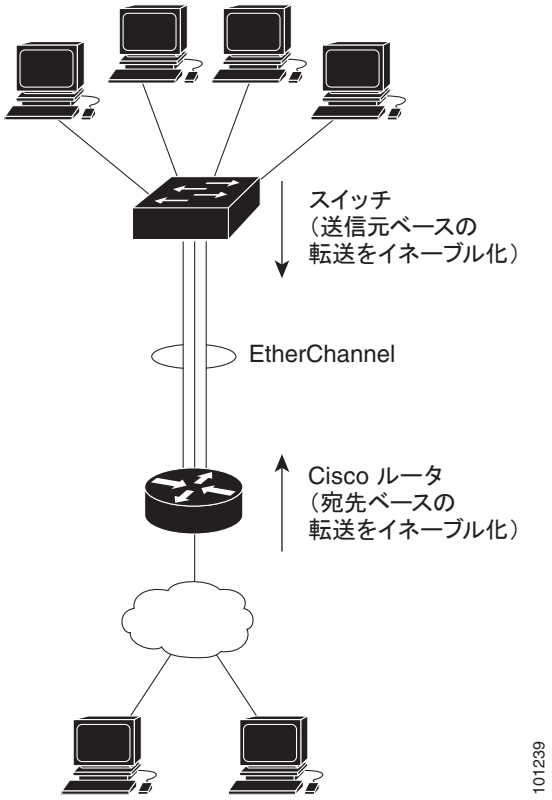
宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、異なるチャネル ポートに送信できます。ただし、異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常に同じチャネル ポートで送信されます。

送信元/宛先 IP アドレスベース転送の場合、パケットは EtherChannel に送信されて、着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたものです。特定のスイッチに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるかが不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

ロード バランシング方式ごとに利点が異なります。ロード バランシング方式は、ネットワーク内のスイッチの位置、および負荷分散が必要なトラフィックの種類に基づいて選択する必要があります。図 40-3 では、4 つのワークステーションからデータを集約しているスイッチからの EtherChannel がルータと通信しています。ルータは単一 MAC アドレス デバイスであるため、スイッチ EtherChannel で送信元ベース転送を行うことにより、スイッチが、ルータで使用可能なすべての帯域幅を使用することが、保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。

設定で一番種類が多くなるオプションを使用してください。たとえば、チャネル上のトラフィックが単一 MAC アドレスのみを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたは IP アドレスを使用した方が、ロード バランシングの効率がよくなる場合があります。

図 40-3　負荷の分散および転送方式



EtherChannel のデフォルト設定

表 40-3　EtherChannel のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポートチャネル論理インターフェイス	未定義
PAgP モード	デフォルトなし。
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし。
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システム プライオリティおよびスイッチ MAC アドレス
ロード バランシング	着信パケットの送信元 MAC アドレスに基づいてスイッチ上で負荷を分散

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問題を回避するために、次の注意事項に従ってください。

- 6 を超える数の EtherChannel をスイッチで設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- LACP EtherChannel は、同じタイプのイーサネット ポートを最大 16 まで使用して設定します。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。**shutdown** インターフェイス コンフィギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの 1 つに転送されます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
  - 許可 VLAN リスト
  - 各 VLAN のスパニングツリー パス コスト
  - 各 VLAN のスパニングツリー ポート プライオリティ
  - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。
- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP が稼働している複数の EtherChannel グループは、同じスイッチ上で共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。
- EtherChannel の一部としてスイッチド ポート アナライザ（SPAN）宛先ポートを設定しないでください。
- EtherChannel の一部としてセキュア ポートを設定したり、セキュア ポートの一部として EtherChannel を設定したりしないでください。
- プライベート VLAN ポートを EtherChannel の一部として設定しないでください。
- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がスイッチ インターフェイス上に設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1x をスイッチ上でグローバルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除してください。
- レイヤ 2 EtherChannel の場合
  - EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。

- トランク ポートから EtherChannel を設定する場合は、すべてのトランクでトランキング モード（ISL（スイッチ間リンク）または IEEE 802.1Q）が同じであることを確認してください。EtherChannel ポートのトランクのモードが一致していないと、予想外の結果になる可能性があります。
- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニングツリー パス コストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。異なるスパニングツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

EtherChannel の設定方法

（注）　EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

レイヤ 2 EtherChannel の設定

2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネル グループにポートを割り当てます。このコマンドにより、ポートチャネル論理インターフェイスが自動的に作成されます。

この必須の作業では、レイヤ 2 EtherChannel にレイヤ 2 イーサネット ポートを設定する方法について説明します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。
ステップ 3	**switchport mode** {**access** | **trunk**} **switchport access vlan** *vlan-id*	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。指定できる範囲は 1 ～ 4096 です。

	コマンド	目的
ステップ 4	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 *channel-group-number* の範囲は 1 ～ 6 です。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP デバイスが検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 • **desirable**：PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **on**：PAgP または LACP を使用せずにポートが強制的にチャネル化されます。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）PAgP 対応のデバイスに接続されたスイッチのポートが **auto** または **desirable** モードの場合に、非サイレント動作を行うようにこのポートを設定します。**non-silent** を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP デバイスが検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**：ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 スイッチおよびデバイスのモードの互換性に関する情報については、「PAgP モード」（P.40-4）および「LACP モード」（P.40-6）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。

EtherChannel ロード バランシングの設定

このタスクはオプションです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}	EtherChannel のロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **src-dst-ip**：送信元および宛先ホスト IP アドレスを指定します。 • **src-dst-mac**：送信元および宛先ホストの MAC アドレスを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

PAgP 学習方式およびプライオリティの設定

このタスクはオプションです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**pagp learn-method** physical-port	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port learning** が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、パケットが送信元に送信されます。集約ポート ラーニングを使用している場合、どの物理ポートにパケットが届くかは重要ではありません。 ラーナーである別のスイッチに接続するには、**physical-port** を選択します。**port-channel load-balance** グローバル コンフィギュレーション コマンドは、必ず **src-mac** に設定してください（「EtherChannel ロード バランシングの設定」（P.40-14）を参照）。 学習方式はリンクの両端で同じ方式に設定する必要があります。

	コマンド	目的
ステップ 4	**pagp port-priority** *priority*	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* に指定できる範囲は 0 ～ 255 です。デフォルトは 128 です。プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ 5	**end**	特権 EXEC モードに戻ります。

LACP ホット スタンバイ ポートの設定

このタスクはオプションです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lacp system-priority** *priority*	LACP システム プライオリティを設定します。 *priority* に指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。 値が小さいほど、システムプライオリティは高くなります。
ステップ 3	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lacp port-priority** ***priority***	LACP ポート プライオリティを設定します。 *priority* に指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ 5	**end**	特権 EXEC モードに戻ります。

EtherChannels のモニタリングおよびメンテナンス

コマンド	目的
show etherchannel [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。ロード バランシング方式またはフレーム配布方式、ポート、ポート チャネル、プロトコルの情報も表示されます。
show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 PAgP 設定、ネイバー情報などの PAgP 情報が表示されます。
show pagp [*channel-group-number*] **dual-active**	デュアルアクティブ検出ステータスが表示されます。
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報が表示されます。

EtherChannel の設定例

EtherChannel の設定：例

次に、EtherChannel を設定し、2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが **desirable** であるチャネル 5 に割り当てる例を示します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

次に、EtherChannel を設定し、2 つのポートを VLAN 10 のスタティック アクセス ポートとして、LACP モードが **active** であるチャネル 5 に割り当てる例を示します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 41

スタティック IP ユニキャスト ルーティングの設定

この章では、スイッチに IP Version 4（IPv4）スタティック IP ユニキャスト ルーティングを設定する方法について説明します。スタティック ルーティングは、スイッチ仮想インターフェイス（SVI）でのみサポートされており、物理インターフェイスではサポートされていません。スイッチでは、ルーティング プロトコルはサポートされていません。

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

スタティック IP ユニキャスト ルーティングの制約事項

- SDM テンプレートがスタティック ルーティングをサポートするように変更されていない場合、デフォルトではスタティック IP ルーティングはスイッチ上でディセーブルです。
- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

スタティック IP ユニキャスト ルーティングの設定に関する情報

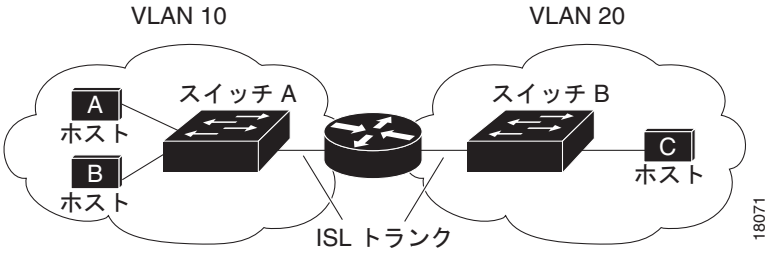
（注） スイッチにルーティング パラメータを設定する場合、使用できるユニキャスト ルート数が最大となるようにシステム リソースを割り当てるには、**sdm prefer lanbase-routing** グローバル コンフィギュレーション コマンドを使用し、ルーティング テンプレートにスイッチング データベース管理（SDM）機能を設定します。SDM テンプレートの詳細については、第 11 章「SDM テンプレートの設定」、またはこのリリースのコマンド リファレンスの **sdm prefer** コマンドを参照してください。

IP ルーティング

一部のネットワーク環境で、VLAN（仮想 LAN）は各ネットワークまたはサブネットワークに関連付けられています。IP ネットワークで、各サブネットワークは 1 つの VLAN に対応しています。VLAN を設定すると、ブロードキャスト ドメインのサイズを制御し、ローカル トラフィックをローカル内にとどめることができます。ただし、異なる VLAN 内のネットワーク デバイスが相互に通信するには、VLAN 間でトラフィックをルーティング（VLAN 間ルーティング）するレイヤ 3 デバイスが必要です。VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

図 41-1 に基本的なルーティング トポロジを示します。スイッチ A は VLAN 10 内、スイッチ B は VLAN 20 内にあります。ルータには各 VLAN のインターフェイスが備わっています。

図 41-1　　ルーティング トポロジの例



VLAN 10 内のホスト A が VLAN 10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。スイッチ A はパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでトラフィックを受信します。ルータはルーティング テーブルを使用して正しい発信インターフェイスを判別し、VLAN 20 インターフェイスを経由してパケットをスイッチ B に送信します。スイッチ B はパケットを受信し、ホスト C に転送します。

スイッチ A と B でスタティック ルーティングをイネーブルにすると、パケットをルーティングするためのルータ デバイスは必要なくなります。

ルーティング タイプ

ルータおよびレイヤ 3 スイッチは、次の方法でパケットをルーティングできます。

- 宛先がルータにとって不明であるトラフィックをデフォルトの出口または宛先に送信するには、デフォルト ルーティングを使用します。
- パケットが事前に設定されたポートから単一のパスを通り、ネットワークの内部または外部に転送されるようにするには、スタティック ルートを使用します。
- ルーティング プロトコルによるルートの動的な計算。

スイッチは、スタティック ルートとデフォルト ルートをサポートします。ルーティング プロトコルはサポートされません。

スタティック IP ユニキャスト ルーティングの設定方法

ルーティングを設定する手順

この手順では、特定のインターフェイスをスイッチ仮想インターフェイス（SVI）にする必要があります。これは、**interface vlan** *vlan_id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスであり、デフォルトではレイヤ 3 インターフェイスです。ルーティングが発生するすべてのレイヤ 3 インターフェイスに、IP アドレスを割り当てる必要があります。「IP アドレスの SVI への割り当て」（P.41-3）を参照してください。

（注）　スイッチでは、16 のスタティック ルート（ユーザ設定のルートとデフォルト ルートを含む）と、管理インターフェイスの直接接続されたルートとデフォルト ルートがサポートされています。スイッチには、各 SVI に割り当てられた IP アドレスを指定できます。ルーティングをイネーブルにする前に、**sdm prefer lanbase-routing** グローバル コンフィギュレーション コマンドを入力して、スイッチをリロードします。

ルーティングを設定する手順は次のとおりです。

- VLAN インターフェイスをサポートするために、スイッチで VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てます。詳細については、第 17 章「VLAN の設定」を参照してください。
- レイヤ 3 インターフェイス（SVI）および物理ルーテッド ポート（スイッチポートなし）を設定します。
- レイヤ 3 インターフェイスに IP アドレスを割り当てます。
- スタティック ルートを設定します。

IP ユニキャスト ルーティングのイネーブル化

デフォルトで、スイッチはレイヤ 2 スイッチング モード、IP ルーティングはディセーブルとなっています。スイッチのレイヤ 3 機能を使用するには、IP ルーティングをイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

IP アドレスの SVI への割り当て

IP ルーティングを設定するには、IP アドレスをレイヤ 3 ネットワーク インターフェイスに割り当てる必要があります。これにより、IP を使用するインターフェイスでホストとの通信が可能になります。IP ルーティングはデフォルトでディセーブルであり、IP アドレスは SVI に割り当てられていません。

IP アドレスは、IP パケットの宛先を特定します。一部の IP アドレスは特殊な目的のために予約されていて、ホスト、サブネット、またはネットワーク アドレスには使用できません。RFC 1166『Internet Numbers』には、これらの IP アドレスに関する公式の説明が記載されています。

インターフェイスには、1 つのプライマリ IP アドレスを設定できます。サブネット マスクは、IP アドレスのネットワーク番号を表すビットを特定します。

この作業では、SVI に IP アドレスおよびネットワーク マスクを割り当てる例を示します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan_id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 VLAN を指定します。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。ルータが特定の宛先へのルートを構築できない場合、スタティック ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

スタティック ルートを削除するには、**no ip route** *prefix mask* {*address* | *interface*} グローバル コンフィギュレーション コマンドを使用します。ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。

インターフェイスがダウンすると、ダウンしたインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。転送ルータのアドレスとして指定されたアドレスへ向かう有効なネクスト ホップがスタティック ルート内に見つからない場合は、IP ルーティング テーブルからそのスタティック ルートも削除されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip route** *prefix mask* {*address* | *interface*} [*distance*]	スタティック ルートを確立します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

IP ネットワークのモニタリングおよびメンテナンス

コマンド	説明
show interfaces [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスの管理ステータスおよび動作ステータスを表示します。

IP ユニキャスト ルーティング の設定に関する追加情報

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS IP アドレス コマンド	『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 15.0*』
Cisco IP ルーティング設定	『*Cisco IOS IP Routing Configuration Guides, Release 15.0*』
SDM テンプレート設定	第 11 章「SDM テンプレートの設定」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 42

IPv6 ホスト機能の設定

（注） IPv6 ホスト機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

この章では、スイッチに IPv6 ホスト機能を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IPv6 ホスト機能の設定の前提条件

- （IPv4 と IPv6 の両方をサポートする）デュアル スタック環境をイネーブルにするには、デュアル IPv4 および IPv6 スイッチ データベース管理（SDM）テンプレートを使用するように、スイッチを設定する必要があります。「デュアル IPv4/IPv6 プロトコル スタック」（P.42-5）を参照してください。

IPv6 ホスト機能の設定に関する情報

IPv6

IPv4 ユーザは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service（QoS）、およびグローバルに一意なアドレスのようなサービスを利用できます。IPv6 アドレス スペースによって、プライベート アドレスの必要性が低下し、ネットワーク エッジの境界ルータでネットワーク アドレス変換（NAT）処理を行う必要性も低下します。

シスコの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 次の URL にある『*Cisco IOS IPv6 Configuration Library*』を参照してください。
  http://www.cisco.com/en/US//docs/ios-xml/ios/ipv6/configuration/15-1mt/ipv6-15-1mt-book.html

ここでは、スイッチへの IPv6 の実装について説明します。内容は次のとおりです。

- 「IPv6 形式のアドレス」（P.42-2）
- 「サポート対象の IPv6 ホスト機能」（P.42-2）
- 「IPv6 ホスティングの設定方法」（P.42-7）

IPv6 形式のアドレス

スイッチがサポートするのは、IPv6 ユニキャスト アドレスだけです。スイッチはサイトローカルなユニキャスト アドレス、エニキャスト アドレス、またはマルチキャスト アドレスをサポートしません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド（n:n:n:n:n:n:n:n. の形式）で表されます。次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回のみです。

2031:0:130F::09C0:080F:130B

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Implementing Addressing and Basic Connectivity」の章にある以下のセクションの内容がスイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレスの出力表示
- 簡易 IPv6 パケット ヘッダー

サポート対象の IPv6 ホスト機能

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

- 「128 ビット幅のユニキャスト アドレス」（P.42-3）
- 「IPv6 の DNS」（P.42-3）
- 「ICMPv6」（P.42-3）
- 「ネイバー探索」（P.42-4）
- 「DRP」（P.42-4）
- 「IPv6 のステートレス自動設定および重複アドレス検出」（P.42-4）
- 「IPv6 アプリケーション」（P.42-4）

- 「デュアル IPv4/IPv6 プロトコル スタック」（P.42-5）
- 「IPv6 上の SNMP および Syslog」（P.42-6）
- 「IPv6 による HTTP」（P.42-6）

スイッチでは、拡張アドレス機能、ヘッダー フォーマットの単純化、拡張子およびオプションのサポートの改善、および拡張ヘッダーのハードウェア解析などがサポートされています。また、ホップ単位の拡張ヘッダー パケットもサポートし、これらをソフトウェアでルーティングまたはブリッジングします。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャスト アドレスをサポートします。サイトに対してローカルなユニキャスト アドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、グローバル ルーティング テーブル内のルーティング テーブル エントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

  これらのアドレスはグローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001（2000::/3）で開始するアドレス範囲が使用されます。プレフィックスが 2000::/3（001）～ E000::/3（111）のアドレスには、Extended Unique Identifier（EUI）64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンクに対してローカルなユニキャスト アドレスをすべてのインターフェイスに自動的に設定するには、修飾 EUI フォーマット内で、リンクに対してローカルなプレフィックス FE80::/10（1111 1110 10）およびインターフェイス ID を使用します。ネイバー探索プロトコル（NDP）およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカル リンク上のノードは、リンクに対してローカルなアドレスを使用します。通信する場合に、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある、「IPv6 Unicast Addresses」を参照してください。

IPv6 の DNS

IPv6 は、ドメイン ネーム システム（DNS）のレコード タイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

ICMPv6

IPv6 のインターネット制御メッセージ プロトコル（ICMP）は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、ネイバー探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼働するプロトコル、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリをサポートします。IPv6 ネイバー探索プロセスは ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためにネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6 パケットのネクスト ホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。このドロップにより、CPU に余分な負荷がかからないようになります。

DRP

スイッチは、ルータのアドバタイズメント メッセージの拡張機能である、IPv6 Default Router Prefernce（DRP）をサポートします。DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。NDP は、到達可能または到達可能の可能性があるルータとして、常に同じルータを選択するか、またはルータ リストから繰り返し使用できます。DRP を使用することにより、IPv6 ホストが、両方ともが到達可能または到達可能の可能性がある 2 台のルータを差別化するように設定できます。

IPv6 の DRP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- ping、traceroute、Telnet、TFTP、および FTP
- IPv6 トランスポートによるセキュア シェル（SSH）
- IPv6 トランスポートによる HTTP サーバ アクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ

- IPv6 アドレスの Cisco Discovery Protocol（CDP）サポート

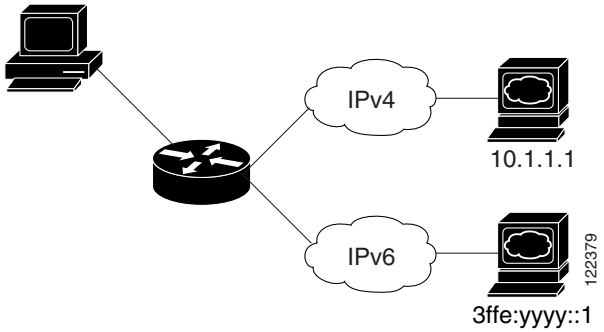
これらのアプリケーションの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Managing Cisco IOS Applications over IPv6」の章および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方に 3 値連想メモリ（TCAM）の使用を割り当てるには、デュアル IPv4/IPv6 テンプレートを使用する必要があります。

図 42-1 に、IP パケットおよび宛先アドレスに基づいて、同じインターフェイスを介して IPv4 および IPv6 トラフィックを転送するルータを示します。

図 42-1　インターフェイス上での IPv4/IPv6 のデュアル サポート



デュアル IPv4/IPv6 スイッチ データベース管理（SDM）テンプレートを使用して、（IPv4 と IPv6 の両方をサポートする）デュアル スタック環境をイネーブルにします。デュアル IPv4/IPv6 SDM テンプレートについての詳細は、第 11 章「SDM テンプレートの設定」を参照してください。

デュアル IPv4 および IPv6 テンプレートを使用すると、デュアル スタック環境でスイッチを使用できるようになります。

- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 を設定しようとすると、警告メッセージが表示されます。
- IPv4 専用環境で、スイッチは Ipv4 QoS および ACL をハードウェアで適用します。IPv6 パケットはサポートされません。
- デュアル IPv4/IPv6 環境で、スイッチは IPv4 QoS および ACL をハードウェアで適用します。
- IPv6 QoS および ACL はサポートされていません。
- デュアル スタック テンプレートを使用すると各リソースの TCAM 容量が少なくなるので、IPv6 を使用しない場合はデュアル スタック テンプレートを使用しないでください。

IPv4/IPv6 プロトコル スタックについての詳細は、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング デバイス間のルートを明示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 上の SNMP および Syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。IPv6 による Syslog は、このトランスポートのアドレス データ タイプをサポートします。

IPv6 による SNMP および Syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

IPv6 に関連するサポートでは、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザ データグラム プロトコル（UDP）SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、IPv6 に関連する SNMP については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6 による Syslog については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 による HTTP

HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。HTTP には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続が確立するためには、基本ネットワーク接続（**ping**）がクライアントとサーバ ホストとの間に存在する必要があります。

IPv6 のデフォルト設定

表 42-1　IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	これがデフォルトです。
IPv6 アドレス	未設定

IPv6 ホスティングの設定方法

IPv6 アドレス指定の設定および IPv6 ホストのイネーブル化

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで指定した *ipv6-address* 変数および *ipv6-prefix* 変数を入力する必要があります。*prefix-length* 変数（スラッシュ（/）で始まる）は、プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。インターフェイス上で IPv6 アドレスを設定すると、リンクに対してローカルなアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャスト アドレスの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスはネイバー探索プロセスで使用される）
- すべてのノードを含む、ルータリンクに対してローカルなマルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルなマルチキャスト グループ FF02::2

IPv6 の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer dual-ipv4-and-ipv6 default**	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**reload**	オペレーティング システムをリロードします。
ステップ 5	**configure terminal**	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンド	目的
ステップ 7	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **ipv6 address** *ipv6-address* **link-local** または **ipv6 enable**	• IPv6 アドレスの下位 64 ビットの拡張固有識別子（EUI）を使用して、グローバル IPv6 アドレスを指定します。 • ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理がイネーブルになります。 • インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクに対してローカルなアドレスでなく、インターフェイス上の特定の、リンクに対してローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。 • インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**end**	特権 EXEC モードに戻ります。

DRP の設定

ルータ アドバタイズメント（RA）メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定される DRP とともに送信されます。DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

リンク上の 2 つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	**ipv6 nd router-preference** {**high** | **medium** | **low**}	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

IPv6 ICMP レート制限の設定

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ（バケットに格納される最大トークン数）は 10 です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 icmp error-interval** *interval* [*bucketsize*]	IPv6 ICMP エラー メッセージの間隔とバケット サイズを設定します。 • *interval :* バケットに追加されるトークンの間隔（ミリ秒）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize* :（任意）バケットに格納される最大トークン数。指定できる範囲は 1 ～ 200 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

IPv6 ホスト情報のモニタリングおよびメンテナンス

コマンド	目的
show ipv6 interface *interface-id*	IPv6 インターフェイスのステータスと設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチ上の IPv6 ルーティング プロトコルを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。
show ip http server history	アクセスした IP アドレス、接続が終了したときの時間を含む、最近 20 回の HTTP サーバへの接続を表示します。
show ip http server connection	アクセスしているローカルおよびリモート IP アドレスを含む、HTTP サーバへの現在の接続を表示します。
show ip http client connection	HTTP サーバへの HTTP クライアント接続の設定値を表示します。
show ip http client history	サーバに対して HTTP クライアントが行った最後の 20 回の要求のリストを表示します。

IPv6 ホスト機能の設定例

IPv6 のイネーブル化：例

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。**show ipv6 interface** EXEC コマンドの出力は、インターフェイスのリンクに対してローカルなプレフィックス FE80::/64 にインターフェイス ID（20B:46FF:FE2F:D940）を付加する方法を示しています。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# interface gigabitethernetfastethernet1/0/11
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernetfastethernet1/0/11
GigabitEthernetFastEthernet1/0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

DRP の設定：例

次に、インターフェイス上のルータに*高い* DRP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv6 ICMP エラー メッセージ間隔の設定

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Switch(config)# ipv6 icmp error-interval 50 20
```

show コマンド出力の表示：例

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

次に、**show ipv6 protocols** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 protocols
IPv6 Routing Protocol is “connected”
IPv6 Routing Protocol is “static”
IPv6 Routing Protocol is “rip fer”
  Interfaces:
    Vlan6
    FastEthernet0/4
    FastEthernet0/11
    FastEthernet0/12
    GigabitEthernet2/0/4
    GigabitEthernet2/0/
    GigabitEthernet1/0/12
Redistribution:
    None
```

次に、**show ipv6 neighbor** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
3FFE:C000:0:7::777                          - 0007.0007.0007  REACH Vl7
3FFE:C101:113:1::33                         - 0000.0000.0033  REACH Fa1/0/13
```

次に、**show ipv6 route** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 route
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
L   FF00::/8 [0/0]
     via Null0, receive
```

次に、**show ipv6 traffic** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
```

```
          0 unknown protocol, 0 not a router
          0 fragments, 0 total reassembled
          0 reassembly timeouts, 0 reassembly failures
    Sent:  36861 generated, 0 forwarded
          0 fragmented into 0 fragments, 0 failed
          0 encapsulation failed, 0 no route, 0 too big
          0 RPF drops, 0 RPF suppressed drops
    Mcast: 1 received, 36861 sent

ICMP statistics:
    Rcvd: 1 input, 0 checksum errors, 0 too short
          0 unknown info type, 0 unknown error type
          unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
          parameter: 0 error, 0 header, 0 option
          0 hopcount expired, 0 reassembly timeout,0 too big
          0 echo request, 0 echo reply
          0 group query, 0 group report, 0 group reduce
          1 router solicit, 0 router advert, 0 redirects
          0 neighbor solicit, 0 neighbor advert
    Sent: 10112 output, 0 rate-limited
          unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
          parameter: 0 error, 0 header, 0 option
          0 hopcount expired, 0 reassembly timeout,0 too big
          0 echo request, 0 echo reply
          0 group query, 0 group report, 0 group reduce
          0 router solicit, 9944 router advert, 0 redirects
          84 neighbor solicit, 84 neighbor advert

UDP statistics:
    Rcvd: 0 input, 0 checksum errors, 0 length errors
          0 no port, 0 dropped
    Sent: 26749 output

TCP statistics:
    Rcvd: 0 input, 0 checksum errors
    Sent: 0 output, 0 retransmitted
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS スタティック IPv6 ルーティング	Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章
IPv6 用 DRP	Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 43

リンク ステート トラッキングの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

リンク ステート トラッキングの設定の制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。
- インターフェイスは、複数のリンクステート グループのメンバにはなれません。
- スイッチ 1 つにつき、設定できるリンクステート グループは 2 つだけです。

リンク ステート トラッキングの設定に関する情報

リンクステート トラッキング

リンクステート トラッキングは、トランク フェールオーバーとも呼ばれ、複数のインターフェイスのリンクステートをバインドする機能です。たとえば、リンクステート トラッキングをサーバ NIC アダプタ チーミング機能とともに使用すると、ネットワークで冗長性が実現されます。サーバ ネットワーク アダプタが、チーミングと呼ばれるプライマリまたはセカンダリ関係で設定され、プライマリ インターフェイスでリンクが消失した場合、接続はセカンダリ インターフェイスに透過的に変更されます。

（注） ポートの集合（EtherChannel）、アクセス モードまたはトランク モードの単一の物理ポート、またはルーテッド ポートをインターフェイスに指定できます。

図 43-1（P.43-4）は、リンクステート トラッキングを使用して設定されたネットワークを示しています。リンクステート トラッキングをイネーブルにするには、*link-state group* を作成し、リンクステート グループに割り当てるインターフェイスを指定します。リンクステート グループでは、これらのインターフェイスはまとめてバンドルされます。*ダウンストリーム インターフェイス*は、*アップストリーム インターフェイス*にバインドされます。サーバに接続されたインターフェイスはダウンストリーム インターフェイスと呼ばれ、ディストリビューション スイッチおよびネットワーク装置に接続されたインターフェイスはアップストリーム インターフェイスと呼ばれます。

図 43-1 の設定により、ネットワーク トラフィック フローのバランスが、次のように保たれます。

- スイッチと他のネットワーク デバイスへのリンクの場合
  - サーバ 1 とサーバ 2 は、プライマリ リンクにスイッチ A を使用し、セカンダリ リンクにスイッチ B を使用しています。
  - サーバ 3 とサーバ 4 は、プライマリ リンクにスイッチ B を使用し、セカンダリ リンクにスイッチ A を使用しています。
- スイッチ A のリンク ステート グループ 1
  - スイッチ A はリンクステート グループ 1 を介して、プライマリ リンクをサーバ 1 およびサーバ 2 に使用します。ポート 1 はサーバ 1 に、ポート 2 はサーバ 2 にそれぞれ接続されます。ポート 1 およびポート 2 はリンクステート グループ 1 でダウンストリーム インターフェイスとして使用します。
  - ポート 5 およびポート 6 は、リンクステート グループ 1 を介して分散スイッチ 1 に接続されます。ポート 5 およびポート 6 は、リンクステート グループ 1 でアップストリーム インターフェイスとして使用します。
- スイッチ A のリンク ステート グループ 2
  - スイッチ A はリンクステートグループ 2 を介して、セカンダリ リンクをサーバ 3 およびサーバ 4 に使用します。ポート 3 はサーバ 3 に、ポート 4 はサーバ 4 にそれぞれ接続されます。ポート 3 およびポート 4 はリンクステート グループ 2 でダウンストリーム インターフェイスとして使用します。
  - ポート 7 およびポート 8 は、リンクステート グループ 2 を介して分散スイッチ 2 に接続されます。ポート 7 およびポート 8 は、リンクステート グループ 2 でアップストリーム インターフェイスとして使用します。
- スイッチ B のリンク ステート グループ 2
  - スイッチ B はリンクステートグループ 2 を介して、プライマリ リンクをサーバ 3 およびサーバ 4 に使用します。ポート 3 はサーバ 3 に、ポート 4 はサーバ 4 にそれぞれ接続されます。ポート 3 およびポート 4 はリンクステート グループ 2 でダウンストリーム インターフェイスとして使用します。
  - ポート 5 およびポート 6 は、リンクステート グループ 2 を介して分散スイッチ 2 に接続されます。ポート 5 およびポート 6 は、リンクステート グループ 2 でアップストリーム インターフェイスとして使用します。
- スイッチ B のリンク ステート グループ 1
  - スイッチ B はリンクステート グループ 1 を介して、セカンダリ リンクをサーバ 1 およびサーバ 2 に使用します。ポート 1 はサーバ 1 に、ポート 2 はサーバ 2 にそれぞれ接続されます。ポート 1 およびポート 2 はリンクステート グループ 1 でダウンストリーム インターフェイスとして使用します。
  - ポート 7 およびポート 8 は、リンクステート グループ 1 を介して分散スイッチ 1 に接続されます。ポート 7 およびポート 8 は、リンクステート グループ 1 でアップストリーム インターフェイスとして使用します。

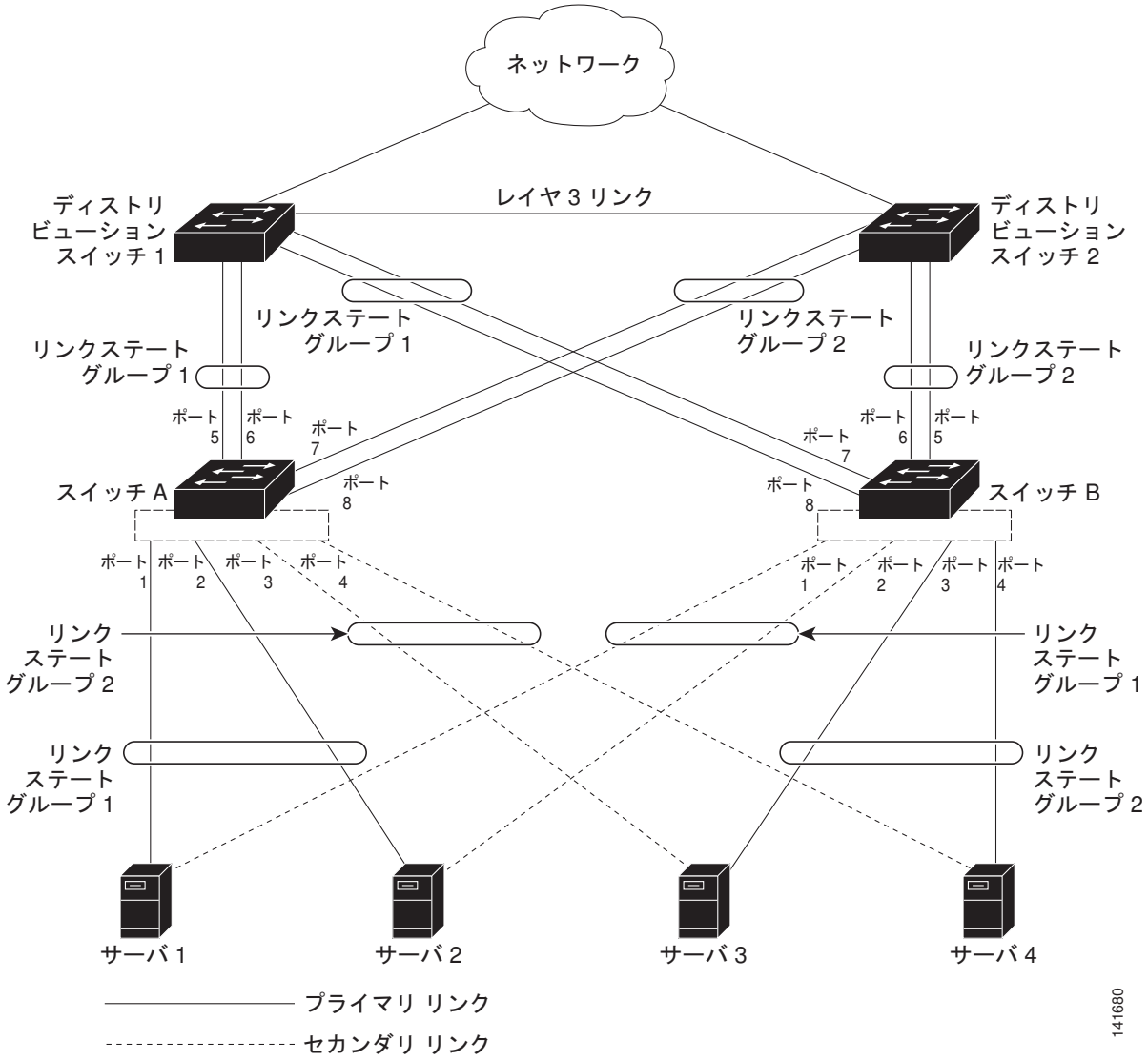
分散スイッチやルータに障害が発生したり、ケーブルが切断されたり、リンクが失われたために、リンクステート グループ内でアップストリーム ポートが利用不能や接続不能になる場合があります。これらは、リンクステート トラッキングがイネーブルの際の、ダウンストリーム インターフェイスとアップストリーム インターフェイス間の相互作用です。

- アップストリーム インターフェイスがリンクアップ ステートの場合、ダウンストリーム インターフェイスをリンクアップ ステートに変更したり、リンクアップ ステートのままにしたりすることができます。
- すべてのアップストリーム インターフェイスが利用不能になった場合、リンクステート トラッキングが自動的にダウンストリーム インターフェイスを errdisable ステートにします。サーバ間の接続は、自動的にプライマリ サーバ インターフェイスからセカンダリ サーバ インターフェイスに変更されます。

  スイッチ A のリンクステート グループ 1 からリンクステート グループ 2 への接続の変更例については、図 43-1（P.43-4）を参照してください。ポート 6 のアップストリーム リンクが切断されても、ダウンストリーム ポート 1 および 2 のリンク ステートは変わりません。ただし、アップストリーム ポート 5 のリンクも切断された場合、ダウンストリーム ポートのリンク ステートがリンクダウン ステートに変更されます。サーバ 1 およびサーバ 2 の接続については、リンクステート グループ 1 からリンクステート グループ 2 へ変更します。ダウンストリーム ポート 3 およびダウンストリーム ポート 4 は、リンクグループ 2 であるためステートを変更しません。
- リンクステート グループが設定されている場合、リンクステート トラッキングはディセーブルで、アップストリーム インターフェイスが切断され、ダウンストリーム インターフェイスのリンク ステートは変更されないままになります。サーバはこのアップストリーム接続が切断されたことを認識せず、セカンダリ インターフェイスにフェールオーバーしません。

障害のあるダウンストリーム ポートをリンクステート グループから削除することで、ダウンストリーム インターフェイスのリンクダウン状態から復旧できます。複数のダウンストリーム インターフェイスを復旧させるには、リンクステート グループをディセーブルにします。

図 43-1　一般的なリンクステート トラッキングの設定



デフォルトのリンクステート トラッキングの設定

リンクステート グループは定義されておらず、リンクステート トラッキングはどのグループでもイネーブルではありません。

リンク ステート トラッキングの設定方法

リンク ステート トラッキングの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**link state track** *number*	リンクステート グループを作成して、リンクステート トラッキングをイネーブルにします。グループ番号は 1 ～ 2 に設定できます。デフォルトは 1 です。
ステップ 3	**interface** *interface-id*	設定する物理インターフェイスまたはインターフェイスの範囲を指定して、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、アクセス モードまたはトランク モード（IEEE 802.1q）のスイッチ ポート、ルーテッド ポート、EtherChannel インターフェイス（スタティックまたは LACP）にバンドルされた、トランク モードの複数ポートが含まれます。
ステップ 4	**link state group** [*number*] {**upstream** | **downstream**}	リンクステート グループを指定し、グループ内のインターフェイスを **upstream** または **downstream** インターフェイスに設定します。グループ番号は 1 ～ 2 に設定できます。デフォルトは 1 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。

リンク ステート トラッキングのモニタリングおよびメンテナンス

コマンド	目的
show link state group	リンクステート グループ情報を表示します。

リンク ステート トラッキングの設定例

リンク ステート情報の表示：例

show link state group コマンドを使用してリンクステート グループの情報を表示します。キーワードを指定せずにこのコマンドを入力すると、すべてのリンクステート グループの情報が表示されます。特定のグループの情報を表示するには、グループ番号を入力します。グループの詳細情報を表示するには、detail キーワードを入力します。

次の例では、**show link state group 1** コマンドの出力を示します。

```
Switch> show link state group 1
```

```
Link State Group: 1      Status: Enabled, Down
```

次の例では、**show link state group detail** コマンドの出力を示します。

```
Switch> show link state group detail

(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Fa1/7(Dwn) Fa1/8(Dwn)
Downstream Interfaces : Fa1/3(Dis) Fa1/4(Dis) Fa1/5(Dis) Fa1/6(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Fa1/6(Dwn) Fa1/7(Dwn) Fa1/8(Dwn)
Downstream Interfaces : Fa1/2(Dis) Fa1/3(Dis) Fa1/4(Dis) Fa1/5(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

リンク ステート グループの作成：例

次に、リンク ステート グループを作成してインターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/2
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
EtherChannel コンフィギュレーション	*第 40 章「EtherChannel の設定」*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 44

IPv6 MLD スヌーピングの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IPv6 MLD スヌーピングの設定の前提条件

- IPv6 を使用するには、デュアル IPv4 および IPv6 スイッチング データベース管理（SDM）テンプレートがスイッチに設定されている必要があります。**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力して、テンプレートを選択します。

IPv6 MLD スヌーピングの設定に関する制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- スイッチ上で Multicast Listener Discovery（MLD）スヌーピングを使用して、スイッチド ネットワーク内のクライアントおよびルータに IP バージョン 6（IPv6）マルチキャスト データを効率的に配信することができます。

IPv6 MLD スヌーピングの設定に関する情報

IPv6 MLD スヌーピング

IP バージョン 4（IPv4）では、レイヤ 2 スイッチはインターネット グループ管理プロトコル（IGMP）スヌーピングを使用して、ダイナミックにレイヤ 2 インターフェイスを設定することにより、マルチキャスト トラフィックのフラッディングを抑制します。そのため、マルチキャスト トラフィックは IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングを使用すると、IPv6 マルチキャスト

データは VLAN（仮想 LAN）内のすべてのポートにフラッディングされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、直接接続されたリンク上のマルチキャスト リスナー（IPv6 マルチキャスト パケットを受信するノード）の存在、および隣接ノードの対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生しています。MLD バージョン 1（MLDv1）は IGMPv2 と、MLD バージョン 2（MLDv2）は IGMPv3 とそれぞれ同等です。MLD は ICMP バージョン 6（ICMPv6）のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング：MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 基本スヌーピング（MBSS）：MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。

（注）　スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 拡張スヌーピング（MESS）をサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できます。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト MAC アドレス テーブルはソフトウェアで構築され、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアおよびハードウェアで構築されます。その後、スイッチはハードウェアで IPv6 マルチキャストアドレスに基づくブリッジングを実行します。

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener Query：IGMPv2 クエリーと同等で、General Query または Mulicast-Address-Specific Query（MASQ）のいずれかになります。
- Multicast Listener Report：IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ：IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに応答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト MAC アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャストアドレス エージングを維持します。

（注）　IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4096）を使用している場合は、スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに応答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ（IGMP Leave メッセージと同等）を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチはメッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバーシップの削除を設定できます。1 つのアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合のみです。デフォルトの回数は 2 回です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ 2 インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。
- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。

- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスおよび IPv6 マルチキャスト MAC アドレスが VLAN の MLD データベースに入力されます。その後、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバ ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数の観点から制御できます。アドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、**ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドにより設定されます。デフォルトの回数は 2 回です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応答時間は、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドにより設定します。削除されたポートがマルチキャスト アドレスの最後のメンバである場合は、マルチキャスト アドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

TCN 処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知（TCN）送信請求をイネーブルにすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリーによりすべての IPv6 マルチキャスト トラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにのみマルチキャスト データの送信を開始します。この値は、**ipv6 mld snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルトでは、2 つのクエリーが送信されます。スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

MLD スヌーピングのデフォルト設定

表 44-1　MLD スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング（グローバル）	ディセーブル
MLD スヌーピング（VLAN 単位）	イネーブル VLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル
MLD スヌーピングの堅牢性変数	グローバル：2、VLAN 単位：0 **（注）** VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル：2、VLAN 単位：0 **（注）** VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー インターバル	グローバル：1000（1 秒）、VLAN：0 **（注）** VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	ディセーブル
TCN クエリー カウント	2.
MLD リスナー抑制	イネーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。

- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4096）を使用している場合は、スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチで保持可能なマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチで保持可能なアドレス エントリの最大数は 1000 です。

MLD スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルト ステート（イネーブル）の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

マルチキャスト ルータ ポート

MLD スヌーピングでは、MLD クエリーおよび PIMv6 クエリーを介してルータ ポートについて学習しますが、コマンドライン インターフェイス（CLI）を使用しても VLAN にマルチキャスト ルータ ポートを追加できます。マルチキャスト ルータ ポートを追加する（マルチキャスト ルータにスタティック接続を追加する）には、スイッチで **ipv6 mld snooping vlan mrouter** グローバル コンフィギュレーション コマンドを使用します。

MLD 即時脱退

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出するとただちに、マルチキャスト グループからポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにしてはなりません。

MLD スヌーピング クエリー

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

IPv6 MLD スヌーピングの設定方法

（注）　IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4096）を使用している場合は、スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

MLD スヌーピングのイネーブル化またはディセーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping**	スイッチで MLD スヌーピングをグローバルにイネーブルにします。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id*	（任意）VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。 VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**reload**	オペレーティング システムをリロードします。

スタティックなマルチキャスト グループの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **static** *ipv6_multicast_address* **interface** *interface-id*	マルチキャスト グループのメンバとしてレイヤ 2 ポートにマルチキャスト グループを静的に設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。 • *ipv6_multicast_address* は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。 • *interface-id* は、メンバ ポートです。物理インターフェイスまたはポート チャネル（1 ～ 48）に設定できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

マルチキャスト ルータ ポートの設定

（注）　マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id*	マルチキャスト ルータの VLAN ID を指定して、マルチキャスト ルータにインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

MLD 即時脱退のイネーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **immediate-leave**	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

MLD スヌーピング クエリーの設定

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping robustness-variable** *value*	（任意）スイッチが一般クエリーに応答しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ～ 3 です。デフォルトは 2 です。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value*	（任意）VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャスト アドレスがエージング アウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は 1 ～ 3 です。デフォルトは 0 です。0 に設定すると、使用される数はグローバルな堅牢性変数の値になります。
ステップ 4	**ipv6 mld snooping last-listener-query-count** *count*	（任意）MLD クライアントがエージング アウトされる前にスイッチが送信する MASQ 数を設定します。指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。クエリーは 1 秒後に送信されます。

	コマンド	目的
ステップ 5	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-count** *count*	（任意）VLAN 単位で last-listener クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ～ 7 です。デフォルトは 0 です。0 に設定すると、グローバルなカウント値が使用されます。クエリーは 1 秒後に送信されます。
ステップ 6	**ipv6 mld snooping last-listener-query-interval** *interval*	（任意）スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100 ～ 32,768 ミリ秒です。デフォルト値は 1000（1 秒）です。
ステップ 7	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-interval** *interval*	（任意）VLAN 単位で last-listener クエリー インターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ～ 32,768 ミリ秒です。デフォルトは 0 です。0 に設定すると、グローバルな最後のリスナー クエリー インターバルが使用されます。
ステップ 8	**ipv6 mld snooping tcn query solicit**	（任意）トポロジ変更通知（TCN）をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャスト データをマルチキャスト データの受信を要求するポートに対してのみ送信します。デフォルトでは、TCN はディセーブルに設定されています。
ステップ 9	**ipv6 mld snooping tcn flood query count** *count*	（任意）TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。

MLD リスナー メッセージ抑制のディセーブル化

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ipv6 mld snooping listener-message-suppression**	MLD メッセージ抑制をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

IPv6 MLD スヌーピングのモニタリングおよびメンテナンス

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの MLD スヌーピング情報を表示できます。MLD スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

コマンド	目的
show ipv6 mld snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。
show ipv6 mld snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4096 です。
show ipv6 mld snooping multicast-address [**vlan** *vlan-id*] [**count** | **dynamic** | **user**]	すべての IPv6 マルチキャスト アドレス情報あるいはスイッチまたは VLAN の特定の IPv6 マルチキャスト アドレス情報を表示します。 • **count** を入力して、スイッチまたは VLAN のグループ数を表示します。 • **dynamic** を入力して、スイッチまたは VLAN の MLD スヌーピング学習済みグループ情報を表示します。 • **user** を入力して、スイッチまたは VLAN の MLD スヌーピング ユーザ設定グループ情報を表示します。
show ipv6 mld snooping multicast-address vlan *vlan-id* [*ipv6-multicast-address*]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。
show ipv6 mld snooping multicast-address user または **show ipv6 mld snooping multicast-address vlan** *vlan-id* **user**	スタティック メンバ ポートおよび IPv6 アドレスを確認します。
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。
show ipv6 mld snooping	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。

IPv6 MLD スヌーピングの設定例

IPv6 マルチキャスト グループをスタティックに設定：例

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet1/1
Switch(config)# end
```

VLAN へのマルチキャスト ルータ ポートの追加：例

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet1/2
Switch(config)# exit
```

VLAN で MLD 即時脱退のイネーブル化：例

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit
```

MLD スヌーピングのグローバルな堅牢性の設定：例

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

MLD スヌーピングの最後のリスナー クエリー パラメータの設定：例

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
SDM テンプレート	第 11 章「SDM テンプレートの設定」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 45

Cisco IOS IP SLA 動作の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Cisco IOS IP SLA 動作の前提条件

- IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用して、お使いのソフトウェア イメージでサポートされている動作タイプを確認することを推奨します。

Cisco IOS IP SLA 動作設定の制約事項

- IP SLA 応答側には、LAN Base イメージを実行する Catalyst 2960 スイッチまたは IE2000 スイッチ、あるいは IP Base イメージを実行する Catalyst 3560 スイッチまたは 3750 スイッチのような Cisco IOS レイヤ 2 の応答側に設定可能なスイッチを使用できます。Responder は、IP SLA 機能を全面的にサポートする必要はありません。
- スイッチでは、ゲートキーパー登録遅延動作測定を使用する Voice over IP（VoIP）サービス レベルをサポートしません。IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェア イメージで動作タイプがサポートされていることを確認してください。

Cisco IOS IP SLA 動作設定に関する情報

この章では、Cisco IOS IP サービス レベル契約（SLA）を使用する方法について説明します。Cisco IP SLA は Cisco IOS ソフトウェアの一部であり、シスコのお客様は連続的で信頼性の高い確実な方法でトラフィックを生成するアクティブ トラフィック モニタリングを行って IP アプリケーションとサービスの IP サービス レベルを分析し、ネットワーク パフォーマンスを測定することができます。Cisco IOS SLA を使用すると、サービス プロバイダーのお客様はサービス レベル契約の検討と提供、企業の

お客様はサービス レベルの検証、外部委託しているサービス レベル契約の検証、およびネットワーク パフォーマンスを把握することができます。Cisco IOS IP SLA は、ネットワーク アセスメントを実行することで Quality of Service（QoS）の検証、新しいサービス導入の簡易化、ネットワーク トラブルシューティングの補助を可能にします。

Cisco IOS IP SLA

CiscoIOS IP SLA はネットワークにデータを送信し、複数のネットワーク間あるいは複数のネットワーク パス内のパフォーマンスを測定します。ネットワーク データおよび IP サービスをシミュレーションし、ネットワーク パフォーマンス情報をリアル タイムで収集します。Cisco IOS IP SLA は、Cisco IOS デバイス間のトラフィックまたは Cisco IOS デバイスからネットワーク アプリケーション サーバのようなリモート IP デバイスへのトラフィックを生成し、分析します。さまざまな Cisco IOS IP SLA 動作で評価を実行し、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用します。

Cisco IOS IP SLA 動作に応じてシスコ デバイスのネットワーク パフォーマンス統計情報がモニタリングされ、コマンドライン インターフェイス（CLI）MIB および簡易ネットワーク管理プロトコル（SNMP）MIB に格納されます。IP SLA パケットには設定可能な IP レイヤ オプションとアプリケーション層オプションがあります。たとえば、送信元および宛先の IP アドレス、ユーザ データグラム プロトコル（UDP）/TCP ポート番号、サービス タイプ（ToS）バイト（Differentiated Services Code Point（DSCP）および IP プレフィックス ビットを含む）、バーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンス、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ 2 転送に依存していないので、異なるネットワーク間にエンドツーエンド動作を設定してエンド ユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA は、次のような一意のパフォーマンス メトリックのサブセットを収集します。

- 遅延（往復および一方向）
- ジッター（方向性あり）
- パケット損失（方向性あり）
- パケット シーケンス（パケット順序）
- パス（ホップ単位）
- 接続（方向性あり）
- サーバまたは Web サイトのダウンロード時間

Cisco IP SLA は SNMP によるアクセスが可能なので、Cisco Works Internetwork Performance Monitor（IPM）やサードパーティ製パフォーマンス管理製品などのパフォーマンス モニタリング（PM）アプリケーションでも使用できます。IP SLA を使用すると次のような利点があります。

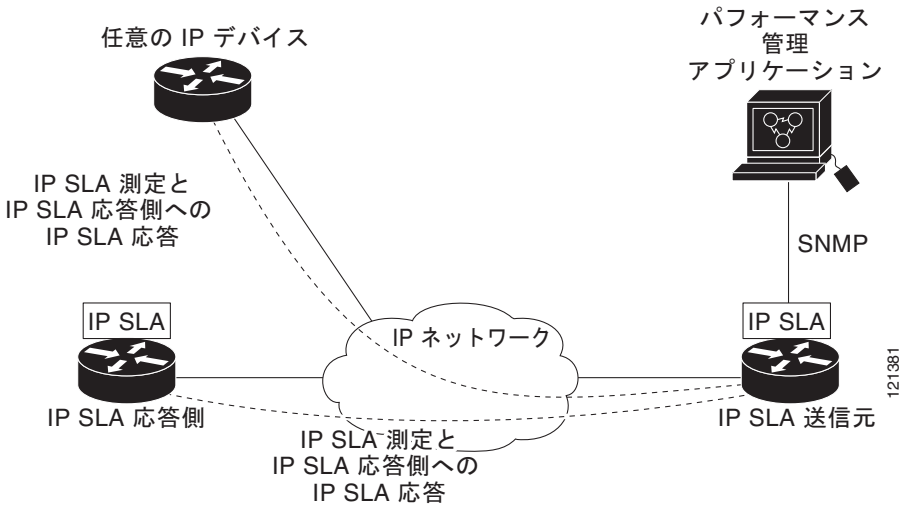
- SLA モニタリング、評価、検証。
- ネットワーク パフォーマンス モニタリング。
  - ネットワーク内のジッター、遅延、パケット損失が測定できる。
  - 連続的で信頼性のある確実な評価ができる。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに適していることを確認できる。
- 端末間のネットワーク アベイラビリティをモニタリングして、ネットワーク リソースをあらかじめ検証し接続をテストできる（たとえば、ビジネス上の重要なデータを保存する NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる）。
- 信頼性の高い評価を連続的に行ってネットワーク動作のトラブルシューティングを行うので、問題をすぐに特定しトラブルシューティングにかかる時間を短縮できる。

- マルチプロトコル ラベル スイッチング（MPLS）パフォーマンス モニタリングとネットワークの検証を行う（MPLS をサポートするスイッチの場合）。

Cisco IOS IP SLA によるネットワーク パフォーマンスの測定

IP SLA を使用して、プローブを物理的に配置せずに、コア、分散、エッジといったネットワーク内の任意のエリア間のパフォーマンスをモニタリングすることができます。2 つのネットワーク デバイス間のネットワーク パフォーマンスは、生成トラフィックで測定します。図 45-1 に、送信元デバイスが宛先デバイスに生成パケットを送信するときに IP SLA が開始される手順を示します。宛先デバイスがパケットを受信すると、IP SLA 動作の種類によって、送信元のタイム スタンプ情報に応じてパフォーマンス メトリックを算出します。IP SLA 動作は、特定のプロトコル（UDP など）を使用してネットワークの送信元から宛先へのネットワーク測定を行います。

図 45-1　　Cisco IOS IP SLA 動作



IP SLA ネットワーク パフォーマンス測定を実施する手順は次のとおりです。

1. 必要であれば、IP SLA Responder をイネーブルにします。
2. 必要な IP SLA 動作タイプを設定します。
3. 指定された動作タイプのオプションを設定します。
4. 必要であれば、しきい値条件を設定します。
5. 動作の実行スケジュールを指定し、しばらく動作を実行して統計情報を収集します。
6. Cisco IOS CLI を使用するかネットワーク管理システム（NMS）と SNMP を併用して、動作の結果を表示し確認します。

IP SLA Responder と IP SLA コントロール プロトコル

IP SLA Responder は宛先シスコ デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求パケットを予想して応答します。Responder は専用プローブなしで正確な測定を行います。Responder は、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロール プロトコルを通じて実現します。Cisco IOS デバイスだけが宛先 IP SLA Responder の送信元になります。

図 45-1 に、IP ネットワーク内での Cisco IOS IP SLA Responder の配置場所を示します。Responder は、IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートで受信します。コントロール メッセージを受信したら、指定された UDP または TCP ポートを指定された時間だけイネーブルにします。この間に、Responder は要求を受け付け、応答します。Responder は、IP SLA パケットに応答した後または指定の時間が経過したらポートをディセーブルにします。セキュリティの向上のために、コントロール メッセージでは MD5 認証が利用できます。

すべての IP SLA 動作に対して宛先デバイスの Responder をイネーブルにする必要はありません。たとえば、宛先ルータが提供しているサービス（Telnet や HTTP など）は Responder では必要ありません。他社製のデバイスに IP SLA Responder を設定することはできません。また、Cisco IOS IP SLA はこれらのデバイス固有のサービスに対してだけ動作パケットを送信できます。

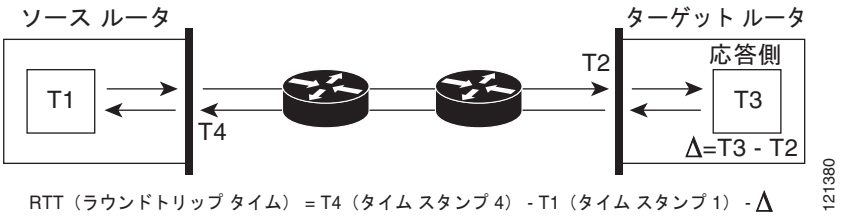
IP SLA の応答時間の計算

スイッチとルータは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。この遅延により応答時間が影響を受けます。テストパケットの応答が処理待ちのキューに入っていることもあるからです。この場合、応答時間は正しいネットワーク遅延を反映しません。IP SLA はソース デバイスとターゲット デバイス（Responder が使用されている場合）の処理遅延を最小化し、正しいラウンドトリップ時間（RTT）を識別します。IP SLA テスト パケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA Responder がイネーブルの場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲット デバイスでタイム スタンプを付け、処理時間は含めません。タイム スタンプはサブミリ秒単位で構成されます。

図 45-2 に、Responder の動作を示します。RTT を算出するためのタイム スタンプが 4 つ付けられます。ターゲット ルータでレスポンダ機能がイネーブルの場合、タイム スタンプ 3（TS3）からタイム スタンプ 2（TS2）を引いてテスト パケットの処理にかかった時間を求め、デルタ（Δ）で表します。次に全体の RTT からこのデルタの値を引きます。IP SLA により、この方法はソース ルータにも適用されます。その場合、着信タイム スタンプ 4（TS4）が割り込みレベルで付けられ、より正確な結果を得ることができます。

図 45-2　　Cisco IOS IP SLA Responder タイム スタンプ



この他にも、ターゲット デバイスに 2 つのタイム スタンプがあれば一方向遅延、ジッター、方向性を持つパケット損失がトラッキングできるという利点があります。大半のネットワーク動作は非同期なので、このような統計情報があるのは問題です。ただし一方向遅延測定を取り込むには、ソース ルータとターゲット ルータの両方にネットワーク タイム プロトコル（NTP）を設定し、両方のルータを同じくロック ソースに同期させる必要があります。一方向ジッター測定にはクロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合、統計情報の取り込みとエラー情報の収集から開始するように動作のスケジューリングをします。スケジューリングは、すぐに動作を開始する、または特定の月、日、時刻に開始するように設定できます。また、pending オプションを使用して、あとで動作を開始するように設定することもできます。pending オプションは動作の内部状態に関するもので、SNMP で表示できます。トリガーを待機する反応（しきい値）動作の場合も pending オプションを使用します。スケジューリングでは、1 度に 1 つの IP SLA 動作をさせることも、グループの動作をさせることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB で 1 つのコマンドを使用して、IP サービス イメージを稼働する複数の IP SLA 動作をスケジューリングできます。等間隔で動作を実行するようにスケジューリングすると、IP SLA モニタリング トラフィックの数を制御できます。IP SLA 動作をこのように分散させると CPU 利用率を最小限に抑え、ネットワーク スケーラビリティを向上させることができます。

IP SLA 動作のしきい値のモニタリング

サービス レベル契約モニタリングを正しくサポートするには、違反が発生した場合にすぐに通知されるメカニズムにする必要があります。IP SLA は SNMP トラップを送信して、次のような場合にイベントをトリガーします。

- 接続の損失
- タイムアウト
- RTT しきい値
- 平均ジッターしきい値
- 一方向パケット損失
- 一方向ジッター
- 一方向平均オピニオン評点（MOS）
- 一方向遅延

IP SLA しきい値違反が発生した場合も、あとで分析するために別の IP SLA 動作がトリガーされます。たとえば、回数を増やしたり、ICMP パス エコーや ICMP パス ジッター動作を開始してトラブルシューティングを行うことができます。

しきい値タイプとレベル設定の決定は複雑で、ネットワークで使用する IP サービス タイプによって異なります。

UDP ジッター動作を使用した IP サービス レベル

ジッターはパケット間の遅延がばらつくことを指します。発信元から宛先に向かって複数のパケットを 10 ミリ秒遅れで送信した場合、ネットワークが正常に動作していれば宛先でも 10 ミリ秒遅れで受信します。しかし、ネットワーク内に遅延がある場合（キューの発生や別のルータ経由で到着するなど）、パケットの到着遅延が 10 ミリ秒を上回ったり、下回ったりします。正のジッター値は、パケットの到着が 10 ミリ秒を超えていることを意味します。パケットの到着が 12 ミリ秒の場合のジッター値は +2 ミリ秒（正の値）です。8 ミリ秒で到着する場合は、2 ミリ秒（負の値）です。遅延による影響を受けやすいネットワークの場合、正のジッター値は望ましくありません。ジッター値 0 が理想的です。

ジッターのモニタリング以外にも、IP SLA UDP ジッター動作を多目的データ収集動作に使用できます。パケット IP SLA は搬送パケットを生成し、送信元ターゲットと動作ターゲット間でシーケンス情報の送受信とタイム スタンプの送受信を行います。以上の点に基づき、UDP ジッター動作は次のデータを測定します。

- 方向別ジッター（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均 RTT）

データを送受信するパスが異なる場合もあるので（非同期）、方向別データを使用すればネットワークで発生している輻輳や他の問題の場所を簡単に突き止めることができます。

UDP ジッター動作では合成（シミュレーション）UDP トラフィックを生成し、送信元ルータからターゲット ルータに多数の UDP パケットを送信します。その際の各パケットのサイズ、パケット同士の間隔、送信間隔は決められています。デフォルトでは、10 バイトのペイロード サイズのパケット フレームを 10 ミリ秒で 10 個生成し、60 秒間隔で送信します。これらのパラメータは、提供する IP サービスを最適にシミュレートするように設定できます。

一方向遅延を正確に測定する場合、NTP などによる送信元デバイスとターゲット デバイス間のクロック同期が必要です。一方向ジッターおよびパケット損失を測定する場合は、クロック同期は不要です。送信元デバイスとターゲット デバイスのクロックが同期されていない場合、一方向ジッターおよびパケット損失データは戻されますが、UDP ジッター動作による一方向遅延測定の値は *0* で戻ります。

（注） 送信元デバイスに UDP ジッター動作を設定する前に、ターゲット デバイス（動作ターゲット）の IP SLA 応答側を有効にしておく必要があります。

ICMP エコー動作を使用した IP サービス レベル

ICMP エコー動作は、シスコ デバイスと IP を使用する任意のデバイスとの間でエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセージを宛先に送信して ICMP エコー応答を受信するまでの時間を測定して算出します。大多数のカスタマーが IP SLA ICMP ベース動作、社内 ping テスト、ping ベース専用プローブを使用して、送信元 IP SLA デバイスと宛先 IP デバイス間の応答時間を測定しています。IP SLA ICMP エコー動作は、ICMP ping テストと同じ仕様に準拠しており、どちらの方法でも同じ応答時間が得られます。

（注） この動作では、IP SLA 応答側を有効にしておく必要はありません。

Cisco IOS IP SLA 動作の設定方法

（注） スイッチでは、このガイドで説明する IP SLA コマンドや動作がすべてサポートされているわけではありません。スイッチでは、UDP ジッター、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッター、FTP、DNS、DHCP を使用する IP サービス レベル分析がサポートされます。また、複数動作スケジューリングおよび事前に設定されたしきい値のモニタリングもサポートされます。ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービス レベルはサポートしていません。

IP SLA Responder の設定

はじめる前に

IP SLA Responder が機能するためには、Catalyst 3750 スイッチまたは Catalyst 3560 スイッチのような、IP サービス イメージを実行して IP SLA をすべてサポートしている送信元デバイスを設定する必要があります。送信元デバイスの設定情報については、マニュアルを参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla responder** {**tcp-connect** | **udp-echo**} **ipaddress** *ip-address* **port** *port-number*	スイッチを IP SLA 応答側として設定します。 オプションのキーワードの意味は次のとおりです。 • **tcp-connect**：Responder の TCP 接続動作をイネーブルにします。 • **udp-echo**：Responder のユーザ データグラム プロトコル（UDP）エコー動作またはジッター動作をイネーブルにします。 • **ipaddress** *ip-address*：宛先 IP アドレスを入力します。 • **port** *port-number*：宛先ポート番号を入力します。 **（注）** IP アドレスとポート番号は、IP SLA 動作のソース デバイスに設定した IP アドレスおよびポート番号と一致している必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。

UDP ジッター動作の設定

はじめる前に

送信元デバイスに UDP ジッター動作を設定する前に、ターゲット デバイス（動作ターゲット）の IP SLA 応答側を有効にしておく必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]	IP SLA 動作を UDP ジッター作として設定し、UDP ジッター コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 • （任意）**source-ip** {*ip-address* | *hostname*} *:* 送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 • （任意）**source-port** *port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 • （任意）**control**：IP SLA コントロール メッセージの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA コントロール メッセージが宛先デバイスに送信されて、IP SLA 応答側との接続が確立します。 • （任意）**num-packets** *number-of-packets*：生成するパケット数を入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 • （任意）**interval** *inter-packet-interval*：パケットの送信間隔をミリ秒で指定します。指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 4	**frequency** *seconds*	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 5	**exit**	UDP ジッター コンフィギュレーション サブモードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR のエントリ番号を入力します。 • （任意）**life**：動作の実行を無制限（**forever**）に指定するか、*秒数*を指定します。範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 – 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 – **pending** と入力すれば、開始時刻を指定するまでは情報を収集しません。 – **now** と入力すれば、ただちに動作を開始します。 – **after** *hh:mm:ss* と入力すれば、指定した時刻の経過後に動作を開始します。 • （任意）**ageout** *seconds*：情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

ICMP エコー動作を使用した IP サービス レベルの分析

（注）　この動作では、IP SLA 応答側を有効にしておく必要はありません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-id*]	IP SLA 動作を ICMP エコー動作として設定し、ICMP エコー コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • （任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 • （任意）**source-interface** *interface-id*：動作に対する送信元インターフェイスを指定します。
ステップ 4	**frequency** *seconds*	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 5	**exit**	UDP ジッター コンフィギュレーション サブモードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR のエントリ番号を入力します。 • （任意）**life**：動作の実行を無制限（**forever**）に指定するか、*秒数*を指定します。範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 – 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 – **pending** と入力すれば、開始時刻を指定するまでは情報を収集しません。 – **now** と入力すれば、ただちに動作を開始します。 – **after** *hh:mm:ss* と入力すれば、指定した時刻の経過後に動作を開始します。 • （任意）**ageout** *seconds*：情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 7	end	特権 EXEC モードに戻ります。

Cisco IP SLA 動作のモニタリングおよびメンテナンス

コマンド	目的
show ip sla application	Cisco IOS IP SLA のグローバル情報を表示します。
show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する、デフォルト値をすべて含めた設定値を表示します。
show ip sla enhanced-history {**collection-statistics** | **distribution statistics**} [*entry-number*]	収集した履歴バケットの拡張履歴統計情報、あるいはすべての IP SLA 動作または特定の IP SLA 動作に関する分散統計情報を表示します。
show ip sla ethernet-monitor configuration [*entry-number*]	IP SLA 自動イーサネット設定を表示します。
show ip sla event-publisher	IP SLA の通知を受信するために登録されているクライアント アプリケーションのリストを表示します。
show ip sla group schedule [*schedule-entry-number*]	IP SLA グループ スケジューリング設定と個別情報を表示します。
show ip sla history [*entry-number* | **full** | **tabular**]	すべての IP SLA 動作について収集した履歴を表示します。
show ip sla mpls-lsp-monitor {**collection-statistics** | **configuration** | **ldp operational-state** | **scan-queue** | **summary** [*entry-number*] | **neighbors**}	MPLS ラベル スイッチド パス（LSP）ヘルス モニタ動作を表示します。
show ip sla reaction-configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する、予防的しきい値のモニタリングの設定を表示します。
show ip sla reaction-trigger [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する反応トリガー情報を表示します。
show ip sla responder	IP SLA 応答側の情報を表示します。
show ip sla standards	IP SLA 標準に関する情報を表示します。
show ip sla statistics [*entry-number* | **aggregated** | **details**]	動作ステータスおよび統計情報の現在値または合計値を表示します。

Cisco IP SLA 動作の設定例

ICMP エコー IP SLA 動作の設定：例

次に、ICMP エコー IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.
```

```
Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

show ip sla コマンドの出力：例

コマンド出力例は次のとおりです。

```
Switch# show ip sla application

        IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0

        Supported Operation Types
Type of Operation to Perform: 802.1agEcho
Type of Operation to Perform: 802.1agJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho
```

```
IP SLAs low memory water mark: 21741224
```

UDP ジッター IP SLA 動作の Responder の設定：例

次に、デバイスを UDP ジッター IP SLA 動作の Responder に設定する例を示します。UDP ジッター IP SLA 動作については次の項で説明します。

```
Switch(config)# ip sla responder udp-echo 172.29.139.134 5000
```

UDP ジッター IP SLA 動作の設定：例

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
IP SLA コマンドと設定	Cisco.com にある『*Cisco IOS IP SLAs Configuration Guide*』 Cisco.com にある『*Cisco IOS IP SLAs Command Reference* 』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 46

レイヤ 2 NAT の設定

この章では、Cisco IOS Release 15.0(2)EB で導入されたレイヤ 2 NAT 機能を設定する際に役立つ情報を提供します。

（注） Cisco Industrial Ethernet 2000 シリーズ スイッチの詳細については、www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html にあるリリース ノート、コマンド リファレンス、およびコンフィギュレーション ガイドを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このマニュアルで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

レイヤ 2 NAT の前提条件

レイヤ 2 NAT は Cisco IOS 15.0(2)EB 以降で使用可能な拡張 LAN ベース フィーチャ セットに含まれています。モデルによってライセンスのアップグレードおよびソフトウェアのアップグレードを必要とする可能性があります。詳細については、www.cisco.com/en/US/docs/switches/lan/cisco_ie2000/software/release/15_0_2_eb/upgrade/guide/ie2000_ug.html を参照してください。

レイヤ 2 NAT 設定の制約事項

- レイヤ 2 NAT は Cisco IOS 15.0(2)EB 以降で使用可能な拡張 LAN ベース フィーチャ セットに含まれています。
- IPv4 アドレスのみ変換できます。
- レイヤ 2 NAT はユニキャスト トラフィックにのみ適用されます。未変換のユニキャスト トラフィック、マルチキャスト トラフィック、および IGMP トラフィックを許可することができます。
- レイヤ 2 NAT のホストの変換を設定する場合は、DHCP クライアントとして設定しないでください。

ガイドライン

アドレスの変換を指定するレイヤ 2 NAT インスタンスを設定する必要があります。その後、インターフェイスおよび VLAN にこれらのインスタンスを接続します。一致しないトラフィックと変換するよう設定されていないトラフィック タイプでは、トラフィックの許可またはドロップを選択できます。送受信されたパケットに関する詳細な統計情報を確認できます。

- このスイッチの 2 個のアップリンク ポートに関してレイヤ 2 NAT を設定できます。
- ダウンリンク ポートは、VLAN、トランク、レイヤ 2 チャネルなどがあります。
- スイッチには、128 のレイヤ 2 NAT インスタンスを設定できます。
- 設定できる変換エントリは 128 個です。
- レイヤ 2 NAT 設定では最大 128 の VLAN が利用できます。
- ARP、ICMP などの特定のプロトコルは、レイヤ 2 NAT で透過しませんが、これはデフォルトで「固定」されています。

レイヤ 2 NAT 設定に関する情報

概念について

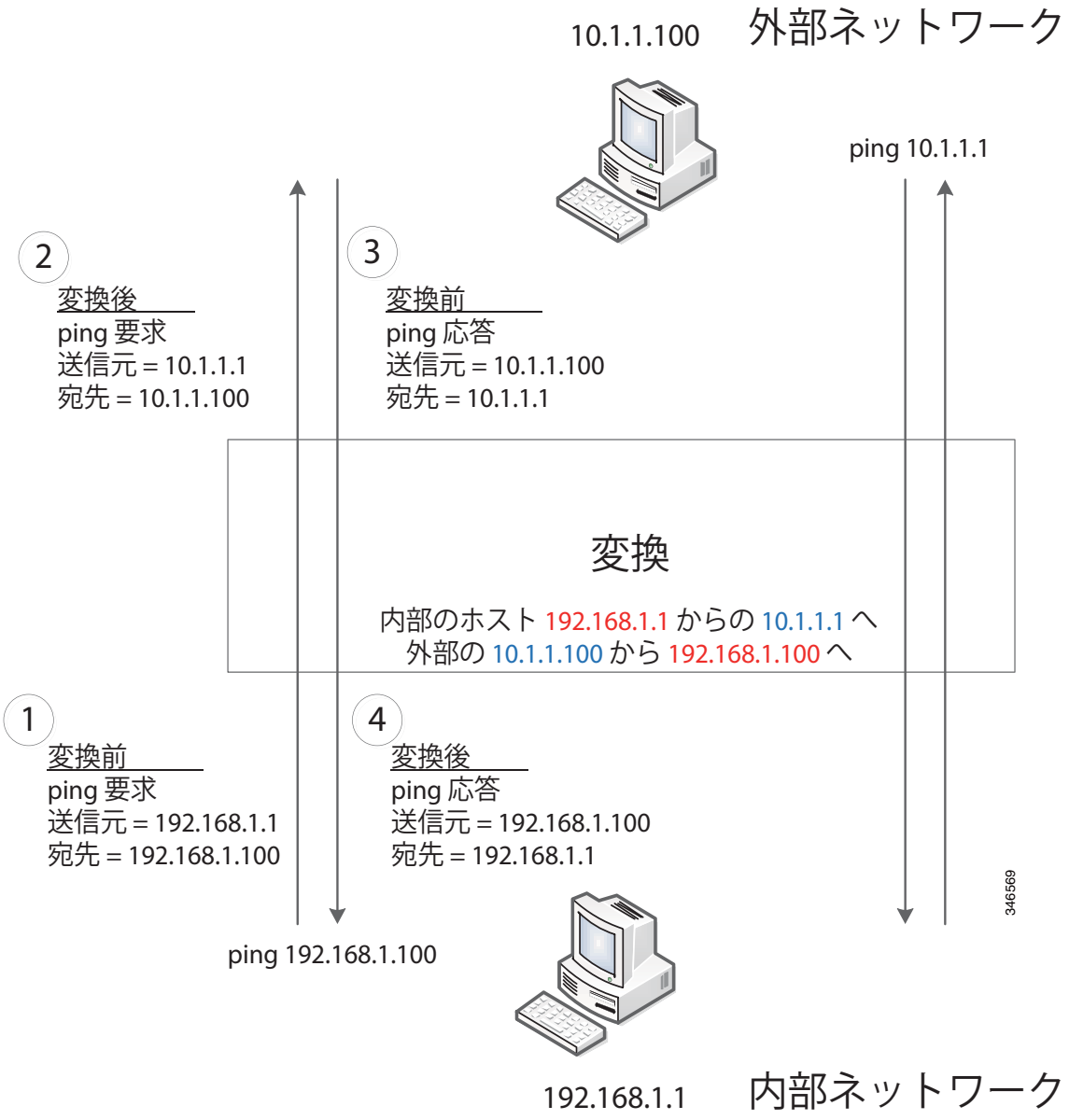
1 対 1（1 : 1）レイヤ 2 NAT は、固有のパブリック IP アドレスを既存のプライベート IP アドレス（エンド デバイス）に割り当てるサービスであり、エンド デバイスがプライベートとパブリック サブネット上で通信できるようになります。このサービスは、NAT 対応デバイスで設定され、エンド デバイスに物理的にプログラムされた IP アドレスのパブリックでの「エイリアス」です。これは、通常 NAT デバイスでテーブルとして表されます。

レイヤ 2 NAT には、プライベートからパブリックおよびパブリックからプライベートへサブネットの変換を定義できる 2 種類の変換テーブルがあります。レイヤ 2 NAT はスイッチの負荷全体で、一貫した高レベルの（bump-in-the-wire）パフォーマンスを提供するハードウェア ベースの機能です。またこの機能は、拡張されたネットワーク セグメンテーション用の NAT 境界で複数の VLAN をサポートします。リング アーキテクチャのサポートは NAT 境界で冗長が可能なレイヤ 2 NAT に組み込まれています。

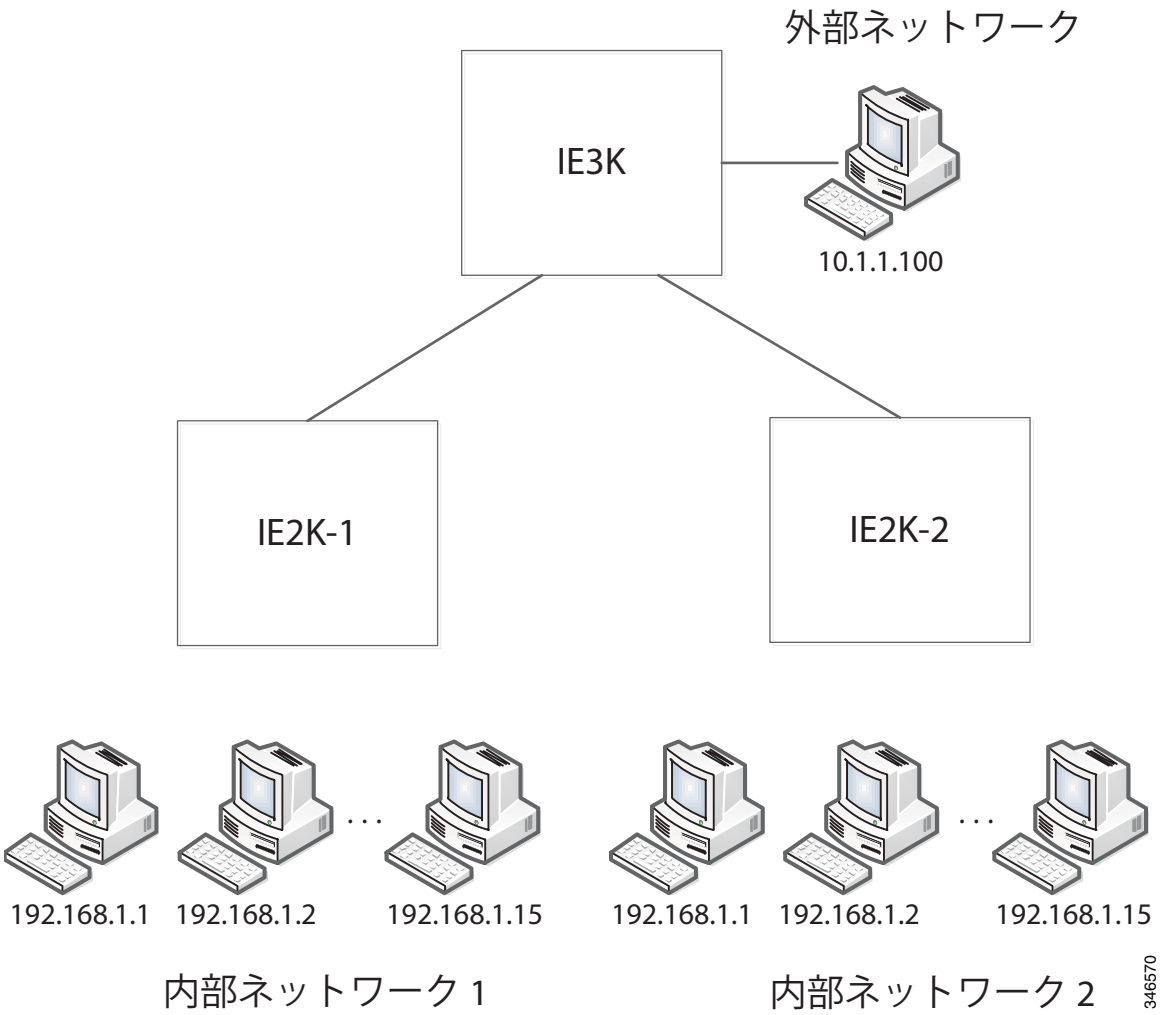
図 46-1 レイヤ 2 NAT では、192.168.1.x ネットワークのセンサーと 10.1.1.x ネットワークの通信制御装置間でアドレスを変換します。

1. 192.168.1.1 のセンサーが通信制御装置に「内部」アドレス 192.168.1.100 を使用して ping 要求を送信します。
2. パケットが内部ネットワークから送信される前に、レイヤ 2 NAT は送信元アドレスを 10.1.1.1 へ、宛先アドレスを 10.1.1.100 へと変換します。
3. 通信制御装置は 10.1.1.1 へ ping 応答を送信します。
4. パケットが内部ネットワークで受信されると、レイヤ 2 NAT は送信元アドレスを 192.168.1.100 へ、宛先アドレスを 192.168.1.1 へ変換します。

図 46-1　ネットワーク間のアドレス変換



大規模なノードでは、サブネット内のすべてのデバイスに対してただちに変換をイネーブルにできます。この場合、内部ネットワーク 1 からのアドレスは 10.1.1.0/28 サブネットで外部アドレスに変換することができ、ネットワーク 2 からのアドレスは 10.1.1.16/28 サブネットで外部アドレスに変換することができます。各サブネットのアドレスはすべて 1 つのコマンドを使って変換できます。



管理インターフェイスの使用

管理インターフェイスはレイヤ 2 NAT 機能の先にあります。そのためこのインターフェイスはプライベート ネットワーク VLAN 上にはありません。プライベート ネットワーク VLAN 上に存在する場合は、内部アドレスを割り当て、内部の変換を設定します。

レイヤ 2 NAT の設定方法

レイヤ 2 NAT のデフォルト設定

機能	デフォルト設定
一致しないトラフィックまたは変換するように設定されていないトラフィック タイプのパケットの許可またはドロップ	すべての一致しない、マルチキャストの IGMP パケットをドロップする。
プロトコル フィックスアップ	ARP のフィックスアップ

レイヤ 2 NAT のセットアップ

レイヤ 2 NAT を設定するには、次の手順を実行します。この章の詳細については、例を参照してください。

	コマンド	目的
ステップ 1	**configure**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**l2nat instance** *instance_name*	新しいレイヤ 2 NAT インスタンスを作成します。インスタンスを作成した後、そのインスタンスのサブモードを開始する場合もこのコマンドを使用します。
ステップ 3	**inside from** [*host* | *range* | *network*] *original ip* to *translated ip*[*mask*] *number* | *mask*	内部アドレスを外部アドレスへ変換します。単一のホスト アドレス、ホスト アドレスの範囲、またはサブネット内のすべてのアドレスを変換できます。発信トラフィックの送信元アドレスと着信トラフィックの宛先アドレスを変換します。
ステップ 4	**outside from** [*host* | *range* | *network*] *original ip* to *translated ip*[*mask*] *number* | *mask*	外部アドレスを内部アドレスへ変換します。単一のホスト アドレス、ホスト アドレスの範囲、またはサブネット内のすべてのアドレスを変換できます。発信トラフィックの宛先アドレスおよび着信トラフィックの送信元アドレスを変換します。
ステップ 5	**exit**	config-l2nat モードを終了します。
ステップ 6	**interface** *interface-id*	指定したインターフェイス（アップリンク ポートのみ）のインターフェイス コンフィギュレーション モードにアクセスします。
ステップ 7	**l2nat** *instance_name* [*vlan* | *vlan_range*]	VLAN または VLAN 範囲に指定されたレイヤ 2 NAT のインスタンスを適用します。このパラメータが欠落している場合、レイヤ 2 NAT インスタンスはネイティブ VLAN に適用されます。
ステップ 8	**end**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**show l2nat instance** *instance_name*	指定されたレイヤ 2 NAT インスタンスの設定の詳細を表示します。
ステップ 10	**show l2nat statistics**	両方のアップリンク ポートについてレイヤ 2 NAT の統計情報を表示します。
ステップ 11	**end**	特権 EXEC モードに戻ります。

レイヤ 2 NAT 設定のモニタリング

表 46-1　レイヤ 2 NAT 設定の表示

コマンド	目的
show l2nat instance	指定されたレイヤ 2 NAT インスタンスの設定の詳細を表示します。
show l2nat interface	1 つまたは複数のインターフェイスでのレイヤ 2 NAT インスタンスの設定の詳細を表示します。
show l2nat statistics	すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。
show l2nat statistics interface	指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。

レイヤ 2 NAT 設定のトラブルシューティング

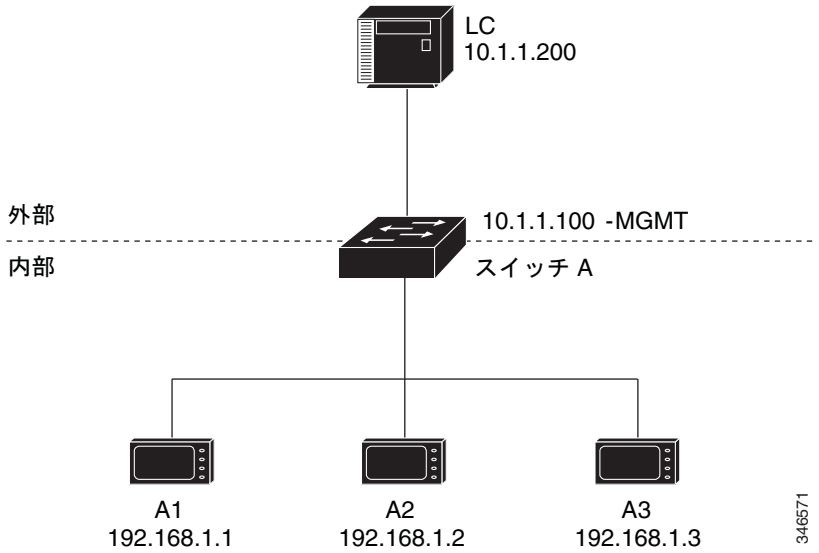
表 46-2　レイヤ 2 NAT 設定のトラブルシューティング

コマンド	目的
debug l2nat	設定が適用されたときにリアルタイムでのレイヤ 2 NAT 設定の詳細の表示をイネーブルにします。

設定例

基本的な内部から外部への通信の例

図 46-2　基本的な内部から外部への通信



ここでは、A1 はアップリンク ポートに直接接続されたロジック コントローラ LC と通信する必要があります。レイヤ 2 NAT インスタンスは、外部ネットワーク（10.1.1.1）上での A1 のアドレスと内部ネットワーク（192.168.1.250）上での LC のアドレスを提供するように設定されています。

ここで次の通信が発生します。

1. A1 が ARP 要求を送信します。
   SA: 192.168.1.1
   DA: 192.168.1.250
2. Cisco スイッチ A は ARP 要求をフィックスアップします。
   SA: 10.1.1.1
   DA: 10.1.1.200
3. LC は要求を受信し、10.1.1.1 の MAC アドレスを学習します。
4. LC が応答を送信します。
   SA: 10.1.1.200
   DA: 10.1.1.1
5. Cisco スイッチ A は ARP 応答をフィックスアップします。
   SA: 192.168.1.250
   DA: 192.168.1.1
6. A1 は 192.168.1.250 の MAC アドレスを学習し、通信を開始します。

（注）　スイッチの管理インターフェイスは内部ネットワーク 192.168.1.x. とは別の VLAN に属している必要があります。

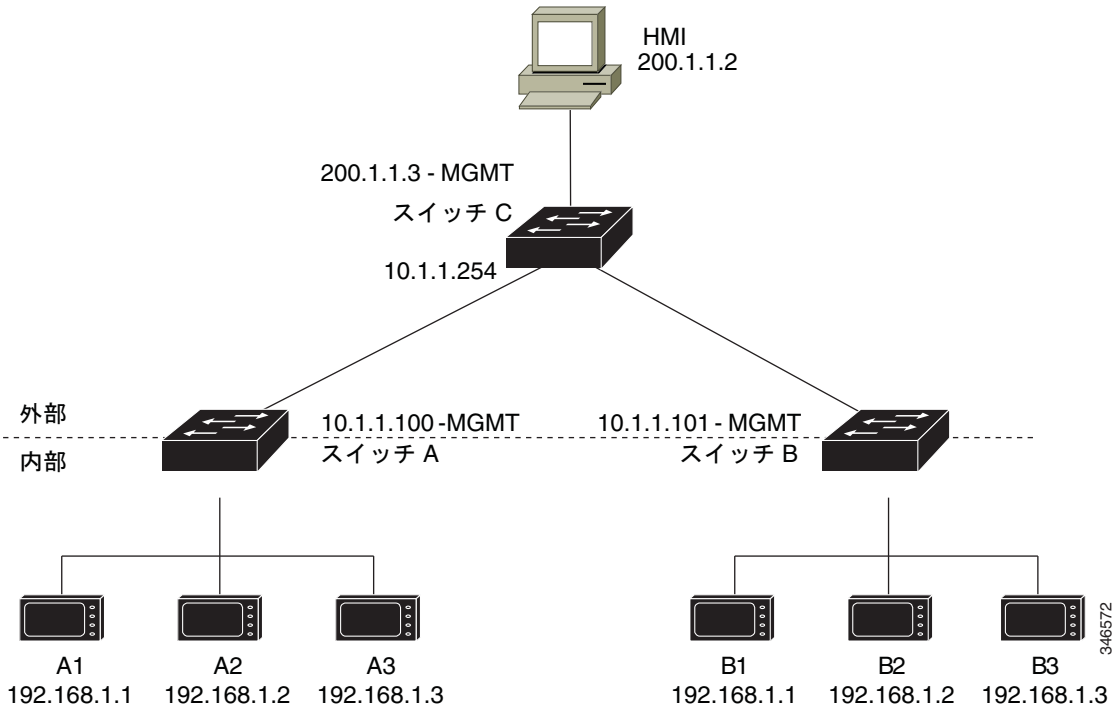
表 46-2 に、ここでの設定作業を示します。レイヤ 2 NAT インスタンスが作成され、2 つの変換エントリを追加し、インスタンスをインターフェイスに適用します。ARP フィックスアップはデフォルトでイネーブルです。

表 46-3　基本的な内部から外部への例での Cisco スイッチ A の設定

	コマンド	目的
ステップ 1	Switch# **configure**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# **l2nat instance A-LC**	A-LC という新しいレイヤ 2 NAT インスタンスを作成します。
ステップ 3	Switch(config-l2nat)# **inside from host 192.168.1.1 to 10.1.1.1**	A1 の内部アドレスを外部アドレスへ変換します。
ステップ 4	Switch(config-l2nat)# **outside from host 10.1.1.200 to 192.168.1.250**	LC の外部アドレスを内部アドレスへ変換します。
ステップ 5	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
ステップ 6	Switch(config)# **interface Gi1/1**	アップリンク ポートのインターフェイス コンフィギュレーション モードにアクセスします。
ステップ 7	Switch(config-if)# **l2nat A-LC**	このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。
ステップ 8	Switch# **end**	特権 EXEC モードに戻ります。

重複する IP アドレスの例

図 46-3　IP アドレスの重複



ここでは、2 台のマシン ノードで 192.168.1.x 領域のアドレスが事前設定されています。レイヤ 2 NAT は、これらのアドレスを外部ネットワークの別のサブネット上で一意のアドレスに変換するために使用されます。また、マシン間の通信で、ノード A のマシンはノード B の領域で一意のアドレスを必要とし、ノード B のマシンはノード A の領域で一意のアドレスが必要です。

- スイッチ C は 192.168.1.x 領域でのアドレスが必要です。パケットがノード A またはノード B で受信されると、スイッチ C の 10.1.254 というアドレスが 192.168.1.254 に変換されます。パケットがノード A またはノード B から送信されると、スイッチ C の 192.168.1.254 というアドレスは 10.1.1.254 に変換されます。
- ノード A とノード B のマシンは 10.1.1.x 領域で一意のアドレスが必要です。設定の容易さと使いやすさを実現するために、10.1.1.x 領域は 10.1.1.0、10.1.1.16、10.1.1.32 などのサブネットに分割されます。各サブネットは異なるノードに使用できます。この例では、10.1.1.16 はノード A に使用され、10.1.1.32 はノード B に使用されます。
- ノード A とノード B のマシンはデータを交換するための一意のアドレスが必要です。使用可能なアドレスはサブネットに分割されます。便宜上、ノード A のマシン用の 10.1.1.16 サブネット アドレスは、ノード B の 192.168.1.16 サブネット アドレスへ変換されます。ノード B マシン用の 10.1.1.32 サブネット アドレスは、ノード A の 192.168.1.32 サブネット アドレスに変換されます。

- マシンは各ネットワークで一意のアドレスを持ちます。

	ノード A のアドレス	外部ネットワークのアドレス	ノード B のアドレス
スイッチ A のネットワーク アドレス	192.168.1.0	10.1.1.16	192.168.1.16
A1	192.168.1.1	10.1.1.17	192.168.1.17
A2	192.168.1.2	10.1.1.18	192.168.1.18
A3	192.168.1.3	10.1.1.19	192.168.1.19
Cisco スイッチ B のネットワーク アドレス	192.168.1.32	10.1.1.32	192.168.1.0
B1	192.168.1.33	10.1.1.33	192.168.1.1
B2	192.168.1.34	10.1.1.34	192.168.1.2
B3	192.168.1.35	10.1.1.35	192.168.1.3
スイッチ C	192.168.1.254	10.1.1.254	192.168.1.254

表 46-4 に、スイッチ A の設定作業を示します。表 46-5 に、Cisco スイッチ B の設定作業を示します。

表 46-4　アドレス重複の場合のスイッチ A の設定

	コマンド	目的
ステップ 1	Switch# **configure**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# **l2nat instance A-Subnet**	A-Subnet という新しいレイヤ 2 NAT インスタンスを作成します。
ステップ 3	Switch(config-l2nat)# **inside from network 192.168.1.0 to 10.1.1.16 mask 255.255.255.240**	ノード A のマシンの内部アドレスを 10.1.1.16 255.255.255.240 サブネットのアドレスへ変換します。
ステップ 4	Switch(config-l2nat)# **outside from host 10.1.1.254 to 192.168.1.254**	スイッチ C の外部アドレスを内部アドレスへ変換します。
ステップ 5	Switch(config-l2nat)# **outside from network 10.1.1.32 to 192.168.1.32 255.255.255.240**	ノード B のマシンの外部アドレスをノード B の内部アドレスに変換します。
ステップ 6	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
ステップ 7	Switch(config)# **interface Gi1/1**	アップリンク ポートのインターフェイス コンフィギュレーション モードにアクセスします。
ステップ 8	Switch(config-if)# **l2nat A-Subnet**	このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。
ステップ 9	Switch# **end**	特権 EXEC モードに戻ります。

表 46-5　サブネットの場合のスイッチ B の設定

	コマンド	目的
ステップ 1	Switch# **configure**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# **l2nat instance B-Subnet**	B-Subnet という新しいレイヤ 2 NAT インスタンスを作成します。
ステップ 3	Switch(config-l2nat)# **inside from network 192.168.1.0 to 10.1.1.32 255.255.255.240**	ノード B のマシンの内部アドレスを 10.1.1.32 255.255.255.240 サブネットのアドレスへ変換します。
ステップ 4	Switch(config-l2nat)# **outside from host 10.1.1.254 to 192.168.1.254**	スイッチ C の外部アドレスを内部アドレスへ変換します。
ステップ 5	Switch(config-l2nat)# **outside from network 10.1.1.16 to 192.168.1.16 255.255.255.240**	ノード A のマシンの外部アドレスをノード A の内部アドレスに変換します。
ステップ 6	Switch(config-l2nat)# **outside from network 10.1.1.32 to 192.168.1.0 255.255.255.240**	ノード B のマシンの外部アドレスをノード B の内部アドレスに変換します。
ステップ 7	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
ステップ 8	Switch(config)# **interface Gi1/1**	アップリンク ポートのインターフェイス コンフィギュレーション モードにアクセスします。
ステップ 9	Switch(config-if)# **l2nat name1**	このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。
ステップ 10	Switch# **show l2nat instance name1**	指定されたレイヤ 2 NAT インスタンスの設定の詳細を表示します。
ステップ 11	Switch# **show l2nat statistics**	レイヤ 2 NAT の統計情報を表示します。
ステップ 12	Switch# **end**	特権 EXEC モードに戻ります。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
このスイッチの Cisco IOS コマンド	『*Cisco IE2000 Switch Series Command Reference*』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
ライセンス アップグレードの手順	『*Software Activation Licensing Upgrade Instructions for the Cisco IE2000 Switch Series*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

CHAPTER 47

トラブルシューティング

この章では、スイッチが稼働する Cisco IOS ソフトウェアに関連する問題を特定し、解決する方法について説明します。問題の性質に応じて、コマンドライン インターフェイス（CLI）、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。

LED の説明など、トラブルシューティングの詳細については、*ハードウェア インストレーション ガイド*を参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

トラブルシューティング情報

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは速度（10 Mbps、100 Mbps、および SFP モジュール ポート以外の 1000 Mbps）およびデュプレックス（半二重または全二重）に関するスイッチの設定を管理します。このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている場合。

スイッチのパフォーマンスを最大限に引き出してリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。

（注）　接続先装置が自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定を一致させます。速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

SFP モジュールのセキュリティと識別

シスコの SFP モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティ コード、および巡回冗長検査（CRC）が格納されたシリアル EEPROM を備えています。スイッチに SFP モジュールを装着すると、スイッチ ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを errdisable ステートにします。

（注）　セキュリティ エラー メッセージは、GBIC_SECURITY 機能を参照します。スイッチは、SFP モジュールをサポートしていますが、GBIC（ギガビット インターフェイス コンバータ）モジュールはサポートしていません。エラー メッセージ テキストは、GBIC インターフェイスおよびモジュールを参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェイスを参照します。エラー メッセージの詳細については、このリリースに対応するシステム メッセージ ガイドを参照してください。

他社の SFP モジュールを使用している場合、スイッチから SFP モジュールを取り外し、シスコのモジュールに交換します。シスコの SFP モジュールを装着したら、**errdisable recovery cause gbic-invalid** グローバル コンフィギュレーション コマンドを使用してポート ステータスを確認し、errdisable ステートから回復する時間間隔を入力します。この時間間隔が経過すると、スイッチは errdisable ステートからインターフェイスを復帰させ、操作を再試行します。**errdisable recovery** コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダー データ情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラー メッセージが生成されます。この場合、SFP モジュールを取り外して再び装着してください。それでも障害が発生する場合は、SFP モジュールが不良品である可能性があります。

ping

スイッチは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。ping はアドレスにエコー要求パケットを送信し、応答を待ちます。ping は次のいずれかの応答を返します。

- 正常な応答：正常な応答（*hostname* が存在する）は、ネットワーク トラフィックにもよりますが、1 ～ 10 秒以内で発生します。
- 宛先の応答なし：ホストが応答しない場合、*no-answer* メッセージが返ってきます。
- ホスト不明：ホストが存在しない場合、*unknown host* メッセージが返ってきます。
- 宛先に到達不能：デフォルト ゲートウェイが指定されたネットワークに到達できない場合、*destination-unreachable* メッセージが返ってきます。
- ネットワークまたはホストに到達不能：ルート テーブルにホストまたはネットワークに関するエントリがない場合、*network or host unreachable* メッセージが返ってきます。

レイヤ 2 traceroute

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。レイヤ 2 Traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。パス内にあるスイッチの MAC アドレス テーブルを使用してパスを識別します。スイッチがレイヤ 2 traceroute をサポートしないデバイスをパスで検出すると、スイッチはレイヤ 2 トレース キューを送信し続けてタイムアウトにしてしまいます。

スイッチは、送信元デバイスから宛先デバイスへのパスのみを識別できます。パケットが通過する、送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

レイヤ 2 traceroute の使用上の注意事項

- Cisco Discovery Protocol（CDP）がネットワーク上のすべてのデバイスでイネーブルでなければなりません。レイヤ 2 traceroute が適切に動作するために、CDP をディセーブルにしないでください。

  物理パス内のデバイスが CDP に対して透過的な場合、スイッチはこれらのデバイスを通過するパスを識別できません。CDP をイネーブルにする場合の詳細については第 32 章「CDP の設定」を参照してください。

- スイッチは、**ping** 特権 EXEC コマンドを使用して接続をテストする場合に他のスイッチから到達できます。物理パス内のすべてのスイッチは、他のスイッチから到達可能でなければなりません。
- パス内で識別される最大ホップ カウントは 10 です。
- 送信元デバイスから宛先デバイスの物理パス内にないスイッチに、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスのみを表示します。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- マルチキャスト送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラー メッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。
- 指定した送信元および宛先 MAC アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定する場合、スイッチは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用して、IP アドレスを対応する MAC アドレスおよび VLAN ID に関連付けます。
  - 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
  - ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスが解決されない場合は、パスは識別されず、エラー メッセージが表示されます。

- 複数のデバイスがハブを介して 1 つのポートに接続されている場合（たとえば複数の CDP ネイバーがポートで検出された場合）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

IP traceroute

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先として指定できます。また、スイッチは **traceroute** コマンドの出力でホップとして表示される場合があります。スイッチを traceroute の宛先とすると、スイッチは、traceroute の出力で最終の宛先として表示されます。中間スイッチが同じ VLAN 内でポート間のパケットのブリッジングだけを行う場合、traceroute の出力に中間スイッチは表示されません。ただし、中間スイッチが、特定のパケットをルーティングするマルチレイヤ スイッチの場合、中間スイッチは traceroute の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの Time To Live（TTL; 存続可能時間）フィールドを使用して、ルータおよびサーバで特定のリターン メッセージが生成されるようにします。traceroute の実行は、UDP データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、インターネット制御メッセージ プロトコル（ICMP）time-to-live-exceeded メッセージを送信元に送信します。traceroute は、ICMP time-to-live-exceeded メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、traceroute は TTL 値が 2 の UDP パケットを送信します。1 番めのルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番めのルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、time-to-live-exceeded メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、traceroute は、データグラムの UDP 宛先ポート番号を、宛先ホストが使用する可能性のない大きな値に設定します。ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛てのデータグラムを受信すると、送信元に ICMP *ポート到達不能*エラーを送信します。ポート到達不能エラーを除くすべてのエラーは中間ホップから送信されるため、ポート到達不能エラーを受信するということは、このメッセージが宛先ポートから送信されたことを意味します。

TDR

Time Domain Reflector（TDR）機能を使用すると、ケーブル配線の問題を診断して解決できます。TDR 稼働時、ローカル デバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号を比べます。

TDR は、銅線のイーサネット 10/100 および 10/100/1000 ポートでサポートされます。SFP モジュール ポートではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペア ケーブルの導線のオープン、損傷、切断：導線がリモート デバイスからの導線に接続されていない状態。
- ツイストペア ケーブルの導線のショート：導線が互いに接触している状態、またはリモート デバイスからの導線に接触している状態。たとえば、ツイスト ペア ケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペア ケーブルのショートが発生します。

ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを検出できます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- スイッチの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2 つのデバイス間の接続のトラブルシューティング

crashinfo ファイル

crashinfo ファイルには、シスコのテクニカル サポート担当者が Cisco IOS イメージの障害（クラッシュ）が原因で起きた問題をデバッグするときに使用する情報が保存されています。スイッチは障害発生時にその情報をコンソールに書き込みます。スイッチは次の 2 つのタイプの crashinfo ファイルを作成します。

- 基本 crashinfo ファイル：障害発生後に Cisco IOS イメージを起動すると、スイッチが自動的にこのファイルを作成します。
- 拡張 crashinfo ファイル：システム障害の発生時に、スイッチがこのファイルを自動的に作成します。

基本 crashinfo ファイル

この基本ファイルに保存される情報は、障害が発生した Cisco IOS イメージの名前、バージョン、プロセッサ レジスタのリスト、および他のスイッチ特有の情報です。**show tech-support** 特権 EXEC コマンドを使用することによって、この情報をシスコのテクニカル サポート担当者に提供できます。

基本 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。

flash:/crashinfo/

ファイル名は crashinfo_*n* になります。*n* には一連の番号が入ります。

新しい crashinfo ファイルが作成されるたびに、前のシーケンス番号より大きいシーケンス番号が使用されるので、シーケンス番号が最大のファイルに、最新の障害が記述されています。タイムスタンプではなく、バージョン番号を使用するのは、スイッチにリアルタイム クロックが組み込まれていないからです。ファイル作成時にシステムが使用するファイル名を変更することはできません。ただし、ファイルが作成されてから、**rename** 特権 EXEC コマンドを使用して名前を変更することもできますが、**show tech-support** 特権 EXEC コマンドを実行しても、名前が変更されたファイルの内容は表示されません。**delete** 特権 EXEC コマンドを使用して crashinfo ファイルを削除できます。

最新の crashinfo ファイル（つまり、ファイル名の末尾のシーケンス番号が最大であるファイル）を表示する場合は、**show tech-support** 特権 EXEC コマンドを使用します。**more** 特権 EXEC コマンド、**copy** 特権 EXEC コマンドなど、ファイルのコピーまたは表示が可能な任意のコマンドを使用して、ファイルにアクセスすることもできます。

拡張 crashinfo ファイル

スイッチは、システム障害の発生時に拡張 crashinfo ファイルを作成します。拡張ファイルに保存される情報は、スイッチの障害となった原因を特定するのに役立つ追加情報です。このファイルに手動でアクセスし、**more** または **copy** 特権 EXEC コマンドを使用すると、シスコのテクニカル サポート担当者にこの情報を提供できます。

拡張 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。

flash:/crashinfo_ext/

ファイル名は crashinfo_ext_*n* になります。*n* には一連の番号が入ります。

no exception crashinfo グローバル コンフィギュレーション コマンドを使用すると、スイッチが拡張 crashinfo ファイルを作成しないように設定できます。

CPU 使用率

ここでは、CPU 利用の過重が原因で起こりうる問題の症状を一覧し、CPU 使用率の問題の検証方法について説明します。表 47-1 は、CPU 使用率に関する特定可能な主な問題を一覧しています。この表には、考えられる原因と修正措置が示してあり、それぞれに Cisco.com の『*Troubleshooting High CPU Utilization*』へのリンクが張られています。

CPU 使用率が高すぎることで次の症状が発生する可能性がありますが、他の原因で発生する場合もあります。

- スパニングツリー トポロジの変更
- 通信が切断されたために EtherChannel リンクがダウンした
- 管理要求（ICMP ping、SNMP のタイムアウト、低速な Telnet または SSH セッション）に応答できない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA の失敗
- スイッチが要求を転送しない、または要求に応答しない場合の DHCP または IEEE 802.1x の処理の失敗

CPU 使用率が高くなる問題と原因

CPU 使用率が高いことが問題となっているかどうか判別するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行目にある下線が付いた部分に注目してください。

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

この例は、正常な CPU 使用率を示しています。この出力によると、最後の 5 秒間の使用率が *8%/0%* となっていますが、この意味は次のとおりです。

- Cisco IOS の処理時間と割り込みの処理にかかった時間を合わせた CPU の合計の使用率は全体の 8%

- 割り込みの処理にかかった時間は全体の 0%

表 47-1　CPU 使用率に関する問題のトラブルシューティング

問題のタイプ	原因	修正措置
割り込みのパーセント値が合計の CPU 使用率の値とほぼ同程度に高い	CPU がネットワークから受信するパケット数が多すぎる。	ネットワーク パケットのソースを判別する。データの流れを遮断するか、スイッチの設定を変更します。「Analyzing Network Traffic」を参照してください。
割り込みの所要時間は最小限であったにもかかわらず CPU の合計使用率が 50% を超える	CPU 時間を過度に消費する Cisco IOS 処理が 1 つ以上存在する。これは通常、処理をアクティブ化するイベントによって始動されます。	異常なイベントを特定して根本的な原因を解消します。「Debugging Active Processes」を参照してください。

- CPU 使用率の詳細および使用率の問題を解決する方法については、Cisco.com の『*Troubleshooting High CPU Utilization*』を参照してください。

トラブルシューティング方法

ソフトウェア障害からの回復

スイッチ ソフトウェアが破損する状況としては、アップグレードを行った場合、スイッチに誤ったファイルをダウンロードした場合、イメージ ファイルを削除した場合などが考えられます。いずれの場合にも、スイッチは電源投入時自己診断テスト（POST）に失敗し、接続できなくなります。

次の手順では、XMODEM プロトコルを使用して、破損したイメージ ファイルまたは間違ったイメージ ファイルを回復します。XMODEM プロトコルをサポートするソフトウェア パッケージは多数あり、使用するエミュレーション ソフトウェアによって、この手順は異なります。

ここで紹介する回復手順を実行するには、スイッチを直接操作する必要があります。

ステップ 1　PC 上で、Cisco.com から tar 形式のソフトウェア イメージ ファイル（*image_filename.tar*）をダウンロードします。

Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルとして格納されます。Cisco.com 上のソフトウェア イメージ ファイルの検索方法については、リリース ノートを参照してください。

ステップ 2　tar ファイルから bin ファイルを抽出します。

- Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して bin ファイルを特定し、抽出します。
- UNIX を使用している場合は、次の手順に従ってください。
  1. **tar -tvf** <*image_filename.tar*> UNIX コマンドを使用して、tar ファイルの内容を表示します。

     ```
     switch% tar -tvf image_filename.tar
     ```
  2. **tar -xvf** <*image_filename.tar*> <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルを特定し、抽出します。

     ```
     switch% tar -xvf image_filename.tar image_filename.binx

     x image_name.bin, 3970586 bytes, 7756 tape blocks
     ```

3. **ls -l** <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。

```
switch% ls -l image_filename.bin-rwxr-xr-x   1 bschuett eng      6365325 May 19
13:03
<insert path for lan base image>

-rw-r--r--   1 boba      3970586 Apr 21 12:00 image_name.bin
```

ステップ 3　XMODEM プロトコルをサポートする端末エミュレーション ソフトウェアを備えた PC を、スイッチのコンソール ポートに接続します。

ステップ 4　エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 5　スイッチの電源コードを取り外します。

ステップ 6　[Express Setup] ボタンを押しながら、電源コードをスイッチに再接続します。

ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、[Express Setup] ボタンを放します。ソフトウェアに関する数行分の情報と指示が表示されます。

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software#

flash_init
load_helper
boot
```

ステップ 7　フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

ステップ 8　コンソール ポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 9　ヘルパー ファイルがある場合にはロードします。

```
switch: load_helper
```

ステップ 10　XMODEM プロトコルを使用して、ファイル転送を開始します。

```
switch: copy xmodem: flash:image_filename.bin
```

ステップ 11　XMODEM 要求が表示されたら、端末エミュレーション ソフトウェアに適切なコマンドを使用して、転送を開始し、ソフトウェア イメージをフラッシュ メモリにコピーします。

ステップ 12　新規にダウンロードされた Cisco IOS イメージを起動します。

```
switch:boot flash:image_filename.bin
```

ステップ 13　**archive download-sw** 特権 EXEC コマンドを使用して、スイッチにソフトウェア イメージをダウンロードします。

ステップ 14　**reload** 特権 EXEC コマンドを使用してスイッチを再起動し、新しいソフトウェア イメージが適切に動作していることを確認します。

ステップ 15　スイッチから、flash:*image_filename.bin* ファイルを削除します。

パスワードを忘れた場合の回復

パスワードを忘れた場合は、スイッチのパスワードを削除して新しく設定できます。

手順を開始する前に、次の点を確認してください。

- スイッチに物理的にアクセスできること。
- イネーブルになっていて装置に接続されていないスイッチ ポートが 1 つ以上あること。

スイッチのパスワードを削除して新しく設定するには、次の手順を実行します。

ステップ 1　SETUP LED がグリーンに点滅し、使用可能なスイッチ ダウンリンク ポートの LED がグリーンに点滅するまで、[Express Setup] ボタンを押し続けます。

PC またはラップトップの接続に使用できるスイッチ ダウンリンク ポートの空きがない場合は、いずれかのスイッチ ダウンリンク ポートから装置を接続解除します。もう一度、SETUP LED とポートの LED がグリーンに点滅するまで [Express Setup] ボタンを押し続けます。

ステップ 2　LED がグリーンに点滅しているポートに、PC またはラップトップを接続します。

SETUP LED とスイッチ ダウンリンク ポートの LED が点滅を中止し、グリーンに点灯します。

ステップ 3　[Express Setup] ボタンを押し続けます。SETUP LED が再度グリーンに点滅し始めます。SETUP LED がグリーンに点灯するまで（約 5 秒間）、ボタンを押したままにします。すぐに [Express Setup] ボタンを放します。

この手順によって、他の設定に影響を与えることなく、パスワードが削除されます。これで、パスワードを入力せずに、コンソール ポートまたはデバイス マネージャからスイッチにアクセスできるようになりました。

ステップ 4　デバイス マネージャの [Express Setup] ウィンドウを使用するか、コマンドライン インターフェイスで **enable secret** グローバル コンフィギュレーション コマンドを使用して、新しいパスワードを入力します。

クラスタ メンバ スイッチとの接続の回復

構成によっては、コマンド スイッチとメンバ スイッチ間の接続を維持できない場合があります。メンバに対する管理接続を維持できなくなった場合で、かつ、メンバ スイッチが正常にパケットを転送している場合は、次の矛盾がないかどうかを確認してください。

- メンバ スイッチ（Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ）は、ネットワーク ポートとして定義されたポートを介してコマンド スイッチに接続することはできません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 メンバ スイッチは、同じ管理 VLAN に所属するポートを介してコマンド スイッチに接続する必要があります。
- セキュア ポートを介してコマンド スイッチに接続するメンバ スイッチ（Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ）は、セキュリティ違反が原因でポートがディセーブルになった場合、接続不能になることがあります。

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネット間でルーティングされるように IP ルーティングを設定する必要があります。詳細については、第 41 章「スタティック IP ユニキャスト ルーティングの設定」を参照してください。

IP ルーティングは、デフォルトではすべてのスイッチでディセーブルになります。IP ルーティングをイネーブルにする場合、または設定する必要がある場合は、第 41 章「スタティック IP ユニキャスト ルーティングの設定」を参照してください。

スイッチからネットワーク上の別のデバイスに ping を実行するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
ping ip *host* | *address*	IP またはホスト名やネットワーク アドレスを指定してリモート ホストへ ping を実行します。

（注）　**ping** コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

次に、IP ホストに ping を実行する例を示します。

```
Switch# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

表 47-2 で、ping の文字出力について説明します。

表 47-2　ping の出力表示文字

文字	説明
!	感嘆符 1 個につき 1 回の応答を受信したことを示します。
.	ピリオド 1 個につき応答待ちの間にネットワーク サーバのタイムアウトが 1 回発生したことを示します。
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス（デフォルトでは Ctrl+^ X）を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

IP traceroute の実行

ネットワーク上でパケットが通過するパスを追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
traceroute ip *host*	ネットワーク上でパケットが通過するパスを追跡します。

（注）　**traceroute** 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

次に、IP ホストに **traceroute** を実行する例を示します。

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

  1 172.2.52.1 0 msec 0 msec 4 msec
  2 172.2.1.203 12 msec 8 msec 0 msec
  3 171.9.16.6 4 msec 0 msec 0 msec
  4 171.9.4.5 0 msec 4 msec 0 msec
  5 171.9.121.34 0 msec 4 msec 4 msec
  6 171.9.15.9 120 msec 132 msec 128 msec
  7 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

ディスプレイには、送信される 3 つのプローブごとに、ホップ カウント、ルータの IP アドレス、およびラウンドトリップ タイム（ミリ秒単位）が表示されます。

表 47-3　traceroute の出力表示文字

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセス リストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	発信元。
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトでは Ctrl+^ X）を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

TDR の実行および結果の表示

TDR を実行する場合、**test cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを実行します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを実行します。出力フィールドの説明に関しては、このリリースに対応するコマンド リファレンスを参照してください。

特定機能に関するデバッグのイネーブル化

注意　デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。たとえば、スイッチド ポート アナライザ（SPAN）に対するデバッグをイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# debug span-session
```

スイッチは **no** 形式のコマンドが入力されるまで、出力を生成し続けます。

debug コマンドをイネーブルにしても、出力が表示されない場合は、次の状況が考えられます。

- モニタするトラフィック タイプを生成するようにスイッチが正しく設定されていない可能性があります。**show running-config** コマンドを使用して、設定を確認してください。
- スイッチが正しく設定されていても、デバッグがイネーブルである間にモニタすべきタイプのトラフィックを生成しないことがあります。デバッグする機能によっては、TCP/IP の **ping** コマンドなどを使用すると、ネットワーク トラフィックを生成できます。

SPAN のデバッグをディセーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# no debug span-session
```

また、特権 EXEC モードで **undebug** 形式のコマンドを入力することもできます。

```
Switch# undebug span-session
```

各デバッグ オプションのステートを表示するには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# show debugging
```

システム全体診断のイネーブル化

システム全体診断をイネーブルにするには、特権 EXEC モードで、次のコマンドを入力します。

```
Switch# debug all
```

注意　デバッグ出力は他のネットワーク トラフィックより優先され、**debug all** 特権 EXEC コマンドは他の **debug** コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。状況にかかわらず、特定性の高い **debug** コマンドを使用するのが原則です。

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

デバッグおよびエラー メッセージ出力のリダイレクト

ネットワーク サーバはデフォルトで、**debug** コマンドおよびシステム エラー メッセージの出力をコンソールに送信します。このデフォルトの設定を使用する場合は、コンソール ポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニタできます。

指定できる宛先として、コンソール、仮想端末、内部バッファ、および syslog サーバを実行している UNIX ホストがあります。Syslog フォーマットは、4.3 BSD UNIX およびそのバリエーションと互換性があります。

（注）　デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。コンソールでメッセージ ロギングを行うと、オーバーヘッドが非常に大きくなりますが、仮想端末でメッセージ ロギングを行うと、オーバーヘッドが小さくなります。Syslog サーバでメッセージ ロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システム メッセージ ロギングの詳細については、第 35 章「システム メッセージ ロギングの設定」を参照してください。

情報のモニタリング

物理パス

次のいずれかの特権 EXEC コマンドを使用して、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを表示できます。

- **tracetroute mac** [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]
- **tracetroute mac ip** {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

詳細については、このリリースのコマンド リファレンスを参照してください。

SFP モジュール ステータス

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理または動作ステータスを確認できます。このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現状などの動作ステータスと、アラーム ステータスを表示します。また、このコマンドを使用して SFP モジュールの速度およびデュプレックス設定も確認できます。詳細については、このリリースのコマンド リファレンスに記載された「**show interfaces transceiver**」コマンドの説明を参照してください。

トラブルシューティングの例

show platform forward コマンド

show platform forward 特権 EXEC コマンドの出力からは、インターフェイスに入るパケットがシステムを介して送信された場合、転送結果に関して、有意義な情報がいくつか得られます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポート マップ、ビットマップ、および出力側の情報が表示されます。

このコマンドで出力される情報のほとんどは、主に、スイッチの特定用途向け集積回路（ASIC）に関する詳細情報を使用するテクニカル サポート担当者に役立つものです。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

次に、VLAN 5 のポート 1 に入るパケットが、不明な MAC アドレスにアドレス指定されている場合の **show platform forward** コマンドの出力例を示します。パケットは VLAN 5 内のその他のすべてのポートに対してフラッディングされなければなりません。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2
udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050002_00020002-00_00000000_00000000     00C71   0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

========================================
Egress:Asic 2, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/1    0005 0001.0001.0001  0002.0002.0002

----------------------------------------
Packet 2
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/1    0005 0001.0001.0001  0002.0002.0002
```

```
----------------------------------------
<output truncated>
----------------------------------------
Packet 10
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000
Packet dropped due to failed DEJA_VU Check on Gi1/0/2
Packet dropped due to failed DEJA_VU Check on Gi1/2
```

次に、VLAN 5 のポート 1 に着信するパケットを、VLAN 上の別のポートで学習済みのアドレスに送信する場合の出力例を示します。パケットは、アドレスを学習したポートから転送する必要があります。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                   Key-Used                    Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050009_43A80145-00_00000000_00000000     00086   02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003

========================================
Egress:Asic 3, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port            Vlan      SrcMac          DstMac    Cos  Dscpv
interface-id    0005 0001.0001.0001  0009.43A8.0145
```

次に、VLAN 5 内のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが不明である場合の出力例を示します。デフォルト ルートが設定されていないため、パケットはドロップされます。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                   Key-Used                    Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_0D020202     010F0   01880290
L3Scndr  12_0D020202_0D010101-00_40000014_000A0000     034E0   000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000
```

次に、VLAN 5 内のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが IP ルーティング テーブル内の IP アドレスに設定されている場合の出力例を示します。パケットはルーティング テーブルの指定どおりに転送されます。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
```

```
 Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_10010A05_0A010505-00_41000014_000A0000      01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_10010A05      010F0   01880290
L3Scndr  12_10010A05_0A010505-00_40000014_000A0000      01D28   30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

========================================
Egress:Asic 3, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000      01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/2    0007 XXXX.XXXX.0246  0009.43A8.0147
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
その他のトラブルシューティング情報	*ハードウェア インストレーション ガイド*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

APPENDIX A

Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作

この付録では、スイッチのフラッシュ ファイル システムの操作方法、コンフィギュレーション ファイルのコピー方法、スイッチにソフトウェア イメージをアーカイブ（アップロードおよびダウンロード）する方法について説明します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、Cisco.com でこのリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Configuration Fundamentals Command Reference, Release 15.0*』を参照してください。

フラッシュ ファイル システムの操作

フラッシュ ファイル システムは、ファイルを格納できる単一のフラッシュ デバイスです。ソフトウェア イメージおよびコンフィギュレーション ファイルの管理に役立つ複数のコマンドも備えています。スイッチのデフォルトのフラッシュ ファイル システムは *flash:* です。

スイッチには、Cisco IOS ソフトウェアのイメージおよびコンフィギュレーション ファイルを格納するリムーバブル コンパクト フラッシュ カードがあります。コンパクト フラッシュ カードを取り外しても、Cisco IOS ソフトウェアのリロードが必要にならない限り、スイッチ動作は中断されません。ただし、コンパクト フラッシュ カードを取り外すと、フラッシュ ファイル システムにアクセスできなくなり、アクセスを試みるとエラー メッセージが生成されます。

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

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

スイッチのコンパクト フラッシュ メモリ カードの取り外しまたは交換方法については、*ハードウェア インストレーション ガイド*を参照してください。

使用可能なファイル システムの表示

スイッチで使用可能なファイル システムを表示するには、**show file systems** 特権 EXEC コマンドを使用します（次の例を参照）。

```
Switch# show file systems

File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     ro   bs:
*  134086656   117346304     flash     rw   flash:
           -           -    opaque     rw   system:
           -           -    opaque     rw   tmpsys:
      524288      518334     nvram     rw   nvram:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -    opaque     rw   null:
           -           -    opaque     ro   tar:
           -           -   network     rw   tftp:
           -           -   network     rw   rcp:
           -           -   network     rw   http:
           -           -   network     rw   ftp:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:

Switch#
```

サポートされていない SD フラッシュ メモリ カードの検出

スイッチを開始したときに、サポートされていないセキュア デジタル（SD）フラッシュ メモリ カードが検出されたか、またはスイッチの実行中にサポートされていない SD フラッシュ メモリ カードを挿入すると、次の警告メッセージが表示されます。

```
WARNING: Non-IT SD flash detected.Use of this card during normal
         operation can impact and severely degrade performance of the system.
          Please use supported SD flash cards only.
```

画面に SD フラッシュ メモリ カードに関する情報を表示するには、**show platform sdflash** 特権 EXEC コマンドを使用します。

次の例は、サポートされていない SD フラッシュ メモリ カードを示しています。

```
Switch# show platform sdflash
SD Flash Manufacturer      : SMART MODULAR (ID=27h) - Non IT
         Size              : 485MB
         Serial number     : B01000A5
         Revision          : 2.0
         Manufacturing date: 12/2009
```

次の例は、サポートされている SD フラッシュ メモリ カードを示しています。

```
Switch# show platform sdflash
```

```
SD Flash Manufacturer      : SMART MODULAR (ID=27h)
         Size                           : 972MB
         Serial number         : 07000019
         Revision                    : 2.0
         Manufacturing date: 3/2010
```

（注）　**show platform sdflash** 特権 EXEC コマンドを入力したときに表示される名前、日付、およびその他のフィールドは、SD フラッシュ メモリ カードの製造元によって異なります。ただし、その SD フラッシュ メモリ カードがサポートされていない場合、製造元の名前の後に「Non IT」が表示されます。

（注）　**show platform sdflash** 特権 EXEC コマンドの出力は、**show tech-support** 特権 EXEC コマンドの出力にも含まれます。

SD フラッシュ メモリ カード LED

表 A-1　　SD フラッシュ メモリ カード LED

色	システム ステータス
Off/ グリーンで点滅	SD フラッシュ メモリ カードが動作中に遷移します。
オレンジでゆっくり点滅	SD フラッシュ メモリ カードはサポートされていません。
オレンジですばやく点滅	SD フラッシュ メモリ カードがありません。
オレンジ	SD フラッシュ メモリ カードへのアクセス エラー。 Cisco IOS ブート イメージが見つかりませんでした。
グリーン	SD フラッシュ メモリ カードが機能しています。

デフォルト ファイル システムの設定

表 A-2　　show file systems フィールドの説明

フィールド	値
Size(b)	ファイル システムのメモリ サイズ（バイト単位）です。
Free(b)	ファイル システムの空きメモリ サイズ（バイト単位）です。

表 A-2　show file systems フィールドの説明 （続き）

フィールド	値
Type	ファイル システムのタイプです。 **flash**：ファイル システムはフラッシュ メモリ デバイス用です。 **nvram**：ファイル システムは NVRAM（不揮発性 RAM）デバイス用です。 **opaque**：ファイル システムはローカルに生成された *pseudo* ファイル システム（*system* など）、または brimux などのダウンロード インターフェイスです。 **unknown**：ファイル システムのタイプは不明です。
Flags	ファイル システムの権限です。 **ro**：読み取り専用です。 **rw**：読み取り / 書き込みです。 **wo**：書き込み専用です。
Prefixes	ファイル システムのエイリアスです。 **flash:**：フラッシュ ファイル システムです。 **nvram:**：NVRAM です。 **null:**：コピーのヌル宛先です。リモート ファイルをヌルへコピーして、サイズを判別できます。 **rcp:**：Remote Copy Protocol（RCP）ネットワーク サーバです。 **system:**：実行コンフィギュレーションを含むシステム メモリが格納されています。 **tftp:**：TFTP ネットワーク サーバです。 **xmodem:**：XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。 **ymodem:**：YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。

デフォルトのファイル システムとして使用されるファイル システムまたはディレクトリを指定するには、**cd** *filesystem:* 特権 EXEC コマンドを使用します。デフォルト ファイル システムを設定すると、関連するコマンドを実行するときに *filesystem:* 引数を省略できます。たとえば、オプションの *filesystem:* 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは *flash:* です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

ファイル システム上のファイル情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコンフィギュレーション ファイルが格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマンドで使用できます。

ファイル システムのファイルに関する情報を表示するには、表 A-3 に記載された特権 EXEC コマンドのいずれかを使用します。

表 A-3　ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [**/all**] [*filesystem***:**][*filename*]	ファイル システムのファイル リストを表示します。
show file systems	ファイル システムのファイルごとの詳細を表示します。
show file information *file-url*	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイルの記述子リストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

ディレクトリの変更および作業ディレクトリの表示

ディレクトリの変更や、作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 *filesystem***:** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。
ステップ 2	**cd new_configs**	目的のディレクトリに変更します。 コマンド例では、*new_configs* という名前のディレクトリに変更する方法を示します。
ステップ 3	**pwd**	作業ディレクトリを表示します。

ディレクトリの作成および削除

特権 EXEC モードを開始して、ディレクトリを作成および削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 *filesystem***:** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。
ステップ 2	**mkdir old_configs**	新しいディレクトリを作成します。 コマンド例では、*old_configs* という名前のディレクトリの作成方法を示します。 ディレクトリ名では、大文字と小文字が区別されます。 スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。
ステップ 3	**dir** *filesystem***:**	入力を確認します。

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、**delete /force/recursive** *filesystem***:/***file-url* 特権 EXEC コマンドを使用します。

名前で指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

filesystem には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。*file-url* には、削除するディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

注意　ファイルおよびディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

送信元から宛先にファイルをコピーするには、**copy** *source-url destination-url* 特権 EXEC コマンドを使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドを実行すると、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存され、システム初期化中のコンフィギュレーションとして使用されます。

XMODEM または YMODEM プロトコルを使用するネットワーク マシンのファイルに対する送信元として特殊なファイル システム（**xmodem:**、**ymodem:**）を指定し、そこからコピーすることもできます。

ネットワーク ファイル システムの URL には、**ftp:**、**rcp:**、**tftp:** などがあります。構文は次のとおりです。

- FTP：**ftp:**[[*//username* [**:***password*]**@***location*]*/directory*]*/filename*
- RCP：**rcp:**[[*//username***@***location*]*/directory*]*/filename*
- TFTP：**tftp:**[[*//location*]*/directory*]*/filename*

ローカルにある書き込み可能なファイル システムには flash: などがあります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスへ（たとえば、**copy flash: flash:** コマンドは無効）

コンフィギュレーション ファイルによる **copy** コマンドの具体的な使用例については、「コンフィギュレーション ファイルの操作」（P.A-9）を参照してください。

新しいバージョンをダウンロードするか、または既存のバージョンをアップロードして、ソフトウェア イメージをコピーするには、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドを使用します。詳細については、「ソフトウェア イメージの操作」（P.A-24）を参照してください。

ファイルの削除

フラッシュ メモリ デバイスのファイルが不要になった場合は、そのファイルを永久に削除できます。指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、**delete** [**/force**] [**/recursive**] [*filesystem***:**]*/file-url* 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

*filesystem***:** オプションを省略すると、**cd** コマンドで指定したデフォルトのデバイスが使用されます。*file-url* には、削除するファイルのパス（ディレクトリ）および名前を指定します。

ファイルを削除しようとすると、削除の確認を求めるプロンプトが表示されます。

注意　ファイルが削除された場合、その内容は回復できません。

次に、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する例を示します。

```
Switch# delete myconfig
```

tar ファイルの作成、表示、および抽出

tar ファイルを作成してそこにファイルを書き込んだり、tar ファイル内のファイルをリスト表示したり、tar ファイルからファイルを抽出したりできます（次の項を参照）。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

tar ファイルの作成

tar ファイルを作成してそこにファイルを書き込むには、次の特権 EXEC コマンドを使用します。

archive tar/create *destination-url* **flash:***/file-url*

destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:
- FTP の場合の構文は次のとおりです。
  ftp:[[*//username*[**:***password*]**@***location*]*/directory*]*/tar-filename***.tar**
- RCP の場合の構文は次のとおりです。
  rcp:[[*//username***@***location*]*/directory*]*/tar-filename***.tar**
- TFTP の場合の構文は次のとおりです。
  tftp:[[*//location*]*/directory*]*/tar-filename***.tar**

*tar-filename***.tar** は、作成する tar ファイルです。

flash:/*file-url* には、新しい tar ファイルの作成元になる、ローカル フラッシュ ファイル システム上の場所を指定します。送信元ディレクトリ内に格納されているオプションのファイルまたはディレクトリのリストを指定して、新しい tar ファイルに書き込むこともできます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

次の例では、tar ファイルを作成する方法を示します。次のコマンドを実行すると、ローカルなフラッシュデバイスのディレクトリ *new-configs* の内容が、172.20.10.30 にある TFTP サーバ上のファイル *saved.tar* に書き込まれます。

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

tar ファイルの内容の表示

画面に tar ファイルの内容を表示するには、次の特権 EXEC コマンドを使用します。

archive tar/table *source-url*

source-url には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:
- FTP の場合の構文は次のとおりです。
  ftp:[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar**
- RCP の場合の構文は次のとおりです。
  rcp:[[//*username***@***location*]/*directory*]/*tar-filename***.tar**
- TFTP の場合の構文は次のとおりです。
  tftp:[[//*location*]/*directory*]/*tar-filename***.tar**

*tar-filename***.tar** は、表示する tar ファイルです。

tar ファイルの後ろにオプションのファイルまたはディレクトリ リストを指定して、表示するファイルを制限することもできます。リストを指定すると、リスト内のファイルのみが表示されます。何も指定しないと、すべてのファイルおよびディレクトリが表示されます。

次に、フラッシュ メモリ内にあるスイッチ tar ファイルの内容を表示する例を示します。

```
Switch# archive tar /table flash:image-name.tar
image-name/ (directory)
image-name/html/ (directory)
image-name/html/file.html (0 bytes)
image-name/image-name.bin (610856 bytes)
image-name/info (219 bytes)
```

次の例では、*/html* ディレクトリおよびその内容だけを表示する方法を示します。

```
Switch# archive tar /table flash: image-name/html
cimage-name/html
cimage-name/html/ (directory)
cimage-name/html/const.htm (556 bytes)
cimage-name/html/xhome.htm (9373 bytes)
cimage-name/html/menu.css (1654 bytes)
<output truncated>
```

tar ファイルの抽出

tar ファイルをフラッシュ ファイル システム上のディレクトリに抽出するには、次の特権 EXEC コマンドを使用します。

archive tar/xtract *source-url* **flash:**/*file-url* [*dir/file...*]

source-url には、ローカル ファイル システムの送信元 URL のエイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:
- FTP の場合の構文は次のとおりです。
  ftp:[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar**
- RCP の場合の構文は次のとおりです。
  rcp:[[//*username***@***location*]/*directory*]/*tar-filename***.tar**
- TFTP の場合の構文は次のとおりです。
  tftp:[[//*location*]/*directory*]/*tar-filename***.tar**

*tar-filename***.tar** は、ファイルの抽出元の tar ファイルです。

flash:/*file-url* [*dir/file...*] には、tar ファイルが抽出されるローカル フラッシュ ファイル システムの場所を指定します。tar ファイルから抽出されるファイルまたはディレクトリのオプション リストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

次に、172.20.10.30 の TFTP サーバ上にある tar ファイルの内容を抽出する例を示します。ここでは、ローカル フラッシュ ファイル システムのルート ディレクトリに単に *new-configs* ディレクトリを抽出しています。*saved.tar* ファイルの残りのファイルは無視されます。

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

ファイルの内容の表示

リモート ファイル システム上のファイルを含めて、読み取り可能ファイルの内容を表示するには、**more** [**/ascii** | **/binary** | **/ebcdic**] *file-url* 特権 EXEC コマンドを使用します。

次に、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示する例を示します。

```
Switch# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

コンフィギュレーション ファイルの操作

ここでは、コンフィギュレーション ファイルの作成、ロード、およびメンテナンスの手順について説明します。

コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力されたコマンドが格納されています。基本的なコンフィギュレーション ファイルを作成するには、**setup** プログラムを使用するか、または **setup** 特権 EXEC コマンドを使用します。詳細については、第 4 章「スイッチ セットアップの設定」を参照してください。

TFTP、FTP、または RCP サーバから、スイッチの実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにコンフィギュレーション ファイルをコピー（*ダウンロード*）できます。次のいずれかの目的でこの操作が必要になります。

- バックアップ コンフィギュレーション ファイルを復元するため。
- コンフィギュレーション ファイルを別のスイッチに使用するため。たとえば、ネットワークに別のスイッチを追加して、元のスイッチと同じ設定にできます。ファイルを新しいスイッチにコピーすると、ファイル全体を再作成しないで、関連部分を変更できます。
- すべてのスイッチのコンフィギュレーションが同じになるように、ネットワーク内のすべてのスイッチに同じコンフィギュレーション コマンドをロードするため。

スイッチからファイル サーバにコンフィギュレーション ファイルをコピー（*アップロード*）するには、TFTP、FTP、または RCP を使用します。内容を変更する前に、現在のコンフィギュレーション ファイルをサーバにバックアップしておくと、後でサーバから元のコンフィギュレーション ファイルを復元できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成すると、スイッチを設定するときに役立ちます。コンフィギュレーション ファイルには、1 台または複数のスイッチを設定する場合に必要となるコマンドの一部、またはすべてを格納できます。たとえば、同じハードウェア構成の複数のスイッチに、同じコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- スイッチを最初に設定する場合、コンソール ポートから接続することを推奨します。コンソール ポートとの直接接続ではなく、ネットワーク接続を介してスイッチにアクセスする場合は、設定の変更によっては（スイッチの IP アドレスの変更やポートのディセーブル化など）、スイッチとの接続が切断される可能性があることにご注意ください。
- スイッチにパスワードが設定されていない場合は、**enable secret** *secret-password* グローバル コンフィギュレーション コマンドを使用して、パスワードを設定することを推奨します。

（注）　**copy** {**ftp: | rcp: | tftp:**} **system:running-config** 特権 EXEC コマンドを実行すると、コマンドラインにコマンドを入力した場合と同様に、スイッチにコンフィギュレーション ファイルがロードされます。コマンドを追加するまで、既存の実行コンフィギュレーションは消去されません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内のコマンドの中には、置き換えたり無効にしたりできないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わされた（コピーされたコンフィギュレーション ファイルが優先する）コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルを復元して、サーバに保存されたファイルの正確なコピーを作成す

るには、コンフィギュレーション ファイルを直接スタートアップ コンフィギュレーションにコピーして（**copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** 特権 EXEC コマンドを使用）、スイッチを再起動します。

コンフィギュレーション ファイルのタイプおよび場所

スタートアップ コンフィギュレーション ファイルは、ソフトウェアを設定するために、システムの起動中に使用されます。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が格納されています。2 つのコンフィギュレーション ファイルは別々の設定にできます。たとえば、一時的に設定を変更しなければならない場合があります。この場合は、実行コンフィギュレーションを変更した後、**copy running-config startup-config** 特権 EXEC コマンドによる設定の保存は行わないようにします。

実行コンフィギュレーションは DRAM に保存されますが、スタートアップ コンフィギュレーションはフラッシュ メモリの NVRAM セクションに保存されます。

テキスト エディタによるコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成する場合は、システムが適切に応答できるように、コマンドを論理的に並べる必要があります。次に、コンフィギュレーション ファイルの作成方法の一例を示します。

ステップ 1　スイッチからサーバに既存のコンフィギュレーションをコピーします。

詳細については、「TFTP によるコンフィギュレーション ファイルのダウンロード」（P.A-12）、「FTP によるコンフィギュレーション ファイルのダウンロード」（P.A-15）、または「RCP によるコンフィギュレーション ファイルのダウンロード」（P.A-18）を参照してください。

ステップ 2　UNIX の vi または emacs、PC のメモ帳などのテキスト エディタで、コンフィギュレーション ファイルを開きます。

ステップ 3　目的のコマンドが格納されたコンフィギュレーション ファイルの一部を抽出して、新しいファイルに保存します。

ステップ 4　コンフィギュレーション ファイルをサーバ内の適切な場所にコピーします。たとえば、ファイルをワークステーションの TFTP ディレクトリ（UNIX ワークステーションの場合は、通常は /tftpboot）にコピーします。

ステップ 5　ファイルに関する権限が world-read に設定されていることを確認します。

TFTP によるコンフィギュレーション ファイルのコピー

作成したコンフィギュレーション ファイルを使用してスイッチを設定したり、別のスイッチからダウンロードしたり、TFTP サーバからダウンロードできます。また、コンフィギュレーション ファイルを TFTP サーバにコピー（アップロード）して、格納できます。

TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  （注）　/etc/inetd.conf および /etc/services ファイルを変更した後に、inetd デーモンを再起動する必要があります。このデーモンを再起動するには、inetd プロセスを終了して再起動するか、または **fastboot** コマンド（SunOS 4.x の場合）や **reboot** コマンド（Solaris 2.x または SunOS 5.x の場合）を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするコンフィギュレーション ファイルが TFTP サーバ上の正しいディレクトリ内にあることを確認します（UNIX ワークステーションの場合は、通常 /tftpboot）。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。
- コンフィギュレーション ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* は、サーバにアップロードするときに使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル（空のファイルを作成する必要があった場合は、空のファイルを含む）を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

ステップ 1　コンフィギュレーション ファイルをワークステーションの適切な TFTP ディレクトリにコピーします。

ステップ 2　「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-12）を参照して、TFTP サーバが適切に設定されていることを確認します。

ステップ 3　コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

ステップ 4　TFTP サーバからコンフィギュレーション ファイルをダウンロードして、スイッチを設定します。

TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **system:running-config**
- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **nvram:startup-config**

このコンフィギュレーション ファイルを実行すると、ダウンロードが実行され、ファイルが行単位で解析されてコマンドが実行されます。

次に、IP アドレス 172.16.2.155 上にあるファイル *tokyo-confg* からソフトウェアを設定する例を示します。

```
Switch# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

TFTP によるコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして格納するには、次の手順を実行します。

ステップ 1　「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-12）を参照して、TFTP サーバが適切に設定されていることを確認します。

ステップ 2　コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

ステップ 3　スイッチのコンフィギュレーションを TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy system:running-config tftp:**[[[*//location*]*/directory*]*/filename*]
- **copy nvram:startup-config tftp:**[[[*//location*]*/directory*]*/filename*]

TFTP サーバにファイルがアップロードされます。

次に、スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードする例を示します。

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [OK]
```

FTP によるコンフィギュレーション ファイルのコピー

FTP サーバから、または FTP サーバに、コンフィギュレーション ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してコンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- anonymous

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）
- スイッチが作成した *username@switchname.domain* パスワード。変数 *username* は現在のセッションに関連付けられているユーザ名、*switchname* は設定されているホスト名、*domain* はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリに置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して、すべてのコピー処理中に使用する新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

- コンフィギュレーション ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、FTP サーバを適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-14）を参照して、FTP サーバが適切に設定されていることを確認します。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**configure terminal**	スイッチ上で、グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] **system:running-config** または **copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] **nvram:startup-config**	FTP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-confg* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-confg* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスイッチのスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
```

```
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-14）を参照して、FTP サーバが適切に設定されていることを確認します。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy system:running-config ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] または **copy nvram:startup-config ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]	FTP を使用して、スイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定場所に格納します。

次に、実行コンフィギュレーション ファイル *switch2-confg* を、IP アドレスが 172.16.101.101 であるリモート ホスト上のディレクトリ *netadmin1* にコピーする例を示します。

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-confg
Write file switch2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをサーバに格納して、ファイルをコピーする例を示します。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
```

```
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

RCP によるコンフィギュレーション ファイルのコピー

リモート ホストとスイッチ間でコンフィギュレーション ファイルをダウンロード、アップロード、およびコピーするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは rsh をサポートするサーバにアクセスするだけですみます （ほとんどの UNIX システムは rsh をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。コンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、**username** コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スイッチのホスト名。

RCP コピー要求を正常に終了させるには、ネットワーク サーバ上にリモート ユーザ名用のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、rsh がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチとサーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、RCP サーバへの接続を確認します。

- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのコピー処理中に **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用し、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、そのユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。
- ファイルを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

このスイッチの IP アドレスを *Switch1.company.com* に変換する場合は、RCP サーバ上の User0 用の .rhosts ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-17）を参照して、RCP サーバが適切に設定されていることを確認します。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **system:running-config** または **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **nvram:startup-config**	RCP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-confg* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-confg* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-17）を参照して、RCP サーバが適切に設定されていることを確認します。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy system:running-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] または **copy nvram:startup-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]	RCP を使用して、コンフィギュレーション ファイルをスイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコピーします。

次に、実行コンフィギュレーション ファイル *switch2-confg* を、IP アドレスが 172.16.101.101 であるリモート ホスト上のディレクトリ *netadmin1* にコピーする例を示します。

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-confg
Write file switch-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバ上に格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

設定情報の消去

スタートアップ コンフィギュレーションから設定情報を消去できます。スタートアップ コンフィギュレーションを使用しないでスイッチを再起動すると、スイッチはセットアップ プログラムを開始し、新しい設定でスイッチを再設定できます。

スタートアップ コンフィギュレーション ファイルの消去

スタートアップ コンフィギュレーションを消去するには、**erase nvram:** または **erase startup-config** 特権 EXEC コマンドを使用します。

注意　削除されたスタートアップ コンフィギュレーション ファイルは復元できません。

格納されたコンフィギュレーション ファイルの削除

保存された設定をフラッシュ メモリから削除するには、**delete flash:***filename* 特権 EXEC コマンドを使用します。**file prompt** グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削除する前に確認を求めるプロンプトが表示されます。デフォルトでは、スイッチは、破壊的なファイル操作に関する確認をプロンプトで要求します。**file prompt** コマンドの詳細については、『*Cisco IOS Command Reference for Release 12.2*』を参照してください。

注意　削除されたファイルは復元できません。

コンフィギュレーションの交換またはロール バック

コンフィギュレーション交換およびロールバック機能を使用すると、実行コンフィギュレーションと保存されている任意の Cisco IOS コンフィギュレーション ファイルを交換できます。ロールバック機能を使用すると以前のコンフィギュレーションに戻すことができます。

コンフィギュレーションの交換およびロールバックの概要

コンフィギュレーションのアーカイブ

コンフィギュレーション アーカイブは、コンフィギュレーション ファイルのアーカイブを保管、構成、管理するメカニズムです。**configure replace** 特権 EXEC コマンドを使用すると、コンフィギュレーション ロールバック機能が向上します。または、**copy running-config** *destination-url* 特権 EXEC コマンドを使用して実行コンフィギュレーションのコピーを保存し、交換ファイルをローカルまたはリモートで保存することができます。ただし、この方法ではファイルの自動管理を行うことはできません。コンフィギュレーション交換およびロールバック機能を使用すれば、実行コンフィギュレーションのコピーを自動的にコンフィギュレーション アーカイブに保存できます。

archive config 特権 EXEC コマンドを使用して、コンフィギュレーションをコンフィギュレーション アーカイブに保存します。その際は標準のディレクトリとファイル名のプレフィックスが使用され、連続ファイルを保存するたびにバージョン番号（およびオプションでタイムスタンプ）が自動的に付加されます。このときのバージョン番号は 1 つずつ大きくなります。アーカイブに保存する実行コンフィギュレーションの数は指定することができます。保存したファイル数が指定数に達した場合は、次の新しいファイルを保存するときに最も古いファイルが自動的に削除されます。**show archive** 特権 EXEC コマンドを使用すると、コンフィギュレーション アーカイブに保存されたすべてのコンフィギュレーション ファイルを表示できます。

Cisco IOS コンフィギュレーション アーカイブでは、コンフィギュレーション ファイルを保存し、**configure replace** コマンドで使用します。ファイル システムは、FTP、HTTP、RCP、TFTP のいずれかです。

コンフィギュレーションの交換

configure replace 特権 EXEC コマンドを使用すると、実行コンフィギュレーションと保存されている任意のコンフィギュレーション ファイルを交換できます。**configure replace** コマンドを入力すると実行コンフィギュレーションと指定した交換コンフィギュレーションが比較され、コンフィギュレーションの差分が生成されます。生成された差分がコンフィギュレーションの交換に使用されます。コンフィギュレーション交換は、通常 3 回以下のパスで完了します。ループを防ぐために 6 回以上のパスが実行されることはありません。

copy *source-url* **running-config** 特権 EXEC コマンドを使用すると、保存されているコンフィギュレーション ファイルが実行コンフィギュレーションに保存できます。このコマンドを **configure replace** *target-url* 特権コマンドの代わりに使用する場合は、次のような違いがある点に注意してください。

- **copy** *source-url* **running-config** コマンドはマージ動作であり、コピー元ファイルと実行コンフィギュレーションのコマンドをすべて保存します。このコマンドでは、コピー元ファイルに実行コンフィギュレーションのコマンドがない場合でも実行コンフィギュレーションのコマンドを削除しません。**configure replace** *target-url* コマンドの場合は、交換先のファイルに実行コンフィギュレーションのコマンドがない場合は実行コンフィギュレーションから削除し、実行コンフィギュレーションにないコマンドがある場合はそのコマンドを追加します。
- **copy** *source-url* **running-config** コマンドのコピー元ファイルとして、部分コンフィギュレーション ファイルを使用できます。**configure replace** *target-url* コマンドの交換ファイルとして、完全なコンフィギュレーション ファイルを使用する必要があります。

コンフィギュレーションのロール バック

configure replace コマンドを使用して、前回コンフィギュレーションを保存した後で行った変更をロール バックさせることもできます。コンフィギュレーション ロールバック機能では、コンフィギュレーションを特定の変更時点に戻すのではなく、保存されているコンフィギュレーション ファイルに基づいて特定のコンフィギュレーションに戻します。

コンフィギュレーション ロールバック機能を利用する場合は、コンフィギュレーションを変更する前に実行コンフィギュレーションを保存する必要があります。その後、コンフィギュレーションを変更した後で **configure replace** *target-url* コマンドを使用し、保存したコンフィギュレーション ファイルを使って変更をロール バックします。

保存されている任意のファイルをロールバック コンフィギュレーションとして指定できます。一部のロールバック モデルと同様、ロールバック回数は無制限です。

設定時の注意事項

コンフィギュレーション交換およびロールバックを設定し実行する場合は、次の注意事項に従ってください。

- スイッチのメモリの空き容量が、2 つのコンフィギュレーション ファイル（実行コンフィギュレーションと保存されている交換コンフィギュレーション）の合計容量よりも大きいことを確認します。スイッチのメモリ容量の方が小さい場合、コンフィギュレーション交換は実行されません。
- また、スイッチにコンフィギュレーション交換やロールバック コンフィギュレーション コマンドが実行できるほどの空き容量があることも確認してください。
- ネットワーク デバイスの物理コンポーネント（物理インターフェイスなど）に関連するコンフィギュレーション コマンドを実行コンフィギュレーションに追加または削除することはできません。
  - インターフェイスがデバイス上に物理的に存在する場合、コンフィギュレーション交換を行っても実行コンフィギュレーションから **interface** *interface-id* コマンド行を削除することはできません。
  - インターフェイスがデバイス上に物理的に存在しない場合、**interface** *interface-id* コマンド行を実行コンフィギュレーションに追加することはできません。
- **configure replace** コマンドを使用する場合、保存されているコンフィギュレーションを実行コンフィギュレーションの交換コンフィギュレーション ファイルとして指定する必要があります。交換ファイルは Cisco IOS デバイスによって生成された完全なコンフィギュレーションであることが必要です（たとえば **copy running-config** *destination-url* コマンドで生成したコンフィギュレーション）。

（注） 交換コンフィギュレーション ファイルを外部に生成する場合、Cisco IOS デバイスで生成したファイルのフォーマットと一致する必要があります。

コンフィギュレーション アーカイブの設定

configure replace コマンドをコンフィギュレーション アーカイブおよび **archive config** コマンドとともに使用することは任意ですが、コンフィギュレーション ロールバックを行うときに大きな利点があります。**archive config** コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**archive**	アーカイブ コンフィギュレーション モードを開始します。
ステップ 3	**path** *url*	コンフィギュレーション アーカイブに、ファイルのディレクトリとファイル名プレフィックスを指定します。
ステップ 4	**maximum** *number*	（任意）コンフィギュレーション アーカイブに保存する実行コンフィギュレーションのアーカイブ ファイルの最大数を指定します。 *number*：コンフィギュレーション アーカイブでの実行コンフィギュレーション ファイルの最大数。有効な値は 1 ～ 14 で、デフォルトは 10 です。 **（注）** このコマンドを使用する前に **path** アーカイブ コンフィギュレーション コマンドを入力して、コンフィギュレーション アーカイブのファイルのディレクトリとファイル名プレフィックスを指定しておく必要があります。
ステップ 5	**time-period** *minutes*	（任意）コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を設定します。 *minutes*：コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブを自動保存する間隔を、分単位で指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

コンフィギュレーション交換またはロールバック動作の実行

実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**archive config**	（任意）実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。 **（注）** **path** アーカイブ コンフィギュレーション コマンドを入力してから、このコマンドを実行します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3		実行コンフィギュレーションに必要な変更を行います。
ステップ 4	**exit**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**configure replace** *target-url* [**list**] [**force**] [**time** *seconds*] [**nolock**]	実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換します。 *target-url*：保存されているコンフィギュレーション ファイルの URL（ファイル システムからアクセス可能）。実行コンフィギュレーションと交換するファイルで、ステップ 2 で **archive config** 特権 EXEC コマンドを使用して作成したコンフィギュレーション ファイルなどです。 **list**：コンフィギュレーション交換動作のパスごとにソフトウェア パーサーによって適用されるコマンド エントリのリストを表示します。パスの合計数も表示されます。 **force**：実行コンフィギュレーションファイルと指定した保存済みコンフィギュレーション ファイルの交換を確認なしで実行します。 **time** *seconds*：**configure confirm** コマンドを入力して実行コンフィギュレーション ファイルとの交換を確認するまでの時間を秒単位で指定します。指定時間内に **configure confirm** コマンドを入力しない場合、コンフィギュレーション交換動作が自動的に停止します（つまり、実行コンフィギュレーション ファイルは **configure replace** コマンドを入力する以前に存在していたコンフィギュレーションに保存されます）。 （注）　**time** *seconds* コマンドライン オプションを使用する前に、コンフィギュレーション アーカイブをイネーブルにしておく必要があります。 **nolock**：コンフィギュレーション交換動作時に他のユーザが実行コンフィギュレーションを変更できないようにする実行コンフィギュレーション ファイルのロックをディセーブルにします。
ステップ 6	**configure confirm**	（任意）実行コンフィギュレーションと保存されているコンフィギュレーション ファイルとの交換を確認します。 （注）　このコマンドは、**time** *seconds* キーワードと **configure replace** コマンドの引数が指定されている場合にだけ使用します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ソフトウェア イメージの操作

ここでは、システム ソフトウェア、Cisco IOS コード、および組み込みのデバイス マネージャ ソフトウェアを格納するソフトウェア イメージ ファイルをアーカイブ（ダウンロードおよびアップロード）する方法を示します。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

スイッチ ソフトウェアをアップグレードするには、TFTP、FTP、または RCP サーバからスイッチ イメージ ファイルをダウンロードします。TFTP サーバへアクセスできない場合、Web ブラウザ（HTTP）で PC またはワークステーションへ直接ソフトウェア イメージ ファイルをダウンロードします。次にデバイス マネージャまたは Cisco Network Assistant を使用してスイッチをアップグレードします。TFTP サーバまたは Web ブラウザ（HTTP）を使用したスイッチのアップグレードについては、リリース ノートを参照してください。

現在のイメージを新しいイメージで置き換えたり、ダウンロード後に現在のイメージをフラッシュ メモリに保存したりできます。

バックアップのために、スイッチ イメージ ファイルを TFTP、FTP、または RCP サーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。

（注）　ソフトウェア イメージ、およびサポートされているアップグレード パスの一覧については、スイッチに付属のリリース ノートを参照してください。

スイッチ上のイメージの場所

Cisco IOS イメージは、バージョン番号を表すディレクトリ内に *.bin* ファイルとして格納されます。サブディレクトリには、Web 管理に必要なファイルが格納されます。イメージはシステム ボードのフラッシュ メモリ（flash:）に格納されます。

show version 特権 EXEC コマンドを使用すると、スイッチで現在稼働しているソフトウェア バージョンを参照できます。画面上で、`System image file is...` で始まる行を調べます。この行は、イメージが格納されているフラッシュ メモリ内のディレクトリ名を示します。

dir *filesystem*: 特権 EXEC コマンドを使用して、フラッシュ メモリに格納されている他のソフトウェア イメージのディレクトリ名を調べることもできます。**archive download-sw /directory** 特権 EXE コマンドを使用して、各 tar ファイルに対してパス全体を指定する代わりに、ディレクトリの後ろにダウンロードする tar ファイルまたは tar ファイルのリストを続けることでディレクトリの指定を 1 回で済ませることが可能です。

サーバまたは Cisco.com 上のイメージの tar ファイル形式

サーバ上にあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは、次のファイルを含む tar ファイル形式で提供されます。

- tar ファイルの内容を表形式で示す *info* ファイル
- Cisco IOS イメージや Web 管理用ファイルなど、他のイメージおよびファイルが格納された 1 つまたは複数のサブディレクトリ

次に、info ファイルに格納された情報の一部の例を示します。表 A-4 に、この情報の詳細を示します。

```
system_type:0x00000000:image-name
    image_family:xxxx
    stacking_number:x
    info_end:
version_suffix:xxxx
    version_directory:image-name
    image_system_type_id:0x00000000
    image_name:image-nameB.bin
    ios_image_file_size:6398464
    total_image_file_size:8133632
    image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
    image_family:xxxx
    stacking_number:x
```

```
    board_ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002
0x40110000
    info_end:
```

（注）　stacking_number フィールドは無視してください。このフィールドはスイッチに適用されません。

表 A-4　　info ファイルの説明

フィールド	説明
version_suffix	Cisco IOS イメージ バージョン ストリングのサフィックスを指定します。
version_directory	Cisco IOS イメージおよび HTML サブディレクトリがインストールされているディレクトリを指定します。
image_name	tar ファイル内の Cisco IOS イメージの名前を指定します。
ios_image_file_size	tar ファイル内の Cisco IOS イメージのサイズを指定します。このサイズは、Cisco IOS イメージのみを保持するために必要なフラッシュ メモリ サイズの概算値です。
total_image_file_size	tar ファイル内のすべてのイメージ（Cisco IOS イメージおよび Web 管理ファイル）のサイズを指定します。このサイズは、これらのファイルを保持するために必要なフラッシュ メモリ サイズの概算値です。
image_feature	イメージの主な機能に関する説明です。
image_min_dram	このイメージを実行するために必要な DRAM の最小サイズを指定します。
image_family	ソフトウェアをインストールできる製品ファミリに関する説明です。

TFTP によるイメージ ファイルのコピー

TFTP サーバからスイッチ イメージをダウンロードしたり、スイッチから TFTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードするために使用できます。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

/etc/services ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```

（注）　/etc/inetd.conf および /etc/services ファイルを変更した後に、inetd デーモンを再起動する必要があります。このデーモンを再起動するには、inetd プロセスを終了して再起動するか、または **fastboot** コマンド（SunOS 4.x の場合）や **reboot** コマンド（Solaris 2.x または SunOS 5.x の場合）を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするイメージが TFTP サーバ上の正しいディレクトリ内にあることを確認します（UNIX ワークステーションの場合は、通常 /tftpboot）。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。
- イメージ ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* は、イメージをサーバにアップロードするときに使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル（空のファイルを作成する必要があった場合は、空のファイルを含む）を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

TFTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 3 を実行します。現在のイメージを保存するには、ステップ 3 へ進みます。

	コマンド	目的
ステップ 1	イメージをワークステーション上の適切な TFTP ディレクトリにコピーします。TFTP サーバが適切に設定されていることを確認します（「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.A-26）を参照）。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	

	コマンド	目的
ステップ 3	**archive download-sw /overwrite /reload tftp:**[[//*location*]/*directory*]/*image-name*.**tar**	TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //*location* には、TFTP サーバの IP アドレスを指定します。 • /*directory*/*image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ 4	**archive download-sw/leave-old-sw/reload tftp:**[[//*location*]/*directory*]/*image-name*.**tar**	TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //*location* には、TFTP サーバの IP アドレスを指定します。 • /*directory*/*image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注） フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼働中のイメージを保存しようとすると、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス（flash:）にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いイメージを保存した場合は（**/leave-old-sw** キーワードを指定した場合は）、**delete /force/recursive** *filesystem*:/*file-url* 特権 EXEC コマンドを入力して、そのイメージを削除できます。*filesystem* には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。*file-url* には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

TFTP によるイメージ ファイルのアップロード

スイッチから TFTP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	TFTP サーバが適切に設定されていることを確認します（「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.A-26）を参照）。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**archive upload-sw tftp:**[[*//location*]*/directory*]*/image-name*.**tar**	現在稼働中のスイッチ イメージを TFTP サーバにアップロードします。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。*image-name*.**tar** は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのコピー

FTP サーバからスイッチ イメージをダウンロードしたり、スイッチから FTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

FTP によるイメージ ファイルのダウンロードまたはアップロードの準備

FTP サーバから、または FTP サーバに、イメージ ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名（ユーザ名が指定されている場合）。
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- anonymous

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたパスワード（パスワードが指定されている場合）
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）
- スイッチが作成した *username@switchname.domain* パスワード。変数 *username* は現在のセッションに関連付けられているユーザ名、*switchname* は設定されているホスト名、*domain* はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。

サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

FTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、FTP サーバへの接続をチェックします。

- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して、新しい FTP ユーザ名を作成します。新しい名前は、すべてのアーカイブ処理中に使用されます。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。ユーザ名をこの処理のためだけに指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンド内でユーザ名を指定します。
- イメージ ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを上書きしたり、保存したりできます。

FTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 7 の手順を実行します。現在のイメージを保存するには、ステップ 7 へ進みます。

	コマンド	目的
ステップ 1	「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-14）を参照して、FTP サーバが適切に設定されていることを確認します。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]/ *image-name***.tar**	FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//username*[**:***password*] には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられている必要があります。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • *directory*/*image-name***.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ 8	**archive download-sw/leave-old-sw/reload ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]/ *image-name***.tar**	FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//username*[**:***password*] には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • *directory*/*image-name***.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注） フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼働中のイメージを保存しようとすると、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス（flash:）にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いイメージを保存した場合は（**/leave-old-sw** キーワードを指定した場合は）、**delete /force/recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力して、そのイメージを削除できます。*filesystem* には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更*しないでください*。

FTP によるイメージ ファイルのアップロード

スイッチから FTP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-14）を参照して、FTP サーバが適切に設定されていることを確認します。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。

	コマンド	目的
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**archive upload-sw ftp:**[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*image-name***.tar**	現在稼働中のスイッチ イメージを FTP サーバにアップロードします。 • *//username**:**password* には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。 • *@location* には、FTP サーバの IP アドレスを指定します。 • */directory/image-name***.tar** には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。*image-name***.tar** は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更*しないで*ください。

RCP によるイメージ ファイルのコピー

RCP サーバからスイッチ イメージをダウンロードしたり、スイッチから RCP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

リモート ホストとスイッチの間でイメージ ファイルをダウンロードおよびアップロードするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のように

ファイル配信用サーバを作成する必要がありません。ユーザは rsh をサポートするサーバにアクセスするだけですみます （ほとんどの UNIX システムは rsh をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。RCP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名（ユーザ名が指定されている場合）。
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、**username** コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スイッチのホスト名。

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、rsh がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチとサーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、RCP サーバへの接続を確認します。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのアーカイブ処理中に使用される **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用して、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。
- イメージを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。

  たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

  ```
  hostname Switch1
  ip rcmd remote-username User0
  ```

  このスイッチの IP アドレスを *Switch1.company.com* に変換する場合は、RCP サーバ上の User0 用の .rhosts ファイルに次の行が含まれている必要があります。

  ```
  Switch1.company.com Switch1
  ```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

RCP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 6 の手順を実行します。現在のイメージを保存するには、ステップ 6 へ進みます。

	コマンド	目的
ステップ 1	「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-17）を参照して、RCP サーバが適切に設定されていることを確認します。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**archive download-sw /overwrite /reload rcp:**[[[//[*username***@**]*location*]/*directory*]/*image-name***.tar**]	RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//username* には、ユーザ名を指定します。RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。 • ***@****location* には、RCP サーバの IP アドレスを指定します。 • */directory/image-name***.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

	コマンド	目的
ステップ 7	**archive download-sw/leave-old-sw/reload rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //*username* には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。 • @*location* には、RCP サーバの IP アドレスを指定します。 • /*directory*]/*image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注） フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、稼働中のイメージを保存しようとすると、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス（flash:）にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いソフトウェアを保存した場合は（**/leave-old-sw** キーワードを指定した場合は）、**delete /force/recursive** *filesystem*:/*file-url* 特権 EXEC コマンドを入力して、そのイメージを削除できます。*filesystem* には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

注意 ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更*しないで*ください。

RCP によるイメージ ファイルのアップロード

スイッチから RCP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを RCP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.A-17）を参照して、RCP サーバが適切に設定されていることを確認します。	
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。	
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**archive upload-sw rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	現在稼働中のスイッチ イメージを RCP サーバにアップロードします。 • *//username* には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。 • *@location* には、RCP サーバの IP アドレスを指定します。 • */directory*]/*image-name*.**tar** には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 • *image-name*.**tar** は、サーバに保存するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

INDEX

数字

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

つ

て

と

な

に

ね

は

ひ

ふ

へ

ほ

ま

み

む

め

も

ゆ

ら

り

る

れ

ろ

わ

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/