Cisco ME 3400E イーサネット アクセス スイッチ ソフトウェア コンフィギュレーション ガイド

Cisco ME 3400E Ethernet Access Switch Software Configuration Guide

Cisco IOS リリース 12.2(52)SE

2009 年 9 月

Text Part Number: OL-16485-03-J

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

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

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Cisco ME 3400E イーサネット アクセス スイッチ ソフトウェア コンフィギュレーション ガイド
© 2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2009–2010, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

はじめに xliii

対象読者 xliii

目的 xliii

表記法 xliv

関連資料 xliv

マニュアルの入手方法およびテクニカル サポート xlv

CHAPTER 1 概要 1-1

機能 1-1

パフォーマンスの特長 1-2

管理オプション 1-3

管理機能 1-4

アベイラビリティ機能 1-6

VLAN 機能 1-7

セキュリティ機能 1-7

加入者に対するセキュリティ 1-7

スイッチ セキュリティ 1-8

ネットワーク セキュリティ 1-9

QoS 機能および CoS 機能 1-9

レイヤ 2 VPN サービス 1-10

レイヤ 3 機能 1-11

レイヤ 3 VPN サービス 1-12

モニタリング機能 1-12

スイッチ初期設定後のデフォルト設定値 1-13

ネットワークの構成例 1-16

集合住宅のネットワークまたはイーサネット / 加入者ネットワーク 1-16

レイヤ 2 VPN アプリケーション 1-17

マルチ VRF CE アプリケーション 1-18

次の作業 1-19

CHAPTER 2 CLI の使用方法 2-1

コマンド モードの概要 2-1

ヘルプ システムの概要 2-3

コマンドの省略形 2-3

コマンドの no および default 形式の概要 2-3
CLI エラー メッセージについて 2-4
コマンド履歴の使用方法 2-4
コマンド履歴バッファ サイズの変更 2-4
コマンドの呼び出し方法 2-5
コマンド履歴機能のディセーブル化 2-5
編集機能の使用方法 2-5
編集機能のイネーブル化およびディセーブル化 2-6
キーストロークによるコマンドの編集 2-6
折り返すコマンドラインの編集 2-7
show および more コマンドの出力の検索とフィルタリング 2-8
CLI のアクセス 2-8
コンソール接続または Telnet を使用した CLI へのアクセス 2-8

CHAPTER 3 スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て 3-1
起動プロセスの概要 3-1
スイッチ情報の割り当て 3-2
デフォルトのスイッチ情報 3-3
DHCP ベースの自動設定の概要 3-3
DHCP クライアントの要求プロセス 3-4
DHCP ベースの自動設定およびイメージ アップデートの概要 3-5
DHCP 自動設定 3-5
DHCP 自動イメージ アップデート 3-5
注意事項および制限事項 3-6
DHCP ベースの自動設定機能の設定 3-6
DHCP サーバ設定時の注意事項 3-6
TFTP サーバの設定 3-7
DNS の設定 3-8
リレー デバイスの設定 3-8
コンフィギュレーション ファイルの取得 3-9
設定例 3-10
DHCP の自動設定機能およびイメージ アップデート機能の設定 3-12
DHCP 自動設定機能の設定（コンフィギュレーション ファイルだけ） 3-12
DHCP 自動イメージ アップデート機能の設定（コンフィギュレーション ファイルとイメージ） 3-13
クライアントの設定 3-14
手動での IP 情報の割り当て 3-15
実行コンフィギュレーションの確認と保存 3-16
スタートアップ コンフィギュレーションの変更 3-18

デフォルトのブート コンフィギュレーション 3-18
コンフィギュレーション ファイルの自動ダウンロード 3-18
ファイル名の指定によるシステム コンフィギュレーションの読み取りと書き込み 3-19
手動による起動 3-19
特定のソフトウェア イメージの起動 3-20
環境変数の管理 3-21
ソフトウェア イメージのリロードのスケジューリング 3-22
リロードのスケジューリング設定 3-23
リロードのスケジューリング情報の表示 3-24

CHAPTER 4 **Cisco IOS Configuration Engine の設定 4-1**
Cisco Configuration Engine ソフトウェアの概要 4-1
Configuration Service 4-2
Event Service 4-3
Name Space Mapper 4-3
CNS ID およびデバイスのホスト名についての注釈 4-3
ConfigID 4-3
DeviceID 4-4
ホスト名および DeviceID 4-4
ホスト名、DeviceID、ConfigID の使用方法 4-4
Cisco IOS エージェントの概要 4-5
初期設定 4-5
差分（部分）設定 4-6
同期設定 4-6
Cisco IOS エージェントの設定 4-6
自動 CNS 設定のイネーブル化 4-7
CNS イベント エージェントのイネーブル化 4-7
Cisco IOS CNS エージェントのイネーブル化 4-9
初期設定のイネーブル化 4-9
部分設定のイネーブル化 4-13
Cisco IOS イメージ エージェントによるデバイスのアップグレード 4-14
CNS イメージ エージェントの条件 4-14
CNS イメージ エージェントの制限事項 4-14
CNS コンフィギュレーションの表示 4-15

CHAPTER 5 **スイッチの管理 5-1**
システム日時の管理 5-1
システム クロックの概要 5-2
NTP の概要 5-2

NTP の設定 5-4
NTP のデフォルト設定 5-4
NTP 認証の設定 5-4
NTP アソシエーションの設定 5-5
NTP ブロードキャスト サービスの設定 5-7
NTP アクセス制限の設定 5-8
NTP パケット用の送信元 IP アドレスの設定 5-10
NTP 設定の表示 5-11
手動での日時の設定 5-11
システム クロックの設定 5-11
日時設定の表示 5-12
タイム ゾーンの設定 5-12
夏時間の設定 5-13
システム名およびプロンプトの設定 5-14
デフォルトのシステム名およびプロンプトの設定 5-15
システム名の設定 5-15
DNS の概要 5-15
DNS のデフォルト設定 5-16
DNS の設定 5-16
DNS 設定の表示 5-17
バナーの作成 5-17
バナーのデフォルト設定 5-17
MoTD ログイン バナーの設定 5-18
ログイン バナーの設定 5-19
MAC アドレス テーブルの管理 5-19
アドレス テーブルの作成 5-20
MAC アドレスと VLAN 5-20
MAC アドレス テーブルのデフォルト設定 5-21
アドレス エージング タイムの変更 5-21
ダイナミック アドレス エントリの削除 5-22
MAC アドレス変更通知トラップの設定 5-22
MAC アドレス移動通知トラップの設定 5-24
MAC しきい値通知トラップの設定 5-26
スタティック アドレス エントリの追加および削除 5-27
ユニキャスト MAC アドレス フィルタリングの設定 5-28
VLAN 上での MAC アドレス学習のディセーブル化 5-29
アドレス テーブル エントリの表示 5-31
ARP テーブルの管理 5-31

CHAPTER 6 スイッチ アラームの設定 6-1
外部アラームの設定 6-1
電源装置アラームの設定 6-3
電源不在アラーム 6-4
DC 電源フィード アラーム 6-4

CHAPTER 7 SDM テンプレートの設定 7-1
SDM テンプレートの概要 7-1
デュアル IPv4 および IPv6 SDM テンプレート 7-2
スイッチ SDM テンプレートの設定 7-3
デフォルトの SDM テンプレート 7-4
SDM テンプレートの設定時の注意事項 7-4
SDM テンプレートの設定 7-5
SDM テンプレートの表示 7-6

CHAPTER 8 スイッチベースの認証の設定 8-1
スイッチへの不正アクセスの防止 8-1
特権 EXEC コマンドへのアクセスの保護 8-2
デフォルトのパスワードおよび権限レベル設定 8-2
スタティック イネーブル パスワードの設定または変更 8-3
暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 8-3
パスワード回復のディセーブル化 8-5
端末回線に対する Telnet パスワードの設定 8-6
ユーザ名とパスワードのペアの設定 8-7
複数の権限レベルの設定 8-7
コマンドの権限レベルの設定 8-8
回線に対するデフォルトの権限レベルの変更 8-9
権限レベルへのログインおよび終了 8-9
TACACS+ によるスイッチ アクセスの制御 8-10
TACACS+ の概要 8-10
TACACS+ の動作 8-12
TACACS+ の設定 8-12
TACACS+ のデフォルト設定 8-13
TACACS+ サーバ ホストの特定と認証鍵の設定 8-13
TACACS+ ログイン認証の設定 8-14
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定 8-16
TACACS+ アカウンティングの開始 8-16
TACACS+ 設定の表示 8-17

RADIUS によるスイッチ アクセスの制御 8-17
RADIUS の概要 8-18
RADIUS の動作 8-19
RADIUS の設定 8-20
RADIUS のデフォルト設定 8-20
RADIUS サーバ ホストの特定 8-20
RADIUS ログイン認証の設定 8-23
AAA サーバ グループの定義 8-25
ユーザ イネーブル アクセスおよびネットワーク サービス用の RADIUS 許可の設定 8-27
RADIUS アカウンティングの開始 8-28
すべての RADIUS サーバに対する設定 8-29
ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法 8-29
ベンダー固有の RADIUS サーバ通信用にスイッチを設定する方法 8-30
RADIUS ロード バランシングの設定 8-31
RADIUS 設定の表示 8-32
Kerberos によるスイッチ アクセスの制御 8-32
Kerberos の概要 8-32
Kerberos の動作 8-34
境界スイッチに対する認証の取得 8-35
KDC からの TGT の取得 8-35
ネットワーク サービスに対する認証の取得 8-35
Kerberos の設定 8-35
スイッチのローカル認証および許可の設定 8-36
Secure Shell のためのスイッチの設定 8-37
SSH の概要 8-38
SSH サーバ、統合クライアント、およびサポート対象バージョン 8-38
制限事項 8-39
SSH の設定 8-39
設定時の注意事項 8-39
スイッチでの SSH 実行の設定 8-39
SSH サーバの設定 8-40
SSH の設定およびステータスの表示 8-41
SCP のためのスイッチの設定 8-42
Secure Copy について 8-42

CHAPTER 9 **IEEE 802.1x ポートベースの認証の設定** 9-1
IEEE 802.1x ポートベースの認証の概要 9-1
デバイスの役割 9-2

認証の開始とメッセージ交換 9-3
許可ステートおよび無許可ステートのポート 9-4
802.1x アカウンティング 9-5
802.1x アカウンティングのアトリビュートと値のペア 9-5
802.1x ホスト モード 9-6
802.1x 準備状態チェック 9-7
ポート セキュリティを含む 802.1x 9-7
VLAN 割り当てを含む 802.1x 9-8
802.1x ユーザ分散 9-9
802.1x ユーザ分散の設定ガイドライン 9-9
ネットワーク エッジ アクセス トポロジ（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ 9-10
ガイドライン 9-11
コモン セッション ID 9-11
IEEE 802.1x 認証の設定 9-12
802.1x のデフォルト設定 9-13
802.1x 設定時の注意事項 9-13
ポート単位の許可デバイスの最大数 9-14
802.1x 準備状態チェックの設定 9-14
802.1x 違反モードの設定 9-15
802.1x 認証の設定 9-16
スイッチと RADIUS サーバ間通信を設定する方法 9-17
定期的な再認証の設定 9-18
手動によるポート接続クライアントの再認証 9-19
待機時間の変更 9-19
スイッチとクライアント間の再送信時間の変更 9-20
スイッチとクライアント間のフレーム再送信回数の設定 9-21
再認証回数の設定 9-21
ホスト モードの設定 9-22
802.1x 設定をデフォルト値にリセットする方法 9-23
802.1x アカウンティングの設定 9-23
802.1x ユーザ分散の設定 9-24
オーセンティケータおよび、NEAT を使用したサプリカント スイッチの設定 9-25
ASP を使用した NEAT の設定 9-27
802.1x 統計情報およびステータスの表示 9-27

CHAPTER 10 インターフェイスの設定 10-1
インターフェイス タイプの概要 10-1
UNI、NNI、および ENI の各ポート タイプ 10-2
ポートベースの VLAN 10-3

スイッチ ポート 10-4
アクセス ポート 10-4
トランク ポート 10-4
トンネル ポート 10-5
ルーテッド ポート 10-5
イーサネット管理ポート 10-6
スイッチ仮想インターフェイス 10-6
EtherChannel ポート グループ 10-7
デュアルパーパス ポート 10-7
インターフェイスの接続 10-8
インターフェイス コンフィギュレーション モードの使用方法 10-8
インターフェイスの設定手順 10-9
インターフェイスの範囲設定 10-10
インターフェイス範囲マクロの設定と使用方法 10-11
イーサネット管理ポートの使用方法 10-13
イーサネット管理ポートの概要 10-13
イーサネット管理ポート上でサポートされている機能 10-15
イーサネット管理ポートの設定 10-15
TFTP とイーサネット管理ポート 10-15
イーサネット インターフェイスの設定 10-16
イーサネット インターフェイスのデフォルト設定 10-16
ポート タイプの設定 10-18
インターフェイス速度とデュプレックス モードの設定 10-19
速度およびデュプレックスの設定に関する注意事項 10-19
インターフェイス速度およびデュプレックスに関するパラメータの設定 10-20
デュアルパーパス ポートの設定 10-22
IEEE 802.3X フロー制御の設定 10-24
インターフェイスの自動 MDIX の設定 10-25
インターフェイスに関する説明の追加 10-26
レイヤ 3 インターフェイスの設定 10-27
システム MTU の設定 10-29
インターフェイスのモニタおよびメンテナンス 10-31
インターフェイス ステータスのモニタ 10-31
インターフェイスおよびカウンタのクリアとリセット 10-32
インターフェイスのシャットダウンおよび再起動 10-33

CHAPTER 11 **コマンド マクロの設定** 11-1
コマンド マクロの概要 11-1
コマンド マクロの設定 11-1

コマンド マクロのデフォルト設定 11-2
コマンド マクロ設定時の注意事項 11-2
コマンド マクロの作成 11-3
コマンド マクロの適用 11-4
コマンド マクロの表示 11-5

CHAPTER 12 VLAN の設定 12-1
VLAN の概要 12-1
サポート対象の VLAN 12-3
標準範囲 VLAN 12-3
拡張範囲 VLAN 12-4
VLAN ポート メンバーシップ モード 12-4
UNI-ENI VLAN 12-5
VLAN の作成および変更 12-7
イーサネット VLAN のデフォルト設定 12-7
VLAN 設定時の注意事項 12-8
イーサネット VLAN の作成または変更 12-9
VLAN へのスタティックアクセス ポートの割り当て 12-11
内部 VLAN ID を指定した拡張範囲 VLAN の作成 12-12
UNI-ENI VLAN の設定 12-13
設定時の注意事項 12-13
UNI-ENI VLAN の設定 12-14
VLAN の表示 12-15
VLAN トランクの設定 12-15
トランキングの概要 12-15
IEEE 802.1Q の設定に関する注意事項 12-16
レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定 12-17
トランク ポートとしてのイーサネット インターフェイスの設定 12-17
他の機能との相互作用 12-17
トランク ポートの設定 12-18
トランク上での許可 VLAN の定義 12-18
タグなしトラフィック用ネイティブ VLAN の設定 12-20
トランク ポートの負荷分散の設定 12-20
STP ポート プライオリティによる負荷分散 12-21
STP パス コストによる負荷分散 12-22
VMPS の設定 12-24
VMPS の概要 12-24
ダイナミック アクセス ポート VLAN メンバーシップ 12-25
VMPS クライアントのデフォルト設定 12-26

VMPS 設定時の注意事項 12-26
VMPS クライアントの設定 12-26
VMPS の IP アドレスの入力 12-27
VMPS クライアントのダイナミック アクセス ポートの設定 12-27
VLAN メンバーシップの再確認 12-28
再確認インターバルの変更 12-28
再試行回数の変更 12-29
VMPS のモニタ 12-29
ダイナミック アクセス ポート VLAN メンバーシップのトラブルシューティング 12-30
VMPS の構成例 12-30

CHAPTER 13 **プライベート VLAN の設定** 13-1
プライベート VLAN の概要 13-1
プライベート VLAN およびプライベート VLAN ポートのタイプ 13-2
プライベート VLAN での IP アドレッシング方式 13-4
複数のスイッチにまたがるプライベート VLAN 13-4
プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック 13-5
プライベート VLAN と SVI 13-6
プライベート VLAN の設定 13-6
プライベート VLAN の設定手順 13-6
デフォルトのプライベート VLAN 設定 13-7
プライベート VLAN 設定時の注意事項 13-7
セカンダリおよびプライマリ VLAN の設定 13-7
プライベート VLAN ポート設定 13-9
他の機能との間の制限 13-10
プライベート VLAN への VLAN の設定と関連付け 13-10
プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 13-12
プライベート VLAN プロミスキャス ポートとしてのレイヤ 2 インターフェイスの設定 13-13
セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング 13-15
プライベート VLAN のモニタリング 13-16

CHAPTER 14 **IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定** 14-1
802.1Q トンネリングの概要 14-1
802.1Q トンネリングの設定 14-4
802.1Q トンネリングのデフォルト設定 14-4
802.1Q トンネリング設定時の注意事項 14-4

ネイティブ VLAN 14-4
システム MTU 14-6
802.1Q トンネリングおよびその他の機能 14-6
802.1Q トンネリング ポートの設定 14-7
VLAN マッピングの概要 14-8
カスタマー VLAN のサービス プロバイダー VLAN へのマッピング 14-9
VLAN マッピングの設定 14-9
VLAN マッピングのデフォルト設定 14-9
VLAN マッピング設定時の注意事項 14-10
VLAN マッピングの設定 14-10
One-to-One マッピング 14-10
トランク ポートの従来の QinQ 14-11
トランク ポートの選択した QinQ 14-12
レイヤ 2 プロトコル トンネリングの概要 14-13
レイヤ 2 プロトコル トンネリングの設定 14-16
レイヤ 2 プロトコル トンネリングのデフォルト設定 14-17
レイヤ 2 プロトコル トンネリング設定時の注意事項 14-18
レイヤ 2 プロトコル トンネリングの設定 14-19
EtherChannel のレイヤ 2 トンネリングの設定 14-20
サービス プロバイダー エッジ スイッチの設定 14-20
カスタマー スイッチの設定 14-22
トンネリングおよびマッピング ステータスのモニタおよびメンテナンス 14-24

CHAPTER 15 **STP の設定** 15-1
スパニング ツリー機能の概要 15-1
STP の概要 15-2
スパニング ツリー トポロジと BPDU 15-3
ブリッジ ID、スイッチ プライオリティ、および拡張システム ID 15-4
スパニング ツリー インターフェイスのステート 15-5
ブロッキング ステート 15-6
リスニング ステート 15-7
ラーニング ステート 15-7
フォワーディング ステート 15-7
ディセーブル ステート 15-8
スイッチまたはポートがルート スイッチまたはルート ポートになる方法 15-8
スパニング ツリーおよび冗長接続 15-9
スパニング ツリー アドレスの管理 15-9
接続を維持するための有効期間の短縮 15-9
スパニング ツリー モードとプロトコル 15-10

スパニング ツリー インスタンスのサポート 15-11
スパニング ツリーの相互運用性と下位互換性 15-11
STP および IEEE 802.1Q トランク 15-11
スパニング ツリー機能の設定 15-12
スパニング ツリーのデフォルト設定 15-12
スパニング ツリーの設定時の注意事項 15-13
ENI 上のスパニング ツリーをイネーブルにする 15-14
スパニング ツリー モードの変更 15-14
スパニング ツリーのディセーブル化 15-16
ルート スイッチの設定 15-16
セカンダリ ルート スイッチの設定 15-18
ポート プライオリティの設定 15-18
パス コストの設定 15-20
VLAN のスイッチ プライオリティの設定 15-21
スパニング ツリー タイマーの設定 15-22
hello タイムの設定 15-22
VLAN の転送遅延時間の設定 15-23
VLAN の最大エージング タイムの設定 15-24
スパニング ツリー ステータスの表示 15-24

CHAPTER 16 **MSTP の設定** 16-1
MSTP の概要 16-2
MST リージョン 16-2
IST、CIST、および CST 16-3
MST リージョン内の動作 16-3
MST リージョン間の動作 16-4
IEEE 802.1s の用語 16-5
ホップ カウント 16-6
境界ポート 16-6
IEEE 802.1s の実装 16-7
ポート役割命名の変更 16-7
レガシー スイッチと標準スイッチ間の相互運用 16-7
単一方向リンク障害の検出 16-8
IEEE 802.1D STP との相互運用性 16-9
RSTP の概要 16-9
ポートの役割およびアクティブ トポロジ 16-9
高速コンバージェンス 16-10
ポートの役割の同期化 16-12
BPDU のフォーマットおよびプロセス 16-12

優位 BPDU 情報の処理 16-13
下位 BPDU 情報の処理 16-13
トポロジの変更 16-14
MSTP 機能の設定 16-14
MSTP のデフォルト設定 16-15
MSTP 設定時の注意事項 16-15
MST リージョンの設定の指定および MSTP のイネーブル設定 16-16
ルート スイッチの設定 16-18
セカンダリ ルート スイッチの設定 16-19
ポート プライオリティの設定 16-20
パス コストの設定 16-22
スイッチ プライオリティの設定 16-23
hello タイムの設定 16-24
転送遅延時間の設定 16-24
最大エージング タイムの設定 16-25
最大ホップ カウントの設定 16-25
リンク タイプの指定による高速移行の保証 16-26
ネイバ タイプの指定 16-27
プロトコル移行プロセスの再起動 16-28
MST コンフィギュレーションおよびステータスの表示 16-29

CHAPTER 17 **オプションのスパニング ツリー機能の設定方法** 17-1
オプションのスパニング ツリー機能の概要 17-1
PortFast の概要 17-2
BPDU ガードの概要 17-3
BPDU フィルタリングの概要 17-3
EtherChannel ガードの概要 17-4
ルート ガードの概要 17-4
ループ ガードの概要 17-5
オプションのスパニング ツリー機能の設定方法 17-5
オプションのスパニング ツリー機能のデフォルト設定 17-6
オプションのスパニング ツリー機能の設定時の注意事項 17-6
PortFast のイネーブル化 17-6
BPDU ガードのイネーブル化 17-8
BPDU フィルタリングのイネーブル化 17-9
EtherChannel ガードのイネーブル化 17-10
ルート ガードのイネーブル化 17-11
ループ ガードのイネーブル化 17-12
スパニング ツリー ステータスの表示 17-12

CHAPTER 18 レジリエント イーサネット プロトコルの設定 18-1
REP の概要 18-1
リンク完全性 18-3
高速コンバージェンス 18-4
VLAN ロード バランシング 18-4
スパニング ツリー インタラクション 18-6
REP ポート 18-6
REP の設定 18-6
REP のデフォルト設定 18-7
REP 設定時の注意事項 18-7
REP 管理 VLAN の設定 18-9
REP インターフェイスの設定 18-10
VLAN ロード バランシングの手動によるプリエンプションの設定 18-14
REP の SNMP トラップの設定 18-14
REP のモニタリング 18-15

CHAPTER 19 Flex Link および MAC アドレス テーブル移行更新機能の設定 19-1
Flex Link および MAC アドレス テーブル移行更新機能の概要 19-1
Flex Link 19-1
VLAN Flex Link のロード バランシングおよびサポート 19-2
Flex Link マルチキャスト高速コンバージェンス 19-3
他の Flex Link ポートの mrouter ポートとしての学習 19-3
IGMP レポートの生成 19-4
IGMP レポートの通過許可 19-4
MAC アドレス テーブル移行更新 19-7
Flex Link および MAC アドレス テーブル移行更新機能の設定 19-8
デフォルト設定 19-8
設定時の注意事項 19-9
Flex Link の設定 19-10
Flex Link での VLAN ロード バランシングの設定 19-12
MAC アドレス テーブル移行更新機能の設定 19-13
Flex Link および MAC アドレス テーブル移行更新機能のモニタリング 19-15

CHAPTER 20 DHCP 機能および IP ソース ガードの設定 20-1
DHCP 機能の概要 20-1
DHCP サーバ 20-2
DHCP リレー エージェント 20-2
DHCP スヌーピング 20-2
Option 82 データ挿入 20-3

Cisco IOS DHCP サーバ データベース 20-6
DHCP スヌーピング バインディング データベース 20-6
DHCP 機能の設定 20-7
DHCP のデフォルト設定 20-8
DHCP スヌーピング設定時の注意事項 20-8
DHCP サーバの設定 20-10
DHCP リレー エージェントの設定 20-10
パケット転送アドレスの指定 20-10
DHCP スヌーピングおよび Option 82 のイネーブル化 20-12
プライベート VLAN での DHCP スヌーピングのイネーブル化 20-14
Cisco IOS DHCP サーバ データベースのイネーブル化 20-14
DHCP スヌーピング バインディング データベース エージェントのイネーブル化 20-14
DHCP スヌーピング情報の表示 20-15
DHCP サーバ ポートベース アドレス 割り当て 20-16
DHCP サーバ ポートベース アドレス 割り当ての設定 20-16
ポートベース アドレス割り当てのデフォルト設定 20-16
ポートベース アドレス割り当て設定のガイドライン 20-16
DHCP サーバ ポートベース アドレス 割り当てのイネーブル化 20-17
DHCP サーバ ポートベース アドレス 割り当ての表示 20-19
IP ソース ガードの概要 20-20
送信元 IP アドレス フィルタリング 20-20
送信元 IP および MAC アドレス フィルタリング 20-21
スタティック ホスト用 IP ソース ガード 20-21
IP ソース ガードの設定 20-22
デフォルトの IP ソース ガードの設定 20-22
IP ソース ガード設定時の注意事項 20-22
IP ソース ガードのイネーブル化 20-23
スタティック ホスト用 IP ソース ガードの設定 20-24
レイヤ 2 アクセス ポート上におけるスタティック ホスト用 IP ソース ガードの設定 20-24
プライベート VLAN ホスト ポート上におけるスタティック ホスト用 IP ソース ガードの設定 20-28
IP ソース ガード情報の表示 20-30

CHAPTER 21 **ダイナミック ARP 検査の設定** 21-1
ダイナミック ARP 検査の概要 21-1
インターフェイス信頼状態およびネットワーク セキュリティ 21-3
ARP パケットのレート制限 21-4
ARP ACL と DHCP スヌーピング エントリの相対的なプライオリティ 21-4

廃棄されたパケットのロギング 21-5
ダイナミック ARP 検査の設定 21-5
デフォルトのダイナミック ARP 検査の設定 21-5
ダイナミック ARP 検査の設定時の注意事項 21-6
DHCP 環境でのダイナミック ARP 検査の設定 21-7
非 DHCP 環境の ARP ACL の設定 21-9
着信 ARP パケットのレート制限 21-11
妥当性チェックの実行 21-13
ログ バッファの設定 21-14
ダイナミック ARP 検査情報の表示 21-15

CHAPTER 22 **IGMP スヌーピングおよび MVR の設定 22-1**
IGMP スヌーピングの概要 22-1
IGMP バージョン 22-2
マルチキャスト グループへの参加 22-3
マルチキャスト グループからの脱退 22-5
即時脱退 22-6
IGMP の設定可能な Leave タイマー 22-6
IGMP レポート抑制 22-6
IGMP スヌーピングの設定 22-7
IGMP スヌーピングのデフォルト設定 22-7
IGMP スヌーピングのイネーブル化またはディセーブル化 22-7
マルチキャスト ルータ ポートの設定 22-8
グループに参加するホストのスタティックな設定 22-9
IGMP 即時脱退のイネーブル化 22-10
IGMP Leave タイマーの設定 22-10
TCN 関連コマンドの設定 22-11
TCN イベント後のマルチキャスト フラッディング時間の制御 22-11
フラッディング モードからの回復 22-12
TCN イベント中のマルチキャスト フラッディングのディセーブル化 22-13
IGMP スヌーピング クエリアの設定 22-13
IGMP レポート抑制のディセーブル化 22-15
IGMP スヌーピング情報の表示 22-15
MVR の概要 22-17
マルチキャスト TV アプリケーションでの MVR の使用方法 22-17
MVR の設定 22-19
MVR のデフォルト設定 22-19
MVR 設定時の注意事項および制限事項 22-20
MVR グローバル パラメータの設定 22-20

アクセス ポート上での MVR の設定 22-22
トランク ポート上での MVR の設定 22-23
MVR 情報の表示 22-25
IGMP フィルタリングおよび IGMP スロットリングの設定 22-25
IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定 22-26
IGMP プロファイルの設定 22-27
IGMP プロファイルの適用 22-28
IGMP グループの最大数の設定 22-28
IGMP スロットリング アクションの設定 22-29
IGMP フィルタリングおよび IGMP スロットリングの設定の表示 22-30

CHAPTER 23 **ポートベースのトラフィック制御の設定** 23-1
ストーム制御の設定 23-1
ストーム制御の概要 23-1
ストーム制御のデフォルト設定 23-3
ストーム制御およびしきい値レベルの設定 23-3
保護ポートの設定 23-5
保護ポートのデフォルト設定 23-6
保護ポートの設定時の注意事項 23-6
保護ポートの設定 23-6
ポート ブロッキングの設定 23-7
ポート ブロッキングのデフォルト設定 23-7
インターフェイスでのフラッディング トラフィックのブロック 23-7
ポート セキュリティの設定 23-8
ポート セキュリティの概要 23-9
セキュア MAC アドレス 23-9
セキュリティ違反 23-10
ポート セキュリティのデフォルト設定 23-10
ポート セキュリティ設定時の注意事項 23-11
ポート セキュリティのイネーブル化と設定 23-12
ポート セキュリティ エージングのイネーブル化と設定 23-15
ポート セキュリティおよびプライベート VLAN 23-17
ポートベースのトラフィック制御設定の表示 23-18

CHAPTER 24 **CDP の設定** 24-1
CDP の概要 24-1
CDP の設定 24-2
CDP のデフォルト設定 24-2

CDP 特性の設定 24-2
CDP のディセーブル化およびイネーブル化 24-3
インターフェイスでの CDP のディセーブル化およびイネーブル化 24-4
CDP のモニタリングおよびメンテナンス 24-5

CHAPTER 25 **LLDP および LLDP-MED の設定** 25-1
LLDP および LLDP-MED の概要 25-1
LLDP の概要 25-1
LLDP-MED の概要 25-2
LLDP および LLDP-MED の設定 25-3
LLDP のデフォルト設定 25-3
LLDP 特性の設定 25-4
グローバルでの LLDP のディセーブル化およびイネーブル化 25-4
インターフェイスでの LLDP のディセーブル化およびイネーブル化 25-5
LLDP-MED TLV の設定 25-6
LLDP および LLDP-MED のモニタおよびメンテナンス 25-7

CHAPTER 26 **UDLD の設定** 26-1
UDLD の概要 26-1
動作モード 26-1
単一方向リンクの検出方法 26-2
UDLD の設定 26-3
UDLD のデフォルト設定 26-4
設定時の注意事項 26-4
UDLD のグローバルなイネーブル化 26-5
インターフェイスでの UDLD のイネーブル化 26-5
UDLD によりディセーブル化されたインターフェイスのリセット 26-6
UDLD ステータスの表示 26-7

CHAPTER 27 **SPAN および RSPAN の設定** 27-1
SPAN および RSPAN の概要 27-1
ローカル SPAN 27-2
Remote SPAN 27-2
SPAN および RSPAN の概念と用語 27-3
SPAN セッション 27-3
監視対象トラフィック 27-4
送信元ポート 27-5
送信元 VLAN 27-6
VLAN フィルタリング 27-6

宛先ポート 27-7
RSPAN VLAN 27-8
SPAN および RSPAN の他の機能との相互作用 27-8
SPAN および RSPAN の設定 27-9
SPAN および RSPAN のデフォルト設定 27-9
ローカル SPAN の設定 27-10
SPAN 設定時の注意事項 27-10
ローカル SPAN セッションの作成 27-11
ローカル SPAN セッションの作成および入力トラフィックの設定 27-14
フィルタリングする VLAN の指定 27-16
RSPAN の設定 27-17
RSPAN 設定時の注意事項 27-17
RSPAN VLAN としての VLAN の設定 27-18
RSPAN 送信元セッションの作成 27-19
RSPAN 宛先セッションの作成 27-20
RSPAN 宛先セッションの作成および入力トラフィックの設定 27-21
フィルタリングする VLAN の指定 27-23
SPAN および RSPAN ステータスの表示 27-24

CHAPTER 28 **RMON の設定** 28-1
RMON の概要 28-1
RMON の設定 28-2
RMON のデフォルト設定 28-3
RMON アラームおよびイベントの設定 28-3
インターフェイスでのグループ履歴統計情報の収集 28-5
インターフェイスでのグループ イーサネット統計情報の収集 28-5
RMON ステータスの表示 28-6

CHAPTER 29 **システム メッセージ ロギングの設定** 29-1
システム メッセージ ロギングの概要 29-1
システム メッセージ ロギングの設定 29-2
システム ログ メッセージ形式 29-2
システム メッセージ ロギングのデフォルト設定 29-3
メッセージ ロギングのディセーブル化 29-4
メッセージ出力先デバイスの設定 29-5
ログ メッセージの同期化 29-6
ログ メッセージのタイムスタンプのイネーブル化およびディセーブル化 29-7
ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 29-8
メッセージの重大度の定義 29-8

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限 29-10
設定変更ロギングのイネーブル化 29-10
UNIX Syslog サーバの設定 29-11
UNIX Syslog デーモンへのメッセージのロギング 29-12
UNIX システム ロギング ファシリティの設定 29-12
ロギング設定の表示 29-13

CHAPTER 30 **SNMP の設定** 30-1
SNMP の概要 30-1
SNMP のバージョン 30-2
SNMP マネージャの機能 30-3
SNMP エージェントの機能 30-4
SNMP コミュニティ ストリング 30-4
SNMP による MIB 変数へのアクセス 30-4
SNMP 通知 30-5
SNMP ifIndex MIB オブジェクト値 30-6
MIB データの収集および転送 30-6
SNMP の設定 30-7
SNMP のデフォルト設定 30-7
SNMP 設定時の注意事項 30-7
SNMP エージェントのディセーブル化 30-8
コミュニティ ストリングの設定 30-9
SNMP グループおよびユーザの設定 30-10
SNMP 通知の設定 30-13
CPU しきい値通知のタイプと値の設定 30-17
エージェント コンタクトおよびロケーションの設定 30-18
SNMP 経由で使用する TFTP サーバの制限 30-18
MIB データ収集および転送の設定 30-19
Cisco Process MIB CPU しきい値テーブルの設定 30-22
SNMP の例 30-22
SNMP ステータスの表示 30-24

CHAPTER 31 **Embedded Event Manager の設定** 31-1
Embedded Event Manager の概要 31-1
イベント ディテクタ 31-3
Embedded Event Manager のアクション 31-4
Embedded Event Manager ポリシー 31-4
Embedded Event Manager の環境変数 31-5
EEM 3.2 31-5

Embedded Event Manager の設定 31-6
Embedded Event Manager アプレットの登録および定義 31-6
Embedded Event Manager TCL スクリプトの登録および定義 31-7
Embedded Event Manager 情報の表示 31-8

CHAPTER 32 **ACL によるネットワーク セキュリティの設定 32-1**
ACL の概要 32-1
サポートされる ACL 32-2
ポート ACL 32-3
ルータ ACL 32-4
VLAN マップ 32-5
分割されたトラフィックおよび分割されていないトラフィックの処理 32-5
IPv4 ACL の設定 32-6
標準および拡張 IPv4 ACL の作成 32-7
IPv4 アクセス リスト番号 32-8
ACL のロギング 32-8
番号付き標準 ACL の作成 32-9
番号付き拡張 ACL の作成 32-10
ACL 内の ACE の並べ替え 32-14
名前付きの標準および拡張 ACL の作成 32-14
ACL での時間範囲の使用法 32-16
ACL へのコメントの挿入 32-18
端末回線への IPv4 ACL の適用 32-18
インターフェイスへの IPv4 ACL の適用 32-19
IP ACL のハードウェアおよびソフトウェア処理 32-20
ACL のトラブルシューティング 32-21
IPv4 ACL の設定例 32-22
番号付き ACL 32-23
拡張 ACL 32-24
名前付き ACL 32-24
IP ACL に適用される時間範囲 32-25
コメント付きの IP ACL エントリ 32-25
ACL のロギング 32-26
名前付き MAC 拡張 ACL の作成 32-27
レイヤ 2 インターフェイスへの MAC ACL の適用 32-28
VLAN マップの設定 32-30
VLAN マップ設定時の注意事項 32-30
VLAN マップの作成 32-32
ACL および VLAN マップの例 32-32

VLAN への VLAN マップの適用 32-34
ネットワークでの VLAN マップの使用法 32-35
ワイヤリング クローゼットの構成 32-35
別の VLAN にあるサーバへのアクセス拒否 32-36
ルータ ACL を VLAN マップと組み合せて使用する方法 32-37
VLAN マップとルータ ACL の設定時の注意事項 32-37
VLAN に適用されるルータ ACL と VLAN マップの例 32-38
ACL およびスイッチド パケット 32-38
ACL およびルーテッド パケット 32-39
ACL およびマルチキャスト パケット 32-40
IPv4 ACL の設定の表示 32-40

CHAPTER 33 **コントロール プレーンのセキュリティ設定 33-1**
コントロール プレーンのセキュリティの概要 33-1
コントロール プレーンのセキュリティ設定 33-6
コントロール プレーンのセキュリティのモニタリング 33-8

CHAPTER 34 **QoS の設定 34-1**
QoS の概要 34-1
MQC 34-3
入力ポリシーおよび出力ポリシー 34-4
入力ポリシー マップ 34-5
出力ポリシー マップ 34-5
分類 34-6
クラス マップ 34-7
match コマンド 34-8
レイヤ 2 CoS に基づく分類 34-8
IP precedence に基づく分類 34-9
IP DSCP に基づく分類 34-9
802.1Q トンネリング CoS マッピング 34-10
分類の比較 34-11
QoS ACL に基づく分類 34-11
QoS グループ に基づく分類 34-12
VLAN ID に基づく分類 34-13
テーブル マップ 34-15
ポリシング 34-16
個別のポリシング 34-17
集約ポリシング 34-19
無条件のプライオリティ ポリシング 34-21

マーキング 34-22
Performance-Monitoring プロトコルの QoS 処理 34-23
Cisco IP-SLAs 34-24
双方向アクティブ測定プロトコル 34-24
IP-SLA および TWAMP プローブの QoS 処理 34-24
マーキング 34-24
キューイング 34-24
CPU 生成トラフィックの QoS マーキング 34-24
CPU 生成トラフィックの QoS キューイング 34-25
設定時の注意事項 34-26
輻輳管理およびスケジューリング 34-27
トラフィック シェーピング 34-28
CBWFQ 34-30
プライオリティ キューイング 34-32
輻輳回避およびキューイング 34-34
QoS の設定 34-37
デフォルトの QoS 設定 34-37
QoS 設定時の注意事項 34-37
ACL を使用したトラフィックの分類 34-39
IP 標準 ACL の作成 34-39
IP 拡張 ACL の作成 34-41
レイヤ 2 MAC ACL の作成 34-42
クラス マップを使用したトラフィック クラスの定義 34-43
テーブル マップの設定 34-45
インターフェイスへのトラフィック ポリシーの付加 34-47
入力ポリシー マップの設定 34-47
個別のポリシングを含む入力ポリシー マップの設定 34-48
集約ポリシングを含む入力ポリシー マップの設定 34-54
マーキングを含む入力ポリシー マップの設定 34-58
階層型入力ポリシー マップを含むポート単位、VLAN 単位 QoS の設定 34-60
出力ポリシー マップの設定 34-65
CBWFQ を含む出力ポリシー マップの設定 34-67
クラスベース シェーピングを含む出力ポリシー マップの設定 34-68
ポート シェーピングを含む出力ポリシー マップの設定 34-70
クラスベース プライオリティ キューイングを含む出力ポリシー マップの設定 34-71
WTD を含む出力ポリシー マップの設定 34-75
CPU 生成トラフィックの QoS マーキングおよびキューイングの設定 34-78
QoS 情報の表示 34-83
QoS 統計情報 34-84

ポリシー マップの設定例 34-84
カスタマー A の QoS 設定 34-85
カスタマー B の QoS 設定 34-87
出力ポリシーの変更および分類基準の追加と削除 34-87
出力ポリシーの変更およびキューイングまたはスケジューリング パラメータの変更 34-88
出力ポリシーの変更および設定済み動作の追加または削除 34-89
出力ポリシーの変更およびクラスの追加または削除 34-90

CHAPTER 35 **EtherChannel およびリンクステート トラッキングの設定 35-1**
EtherChannel の概要 35-1
EtherChannel の概要 35-2
ポート チャネル インターフェイス 35-3
ポート集約プロトコル 35-4
PAgP モード 35-5
PAgP と他の機能との相互作用 35-5
Link Aggregation Control Protocol 35-6
LACP モード 35-6
LACP と他の機能との相互作用 35-7
EherChannel の on モード 35-7
ロード バランシングおよび転送方式 35-7
EtherChannel の設定 35-9
EtherChannel のデフォルト設定 35-10
EtherChannel 設定時の注意事項 35-10
レイヤ 2 EtherChannel の設定 35-12
レイヤ 3 EtherChannel の設定 35-14
ポート チャネル論理インターフェイスの作成 35-14
物理インターフェイスの設定 35-15
EtherChannel ロード バランシングの設定 35-17
PAgP 学習方式およびプライオリティの設定 35-18
LACP ホットスタンバイ ポートの設定 35-19
LACP システム プライオリティの設定 35-20
LACP ポート プライオリティの設定 35-21
EtherChannel、PAgP、および LACP ステータスの表示 35-22
リンクステート追跡の概要 35-22
リンクステート追跡の設定 35-24
リンクステート追跡のデフォルト設定 35-24
リンクステート追跡の設定上の注意事項 35-24
リンクステート追跡の設定 35-24

リンクステート追跡ステータスの表示 35-25

CHAPTER 36 IP ユニキャスト ルーティングの設定 36-1

IP ルーティングの概要 36-2
ルーティングのタイプ 36-2
ルーティングを設定する手順 36-3
IP アドレス指定の設定 36-4
アドレス指定のデフォルト設定 36-4
ネットワーク インターフェイスへの IP アドレスの割り当て 36-5
サブネット ゼロの使用 36-6
クラスレス ルーティング 36-6
アドレス解決方法の設定 36-8
スタティック ARP キャッシュの定義 36-8
ARP カプセル化の設定 36-10
プロキシ ARP のイネーブル化 36-10
IP ルーティングがディセーブルの場合のルーティング支援機能 36-11
プロキシ ARP 36-11
デフォルト ゲートウェイ 36-11
IRDP 36-12
ブロードキャスト パケットの処理方法の設定 36-13
指定ブロードキャストから物理ブロードキャストへの変換のイネーブル化 36-14
UDP ブロードキャスト パケットおよびプロトコルの転送 36-15
IP ブロードキャスト アドレスの確立 36-16
IP ブロードキャストのフラッディング 36-17
IP アドレス指定のモニタリングおよびメンテナンス 36-18
IPv4 ユニキャスト ルーティングのイネーブル化 36-19
RIP の設定 36-20
RIP のデフォルト設定 36-20
基本的な RIP パラメータの設定 36-21
RIP 認証の設定 36-23
スプリット ホライズンの設定 36-23
サマリー アドレスの設定 36-24
OSPF の設定 36-25
OSPF のデフォルト設定 36-27
NSF 認識 36-28
基本的な OSPF パラメータの設定 36-28
OSPF インターフェイスの設定 36-29
OSPF のネットワーク タイプの設定 36-30
非ブロードキャスト ネットワークに対する OSPF の設定 36-31

OSPF インターフェイスに対するネットワーク タイプの設定 36-31
OSPF エリア パラメータの設定 36-33
その他の OSPF パラメータの設定 36-34
LSA グループ ペーシングの変更 36-36
ループバック インターフェイスの設定 36-36
OSPF のモニタリング 36-37
EIGRP の設定 36-38
EIGRP のデフォルト設定 36-39
NSF 認識 36-40
基本的な EIGRP パラメータの設定 36-40
EIGRP インターフェイスの設定 36-41
EIGRP ルート認証の設定 36-42
EIGRP スタブ ルーティングの設定 36-43
EIGRP のモニタリングおよびメンテナンス 36-45
BGP の設定 36-45
BGP のデフォルト設定 36-48
NSF 認識 36-50
BGP ルーティングのイネーブル化 36-50
ルーティング ポリシー変更の管理 36-52
BGP 判断アトリビュートの設定 36-54
ルート マップによる BGP フィルタリングの設定 36-56
ネイバー単位での BGP フィルタリングの設定 36-57
BGP フィルタリング用のプレフィクス リストの設定 36-58
BGP コミュニティ フィルタリングの設定 36-59
BGP ネイバーおよびピア グループの設定 36-61
集約アドレスの設定 36-63
ルーティング ドメイン連合の設定 36-63
BGP ルート リフレクタの設定 36-64
ルート ダンプニングの設定 36-65
BGP のモニタリングおよびメンテナンス 36-66
ISO CLNS ルーティングの設定 36-67
IS-IS ダイナミック ルーティングの設定 36-68
IS-IS のデフォルト設定 36-69
NSF 認識 36-69
IS-IS ルーティングのイネーブル化 36-70
IS-IS グローバル パラメータの設定 36-72
IS-IS インターフェイス パラメータの設定 36-74
IS-IS のモニタリングおよびメンテナンス 36-76
BFD の設定 36-78

BFD のデフォルト設定 36-80
BFD のデフォルト設定に関する注意事項 36-80
インターフェイスに対する BFD セッション パラメータの設定 36-80
BFD ルーティング プロトコル クライアントのイネーブル化 36-82
OSFP に対する BFD の設定 36-82
IS-IS に対する BFD の設定 36-83
BGP に対する BFD の設定 36-85
EIGRP に対する BFD の設定 36-86
HSRP に対する BFD の設定 36-86
BFD エコー モードのディセーブル化 36-87
マルチ VRF CE の設定 36-88
マルチ VRF CE の概要 36-88
マルチ VRF CE のデフォルト設定 36-90
マルチ VRF CE の設定時の注意事項 36-91
VRF の設定 36-91
VRF 認識サービスの設定 36-92
ARP のユーザ インターフェイス 36-93
PING のユーザ インターフェイス 36-93
SNMP のユーザ インターフェイス 36-93
HSRP のユーザ インターフェイス 36-94
syslog のユーザ インターフェイス 36-94
traceroute のユーザ インターフェイス 36-95
FTP および TFTP のユーザ インターフェイス 36-95
VPN ルーティング セッションの設定 36-95
BGP PE/CE ルーティング セッションの設定 36-96
マルチ VRF CE の設定例 36-97
マルチ VRF CE ステータスの表示 36-101
プロトコルに依存しない機能の設定 36-101
CEF の設定 36-101
等価コスト ルーティング パスの個数の設定 36-103
スタティック ユニキャスト ルートの設定 36-103
デフォルトのルートおよびネットワークの指定 36-105
ルート マップによるルーティング情報の再配布 36-105
PBR の設定 36-109
PBR 設定時の注意事項 36-110
PBR のイネーブル化 36-111
ルーティング情報のフィルタリング 36-113
受動インターフェイスの設定 36-113
ルーティング アップデートのアドバタイズおよび処理の制御 36-114
ルーティング情報の送信元のフィルタリング 36-115

認証鍵の管理 36-116
IP ネットワークのモニタリングおよびメンテナンス 36-117

CHAPTER 37 IPv6 ユニキャスト ルーティングの設定 37-1
IPv6 の概要 37-1
IPv6 アドレス 37-2
サポート対象の IPv6 ユニキャスト ルーティング機能 37-2
128 ビット幅のユニキャスト アドレス 37-3
IPv6 の DNS 37-4
IPv6 ユニキャストのパス MTU ディスカバリ 37-4
ICMPv6 37-4
近隣探索 37-4
デフォルト ルータ プリファレンス（DRP） 37-4
IPv6 のステートレス自動設定および重複アドレス検出 37-5
IPv6 アプリケーション 37-5
デュアル IPv4 および IPv6 プロトコル スタック 37-5
IPv6 の DHCP アドレス割り当て 37-6
IPv6 のスタティック ルート 37-6
IPv6 の RIP 37-6
IPv6 の OSPF 37-7
EIGRP IPv6 37-7
IPv6 のマルチプロトコル BGP 37-7
IPv6 上の NMP および Syslog 37-7
IPv6 上の HTTP 37-8
サポートされていない IPv6 ユニキャスト ルーティング機能 37-8
制限事項 37-9
IPv6 の設定 37-9
IPv6 のデフォルト設定 37-10
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化 37-10
デフォルト ルータ プリファレンスの設定 37-12
IPv4 および IPv6 プロトコル スタックの設定 37-13
IPv6 の DHCP アドレス割り当ての設定 37-15
DHCPv6 アドレス割り当てのデフォルト設定 37-15
DHCPv6 アドレス割り当ての注意事項 37-15
DHCPv6 サーバ機能のイネーブル化 37-16
DHCPv6 クライアント機能のイネーブル化 37-18
IPv6 ICMP レート制限の設定 37-18
IPv6 の CEF の設定 37-19
IPv6 のスタティック ルーティングの設定 37-19

IPv6 RIP の設定 37-21
IPv6 OSPF の設定 37-22
IPv6 の EIGRP の設定 37-24
IPv6 の BGP の設定 37-24
IPv6 の表示 37-26

CHAPTER 38 **IPv6 MLD スヌーピングの設定** 38-1
MLD スヌーピングの概要 38-1
MLD メッセージ 38-2
MLD クエリー 38-3
マルチキャスト クライアント エージングのロバストネス 38-3
マルチキャスト ルータ ディスカバリ 38-3
MLD レポート 38-4
MLD Done メッセージと即時脱退 38-4
トポロジー変更通知の処理 38-5
IPv6 MLD スヌーピングの設定 38-5
MLD スヌーピングのデフォルト設定 38-5
MLD スヌーピング設定時の注意事項 38-6
MLD スヌーピングのイネーブル化またはディセーブル化 38-6
スタティック マルチキャスト グループの設定 38-8
マルチキャスト ルータ ポートの設定 38-8
MLD 即時脱退のイネーブル化 38-9
MLD スヌーピング クエリーの設定 38-10
MLD リスナー メッセージ抑制のディセーブル化 38-11
MLD スヌーピング情報の表示 38-12

CHAPTER 39 **IPv6 ACL の設定** 39-1
IPv6 ACL の概要 39-2
サポートされている ACL の機能 39-2
IPv6 ACL の制限事項 39-3
IPv6 ACL の設定 39-3
IPv6 ACL のデフォルト設定 39-4
他の機能およびスイッチとの相互作用 39-4
IPv6 ACL の作成 39-4
インターフェイスへの IPv6 ACL の適用 39-7
IPv6 ACL の表示 39-8

CHAPTER 40 **HSRP の設定** 40-1
HSRP の概要 40-1

HSRP のバージョン 40-3
Multiple HSRP 40-4
HSRP の設定 40-5
HSRP のデフォルト設定 40-5
HSRP 設定時の注意事項 40-6
HSRP のイネーブル化 40-6
HSRP のプライオリティの設定 40-8
MHSRP の設定 40-10
HSRP 認証およびタイマーの設定 40-11
ICMP リダイレクト メッセージの HSRP サポートのイネーブル化 40-12
HSRP 設定の表示 40-12

CHAPTER 41 **Cisco IOS IP SLA 動作の設定** 41-1
Cisco IOS IP SLA の概要 41-2
Cisco IOS IP SLA を使用したネットワーク パフォーマンスの測定 41-3
IP SLA レスポンダと IP SLA 制御プロトコル 41-4
IP SLA に対する応答時間の算出 41-4
IP SLA 動作のスケジューリング 41-5
IP SLA 動作のしきい値のモニタリング 41-6
IP SLA 動作の設定 41-6
デフォルト設定 41-6
設定時の注意事項 41-7
IP SLA レスポンダの設定 41-8
UDP ジッタ動作による IP サービス レベルの分析 41-8
ICMP エコー動作による IP サービス レベルの分析 41-11
IP SLA 動作のモニタリング 41-13
TWAMP の概要 41-14
TWAMP の設定 41-15
TWAMP サーバの設定 41-15
TWAMP リフレクタの設定 41-16
TWAMP に関するトラブルシューティング 41-16

CHAPTER 42 **拡張オブジェクト トラッキングの設定** 42-1
拡張オブジェクト トラッキングの概要 42-1
拡張オブジェクト トラッキング機能の設定 42-2
デフォルト設定 42-2
インターフェイス ライン プロトコルまたは IP ルーティング ステートの追跡 42-2
追跡リストの設定 42-3
ブール式を使用した追跡リストの設定 42-4

ウェイトしきい値を使用した追跡リストの設定 42-5
パーセントしきい値を使用した追跡リストの設定 42-6
HSRP オブジェクト トラッキングの設定 42-7
他のトラッキング特性の設定 42-8
IP SLA オブジェクト トラッキングの設定 42-9
スタティック ルーティング サポートの設定 42-10
プライマリ インターフェイスの設定 42-11
Cisco IP SLAs Monitoring Agent および追跡オブジェクトの設定 42-11
ルーティング ポリシーおよびデフォルト ルートの設定 42-12
拡張オブジェクト トラッキングのモニタリング 42-13

CHAPTER 43 イーサネット OAM、CFM、および E-LMI の設定 43-1
イーサネット CFM の概要 43-2
CFM ドメイン 43-2
メンテナンス アソシエーションとメンテナンス ポイント 43-3
CFM メッセージ 43-5
クロスチェック機能およびスタティック リモート MEP 43-5
SNMP トラップと障害アラーム 43-6
設定エラー リスト 43-6
CFM バージョンの相互運用性 43-6
CFM の IP SLAs サポート 43-7
イーサネット CFM の設定 43-7
イーサネット CFM のデフォルト設定 43-8
イーサネット CFM 設定時の注意事項 43-8
CFM ドメインの設定 43-9
イーサネット CFM クロスチェックの設定 43-12
スタティック リモート MEP の設定 43-13
ポート MEP の設定 43-14
SNMP トラップの設定 43-15
障害アラームの設定 43-16
IP SLA CFM 動作の設定 43-17
IP SLA CFM プローブまたはジッタ動作の手動設定 43-18
エンドポイント ディスカバリによる IP SLA 動作の設定 43-20
CFM ITU-T Y.1731 障害管理の概要 43-21
Y.1731 の用語 43-22
アラーム表示信号 43-22
イーサネット リモート障害表示 43-23
イーサネット ロック信号 43-23
マルチキャスト イーサネット ループバック 43-23

Y.1731 障害管理の設定 43-24
デフォルト Y.1731 設定 43-24
ETH-AIS の設定 43-24
ETH-LCK の設定 43-26
マルチキャスト イーサネット ループバックの使用 43-29
イーサネット CFM 情報の管理および表示 43-29
イーサネット OAM プロトコルの概要 43-31
OAM 機能 43-32
OAM メッセージ 43-32
イーサネット OAM のセット アップおよび設定 43-32
イーサネット OAM のデフォルト設定 43-33
イーサネット OAM 設定時の注意事項 43-33
インターフェイス上でのイーサネット OAM のイネーブル化 43-33
イーサネット OAM リモート ループバックのイネーブル化 43-34
イーサネット OAM リンク モニタリングの設定 43-35
イーサネット OAM リモート障害表示の設定 43-38
イーサネット OAM テンプレートの設定 43-39
イーサネット OAM プロトコル情報の表示 43-41
イーサネット ループバックのイネーブル化 43-42
E-LMI の概要 43-46
E-LMI の OAM マネージャとの相互作用 43-46
CFM の OAM マネージャとの相互作用 43-47
E-LMI の設定 43-47
E-LMI のデフォルト設定 43-47
E-LMI および OAM マネージャ設定時の注意事項 43-48
OAM マネージャの設定 43-48
E-LMI のイネーブル化 43-51
イーサネット OAM マネージャの設定例 43-52
PE デバイスの設定 43-52
CE デバイスの設定 43-53
E-LMI および OAM マネージャの情報の表示 43-53
イーサネット CFM とイーサネット OAM の相互作用 43-54
イーサネット OAM の CFM との相互作用の設定 43-54
OAM マネージャの設定 43-55
イーサネット OAM のイネーブル化 43-55
イーサネット OAM および CFM 設定の例 43-56

CHAPTER 44 **IP マルチキャスト ルーティングの設定** 44-1
シスコの IP マルチキャスト ルーティングの実装の概要 44-1

IGMP の概要 44-2
IGMP バージョン 1 44-3
IGMP バージョン 2 44-3
PIM の概要 44-3
PIM のバージョン 44-4
PIM のモード 44-4
PIM スタブ ルーティング 44-5
IGMP ヘルパー 44-6
自動 RP 44-6
BSR 44-7
マルチキャスト転送およびリバース パス チェック 44-7
IP マルチキャスト ルーティングの設定 44-9
マルチキャスト ルーティングのデフォルト設定 44-9
マルチキャスト ルーティング設定時の注意事項 44-9
PIMv1 および PIMv2 の相互運用性 44-10
自動 RP および BSR 設定時の注意事項 44-10
基本的なマルチキャスト ルーティングの設定 44-11
PIM スタブ ルーティングの設定 44-13
PIM スタブ ルーティング設定時の注意事項 44-13
PIM スタブ ルーティングのイネーブル化 44-14
Source-Specific Multicast の設定 44-15
SSM コンポーネントの概要 44-15
Internet Standard Multicast と SSM の相違点 44-15
SSM IP アドレスの範囲 44-16
SSM の動作 44-16
IGMPv3 ホスト シグナリング 44-17
設定時の注意事項 44-17
SSM の設定 44-18
SSM のモニタリング 44-18
Source Specific Multicast マッピングの設定 44-18
設定時の注意事項および制限事項 44-19
SSM マッピングの概要 44-19
SSM マッピングの設定 44-21
SSM マッピングのモニタリング 44-23
RP の設定 44-24
マルチキャスト グループへの RP の手動割り当て 44-24
自動 RP の設定 44-26
PIMv2 BSR の設定 44-30
自動 RP および BSR の使用法 44-34
RP マッピング情報のモニタ 44-35

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング 44-35
高度な PIM 機能の設定 44-36
PIM 共有ツリーおよび送信元ツリーの概要 44-36
PIM SPT 使用の延期 44-37
PIM ルータクエリー メッセージ インターバルの変更 44-38
オプションの IGMP 機能の設定 44-39
IGMP のデフォルト設定 44-39
グループのメンバーとしてのスイッチの設定 44-40
IP マルチキャスト グループへのアクセスの制御 44-41
IGMP バージョンの変更 44-42
IGMP ホストクエリー メッセージ インターバルの変更 44-42
IGMPv2 の IGMP クエリー タイムアウトの変更 44-43
IGMPv2 の最大クエリー応答時間の変更 44-44
スタティックに接続されたメンバーとしてのスイッチの設定 44-44
オプションのマルチキャスト ルーティング機能の設定 44-45
sdr リスナー サポート機能の設定 44-45
sdr リスナー サポート機能のイネーブル化 44-46
sdr キャッシュ エントリの存在期間の制限 44-46
IP マルチキャスト境界の設定 44-47
IP マルチキャスト ルーティングのモニタおよびメンテナンス 44-48
キャッシュ、テーブル、およびデータベースのクリア 44-49
システムおよびネットワーク統計情報の表示 44-49
IP マルチキャスト ルーティングのモニタ 44-50

CHAPTER 45 **MSDP の設定** 45-1
MSDP の概要 45-1
MSDP の動作 45-2
MSDP の利点 45-3
MSDP の設定 45-3
MSDP のデフォルト設定 45-3
デフォルトの MSDP ピアの設定 45-4
SA ステートのキャッシング 45-6
MSDP ピアからの送信元情報の要求 45-8
スイッチから発信される送信元情報の制御 45-8
送信元の再配信 45-9
SA 要求メッセージのフィルタリング 45-10
スイッチで転送される送信元情報の制御 45-11
フィルタの使用法 45-12

SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限 45-13
スイッチで受信される送信元情報の制御 45-13
MSDP メッシュ グループの設定 45-15
MSDP ピアのシャットダウン 45-15
MSDP への境界 PIM DM 領域の追加 45-16
RP アドレス以外の発信元アドレスの設定 45-17
MSDP のモニタおよびメンテナンス 45-17

CHAPTER 46 トラブルシューティング 46-1
ソフトウェアの障害からの回復 46-2
パスワードを忘れた場合の回復 46-3
パスワード回復がイネーブルになっている場合の手順 46-4
パスワード回復がディセーブルになっている場合の手順 46-6
自動ネゴシエーションの不一致の防止 46-8
SFP モジュールのセキュリティと識別 46-8
SFP モジュール ステータスのモニタリング 46-9
温度のモニタリング 46-9
ping の使用 46-10
ping の概要 46-10
ping の使用 46-10
すべてのソフトウェア バージョン 46-11
メトロ IP アクセス イメージ 46-11
ping 応答 46-12
要約 46-12
レイヤ 2 traceroute の使用 46-13
レイヤ 2 traceroute の概要 46-13
レイヤ 2 traceroute の使用上の注意事項 46-13
物理パスの表示 46-14
IP traceroute の使用 46-15
IP traceroute の概要 46-15
IP traceroute の実行 46-15
TDR の使用 46-16
TDR の概要 46-16
TDR の実行および結果の表示 46-17
debug コマンドの使用 46-17
特定の機能に関するデバッグのイネーブル化 46-18
全システム診断のイネーブル化 46-18

デバッグおよびエラー メッセージ出力のリダイレクト 46-18
show platform forward コマンドの使用例 46-19
crashinfo ファイルの使用 46-21
オンボード障害ロギングの使用 46-21
OBFL の概要 46-22
OBFL の設定 46-22
OBFL 情報の表示 46-23

CHAPTER 47 **オンライン診断の設定 47-1**
オンライン診断の概要 47-1
オンライン診断の設定 47-2
スケジューリング オンライン診断 47-2
ヘルス モニタリング診断テストの設定 47-4
オンライン診断テストの実行 47-6
オンライン診断テストの開始 47-6
オンライン診断テストおよび結果の表示 47-7

APPENDIX A **サポートされている MIB A-1**
MIB リスト A-1
FTP による MIB ファイルへのアクセス A-3

APPENDIX B **Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作 B-1**
フラッシュ ファイル システムの操作 B-1
使用可能なファイル システムの表示 B-2
デフォルトのファイル システムの設定 B-3
ファイル システム上のファイルに関する情報の表示 B-3
ディレクトリの変更と作業ディレクトリの表示 B-3
ディレクトリの作成および削除 B-4
ファイルのコピー B-4
ファイルの削除 B-5
tar ファイルの作成、表示、および抽出 B-6
tar ファイルの作成 B-6
tar ファイルの内容の表示 B-6
tar ファイルの抽出 B-7
ファイルの内容の表示 B-8
コンフィギュレーション ファイルの操作 B-8
コンフィギュレーション ファイルの作成および使用に関する注意事項 B-9
コンフィギュレーション ファイルのタイプおよび場所 B-9

テキスト エディタによるコンフィギュレーション ファイルの作成 B-10
TFTP によるコンフィギュレーション ファイルのコピー B-10
TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備 B-10
TFTP によるコンフィギュレーション ファイルのダウンロード B-11
TFTP によるコンフィギュレーション ファイルのアップロード B-12
FTP によるコンフィギュレーション ファイルのコピー B-12
FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備 B-13
FTP によるコンフィギュレーション ファイルのダウンロード B-13
FTP によるコンフィギュレーション ファイルのアップロード B-14
RCP によるコンフィギュレーション ファイルのコピー B-15
RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備 B-16
RCP によるコンフィギュレーション ファイルのダウンロード B-17
RCP によるコンフィギュレーション ファイルのアップロード B-18
設定情報の消去 B-19
スタートアップ コンフィギュレーション ファイルの消去 B-19
格納されたコンフィギュレーション ファイルの削除 B-19
コンフィギュレーションの置換とロールバック B-19
コンフィギュレーションの置換とロールバックの概要 B-19
コンフィギュレーションの置換とロールバックに関する注意事項 B-21
コンフィギュレーション アーカイブの設定 B-21
コンフィギュレーションの置換処理またはロールバック処理の実行 B-22
ソフトウェア イメージの操作 B-23
スイッチ上のイメージの場所 B-24
サーバまたは Cisco.com 上のイメージの tar ファイル形式 B-24
TFTP によるイメージ ファイルのコピー B-25
TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備 B-26
TFTP によるイメージ ファイルのダウンロード B-26
TFTP によるイメージ ファイルのアップロード B-28
FTP によるイメージ ファイルのコピー B-28
FTP によるイメージ ファイルのダウンロードまたはアップロードの準備 B-29
FTP によるイメージ ファイルのダウンロード B-30
FTP によるイメージ ファイルのアップロード B-32
RCP によるイメージ ファイルのコピー B-33
RCP によるイメージ ファイルのダウンロードまたはアップロードの準備 B-34
RCP によるイメージ ファイルのダウンロード B-35
RCP によるイメージ ファイルのアップロード B-37

APPENDIX C Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド C-1

アクセス コントロール リスト C-1
サポートされていない特権 EXEC コマンド C-1
サポートされていないグローバル コンフィギュレーション コマンド C-1
ARP コマンド C-1
サポートされていないグローバル コンフィギュレーション コマンド C-1
サポートされていないインターフェイス コンフィギュレーション コマンド C-2
ブートローダ コマンド C-2
サポートされていないユーザ EXEC コマンド C-2
サポートされていないグローバル コンフィギュレーション コマンド C-2
デバッグ コマンド C-2
Embedded Event Manager C-2
サポートされていない特権 EXEC コマンド C-2
サポートされていないグローバル コンフィギュレーション コマンド C-2
サポートされていない Applet コンフィギュレーション モードのコマンド C-3
HSRP C-3
サポートされていないグローバル コンフィギュレーション コマンド C-3
サポートされていないインターフェイス コンフィギュレーション コマンド C-3
IEEE 802.1x C-3
サポートされていないグローバル コンフィギュレーション コマンド C-3
サポートされていないインターフェイス コンフィギュレーション コマンド C-3
サポートされていない特権 EXEC コマンド C-4
サポートされていないグローバル コンフィギュレーション コマンド C-4
サポートされていないインターフェイス コンフィギュレーション コマンド C-4
IGMP スヌーピング コマンド C-4
サポートされていないグローバル コンフィギュレーション コマンド C-4
インターフェイス コマンド C-5
サポートされていない特権 EXEC コマンド C-5
サポートされていないグローバル コンフィギュレーション コマンド C-5
サポートされていないインターフェイス コンフィギュレーション コマンド C-5
IP マルチキャスト ルーティング C-5
サポートされていない特権 EXEC コマンド C-5
サポートされていないグローバル コンフィギュレーション コマンド C-6
サポートされていないインターフェイス コンフィギュレーション コマンド C-6
IP ユニキャスト ルーティング C-6
サポートされていない特権 EXEC コマンドまたはユーザ EXEC コマンド C-6
サポートされていないグローバル コンフィギュレーション コマンド C-7
サポートされていないインターフェイス コンフィギュレーション コマンド C-7

サポートされていない BGP ルータ コンフィギュレーション コマンド C-8
サポートされていない VPN コンフィギュレーション コマンド C-8
サポートされていないルート マップ コマンド C-8
MAC アドレス C-9
サポートされていない特権 EXEC コマンド C-9
サポートされていないグローバル コンフィギュレーション コマンド C-9
その他 C-9
サポートされていないユーザ EXEC コマンド C-9
サポートされていない特権 EXEC コマンド C-9
サポートされていないグローバル コンフィギュレーション コマンド C-10
サポートされていない show platform コマンド C-10
MSDP C-10
サポートされていない特権 EXEC コマンド C-10
サポートされていないグローバル コンフィギュレーション コマンド C-11
NetFlow C-11
サポートされていないグローバル コンフィギュレーション コマンド C-11
QoS C-11
サポートされていないグローバル コンフィギュレーション コマンド C-11
サポートされていないインターフェイス コンフィギュレーション コマンド C-11
サポートされていない policy-map Class Police Configuration Mode コマンド C-11
RADIUS C-11
サポートされていないグローバル コンフィギュレーション コマンド C-11
SNMP C-12
サポートされていないグローバル コンフィギュレーション コマンド C-12
スパニングツリー C-12
サポートされていないグローバル コンフィギュレーション コマンド C-12
サポートされていないインターフェイス コンフィギュレーション コマンド C-12
ストーム制御 C-12
サポートされていないグローバル コンフィギュレーション コマンド C-12
サポートされていないインターフェイス コンフィギュレーション コマンド C-12
VLAN C-13
サポートされていないグローバル コンフィギュレーション コマンド C-13
サポートされていないユーザ EXEC コマンド C-13
サポートされていない VLAN データベース コマンド C-13

INDEX

はじめに

対象読者

このマニュアルは、Cisco Metro Ethernet（ME）3400E シリーズ イーサネット アクセス スイッチ（以降、*スイッチ*と記載）を管理するネットワーキングの専門家を対象としたものです。このマニュアルを使用するには、イーサネットと LAN の概念および用語についての知識が必要です。これらの分野に関してさらに詳細なトレーニングや教育を受けたい方には、次の URL にある Cisco Training & Events Web ページでトレーニング コース、自習オプション、セミナー、および技術者認定プログラムを含めた学習機会を提供しています。

http://www.cisco.com/web/learning/index.html

目的

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

- メトロ アクセス イメージは、IEEE 802.1Q トンネリング、レイヤ 2 プロトコル トンネリング、ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査、IP ソース ガードなどの追加機能を備えています。
- メトロ IP アクセス イメージでは、Routing Information Protocol（RIP）、Open Shortest Path First（OSPF）Protocol、Border Gateway Protocol（BGP）、および Enhanced Interior Gateway Routing Protocol（EIGRP）に対する IP ルーティングのサポート、Customer Edge（CE; カスタマー エッジ）デバイスの複数の VPN ルーティング/転送（マルチ VRF-CE）デバイス、および IP マルチキャスト ルーティングなどのレイヤ 3 機能が追加されています。

このマニュアルでは、Cisco ME 3400E スイッチで使用するために作成または変更されたコマンドの使用手順を扱っています。これらのコマンドについては、詳しい説明は行っていません。コマンドの詳細については、このリリースの『*Cisco ME 3400E Ethernet Access Switch Command Reference*』を参照してください。標準の Cisco IOS コマンドについては、次の URL の Cisco IOS 資料を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html

また、表示されるシステム メッセージやスイッチの設置方法については取り扱っていません。詳細については、このリリースの『*Cisco ME 3400 and ME 2400 Switch System Message Guide*』および『*Cisco ME 3400E Ethernet Access Switch Hardware Installation Guide*』を参照してください。

マニュアルの最新情報については、このリリースのリリース ノートを参照してください。

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

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

対話形式の例では、次の表記法を使用しています。

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

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

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

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

関連資料

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

http://www.cisco.com/en/US/products/ps9637/tsd_products_support_series_home.html

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

- 初期設定については、ハードウェア インストレーション ガイドの付録「Configuring the Switch with the CLI-Based Setup Program」を参照してください。
- アップグレード情報については、リリース ノートの「Downloading Software」を参照してください。

- 『*Release Notes for the Cisco ME 3400E Ethernet Access Switch*』
- 『*Cisco ME 3400E Ethernet Access Switch Software Configuration Guide*』
- 『*Cisco ME 3400E Ethernet Access Switch Command Reference*』
- 『*Cisco ME 3400E, ME 3400, and ME 2400 Switch System Message Guide*』
- 『*Cisco ME 3400E Ethernet Access Switch Hardware Installation Guide*』

- 『*Cisco ME 3400E Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Cisco ME 3400E Ethernet Access Switch*』
- 『*Cisco Small Form-Factor Pluggable Modules Installation Notes*』
- 『*Cisco CWDM GBIC and CWDM SFP Installation Note*』
- これらの互換性マトリクス ドキュメントは、Cisco.com の次のページで入手可能です。

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

  - 『*Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*』
  - 『*Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*』
  - 『*Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*』
  - 『*Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*』

マニュアルの入手方法およびテクニカル サポート

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

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

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

CHAPTER 1

概要

この章では、Cisco Metro Ethernet（ME）3400E シリーズ イーサネット アクセス スイッチ ソフトウェアについて説明します。具体的な内容は次のとおりです。

- 「機能」（P.1-1）
- 「スイッチ初期設定後のデフォルト設定値」（P.1-13）
- 「ネットワークの構成例」（P.1-16）
- 「次の作業」（P.1-19）

このマニュアル内では、「IP」と表記した場合は IP バージョン 4（IPv4）を表すものとし、IP バージョン 6 を表す場合は「IPv6」と明記します。

機能

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

- メトロ アクセス イメージは、IEEE 802.1Q トンネリング、レイヤ 2 プロトコル トンネリング、ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査、IP ソース ガードなどの追加機能を備えています。
- メトロ IP アクセス イメージは、Routing Information Protocol（RIP）、Open Shortest Path First（OSPF）プロトコル、Border Gateway Protocol（BGP）、および Enhanced Interior Gateway Routing Protocol（EIGRP）に対する IP ルーティングのサポート、Intermediate System-to-Intermediate System（IS-IS）ダイナミック ルーティング、Bidirectional Forwarding Detection （BFD; 双方向フォワーディング検出）プロトコル、Customer Edge（CE; カスタマーエッジ）デバイスの Multiple VPN Routing/Forwarding（マルチ VRF）インスタンス（マルチ VRF CE）、および IP マルチキャスト ルーティングの Protocol-Independent Multicast（PIM）の sparse（希薄）モード（SM）および dense（稠密）モード（DM）などのレイヤ 3 機能が追加されています。

（注） 特記されていないかぎり、この章およびこのマニュアルで説明されている機能はいずれも、すべてのイメージでサポートされています。

この章で特記されている機能の中には、スイッチ ソフトウェア イメージの暗号化（暗号化をサポートしている）バージョンでだけ使用可能なものもあります。こうした機能を使用するには、その使用権限を取得し、Cisco.com からソフトウェアの暗号化バージョンをダウンロードする必要があります。詳細については、このリリースのリリース ノートを参照してください。

Cisco ME スイッチには、Network Node Interface（NNI; ネットワーク ノード インターフェイス）および User Network Interface（UNI; ユーザ ネットワーク インターフェイス）という 2 つのタイプのインターフェイスがデフォルトで用意されています。NNI はサービス プロバイダー ネットワークへの接続に使用され、UNI は顧客ネットワークへの接続に使用されます。一部の機能は、このいずれかのポート タイプでだけサポートされます。また、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）を設定することもできます。ENI は通常、ユーザ ネットワーク側インターフェイスとして使用され、そのデフォルト設定および機能は UNI と同じです。ただし、設定により Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）、Link Layer Discovery Protocol（LLDP; リンク レイヤ検出プロトコル）、および EtherChannel の Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）または Port Aggregation Protocol（PAgP; ポート集約プロトコル）用のプロトコル制御パケットをサポートできます。

- 「パフォーマンスの特長」（P.1-2）
- 「管理オプション」（P.1-3）
- 「管理機能」（P.1-4）（ソフトウェアの暗号化バージョンを必要とする機能を含む）
- 「アベイラビリティ機能」（P.1-6）
- 「VLAN 機能」（P.1-7）
- 「セキュリティ機能」（P.1-7）（スイッチ ソフトウェアの暗号化バージョンを必要とする機能を含む）
- 「QoS 機能および CoS 機能」（P.1-9）
- 「レイヤ 2 VPN サービス」（P.1-10）
- 「レイヤ 3 機能」（P.1-11）（メトロ IP アクセス イメージが必要）
- 「レイヤ 3 VPN サービス」（P.1-12）（メトロ IP アクセス イメージが必要）
- 「モニタリング機能」（P.1-12）

パフォーマンスの特長

- すべてのスイッチ ポートにおけるポート速度の自動検知とデュプレックス モードの自動ネゴシエーションにより、帯域利用が最適化されます。
- 10/100 Mbps インターフェイスと 10/100/1000 Mbps インターフェイス、および 10/100/1000 BASE-T/TX Small Form-factor Pluggable（SFP）モジュール インターフェイス上の Automatic Medium-Dependent Interface crossover（Auto MDIX）機能によって、インターフェイスは必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定できます。
- ルーテッド フレームの場合は最大 1998 バイト、ハードウェアでブリッジングされるフレームの場合は最大 9000 バイト、ソフトウェアでブリッジングされるフレームの場合は最大 2000 バイトのサポートを実現します。
- すべてのポートで IEEE 802.3x フロー制御（スイッチは、ポーズ フレームを送信しない）を行います。
- EtherChannel により、耐障害性を高め、スイッチ、ルータ、およびサーバ間に最大 8 Gbps（ギガビット EtherChannel）または 800 Mbps（ファスト EtherChannel）の全二重の帯域幅を確保します。
- PAgP および LACP により EtherChannel リンク（NNI または ENI に限りサポート）が自動的に作成されます。
- レイヤ 2 およびレイヤ 3 パケットをギガビット回線レートで転送します。

- ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストーム防止用のポート単位のストーム制御を行います。
- レイヤ 2 の不明なユニキャスト トラフィック、マルチキャスト トラフィック、およびブリッジド ブロードキャスト トラフィックの転送時にポート ブロッキングを行います。
- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）バージョン 1、2、および 3 の IGMP スヌーピングにより、マルチメディア トラフィックおよびマルチキャスト トラフィックを効率的に転送できます。
- IGMP レポート抑制により、マルチキャスト ルータのクエリーごとに 1 つの IGMP レポートがマルチキャスト デバイスに送信されます（IGMPv1 クエリーまたは IGMPv2 クエリーに限りサポート）。
- IGMP スヌーピング クエリアのサポートにより、IGMP 一般クエリー メッセージが定期的に生成されるようにスイッチを設定できます。
- IGMP ヘルパーにより、マルチキャスト ストリームへのホスト加入要求を、スイッチから特定の IP 宛先アドレスへ転送できます（メトロ IP アクセス イメージが必要）。
- Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）により、マルチキャスト VLAN 内でマルチキャスト ストリームを継続的に送信し、かつ帯域幅およびセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離できます。各スイッチ上では最大 512 のマルチキャスト エントリがサポートされています。
- MVR over trunk port（MVRoT）のサポートにより、トランク ポートを MVR 受信ポートとして設定できます。
- IGMP フィルタリングにより、スイッチ ポート上のホストが所属できるマルチキャスト グループ セットを管理できます。
- IGMP スロットリングにより、IGMP 転送テーブル内のエントリ数が上限に達した場合のアクションを設定できます。
- 設定可能な IGMP 脱退タイマーにより、ネットワークの脱退遅延を設定します。
- Switch Database Management（SDM; スイッチ データベース管理）テンプレートにより、ユーザが選択した機能を最大限サポートできるようなシステム リソースの割り当てを行えます。また、IPv6 アドレスのサポート用として、デュアル IPv4/IPv6 テンプレートが用意されています。
- RADIUS サーバのロード バランシングにより、アクセス要求や認証要求がサーバ グループ全体で均等に分散されます。
- MVR の拡張機能として、スイッチがダイナミック MVR モードの場合には最大 2000 の MVR グループを設定できるだけでなく、新たに追加されたコマンド（**mvr ringmode flood**）を使用することで、リング トポロジでの転送をメンバー ポートに制限できます。

管理オプション

- Command Line Interface（CLI; コマンドライン インターフェイス）: Cisco IOS ソフトウェアでは、デスクトップ スイッチング機能および Multilayer Switching（MLS; マルチレイヤ スイッチング）機能がサポートされています。CLI には、スイッチのコンソール ポートに直接管理ステーションを接続するか、リモート管理ステーションから Telnet を使用してアクセスできます。CLI の詳細については、第 2 章「CLI の使用方法」を参照してください。
- Cisco Configuration Engine : Cisco Configuration Engine は、スイッチ ソフトウェアに組み込まれた Cisco IOS CNS エージェントと連携するネットワーク管理デバイスです。スイッチ固有の設定変更を生成してスイッチに送信し、設定変更を実行して結果をロギングすることで、初期設定および設定更新を自動化できます。Cisco IOS エージェントの使用に関する詳細については、第 4 章「Cisco IOS Configuration Engine の設定」を参照してください。

- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）: SNMP 管理アプリケーションには、CiscoWorks2000 LAN Management Suite（LMS）や HP OpenView などがあります。HP OpenView や SunNet Manager などのプラットフォームが稼動している SNMP 対応管理ステーションを使用してスイッチを管理できます。スイッチは、広範囲の拡張 Management Information Base（MIB; 管理情報ベース）セットおよび 4 種類の （RMON; リモート モニタリング）グループをサポートしています。SNMP の詳細については、第 30 章「SNMP の設定」を参照してください。

管理機能

（注）　ここに列挙した暗号化 Secure Shell（SSH；セキュア シェル）機能は、スイッチ ソフトウェア イメージの暗号化バージョンでだけ使用できます。

- IP アドレス、デフォルト ゲートウェイ、ホスト名、Domain Name System（DNS; ドメイン ネーム システム）、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ名などのスイッチ情報の設定に関して、Dynamic Host Configuration Protocol（DHCP）をサポートします。
- DHCP リレーにより、IP アドレス要求など DHCP クライアントからの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ブロードキャストが転送されます。
- DHCP サーバにより、IP アドレスおよびその他の DHCP オプションが IP ホストに自動で割り当てられます。
- DHCP ベースの自動設定およびイメージ アップデートにより、指定された設定および新しいイメージが多数のスイッチにダウンロードされます。
- DHCP サーバによるポート ベースのアドレス割り当てにより、スイッチ ポートには IP アドレスが事前に割り当てられます。
- DNS サーバへの有向ユニキャスト要求により、IP アドレスおよび対応ホスト名からスイッチを特定できるほか、TFTP サーバへの有向ユニキャスト要求により、ソフトウェア アップグレードを TFTP サーバから管理できます。
- ARP によって、IP アドレスおよび対応 MAC アドレスからスイッチを特定できます。
- ユニキャスト MAC アドレス フィルタリングにより、特定の送信元 MAC アドレスまたは宛先 MAC アドレスを持つパケットを廃棄できます。
- 設定可能な MAC アドレス スケーリングにより、VLAN 上での MAC アドレス学習をディセーブルにして、MAC アドレス テーブルのサイズを制限できます。
- CDP バージョン 1 および 2 により、ネットワーク トポロジを検出できるだけでなく、そのネットワーク上にあるスイッチやその他のシスコ製デバイスを相互にマッピングできます（NNI ではデフォルトでサポート、ENI ではイネーブル化可能、UNI ではサポートなし）。
- LLDP および LLDP Media Endpoint Discovery（LLDP-MED）により、サードパーティ製の IP 電話との相互運用性が実現されます（NNI または ENI でだけサポート）。
- LLDP-MED ロケーション TLV のサポートにより、スイッチからエンドポイント デバイスへロケーション情報が送信されます。
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）により、外部ソースから全スイッチへ一貫したタイム スタンプが提供されます。
- Cisco IOS File System（IFS）により、スイッチが使用するすべてのファイル システムに対して共通のインターフェイスを使用できます。

- 帯域内管理アクセスにより、ネットワーク上の複数の CLI ベース セッションに対して、最大 16 の Telnet 接続を同時に行えます。
- 帯域内管理アクセスにより、ネットワーク上の複数の CLI ベース セッションに対して、最大 5 つの暗号化 SSH 接続を同時に行えます（スイッチ ソフトウェアの暗号化バージョンが必要）。
- SNMP バージョン 1、2c、3 の get 要求および set 要求を介した帯域内管理アクセスが可能です。
- スイッチのコンソール ポートから、直接接続された端末への帯域外管理アクセスや、シリアル接続またはモデムを経由したリモート ターミナルへの帯域外管理アクセスが可能です。
- イーサネット管理ポートから PC への帯域外管理アクセスが可能です。
- ユーザ定義のコマンド マクロにより、複数のスイッチ間の配置を単純化するカスタム スイッチ設定を作成できます。
- メトロ イーサネットの Operation, Administration, and Maintenance（OAM; 運用管理および保守）IEEE 802.1ag Connectivity Fault Management（CFM）、カスタマーエッジ スイッチおよびプロバイダーエッジ スイッチにおける Ethernet Line Management Interface（E-LMI）、IEEE 802.3ah イーサネット OAM ディスカバリ、リンク モニタリング、リモート障害検知、およびリモート ループバックをサポートしています。
- イーサネット ループバック機能のサポートにより、リモート デバイスへの接続をテストできます。無停止ループバック テストを行うための VLAN ループバックと、全パスの QoS（Quality Of Service）を双方向でテストするための端末ループバックがあります（メトロ IP アクセス イメージが必要）。
- コンフィギュレーションの置換およびロールバックにより、スイッチ上の実行コンフィギュレーションを、保存されている Cisco IOS コンフィギュレーション ファイルで置換できます。
- Source Specific Multicast（SSM）マッピングにより、マルチキャスト アプリケーションでは送信元のマッピングが可能になります。これにより、IGMPv2 クライアントは SSM を利用できるようになり、リスナーはマルチキャストの送信元にダイナミックに接続できるようになります。またアプリケーションへの依存度も軽減されます。
- Cisco IOS でサポートされている HTTP クライアントは、IPv4 HTTP サーバおよび IPv6 HTTP サーバのどちらに対しても要求を送信できます。また Cisco IOS でサポートされている HTTP サーバは、IPv4 HTTP クライアントおよび IPv6 HTTP クライアントのどちらから送信された HTTP 要求も処理できます（メトロ IP アクセス イメージが必要）。
- IPv6 では、ステートレス自動設定がサポートされています。これにより、リンク、サブネット、およびサイトのアドレス指定変更を管理できます。ホスト IP アドレスやモバイル IP アドレスの管理に有用です（メトロ IP アクセス イメージが必要）。
- CPU 利用率のしきい値トラップにより、CPU の利用率をモニタできます。
- DHCPDISCOVER パケットの Option 12 フィールドにホスト名を指定できます。これにより、DHCP プロトコルを使用して同一のコンフィギュレーション ファイルを送信できます。
- DHCP スヌーピングの機能拡張として、DHCP の Option 82 フィールドの回線 ID サブオプションに対して固定型ストリング ベース フォーマットを選択できるようになっています。

アベイラビリティ機能

- UniDirectional Link Detection（UDLD; 単方向リンク検出）およびアグレッシブ UDLD により、不適切な光ファイバ配線またはポート障害によって生じる光ファイバ インターフェイス上の単方向リンクを検出してディセーブル化できます。
- IEEE 802.1D Spanning Tree Protocol（STP; スパニング ツリー プロトコル）により、冗長バックボーン接続とループのないネットワークを実現できます（NNI ではデフォルトでサポート、ENI ではイネーブル化可能、UNI ではサポートなし）。STP には次の機能があります。
  - 最大 128 のスパニング ツリー インスタンスをサポート
  - Per-VLAN Spanning-Tree Plus（PVST+）による VLAN 間のロード バランシング
  - Rapid Per-VLAN Spanning-Tree Plus（rapid-PVST+）による VLAN 間のロード バランシングとスパニング ツリー インスタンスの高速コンバージェンス
- NNI または ENI で動作する IEEE 802.1s Multiple Spanning-Tree Protocol（MSTP; マルチ スパニング ツリー プロトコル）により、複数の VLAN をスパニング ツリー インスタンスにグループ化できるほか、データ トラフィックとロード バランシングに使用するフォワーディング パスを複数構成できます。さらに、IEEE802.1w Rapid Spanning-Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）をベースにした rapid PVST+ により、ルートおよび指定ポートの NNI またはスパニング ツリー対応の ENI を即座にフォワーディング ステートへ移行することでスパニング ツリーの高速コンバージェンスが可能です。
- スパニング ツリーがイネーブルになっている NNI および ENI では、Optional spanning-tree features available in PVST+ モード、rapid-PVST+ モード、および MSTP モードで、次のようなオプションのスパニング ツリー機能を使用できます。
  - PortFast：スパニング ツリー ポートをブロッキング ステートからフォワーディング ステートに即時に移行することで転送遅延を解消
  - Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガード：BPDU を受信する PortFast 対応のポートをシャット ダウン
  - BPDU フィルタリング：PortFast 対応のポートで BPDU が送受信されるのを防止
  - ルート ガード機能：ネットワーク コア外のスイッチがスパニング ツリー ルートとして使用されるのを防止
  - ループ ガード：単方向リンクを引き起こす障害によって代替ポートまたはルート ポートである NNI または ENI が指定ポートとして使用されるのを防止
- STP の代替手段として相互にバックアップする Flex Link レイヤ 2 インターフェイスと、プリエンプションされるスイッチオーバーおよび双方向高速コンバージェンスにより、ループのないネットワークでの基本的なリンク冗長性が確保されます。MAC アドレス テーブル移行更新機能とも呼ばれます。
- Flex Link マルチキャスト高速コンバージェンスにより、Flex Link に障害が発生したあとのマルチキャスト トラフィックのコンバージェンス時間が短縮されます。
- リンクステート トラッキングにより、接続されたホストおよびサーバからのアップストリーム トラフィックを伝送するポートのステートをミラーリングし、他の Cisco Ethernet スイッチ上の動作リンクにサーバ トラフィックをフェールオーバーできます。
- Resilient Ethernet Protocol（REP; レジリエント イーサネット プロトコル）により、スパニング ツリーを使用しないコンバージェンス時間の短縮とネットワーク ループ防止が可能です。
- REP のサポートに合せてカウンタおよびタイマーの機能が拡張されています。ネイバー ポートが REP に対応していない場合に REP エッジ ポートを使用できます。
- Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）により、レイヤ 3 ルータの冗長性が確保されます（メトロ IP アクセス イメージが必要）。

- 等価コスト ルーティングにより、リンク レベルおよびスイッチ レベルでの冗長性が確保されます（メトロ IP アクセス イメージが必要）。
- Shorter REP hello により、REP Link Status Layer（LSL; リンク ステータス レイヤ）の経過時間タイマーの範囲が 3000 ～ 10000 ミリ秒（500 ミリ秒間隔）から 120 ～ 10000 ミリ秒（40 ミリ秒間隔）に変更されています。

VLAN 機能

- 最大 1005 の VLAN がサポートされているため、ユーザを適切なネットワーク リソース、トラフィック パターン、および帯域に対応付けられた VLAN に割り当てることが可能です。
- IEEE 802.1Q 標準によって許可された 1 ～ 4094 の範囲の VLAN ID が完全にサポートされています。
- VLAN Query Protocol（VQP; VLAN クエリー プロトコル）により、ダイナミック VLAN メンバーシップがサポートされています。
- 全ポートでの IEEE 802.1Q トランキング カプセル化により、ネットワークの移動、追加、および変更、ブロードキャストおよびマルチキャスト トラフィックの管理と制御、高度なセキュリティを要するユーザやネットワーク リソースに対して VLAN グループを作成することによるネットワーク セキュリティが実現されています。
- VLAN 1 の最小化によって、VLAN 1 を個々の VLAN トランク リンクでディセーブル化できます。これにより、スパニング ツリー ループまたはストームのリスクが軽減されます。この機能をイネーブルにすると、ユーザ トラフィックはトランク上では送受信されません。スイッチ CPU は、これまでどおり制御プロトコル フレームを送受信します。
- UNI-ENI 独立 VLAN により、カスタマー VLAN を、同一スイッチ上の他のカスタマー VLAN から分離できます。同一の UNI-ENI 独立 VLAN に属するスイッチでは、UNI または ENI 間のローカル スイッチングが実行されません。
- プライベート VLAN により、VLAN のスケーラビリティの問題に対処できるほか、IP アドレスの割り当てをより細かく制御したり、レイヤ 2 ポートを他のスイッチ上のポートから分離したりできます。
- PVLAN ホストのポート セキュリティにより、ポートで学習される MAC アドレスの数を制限できるほか、ポートで学習できる MAC アドレスを定義できます。
- VLAN Flex Link ロード バランシングにより、STP を使用することなく、レイヤ 2 の冗長性を確保できます。プライマリ リンクおよびバックアップ リンクとして設定されるインターフェイスのペアにより、VLAN に基づいてトラフィックの負荷を分散できます。
- カスタマー ネットワークに接続されたトランク ポート上での VLAN マッピング（または VLAN ID 変換）により、Customer VLAN（C-VLAN; カスタマー VLAN）を Service Provider VLAN（S-VLAN; サービス プロバイダー VLAN）にマッピングできます。

セキュリティ機能

スイッチは、加入者、スイッチ、およびネットワークに対するセキュリティ機能を備えています。

加入者に対するセキュリティ

- デフォルトでは、各加入者の独立性を確保するため、加入者ポート間のローカル スイッチングはディセーブルに設定されています。

- DHCP スヌーピングにより、信頼できないホストと DHCP サーバの間で、信頼できない DHCP メッセージのフィルタリング処理を行えます。
- DHCP スヌーピング統計情報の **show** コマンドにより、DHCP スヌーピング統計情報をサマリー形式または詳細形式で表示できます。また **clear** コマンドにより、DHCP スヌーピング統計情報を削除できます。
- IP ソース ガードにより、DHCP スヌーピング データベースおよび IP 送信元バインディングに基づいて、ルーティングされないインターフェイス上でトラフィックを制限できます。
- ダイナミック ARP 検査により、無効な ARP 要求や応答を同じ VLAN 内の他のポートにリレーしないことで、スイッチに対する悪意のある攻撃を防御できます。

スイッチ セキュリティ

（注） ここに示した Kerberos 機能は、スイッチ ソフトウェア イメージの暗号化バージョンでだけ使用できます。

- パスワードによって保護された管理インターフェイスへのアクセス（読み取り専用および読み取り/書き込み）により、不正な設定変更を防止できます。
- 認証および許可されたユーザに限ってコンフィギュレーション ファイルにアクセスできるようにしたコンフィギュレーション ファイル セキュリティ機能によって、ユーザがパスワード回復プロセスを使用してコンフィギュレーション ファイルにアクセスするのを防止できます。
- マルチレベルのセキュリティにより、セキュリティ レベル、通知、および対応動作を選択できます。
- ポート セキュリティ オプションにより、ポートへのアクセスを許可するステーションの MAC アドレスを制限したり識別したりできます。
- ポート セキュリティ エージングにより、ポート上のセキュア アドレスに対してエージング タイムを設定できます。
- LLDP および LLDP-Media Extensions（LLDP-MED; LLDP メディア拡張）により、マルチベンダー ネットワークでの相互運用性に対して IEEE 802.1AB リンク レイヤ検出プロトコルがサポートされます。スイッチは、速度、デュプレックス、および電力の設定を IP 電話などのエンド デバイスと交換します。
- UNI および ENI のデフォルト ポート ステートはディセーブルです。
- 自動コントロール プレーン保護機能により、UNI または ENI 上のレイヤ 2 制御トラフィックによって偶発的または意図的に生じる過負荷から CPU が保護されます。
- サービス プロバイダーの柔軟な対応を可能にする設定可能コントロール プレーン セキュリティ機能により、カスタマーのコントロール プレーン トラフィックをポート単位およびプロトコル単位で廃棄できます。CDP、STP、LLDP、LACP、または PAgP に対して ENI プロトコル制御パケットを設定できます。
- Terminal Access Controller Access Control System Plus（TACACS+）は、TACACS サーバを介してネットワーク セキュリティを管理するシスコ独自の機能です。
- Remote Authentication Dial-In User Service（RADIUS）により、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サービスを使用して、リモート ユーザの ID の検証、アクセスの許可、およびアクションの追跡を実行できます。
- Kerberos セキュリティ システムにより、信頼できる第三者を通じてネットワーク リソースの要求を認証できます（スイッチ ソフトウェアの暗号化バージョンが必要）。

ネットワーク セキュリティ

- スタティック MAC アドレス指定を使用することで、セキュリティを確保できます。
- 標準および拡張 IP Access Control List（ACL; アクセス制御リスト）により、ルーテッド インターフェイス（ルータ ACL）と VLAN の両方向およびレイヤ 2 インターフェイス（ポート ACL）の受信方向に関するセキュリティ ポリシーを定義できます。
- インターフェイスに適用される IPv6 ACL により、IPv6 トラフィックのフィルタリングを行えます。
- 拡張 MAC ACL により、レイヤ 2 インターフェイスの受信方向に関するセキュリティ ポリシーを定義できます。
- VLAN ACL（VLAN マップ）により、MAC ヘッダー、IP ヘッダー、および TCP/UDP ヘッダー内の情報を基にしたトラフィックのフィルタリングを行い、VLAN 内のセキュリティを確保できます。
- 送信元および宛先 MAC ベースの ACL により、非 IP トラフィックのフィルタリングを行えます。
- IEEE 802.1X ポートベースの認証により、不正なデバイス（クライアント）がネットワークにアクセスするのを防止できます。次の機能がサポートされています。
  - VLAN 割り当て：IEEE 802.1X 認証ユーザを特定の VLAN に制限できます。
  - ポート セキュリティ：IEEE 802.1X ポートへのアクセスを制御できます。
  - IEEE 802.1X アカウンティング：ネットワークの使用状況を追跡できます。
  - 802.1x 準備状態チェック：スイッチ上で 802.1x の設定を行う前に、接続されているエンド ホストの準備状態を判定できます。
  - 802.1x スイッチ サプリカントによる Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）、Client Information Signalling Protocol（CISP; クライアント情報シグナリング プロトコル）によるホスト許可、および自動イネーブル化：ワイヤリング クローゼット外部のスイッチを、他のスイッチに対するサプリカントとして認証できます。
- スタティック ホスト上では、IP ソース ガードがサポートされています。
- IEEE 802.1x ユーザ分散により、複数の VLAN でユーザのロードバランシングを行えます。これにより、複数の VLAN が配置されたネットワークのスケーラビリティを向上させることが可能です。認可されたユーザは、RADIUS サーバにより割り当てられたグループ内でメンバーが最も少ない VLAN に割り当てられます。
- SNMP バージョン 3（SNMPv3）で Triple Data Encryption Standard（3DES; トリプル DES）および Advanced Encryption Standard（AES; 高度暗号化規格）がサポートされています。このリリースでは、SNMPv3 に対する暗号化アルゴリズムとして、168 ビットの 3DES および 128 ビット、192 ビット、および 256 ビットの AES が新たにサポートされています。
- IPv6 MLD スヌーピング、IPv6 eBGP、IPv6 SNMP、syslog、HTTP を含め、IPv6 が追加サポートされています。

QoS 機能および CoS 機能

- 設定可能コントロール プレーン キュー割り当てにより、CPU で生成されたトラフィックのコントロール プレーン トラフィックを、特定の出力キューに割り当てることが可能です。
- Cisco Modular Quality of Service Command Line Interface（MQC; モジュラ QoS コマンドライン インターフェイス）が実装されています。

- IP precedence、Differential Service Code（DSCP）、および IEEE 802.1p Class of Service（CoS; サービス クラス）パケット フィールドに基づく分類、ACL 検索、または出力分類への QoS ラベルの割り当てが可能です。
- ポリシング
  - 平均レートおよびバースト レートに基づく 1 レート ポリシング：1 つのポリサーが対象
  - 2 カラー ポリシング：レートに適合するパケットまたはレートを超過するパケットにより異なる動作を許可
  - 集約ポリシング：複数のトラフィック クラスで共有されるポリサーが対象
  - 入力 2 レート、3 カラー ポリシング：個別のポリサーまたは集約ポリサーが対象
- 輻輳回避メカニズムである Weighted Tail Drop（WTD; 重み付きテール ドロップ）により、キューの長さを管理し、異なるトラフィック分類ごとに廃棄優先順位を決定できます。
- テーブル マップにより、DSCP、CoS、IP precedence の各値をマッピングできます。
- キューイングおよびスケジューリング。
  - Shaped Round Robin（SRR; シェイプド ラウンド ロビン）トラフィック シェーピングにより、すべてのキューのパケットを混在させて、トラフィック バーストを最小化できます。
  - クラスベース トラフィック シェーピングにより、トラフィック クラスの最大許容平均レートを指定できます。
  - ポート シェーピングにより、ポートの最大許容平均レートを指定できます。
  - Class-based Weight Queuing（CBWFQ; クラス ベース均等化キューイング）により、トラフィック クラスに合せて帯域幅を制御できます。
  - WTD により、指定されたトラフィック クラスのキュー サイズを調整できます。
  - 低遅延プライオリティ キューイングにより、特定のトラフィックへの優先処理を許可できます。
- ポート単位、VLAN 単位 QoS により、所定のインターフェイスのユーザ指定 VLAN で伝送されるトラフィックを制御できます。IOS ソフトウェア リリース 12.2（25）SEG 以降では、VLAN 単位の分類に階層型ポリシーマップを使用して、トランク ポートにポート単位、VLAN 単位の階層型ポリシー マップを適用できます。
- CPU 保護をディセーブルにするオプションにより、使用できる QoS ポリシング機能が、1 ポートにつき 45 から 64 （4 ポートごとに 63）に増加しました。

レイヤ 2 VPN サービス

- IEEE 802.1Q トンネリングにより、サービス プロバイダーはカスタマーに複数のポイント レイヤ 2 VPN サービスを提供できます。
- レイヤ 2 プロトコル トンネリングにより、カスタマーは BPDU、CDP、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）、PAgP、LACP、および UDLD などのプロトコルを制御して、サービス プロバイダー ネットワーク間でトンネリングを行えます。
- カスタマー ネットワークに接続されたトランク ポート上での VLAN マッピング（または VLAN ID 変換）により、Customer VLAN（C-VLAN; カスタマー VLAN）を Service Provider VLAN（S-VLAN; サービス プロバイダー VLAN）にマッピングできます。

レイヤ 3 機能

（注）　レイヤ 3 機能は、スイッチでメトロ IP アクセス イメージが稼動している場合に限り使用できます。

- HSRP バージョン 1（HSRPv1）および HSRP バージョン 2（HSRPv2）により、レイヤ 3 ルータの冗長性が確保されます。
- 次の IP ルーティング プロトコルにより、ロード バランシングとスケーラブルなルーテッド バックボーンを構築できます。
  - RIP バージョン 1 および 2
  - OSPF
  - EIGRP
  - BGP バージョン 4
  - IS-IS ダイナミック ルーティング
  - BFD プロトコル：OSPF、IS-IS、BGP、EIGRP、または HSRP の各ルーティング プロトコルのフォワーディング パス障害を検出できます。
- 2 つ以上の VLAN 間における完全レイヤ 3 ルーティングに対応した IP ルーティング（VLAN 間ルーティング）により、各 VLAN は独自の自律データリンク ドメインを維持できます。
- Policy-Based Routing（PBR; ポリシー ベース ルーティング）により、トラフィック フローに定義済みポリシーを設定できます。
- スタティック IP ルーティングにより、ネットワーク パス情報のルーティング テーブルを手動で作成できます。
- 等価コスト ルーティングにより、ロード バランシングおよび冗長構成が可能です。
- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）および ICMP Router Discovery Protocol（IRDP）により、ルータのアドバタイズメントおよびルータ請求メッセージを使用して、直接接続されたサブネット上にあるルータのアドレスを検出できます。
- PIM により、ネットワーク内でのマルチキャスト ルーティングが可能です。これにより、ネットワーク内のデバイスは要求されたマルチキャスト フィードを受信できるほか、マルチキャストに参加しないスイッチをプルーニングできます。PIM-SM モード、PIM-DM モード、および PIM sparse-dense モードもサポートされています。
- SSM PIM プロトコルのサポート：ビデオなどのマルチキャスト アプリケーションを最適化できます。
- Multicast Source Discovery Protocol（MSDP）により、複数の PIM-SM ドメインを接続できます。
- DHCP リレーにより、IP アドレス要求など DHCP クライアントからの UDP ブロードキャストを転送できます。
- DHCP for IPv6 のリレー、クライアント、サーバ アドレス割り当て、およびプレフィクス委任がサポートされています。
- IPv6 ユニキャスト ルーティング機能により、スタティック ルーティング、RIP、または OSPF を使用し、設定済みインターフェイスを介して IPv6 トラフィックを転送できます。
- IPv6 Default Router Preference（DRP; デフォルト ルータ プリファレンス）により、ホストが適切なルータを選択するための機能が向上しています。
- IPv6 トランスポートを利用する EIGRP IPv6 のサポートにより、IPv6 ピアとの通信および IPv6 ルートのアドバタイズが可能です。

レイヤ 3 VPN サービス

ここで説明する機能は、スイッチでメトロ IP アクセス イメージが稼動している場合にだけ使用できます。

- マルチ VRF CE により、サービス プロバイダーは、複数の VPN をサポートし、VPN 間で 重複した IP アドレスを使用できます。
- マルチ VRF Lite により、ネットワーク バーチャライゼーション用のプライベート ルーティング ドメインや、バーチャル プライベート マルチキャスト ネットワークを構成できます。
- VRF と EIGRP には互換性があります。

モニタリング機能

- スイッチ LED により、ポート レベルおよびスイッチ レベルのステータスを確認できます。
- 設定可能外部アラーム入力により、アラームの場合と同様、取り外された電源や故障した電源、入力のない電源を特定できます。
- MAC アドレス通知トラップおよび RADIUS アカウンティングにより、スイッチが学習または削除した MAC アドレスを保存して、ネットワークのユーザを追跡できます。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN; リモート SPAN）により、任意のポートまたは VLAN のトラフィックをモニタリングできます。
- Intrusion Detection System（IDS; 侵入検知システム）における SPAN および RSPAN のサポートにより、ネットワーク セキュリティ違反のモニタリング、対処、および報告を行えます。
- 組み込み RMON エージェントの 4 つのグループ（履歴、統計、アラーム、イベント）により、ネットワークのモニタリングとトラフィックの分析が可能です。
- Syslog 機能により、認証エラーまたは許可エラー、リソースの問題、およびタイムアウト イベントに関してシステム メッセージをロギングできます。
- レイヤ 2 traceroute により、パケットが送信元デバイスから宛先デバイスへ送られる物理パスを特定できます。
- Time Domain Reflector（TDR; タイム ドメイン反射率計）により、銅線イーサネット 10/100 ポートにおけるケーブル配線の問題の診断と解決を行います。
- SFP モジュール診断管理インターフェイスにより、SFP モジュールの物理ステータスおよび動作ステータスをモニタリングできます。
- オンライン診断により、稼動中のネットワークにスイッチを接続したまま、そのスイッチのハードウェア機能をテストできます。
- On-Board Failure Logging（OBFL; オンボード障害ロギング）により、スイッチおよびそれに接続されている電源についての情報を収集できます。
- HSRP クライアントの拡張オブジェクト トラッキング（メトロ IP アクセス イメージが必要）。
- IP Service Level Agreement（IP SLA; IP サービス レベル契約）のサポート：アクティブなトラフィック モニタリングによりネットワーク パフォーマンスを測定できます。
- IP SLA EOT により、遅延、ジッタ、パケット損失などのアクションによってトリガされる IP SLA トラッキング動作からの出力に基づいて、フェールオーバーによるスタンバイ ルータへの引き継ぎが行われます。
- EOT および IP SLA EOT スタティック ルートのサポートにより、事前設定されたスタティック ルートまたは DHCP ルートがダウンした場合に、それを検出できます。

- メトロ イーサネット対応の IP SLA により、IEEE 802.1ag イーサネット OAM 機能を使用して、メトロ イーサネット ネットワークにおける接続性、ジッタ、および遅延の検証を行えます。
- Embedded Event Manager（EEM）により、主要なシステム イベントのモニタリングとポリシーに基づいたイベント処理を行うことで、デバイスおよびシステムを管理できます。
- EEM 3.2 のサポートにより、近隣探索、ID、および MAC アドレス テーブルに関するイベントの検出が可能です。
- TWAMP 基準のサポートにより、このプロトコルをサポートする 2 つのデバイス間でラウンドトリップ ネットワーク パフォーマンスを測定できます。

スイッチ初期設定後のデフォルト設定値

スイッチはプラグアンドプレイ対応として設計されているため、基本的な IP 情報をスイッチに割り当て、そのスイッチをネットワーク内の他のデバイスに接続する以外、ユーザが行うべき作業はありません。ただし、ネットワークに対するさまざまな必要性に応じて、インターフェイス固有の設定値やシステム全体の設定値を変更できます。

（注）　CLI ベースのセットアップ プログラムを使用して IP アドレスを割り当てる方法については、ハードウェア インストール ガイドを参照してください。

スイッチの設定をまったく行わない場合、Cisco ME 3400E スイッチはデフォルト設定（表 1-1 を参照）で動作します。

表 1-1　スイッチ初期設定後のデフォルト設定値

機能	デフォルト設定	詳細
スイッチの IP アドレス、サブネット マスク、およびデフォルト ゲートウェイ	0.0.0.0	第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」
ドメイン名	なし	
パスワード	定義なし	第 5 章「スイッチの管理」
TACACS+	ディセーブル	
RADIUS	ディセーブル	
システム名およびプロンプト	*スイッチ*	
NTP	イネーブル	
DNS	イネーブル	
IEEE 802.1x	ディセーブル	第 9 章「IEEE 802.1x ポートベースの認証の設定」
DHCP		
• DHCP クライアント	イネーブル	第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」 第 20 章「DHCP 機能および IP ソースガードの設定」
• DHCP サーバ	イネーブル（DHCP サーバとして動作するデバイスが設定されており、かつイネーブルである場合）	
• DHCP リレー エージェント	イネーブル（DHCP リレー エージェントとして動作するデバイスが設定されており、かつイネーブルである場合）	

表 1-1　スイッチ初期設定後のデフォルト設定値 （続き）

機能	デフォルト設定	詳細
ポート パラメータ		
• ポート タイプ	ギガビット イーサネット：NNI、ファスト イーサネット ポート：UNI	第 10 章「インターフェイスの設定」
• 動作モード	レイヤ 2（スイッチ ポート）	
• ポート イネーブル ステート	NNI：イネーブル、UNI および ENI：ディセーブル	
• インターフェイス速度およびデュプレックス モード	自動ネゴシエーション	
• 自動 MDIX	イネーブル	
• フロー制御	消灯	
コマンド マクロ	設定なし	第 11 章「コマンド マクロの設定」
VLAN		
• デフォルト VLAN	VLAN 1	第 12 章「VLAN の設定」
• VLAN インターフェイス モード	アクセス	
• VLAN タイプ	UNI 独立	
• プライベート VLAN	設定なし	第 13 章「プライベート VLAN の設定」
ダイナミック ARP インスペクション	すべての VLAN でディセーブル	第 21 章「ダイナミック ARP 検査の設定」
トンネリング		
• 802.1Q トンネリング	ディセーブル	第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」
• レイヤ 2 プロトコル トンネリング	ディセーブル	
スパニング ツリー プロトコル		
• STP	Rapid PVST+（VLAN 1 の NNI でイネーブル）	第 15 章「STP の設定」
• MSTP	ディセーブル（UNI ではサポートなし、ENI では設定可能）	第 16 章「MSTP の設定」
• オプションのスパニング ツリー機能	ディセーブル（UNI ではサポートなし、ENI では設定可能）	第 17 章「オプションのスパニング ツリー機能の設定方法」
レジリエント イーサネット プロトコル	設定なし	第 18 章「レジリエント イーサネット プロトコルの設定」
Flex Link	設定なし	第 19 章「Flex Link および MAC アドレス テーブル移行更新機能の設定」
DHCP スヌーピング	ディセーブル	第 20 章「DHCP 機能および IP ソース ガードの設定」
IP ソース ガード	ディセーブル	第 20 章「DHCP 機能および IP ソース ガードの設定」
IGMP スヌーピング		
• IGMP スヌーピング	イネーブル	第 22 章「IGMP スヌーピングおよび MVR の設定」
• IGMP フィルタリング	適用なし	
• IGMP クエリア	ディセーブル	
• MVR	ディセーブル	

表 1-1　スイッチ初期設定後のデフォルト設定値 （続き）

機能	デフォルト設定	詳細
IGMP スロットリング	拒否	第 22 章「IGMP スヌーピングおよび MVR の設定」
ポートベースのトラフィック制御		
• ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームの制御	ディセーブル	第 23 章「ポートベースのトラフィック制御の設定」
• 保護ポート	定義なし	
• ユニキャスト トラフィック フラッディングおよびマルチキャスト トラフィック フラッディング	ブロックなし	
• セキュア ポート	設定なし	
CDP	NNI ではイネーブル、ENI ではディセーブル、UNI ではサポートなし	第 24 章「CDP の設定」
LLDP	ディセーブル（UNI ではサポートなし）	第 25 章「LLDP および LLDP-MED の設定」
UDLD	ディセーブル	第 26 章「UDLD の設定」
SPAN および RSPAN	ディセーブル	第 27 章「SPAN および RSPAN の設定」
RMON	ディセーブル	第 28 章「RMON の設定」
syslog メッセージ	イネーブル（コンソールでのみ表示）	第 29 章「システム メッセージ ロギングの設定」
SNMP	イネーブル（バージョン 1）	第 30 章「SNMP の設定」
ACL	設定なし	第 32 章「ACL によるネットワーク セキュリティの設定」
QoS	設定なし	第 34 章「QoS の設定」
EtherChannel	設定なし	第 35 章「EtherChannel およびリンク ステート トラッキングの設定」
IP ユニキャスト ルーティング		
• IP ルーティングおよび IP ルーティング プロトコル	ディセーブル	第 36 章「IP ユニキャスト ルーティングの設定」
• マルチ VRF CE	ディセーブル	
HSRP グループ（メトロ IP アクセス イメージが必要）	設定なし	第 40 章「HSRP の設定」
Cisco IOS IP SLA	設定なし	第 41 章「Cisco IOS IP SLA 動作の設定」
拡張オブジェクト トラッキング	追跡対象のオブジェクトおよびリストは未設定	第 42 章「拡張オブジェクト トラッキングの設定」
IP マルチキャスト ルーティング（メトロ IP アクセス イメージが必要）	全インターフェイスでディセーブル	第 44 章「IP マルチキャスト ルーティングの設定」
MSDP（メトロ IP アクセス イメージが必要）	ディセーブル	第 45 章「MSDP の設定」

表 1-1　スイッチ初期設定後のデフォルト設定値 （続き）

機能	デフォルト設定	詳細
イーサネット OAM		
• CFM	グローバルでディセーブル、インターフェイス単位でイネーブル	第 43 章「イーサネット OAM、CFM、および E-LMI の設定」
• E-LMI	グローバルでディセーブル	
• イーサネット OAM プロトコル（IEEE 802.3ah）	全インターフェイスでディセーブル	

ネットワークの構成例

ここでは、ネットワーク構成の概要について説明します。また、スイッチを使用して専用ネットワークセグメントを作成し、ファスト イーサネット接続およびギガビット イーサネット接続を介してそれらのセグメントを相互接続する具体例についても説明します。

- 「集合住宅のネットワークまたはイーサネット / 加入者ネットワーク」（P.1-16）
- 「レイヤ 2 VPN アプリケーション」（P.1-17）
- 「マルチ VRF CE アプリケーション」（P.1-18）

集合住宅のネットワークまたはイーサネット / 加入者ネットワーク

メトロ イーサネットは、都市圏で音声サービス、ビデオ サービス、およびインターネット アクセス サービスを提供するサービス プロバイダー向けのアクセス テクノロジーです。メトロ イーサネット User-facing Provider Edge（UPE; ユーザ側プロバイダー エッジ）スイッチを使用すると、帯域幅を効率的に利用できるほか、これらのサービスに必要となるセキュリティや QoS が確保されます。

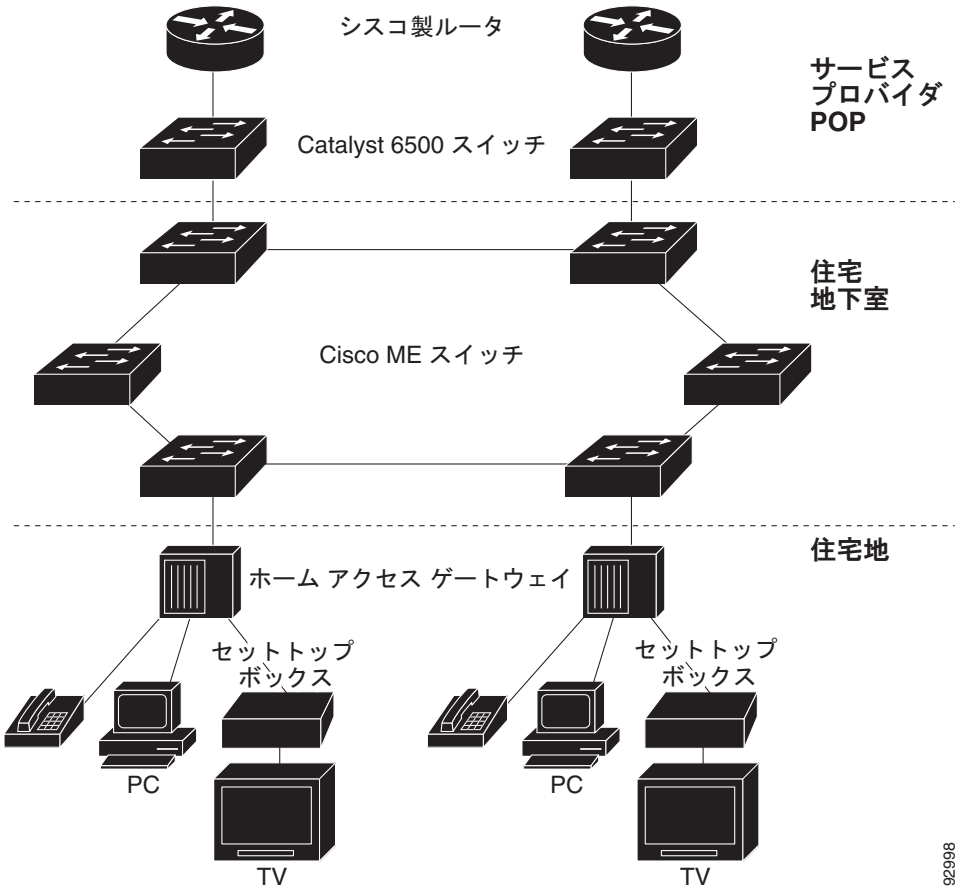
図 1-1 は、1000BASE-X SFP モジュール ポートを介して接続された Cisco ME 3400E イーサネット アクセス スイッチを使用してマルチテナント ユニットを処理する、住宅地でのギガビット イーサネット リングを示したものです。住宅側のスイッチとして Cisco ME スイッチを使用することで、カスタマーとサービス プロバイダーの Point-of Presence（POP; アクセス ポイント）との間で高速接続が実現されます。

ホーム アクセス ゲートウェイは、802.1Q トランクとして設定された UNI または ENI を介して ME スイッチに接続されます。これらのポートのデフォルト動作では、ポート間のローカル スイッチングは行えないため、加入者は相互に保護されます。また、UNI ではカスタマーからの制御プロトコルが処理されないため、DoS 攻撃を回避できます。Cisco ME スイッチは、MAC スプーフィングや IP スプーフィングを防ぐために、ポート セキュリティや IP ソース ガードなどのメカニズムも備えています。サービス プロバイダーは、高度な ACL を使用することにより、ネットワークに着信するトラフィックのタイプを細かく制御できます。

トラフィック タイプごとに異なる QoS を実現するため、Cisco ME スイッチでは、レイヤ 2 ～レイヤ 4 の情報に基づいてトラフィック タイプの特定、ポリシング、マーキング、およびスケジューリングを行えます。Cisco ME スイッチの Cisco MQC を使用することで、QoS を効率的に設定できます。入力 UNI 上でポリシング機能を設定すると、カスタマーが送信に使用できる帯域幅量を常に課金対象の範囲内に収めることができます。出力 NNI では、4 種類のキューを使用して、トラフィック タイプごとに異なるプライオリティ レベルを設定できます。1 つのキューを低遅延キューとして割り当てることにより、音声など遅延に影響されやすいトラフィックを迅速に処理できます。また、低遅延キューにレート制限を設定することにより、誤設定のために他のキューの処理が阻害されるのを回避できます。

ある VLAN のエンド ステーションが別の VLAN のエンド ステーションと通信する必要がある場合は、ルータまたはスイッチにより VLAN 内ルーティングが行われ、該当する宛先 VLAN にトラフィックがルーティングされます。VLAN ACL（VLAN マップ）を使用すると、VLAN 内セキュリティが確保され、ネットワークの重要なエリアに対する不正ユーザのアクセスを防止できます。ルータは、ファイアウォール サービス、Network Address Translation（NAT; ネットワーク アドレス変換）サービス、Voice-over-IP（VoIP）ゲートウェイ サービス、WAN アクセス、およびインターネット アクセスも提供します。

図 1-1　集合住宅構成での Cisco ME スイッチ



レイヤ 2 VPN アプリケーション

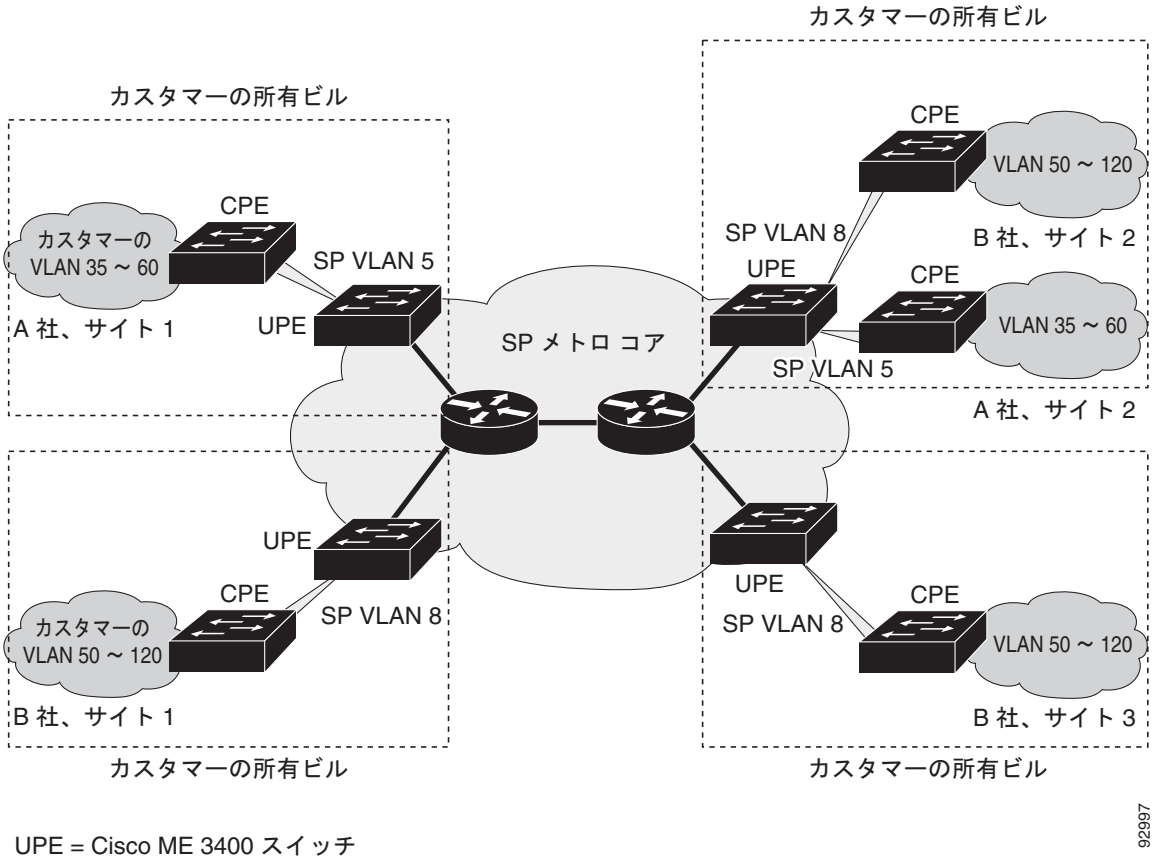
企業カスタマーは、高帯域を利用するだけでなく、プライベート ネットワークをサービス プロバイダーの共有インフラストラクチャ全体にまで拡張する必要があります。サービス プロバイダーは、WAN ネットワーク内でイーサネットを使用することにより、企業カスタマーの帯域幅要件を満たすと同時に、VPN 機能を使用してカスタマー ネットワークを拡張できます。

企業カスタマーは、レイヤ 2 VPN を使用して、サービス プロバイダーのネットワーク上に任意タイプのトラフィック を透過的に移行し、サービス プロバイダーのインフラストラクチャ上で仮想パイプを作成できます。レイヤ 3 VPN サービスとは対照的に、レイヤ 2 VPN では、企業の UPE スイッチの設定および管理を最小化することにより、運用コストが抑えられます。Cisco ME 3400 スイッチを使用してレイヤ 2 VPN を確立すれば、所在地が異なるカスタマーは互いにサービス プロバイダー ネットワークを介して情報を交換できるため、専用回線は必要なくなります。

図 1-2 では、Customer-Premises Equipment（CPE; 顧客宅内機器）スイッチに接続されたカスタマー サイトで、Cisco ME 3400E スイッチが UPE として使用されています。スイッチでは、カスタマーの IEEE 802.1Q タグの先頭にあるサービス プロバイダーの VLAN ID で、カスタマー トラフィックをタグ付けできます。Cisco ME 3400 スイッチは、二重タグをサポートすることで、カスタマーごとの仮想トンネルを実現し、カスタマー間で VLAN ID が重複しないようにします。Cisco ME 3400E スイッチは、データ プレーンを分離できるだけでなく、カスタマーの制御プロトコルをトンネリングすることもできます。スイッチは、レイヤ 2 プロトコル トンネリングを使用して、各カスタマーのコントロール プレーン トラフィックをカプセル化し、サービス プロバイダー ネットワーク上で透過的に送信します。

これらの機能の設定に関する詳細は、第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

図 1-2　　レイヤ 2 VPN の構成



マルチ VRF CE アプリケーション

VPN は、共通ルーティング テーブルを共有するサイトの集合です。カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーでは、VPN Routing/Forwarding（VRF; VPN ルーティングおよび転送）テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスが関連付けられます。サービス プロバイダーは、マルチ VRF CE を使用することで、IP アドレスが重複した複数の VPN をサポートできます。

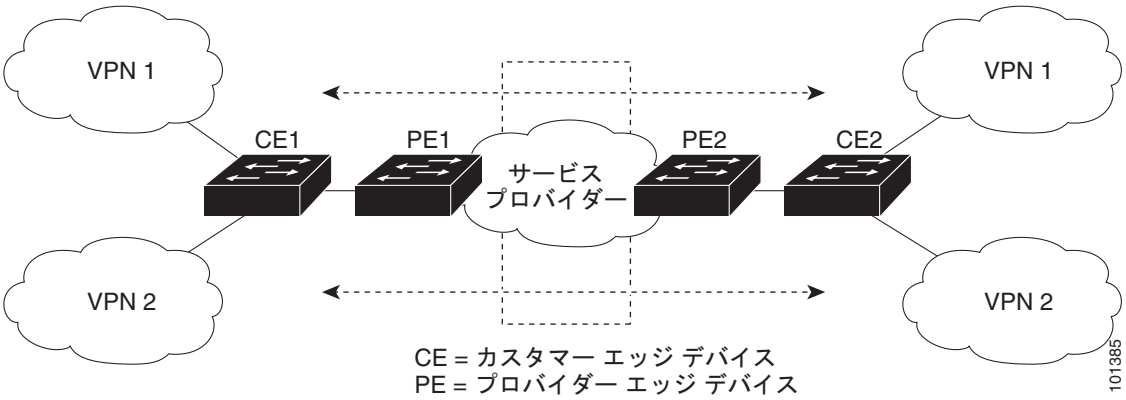
マルチ VRF CE には、次のようなデバイスがあります。

- Customer edge（CE; カスタマー エッジ）: カスタマーは、CE デバイスにより、1 つまたは複数の Provider Edge（PE; プロバイダー エッジ）ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカル ルートをルータにアドバタイズし、そのルータからリモート VPN ルートを学習します。Cisco ME 3400 スイッチは CE デバイスとして使用できます。
- Provider edge（PE; プロバイダー エッジ）: PE ルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE デバイスとルーティング情報を交換します。PE は、直接接続された VPN の VPN ルートを維持するためだけに必要です。サービス プロバイダー VPN ルートのすべてを維持する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。
- CE デバイスに接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

マルチ VRF CE では、複数のカスタマーが 1 つの CE を共有でき、CE と PE の間ではただ 1 つの物理リンクが使用されます。共有 CE は、カスタマーごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、カスタマーごとにパケットをスイッチングまたはルーティングします。マルチ VRF CE は、制限付きの PE 機能を CE デバイスに拡張して、別々の VRF テーブルを維持し、VPN のプライバシおよびセキュリティを支店に拡張します。

図 1-3 は、Cisco ME 3400E スイッチを複数の仮想 CE として使用した構成を示したものです。このシナリオは、中小企業など、VPN サービスの帯域幅要件が低いカスタマーに適しています。このような場合、Cisco ME スイッチではマルチ VRF CE のサポートが必要です。マルチ VRF CE はレイヤ 3 機能であるため、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスであることが必要です。

図 1-3　　複数の仮想 CE



マルチ VRF CE の詳細は、「マルチ VRF CE の設定」（P.36-88）を参照してください。

次の作業

スイッチの設定の前に、スタートアップ情報について次の章を参照してください。

- 第 2 章「CLI の使用方法」
- 第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」
- 第 4 章「Cisco IOS Configuration Engine の設定」

CHAPTER 2

CLI の使用方法

この章では、Cisco ME 3400E イーサネット アクセス スイッチを設定するための Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）とその使用方法について説明します。具体的な内容は次のとおりです。

- 「コマンド モードの概要」（P.2-1）
- 「ヘルプ システムの概要」（P.2-3）
- 「コマンドの省略形」（P.2-3）
- 「コマンドの no および default 形式の概要」（P.2-3）
- 「CLI エラー メッセージについて」（P.2-4）
- 「コマンド履歴の使用方法」（P.2-4）
- 「編集機能の使用方法」（P.2-5）
- 「show および more コマンドの出力の検索とフィルタリング」（P.2-8）
- 「CLI のアクセス」（P.2-8）

コマンド モードの概要

Cisco IOS ユーザ インターフェイスには、さまざまなモードがあります。使用できるコマンドは、コマンド モードによって異なります。システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドのリストが表示されます。

スイッチ上のセッションは、ユーザ モード（ユーザ EXEC モード）で開始します。ユーザ EXEC モードでは、限られたコマンドのサブセットしか使用できません。たとえば、現在のコンフィギュレーション ステータスを表示する **show** コマンド、カウンタまたはインターフェイスをクリアする **clear** コマンドなど、ユーザ EXEC コマンドのほとんどは 1 回限りのコマンドです。ユーザ EXEC コマンドは、スイッチを再起動すると失われます。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードを入力する必要があります。このモードでは、任意の特権 EXEC コマンドを使用できるほか、グローバル コンフィギュレーション モードを開始できます。

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

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

表 2-1　コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとのセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで **enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	入力したコマンドを確認します。このモードへの不正アクセスを防止するには、パスワードを使用します。
グローバル コンフィギュレーション	特権 EXEC モードで **configure** コマンドを入力します。	`Switch(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** を入力するか、**Ctrl+Z** キーを押します。	スイッチ全体に適用されるパラメータを設定します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** を入力します。 特権 EXEC モードに戻るには、**Ctrl+Z** キーを押すか、**end** を入力します。	VLAN（仮想 LAN）パラメータを設定します。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで（インターフェイスを指定して）**interface** コマンドを入力します。	`Switch(config-if)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、**Ctrl+Z** キーを押すか、**end** を入力します。	イーサネット ポートのパラメータを設定します。 インターフェイスの定義方法の詳細については、「インターフェイス コンフィギュレーション モードの使用方法」（P.10-8）を参照してください。 同じパラメータで複数のインターフェイスを設定する場合は、「インターフェイスの範囲設定」（P.10-10）を参照してください。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**linevty** コマンドまたは **line console** コマンドを使用して、回線を指定します。	`Switch(config-line)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、**Ctrl+Z** キーを押すか、**end** を入力します。	端末回線のパラメータを設定します。

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

ヘルプ システムの概要

システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドのリストが表示されます。コマンドに関連するキーワードおよび引数のリストも表示されます（表 2-2 を参照）。

表 2-2　ヘルプの概要

コマンド	目的
help	各コマンド モードのヘルプ システムの簡単な説明が表示されます。

コマンドの省略形 **?**	特定の文字列で始まるコマンドのリストが表示されます。
	次に例を示します。
	`Switch# di?`
	`dir disable disconnect`

コマンドの省略形 **<Tab>**	不完全なコマンド名を完全にします。
	次に例を示します。
	`Switch# sh conf<tab>`
	`Switch# show configuration`

?	特定のコマンド モードで利用できるコマンドをすべて表示します。 次に例を示します。 `Switch> ?`
コマンド **?**	あるコマンドに関連するキーワードを表示します。 次に例を示します。 `Switch> show ?`

コマンド キーワード **?**	あるキーワードに関連する引数を表示します。
	次に例を示します。
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`

コマンドの省略形

スイッチがコマンドを一意のものとして認識できるだけの文字を入力する必要があります。

showconfiguration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
Switch# show conf
```

コマンドの no および default 形式の概要

ほとんどすべてのコンフィギュレーション コマンドに、**no** 形式があります。通常、機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に、**no** 形式を使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイ

スのシャットダウンが取り消されます。キーワード **no** なしでコマンドを使用すると、ディセーブルにされていた機能が再度イネーブルになるか、デフォルトでディセーブルに設定されている機能がイネーブルになります。

コンフィギュレーション コマンドも **default** 形式を使用できます。コマンドの **default** 形式を使用すると、コマンド設定がデフォルト値に戻ります。ほとんどのコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じです。ただし、一部のコマンドはデフォルトでイネーブルに設定されており、変数を特定のデフォルト値に設定しています。このような場合、**default** コマンドはそのコマンドをイネーブルにし、変数をそのデフォルト値に設定します。

CLI エラー メッセージについて

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

表 2-3　CLI の主なエラー メッセージ

エラー メッセージ	意味	ヘルプの利用方法
`% Ambiguous command: "show con"`	スイッチがコマンドとして認識できるだけの文字が入力されていません。	コマンドを再入力し、そのあとに疑問符（?）を入力します。コマンドと疑問符の間にはスペースを入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必要なキーワードまたは値が十分ではありません。	コマンドを再入力し、そのあとに疑問符（?）を入力します。コマンドと疑問符の間にはスペースを入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。キャレット（^）記号は間違っている箇所を示しています。	疑問符（?）を入力すると、そのコマンド モードで利用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コマンド履歴の使用方法

ソフトウェアは、入力されたコマンドの履歴（記録）を備えています。コマンド履歴機能は、アクセス リストなど長いか複雑なコマンドや入力を呼び出す場合に特に便利です。次に説明するように、この機能を必要に応じてカスタマイズできます。

- 「コマンド履歴バッファ サイズの変更」（P.2-4）（任意）
- 「コマンドの呼び出し方法」（P.2-5）（任意）
- 「コマンド履歴機能のディセーブル化」（P.2-5）（任意）

コマンド履歴バッファ サイズの変更

デフォルト設定では、スイッチは履歴バッファに 10 のコマンドラインを記録します。現在の端末セッションまたは特定回線のすべてのセッションに対してこの数値を変更できます。この手順は任意です。

特権 EXEC モードで次のコマンドを入力して、現在の端末セッションでスイッチが記録するコマンドライン数を変更します。

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

指定できる範囲は 0 ～ 256 です。

ライン コンフィギュレーション モードで次のコマンドを入力して、特定の回線上のすべてのセッションでスイッチが記録するコマンドライン数を設定します。

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

指定できる範囲は 0 ～ 256 です。

コマンドの呼び出し方法

履歴バッファからコマンドを呼び出すには、表 2-4 に記載されている動作のいずれかを実行します。これらのアクションは任意です。

表 2-4　コマンドの呼び出し方法

動作[1]	結果
Ctrl+P キーまたは↑キーを押す	最も新しいコマンドから履歴バッファのコマンドを呼び出します。このキー操作を繰り返すと、続けて古いコマンドが呼び出されます。
Ctrl+N キーまたは↓キーを押す	**Ctrl+P** キーまたは↑キーでコマンドが呼び出されてから、履歴バッファの新しいコマンドに戻ります。このキー操作を繰り返すと、続けて新しいコマンドが呼び出されます。
show history	特権 EXEC モードで直前に入力されたコマンドをいくつか表示します。表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定によって制御されます。

1. 矢印キーは、VT100 などの ANSI 準拠端末だけで動作します。

コマンド履歴機能のディセーブル化

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

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

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

編集機能の使用方法

ここでは、コマンド ラインの操作に役立つ編集機能について説明します。

- 「編集機能のイネーブル化およびディセーブル化」（P.2-6）（任意）
- 「キーストロークによるコマンドの編集」（P.2-6）（任意）
- 「折り返すコマンドラインの編集」（P.2-7）（任意）

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的にイネーブルになりますが、ディセーブルまたはイネーブルを切り替えたり、特定の回線に対してだけ拡張編集機能を使用するように設定したりできます。この手順は任意です。

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

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

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

```
Switch# terminal editing
```

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

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

キーストロークによるコマンドの編集

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

表 2-5　キーストロークによるコマンドの編集

機能	キーストローク[1]	目的
コマンド回線上を移動して変更または修正を行います。	**Ctrl+B** キー、または← キーを押す。	カーソルを 1 文字分後退させます。
	Ctrl+F キー、または→ キーを押す。	カーソルを 1 文字分前に進めます。
	Ctrl+A キーを押す。	カーソルをコマンドラインの先頭に移動します。
	Ctrl+E キーを押す。	カーソルをコマンドラインの終わりに移動します。
	Esc+B キーを押す。	カーソルを 1 ワード分後退させます。
	Esc+F キーを押す。	カーソルを 1 ワード分前に進めます。
	Ctrl+T キーを押す。	カーソルの左側の文字をカーソルの位置にある文字と置き換えます。
バッファからすべてのコマンドを呼び出し、コマンドラインにペーストします。スイッチは直前に削除された 10 項目をバッファに記録します。	**Ctrl+Y** キーを押す。	バッファ内の最も新しいエントリを呼び出します。
	Esc+Y キーを押す。	バッファの次のエントリを呼び出します。 バッファには直前に削除または切り取りした 10 項しか記録されていません。11 回以上 **Esc+Y** キーを押すと、バッファの最初のエントリに戻ります。
エントリを誤って入力した場合、または取りやめたい場合に削除します。	**Delete** キーまたは **Backspace** キーを押す。	カーソルの左側の文字を消去します。

表 2-5　キーストロークによるコマンドの編集 （続き）

機能	キーストローク[1]	目的
	Ctrl+D キーを押す。	カーソルの位置にある文字を削除します。
	Ctrl+K キーを押す。	カーソルの位置からコマンドラインの終わりまでの文字をすべて削除します。
	Ctrl+U キーまたは **Ctrl+X** キーを押す。	カーソルの位置からコマンドラインの先頭までの文字をすべて削除します。
	Ctrl+W キーを押す。	カーソルの左側のワードを削除します。
	Esc+D キーを押す。	カーソルの位置からワードの終わりまで削除します。
小文字と大文字にする、または一連の文字を大文字にします。	**Esc+C** キーを押す。	カーソルの位置にある文字を大文字にします。
	Esc+L キーを押す。	カーソルの位置にあるワードを小文字にします。
	Esc+U キーを押す。	カーソルの位置からワードの終わりまでを大文字にします。
特定のキーストロークを実行可能コマンドとして指定します（ショートカットとして指定の可能性あり）。	**Ctrl+V** キーまたは **Esc+Q** キーを押す。	
端末の画面が表示できる範囲より長い行または画面を下にスクロールします。 （注）　**show** コマンドの出力など、端末画面で表示しきれない行のある出力には、More プロンプトを使用します。More プロンプトが表示されている場合は、いつでも **Return** キーおよび **Space** バーのキーストロークを使用できます。	**Return** キーを押す。	1 行下にスクロールします。
	Space バーを押す。	1 画面下にスクロールします。
スイッチのメッセージが急に表示された場合に現在のコマンドラインを再表示します。	**Ctrl+L** キーまたは **Ctrl+R** キーを押す。	現在のコマンドラインを再表示します。

1. 矢印キーは、VT100 などの ANSI 準拠端末だけで動作します。

折り返すコマンドラインの編集

画面上で 1 行を超えるコマンドに対して折り返し機能を使用できます。カーソルが右マージンに達すると、コマンドラインは 10 スペース分、左にシフトします。その行の最初の 10 文字は見えませんが、スクロールして戻り、コマンドの先頭で構文を確認できます。キーストローク アクションは任意です。

コマンドの先頭に戻るには、**Ctrl+B** または←キーを繰り返し押します。**Ctrl+A** キーを押して行の先頭にすぐ移動することもできます。

（注）　矢印キーは、VT100 などの ANSI 準拠端末だけで動作します。

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

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

入力の終了後、**Ctrl+A** キーを押して完全な構文を確認してから **Return** キーを押してコマンドを実行してください。行の終わりに表示されるドル記号（$）は行が右にシフトしたことを示します。

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

ソフトウェアでは、端末の画面が 80 カラムであると仮定しています。それ以外の幅の場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。

以前の複雑なコマンド エントリを呼び出して変更するには、コマンド履歴機能で行折り返しを使用します。以前のコマンド エントリの呼び出しについては、「キーストロークによるコマンドの編集」（P.2-6）を参照してください。

show および more コマンドの出力の検索とフィルタリング

show コマンドおよび **more** コマンドの出力は、検索してフィルタリングすることができます。大量の出力をソートしたり、見る必要のない出力を省略したりする場合に便利です。これらのコマンドの使用は任意です。

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

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

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力すると、*output* が含まれている行は表示されませんが、*Output* が含まれている行は表示されます。

出力に *protocol* がある行だけを組み入れる方法を、次に示します。

```
Switch# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

CLI のアクセス

コンソール接続、Telnet、またはブラウザを使用して、CLI にアクセスできます。

コンソール接続または Telnet を使用した CLI へのアクセス

CLI にアクセスするには、スイッチに付属のハードウェア インストレーション ガイドに記載されているように、まずスイッチのコンソール ポートに端末または PC を接続し、スイッチに電源を投入する必要があります。次に、起動プロセスと IP 情報の割り当てに使用できるオプションについて理解するため、第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」を参照してください。

スイッチが設定済みの場合は、ローカル コンソール接続またはリモート Telnet セッションを介して CLI にアクセスできますが、この種のアクセスでは最初にスイッチを設定する必要があります。詳細については、「端末回線に対する Telnet パスワードの設定」（P.8-6）を参照してください。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチのコンソール ポートを管理ステーションまたはダイヤルアップ モデムに接続する。コンソール ポートへの接続の詳細については、スイッチのハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションで、Telnet TCP/IP または暗号化 Secure Shell（SSH; セキュア シェル）パッケージを使用する。スイッチは Telnet または SSH クライアントとネットワーク接続し、イネーブル シークレット パスワードを設定しておく必要があります。

  スイッチに Telnet アクセスを設定する方法については、「端末回線に対する Telnet パスワードの設定」（P.8-6）を参照してください。このスイッチは同時に最大 16 の Telnet セッションをサポートします。ある Telnet ユーザが行った変更は、他のすべての Telnet セッションにも反映されます。

  スイッチに SSH を設定する方法については、「Secure Shell のためのスイッチの設定」（P.8-37）を参照してください。スイッチは最大 5 の安全な SSH セッションを同時にサポートします。

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

CHAPTER 3

スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て

この章では、自動および手動による方法で、Cisco Metro Ethernet（ME）3400E イーサネット アクセス スイッチの初期設定（スイッチの IP アドレスの割り当てやデフォルト ゲートウェイの情報など）を作成する方法について説明します。また、スイッチのスタートアップ コンフィギュレーションの変更方法についても説明します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、および『*Cisco IOS Software Documentation, 12.2 Mainline Release, Command References, Volume 1 of 3: Addressing and Services*』を参照してください。

この章で説明する内容は、次のとおりです。

- 「起動プロセスの概要」（P.3-1）
- 「スイッチ情報の割り当て」（P.3-2）
- 「実行コンフィギュレーションの確認と保存」（P.3-16）
- 「スタートアップ コンフィギュレーションの変更」（P.3-18）
- 「ソフトウェア イメージのリロードのスケジューリング」（P.3-22）

（注） IP アドレスおよび DHCP の設定に関するこの章の情報は、IP バージョン 4（IPv4）に特化したものです。

起動プロセスの概要

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

通常の起動プロセスにはブートローダ ソフトウェアの操作も含まれます。ブートローダは次の機能を実行します。

- 下位レベル CPU の初期化。CPU レジスタを初期化することにより、物理メモリのマッピング領域、容量、速度などを制御します。
- CPU サブシステムの Power-On Self-Test（POST; 電源投入時セルフテスト）。CPU DRAM と、フラッシュ デバイスのうちフラッシュ ファイル システムを構成する部分をテストします。

- システム ボード上のフラッシュ ファイル システムを初期化します。
- デフォルトのオペレーティング システム ソフトウェア イメージをメモリにロードし、スイッチを起動します。

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

オペレーティング システムが重大な障害によって使用不能になった場合は、ブートローダがシステムへのトラップドア アクセスを行います。トラップドア メカニズムによるシステムへのアクセス機能により、必要に応じて、フラッシュ ファイル システムのフォーマット、XMODEM プロトコルによるオペレーティング システム ソフトウェアイメージの再インストール、失ったパスワードの回復を行ってから最終的にオペレーティング システムを再起動できます。詳細については、「ソフトウェアの障害からの回復」（P.46-2）および「パスワードを忘れた場合の回復」（P.46-3）を参照してください。

（注）　パスワード回復はディセーブルにすることができます。詳細については、「パスワード回復のディセーブル化」（P.8-5）を参照してください。

スイッチ情報を割り当てるには、まず PC または端末がコンソール ポートに接続されており、かつ PC または端末エミュレーション ソフトウェアのボー レートおよび文字フォーマットがスイッチのコンソール ポートのものと一致していることを確認します。

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

（注）　データ ビット オプションが 8 に設定されている場合、パリティ オプションは none（なし）に設定します。

- ストップ ビットのデフォルトは 1 です。
- パリティ設定のデフォルトは none（なし）です。

スイッチ情報の割り当て

IP 情報の割り当ては、スイッチのセットアップ プログラムまたは DHCP サーバを使用して行えるほか、手動で行うこともできます。

特定の IP 情報をプロンプトから指定する場合は、スイッチのセットアップ プログラムを使用します。このプログラムを使用すると、ホスト名とイネーブル シークレット パスワードを設定することもできます。任意で、Telnet パスワードを割り当てることもできます（リモート管理時のセキュリティ用）。セットアップ プログラムの詳細については、ハードウェア インストレーション ガイドの付録「Configuring the Switch with the CLI-Based Setup Program」を参照してください。

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

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

スイッチの設定手順について十分な知識がある場合は、手動でスイッチを設定してください。そうでない場合は、前述のセットアップ プログラムを使用します。

ここでは、次の設定情報について説明します。

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

デフォルトのスイッチ情報

表 3-1 に、デフォルトのスイッチ情報を示します。

表 3-1　デフォルトのスイッチ情報

機能	デフォルト設定
IP アドレスおよびサブネット マスク	IP アドレスまたはサブネット マスクは定義されていません。
デフォルト ゲートウェイ	デフォルト ゲートウェイは定義されていません。
イネーブル シークレット パスワード	パスワードは定義されていません。
ホスト名	出荷時に割り当てられているデフォルトのホスト名は *Switch* です。
Telnet パスワード	パスワードは定義されていません。

DHCP ベースの自動設定の概要

DHCP は、インターネット ホストおよびインターネットワーキング デバイスに設定情報を提供します。このプロトコルは、2 つのコンポーネントで構成されています。1 つは DHCP サーバからデバイスにコンフィギュレーション パラメータを提供するコンポーネント、もう 1 つはデバイスにネットワーク アドレスを割り当てるコンポーネントです。DHCP はクライアント サーバ モデルに基づいています。指定された DHCP サーバが、ダイナミックに設定されるデバイスに対して、ネットワーク アドレスを割り当て、コンフィギュレーション パラメータを提供します。スイッチは、DHCP クライアントとしても DHCP サーバとしても機能させることが可能です。

DHCP ベースの自動設定が機能している場合、スイッチ（DHCP クライアント）は起動時に、IP アドレス情報およびコンフィギュレーション ファイルに基づいて自動で設定されます。

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

スイッチの DHCP サーバは、スイッチと同じ LAN 上であっても、異なる LAN 上にあってもかまいません。DHCP サーバが別の LAN 上で実行されている場合は、スイッチと DHCP サーバとの間に DHCP リレー デバイスを設定する必要があります。リレー デバイスは、直接接続されている 2 つの LAN 間でブロードキャスト トラフィックを転送します。ルータでは、受信したパケットの宛先 IP アドレスに基づくパケットの転送は行われますが、ブロードキャスト パケットの転送は行われません。

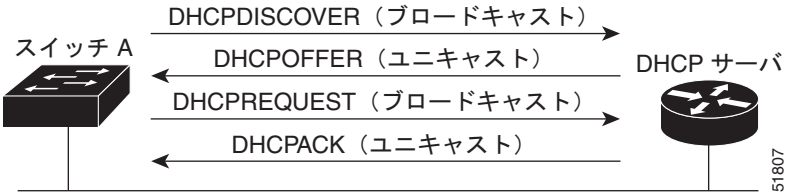
DHCP ベースの自動設定は、スイッチの BOOTP クライアント機能に代わるものです。

DHCP クライアントの要求プロセス

スイッチの起動時、そのスイッチにコンフィギュレーション ファイルがない場合は、DHCP クライアントが起動し、DHCP サーバに対して設定情報を要求します。コンフィギュレーション ファイルが存在し、そのコンフィギュレーションに特定のルーテッド インターフェイス上の **ip address dhcp** インターフェイス コンフィギュレーション コマンドが含まれている場合は、DHCP クライアントが起動し、これらのインターフェイスの IP アドレス情報を要求します。

図 3-1 に、DHCP クライアントと DHCP サーバの間でメッセージが交換される順序を示します。

図 3-1　　DHCP クライアントとサーバのメッセージ交換



クライアントであるスイッチ A は、DHCPDISCOVER メッセージをブロードキャストし、DHCP サーバを検索します。DHCP サーバは、DHCPOFFER ユニキャスト メッセージによって、コンフィギュレーション パラメータ（IP アドレス、サブネット マスク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレスのリースなど）をクライアントに提供します。

クライアントは、DHCPREQUEST ブロードキャスト メッセージにより、DHCP サーバに対して、提供された設定情報の正式な要求を返します。この要求は、クライアントから DHCPDISCOVER ブロードキャスト メッセージを受信した他の DHCP サーバすべてにブロードキャストされます。これは、これらのサーバが、クライアントに提供した IP アドレスを再要求できるようにするためです。

DHCP サーバは、クライアントに DHCPACK ユニキャスト メッセージを返すことによって、クライアントに IP アドレスが割り当てられたことを確認します。このメッセージにより、クライアントとサーバがバインドされ、クライアントは、サーバから受信した設定情報を使用します。スイッチが受信する情報量は、DHCP サーバの設定方法によって異なります。詳細については、「TFTP サーバの設定」（P.3-7）を参照してください。

クライアントに対して送信された DHCPOFFER ユニキャスト メッセージのコンフィギュレーション パラメータが無効の場合（コンフィギュレーション エラーがある場合）、クライアントは DHCP サーバに DHCPDECLINE ブロードキャスト メッセージを返します。

この場合 DHCP サーバは、クライアントに DHCPNAK 拒否ブロードキャスト メッセージを送信します。これは、提供されたコンフィギュレーション パラメータが割り当てられておらず、パラメータのネゴシエーション中にエラーが発生したこと、または DHCPOFFER メッセージに対するクライアントからの応答が遅いこと（DHCP サーバが同じパラメータを他のクライアントに割り当てたこと）を意味します。

DHCP クライアントは、複数の DHCP サーバまたは BOOTP サーバから提供される情報を受信することがあります。いずれの情報も取得できますが、通常は最初に受信した情報が取得されます。DHCP サーバから提供される情報は、クライアントに IP アドレスが割り当てられることを保証するものではありません。ただし、サーバは通常、クライアントがアドレスを正式に要求するまでアドレスを予約しています。スイッチは、BOOTP サーバからの応答を受け入れて設定を行う際、TFTP 要求を（ユニキャストするのではなく）ブロードキャストすることて、スイッチ コンフィギュレーション ファイルを取得します。

DHCP のホスト名オプションを使用すると、1 つのグループを構成する複数のスイッチが一元管理 DHCP サーバからホスト名および標準設定を取得できるよう、設定できます。クライアント（スイッチ）から送信される DHCPDISCOVER メッセージには、オプション 12 フィールドが含まれます。こ

のフィールドは、DHCP サーバにホスト名およびその他のコンフィギュレーション パラメータを要求する際に使用されます。コンフィギュレーション ファイルの内容は、DHCP から取得したホスト名を除けば、すべてのクライアントに対して同一です。

クライアントのホスト名がデフォルトの場合（**hostname** *name* グローバル コンフィギュレーション コマンドが設定されていない場合、または **no hostname** グローバル コンフィギュレーション コマンドが入力されホスト名が削除された場合）、**ip address dhcp** インターフェイス コンフィギュレーション コマンドを実行しても、パケットには DHCP のホスト名オプションは含まれません。この場合、クライアントは、インターフェイスの IP アドレスを取得中に DHCP インタラクションから DCHP のホスト名オプションを受信すると、それを受け入れ、システムにホスト名が設定されていることを示すフラグを設定します。

DHCP ベースの自動設定およびイメージ アップデートの概要

DHCP イメージ アップグレード機能を使用すると、ネットワーク内の 1 つまたは複数のスイッチに新しいイメージおよびコンフィギュレーション ファイルがダウンロードされるよう、DHCP サーバを設定できます。これにより、スイッチを新たにネットワークへ追加した場合、各スイッチが受け取るイメージおよびコンフィギュレーションを統一できます。

DHCP イメージ アップグレードには 2 つの種類があります。1 つは DHCP 自動設定、もう 1 つは DHCP 自動イメージ アップデートです。

DHCP 自動設定

DHCP 自動設定を使用すると、ネットワーク内の 1 つまたは複数のスイッチに対して、DHCP サーバからコンフィギュレーションをダウンロードできます。ダウンロードされたコンフィギュレーション ファイルは、そのスイッチの実行コンフィギュレーションとなります。フラッシュ内に保存されているブートアップ コンフィギュレーションは、スイッチがリロードされるまで上書きされません。

DHCP 自動イメージ アップデート

DHCP 自動設定と DHCP 自動イメージ アップデートを併用すると、ネットワーク内の 1 つまたは複数のスイッチに、コンフィギュレーション*および*新しいイメージの両方をダウンロードできます。新しいコンフィギュレーションおよびイメージをダウンロードするスイッチ（または複数のスイッチ）は、コンフィギュレーションやイメージが未設定の状態（または出荷時のデフォルト設定がロードされただけの状態）でも構いません。

コンフィギュレーションがすでに存在するスイッチに新しいコンフィギュレーションがダウンロードされると、そのコンフィギュレーションは、スイッチに格納されているコンフィギュレーション ファイルに追加されます （ダウンロードされたコンフィギュレーションにより既存のコンフィギュレーションが上書きされることはありません）。

（注） スイッチ上で DHCP 自動イメージ アップデートをイネーブルにするには、イメージ ファイルおよびコンフィギュレーション ファイルがロードされる TFTP サーバに、オプション 67（コンフィギュレーション ファイルの名前）、オプション 66（DHCP サーバのホスト名）、オプション 150（TFTP サーバのアドレス）、およびオプション 125 （ファイルの内容説明）を適切に設定する必要があります。

スイッチを DHCP サーバとして設定するときの手順については、「DHCP ベースの自動設定機能の設定」（P.3-6）および『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP addressing and Services」の章の「Configuring DHCP」を参照してください。

ネットワーク内にスイッチを設置したら、自動イメージ アップデート機能が始動します。ダウンロードされたコンフィギュレーション ファイルは、スイッチの実行コンフィギュレーションに保存されます。また、新しいイメージがスイッチにダウンロードされ、インストールされます。このコンフィギュレーションは、スイッチを再起動した時点で、そのスイッチに保存されているコンフィギュレーションに格納されます。

注意事項および制限事項

注意事項は次のとおりです。

- ネットワーク内でアップ状態にあるレイヤ 3 インターフェイスの中に、割り当てられた IP アドレスを持たないものが 1 つも存在しない場合、保存済みコンフィギュレーションによる DHCP ベースの自動設定プロセスは停止します。
- 保存済みコンフィギュレーションによる DHCP ベースの自動設定機能を使用する場合、タイムアウト時間を設定しないと、IP アドレスのダウンロードの試行が無制限に繰り返されます。
- コンフィギュレーション ファイルがダウンロードできない、または破損した場合、自動インストール プロセスは停止します。

（注）　TFTP からダウンロードされたコンフィギュレーション ファイルは、実行コンフィギュレーション内の既存コンフィギュレーションとマージされますが、**write memory** 特権 EXEC コマンドまたは **copy running-configuration startup-configuration** 特権 EXEC コマンドを実行しない限り、NVRAM には保存されません。ダウンロードされたコンフィギュレーションがスタートアップ コンフィギュレーションに保存された場合、それに続くシステムの再起動時に、この機能はトリガされません。

DHCP ベースの自動設定機能の設定

ここでは、次の設定情報について説明します。

- 「DHCP サーバ設定時の注意事項」（P.3-6）
- 「TFTP サーバの設定」（P.3-7）
- 「DNS の設定」（P.3-8）
- 「リレー デバイスの設定」（P.3-8）
- 「コンフィギュレーション ファイルの取得」（P.3-9）
- 「設定例」（P.3-10）

DHCP サーバとしてシスコ製デバイスを使用している場合の DHCP 設定に関する詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Addressing and Services」にある「Configuring DHCP」を参照してください。

DHCP サーバ設定時の注意事項

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

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

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

- クライアントの IP アドレス（必須）

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

スイッチに TFTP サーバからのコンフィギュレーション ファイルを受信させる場合は、DHCP サーバに次のリース オプションを設定する必要があります。

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

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

DHCP サーバに前述のリース オプションを設定しない場合、サーバはクライアント要求に対して設定済みパラメータだけで応答します。応答に IP アドレスおよびサブネット マスクが含まれていない場合は、スイッチを設定できません。ルータの IP アドレスまたは TFTP サーバ名が見つからない場合、スイッチは TFTP 要求をユニキャストではなく、ブロードキャストで送信することがあります。他のリース オプションについては、使用できない場合でも自動設定に影響はありません。

スイッチは、DHCP サーバとして機能させることもできます。デフォルトでは、Cisco IOS DHCP サーバおよびリレー エージェント機能は、スイッチ上でイネーブルになっていますが、設定が行われていません。このため、これらの機能は動作しません。DHCP サーバとしてシスコ製デバイスを使用している場合の DHCP 設定に関する詳細については、『*Cisco IOS IP Configuration Guide*』（Cisco.com ページから [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] を選択）の「IP Addressing and Services」にある「Configuring DHCP」を参照してください。

TFTP サーバの設定

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

コンフィギュレーション ファイル名および TFTP サーバを指定しなかった場合、またはコンフィギュレーション ファイルをダウンロードできなかった場合、スイッチはさまざまなファイル名と TFTP サーバ アドレスの組み合せによりコンフィギュレーション ファイルをダウンロードしようとします。このようなファイル名としては、指定されたコンフィギュレーション ファイル名（存在する場合）のほか、network-config、cisconet.cfg 、*hostname*.config、*hostname*.cfg などのファイル名が使用されます。ただし、*hostname* はスイッチの現在のホスト名を表わします。また TFTP サーバ アドレスとしては、指定された TFTP サーバのアドレス（存在する場合）およびブロードキャスト アドレス（255.255.255.255）が使用されます。

スイッチがコンフィギュレーション ファイルを正常にダウンロードするには、TFTP サーバのベース ディレクトリに 1 つまたは複数のコンフィギュレーション ファイルが存在する必要があります。該当するファイルは、次のとおりです。

- DHCP 応答に指定されるコンフィギュレーション ファイル（スイッチの実際のコンフィギュレーション ファイル）
- network-confg ファイルまたは cisconet.cfg ファイル（デフォルトのコンフィギュレーション ファイル）

- router-confg ファイルまたは ciscortr.cfg ファイル（これらのファイルには、すべてのスイッチに共通のコマンドが含まれています。通常、DHCP サーバと TFTP サーバが適正に設定されていれば、これらのファイルは使用されません）

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

使用する TFTP サーバがスイッチとは異なる LAN 上にある場合、またはスイッチから TFTP サーバへのアクセスにブロードキャスト アドレスが使用される場合（前述のすべての必須情報が DHCP サーバの応答に含まれていない場合に発生）は、リレーを設定して TFTP サーバに TFTP パケットを転送する必要があります。詳細については、「リレー デバイスの設定」（P.3-8）を参照してください。こうした状況に対する対処方法としては、必要な情報をすべて使用して DHCP サーバを設定することが推奨されます。

DNS の設定

DHCP サーバでは、DNS サーバを使用して、TFTP サーバ名から IP アドレスを取得します。DNS サーバには、TFTP サーバ名から IP アドレスへのマッピングを設定する必要があります。TFTP サーバには、スイッチのコンフィギュレーション ファイルが保持されています。

DHCP サーバのリース データベースには、DNS サーバの IP アドレスを設定できます。DNS サーバからは、DHCP 応答により IP アドレスが取得されます。リース データベースには、DNS サーバの IP アドレスを 2 つまで入力できます。

DNS サーバは、スイッチと同じ LAN 上にあっても、異なる LAN 上にあってもかまいません。異なる LAN 上にある場合、スイッチはルータ経由で DHCP サーバにアクセス可できることが必要です。

リレー デバイスの設定

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

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

たとえば、図 3-2 では、ルータ インターフェイスを次のように設定しています。

インターフェイス 10.0.0.2

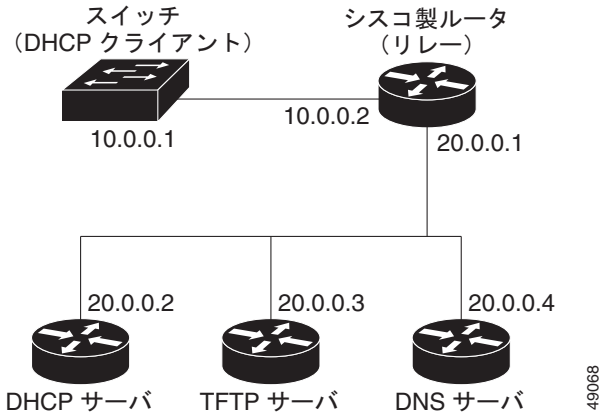
```
router(config-if)# ip helper-address 20.0.0.2
router(config-if)# ip helper-address 20.0.0.3
router(config-if)# ip helper-address 20.0.0.4
```

インターフェイス 20.0.0.1

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

（注）　スイッチをリレー デバイスとして機能させる場合は、インターフェイスをルーテッド ポートとして設定してください。詳細については、「ルーテッド ポート」（P.10-5）および「レイヤ 3 インターフェイスの設定」（P.10-27）を参照してください。

図 3-2　自動設定で使用されるリレー デバイス



コンフィギュレーション ファイルの取得

DHCP の予約済みリースで IP アドレスおよびコンフィギュレーション ファイル名を取得できるかどうかに応じて、スイッチは次の方法で設定情報を取得します。

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

  スイッチは、DHCP サーバから IP アドレス、サブネット マスク、TFTP サーバ アドレス、およびコンフィギュレーション ファイル名を取得します。さらにスイッチは、TFTP サーバのベース ディレクトリから指定のコンフィギュレーション ファイルを取得するために、TFTP サーバへユニキャスト メッセージを送信します。指定のコンフィギュレーション ファイルを受信すると、スイッチの起動プロセスは完了します。

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

  スイッチは、DHCP サーバから IP アドレス、サブネット マスク、およびコンフィギュレーション ファイル名を取得します。さらにスイッチは、TFTP サーバのベース ディレクトリから指定のコンフィギュレーション ファイルを取得するために、TFTP サーバへブロードキャスト メッセージを送信します。指定のコンフィギュレーション ファイルを受信すると、スイッチの起動プロセスは完了します。

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

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

  デフォルトのコンフィギュレーション ファイルには、スイッチのホスト名と IP アドレスのマッピング情報が含まれています。スイッチは、ファイル内の情報を自身のホスト テーブルに読み込み、ホスト名を取得します。ファイルにホスト名が含まれていない場合、スイッチは DHCP 応答に含まれているホスト名を使用します。DHCP 応答にホスト名が指定されていない場合、スイッチはホスト名としてデフォルトの *Switch* を使用します。

デフォルトのコンフィギュレーション ファイルまたは DHCP 応答からホスト名を取得すると、スイッチは TFTP サーバからホスト名と同名のコンフィギュレーション ファイルを読み込みます（network-confg または cisconet.cfg のどちらを先に読み込んだかによって、ファイル名は *hostname*-confg または *hostname*.cfg になります）。cisconet.cfg ファイルを読み込んだ場合、ホストのファイル名は 8 文字に切り詰められます。

network-confg、cisconet.cfg、またはホスト名のファイルを読み込めなかった場合、スイッチは router-confg ファイルを読み込みます。router-confg ファイルが読み込めない場合、スイッチは ciscortr.cfg ファイルを読み込みます。

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

設定例

図 3-3 は、DHCP ベースの自動設定を使用して IP 情報を取得するネットワークの例を示したものです。

図 3-3　DHCP ベースの自動設定ネットワークの例

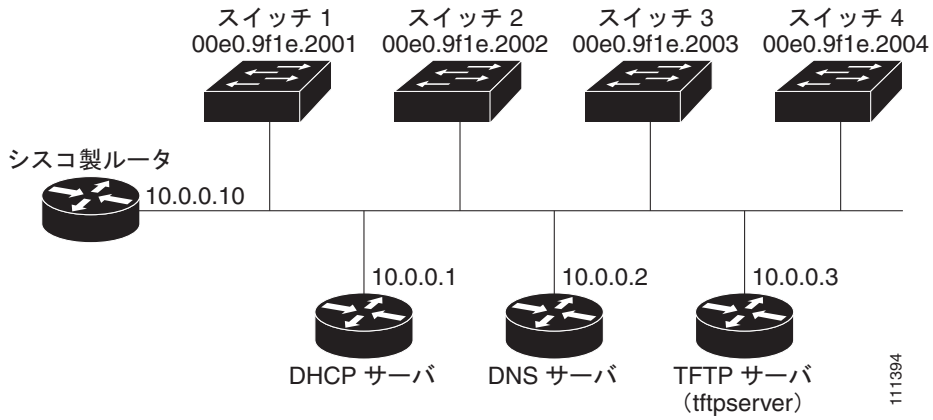


表 3-2 は、DHCP サーバの予約済みリースの設定を示したものです。

表 3-2　DHCP サーバの設定

	スイッチ A	スイッチ B	スイッチ C	スイッチ D
バインド キー（ハードウェア アドレス）	00e0.9f1e.2001	00e0.9f1e.2002	00e0.9f1e.2003	00e0.9f1e.2004
IP アドレス	10.0.0.21	10.0.0.22	10.0.0.23	10.0.0.24
サブネット マスク	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
ルータ アドレス	10.0.0.10	10.0.0.10	10.0.0.10	10.0.0.10
DNS サーバ アドレス	10.0.0.2	10.0.0.2	10.0.0.2	10.0.0.2
TFTP サーバ名	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*

表 3-2　DHCP サーバの設定 （続き）

	スイッチ A	スイッチ B	スイッチ C	スイッチ D
ブート ファイル名（コンフィギュレーション ファイル）（任意）	switcha-confg	switchb-confg	switchc-confg	switchd-confg
ホスト名（任意）	switcha	switchb	switchc	switchd

DNS サーバの設定

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

TFTP サーバの設定（UNIX 上）

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

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

DHCP クライアントの設定

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

設定の説明

図 3-3 では、スイッチ A はコンフィギュレーション ファイルを次のように取得します。

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

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

DHCP の自動設定機能およびイメージ アップデート機能の設定

DHCP を使用してスイッチに新しいイメージおよび新しいコンフィギュレーションをダウンロードする場合は、スイッチを少なくとも 2 つ設定する必要があります。1 つは DHCP サーバ、1 つは TFTP サーバとして機能させます。クライアント スイッチは、新しいコンフィギュレーション ファイルだけをダウンロードするか、新しいコンフィギュレーション ファイルと新しいイメージ ファイルの両方をダウンロードするかのどちらかに設定します。

DHCP 自動設定機能の設定（コンフィギュレーション ファイルだけ）

新しいスイッチ上で新しいコンフィギュレーション ファイルをダウンロードするために TFTP 設定および DHCP 設定に対する DHCP 自動設定機能を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp** *poolname*	DHCP サーバのアドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**bootfile** *filename*	ブート イメージとして使用するコンフィギュレーション ファイルの名前を指定します。
ステップ 4	**network** *network-number mask prefix-length*	DHCP アドレス プールのサブネット ネットワーク番号およびサブネット マスクを指定します。 **（注）** prefix length には、アドレス プレフィクスのビット数（プレフィクス長）を指定します。プレフィクスは、クライアントのネットワーク マスクを指定するための代替手段です。プレフィクス長はスラッシュ（/）に続けて指定します。
ステップ 5	**default-router** *address*	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。
ステップ 6	**option 150** *address*	TFTP サーバの IP アドレスを指定します。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**tftp-server flash**:*filename.text*	TFTP サーバ上にあるコンフィギュレーション ファイルを指定します。
ステップ 9	**interface** ***interface-id***	コンフィギュレーション ファイルを受け取るクライアントのアドレスを指定します。
ステップ 10	**no switchport**	インターフェイスをレイヤ 3 モードにします。
ステップ 11	**ip address** *address mask*	インターフェイスの IP アドレスおよびマスクを指定します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、コンフィギュレーション ファイルをダウンロードするためにスイッチを DHCP サーバとして設定する方法の例を示します。

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# exit
```

```
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

DHCP 自動イメージ アップデート機能の設定（コンフィギュレーション ファイルとイメージ）

新しいスイッチ上で新しいイメージおよび新しいコンフィギュレーション ファイルをダウンロードするために TFTP 設定および DHCP 設定に対する DHCP 自動設定機能を設定するには、特権 EXEC モードで次の手順を実行します。

（注） この表に示した手順を実行する場合は、スイッチにアップロードするテキスト ファイル（autoinstall_dhcp など）を事前に作成しておく必要があります。このテキスト ファイルには、ダウンロードするイメージの名前を記述します。このイメージは、bin ファイルではなく、tar ファイルであることが必要です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *name*	DHCP サーバのアドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**bootfile** *filename*	ブート イメージとして使用するファイルの名前を指定します。
ステップ 4	**network** *network-number mask prefix-length*	DHCP アドレス プールのサブネット ネットワーク番号およびサブネット マスクを指定します。 **（注）** prefix length には、アドレス プレフィクスのビット数（プレフィクス長）を指定します。プレフィクスは、クライアントのネットワーク マスクを指定するための代替手段です。プレフィクス長はスラッシュ（/）に続けて指定します。
ステップ 5	**default-router** *address*	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。
ステップ 6	**option 150** *address*	TFTP サーバの IP アドレスを指定します。
ステップ 7	**option 125** *hex*	イメージ ファイルへのパスを記述したテキスト ファイルへのパスを指定します。
ステップ 8	**copy tftp flash** *filename.txt*	テキスト ファイルをスイッチにアップロードします。
ステップ 9	**copy tftp flash** *imagename.tar*	新しいイメージ用の tar ファイルをスイッチにアップロードします。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**tftp-server flash:*config.text***	TFTP サーバ上にある Cisco IOS コンフィギュレーション ファイルを指定します。
ステップ 12	**tftp-server flash:*imagename.tar***	TFTP サーバ上にあるイメージの名前を指定します。
ステップ 13	**tftp-server flash:*filename.txt***	ダウンロードするイメージ ファイルの名前が記述されたテキスト ファイルを指定します。
ステップ 14	**interface *interface-id***	コンフィギュレーション ファイルを受け取るクライアントのアドレスを指定します。
ステップ 15	**no switchport**	インターフェイスをレイヤ 3 モードにします。
ステップ 16	**ip address** *address mask*	インターフェイスの IP アドレスおよびマスクを指定します。

	コマンド	目的
ステップ 17	**end**	特権 EXEC モードに戻ります。
ステップ 18	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、コンフィギュレーション ファイルをダウンロードするためにスイッチを DHCP サーバとして設定する方法の例を示します。

```
Switch# config terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:-image-name-mz.122-44.3.SE.tar
Switch(config)# tftp-server flash:boot-config.text
Switch(config)# tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitEthernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

クライアントの設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot host dhcp**	保存済み設定による自動設定をイネーブルにします。
ステップ 3	**boot host retry timeout** *timeout-value*	（任意）システムがコンフィギュレーション ファイルのダウンロードを試行する時間を設定します。 **（注）** タイムアウト時間を設定しないと、DHCP サーバからの IP アドレスのダウンロード試行が無制限に繰り返されます。
ステップ 4	**banner config-save ^C** *warning-message* **^C**	（任意）コンフィギュレーション ファイルを NVRAM に保存する際に表示する警告メッセージを作成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show boot**	設定を確認します。

次に、VLAN 99 のレイヤ 3 SVI インターフェイスを使用して、保存済みコンフィギュレーションによる DHCP ベースの自動設定をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(conf)# boot host dhcp
Switch(conf)# boot host retry timeout 300
Switch(conf)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause
You to Nolonger Automatically Download Configuration Files at Reboot^C
Switch(config)# vlan 99
```

```
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:         no
Manual Boot:          no
HELPER path-list:
NVRAM/Config file
      buffer size:    32768
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
Switch#
```

（注） 設定およびイネーブル化の対象となるのは、レイヤ 3 インターフェイスだけです。IP アドレスおよび保存済みコンフィギュレーションによる DHCP ベースの自動設定は割り当てないでください。

手動での IP 情報の割り当て

Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）に手動で IP 情報を割り当てるには、特権 EXEC モードで次の手順を実行します。スイッチでメトロ IP サービス イメージを実行している場合は、**no switchport** コマンドを使用してポートをレイヤ 3 モードにすれば、そのポートに IP 情報を手動で割り当てることもできます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id*	インターフェイス コンフィギュレーション モードを開始し、IP 情報を割り当てる VLAN を入力します。有効な範囲は 1 ～ 4094 です。ただし、先行ゼロは使用しないでください。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスおよびサブネット マスクを入力します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip default-gateway** *ip-address*	デフォルト ゲートウェイが設定されたスイッチに直接接続されているネクスト ホップ ルータ インターフェイスの IP アドレスを入力します。デフォルト ゲートウェイは、スイッチから宛先 IP アドレスが解決されていない IP パケットを受信します。 デフォルト ゲートウェイが設定されると、スイッチは、ホストが通信する必要のあるリモート ネットワークに接続できます。 **（注）** IP でルーティングするようにスイッチを設定した場合は、デフォルト ゲートウェイを設定する必要はありません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces vlan** *vlan-id*	設定されている IP アドレスを確認します。
ステップ 8	**show ip redirects**	設定されているデフォルト ゲートウェイを確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチの IP アドレスを削除する場合は、**no ip address** インターフェイス コンフィギュレーション コマンドを使用します。Telnet セッションを介してアドレスを削除すると、スイッチへの接続は切断されます。デフォルト ゲートウェイのアドレスを削除するときは、**no ip default-gateway** グローバル コンフィギュレーション コマンドを使用します。

スイッチのシステム名の設定、特権 EXEC コマンドへのアクセスの保護、時刻およびカレンダーの設定については、第 5 章「スイッチの管理」を参照してください。

実行コンフィギュレーションの確認と保存

次の特権 EXEC コマンドを使用すると、入力した設定内容や変更した内容を確認できます。

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

Current configuration : 2010 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3400-3
!
enable password cisco
!
no aaa new-model
ip subnet-zero
no ip domain-lookup
!
table-map test
 default copy
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2,10
!
class-map match-all test1
class-map match-all class2
class-map match-all class1
!
!
policy-map test
  class class1
   police cir percent 30
policy-map test2
  class class2
   police cir 8500 bc 1500
policy-map test3
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 shutdown
```

```
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown

<output truncated>

interface GigabitEthernet0/1
 port-type nni
!
interface GigabitEthernet0/2
 port-type nni
!
interface Vlan1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Vlan10
 ip address 192.168.1.76 255.255.255.0
!
ip default-gateway 192.168.1.3
no ip http server
ip classless
!
!
!
control-plane
!
!
line con 0
 session-timeout 120
 exec-timeout 120 0
 speed 115200
line vty 0 4
 password cisco
 no login
line vty 5 15
 no login
!
!
end
```

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

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

このコマンドを実行すると、設定の内容が保存されます。保存できなかった設定は、次回システム リロード時に失われます。フラッシュ メモリの NVRAM セクションに保存されている情報を表示するには、**show startup-config** 権 EXEC コマンドまたは **more startup-config** 特権 EXEC コマンドを使用します。

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

スタートアップ コンフィギュレーションの変更

- 「デフォルトのブート コンフィギュレーション」（P.3-18）
- 「コンフィギュレーション ファイルの自動ダウンロード」（P.3-18）
- 「手動による起動」（P.3-19）
- 「特定のソフトウェア イメージの起動」（P.3-20）
- 「環境変数の管理」（P.3-21）

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

デフォルトのブート コンフィギュレーション

表 3-3 は、デフォルトのブート コンフィギュレーションについての説明をまとめたものです。

表 3-3　デフォルトのブート コンフィギュレーション

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

コンフィギュレーション ファイルの自動ダウンロード

DHCP ベースの自動設定機能を使用すれば、スイッチにコンフィギュレーション ファイルを自動的にダウンロードできます。詳細については、「DHCP ベースの自動設定の概要」（P.3-3）を参照してください。

ファイル名の指定によるシステム コンフィギュレーションの読み取りと書き込み

デフォルトでは、Cisco IOS ソフトウェアは、*config.text* ファイルを使用して、システム コンフィギュレーションの不揮発性コピーを読み書きします。ただし、別のファイル名を指定することもでき、これは次回起動時にロードされます。

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

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

設定をデフォルトに戻すときは、**no boot config-file** グローバル コンフィギュレーション コマンドを使用します。

手動による起動

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot manual**	次回の起動時にスイッチを手動で起動できるようにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

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

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

特定のソフトウェア イメージの起動

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

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

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

	コマンド	目的
ステップ 4	**show boot**	設定を確認します。 **boot system** グローバル コマンドを使用すると、環境変数 BOOT の設定を変更できます。 次回の起動時にスイッチは、BOOT 環境変数内の情報を使用して自動的にシステムを起動しようとします。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトに戻す場合は、**no boot system** グローバル コンフィギュレーション コマンドを使用します。

環境変数の管理

通常の操作スイッチを使用してブート ローダ モードを開始するには、スイッチのコンソール接続を 9600 bps に設定します。スイッチの電源コードを取り外して、接続し直します。スイッチは、POST を実行してから、自動ブート プロセスを開始します。ブート ローダは、ブートアップ シーケンス中にユーザにブレーク キーの文字を求めるプロンプトを表示します（次の例を参照）。

```
***** The system will autoboot in 5 seconds *****

Send a break key to prevent autobooting.
```

ブレーク キーの文字は、オペレーティング システムごとに異なります。

- UNIX を実行する SUN ワークステーションでは、Ctrl-C がブレーク キーとなります。
- Windows 2000 を実行する PC では、Ctrl-Break がブレーク キーとなります。

Cisco TAC では、一般的なオペレーティング システムのブレーク キー、およびブレーク キーをサポートしていない端末エミュレータで使用できる代替ブレーク キー シーケンスに関するリストが用意されています。このリストを参照する場合は、次の URL にアクセスしてください。

http://www.cisco.com/warp/public/701/61.html#how-to

ブレーク キーを入力すると、ブート ローダの *switch:* プロンプトが表示されます。

スイッチのブートローダ ソフトウェアは、不揮発性環境変数をサポートしています。これらの環境変数を使用することで、ブートローダをはじめ、システム上で稼動するソフトウェアの動作を制御できます。ブートローダの環境変数は、UNIX システムや DOS システム上で設定できる環境変数とほぼ同じものです。

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

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

環境変数には、次の 2 種類のデータが保持されます。

- Cisco IOS コンフィギュレーション ファイルの読み取りを行わないコードを制御するためのデータ。環境変数として保存できるブートローダの機能を拡張または補強するブートローダ ヘルパー ファイルの名前などが、こうしたデータに該当します。
- Cisco IOS コンフィギュレーション ファイルの読み取りを行うコードを制御するためのデータ。環境変数として保存できる Cisco IOS コンフィギュレーション ファイルの名前などが、こうしたデータに該当します。

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

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

表 3-4 は、使用頻度の高い環境変数とその機能に関する説明をまとめたものです。

表 3-4　環境変数

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BOOT	**set BOOT** *filesystem***:**/*file-url ...* 自動起動時にロードおよび実行を試みる実行可能ファイルのリストを指定します。区切り文字にはセミコロンを使用します。BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 環境変数が設定されているにもかかわらず指定されたイメージをロードできない場合、システムはフラッシュ ファイル システムで最初に検出されたブートファイルの起動を試みます。	**boot system** f*ilesystem:/file-url ...* 次回の起動時にロードする Cisco IOS イメージを指定します。このコマンドは、BOOT 環境変数の設定を変更します。
MANUAL_BOOT	**set MANUAL_BOOT yes** スイッチを自動で起動するか手動で起動するかを指定します。 有効値は 1、yes、0、および no です。no または 0 に設定した場合、ブートローダはシステムを自動的に起動しようとします。それ以外に設定した場合は、スイッチをブートローダ モードから手動で起動する必要があります。	**boot manual** 次回の起動時に手動でスイッチを起動できるようにし、環境変数 MANUAL_BOOT の設定を変更します。 システムの次回の再起動時には、スイッチはブートローダ モードになります。システムを起動するには、**boot flash:***filesystem***:**/*file-url* ブートローダ コマンドを使用し、コマンドにはブートイメージの名前を指定します。
CONFIG_FILE	**set CONFIG_FILE flash:**/*file-url* Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を変更します。	**boot config-file flash:**/*file-url* Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。このコマンドを使用すると、環境変数 CONFIG_FILE を変更できます。

ソフトウェア イメージのリロードのスケジューリング

スイッチ上へのソフトウェア イメージのリロードを、時間を置いて（たとえば、スイッチの使用が少ない夜間や週末に）実行するようにスケジューリングできます。また、ネットワーク全体でリロードを同期化できます（たとえば、ネットワークのすべてのスイッチ上でソフトウェアのアップグレードを実行）。

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

リロードのスケジューリング設定

ソフトウェア イメージのリロードを、時間を置いて実行するようにスイッチを設定する場合は、特権 EXEC モードで次のいずれかのコマンドを使用します。

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

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

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

  このコマンドを使用すると、ソフトウェアのリロードを、指定した時刻（24 時間制）に実行するようにスケジューリングできます。月日を指定すると、リロードは指定された日時に実行されるようスケジューリングされます。月日を指定しない場合、リロードは当日の指定された時刻（指定された時刻が現在の時刻よりあとの場合）または翌日（指定された時刻が現在の時刻よりも前の場合）に実行されます。00:00 を指定すると、リロードは午前 0 時にスケジューリングされます。

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

reload コマンドを使用すると、システムを一時停止できます。手動で起動するように設定されていない場合、システムは自動的に再起動します。**reload** コマンドを使用する場合は、あらかじめスイッチの設定情報をスタートアップ コンフィギュレーション（**copy running-config startup-config**）に保存してください。

スイッチが手動で起動するように設定されている場合、仮想端末からのリロードは行わないでください。これは、スイッチがブートローダ モードになり、リモート ユーザがスイッチを制御できるようになるのを回避するためです。

コンフィギュレーション ファイルを変更すると、リロードする前に設定を保存するよう求めるプロンプトが表示されます。存在しないスタートアップ コンフィギュレーション ファイルが環境変数 CONFIG_FILE に指定されていると、保存の際に保存を続行するかどうかを尋ねるメッセージが表示されます。続行すると、システムはリロードのセットアップ モードを開始します。

次に、当日の 7:30 PM にソフトウェアをリロードする手順の例を示します。

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

次に、未来の時刻にソフトウェアをリロードする手順の例を示します。

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

リロードのスケジューリングを取り消すときは、**reload cancel** 特権 EXEC コマンドを使用します。

リロードのスケジューリング情報の表示

リロードのスケジューリングに関する情報を表示してスイッチ上でリロードがスケジューリングされているかどうかを調べるときは、**show reload** 特権 EXEC コマンドを使用します。

リロードの予定実行時刻、リロードの理由（指定されている場合）など、リロードに関する情報が表示されます。

CHAPTER 4

Cisco IOS Configuration Engine の設定

この章では、Cisco ME 3400E スイッチにおける機能の設定方法について説明します。

（注） Cisco Configuration Engine の設定情報の詳細については、http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

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

この章で説明する内容は、次のとおりです。

- 「Cisco Configuration Engine ソフトウェアの概要」（P.4-1）
- 「Cisco IOS エージェントの概要」（P.4-5）
- 「Cisco IOS エージェントの設定」（P.4-6）
- 「CNS コンフィギュレーションの表示」（P.4-15）

Cisco Configuration Engine ソフトウェアの概要

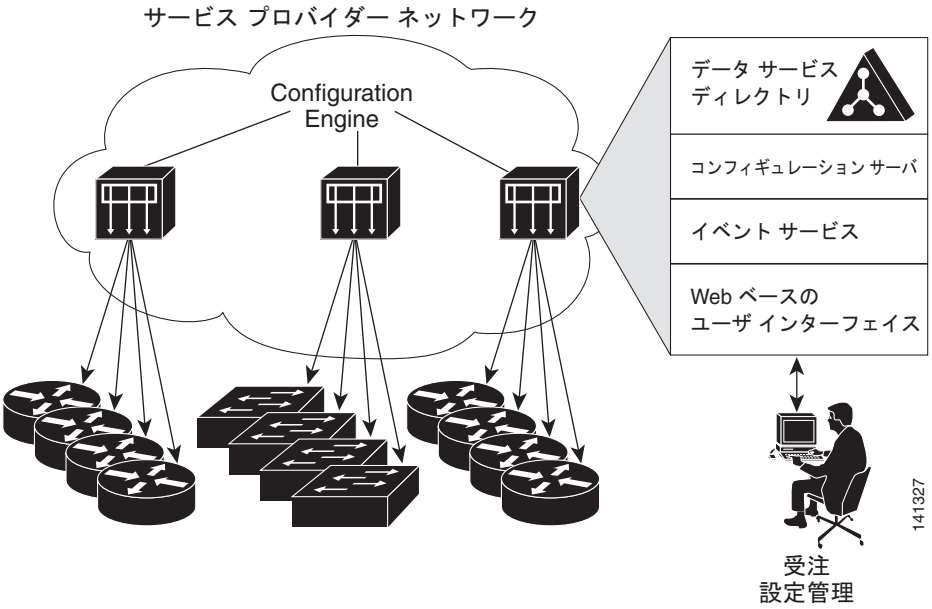
Cisco Configuration Engine はネットワーク管理ソフトウェアで、ネットワーク デバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーション サービスとして機能します（図 4-1 を参照）。各 Configuration Engine は、シスコ製デバイス（スイッチとルータ）およびこれらが提供するサービスのグループを管理し、設定を保存し、必要に応じて配信します。Configuration Engine は、デバイス固有の設定変更を生成してデバイスに送信し、その設定変更を実行して結果をロギングすることで、初期設定および設定更新を自動化します。

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

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

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

図 4-1　Configuration Engine アーキテクチャの概要



ここでは、次の概要について説明します。

- 「Configuration Service」（P.4-2）
- 「Event Service」（P.4-3）
- 「CNS ID およびデバイスのホスト名についての注釈」（P.4-3）

Configuration Service

Configuration Service は、Cisco Configuration Engine のコアとなるコンポーネントです。スイッチ上の Cisco IOS CNS エージェントと連携するコンフィギュレーション サーバで構成されています。Configuration Service は、初期設定および論理グループ別の大量の再設定を行うために、デバイスとサービスの設定をスイッチに配信します。スイッチは、ネットワーク上で初めて起動するときに、Configuration Service から初期設定を受信します。

Configuration Service は、CNS Event Service を使用して設定変更イベントを送受信し、成功および失敗の通知を送信します。

コンフィギュレーション サーバは、コンフィギュレーション テンプレートおよびデバイス固有の設定情報を使用する Web サーバです。この設定情報は、組み込みディレクトリ（スタンドアロン モード）またはリモート ディレクトリ（サーバ モード）に保存されています。

コンフィギュレーション テンプレートは、CLI（コマンドライン インターフェイス）コマンドの形式でスタティックな設定情報を格納するテキスト ファイルです。テンプレート内の変数は、Lightweight Directory Access Protocol（LDAP）URL を使用して指定します。この URL は、ディレクトリに保存されているデバイス固有の設定情報を参照します。

Cisco IOS エージェントは、受信したコンフィギュレーション ファイルの構文を検査して、構文検査の成功または失敗を示すイベントをパブリッシュすることができます。コンフィギュレーション エージェントは、設定を即時適用したり、コンフィギュレーション サーバからの同期化イベントを受信するまで適用を遅らせたりすることが可能です。

Event Service

Configuration Engine は、コンフィギュレーション イベントの受信と生成に Event Service を使用します。イベント エージェントはスイッチ上にあり、Configuration Engine 上のイベント ゲートウェイとスイッチ間の通信を容易にします。

Event Service は、高機能のパブリッシュ / サブスクライブ型の通信方式です。Event Service は、件名ベースのアドレス指定を使用して、宛先にメッセージを送信します。件名ベースのアドレス表記は、メッセージとその宛先に対して単純で均一なネームスペースを定義します。

Name Space Mapper

Configuration Engine には NameSpace Mapper（NSM）が備わっています。NSM は、アプリケーション、デバイス ID またはグループ ID、およびイベントに基づいた、論理的なデバイス グループを管理するための検索サービスを提供します。

Cisco IOS デバイスは、cisco.cns.config.load など、Cisco IOS ソフトウェアで設定されたイベント件名だけを認識します。ネームスペース マッピング サービスを使用すると、希望する命名規則を使用してイベントを指定できます。件名でデータ ストアにデータを入力した場合、NSM はイベント件名文字列を Cisco IOS によって認識されているものに変更します。

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

CNS ID およびデバイスのホスト名についての注釈

Configuration Engine は、設定済みの各スイッチに一意の識別子が関連付けられているものと想定しています。一意の識別子は、それぞれ特定のネームスペース内で一意の複数な同義語を取ることができます。Event Service はネームスペースのコンテンツを使用して、メッセージの件名ベース アドレス指定を行います。

Configuration Engine では、2 つのネームスペースが使用されます。1 つはイベント バス用で、もう 1 つはコンフィギュレーション サーバ用です。コンフィギュレーション サーバのネームスペースの場合、デバイスに対して一意の識別子は *ConfigID* です。イベント バスのネームスペースの場合、デバイスに対して一意の CNS 識別子は *DeviceID* です。

Configuration Engine がデバイスに設定を配信する場合は、イベント バスとコンフィギュレーション サーバの両方が使用されるため、設定されたスイッチごとに ConfigID と DeviceID の両方を定義する必要があります。

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

ConfigID

設定済みの各スイッチには一意の ConfigID が設定されます。この ID は、対応するスイッチ CLI アトリビュート セットに対する Configuration Engine ディレクトリへのキーの役割を果たします。スイッチ上で定義された ConfigID は、Configuration Engine 上の対応するスイッチ定義の ConfigID に一致する必要があります。

ConfigID は起動時に決定されます。スイッチのホスト名を再設定した場合でも、デバイスを再起動するまでは変更できません。

DeviceID

イベント バスに参加している設定済みの各スイッチには一意の DeviceID が設定されます。この ID はスイッチの送信元アドレスに似ているので、スイッチをバス上の特定の宛先として設定することができます。**cns config partial** グローバル コンフィギュレーション コマンドで設定されたすべてのスイッチは、イベント バスにアクセスする必要があります。したがって、スイッチ上で生成された DeviceID は、Configuration Engine 上の対応するスイッチ定義の DeviceID と一致する必要があります。

DeviceID の取得元は、スイッチの Cisco IOS ホスト名によって定義されます。ただし、DeviceID の変数とその使用は、スイッチに隣接するイベント ゲートウェイ内に限定されます。

イベント バス上の論理的な Cisco IOS 終端地点はイベント ゲートウェイに組み込まれ、これがスイッチの代わりにプロキシの役目を果たします。イベント ゲートウェイは、イベント バスにとっては、スイッチおよび対応する DeviceID として機能します。

スイッチは、イベント ゲートウェイとの接続が成功するとすぐに、イベント ゲートウェイに対してそのホスト名を宣言します。イベント ゲートウェイは、この接続が確立されるたびに、DeviceID の値を Cisco IOS ホスト名に結合します。イベント ゲートウェイは、スイッチに接続している間に、この DeviceID 値をキャッシュします。

ホスト名および DeviceID

DeviceID はイベント ゲートウェイとの接続時に決定され、スイッチのホスト名を再設定した場合でも変更されません。

スイッチ上のスイッチ ホスト名を変更した場合、DeviceID を更新するには、スイッチとイベント ゲートウェイ間の接続を切断する必要があります。**no cns event** グローバル コンフィギュレーション コマンドのあとに、**cns event** グローバル コンフィギュレーション コマンドを入力します。

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

注意　Configuration Engine ユーザ インターフェイスを使用する場合は、最初に DeviceID フィールドにホスト名を設定する必要があります。この値は、スイッチで **cns config initial** グローバル コンフィギュレーション コマンドを使用 *したあとに*（*使用する前*ではない）取得されます。この設定を行わないと、後続の **cns config partial** グローバル コンフィギュレーション コマンドの処理が正しく機能しません。

ホスト名、DeviceID、ConfigID の使用方法

スタンドアロン モードでは、スイッチにホスト名の値が設定されている場合に、ホスト名に関するイベントが送信されると、DeviceID としてホスト名が使用されます。ホスト名が設定されていない場合は、デバイスの cn=<*value*> に関するイベントが送信されます。

サーバ モードでは、ホスト名は使用されません。サーバ モードでは、バス上でイベントを送信する場合、常に一意の DeviceID アトリビュートが使用されます。このアトリビュートが設定されていない場合は、スイッチを更新できません。

これらのアトリビュートとその他の関連アトリビュート（タグ値のペア）は、Configuration Engine で **Setup** を実行すると設定されます。

（注）　Configuration Engine 上でのセットアップ プログラムの実行の詳細については、次の URL の『Configuration Engine setup and configuration guide』を参照してください。
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/prod_installation_guides_list.html

Cisco IOS エージェントの概要

CNS イベント エージェント機能により、スイッチはイベント バス上でイベントをパブリッシュおよびサブスクライブし、Cisco IOS エージェントと連携できます。Cisco IOS エージェント機能は、次の機能を提供してスイッチをサポートします。

- 「初期設定」（P.4-5）
- 「差分（部分）設定」（P.4-6）
- 「同期設定」（P.4-6）

初期設定

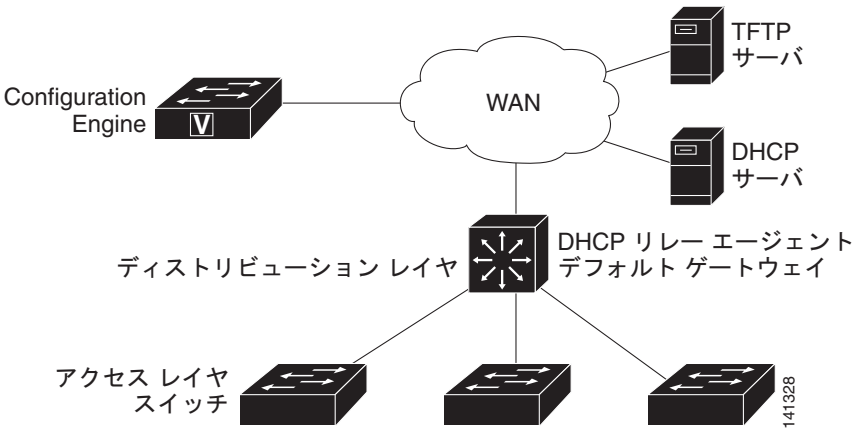
スイッチは初回起動時に、ネットワーク上で Dynamic Host Configuration Protocol（DHCP）要求をブロードキャストして、IP アドレスを取得しようとします。ディストリビューション スイッチはサブネット上に DHCP サーバがないものと見なして、DHCP リレー エージェントとして動作し、要求を DHCP サーバに転送します。要求を受信した DHCP サーバは、新しいスイッチに IP アドレスを割り当てて、DHCP リレー エージェントへのユニキャスト応答に、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバの IP アドレス、ブートストラップ コンフィギュレーション ファイルのパス、およびデフォルト ゲートウェイの IP アドレスを追加します。DHCP リレー エージェントは、この応答をスイッチに転送します。

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

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

図 4-2 に、DHCP ベースの自動設定を使用して初期ブートストラップ コンフィギュレーション ファイルを取得するためのネットワーク構成例を示します。

図 4-2　初期設定の概要



差分（部分）設定

ネットワークが稼動している場合は、Cisco IOS エージェントを使用して新しいサービスを追加できます。スイッチに送信できるのは差分（部分）設定です。実際の設定を送信する方法としては、イベント ゲートウェイを使用してイベント ペイロードとして送信する方法（プッシュ オペレーション）、またはスイッチにプル オペレーションを開始させる信号イベントとして送信する方法があります。

スイッチは設定を適用する前に、構文を検査できます。構文が正しい場合、スイッチは差分設定を適用し、コンフィギュレーション サーバに成功を通知するイベントをパブリッシュします。差分設定が適用されない場合、スイッチはエラー ステータスを示すイベントをパブリッシュします。差分設定が適用された場合、スイッチは差分設定を NVRAM（不揮発性 RAM）に書き込んだり、NVRAM に書き込むように促されるまで待機したりできます。

同期設定

設定を受信したスイッチは、書き込み信号イベントの受信時に、設定の適用を遅らせることが可能です。書き込み信号イベントは、更新された設定を NVRAM に保存しないようにスイッチに指示します。スイッチは更新された設定を実行コンフィギュレーションとして使用します。このようにすると、スイッチの設定が他のネットワーク アクティビティと同期したあとに設定を NVRAM に保存し、次回の再起動時に使用することができます。

Cisco IOS エージェントの設定

スイッチは Cisco IOS ソフトウェアに組み込まれた Cisco IOS エージェントを使用して、接続および自動設定を実行できます（「自動 CNS 設定のイネーブル化」（P.4-7）を参照）。設定を変更するか、またはカスタム設定をインストールする場合は、次に記載された手順を参照してください。

- 「CNS イベント エージェントのイネーブル化」（P.4-7）
- 「Cisco IOS CNS エージェントのイネーブル化」（P.4-9）
- 「Cisco IOS イメージ エージェントによるデバイスのアップグレード」（P.4-14）

自動 CNS 設定のイネーブル化

スイッチの自動 CNS 設定をイネーブルにするには、最初に表 4-1 の条件を満たす必要があります。条件を満たしたら、スイッチに電源を投入します。**setup** プロンプトには何も入力しません。スイッチによって初期設定が開始されます（「初期設定」（P.4-5）を参照）。スイッチにコンフィギュレーション ファイル全体がロードされたら、作業は完了です。

表 4-1　自動設定のイネーブル化の条件

デバイス	必要な設定
アクセス スイッチ	出荷時の設定（コンフィギュレーション ファイルなし）
ディストリビューション スイッチ	• IP ヘルパー アドレス • DHCP リレー エージェントのイネーブル化 • IP ルーティング（デフォルト ゲートウェイとして使用する場合）
DHCP サーバ	• IP アドレスの割り当て • TFTP サーバの IP アドレス • TFTP サーバ上のブートストラップ コンフィギュレーション ファイルへのパス • デフォルト ゲートウェイの IP アドレス
TFTP サーバ	• CNS コンフィギュレーション コマンド（スイッチと Configuration Engine との通信をイネーブルにするコマンド）を格納したブートストラップ コンフィギュレーション ファイル • （デフォルト ホスト名でなく）スイッチの MAC（メディア アクセス制御）アドレスまたはシリアル番号を使用して ConfigID および EventID を生成するようにスイッチを設定します。 • スイッチにコンフィギュレーション ファイルをプッシュするように CNS イベント エージェントを設定します。
CNS Configuration Engine	デバイス タイプごとに 1 つまたは複数のテンプレートで、デバイスの ConfigID をテンプレートにマッピングします。

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

CNS イベント エージェントのイネーブル化

（注）　CNS コンフィギュレーション エージェントをイネーブルにするには、スイッチ上で CNS イベント エージェントをイネーブルにしておく必要があります。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cns event** {*hostname* | *ip-address*} [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**reconnect** *time*] [**source** *ip-address*]	イベント エージェントをイネーブルにして、ゲートウェイ パラメータを入力します。 • {*hostname* | *ip-address*} には、イベント ゲートウェイのホスト名または IP アドレスを入力します。 • （任意）*port number* には、イベント ゲートウェイのポート番号を入力します。デフォルトのポート番号は 11011 です。 • （任意）このゲートウェイがバックアップ ゲートウェイであることを示す場合は、**backup** を入力します（省略するとプライマリ ゲートウェイになります）。 • （任意）**failover-time** *seconds* には、バックアップ ゲートウェイへのルートが確立された後の、スイッチがプライマリ ゲートウェイ ルートを待機する時間を入力します。 • （任意）**keepalive** *seconds* には、スイッチがキープアライブ メッセージを送信する間隔を入力します。*retry-count* には、接続が終了するまでにスイッチから送信される、未応答のキープアライブ メッセージ数を入力します。デフォルトは 0 です。 • （任意）**reconnect** *time* には、イベント ゲートウェイへの再接続が試行される前にスイッチが待機する最大タイム インターバルを入力します。 • （任意）**source** *ip-address* には、このデバイスの送信元 IP アドレスを入力します。 **（注）** **encrypt** および **clock-timeout** *time* の各キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show cns event connections**	イベント エージェントに関する情報を確認します。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

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

Cisco IOS CNS エージェントのイネーブル化

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

- **cns config initial** グローバル コンフィギュレーション コマンド：Cisco IOS エージェントをイネーブルにし、スイッチの初期設定を開始します。
- **cns config partial** グローバル コンフィギュレーション コマンド：Cisco IOS エージェントをイネーブルにし、スイッチの部分設定を開始します。次に、Configuration Engine を使用して、スイッチにリモートから差分設定を送信します。

初期設定のイネーブル化

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cns template connect** *name*	CNS テンプレート接続コンフィギュレーション モードを開始して、CNS 接続テンプレートの名前を指定します。
ステップ 3	**cli** *config-text*	CNS 接続テンプレートのコマンド ラインを入力します。テンプレート内の各コマンド ラインに対してこのステップを繰り返します。
ステップ 4		別の CNS 接続テンプレートを設定するには、ステップ 2 ～ 3 を繰り返します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**cns connect** *name* [**retries** *number*] [**retry-interval** *seconds*] [**sleep** *seconds*] [**timeout** *seconds*]	CNS 接続コンフィギュレーション モードを開始し、CNS 接続プロファイルの名前を指定し、プロファイル パラメータを定義します。本スイッチでは、Configuration Engine への接続に CNS 接続プロファイルが使用されます。 • CNS 接続プロファイルの名前を入力します。 • （任意）**retries** *number* には、接続再試行の回数を入力します。指定できる範囲は 1 ～ 30 です。デフォルト値は 3 です。 • （任意）**retry-interval** *seconds* には、Configuration Engine に対する成功した接続試行間のインターバルを入力します。指定できる範囲は 1 ～ 40 秒です。デフォルト値は 10 秒です。 • （任意）**sleep** *seconds* には、最初の接続試行が発生するまでの制限時間を入力します。指定できる範囲は 0 ～ 250 秒です。デフォルト値は 0 です。 • （任意）**timeout** *seconds* には、接続試行が終了する制限時間を入力します。指定できる範囲は 10 ～ 2000 秒です。デフォルト値は 120 です。

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

	コマンド	目的
ステップ 13	**cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] または **cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**]	（任意）Configuration Engine が使用する一意の EventID または ConfigID を設定します。 • *interface num* には、インターフェイスのタイプ（ethernet、group-async、loopback、virtual-template など）を入力します。この設定は、一意の ID を定義するための IP アドレスまたは MAC アドレスの取得元となるインターフェイスを指定します。 • {**dns-reverse** | **ipaddress** | **mac-address**} には、ホスト名を取得して一意の ID として割り当てる場合は **dns-reverse** を、IP アドレスを使用する場合は **ipaddress** を、一意の ID として MAC アドレスを使用する場合は **mac-address** を入力します。 • （任意）スイッチの識別に使用したイベント ID 値を ID に設定するには、**event** を入力します。 • （任意）スイッチの識別に使用したイメージ ID 値を ID に設定するには、**image** を入力します。 **（注）** **event** キーワードおよび **image** キーワードの両方を省略した場合、イメージ ID 値がスイッチの特定に使用されます。 • {**hardware-serial** | **hostname**| **string** *string* | **udi**} には、一意の ID としてスイッチのシリアル番号を設定する場合は **hardware-serial** を、一意の ID としてスイッチのホスト名を選択する場合は **hostname**（デフォルト）を、一意の ID として **string** *string* に任意のテキスト ストリングを、または、一意の ID として Unique Device Identifier（UDI）を設定する場合は **udi** を入力します。

	コマンド	目的
ステップ 14	**cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**]	Cisco IOS エージェントをイネーブルにし、初期設定を開始します。 • {*hostname* | *ip-address*} には、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port number* には、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • （任意）設定完了時に設定の成功、失敗、または警告のメッセージを表示するには、**event** をイネーブルにします。 • （任意）**cns config initial** グローバル コンフィギュレーション コマンドを入力して得られた設定を NVRAM に自動保存しないように設定するには、**no-persist** を入力します。**no-persist** キーワードを入力しないで **cns config initial** コマンドを使用すると、その結果得られた設定は NVRAM に自動保存されます。 • （任意）**page** *page* には、初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。 • （任意）送信元 IP アドレスに使用する **source** *ip-address* を入力します。 • （任意）このパラメータが入力されたときに構文をチェックするには、**syntax-check** をイネーブルにします。 **（注）** **encrypt**、**status** *url*、および **inventory** の各キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 15	**end**	特権 EXEC モードに戻ります。
ステップ 16	**show cns config connections**	コンフィギュレーション エージェントに関する情報を確認します。
ステップ 17	**show running-config**	設定を確認します。

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

次に、スイッチ設定が不明なときにリモート スイッチ上で初期設定を設定する例を示します（CNS Zero Touch 機能）。

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

次に、スイッチの IP アドレスが不明なときにリモート スイッチ上で初期設定を設定する方法の例を示します。Configuration Engine の IP アドレスは 172.28.129.22 です。

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

部分設定のイネーブル化

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

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

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

Cisco IOS イメージ エージェントによるデバイスのアップグレード

Cisco IOS デバイスの大規模ネットワークを維持する管理者には、イメージ ファイルを多数のリモート デバイスにロードするための自動メカニズムが必要となります。既存のネットワーク管理アプリケーションは、実行するイメージの決定および Cisco オンライン ソフトウェア センターから受信したイメージの管理方法を決定するのに便利です。他のイメージ配信ソリューションでは、数千のデバイスをカバーするようスケールせず、ファイアウォールの向こう側のデバイスにはイメージを配信できません。CNS イメージ エージェントを使用すると、管理されたデバイスはネットワーク接続を開始して、ファイアウォールの向こう側のデバイスにイメージ サーバへのアクセスを許可して、イメージのダウンロードを要求できるようになります。

イメージ エージェントを使用すると、1 つまたは複数のデバイスをダウンロードできます。スイッチには、それらのデバイス上で稼動するイメージ エージェントが必要です。

CNS イメージ エージェントの条件

イメージ エージェントが稼動する 1 つまたは複数のデバイスをアップグレードする前に、次の条件を確認してください。

- ファイル サーバ上の Cisco IOS イメージの格納場所を決定して、他のネットワーキング デバイスがこのイメージを使用できるようにします。イメージの格納および配信に CNS Event Bus を使用する場合、CNS イベント エージェントが設定されている必要があります。
- ファイル サーバをセットアップして、ネットワーキング デバイスが HTTPS プロトコルを使用して新しいイメージをダウンロードできるようにします。
- イメージ エージェント オペレーションにより生成されるエラー メッセージの処理方法を決定します。エラー メッセージは、CNS Event Bus、HTTP、または HTTPS URL に送信できます。

CNS イメージ エージェントの制限事項

自動イメージ ロードの動作中は、Cisco IOS デバイスとイメージを提供するファイル サーバとの接続が切断されないようにする必要があります。イメージのリロードは、メモリ問題および接続問題の対象となります。また、Cisco IOS デバイスが最初のイメージのリロードに失敗した場合、他のイメージをブートできるように、ブート オプションを設定する必要があります。

スイッチで稼動するイメージ エージェントを適用する場合、この他に次の制限事項があります。

- ダウンロードできるのは、tar イメージ ファイルに限られます。bin イメージ ファイルのダウンロードはサポートされません。
- 直接ダウンロード オプションだけがサポートされます。指定の日時にダウンロードをするようにはスケジューリングできません。
- [Associate Image with Device] ウィンドウの [Destination] フィールドは、サポートされません。

詳細については、CNS IE2100 のマニュアルおよび『*Cisco IOS Configuration Fundamentals Configuration Guide*』*Release 12.2* の「File Management」を参照してください。

イメージ エージェントを開始して、新しいイメージの確認およびデバイスのアップグレードを行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip host** {*ip-address*} {*hostname*}	IP アドレスおよびイベント ゲートウェイのホスト名を入力します。
ステップ 3	**cns trusted-server all-agents** {*hostname*}	CNS エージェントの信頼されるサーバを指定します。
ステップ 4	**no cns aaa enable cns event** {*ip-address*} {*port number*}	イベント ゲートウェイ上の Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）認証をディセーブルにします。
ステップ 5	**cns image retry** {*number*}	イメージのリトライ数およびダウンロード数を指定します。
ステップ 6	**cns image server** {*ip-address*} **status** {*ip-address*}	サーバからスイッチにイメージをダウンロードします。
ステップ 7	**end**	特権 EXEC モードに戻ります。

（注）　次に、アドレス **172.20.249.20** のサーバからスイッチをアップグレードする例を示します。

```
Switch(config)> configure terminal
Switch(config)# ip host cns-dsbu.cisco.com 172.20.249.20
Switch(config)# cns trusted-server all-agents cns-dsbu.cisco.com
Switch(config)# no cns aaa enable cns event 172.20.249.20 22022
Switch(config)# cns image retry 1
Switch(config)# cns image server http://172.20.249.20:80/cns/HttpMsgDispatcher status
http://172.20.249.20:80/cns/HttpMsgDispatcher
Switch(config)# end
```

show cns image ステータス ユーザ EXEC コマンドを使用することにより、イメージ ダウンロードのステータスを確認できます。

CNS コンフィギュレーションの表示

表 4-2 に記載された特権 EXEC コマンドを使用すると、CNS コンフィギュレーション情報を表示できます。

表 4-2　CNS コンフィギュレーションの表示

コマンド	目的
show cns config connections	CNS Cisco IOS エージェントの接続のステータスを表示します。
show cns config outstanding	開始したにもかかわらず、まだ終了していない差分（部分）CNS 設定に関する情報を表示します。
show cns config stats	Cisco IOS エージェントの統計情報を表示します。
show cns event connections	CNS イベント エージェントの接続のステータスを表示します。
show cns event stats	CNS イベント エージェントの統計情報を表示します。
show cns event subject	アプリケーションによってサブスクライブされたイベント エージェントの件名リストを表示します。

CHAPTER 5

スイッチの管理

この章では、Cisco ME 3400E イーサネット スイッチを管理するための 1 回限りの手順について説明しています。

この章で説明する内容は、次のとおりです。

- 「システム日時の管理」（P.5-1）
- 「システム名およびプロンプトの設定」（P.5-14）
- 「バナーの作成」（P.5-17）
- 「MAC アドレス テーブルの管理」（P.5-19）
- 「ARP テーブルの管理」（P.5-31）

システム日時の管理

Network Time Protocol（NTP）などの自動設定方式、または手動設定方式を使用して、スイッチのシステム日時を管理します。

（注） ここで説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* を参照してください。

ここでは、次の設定情報について説明します。

- 「システム クロックの概要」（P.5-2）
- 「NTP の概要」（P.5-2）
- 「NTP の設定」（P.5-4）
- 「手動での日時の設定」（P.5-11）

システム クロックの概要

時刻サービスの中核となるのはシステム クロックです。このクロックはシステムがスタートアップした瞬間から稼動し、日時を常時監視します。

システム クロックは、次のソースにより設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

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

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

システム クロックは、時刻が*信頼できる*かどうか（つまり、信頼できると見なされるタイム ソースによって時刻が設定されているか）を常時監視します。信頼できない場合は、時刻は表示目的だけに利用され、再配信されません。設定の詳細については、「手動での日時の設定」（P.5-11）を参照してください。

NTP の概要

NTP は、ネットワーク上のデバイス間の時刻の同期化を目的にしています。NTP は UDP で稼動し、UDP は IP 上で稼動します。NTP は RFC 1305 に規定されています。

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

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

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

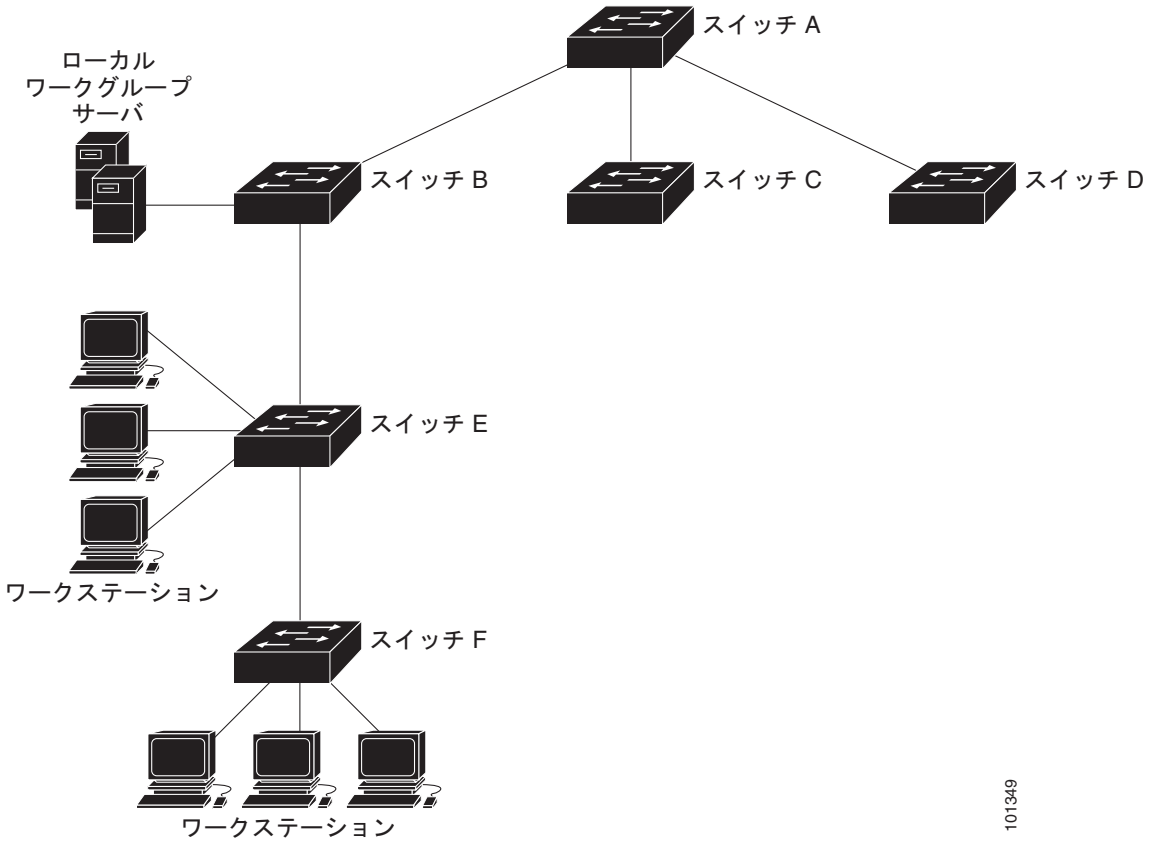
NTP が稼動するデバイス間の通信（*アソシエーション*）は、通常スタティックに設定されます。各デバイスには、アソシエーションを作成すべき全デバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。単にブロードキャスト メッセージを送受信するように各デバイスを設定すればよいので、この代替手段によって設定作業が容易になります。ただし、この場合は、情報の流れは一方向に限られます。

デバイス上で維持される時刻は重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤ってあるいは意図的に設定されることを防いでください。アクセス リスト ベースの制限スキームと暗号化認証メカニズムの、2 つのメカニズムが利用できます。

シスコの NTP はストラタム 1 サービスをサポートしていないので、ラジオ クロックまたは原子時計に接続できません。IP インターネットで利用できるパブリック NTP サーバからネットワークの時刻サービスを受けることを推奨します。

図 5-1 に、NTP を使用した一般的なネットワーク例を示します。スイッチ A は NTP マスターです。スイッチ B、スイッチ C、スイッチ D は、スイッチ A に関連付けられたサーバにおいて NTP サーバ モードで設定されています。スイッチ E はアップストリームおよびダウンストリーム スイッチ（スイッチ B およびスイッチ F）に対する NTP ピアとして設定されています。

図 5-1　　一般的な NTP ネットワーク構成



ネットワークがインターネットに接続されていない場合、シスコの NTP によって、実際には他の方法で時刻が学習されていても、NTP を使用して同期しているように特定のデバイスの動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

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

いくつかのメーカーでは自社のホスト システムに NTP ソフトウェアを組み入れており、UNIX システム用のバージョンやその派生ソフトウェアも利用できます。このソフトウェアによって、ホスト システムも時間が同期化されます。

NTP の設定

スイッチはハードウェアサポート クロックを備えておらず、外部 NTP ソースが利用できないときに、ピアが自身を同期化するための NTP マスター クロックとして機能できません。このスイッチは、カレンダーに対するハードウェア サポートも備えていません。そのため、**ntp update-calendar** および **ntp master** の各グローバル コンフィギュレーション コマンドが使用できません。

ここでは、次の設定情報について説明します。

- 「NTP のデフォルト設定」（P.5-4）
- 「NTP 認証の設定」（P.5-4）
- 「NTP アソシエーションの設定」（P.5-5）
- 「NTP ブロードキャスト サービスの設定」（P.5-7）
- 「NTP アクセス制限の設定」（P.5-8）
- 「NTP パケット用の送信元 IP アドレスの設定」（P.5-10）
- 「NTP 設定の表示」（P.5-11）

NTP のデフォルト設定

表 5-1 に、NTP のデフォルト設定を示します。

表 5-1　NTP のデフォルト設定

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

NTP は、すべてのインターフェイスで、デフォルトでイネーブルに設定されています。すべてのインターフェイスは、NTP パケットを受信します。

NTP 認証の設定

この手順は、NTP サーバの管理者と調整する必要があります。この手順で設定する情報は、時刻を NTP サーバと同期化するためにスイッチが使用するサーバに対応している必要があります。

セキュリティ目的で他のデバイスとのアソシエーション（正確な時間の維持を行う NTP 稼動デバイス間の通信）を認証するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp authenticate**	デフォルトではディセーブルに設定されている NTP 認証機能をイネーブルにします。

	コマンド	目的
ステップ 3	**ntp authentication-key** *number* **md5** *value*	認証鍵を定義します。デフォルト設定では何も定義されていません。 • *number* には、鍵の番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • **md5** は、Message Digest Algorithm 5（MD5）を使用してメッセージ認証サポートが行われることを指定します。 • *value* には、鍵に対する 8 文字までの任意の文字列を入力します。 スイッチとデバイスの双方がいずれかの認証鍵を持ち、**ntp trusted-key** *key-number* コマンドによって鍵番号が指定されていないかぎり、スイッチはデバイスと同期化しません。
ステップ 4	**ntp trusted-key** *key-number*	1 つまたは複数の鍵番号（ステップ 3 で定義したもの）を指定します。ピア NTP デバイスは、このスイッチと同期化するため、このスイッチへの NTP パケット内にこの鍵番号を設定しなければなりません。 デフォルト設定では、信頼される鍵は定義されていません。 *key-number* には、ステップ 3 で定義された鍵を指定します。 このコマンドは、スイッチが、信頼されていないデバイスと誤って同期化するのを防ぎます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

NTP パケットに認証鍵 42 を設定しているデバイスとだけ同期するようにスイッチを設定する例を次に示します。

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

NTP アソシエーションの設定

NTP アソシエーションは、ピア アソシエーション（スイッチを他のデバイスに同期化するか、他のデバイスをスイッチに同期化させるかのどちらかが可能）に設定することも、サーバ アソシエーション（スイッチを他のデバイスに同期化させるだけで、その逆はできない）に設定することもできます。

別のデバイスとの NTP アソシエーションを形成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp peer** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	スイッチのシステム クロックにピアを同期化するか、ピアによって同期化する（ピア アソシエーション）ように設定します。
	または	または
	ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	スイッチのシステム クロックをタイム サーバによって同期化する（サーバ アソシエーション）ように設定します。 ピアまたはサーバ アソシエーションはデフォルトでは定義されていません。 • ピア アソシエーションの *ip-address* には、クロックの同期化を行う、または同期化の対象となるピアの IP アドレスを指定します。サーバ アソシエーションでは、クロックの同期化を行うタイム サーバの IP アドレスを指定します。 • （任意）*number* には、NTP のバージョン番号を指定します。指定できる範囲は 1 ～ 3 です。デフォルトではバージョン 3 が選択されています。 • （任意）*keyid* には、**ntp authentication-key** グローバル コンフィギュレーション コマンドで定義された認証鍵を入力します。 • （任意）*interface* には、IP の送信元アドレスを取得するインターフェイスを指定します。デフォルトでは、送信元 IP アドレスは発信インターフェイスから取得します。 • （任意）キーワード **prefer** を指定すると、このピアまたはサーバが同期化を行う優先ピアまたはサーバになります。このキーワードは、ピアとサーバ間の切り換えを減らします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アソシエーションは、一端のデバイスにしか設定する必要がありません。もう一方のデバイスには自動的にアソシエーションが設定されます。デフォルトの NTP バージョン（バージョン 3）を使用していて NTP が同期化されない場合は、NTP のバージョン 2 を使用してみてください。インターネットで稼動している多くの NTP サーバはバージョン 2 です。

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

NTP バージョン 2 を使用して IP アドレス 172.16.22.44 のピアのクロックに、システム クロックを同期化するようにスイッチを設定する方法を、次の例に示します。

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

NTP ブロードキャスト サービスの設定

NTP が稼動するデバイス間の通信（*アソシエーション*）は通常、スタティックに設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが付与されます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。単にブロードキャスト メッセージを送受信するように各デバイスを設定すればよいので、この代替手段によって設定作業が容易になります。ただし、この場合は、情報の流れは一方向に限られます。

ルータのようにネットワーク上で時刻情報をブロードキャストする NTP ブロードキャスト サーバがある場合、スイッチはインターフェイスごとに NTP ブロードキャスト パケットを送受信できます。スイッチは NTP ブロードキャスト パケットをピアに送信できるので、ピアはそれに同期化できます。スイッチは NTP ブロードキャスト パケットを受信して自身のクロックを同期化することもできます。ここでは、NTP ブロードキャスト パケットの送信と受信の両方の手順について説明します。

NTP ブロードキャスト パケットをピアに送信して、ピアが自身のクロックをスイッチに同期化するよう、スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	NTP ブロードキャスト パケットを送信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 4	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]	NTP ブロードキャスト パケットをピアに送信するインターフェイスをイネーブルにします。 デフォルトでは、この機能はすべてのインターフェイスでディセーブルに設定されています。 • （任意）*number* には、NTP のバージョン番号を指定します。指定できる範囲は 1 ～ 3 です。バージョンを指定しなかった場合は、バージョン 3 が使用されます。 • （任意）*keyid* には、ピアにパケットを送信するときに使用する認証鍵を指定します。 • （任意）*destination-address* には、スイッチにクロックを同期化しているピアの IP アドレスを指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 8		次の手順で説明するように、接続されているピアが NTP ブロードキャスト パケットを受信するように設定します。

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

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast version 2
```

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	NTP ブロードキャスト パケットを受信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と Enhanced Network Interfaces（ENI; 拡張ネットワーク インターフェイス）はディセーブル、NNI はイネーブルに設定されています。
ステップ 4	**ntp broadcast client**	インターフェイスが NTP ブロードキャスト パケットを受信できるようにします。 デフォルトでは、インターフェイスは NTP ブロードキャスト パケットを受信しません。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ntp broadcastdelay** *microseconds*	（任意）スイッチと NTP ブロードキャスト サーバとの間の予測されるラウンドトリップ遅延を変更します。 デフォルトは 3000 マイクロ秒です。指定できる範囲は 1 ～ 999999 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast client
```

NTP アクセス制限の設定

以降で説明するように、2 つのレベルで NTP アクセスを制御できます。

- 「アクセス グループの作成と基本 IP アクセス リストの割り当て」（P.5-8）
- 「特定のインターフェイスでの NTP サービスのディセーブル化」（P.5-10）

アクセス グループの作成と基本 IP アクセス リストの割り当て

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*	アクセス グループを作成し、基本 IP アクセス リストを割り当てます。 キーワードの意味は次のとおりです。 • **query-only**：NTP 制御クエリーに限り許可します。 • **serve-only**：時刻要求に限り許可します。 • **serve**：時刻要求と NTP 制御クエリーは許可しますが、スイッチとリモート デバイスとの同期化は許可しません。 • **peer**：時刻要求と NTP 制御クエリーを許可し、スイッチとリモート デバイスとの同期化を許可します。 *access-list-number* には、1 ～ 99 の範囲で標準の IP アクセス リスト番号を入力します。
ステップ 3	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	アクセス リストを作成します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • キーワード **permit** を入力すると、条件が一致した場合にアクセスを許可します。 • *source* には、スイッチへのアクセスが許可されたデバイスの IP アドレスを入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットを入力します。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否文がデフォルトで存在し、それ以前の文で一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス グループのキーワードは、最小の制限から最大の制限に、次の順序でスキャンされます。

1. **peer**：時刻要求と NTP 制御クエリーを許可し、さらに、アクセス リストの一致基準を満たすアドレスを持つデバイスとスイッチの同期化を許可します。
2. **serve**：時刻要求と NTP 制御クエリーを許可しますが、アクセス リストの一致基準を満たすアドレスを持つデバイスとスイッチの同期は許可しません。
3. **serve-only**：アクセス リストの一致基準を満たすアドレスを持つデバイスからの時刻要求に限り許可します。
4. **query-only**：アクセス リストの一致基準を満たすアドレスを持つデバイスからの NTP 制御クエリーに限り許可します。

送信元 IP アドレスがアクセス リストの複数のアクセス タイプに一致する場合は、最初のタイプが許可されます。アクセス グループが指定されていない場合は、すべてのアクセス タイプがすべてのデバイスに許可されます。いずれかのアクセス グループが指定されている場合は、指定されたアクセス タイプに限り許可されます。

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

次に、スイッチがアクセス リスト 99 からのピアに同期化できるように設定する例を示します。ただし、スイッチはアクセス リスト 42 に対してはアクセスを制限し、時刻要求に限り許可します。

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

特定のインターフェイスでの NTP サービスのディセーブル化

NTP サービスは、すべてのインターフェイスで、デフォルトでイネーブルに設定されています。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、ディセーブルにするインターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と Enhanced Network Interfaces（ENI; 拡張ネットワーク インターフェイス）はディセーブル、NNI はイネーブルに設定されています。
ステップ 4	**ntp disable**	インターフェイス上で NTP パケットの受信をディセーブルにします。 デフォルトでは、すべてのインターフェイスは NTP パケットを受信します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

NTP パケット用の送信元 IP アドレスの設定

スイッチが NTP パケットを送信すると、送信元 IP アドレスは、通常 NTP パケットが送信されたインターフェイスのアドレスに設定されます。すべての NTP パケットに特定の送信元 IP アドレスを使用する場合は、**ntp source** グローバル コンフィギュレーション コマンドを使用します。アドレスは指定されたインターフェイスから取得します。インターフェイス上のアドレスを返信パケット用の宛先として使用できない場合に、このコマンドは便利です。

送信元 IP アドレスの取得先となる特定のインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

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

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

NTP 設定の表示

次の 2 つの特権 EXEC コマンドを使用して NTP 情報を表示できます。

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

この出力に表示されるフィールドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* を参照してください。

手動での日時の設定

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

ここでは、次の設定情報について説明します。

- 「システム クロックの設定」（P.5-11）
- 「日時設定の表示」（P.5-12）
- 「タイム ゾーンの設定」（P.5-12）
- 「夏時間の設定」（P.5-13）

システム クロックの設定

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

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

	コマンド	目的
ステップ 1	**clock set** *hh*:*mm*:*ss day month year* または **clock set** *hh*:*mm*:*ss month day year*	次のいずれかのフォーマットで、手動でシステム クロックを設定します。 • *hh*:*mm*:*ss* には、時刻を時間（24 時間制）、分、秒で指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day* には、当月の日付で日を指定します。 • *month* には、月を名前で指定します。 • *year* には、年を指定します（短縮不可）。

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

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

日時設定の表示

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

システムク ロックは、信頼できる（正確であると確信できる）かどうかを示す *authoritative* フラグを維持します。システム クロックがタイミング ソース（NTP など）によって設定されている場合は、フラグを設定します。時刻が信頼できないものである場合は、表示目的だけで使用されます。クロックが信頼でき、*authoritative* フラグが設定された状態でないと、ピアの時刻が無効でも、フラグはピアがクロックと同期しないようにします。

show clock の表示の前にある記号は、次の意味があります。

- *：時刻は信頼できません。
- （空白）：時刻は信頼できます。
- .：時刻は信頼できますが、NTP は同期していません。

タイム ゾーンの設定

手動でタイム ゾーンを設定するには、特権 EXEC モードで次の手順を実行します。

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

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

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

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

夏時間の設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年特定の日に開始および終了する夏時間を設定します。 夏時間はデフォルトでディセーブルに設定されています。パラメータなしで **clock summer-time** *zone* **recurring** を指定すると、夏時間の規則は米国の規則をデフォルトにします。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何番目の週かを指定します（1 ～ 5、または **last**）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh*:*mm* には、時刻を時間（24 時間制）と分で指定します。 • （任意）*offset* には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次に、夏時間が 4 月の第一日曜の 2 時に始まり、10 月の最終日曜の 2 時に終わるように指定する例を示します。

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

ユーザの居住地域の夏時間が定期的なパターンに従わない場合（次の夏時間のイベントの正確な日時を設定する）は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	最初の日付で夏時間開始の日付を、2 番目の日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何番目の週かを指定します（1 ～ 5、または **last**）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh*:*mm* には、時刻を時間（24 時間制）と分で指定します。 • （任意）*offset* には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

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

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

システム名およびプロンプトの設定

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

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

ここで説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* および『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* を参照してください。

ここでは、次の設定情報について説明します。

- 「デフォルトのシステム名およびプロンプトの設定」（P.5-15）
- 「システム名の設定」（P.5-15）
- 「DNS の概要」（P.5-15）

デフォルトのシステム名およびプロンプトの設定

デフォルトでは、システム名およびプロンプトは *Switch* です。

システム名の設定

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

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

システム名を設定すると、システム プロンプトとしても使用されます。

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

DNS の概要

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

IP によって定義される階層型の命名規則では、デバイスを場所またはドメインで識別できます。ドメイン名の区切りには、ピリオド（.）を使用します。たとえばシスコシステムズは、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com* です。このドメイン内の特定のデバイス、たとえば FTP（ファイル転送プロトコル）システムは、*ftp.cisco.com* で表されます。

IP でドメイン名を追跡するためにドメイン ネーム サーバという概念が定義されています。DNS は、名前と IP アドレスのマッピングをキャッシュ（またはデータベース）に保管します。ドメイン名を IP アドレスにマッピングするには、まず、ホスト名を明示し、ネットワーク上に存在するネーム サーバを指定し、DNS をイネーブルにします。

ここでは、次の設定情報について説明します。

- 「DNS のデフォルト設定」（P.5-16）
- 「DNS の設定」（P.5-16）
- 「DNS 設定の表示」（P.5-17）

DNS のデフォルト設定

表 5-2 に、DNS のデフォルト設定を示します。

表 5-2　DNS のデフォルト設定

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

DNS の設定

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

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

	コマンド	目的
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

DNS 設定の表示

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

バナーの作成

Message-of-The-Day（MoTD）バナーおよびログイン バナーを作成できます。MoTD バナーはログイン時に接続しているすべての端末で表示され、すべてのネットワーク ユーザに影響のあるメッセージ（システムのシャットダウン予告など）を送信するのに便利です。

ログイン バナーも、すべての接続端末で表示されます。表示されるのは、MoTD バナーのあとで、ログイン プロンプトが表示される前です。

（注）　ここで説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* を参照してください。

ここでは、次の設定情報について説明します。

- 「バナーのデフォルト設定」（P.5-17）
- 「MoTD ログイン バナーの設定」（P.5-18）
- 「ログイン バナーの設定」（P.5-19）

バナーのデフォルト設定

MoTD バナーおよびログイン バナーは設定されません。

MoTD ログイン バナーの設定

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

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

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

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

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

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

次に、前の設定により表示されたバナーを示します。

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

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

User Access Verification

Password:
```

ログイン バナーの設定

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

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

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

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

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

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

MAC アドレス テーブルの管理

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

- ダイナミック アドレス：スイッチが学習し、使用されなくなった時点で期限切れとなる送信元 MAC アドレス
- スタティック アドレス：手動で入力するユニキャスト アドレス。これらのアドレスには期限がなく、スイッチがリセットされても失われません。

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN ID、およびアドレスとタイプ（スタティックとダイナミック）に対応付けられたポート番号を保持します。

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

ここでは、次の設定情報について説明します。

- 「アドレス テーブルの作成」（P.5-20）
- 「MAC アドレスと VLAN」（P.5-20）
- 「MAC アドレス テーブルのデフォルト設定」（P.5-21）
- 「アドレス エージング タイムの変更」（P.5-21）
- 「ダイナミック アドレス エントリの削除」（P.5-22）
- 「MAC アドレス変更通知トラップの設定」（P.5-22）
- 「MAC アドレス移動通知トラップの設定」（P.5-24）
- 「MAC しきい値通知トラップの設定」（P.5-26）
- 「スタティック アドレス エントリの追加および削除」（P.5-27）
- 「ユニキャスト MAC アドレス フィルタリングの設定」（P.5-28）
- 「VLAN 上での MAC アドレス学習のディセーブル化」（P.5-29）
- 「アドレス テーブル エントリの表示」（P.5-31）

アドレス テーブルの作成

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

有効期間はグローバルに設定されます。ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、Spanning-Tree Protocol（STP; スパニングツリー プロトコル）によって VLAN ごとの有効期間を短縮することができます。

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

MAC アドレスと VLAN

アドレスはすべて、VLAN と対応付けられます。1 つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定することができます。たとえば、ユニキャスト アドレスは VLAN1 内のポート 1 と、VLAN 5 内のポート 1、ポート 9、ポート 10 に転送できます。

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

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

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

プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。

MAC アドレス学習は VLAN 単位でディセーブルにできます。サービス プロバイダー ネットワーク内のカスタマーは、ネットワークを介して 大量の MAC アドレスをトンネリングし、利用可能な MAC アドレス テーブルのスペースを満たすことができます。MAC アドレスを学習できる VLAN、つまりポートを制御することにより、VLAN 上での MAC アドレス学習を制御し、また、スイッチで利用可能な MAC アドレス テーブル スペースを管理できます。

MAC アドレス学習をディセーブルにする前に、ネットワーク トポロジとスイッチ システム設定に詳しいことを確認してください。VLAN で MAC アドレス学習をディセーブルにすると、ネットワークでフラッディングを引き起こす可能性があります。詳細については、「VLAN 上での MAC アドレス学習のディセーブル化」（P.5-29）を参照してください。

MAC アドレス テーブルのデフォルト設定

表 5-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 5-3　MAC アドレス テーブルのデフォルト設定

機能	デフォルト設定
エージング タイム	300 秒
ダイナミック アドレス	自動学習
スタティック アドレス	設定なし
VLAN 上での MAC アドレス学習	イネーブル

アドレス エージング タイムの変更

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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]	ダイナミック エントリが使用または更新されたあと、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ～ 1000000 秒です。デフォルト値は 300 秒です。0 も入力できます。その場合、期限切れがディセーブルになります。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 *vlan-id* に指定できる範囲は 1 ～ 4094 です。先行ゼロは入力しないでください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table aging-time**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

ダイナミック アドレス エントリの削除

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

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

MAC アドレス変更通知トラップの設定

MAC アドレス変更通知では、MAC アドレスの変更アクティビティを保存することによって、ネットワーク上のユーザが追跡されます。スイッチが MAC アドレスを学習または削除する場合に、SNMP（簡易ネットワーク管理プロトコル）通知トラップを、Network Management System（NMS; ネットワーク管理システム）に送信できます。ネットワークから多数のユーザの出入りがある場合は、トラップインターバル タイムを、通知トラップを組み込むように設定して、ネットワーク トラフィックを削減できます。MAC 通知履歴テーブルには、トラップが設定されたポートごとの MAC アドレス アクティビティが保存されます。MAC アドレス変更通知は、ダイナミックまたはセキュア MAC アドレスに関して生成されます。自アドレス、マルチキャスト アドレス、または他のスタティック アドレスに関しては、通知は生成されません。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信デバイスを指定します。 • *hos-addr* には、NMS の名前または IP アドレスを指定します。 • SNMP トラップをホストに送信するには、**traps**（デフォルト）を指定します。SNMP インフォームをホストに送信するには、**informs** を指定します。 • サポートされる SNMP バージョンを指定します。バージョン 1 がデフォルトですが、インフォームでは使用できません。 • *community-string* には、通知作業で送信する文字列を指定します。この文字列は、**snmp-server host** コマンドで設定できますが、**snmp-server community** コマンドでこの文字列を定義してから **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* には、キーワード **mac-notification** を使用します。
ステップ 3	**nmp-server enable traps mac-notification change**	スイッチが MAC アドレス変更通知トラップを NMS に送信できるようにします。
ステップ 4	**mac address-table notification change**	MAC アドレス変更通知機能をイネーブルにします。
ステップ 5	**mac address-table notification change** [**interval** *value*] | [**history-size** *value*]	トラップ インターバル タイムと履歴テーブルのサイズを入力します。 • （任意）**interval** *value* には、NMS に対して生成される各トラップ セット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ～ 2147483647 秒です。デフォルトは 1 秒です。 • （任意）**history-size** *value* には、MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0 ～ 500 です。デフォルト値は 1 です。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。

	コマンド	目的
ステップ 7	**snmp trap mac-notification change** {**added** | **removed**}	インターフェイス上の MAC アドレス変更通知トラップをイネーブルにします。 • MAC アドレスがインターフェイスに**追加される**際に、トラップをイネーブルにします。 • MAC アドレスがインターフェイスから**削除される**際に、トラップをイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mac address-table notification change interface** **show running-config**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次に、NMS として 172.20.10.10 を指定し、スイッチによる NMS への MAC アドレス通知トラップの送信をイネーブルにして、MAC アドレス変更通知機能をイネーブルにし、インターバル タイムを 123 秒、履歴サイズを 100 エントリ、指定されたポートで MAC アドレスが追加されたときはいつでもトラップをイネーブルに設定する例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification change added
```

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

MAC アドレス移動通知トラップの設定

MAC 移動通知を設定すると、MAC アドレスが、あるポートから同じ LAN 内の別のポートに移動する際には常に SNMP 通知が生成され、ネットワーク管理システムに送信されます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信デバイスを指定します。 • *hos-addr* には、NMS の名前または IP アドレスを指定します。 • SNMP トラップをホストに送信するには、**traps**（デフォルト）を指定します。SNMP インフォームをホストに送信するには、**informs** を指定します。 • サポートされる SNMP バージョンを指定します。バージョン 1 がデフォルトですが、インフォームでは使用できません。 • *community-string* には、通知作業で送信する文字列を指定します。この文字列は、**snmp-server host** コマンドで設定できますが、**snmp-server community** コマンドでこの文字列を定義してから **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* には、キーワード **mac-notification** を使用します。
ステップ 3	**snmp-server enable traps mac-notification move**	スイッチが MAC アドレス移動通知トラップを NMS に送信できるようにします。
ステップ 4	**mac address-table notification mac-move**	MAC アドレス移動通知機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show mac address-table notification mac-move** **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次に、NMS として 172.20.10.10 を指定し、スイッチによる NMS への MAC アドレス移動通知トラップの送信をイネーブルにし、MAC アドレス移動通知機能をイネーブルにし、MAC アドレスがあるポートから他のポートへ移動されたときはいつでもトラップをイネーブルに設定する例を示します。

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

show mac address-table notification mac-move 特権 EXEC コマンドを入力すれば、設定を確認できます。

MAC しきい値通知トラップの設定

MAC しきい値通知を設定すると、MAC アドレス テーブルのしきい値の限度に達するか、超過した場合に、SNMP 通知が生成され、ネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス テーブルしきい値通知トラップを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信デバイスを指定します。 • *hos-addr* には、NMS の名前または IP アドレスを指定します。 • SNMP トラップをホストに送信するには、**traps**（デフォルト）を指定します。SNMP インフォームをホストに送信するには、**informs** を指定します。 • サポートされる SNMP バージョンを指定します。バージョン 1 がデフォルトですが、インフォームでは使用できません。 • *community-string* には、通知作業で送信する文字列を指定します。この文字列は、**snmp-server host** コマンドで設定できますが、**snmp-server community** コマンドでこの文字列を定義してから **snmp-server host** コマンドを使用することを推奨します。 • *notification-type* には、キーワード **mac-notification** を使用します。
ステップ 3	**snmp-server enable traps mac-notification threshold**	スイッチが MAC アドレスしきい値通知トラップを NMS に送信できるようにします。
ステップ 4	**mac address-table notification threshold**	MAC アドレスしきい値通知機能をイネーブルにします。
ステップ 5	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]	MAC アドレスしきい値使用率モニタリングのしきい値を入力します。 • （任意）limit percentage には、MAC アドレス テーブルの使用率を指定します。有効な値は 1 ～ 100 % です。デフォルト値は 50% です。 • （任意）interval time には、通知間の時間を指定します。有効な値は 120 秒以上です。デフォルト値は 120 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mac address-table notification threshold** **show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

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

show mac address-table notification threshold 特権 EXEC コマンドを入力すれば、設定を確認できます。

スタティック アドレス エントリの追加および削除

スタティック アドレスには次の特性があります。

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

スタティック アドレスを追加および削除し、転送動作を定義することができます。転送動作とは、パケットを受信したポートが、そのパケットを他のポートに転送する方法を定義するものです。すべてのポートは 1 つまたは複数の VLAN に関連付けられているので、スイッチは、指定されたポートから、そのアドレスに対応する VLAN ID を取得します。各送信元ポートに個別の宛先ポートのリストを指定できます。

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

アドレス テーブルにスタティック アドレスを追加するには、宛先 MAC ユニキャスト アドレスおよびその送信先となる VLAN を指定します。この宛先アドレスとともに受信されたパケットは、オプション *interface-id* で指定されたインターフェイスへ転送されます。

プライベート VLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての関連 VLAN に設定する必要があります。プライベート VLAN のプライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは関連 VLAN には複製されません。プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	MAC アドレス テーブルにスタティック アドレスを追加します。 • *mac-addr* には、アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 • *vlan-id* には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。有効な VLAN ID は 1 ～ 4094 です。0 から始めないでください。 • *interface-id* には、受信したパケットの転送先となるインターフェイスを指定します。有効なインターフェイスは、物理ポートやポート チャネルなどです。スタティック マルチキャスト アドレスの場合、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合、同時に入力できるインターフェイスは 1 つだけですが、同じ MAC アドレスおよび VLAN ID でコマンドを複数回入力できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table static**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
```

ユニキャスト MAC アドレス フィルタリングの設定

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

この機能を使用する場合、次の注意事項に従ってください。

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

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

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

- CPU に転送されるパケットもサポートされません。

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

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

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

送信元または宛先ユニキャスト MAC アドレスおよび受信先の VLAN を指定することにより、ユニキャスト MAC アドレス フィルタリングをイネーブルにして、スイッチが特定のアドレスを持つパケットを廃棄するように設定します。

スイッチが送信元または宛先ユニキャスト スタティック アドレスを廃棄するよう設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**	ユニキャスト MAC アドレス フィルタリングをイネーブルにして、スイッチが特定の送信元または宛先ユニキャスト スタティック アドレスを持つパケットを廃棄するように設定します。 • *mac-addr* には、送信元または宛先ユニキャスト MAC アドレスを指定します。この MAC アドレスを持つパケットは廃棄されます。 • *vlan-id* には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID は、1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table static**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ユニキャスト MAC アドレス フィルタリングをディセーブルにするには、**no mac address-table static** *mac-addr* **vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

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

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

VLAN 上での MAC アドレス学習のディセーブル化

デフォルトでは、MAC アドレス学習はスイッチのすべての VLAN 上で イネーブルに設定されています。VLAN で MAC アドレス学習を制御する場合、MAC アドレスを学習できる VLAN、つまりポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。MAC アドレス学習をディセーブルにする場合、ネットワーク トポロジおよびスイッチのシステム構成に精通している必要があります。VLAN で MAC アドレス学習をディセーブルにすると、ネットワークでフラッディングを引き起こす可能性があります。

VLAN 上で MAC アドレス学習をディセーブルにする場合は、次の注意事項に従ってください。

- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）が設定されている VLAN 上で MAC アドレス学習をディセーブルにするには、事前に注意が必要です。スイッチはレイヤ 2 ドメイン内のすべての IP パケットをフラッディングします。
- MAC アドレス学習は、1 から 4094 までの 1 つの VLAN ID（例 : **no mac address-table learning vlan 223**）、または、ハイフンやカンマで区切られた一連の VLAN ID（例 : **no mac address-table learning vlan 1-10, 15**）でディセーブルにできます。
- MAC アドレス学習は、2 ポートを装備する VLAN でだけディセーブルにすることを推奨します。3 つ以上のポートを持つ VLAN 上で MAC アドレス学習をディセーブルにすると、スイッチに着信するすべてのパケットがその VLAN ドメイン内でフラッディングされます。
- スイッチが内部的に使用する VLAN では、MAC アドレス学習をディセーブルにできません。入力した VLAN ID が内部 VLAN である場合、スイッチはエラー メッセージを生成して、コマンドを拒否します。使用中の内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。
- 特定のプライベート VLAN のプライマリ VLAN として設定されている VLAN 上で、MAC アドレス学習をディセーブルにした場合でも、MAC アドレスはそのプライベート VLAN に属するセカンダリ VLAN で学習され、その後プライマリ VLAN で複製されます。特定のプライベート VLAN のプライマリ VLAN ではなく、セカンダリ VLAN で MAC アドレス学習をディセーブルにした場合は、MAC アドレスはプライマリ VLAN で学習され、セカンダリ VLAN では複製されます。
- RSPAN VLAN で MAC アドレス学習はディセーブルにできません。設定すること自体できません。
- セキュア ポートを含む VLAN で MAC アドレス学習をディセーブルにする場合、そのポートでは、MAC アドレス学習はディセーブルになりません。ポート セキュリティをディセーブルにすると、設定された MAC アドレス学習ステートがイネーブルになります。

VLAN で MAC アドレス学習をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no mac address-table learning vlan** *vlan-id*	指定された VLAN（複数可）で、MAC アドレス学習をディセーブルにします。1 つの VLAN ID を指定するか、一連の VLAN ID をハイフンまたはカンマで区切って指定できます。指定できる VLAN ID は 1 ～ 4094 です。内部 VLAN にはできません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table learning** [**vlan** *vlan-id*]	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN 上で MAC アドレス学習を再度イネーブルにするには、**default mac address-table learning vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。また、**mac address-table learning vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用しても、VLAN 上で MAC アドレス学習を再度イネーブルにできます。最初のコマンド（**デフォルト**）がデフォルトの状態に戻るので、**show running-config** コマンドの出力には表示されません。2 番目のコマンドを使用すると、**show running-config** 特権 EXEC コマンドで表示される設定となります。

次に、VLAN 200 上で MAC アドレス学習をディセーブルにする例を示します。

```
Switch(config)# no mac address-table learning vlan 200
```

show mac-address-table learning [**vlan** *vlan-id*] 特権 EXEC コマンドを入力すると、すべての VLAN または指定された VLAN の MAC アドレス学習の状態を表示できます。

アドレス テーブル エントリの表示

表 5-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用すると、MAC アドレス テーブルを表示できます。

表 5-4　MAC アドレス テーブル表示用のコマンド

コマンド	説明
show ip igmp snooping groups	すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャスト エントリを表示します。
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table learning	すべての VLAN または指定された VLAN の MAC アドレス学習ステータスを表示します。
show mac address-table notification	MAC 通知パラメータと履歴テーブルを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

ARP テーブルの管理

デバイスと通信するには（たとえば、イーサネットを介して）、ソフトウェアは最初に、そのデバイスの 48 ビット MAC アドレスまたはローカル データ リンク アドレスを学習する必要があります。IP アドレスからローカル データ リンク アドレスを学習するプロセスを、「*アドレス解決*」と呼びます。

Address Resolution Protocol（ARP; アドレス解決プロトコル）は、ホスト IP アドレスを、対応する MAC アドレスと VLAN ID に関連付けます。IP アドレスを使用すると、ARP はそれに関連付けられた MAC アドレスを検索します。MAC アドレスが見つかると、それ以降迅速に検索できるように、IP-MAC アドレス アソシエーションが ARP キャッシュに格納されます。そのあと、IP データグラムはリンクレイヤ フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化、および ARP 要求や応答については、Subnetwork Access Protocol（SNAP）で規定されています。IP インターフェイスでは、標準イーサネット形式の ARP カプセル化（キーワード **arpa** で表される）がデフォルトでイネーブルに設定されています。

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

CLI（コマンドライン インターフェイス）の手順については、Cisco.com で Cisco IOS Release 12.2 のマニュアルを参照してください。

CHAPTER 6

スイッチ アラームの設定

ME 3400E スイッチでは、外部アラーム入力に加え、失われていたり、誤動作したりしている電源、または入力のない電源を特定するためのアラームを設定できます。

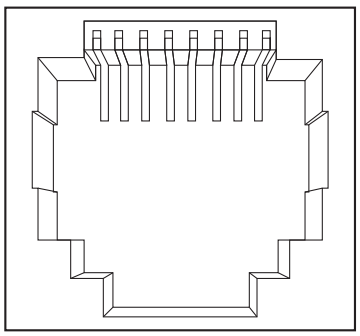
- 「外部アラームの設定」（P.6-1）
- 「電源装置アラームの設定」（P.6-3）

外部アラームの設定

スイッチの前面パネル上のアラーム入力ポートに対して、ドア、温度計、火災報知機といった、ご使用の環境内に存在する外部デバイスからのアラーム入力を最大 4 つまで接続できます。図 6-1 に、アラーム用ピン割り当ての位置を示します。

図 6-1　　アラーム入力ポートのピン割り当て

Pin 番号	アラーム接続
1	アラーム入力 1
2	アラーム入力 2
3	接続なし
4	アラーム入力 3
5	アラーム入力 4
6	接続なし
7	接続なし
8	共通アラーム



各アラーム入力に対して、アラームをトリガーするための開回路または閉回路を設定し、また、アラームの重大度を設定できます。アラームをトリガーすると、システム メッセージが生成されます。アラームの記述名を入力すると、その名前がシステム メッセージ内に表示されます。アラームがトリガーされると、LED ディスプレイも点灯します（LED は通常はオフになっており、これはアラームがないことを意味しています）。LED については、『*Cisco ME-3400E Hardware Installation Guide*』を参照してください。

アラーム トリガーの設定は、**open** か **closed** のいずれかとなります。設定しない場合、回路が閉じるとアラームがトリガーされます。

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

アラームの重大度は、**minor**、**major**、または **critical** に設定できます。重大度はアラーム メッセージに表示され、また、重大度によって、アラームがトリガーされたときの LED の色も設定されます。LED は、マイナー アラームの場合はオレンジ、メジャー アラームの場合は赤で点灯し、クリティカル アラームの場合は赤で点滅します。設定されていない場合、アラームのデフォルトの重大度は、**minor** です。

アラーム接点を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**alarm-contact** *contact-number* **description** ***string***	（任意）アラーム接点番号の説明を設定します。 • *contact-number* に指定できる値は 1 ～ 4 です。 • 説明の文字列は 80 文字までの英数字で指定し、この文字列は、生成されるすべてのシステム メッセージに表示されます。
ステップ 3	**alarm-contact** {*contact-number* | **all**} {**severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}}	アラーム接点番号またはすべての接点番号の、トリガーおよび重大度を設定します。 • 接点番号（1 ～ 4）を入力するか、**すべての**アラームを設定することを指定します。アラーム接点のピン割り当てについては、図 6-1 を参照してください。 • **severity** には、**critical**、**major**、または **minor** を入力します。重大度を設定しない場合、デフォルトは **minor** となります。 • **trigger** には、**open** または **closed** を入力します。トリガーを設定しない場合、回路が **closed** のときにアラームがトリガーされます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show env alarm-contact**	設定したアラーム接点を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アラームの説明を削除するには、**no alarm-contact** *contact-number* **description** 特権 EXEC コマンドを入力します。アラームの重大度を **minor**（デフォルト）に設定するには、**no alarm-contact** {*contact-number* | **all**} **severity** を入力します。アラーム接点のトリガーを **closed**（デフォルト）に設定するには、**no alarm-contact** {*contact-number* | **all**} **trigger** を入力します。

アラーム設定およびステータスを確認するには、**show env alarm-contact** 特権 EXEC コマンドを入力します。

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

（注） 本スイッチでは、これらのアラームの CISCO-ENTITY-ALARM-MIB がサポートされています。

次に、*door sensor* という名前のアラーム入力 2 を、ドアの回路が閉じたときにメジャー アラームをアサートするように設定し、次に、すべてのアラームのステータスおよび設定を表示する例を示します。

```
Switch(config)# alarm-contact 2 description door sensor
Switch(config)# alarm-contact 2 severity major
Switch(config)# alarm-contact 2 trigger closed
Switch(config)# end
Switch(config)# show env alarm-contact
Switch# show env alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: test_1
   Severity:    critical
   Trigger:     open
ALARM CONTACT 2
   Status:      not asserted
   Description: door sensor
   Severity:    major
   Trigger:     closed
ALARM CONTACT 3
   Status:      not asserted
   Description: flood sensor
   Severity:    critical
   Trigger:     closed
ALARM CONTACT 4
   Status:      not asserted
   Description:
   Severity:    critical
   Trigger:     closed
```

電源装置アラームの設定

スイッチ モデルの中には、AC 電源または DC 電源を備えた 2 つの電源スロットを持つものがあります。各スロットに対して提供される電源のステータスとタイプは、スイッチの LED によって示されます。AC 電源には対応する AC 電源入力（AC 1 と AC 2）が用意され、DC 電源には 2 つの DC 入力（DC A および DC B）が用意されています。

デフォルトの電源設定では、スロット 1 に 1 つの電源が取り付けられ、また、**no power-supply dual** 用ソフトウェアが用意されています。これにより、電源が 2 つ取り付けられていないことでトリガーされるアラームを抑制します。スイッチが 2 つの電源で動作している場合、**power-supply dual** グローバル コンフィギュレーション コマンドを入力して、片方の電源が失われたり、動作不能となったりした場合にアラームがトリガーされるようにすることをお勧めします。

DC 電源を使用している場合、両方の DC 入力を接続するのが最も一般的なやり方です。

（注） Cisco ME 3400EG-2CS-A スイッチでは、着脱式の電源はサポートされていません。

スイッチによって電源の障害が検知されると、LED インジケータがトリガーされ、システム メッセージが送信されます。電源が失われたり、出力が不十分だったり、ファンが誤動作したりした場合、電源アラーム インジケータが送信されます。これらのアラーム条件の中には、設定可能なものがあります。

電源不在アラーム

単一の電源（AC または DC）でスイッチを動作させている場合、失われた電源に関連したアラーム条件を抑制できます。**no power-supply dual** グローバル コンフィギュレーション コマンド（デフォルト）を入力すると、電源は 1 つしか存在していないと見なされるように指定できます。その結果、電源が失われているというアラームがスイッチによって生成されなくなります。

no power-supply dual コマンドによって、2 番目の電源の不在、または 2 番目の電源に対する入力の不在に関するメッセージの送信だけを制御できます。ソフトウェアによって、電源が存在しているかどうか、また、入力電圧が存在しているかどうかが検出されます。入力が存在している場合、ソフトウェアによって、出力電圧が存在しているかどうか、また、ファンが動作しているかどうかを検出できます。電源が 1 つしかないと見なされる場合、次の条件および結果が発生する可能性があります。

- 電源が 1 つしか存在しない場合、アラームは送信されません。ただし、この電源が AC 入力に接続されており、電力を受信または送信していない場合、電源障害メッセージが送信されます。
- 電源が 2 つ存在しており、両方の電源が電力を受信および送信している場合、メッセージは送信されません。
- 電源が 2 つ存在しており、片方が AC 入力に接続されて動作しており、もう片方が接続されていない場合、メッセージは送信されません。
- 電源が 2 つ存在しており、両方の電源が AC 入力に接続されているが、片方の電源だけが電力を受信または送信している場合、電源障害メッセージが送信されます。

（注） AC 入力に接続されている AC 電源が電力を受信または送信していない場合は必ず、スイッチによってエラー メッセージが送信されます。

2 つの電源でスイッチを動作させている場合、**power-supply dual** グローバル コンフィギュレーション コマンドを入力して、片方の電源が失われたときにメッセージを送信するようにスイッチを設定します。

DC 電源フィード アラーム

2 つの DC 電源入力は、内部的にブリッジされ、両方の電源スロットにフィードされています。1 つまたは 2 つの DC 電源が設置されている場合、スイッチによって両方の DC 入力が検出されないと、LED アラームおよびシステム メッセージが生成されます。DC 入力を 1 つしか使用したくない場合、**no power-supply dual dc-feed** グローバル コンフィギュレーション コマンドを入力して、2 番目の DC 入力が存在しない場合のアラーム メッセージの送信をディセーブルにできます。このコマンドは、DC 電源がスイッチに設置されている場合にだけ有効です。

このコマンドがどのように設定されているかに関わらず、DC 電源入力（1 つまたは 2 つ）が存在していると見なされていて、電源に問題が検出された場合、電源障害メッセージが生成されます。

電源アラーム メッセージを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **power-supply dual**	スイッチに電源が 1 つだけ設置されている場合にアラームを生成するかどうかを指定します。 • **no power-supply dual** を入力すると、電源が失われた場合のアラーム通知が抑制されます。これはデフォルト設定です。 • **power-supply dual** を入力すると、両方の電源のアラーム通知がイネーブルになります。
ステップ 3	**[no] power-supply dual dc-feed**	DC 電源だけが設置されており、存在している DC 電源入力が 1 つだけの場合にアラームを生成するかどうかを指定します。 • **no power-supply dual dc-feed** を入力すると、DC 電源入力が失われた場合のアラーム通知が抑制されます。 • **power-supply dual dc-feed** を入力すると、存在している DC 電源入力が 1 つの場合のアラーム通知がイネーブルになります。これはデフォルト設定です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show env power**	設定済みの電源エラー通知を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチの電源設定を変更するには、**show env power** ユーザ EXEC コマンドを入力します。

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

次に、存在している電源が 1 つの場合のアラーム通知を抑制する方法と、その設定を変更する例を示します。

```
Switch(config)# no power-supply dual
Switch(config)# end
Switch# show env power
POWER SUPPLY 1 is AC OK
   AC Input  : OK
   Output    : OK
   Fan       : OK
POWER SUPPLY 2 is NOT PRESENT
```

CHAPTER 7

SDM テンプレートの設定

この章では、Cisco ME 3400E イーサネット アクセススイッチで Switch Database Management（SDM; スイッチ データベース管理）テンプレートを設定する方法について説明します。SDM テンプレートの設定は、スイッチでメトロ IP アクセス イメージが稼動している場合に限りサポートされます。

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

- 「SDM テンプレートの概要」（P.7-1）
- 「スイッチ SDM テンプレートの設定」（P.7-3）
- 「SDM テンプレートの表示」（P.7-6）

SDM テンプレートの概要

スイッチでメトロ IP アクセス イメージが稼動している場合には、SDM テンプレートを使用してスイッチのシステム リソースを最適化し、ネットワークでのスイッチの使用方法に応じて、特定の機能をサポートできます。SDM テンプレートは、Ternary CAM（TCAM）リソースを割り当てて、各種機能をサポートします。IP バージョン 4（IPv4）の SDM テンプレートを使用してデフォルト テンプレートを選択すると、システム リソースを均等化できます。レイヤ 2 テンプレートを選択して、ハードウェア内でレイヤ 2 機能だけをサポートすることもできます。

（注） メトロ アクセス イメージを稼動しているスイッチは、レイヤ 2 テンプレートだけをサポートしています。

- レイヤ 2：レイヤ 2 テンプレートは、レイヤ 2 機能用にシステム リソースを最大化し、ルーティングをサポートしません。このテンプレートは、スイッチがレイヤ 2 転送用に使用される場合に使用する必要があります。メトロ IP アクセス イメージを稼動しているスイッチ上でレイヤ 2 テンプレートを選択すると、すべてのルーティングがソフトウェアにより実行されるため、CPU は過負荷となり、ルーティング パフォーマンスは大幅に低下します。
- デフォルト：デフォルト テンプレートは、すべての機能（レイヤ 2 およびレイヤ 3 [ルーティング]）に対してリソースを均衡化します。このテンプレートは、メトロ IP アクセス イメージを稼動しているスイッチ上でだけ使用可能です。スイッチでルーティングがイネーブルである場合にデフォルト テンプレートを使用しなければ、すべてのルーティングはソフトウェアにより実行されるため、CPU は過負荷となり、ルーティング パフォーマンスは大幅に低下します。

また、デュアル IPv4 および IPv6 はデュアル スタック環境をイネーブルにします。「デュアル IPv4 および IPv6 SDM テンプレート」（P.7-2）を参照してください。

表 7-1 に、メトロ IP アクセス イメージを稼動しているスイッチに対して 2 つの IPv4 テンプレートがそれぞれサポートする各リソースの概数を示します。テンプレートの値は、8 つのルーテッド インターフェイスおよび約 1024 の VLAN に基づき、テンプレートの選択時に設定されるおおよそのハードウェア境界を表します。ハードウェア リソースのセクションが満杯の場合、処理できないものはすべて CPU に送信されるため、スイッチのパフォーマンスに著しく影響します。

表 7-1　各テンプレートに割り当てられた機能のリソースの概算

リソース	レイヤ 2	デフォルト
ユニキャスト MAC アドレス	8 K	5 K
IPv4 IGMP グループおよびマルチキャスト ルート（デフォルトのみ）	–	1 K
IPv4 IGMP グループ（レイヤ 2 のみ）	1 K	–
IPv4 マルチキャスト ルート（レイヤ 2 のみ）	0	–
IPv4 IGMP グループおよびマルチキャスト ルート	1 K	–
IPv4 ユニキャスト ルート	0	9 K
• IPv4 ホストに直接接続	–	5 K
• 間接 IPv4 ルート	–	4 K
IPv4 ポリシー ベース ルーティング ACE[1]	0	0.5 K
IPv4 または MAC QoS[2] ACE	0.5 K	0.5 K
IPv4 または MAC セキュリティ ACE	1 K	1 K

1. ACE = Access control entrie（アクセス制御エントリ）。
2. QoS = Quality of service（サービス品質）。

デュアル IPv4 および IPv6 SDM テンプレート

SDM テンプレートを選択すると IP バージョン 6（IPv6）をサポートできます。IPv6 の詳細および IPv6 ルーティングの設定手順については、第 37 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。IPv6 ACL の設定については、第 39 章「IPv6 ACL の設定」を参照してください。

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

デュアル IPv4 および IPv6 テンプレートを使用することにより、IPv4 と IPv6 の両方をサポートするデュアル スタック環境でスイッチを使用できます。デュアル スタック テンプレートを使用すると、各リソースで許容される TCAM 容量が少なくなります。IPv4 トラフィックだけを転送する場合は、使用しないでください。

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

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

- デュアル IPv4/IPv6 VLAN テンプレート：スイッチ上で、IPv4 の基本レイヤ 2、マルチキャスト、QoS、ACL、および IPv6 の基本レイヤ 2 と ACL をサポートします。

このソフトウェア リリースでは、IPv6 マルチキャスト ルーティング、IPv6 QoS、または IPv6 Multicast Listener Discovery（MLD）スヌーピングはサポートされていません。

（注）　IPv4 ルートに必要なのは、1 つの TCAM エントリだけです。IPv6 ではハードウェア圧縮方式が使用されるため、IPv6 ルートは複数の TCAM エントリを使用することができ、ハードウェアで転送されるエントリ数が削減されます。

表 7-2 に、各デュアル テンプレートによって割り当てられた機能リソースの概数を示します。テンプレートの見積もりは、8 つのルーテッド インターフェイス、約 1000 個の VLAN が設定されたスイッチを基準にしています。

表 7-2　デュアル IPv4/IPv6 テンプレートによって許可される機能リソースの概算

リソース	IPv4-and-IPv6 デフォルト	IPv4-and-IPv6 ルーティング	IPv4-and-IPv6 VLAN
ユニキャスト MAC アドレス	2 K	1.5 K	8 K
IPv4 IGMP グループおよびマルチキャスト ルート	1 K	1 K	1 K
IPv4 ユニキャスト ルートの合計：	3 K	2.75 K	0
• IPv4 ホストに直接接続	2 K	1.5 K	0
• 間接 IPv4 ルート	1 K	1.25 K	0
IPv6 マルチキャスト グループ	1 K	1 K	1 K
IPv6 ユニキャスト ルートの合計：	3 K	2.75 K	0
• 直接接続された IPv6 アドレス	2 K	1.5 K	0
• 間接 IPv6 ユニキャスト ルート	1 K	1.25 K	0
IPv4 ポリシー ベース ルーティング ACE	0	0.25 K	0
IPv4 または MAC QoS ACE（合計）	0.75 K	0.75 K	0.75 K
IPv4 または MAC セキュリティの ACE（合計）	1 K	0.5 K	1 K
IPv6 ポリシー ベース ルーティング ACE[1]	0	0.25 K	0
IPv6 QoS ACE	0.5 K	0.5 K	0.5 K
IPv6 セキュリティの ACE	0.5 K	0.5 K	0.5 K

1. IPv6 Policy-Based Routing（PBR; ポリシー ベース ルーティング）はサポートされていません。

スイッチ SDM テンプレートの設定

- 「デフォルトの SDM テンプレート」（P.7-4）
- 「SDM テンプレートの設定時の注意事項」（P.7-4）
- 「SDM テンプレートの設定」（P.7-5）

デフォルトの SDM テンプレート

メトロ IP アクセス イメージを稼動しているスイッチのデフォルトのテンプレートがデフォルト テンプレートです。

メトロ ベース イメージまたはメトロ アクセス イメージを稼動しているスイッチ上でサポートされるデフォルト（だけ）テンプレートは、レイヤ 2 テンプレートです。

SDM テンプレートの設定時の注意事項

SDM テンプレートを選択して設定するときは、次の注意事項に従ってください。

- この設定を有効にするには、スイッチをリロードする必要があります。
- レイヤ 2 機能に対してだけスイッチを使用する場合は、レイヤ 2 テンプレートを選択します。
- スイッチでのルーティングをイネーブルにしない場合は、デフォルト テンプレートを使用しないでください。**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用すると、他の機能がルーティング テンプレート内のユニキャスト ルーティングに割り当てられたメモリを使用するのを防ぐことができます。
- スイッチ上でルーティングをイネーブルにする予定の場合は、デフォルト テンプレートを使用してください。スイッチでルーティングがイネーブルのときにデフォルト テンプレートを使用しないと、ルーティングはソフトウェアにより実行されるため、CPU は過負荷となり、ルーティング パフォーマンスは大幅に低下します。
- 最初にデュアル IPv4/IPv6 テンプレートを選択しないで IPv6 機能を設定しようとすると、警告メッセージが生成されます。
- デュアル スタック テンプレートを使用すると、リソースごとに使用可能な TCAM 容量が少なくなるため、IPv4 トラフィックだけを転送する場合は、このテンプレートを使用しないでください。

SDM テンプレートの設定

SDM テンプレートを使用して、メトロ IP アクセス イメージが稼動するスイッチでテンプレートを選択するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer** {**default** | **dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} | **layer-2**}	スイッチで使用する SDM テンプレートを指定します。 キーワードの意味は次のとおりです。 • **default :** すべての機能を均衡化します。 • **dual-ipv4-and-ipv6** : IPv4 と IPv6 ルーティングを両方サポートするテンプレートを選択します。 – **default** : IPv4/IPv6 のレイヤ 2 およびレイヤ 3 機能を均衡化します。 – **routing** : IPv4 ポリシーベース ルーティングを含む IPv4 および IPv6 ルーティングの使用率を最大限にします。 – **vlan** : IPv4 と IPv6 の VLAN の使用率を最大限にします。 • **layer-2** : レイヤ 2 機能をサポートし、スイッチ上でのルーティングをサポートしません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**reload**	オペレーティング システムをリロードします。

システムの再起動後、**show sdm prefer** 特権 EXEC コマンドを使用して、新しいテンプレート設定を確認できます。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** により、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

次は、テンプレートをレイヤ 2 テンプレートに変更し、スイッチをリロードしなかった場合の出力表示の一例です。

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

  number of unicast mac addresses:                  5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    9K
    number of directly-connected IPv4 hosts:        5K
    number of indirect IPv4 routes:                 4K
  number of IPv4 policy based routing aces:         0.5K
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
On next reload, template will be "layer-2" template.
```

デフォルトのテンプレートに戻すには、**no sdm prefer** グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチにレイヤ 2 テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer layer-2
Switch(config)# end
Switch# reload
Proceed with reload? [confirm]
```

SDM テンプレートの表示

パラメータを指定せずに **show sdm prefer** 特権 EXEC コマンドを使用すると、アクティブ テンプレートが表示されます。**show sdm prefer** [**default** | **dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} | **layer-2**] 特権 EXEC コマンドを使用して、指定されたテンプレートでサポートされるリソース数を表示します。

次の例では、使用中のテンプレートを表示する **show sdm prefer** コマンドの出力例を示します。

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

  number of unicast mac addresses:                  5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    9K
    number of directly-connected IPv4 hosts:        5K
    number of indirect IPv4 routes:                 4K
  number of IPv4 policy based routing aces:         0.5K
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
```

次に、**show sdm prefer layer-2** コマンドの出力例を示します。

```
Switch# show sdm prefer layer-2
"layer-2" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  8K
  number of IPv4 IGMP groups:                       1K
  number of IPv4 multicast routes:                  0
  number of IPv4 unicast routes:                    0
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
```

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

```
Switch# show sdm prefer dual-ipv4-and-ipv6 routing
"desktop IPv4 and IPv6 routing" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  1.5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    2.75K
    number of directly-connected IPv4 hosts:        1.5K
    number of indirect IPv4 routes:                 1.25K
  number of IPv6 multicast groups:                  1.125k
  number of directly-connected IPv6 addresses:      1.5K
  number of indirect IPv6 unicast routes:           1.25K
  number of IPv4 policy based routing aces:         0.25K
  number of IPv4/MAC qos aces:                      0.75K
  number of IPv4/MAC security aces:                 0.5K
  number of IPv6 policy based routing aces:         0.25K
  number of IPv6 qos aces:                          0.5K
  number of IPv6 security aces:                     0.5K
```

CHAPTER 8

スイッチベースの認証の設定

この章では、Cisco ME 3400E スイッチでスイッチベースの認証を設定する方法について説明します。

- 「スイッチへの不正アクセスの防止」（P.8-1）
- 「特権 EXEC コマンドへのアクセスの保護」（P.8-2）
- 「TACACS+ によるスイッチ アクセスの制御」（P.8-10）
- 「RADIUS によるスイッチ アクセスの制御」（P.8-17）
- 「Kerberos によるスイッチ アクセスの制御」（P.8-32）
- 「スイッチのローカル認証および許可の設定」（P.8-36）
- 「Secure Shell のためのスイッチの設定」（P.8-37）
- 「SCP のためのスイッチの設定」（P.8-42）

スイッチへの不正アクセスの防止

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

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

- 最低限のセキュリティとして、各スイッチ ポートでパスワードおよび権限を設定します。このパスワードは、スイッチでローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。詳細については、「特権 EXEC コマンドへのアクセスの保護」（P.8-2）を参照してください。
- 追加のセキュリティ レイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベル（対応する権利および権限付き）を割り当てることもできます。詳細については、「ユーザ名とパスワードのペアの設定」（P.8-7）を参照してください。
- ユーザ名とパスワードのペアを使用する際に、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティ サーバ上のデータベースに保存できます。これにより、複数のネットワーク デバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。詳細については、「TACACS+ によるスイッチ アクセスの制御」（P.8-10）を参照してください。

特権 EXEC コマンドへのアクセスの保護

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

（注）　ここで説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference*』*Release 12.2* を参照してください。

- 「デフォルトのパスワードおよび権限レベル設定」（P.8-2）
- 「スタティック イネーブル パスワードの設定または変更」（P.8-3）
- 「暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護」（P.8-3）
- 「パスワード回復のディセーブル化」（P.8-5）
- 「端末回線に対する Telnet パスワードの設定」（P.8-6）
- 「ユーザ名とパスワードのペアの設定」（P.8-7）
- 「複数の権限レベルの設定」（P.8-7）

デフォルトのパスワードおよび権限レベル設定

表 8-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 8-1　デフォルトのパスワードおよび権限レベル

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

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。スタティック イネーブル パスワードを設定または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** *password*	特権 EXEC モードのアクセス用に新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトでは、パスワードは定義されていません。 *password* には、1 ～ 25 文字の英数字の文字列を指定します。文字列は数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符（?）は、パスワードを作成する場合に、疑問符の前にキーの組み合せ Ctrl+v キーを押せば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。 **abc** を入力します。 **Ctrl+v** キーを押します。 **?123** を入力します。 システムからイネーブル パスワードを入力するよう求められた場合、疑問符の前に Ctrl+v キーを押す必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。 イネーブル パスワードは暗号化されず、スイッチのコンフィギュレーション ファイル内では読み取ることができる状態です。

パスワードを削除するには、**no enable password** グローバル コンフィギュレーション コマンドを使用します。

次に、イネーブル パスワードを *l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
Switch(config)# enable password l1u2c3k4y5
```

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

追加のセキュリティ レイヤを、特にネットワークを越えるパスワードや Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存されているパスワードに対して設定する場合には、**enable password** または **enable secret** の各グローバル コンフィギュレーション コマンドを使用できます。両コマンドはともに同じ働きをします。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード（デフォルト設定）または特定の権限レベルにアクセスするには、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムを使用しているので、**enable secret** コマンドを使用することを推奨します。

enable secret コマンドは **enable password** コマンドに優先します。2 つのコマンドが同時に有効になることはありません。

イネーブルおよびイネーブル シークレット パスワードに暗号化を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted*-password} または **enable secret** [**level** *level*] {*password* | *encryption-type encrypted*-password}	特権 EXEC モードのアクセス用に新しいパスワードを定義するか、既存のパスワードを変更します。 または シークレット パスワードを定義し、非可逆暗号方式を使用して保存します。 • （任意）*level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です（特権 EXEC モード権限）。 • *password* には、1 ～ 25 文字の英数字の文字列を指定します。文字列は数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。 • （任意）*encryption-type* には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか指定できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチ コンフィギュレーションからコピーしたものです。 **（注）** 暗号化タイプを指定してクリア テキスト パスワードを入力した場合は、再度特権 EXEC モードを開始することはできません。暗号化されたパスワードが不明になった場合、どのような方法でも回復できません。
ステップ 3	**service password-encryption**	（任意）パスワードを定義するとき、またはコンフィギュレーションを保存するときに、パスワードを暗号化します。 暗号化によって、コンフィギュレーション ファイルのパスワードが読み取り不能になります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

イネーブル パスワードおよびイネーブル シークレット パスワードの両方が定義されている場合、ユーザはイネーブル シークレット パスワードを入力する必要があります。

特定の権限レベルのパスワードを定義するには、キーワード **level** を使用します。レベルを指定してパスワードを設定したら、そのレベルでアクセスする必要のあるユーザだけにそのパスワードを付与してください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、**privilege level** グローバル コンフィギュレーション コマンドを使用します。詳細については、「複数の権限レベルの設定」（P.8-7）を参照してください。

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

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

権限レベル 2 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

パスワード回復のディセーブル化

デフォルトでは、スイッチに物理アクセスするすべてのエンド ユーザは、スイッチの電源投入時にブート プロセスを中断して新しいパスワードを入力することで、失われたパスワードを回復できます。

パスワード回復ディセーブル機能では、この機能の一部をディセーブルにすることにより、スイッチ パスワードへのアクセスを防止します。この機能がイネーブルな場合、エンド ユーザはシステムをデフォルト設定に戻すことに同意するだけで、ブート プロセスを中断することができます。パスワード回復をディセーブル化しても、ブート プロセスを中断してパスワードを変更できますが、コンフィギュレーション ファイル（config.txt）および VLAN（仮想 LAN）データベース ファイル（vlan.dat）は削除されます。

（注）　パスワード回復をディセーブルにする場合は、エンドユーザがブート プロセスを中断してシステムをデフォルト値に戻す場合に備えて、セキュア サーバ上にコンフィギュレーション ファイルのバックアップ コピーを保管しておいてください。スイッチ上にコンフィギュレーション ファイルのバックアップ コピーを保管しないでください。また、セキュア サーバ上に VLAN データベース ファイルのバックアップ コピーも保管しておくことを推奨します。スイッチがシステムのデフォルト設定に戻ると、XMODEM プロトコルを使用して、保存したファイルをダウンロードできます。詳細については、「パスワードを忘れた場合の回復」（P.46-3）を参照してください。

パスワード回復をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no service password-recovery**	パスワード回復をディセーブルにします。 この設定は、フラッシュ メモリのブート ローダがアクセスできる領域および Cisco IOS イメージに保存されます。ただし、ファイル システムの領域ではないのでユーザはアクセスできません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show version**	コマンド出力の最後の数行を調べて設定を確認します。

パスワード回復を再びイネーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

（注）　**boot manual** グローバル コンフィギュレーション コマンドを使用して、スイッチを手動で起動するように設定している場合は、パスワード回復をディセーブルにできません。このコマンドにより、スイッチの電源再投入後に、ブート ローダ プロンプト（*switch:*）が表示されます。

端末回線に対する Telnet パスワードの設定

初めてスイッチに電源を投入すると、自動セットアップ プログラムが起動して IP 情報を割り当て、引き続き使用するためのデフォルト設定を作成します。セットアップ プログラムは、パスワードによる Telnet アクセス用にスイッチを設定するように求めてきます。このとき、セットアップ プログラムを使用してパスワードを設定しなかった場合は、CLI（コマンドライン インターフェイス）を使用して設定できます。

スイッチを Telnet アクセス用に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		エミュレーション ソフトウェアをインストールした PC またはワークステーションと、スイッチのコンソール ポートを接続します。 コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなしです。コマンドライン プロンプトを表示させるため、Return キーを数回押さなければならない場合があります。
ステップ 2	**enable password** *password*	特権 EXEC モードを開始します。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**line vty 0 15**	Telnet セッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。 コマンド対応スイッチでは、最大 16 のセッションが可能です。0 および 15 を指定することは、使用できる 16 個の Telnet セッションを全部設定することを意味します。
ステップ 5	**password** *password*	1 つまたは複数の回線の Telnet パスワードを入力します。 *password* には、1 ～ 25 文字の英数字の文字列を指定します。文字列は数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。 コマンド **line vty 0 15** の下にパスワードが表示されます。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

パスワードを削除するには、**no password** グローバル コンフィギュレーション コマンドを使用します。

Telnet パスワードを *let45me67in89* に設定する例を示します。

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

ユーザ名とパスワードのペアの設定

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

ユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。この認証システムは、ログイン ユーザ名とパスワードを要求します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	各ユーザのユーザ名、権限レベル、パスワードを入力します。 • *name* には、ユーザ ID を 1 ワードで指定します。スペースや引用符は使用できません。 • （任意）*level* には、アクセス後ユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では、ユーザ EXEC モードでのアクセスとなります。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* には、暗号化されていないパスワードがあとに続く場合は 0 を指定します。暗号化されたパスワードがあとに続く場合は 7 を指定します。 • *password* には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
ステップ 3	**line console 0** または **line vty 0 15**	ライン コンフィギュレーション モードを開始し、コンソール ポート（回線 0）または VTY 回線（回線 0 ～ 15）を設定します。
ステップ 4	**login local**	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定ユーザのユーザ名認証をディセーブルにするには、**no username** *name* グローバル コンフィギュレーション コマンドを使用します。パスワード チェックをディセーブルにし、パスワードなしでの接続を可能にするには、**no login** ライン コンフィギュレーション コマンドを使用します。

複数の権限レベルの設定

Cisco IOS ソフトウェアは、デフォルトで、ユーザ EXEC と特権 EXEC という 2 種類のパスワード セキュリティ モードを備えています。各モードについて、コマンドの階層レベルを最大 16 まで設定できます。複数のパスワードを設定することにより、さまざまなユーザ グループに対して特定のコマンドへのアクセスを許可することができます。

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

ここでは、次の設定情報について説明します。

- 「コマンドの権限レベルの設定」（P.8-8）
- 「回線に対するデフォルトの権限レベルの変更」（P.8-9）
- 「権限レベルへのログインおよび終了」（P.8-9）

コマンドの権限レベルの設定

コマンド モードの権限レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**privilege** *mode* **level** *level command*	コマンドの権限レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合 は **configure** を、EXEC モードの場合は **exec** を、インターフェイス コンフィギュレーション モードの場合は **interface** を、ライン コンフィギュレーション モードの場合は **line** を、それぞれ入力します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限用です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。 • *command* には、アクセスを制限したいコマンドを指定します。
ステップ 3	**enable password level** *level password*	権限レベルのイネーブル パスワードを指定します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限用です。 • *password* には、1 ～ 25 文字の英数字の文字列を指定します。文字列は数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	設定を確認します。 show running-config コマンドはパスワードとアクセス レベルの設定を表示します。show privilege コマンドは、権限レベルの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

configure コマンドを権限レベル 14 に設定し、レベル 14 コマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

回線に対するデフォルトの権限レベルの変更

回線に対するデフォルトの権限レベルを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line vty** *line*	アクセスを制限する仮想端末回線を選択します。
ステップ 3	**privilege level** *level*	回線のデフォルト権限レベルを変更します。 *level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限用です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	設定を確認します。 show running-config コマンドはパスワードとアクセス レベルの設定を表示します。show privilege コマンドは、権限レベルの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

権限レベルへのログインおよび終了

特定の権限レベルにログインし、特定の権限レベルを終了するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**enable** *level*	特定の権限レベルにログインします。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable** *level*	特定の権限レベルを終了します。 *level* に指定できる範囲は 0 ～ 15 です。

TACACS+ によるスイッチ アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus（TACACS+）をイネーブルにして設定する方法について説明します。TACACS+ は、詳細なアカウンティング情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。TACACS+ は、Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）機能が拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用します。

（注）　ここで説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference*』*Release 12.2* を参照してください。

ここでは、次の設定情報について説明します。

- 「TACACS+ の概要」（P.8-10）
- 「TACACS+ の動作」（P.8-12）
- 「TACACS+ の設定」（P.8-12）
- 「TACACS+ 設定の表示」（P.8-17）

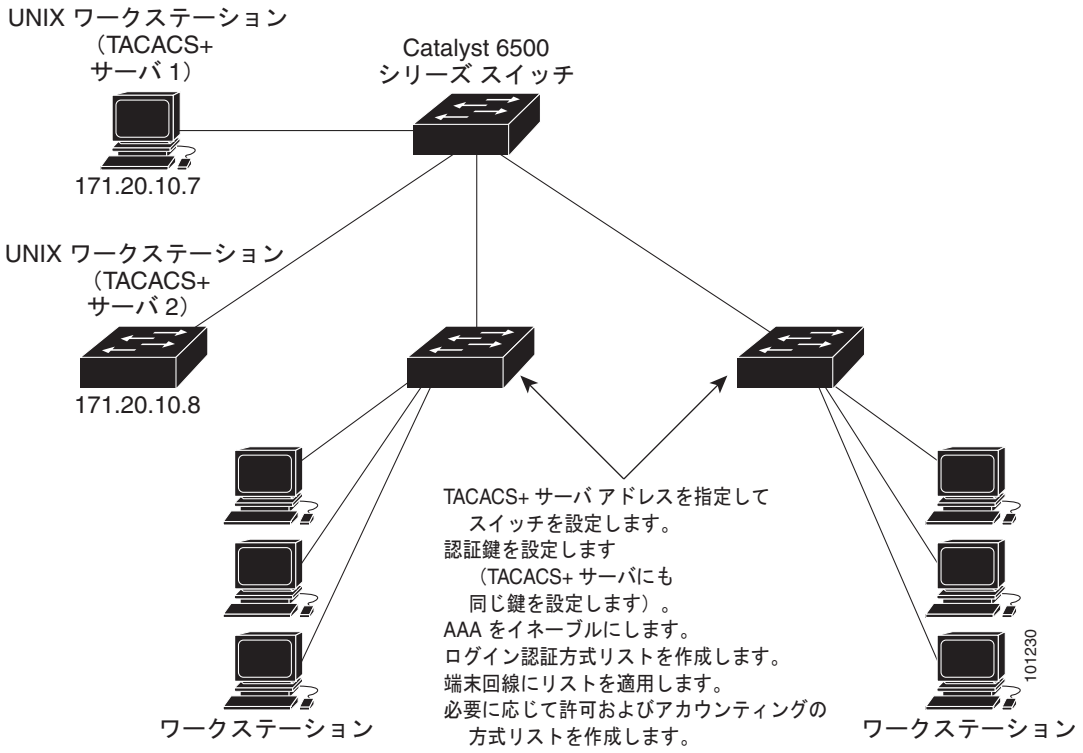
TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼動する TACACS+ デーモンのデータベースで管理されます。スイッチに TACACS+ 機能を設定するには、TACACS+ サーバにアクセスして設定する必要があります。

TACACS+ は、個別のモジュール型認証、認可、およびアカウンティング機能を備えています。TACACS+ により、単一のアクセス制御サーバ（TACACS+ デーモン）が各サービス（認証、認可、アカウンティング）を個別に提供できます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで利用できる他のサービスを使用することができます。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他のシスコ製ルータやアクセス サーバとともにネットワーク アクセス サーバにすることができます。ネットワーク アクセス サーバは、単一のユーザ、ネットワークまたはサブネットワーク、および相互接続されたネットワークとの接続を実現します（図 8-1 を参照）。

図 8-1　一般的な TACACS+ ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の総合的な制御を行います。

  認証機能では、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力されたあと、自宅の住所、母親の旧姓、サービス タイプ、社会保険番号などのいくつかの質問をすることによりユーザを試す）。TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：オートコマンド、アクセス制御、セッション期間、プロトコル サポートの設定といった、ユーザ セッション内でのユーザ機能についてきめ細かい制御を行います。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。

- アカウンティング：課金、監査、レポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況を追跡したり、ユーザ課金用の情報を提供したりすることができます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP [ポイントツーポイント プロトコル] など）、パケット数、およびバイト数が記録されます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモンとの間の認証を行い、スイッチと TACACS+ デーモンとの間のプロトコル交換をすべて暗号化することにより機密保持を実現します。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼動するシステムが必要です。

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立すると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これがユーザに表示されます。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワード プロンプトを取得します。スイッチがパスワード プロンプトを表示し、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

   TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合せを入力するよう指示しますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を受信します。

   - ACCEPT：ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
   - REJECT：ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するよう求められます。
   - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
   - CONTINUE：ユーザは、さらに認証情報の入力を求められます。

   認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザはまず、TACACS+ 認証を正常に終了しなければ TACACS+ 許可に進めません。

3. TACACS+ 許可が必要な場合は、再度 TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答には、そのユーザの EXEC または NETWORK セッション宛てのアトリビュートの形式のデータ、およびユーザがアクセスできるサービスが含まれます。

   - Telnet、Secure Shell（SSH; セキュア シェル）、rlogin、または特権 EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなど）

TACACS+ の設定

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。少なくとも、TACACS+ デーモンを保持するホスト（複数可）を特定し、TACACS+ 認証の方式リストを定義する必要があります。任意で TACACS+ 許可およびアカウンティングの方式リストを定義することもできます。方式リストは、ユーザの認証、認可、およびアカウントを維持するための順序と方式を定義します。方式リストを使用すると、使用するセキュリティ プロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、認可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストを使い果たすまで続きます。

aaa authorization console グローバル コンフィギュレーション コマンドによって、AAA および TACACS+ をコンソール ポート上で動作させることが可能です。

このコマンドについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a00800ca6d8.html#wp1019867

ここでは、次の設定情報について説明します。

- 「TACACS+ のデフォルト設定」（P.8-13）
- 「TACACS+ サーバ ホストの特定と認証鍵の設定」（P.8-13）
- 「TACACS+ ログイン認証の設定」（P.8-14）
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」（P.8-16）
- 「TACACS+ アカウンティングの開始」（P.8-16）

TACACS+ のデフォルト設定

TACACS+ と AAA は、デフォルトでディセーブルに設定されています。

セキュリティの失効を防止するために、ネットワーク管理アプリケーションを使用して TACACS+ を設定することは不可能です。TACACS+ をイネーブルに設定すると、CLI を使用してスイッチにアクセスするユーザを認証します。

（注）　TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ サーバ ホストの特定と認証鍵の設定

認証用に 1 つのサーバを使用することも、既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するよう設定することもできます。設定済みサーバ ホストのサブセットを選択してサーバをグループ化し、特定のサービスに使用することが可能です。サーバ グループは、グローバル サーバホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストを含んでいます。

IP ホストまたは TACACS+ サーバを保持するホストを特定し、任意で暗号鍵を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	TACACS+ サーバを保持する IP ホストまたはホストを識別します。このコマンドを複数回入力すると、優先ホストのリストが作成されます。ソフトウェアは、指定された順序でホストを検索します。 • *hostname* には、ホストの名前または IP アドレスを指定します。 • （任意）**port** *integer* には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は 1 ～ 65535 です。 • （任意）**timeout** *integer* には、スイッチがデーモンからの応答を待つ時間を秒数で指定します。これを過ぎるとスイッチは時間切れとなりエラーを宣言します。デフォルト値は 5 秒です。指定できる範囲は 1 ～ 1000 秒です。 • （任意）**key** *string* には、スイッチと TACACS+ デーモンとの間のすべてのトラフィックを暗号化および暗号解除するための暗号鍵を指定します。暗号化が成功するには TACACS+ デーモンに同じ鍵を設定する必要があります。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 4	**aaa group server tacacs+** *group-name*	（任意）グループ名で AAA サーバ グループを定義します。 このコマンドによって、スイッチはサーバ グループ サブコンフィギュレーション モードになります。
ステップ 5	**server** *ip-address*	（任意）特定の TACACS+ サーバを定義済みサーバ グループに対応付けます。AAA サーバ グループの各 TACACS+ サーバに対してこのステップを繰り返します。 グループの各サーバは、ステップ 2 で定義されている必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show tacacs**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host** *hostname* グローバル コンフィギュレーション コマンドを使用します。設定リストからサーバ グループを削除するには、**no aaa group server tacacs+** *group-name* グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、**no server ip-address** サーバ グループ サブコンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、さまざまなポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストが明示的に定義されたポートを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試すまで続きます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • *login authentication* コマンドに名前付きリストが**指定されていない**場合に使用されるデフォルトのリストを作成するには、キーワード **default** の後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、**enable** *password* グローバル コンフィギュレーション コマンドを使用して、イネーブル パスワードをあらかじめ定義しておく必要があります。 • **group tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、TACACS+ サーバをあらかじめ設定しておく必要があります。詳細については、「TACACS+ サーバ ホストの特定と認証鍵の設定」（P.8-13）を参照してください。 • **line**：回線パスワードを認証に使用します。この認証方式を使用するには、回線パスワードをあらかじめ設定しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **local-case**：大文字と小文字を区別するローカル ユーザ名データベースを認証に使用します。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用して、データベースにユーザ名情報を入力する必要があります。 • **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインの TACACS+ 認証をディセーブルにするかデフォルト値に戻す場合は、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 許可は、ユーザが利用できるサービスを制限します。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

aaa authorization グローバル コンフィギュレーション コマンドにキーワード **tacacs+** を付けて使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec tacacs+ local コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

（注） 許可が設定されている場合でも、CLI を使用してログインする認証済みユーザには、許可が省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network tacacs+**	ネットワーク関連のすべてのサービス要求に対するユーザ TACACS+ 許可をスイッチに設定します。
ステップ 3	**aaa authorization exec tacacs+**	特権 EXEC アクセスの有無を、ユーザ TACACS+ 許可によって判別するようにスイッチを設定します。 キーワード **exec** を指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返されることがあります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ アカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスするサービスと、ユーザが消費するネットワーク リソースを追跡します。AAA アカウンティングがイネーブルに設定されていると、スイッチは、アカウンティング レコードの形式でユーザの活動状況を TACACS+ セキュリティ サーバにレポートします。

各アカウンティング レコードには、アカウンティングの AV のペアが含まれ、セキュリティ サーバ上に保存されます。このデータを分析し、ネットワーク管理、クライアントへの課金、または監査に使用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa accounting network start-stop tacacs+**	ネットワーク関連のすべてのサービス要求に対する TACACS+ アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop tacacs+**	TACACS+ アカウンティングにより、特権 EXEC プロセスの開始時に記録開始アカウンティング通知、終了時に記録停止通知を送信するように設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、**show tacacs** 特権 EXEC コマンドを使用します。

RADIUS によるスイッチ アクセスの制御

ここでは、RADIUS（Remote Authentication Dial-In User Service）をイネーブルにして設定する方法について説明します。RADIUS は、詳細なアカウンティング情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。RADIUS は AAA を介して機能します。RADIUS をイネーブルにするには AAA コマンドを使用します。

（注）　ここで説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference*』*Release 12.2* を参照してください。

ここでは、次の設定情報について説明します。

- 「RADIUS の概要」（P.8-18）
- 「RADIUS の動作」（P.8-19）
- 「RADIUS の設定」（P.8-20）
- 「RADIUS 設定の表示」（P.8-32）

RADIUS の概要

RADIUS は分散型クライアント/サーバ システムで、不正なアクセスからネットワークを保護します。RADIUS クライアントは、サポートされているシスコ製ルータおよびスイッチ上で稼動し、中央 RADUIS サーバに認証要求を送信します。中央 RADUIS サーバには、すべてのユーザの認証およびネットワーク サービス アクセス情報が格納されています。RADUIS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft などのソフトウェア製造元の RADIUS サーバ ソフトウェアが稼動するマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。

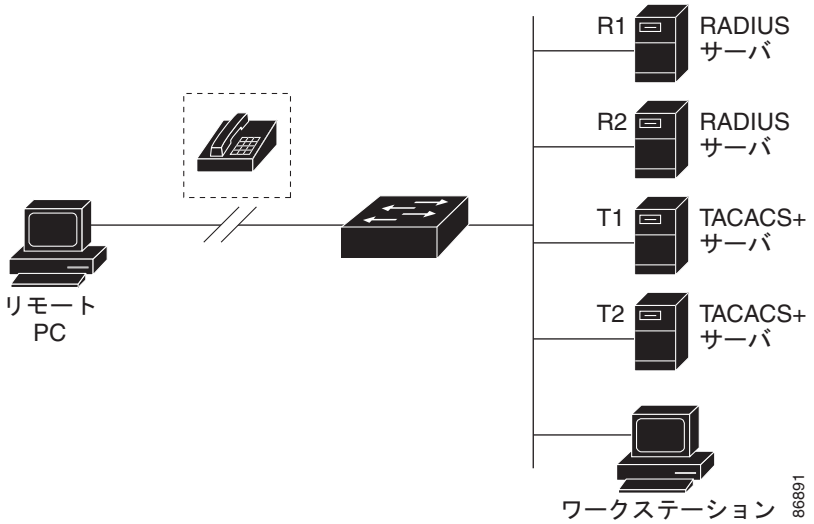
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数のベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADUIS サーバを通じて認証されます。RADUIS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、*スマート カード*アクセス制御システムを使用するアクセス環境。あるケースでは、RADIUS を Enigma のセキュリティ カードと併用してユーザを確認し、ネットワーク リソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアントを含むシスコ製スイッチをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。図 8-2（P.8-19）を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1X などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、第 9 章「IEEE 802.1x ポートベースの認証の設定」を参照してください。
- リソース アカウンティングが必要なネットワーク。RADUIS 認証または許可とは別に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス制御およびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび請求のニーズを満たすこともできます。

RADIUS は、ネットワーク セキュリティが次のような状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP; NetBIOS フレーム制御プロトコル）、NetWare Asynchronous Services Interface（NASI; NetWare 非同期サポート インターフェイス）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製デバイスへの認証には使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

図 8-2　RADIUS から TACACS+ サービスへの移行



RADIUS の動作

RADIUS サーバによってアクセス制御されているスイッチに、ユーザがログインして認証を試みると、次のイベントが発生します。

1. ユーザ名とパスワードの入力を求めるプロンプトが表示されます。
2. ユーザ名と暗号化されたパスワードが、ネットワークを介して RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   a. ACCEPT：ユーザは認証されます。
   b. REJECT：ユーザは認証されず、ユーザ名とパスワードの再入力を求めるプロンプトが表示されるか、アクセスが拒否されます。
   c. CHALLENGE：ユーザからの追加データが要求されます。
   d. CHALLENGE PASSWORD：ユーザは新しいパスワードを選択するよう要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用される追加データがバンドルされています。RADIUS 許可がイネーブルになっている場合、ユーザはまず、RADIUS 認証に成功しなければ RADIUS 許可に進めません。ACCEPT または REJECT パケットの追加データには、次の項目が含まれています。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなど）

RADIUS の設定

ここでは、RADIUS をサポートするようにスイッチを設定する方法について説明します。少なくとも、RADIUS サーバ ソフトウェアが稼動するホスト（複数可）を特定し、RADIUS 認証の方式リストを定義する必要があります。任意で RADIUS 許可およびアカウンティングの方式リストを定義することもできます。

方式リストは、ユーザの認証、認可、およびアカウントを維持するための順序と方式を定義します。方式リストを使用すると、使用するセキュリティ プロトコル（TACACS+ やローカル ユーザ名検索など）を 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、認可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストを使い果たすまで続きます。

スイッチに RADIUS 機能を設定するには、RADIUS サーバにアクセスして設定する必要があります。

ここでは、次の設定情報について説明します。

- 「RADIUS のデフォルト設定」（P.8-20）
- 「RADIUS サーバ ホストの特定」（P.8-20）（必須）
- 「RADIUS ログイン認証の設定」（P.8-23）（必須）
- 「AAA サーバ グループの定義」（P.8-25）（任意）
- 「ユーザ イネーブル アクセスおよびネットワーク サービス用の RADIUS 許可の設定」（P.8-27）（任意）
- 「RADIUS アカウンティングの開始」（P.8-28）（任意）
- 「すべての RADIUS サーバに対する設定」（P.8-29）（任意）
- 「ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法」（P.8-29）（任意）
- 「ベンダー固有の RADIUS サーバ通信用にスイッチを設定する方法」（P.8-30）（任意）
- 「RADIUS ロード バランシングの設定」（P.8-31）（任意）

RADIUS のデフォルト設定

RADIUS と AAA は、デフォルトでディセーブルに設定されています。

セキュリティの失効を防止するために、ネットワーク管理アプリケーション使用して RADIUS を設定することは不可能です。RADIUS をイネーブルに設定すると、CLI を使用して、スイッチにアクセスするユーザを認証します。

RADIUS サーバ ホストの特定

スイッチと RADIUS サーバ間の通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証宛先ポート
- アカウンティング宛先ポート
- キー ストリング
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と各 UDP ポート番号、あるいは IP アドレスと各 UDP ポート番号で識別されます。IP アドレスと UDP ポート番号の組み合せによって一意の識別子が作成され、特定の AAA サービスを提供する RADIUS ホストとしてさまざまなポートを個別に定義できます。この一意の識別子によって、サーバ上の複数の UDP ポートに同じ IP アドレスで RADIUS 要求を送信できるようになります。

同一の RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス（たとえば、アカウンティング）を設定している場合、あとから設定されたホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。この例では、最初のホスト エントリがアカウンティング サービスを提供できない場合は、スイッチは同じデバイス上に設定された 2 番めのホスト エントリでアカウンティング サービスを試行します（RADIUS のホスト エントリは、設定された順序で試行されます）。

RADIUS サーバおよびスイッチは、共有シークレット テキスト ストリングを使用してパスワードを暗号化し、応答を交換します。AAA セキュリティ コマンドを使用するように RADIUS を設定するには、RADIUS サーバ デーモンが稼動するホストと、そのスイッチを共有するシークレット テキスト（キー）ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号化鍵の値は、すべての RADIUS サーバに対してグローバルにサーバ単位で設定することも、グローバルな設定とサーバ単位の設定を組み合せることもできます。この設定を、スイッチと通信するすべての RADIUS サーバに対してグローバルに適用するには、3 つの特別なグローバル コンフィギュレーション コマンド、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** を使用します。特定の RADIUS サーバにこれらの値を適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。

認証用に既存のサーバ ホストをグループ化するために、AAA サーバ グループを使用するようスイッチを設定できます。詳細については、「AAA サーバ グループの定義」（P.8-25）を参照してください。

サーバ単位での RADIUS サーバ通信を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA 認証をイネーブルにします。

	コマンド	目的
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、RADIUS サーバが応答するのを待ってスイッチが再送信するまでのインターバルを指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドの設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しないか、応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信の値を設定しない場合は、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、スイッチと RADIUS サーバ上で稼動する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。鍵は、必ず **radius-server host** コマンドの最後の項目として設定します。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。 1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、必要な回数だけこのコマンドを入力し、それぞれの UDP ポート番号が必ず異なるようにしてください。スイッチ ソフトウェアは、指定された順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信回数、および暗号化鍵の値を設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、**no radius-server host** *hostname* | *ip-address* グローバル コンフィギュレーション コマンドを使用します。

次に、ある RADIUS サーバを認証用に、別の RADIUS サーバをアカウンティング用に設定する例を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次の例は、RADIUS サーバとして *host1* を設定し、認証およびアカウンティングの両方にデフォルト ポートを使用する方法を示します。

```
Switch(config)# radius-server host host1
```

（注）　さらに、RADIUS サーバでいくつかの設定を行う必要があります。この設定とは、スイッチの IP アドレス、およびサーバとスイッチで共有するキー ストリングです。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、さまざまなポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストが明示的に定義されたポートを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試すまで続きます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • *login authentication* コマンドに名前付きリストが**指定されていない**場合に使用されるデフォルトのリストを作成するには、キーワード **default** の後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 – **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、**enable** *password* グローバル コンフィギュレーション コマンドを使用して、イネーブル パスワードをあらかじめ定義しておく必要があります。 – **group radius**：RADIUS 認証を使用します。この認証方式を使用するには、RADIUS サーバをあらかじめ設定しておく必要があります。詳細については、「RADIUS サーバ ホストの特定」（P.8-20）を参照してください。 – **line**：回線パスワードを認証に使用します。この認証方式を使用するには、回線パスワードをあらかじめ設定しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 – **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用します。 – **local-case**：大文字と小文字を区別するローカル ユーザ名データベースを認証に使用します。**username** *password* グローバル コンフィギュレーション コマンドを使用して、データベースにユーザ名情報を入力する必要があります。 – **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインの RADIUS 認証をディセーブルにするかデフォルト値に戻す場合は、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

AAA サーバ グループの定義

認証用に既存のサーバ ホストをグループ化するために、AAA サーバ グループを使用するようスイッチを設定できます。設定済みサーバ ホストのサブセットを選択し、特定のサービスに使用できます。サーバ グループには、グローバル サーバホスト リストを使用します。このリストは、選択したサーバ ホストの IP アドレスのリストです。

サーバ グループには、各エントリが一意の識別子（IP アドレスと UDP ポート番号の組み合せ）を持っていれば、同じサーバに対して複数のホスト エントリを組み込むことができます。また、特定の AAA サービスを提供する RADIUS ホストとして、さまざまなポートを個別に定義できます。同一の RADIUS サーバ上の 2 つの異なるホスト エントリを同じサービス（たとえば、アカウンティング）を設定すると、設定された 2 番めのホスト エントリは、最初のエントリの代替バックアップとして機能します。

定義済みのグループ サーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。IP アドレスでサーバを特定したり、任意の **auth-port** および **acct-port** の各キーワードを使用して複数のホスト インスタンスまたはエントリを識別したりできます。

AAA サーバ グループを定義して特定の RADIUS サーバに対応付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、RADIUS サーバが応答するのを待ってスイッチが再送信するまでのインターバルを指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドの設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しないか、応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信の値を設定しない場合は、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、スイッチと RADIUS サーバ上で稼動する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。鍵は、必ず **radius-server host** コマンドの最後の項目として設定します。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。 1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、必要な回数だけこのコマンドを入力し、それぞれの UDP ポート番号が必ず異なるようにしてください。スイッチ ソフトウェアは、指定された順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信回数、および暗号化鍵の値を設定します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa group server radius** *group-name*	グループ名で AAA サーバ グループを定義します。 このコマンドによって、スイッチはサーバ グループ コンフィギュレーション モードになります。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義済みサーバ グループに対応付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義されている必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「RADIUS ログイン認証の設定」（P.8-23）を参照してください。

特定の RADIUS サーバを削除するには、**no radius-server host** *hostname* | *ip-address* グローバル コンフィギュレーション コマンドを使用します。コンフィギュレーション リストからサーバ グループを削除するには、**no aaa group server radius** *group-name* グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、**no server** *ip-address* サーバ グループコンフィギュレーション コマンドを使用します。

次の例では、2 つの異なる RADIUS グループ サーバ（*group1* と *group2*）を認識するようにスイッチを設定しています。group1 では、同一の RADIUS サーバ上の 2 つの異なるホスト エントリに同じサービスを設定しています。2 番めのホスト エントリは、最初のエントリの代替バックアップとして機能します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

ユーザ イネーブル アクセスおよびネットワーク サービス用の RADIUS 許可の設定

AAA 許可は、ユーザが利用できるサービスを制限します。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

aaa authorization グローバル コンフィギュレーション コマンドにキーワード **radius** を指定して使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、特権 EXEC アクセス許可に RADIUS を使用します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

（注）　許可が設定されている場合でも、CLI を使用してログインする認証済みユーザには、許可が省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network radius**	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。
ステップ 3	**aaa authorization exec radius**	特権 EXEC アクセスの有無を、ユーザ RADIUS 許可によって判別するようにスイッチを設定します。 キーワード **exec** を指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返されることがあります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

RADIUS アカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスするサービスと、ユーザが消費するネットワーク リソースを追跡します。AAA アカウンティングがイネーブルに設定されていると、スイッチは、アカウンティング レコードの形式でユーザの活動状況を RADIUS セキュリティ サーバに報告します。各アカウンティング レコードには、アカウンティングの AV のペアが含まれ、セキュリティ サーバ上に保存されます。このデータを分析し、ネットワーク管理、クライアントへの課金、または監査に使用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに関する RADIUS アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa accounting network start-stop radius**	ネットワーク関連のすべてのサービス要求に関する RADIUS アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop radius**	RADIUS アカウンティングにより、特権 EXEC プロセスの開始時に記録開始アカウンティング通知、特権 EXEC プロセスの終了時に記録停止通知を送信するように設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

すべての RADIUS サーバに対する設定

スイッチとすべての RADIUS サーバ間のグローバル通信コンフィギュレーションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server key** *string*	スイッチとすべての RADIUS サーバとの間で使用する、共有シークレット テキスト ストリングを指定します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。
ステップ 3	**radius-server retransmit** *retries*	スイッチが、サーバに各 RADIUS 要求を送信する回数を指定します。デフォルトは 3 で、指定できる範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout** *seconds*	スイッチが、RADIUS 要求に対する応答を待って要求を再送信するまでの秒数を指定します。デフォルトは 5 秒で、指定できる範囲は 1 ～ 1000 です。
ステップ 5	**radius-server deadtime** *minutes*	認証要求に応答しない RADIUS サーバをスキップする時間を指定します。これにより、要求がタイムアウトするまで待たずに、次の設定サーバを試行することができます。デフォルトは 0 で、指定できる範囲は 1 ～ 1440 分です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

再送信、タイムアウト、デッドタイムの設定をデフォルトに戻すには、これらのコマンドの **no** 形式を使用します。

ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法

Internet Engineering Task Force（IETF）ドラフト規格では、ベンダー固有のアトリビュート（アトリビュート 26）を使用して、スイッチと RADIUS サーバとの間のベンダー固有情報の通信方式を定めています。Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）を使用すると、ベンダーは、汎用に適さない独自の拡張アトリビュートをサポートできます。シスコの実装 RADIUS では、仕様で推奨されたフォーマットを使用して 1 つのベンダー固有オプションをサポートします。シスコのベンダー ID は 9 で、サポート対象のオプションにはベンダータイプ 1 が設定されており、*cisco-avpair* と名前が付けられています。この値は次のフォーマットの文字列です。

```
protocol : attribute sep value *
```

protocol は、特定のタイプの許可に対応するシスコ プロトコル アトリビュートの値です。*attribute* と *value* は、シスコ TACACS+ 仕様で定義されている適正な AV のペアです。*sep* は、必須アトリビュートの場合は「=」、オプションのアトリビュートの場合は「*」です。TACACS+ 許可で利用できるすべての機能は、RADIUS にも使用できます。

たとえば、次の AV ペアは、IP 許可時（PPP の IPCP アドレス割り当て時）に、シスコの *複数の名前付き IP アドレス プール*機能をアクティブにします。

```
cisco-avpair= "ip:addr-pool=first"
```

次の例は、スイッチからログインしているユーザに、特権 EXEC コマンドへの直接アクセスを可能にする方法を示します。

```
cisco-avpair= "shell:priv-lvl=15"
```

次の例は、RADIUS サーバ データベース内の許可 VLAN を指定する方法を示しています。

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

次の例は、この接続中に ASCII 形式の入力 ACL をインターフェイスに適用する方法を示しています。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

次の例は、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する方法を示しています。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

その他のベンダーにも、独自に一意のベンダー ID、オプション、および対応する VSA が割り当てられます。ベンダー ID と VSA の詳細については、RFC 2138 『Remote Authentication Dial-In User Service(RADIUS)』を参照してください。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server vsa send** [**accounting** | **authentication**]	スイッチが、RADIUS IETF アトリビュート 26 に定義されている VSA を認識して使用できるようにします。 • （任意）キーワード **accounting** を使用して、認識される VSA の集合をアカウンティング アトリビュートに限定します。 • （任意）キーワード **authentication** を使用して、認識される VSA の集合を認証アトリビュートに限定します。 キーワードなしでこのコマンドを入力すると、アカウンティングおよび認証の両方の VSA が使用されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RADIUS アトリビュートの完全リスト、または VSA 26 の詳細については、『*Cisco IOS Security Configuration Guide*』*Release 12.2* の付録「RADIUS Attributes」を参照してください。

ベンダー固有の RADIUS サーバ通信用にスイッチを設定する方法

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバとの間のベンダー固有情報の通信方式を規定していますが、一部のベンダーは、固有の方法で RADIUS アトリビュートを機能拡張しています。Cisco IOS ソフトウェアは、ベンダー固有仕様の RADIUS アトリビュートのサブセットをサポートします。

前述したように、RADIUS（ベンダー固有または IETF のドラフト準拠）を設定するには、RADIUS サーバ デーモンが稼動しているホスト、およびスイッチと共有するシークレット テキスト ストリングを指定する必要があります。RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

ベンダー固有の RADIUS サーバ ホスト、および共有シークレット テキスト ストリングを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **non-standard**	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、ベンダー固有の実装 RADIUS を使用していることを明確にします。
ステップ 3	**radius-server key** *string*	スイッチとベンダー固有の RADIUS サーバとの間で使用する、共有シークレット テキスト ストリングを指定します。スイッチおよび RADIUS サーバは、このテキスト ストリングを使用してパスワードを暗号化し、応答を交換します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号化鍵と一致する必要があります。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ベンダー固有の RADIUS ホストを削除するには、**no radius-server host** {*hostname* | *ip-address*} **non-standard** グローバル コンフィギュレーション コマンドを使用します。鍵を削除するには、**no radius-server key** グローバル コンフィギュレーション コマンドを使用します。

次に、ベンダー固有の RADIUS ホストを指定して、スイッチとサーバの間で *rad124* という秘密鍵を使用する例を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

RADIUS ロード バランシングの設定

この機能を使用すれば、アクセスおよび認証要求を、サーバ グループ内のすべての RADIUS サーバに均等に分散できます。詳細については、『Cisco IOS Security Configuration Guide』Release 12.2 の「RADIUS Server Load Balancing」の章を参照してください。

http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrdldbl.html

RADIUS 設定の表示

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

Kerberos によるスイッチ アクセスの制御

ここでは、Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。この機能を使用するには、スイッチ ソフトウェアの暗号化（暗号化をサポートする）バージョンをスイッチにインストールしている必要があります。この機能を使用するには、その許可を取得し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードする必要があります。詳細については、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「Kerberos の概要」（P.8-32）
- 「Kerberos の動作」（P.8-34）
- 「Kerberos の設定」（P.8-35）

Kerberos の設定例については、『*Cisco IOS Security Configuration Guide*』*Release 12.2* の「Security Server Protocols」の章にある「Kerberos Configuration Examples」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html#wp1001396

ここで説明するコマンドの構文および使用方法の詳細については、この URL にある『*Cisco IOS Security Command Reference*』*Release 12.2* の「Security Server Protocols」の章にある「Kerberos Commands」を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html

（注）　Kerberos の構成例および『*Cisco IOS Security Command Reference*』*Release 12.2* では、信頼できるサードパーティとして Cisco ME スイッチを使用しています。このスイッチは Kerberos に対応し、ネットワーク セキュリティ サーバとして設定可能で、Kerberos プロトコルを使用したユーザ認証ができます。

Kerberos の概要

Kerberos はマサチューセッツ工科大学（MIT）が開発した秘密鍵によるネットワーク認証プロトコルです。Data Encryption Standard（DES; データ暗号化規格）という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティを *Key Distribution Center*（KDC; 鍵発行局）と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC（つまり信頼できる Kerberos サーバ）がユーザにチケットを発行します。このチケットには有効期限があり、ユーザ証明書のキャッシュに保存されます。Kerberos サーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。

（注）　Kerberos サーバには、ネットワーク セキュリティ サーバとして設定可能で、Kerberos プロトコルを用いてユーザを認証できる Cisco ME スイッチを使用できます。

Kerberos の証明書発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを 1 回認証すると、ユーザ証明書が有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、（UNIX サーバや PC などの）他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

このソフトウェア リリースでは、Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh（リモート シェル プロトコル）

表 8-2 に、一般的な Kerberos 関連用語とその定義を示します。

表 8-2　　Kerberos の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ネットワークやスイッチにおいてユーザがどのような権限を有していて、またどのような動作を実行できるかを、スイッチが識別する手段
証明書	認証チケット（TGT [1] やサービス証明書など）を表す総称。Kerberos 証明書で、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの認証レベル ラベル。ほとんどの Kerberos プリンシパルは、「*user@REALM*」という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスのある Kerberos プリンシパルは、「*user/instance@REALM*」という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザの許可レベルを指定するのに使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 **（注）**　Kerberos プリンシパルとインスタンスの名前は*すべて小文字*とします。 **（注）**　Kerberos レルム名は*すべて大文字*とします。
KDC[2]	ネットワーク ホストで稼動する Kerberos サーバおよびデータベース プログラムで構成される KDC。
Kerberos 対応	Kerberos 証明書のインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語。

表 8-2　Kerberos の用語 （続き）

用語	定義
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワークサービスに対する別のユーザまたはネットワーク サービスの ID を検証します。 （注）　Kerberos レルム名はすべて大文字とします。
Kerberos サーバ	ネットワーク ホストで稼動しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。
KEYTAB[3]	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス証明書を暗号解除して認証します。Kerberos 5 以前のバージョンでは、KEYTAB は SRVTAB[4] と呼ばれています。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。 （注）　Kerberos プリンシパル名はすべて小文字とします。
サービス証明書	ネットワーク サービスの証明書。KDC から証明書が発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザ TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、SRVTAB は KEYTAB と呼びます。
TGT	身分証明書のことで、KDC が認証済みユーザに発行する証明書。TGT を受け取ったユーザは、KDC が表した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

1. TGT = Ticket Granting Ticket（身分証明書）
2. KDC = Key Distribution Center（鍵発行局）
3. KEYTAB = key table（キー テーブル）
4. SRVTAB = server table（サーバ テーブル）

Kerberos の動作

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定可能で、Kerberos プロトコルを用いてリモート ユーザを認証できる Cisco ME スイッチを使用できます。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモート ユーザは、3 つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

Kerberos サーバとしての Cisco ME スイッチを使用してネットワーク サービスに対して認証を得る手順は、次のとおりです。

1. 「境界スイッチに対する認証の取得」（P.8-35）
2. 「KDC からの TGT の取得」（P.8-35）
3. 「ネットワーク サービスに対する認証の取得」（P.8-35）

境界スイッチに対する認証の取得

ここでは、リモート ユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。その後、このプロセスは次のように進みます。

1. ユーザが、境界ルータへの Kerberos 非対応 Telnet 接続を確立します。
2. ユーザ名とパスワードの入力を求めるプロンプトが表示されます。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使用して TGT の暗号解除を試行します。
   - 暗号解除に成功したら、ユーザはスイッチに対して認証を得ます。
   - 暗号解除に成功しなかった場合、ユーザは、ユーザ名とパスワードを再入力するか（Caps Lock または Num Lock のオン / オフに注意）、別のユーザ名とパスワードを入力してステップ 2 をやり直します。

境界スイッチに対して Kerberos 非対応 Telnet セッションを確立し認証を得たリモート ユーザは、ファイアウォールの内側に入ることに成功しましたが、ネットワーク サービスへのアクセス権を取得するには、さらに KDC に対して直接認証を得る必要があります。KDC が発行する TGT はスイッチに保存されているので、スイッチにログインしないと、追加の認証用に使用できないためです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過しなければならない 2 番めのセキュリティ レイヤについて説明します。ユーザは、ネットワークにアクセスするために、ここで KDC の認証を得て KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『*Cisco IOS Security Configuration Guide*』*Release 12.2* の「Security Server Protocols」の章の「Obtaining a TGT from a KDC」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html#wp1000999

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番めのセキュリティ レイヤについて説明します。TGT を持つユーザは、ここで Kerberos レルム内のネットワーク サービスに対する認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『*Cisco IOS Security Configuration Guide*』*Release 12.2* の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html#wp1001010

Kerberos の設定

リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定して、ユーザおよびネットワーク サービスと通信を行って互いに認証し合う必要があります。これを実行するには、互いを識別する必要があります。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。

ホストおよびユーザのエントリを追加または作成する場合は、次のガイドラインに従ってください。

- Kerberos プリンシパル名はすべて*小文字*とします。
- Kerberos インスタンス名はすべて*小文字*とします。
- Kerberos レルム名はすべて*大文字*とします。

（注）　Kerberos サーバには、ネットワーク セキュリティ サーバとして設定可能で、Kerberos プロトコルを用いてユーザを認証できる Cisco ME スイッチを使用できます。

Kerberos 認証済みサーバ クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

設定については、『*Cisco IOS Security Configuration Guide*』*Release 12.2* の「Security Server Protocols」の章にある「Kerberos Configuration Task List」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

スイッチのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても AAA が動作するように設定できます。この場合、スイッチが認証および許可の処理を行います。この設定ではアカウンティング機能は利用できません。

スイッチをローカル AAA 用に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login default local**	ローカルのユーザ名データベースを使用するようにログイン認証を設定します。キーワード **default** により、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 4	**aaa authorization exec local**	ユーザ AAA 許可を設定し、ローカル データベースを確認し、EXEC シェルをユーザに実行可能にします。
ステップ 5	**aaa authorization network local**	ネットワーク関連のすべてのサービス要求に関する AAA 許可を設定します。

	コマンド	目的
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースを開始し、ユーザ名ベースの認証システムを設定します。 ユーザごとにこのコマンド入力を繰り返します。 • *name* には、ユーザ ID を 1 ワードで指定します。スペースや引用符は使用できません。 • （任意）*level* には、アクセス後ユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では、ユーザ EXEC モードでのアクセスとなります。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* には、暗号化されていないパスワードがあとに続く場合は 0 を、暗号化されたパスワードがあとに続く場合は 7 を指定します。 • *password* には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

Secure Shell のためのスイッチの設定

ここでは、SSH 機能を設定する方法について説明します。この機能を使用するには、スイッチに暗号化ソフトウェア イメージをインストールする必要があります。この機能を使用するには、その許可を取得し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードする必要があります。詳細については、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「SSH の概要」（P.8-38）
- 「SSH の設定」（P.8-39）
- 「SSH の設定およびステータスの表示」（P.8-41）

SSH の設定例については、『*Cisco IOS Security Configuration Guide*』*Cisco IOS Release12.2* の「Configuring Secure Shell」の章にある「SSH Configuration Examples」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html

（注）　ここで使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、および Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。URL は次のとおりです。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html

SSH の概要

SSH は、デバイスへの安全なリモート接続を提供するプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートします。

ここでは、次の内容について説明します。

- 「SSH サーバ、統合クライアント、およびサポート対象バージョン」（P.8-38）
- 「制限事項」（P.8-39）

SSH サーバ、統合クライアント、およびサポート対象バージョン

SSH 機能には、スイッチで稼動するアプリケーションである、SSH サーバおよび SSH 統合クライアントがあります。SSH サーバが稼動するスイッチとの接続には、SSH クライアントを使用できます。SSH サーバは、このリリースでサポートされる SSH クライアントおよび他社製の SSH クライアントと連動します。また SSH クライアントも、このリリースでサポートされる SSH サーバおよび他社製の SSH サーバと連動します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートします。

SSH は、DES 暗号化アルゴリズム、トリプル DES（3DES）暗号化アルゴリズム、およびパスワードベースのユーザ認証をサポートします。

また SSH は、次のユーザ認証方式もサポートします。

- TACACS+（詳細については、「TACACS+ によるスイッチ アクセスの制御」（P.8-10）を参照してください）
- RADIUS（詳細については、「RADIUS によるスイッチ アクセスの制御」（P.8-17）を参照してください）
- ローカル認証および許可（詳細については、「スイッチのローカル認証および許可の設定」（P.8-36）を参照してください）

（注）　このソフトウェア リリースでは、IP Security（IPSec）をサポートしていません。

制限事項

SSH には、次の制限事項が適用されます。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、シェル実行アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、DES（56 ビット）および 3DES（168 ビット）のデータ暗号化ソフトウェアだけでサポートされます。
- スイッチは、Advanced Encryption Standard（AES）対称暗号化アルゴリズムをサポートしません。

SSH の設定

ここでは、次の設定情報について説明します。

- 「設定時の注意事項」（P.8-39）
- 「スイッチでの SSH 実行の設定」（P.8-39）（必須）
- 「SSH サーバの設定」（P.8-40）（スイッチを SSH サーバとして設定している場合にだけ必要）

設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定するときは、次の注意事項に従ってください。

- SSHv1 サーバにより生成された RSA 鍵ペアは、SSHv2 サーバで使用できます。また、その逆も可能です。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力したあと、CLI エラー メッセージが表示される場合、RSA 鍵ペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。詳細については、「スイッチでの SSH 実行の設定」（P.8-39）を参照してください。
- RSA 鍵ペアを生成するときに、「ホスト名が指定されていません」というメッセージが表示される場合があります。表示される場合は、**hostname** グローバル コンフィギュレーション コマンドを使用して、ホスト名を設定する必要があります。
- RSA 鍵ペアを生成するときに、「ドメイン名が指定されていません」というメッセージが表示される場合があります。表示される場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して、IP ドメイン名を設定する必要があります。
- ローカルの AAA 方式を設定する場合は、コンソール上で AAA がディセーブルであることを確認してください。

スイッチでの SSH 実行の設定

スイッチに SSH の実行を設定するには、次の手順を実行します。

1. Cisco.com から暗号化ソフトウェア イメージをダウンロードします。この手順は必須です。詳細については、このリリースのリリース ノートを参照してください。
2. スイッチに、ホスト名および IP ドメイン名を設定します。この手順は、スイッチを SSH サーバとして設定している場合にだけ実行します。
3. スイッチに RSA 鍵ペアを生成します。これにより自動的に SSH がイネーブルになります。この手順は、スイッチを SSH サーバとして設定している場合にだけ実行します。

4. ローカルまたはリモート アクセスにユーザ認証を設定します。この手順は必須です。詳細については、「スイッチのローカル認証および許可の設定」（P.8-36）を参照してください。

ホスト名および IP ドメイン名を設定して、RSA 鍵ペアを生成するには、特権 EXEC モードで次の手順を実行します。この手順は、スイッチを SSH サーバとして設定している場合に必要です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *hostname*	スイッチにホスト名を設定します。
ステップ 3	**ip domain-name** *domain_name*	スイッチにホスト ドメインを設定します。
ステップ 4	**crypto key generate rsa**	スイッチのローカルおよびリモート認証に関して、SSH サーバをイネーブルにして、RSA 鍵ペアを生成します。 モジュール サイズを 1024 ビット以上にすることを推奨します。 RSA 鍵ペアを生成すると、モジュールの長さを入力するよう求められます。モジュールの長さが長い方がセキュリティは高くなりますが、生成および使用に時間がかかります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバのステータスを表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RSA 鍵ペアを削除するには、**crypto key zeroize rsa** グローバル コンフィギュレーション コマンドを使用します。RSA 鍵ペアを削除すると、SSH サーバは自動的にディセーブルになります。

SSH サーバの設定

SSH サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip ssh version** [**1** | **2**]	（任意）スイッチに SSH バージョン 1 または 2 を実行するよう設定します。 • **1**：スイッチに SSH バージョン 1 を実行するように設定します。 • **2**：スイッチに SSH バージョン 2 を実行するように設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合は、SSH サーバにより SSH クライアントがサポートする最新の SSH バージョンが選択されます。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。

	コマンド	目的
ステップ 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}	SSH 制御パラメータを設定します。 • タイムアウト値を秒単位で指定します。デフォルトでは 120 秒です。指定できる範囲は 0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されると、スイッチはデフォルトの CLI ベース セッションのタイムアウト値を使用します。 デフォルトでは、複数の CLI ベース セッションに関する暗号化 SSH 接続を最大 5 つまで同時にネットワーク上で使用できます（セッション 4 に対してセッション 0）。シェル実行が開始されると、CLI ベース セッションのタイムアウト値がデフォルトの 10 分に戻ります。 • クライアントがサーバに対して再認証できる回数を指定します。デフォルトは 3 で、指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合は、このステップを繰り返します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバ接続のステータスを表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの SSH 制御パラメータに戻るには、**no ip ssh** {**timeout** | **authentication-retries**} グローバル コンフィギュレーション コマンドを使用します。

SSH の設定およびステータスの表示

SSH サーバの設定およびステータスを表示するには、表 8-3 に示される特権 EXEC コマンドを 1 つまたは複数使用します。

表 8-3　SSH サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』*Cisco IOS Release12.2* の「Other Security Features」の章にある「Secure Shell Commands」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7cd.html

SCP のためのスイッチの設定

Secure Copy Protocol（SCP）機能は、スイッチ設定またはスイッチ イメージ ファイルをセキュアな認証方法でコピーすることができます。SCP は、Secure Shell（SSH; セキュア シェル）に依存します。SSH は、Berkeley r-tool をセキュアにしたアプリケーションおよびプロトコルです。

SSH を動作させるには、RSA 公開鍵と秘密鍵のペアがスイッチで必要です。セキュアな転送のために SSH に依存している SCP も同様です。

SSH は AAA 認証にも依存しており、したがって SCP は AAA 許可に依存するため、正しい設定が必要になります。

- SCP をイネーブルにする前に、SSH、認証、認可をスイッチで正しく設定します。
- SCP はセキュアな転送のために SSH に依存するので、ルータでは RSA 鍵ペアが必要です。

（注）　SCP を使用する場合、copy コマンドにパスワードは入力できません。プロンプトが表示されてから、パスワードを入力します。

Secure Copy について

Secure Copy 機能を設定するには、次の概念を理解する必要があります。

- SCP の動作は、SCP がセキュリティのために SSH に依存している点を除いて、Berkeley の r-tool スイートからできた remote copy（rcp）と同様です。また、SCP でも AAA の設定が必須であるため、ルータはユーザに正しい権限レベルがあるかどうか判断できます。
- 適切に許可されたユーザは、SCP を使用して、**copy** コマンドにより、スイッチにまたはスイッチから Cisco IOS File System（IFS）内の任意のファイルをコピーできます。許可された管理者も、ワークステーションからこの操作を実行できます。

SCP の設定方法および確認方法については、次の URL にある『*Cisco IOS New Features*』*Cisco IOS Release 12.2* の「Secure Copy Protocol」の章を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b18.html

CHAPTER 9

IEEE 802.1x ポートベースの認証の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチで IEEE 802.1x ポートベースの認証を設定する方法について説明します。LAN がホテルや空港、会社のロビーにまで拡張されて安全でない環境が生じるため、802.1x により無許可の装置（クライアント）によるネットワークへのアクセスを防止します。

この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

（注） IEEE 802.1x（**dot1x**）コマンドの中には、スイッチ上に表示されていても、サポートされていないものがあります。サポートされていないコマンドのリストについては、付録 C「Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド」を参照してください。

この章で説明する内容は、次のとおりです。

- 「IEEE 802.1x ポートベースの認証の概要」（P.9-1）
- 「IEEE 802.1x 認証の設定」（P.9-12）
- 「802.1x 統計情報およびステータスの表示」（P.9-27）

IEEE 802.1x ポートベースの認証の概要

IEEE 802.1x 規格は、クライアント / サーバ ベースのアクセス制御と認証プロトコルについて定義し、不正なクライアントが適切に認証されていない場合は公的にアクセス可能なポートを介した LAN 接続を制限します。認証サーバは、スイッチ ポートに接続された各クライアントを認証してから、スイッチまたは LAN が提供するサービスを利用できるようにします。

クライアントが認証されるまでは、802.1x アクセス制御によって、クライアントに接続したポートを経由する Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、および Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）トラフィックだけを許可します。認証に成功すると、通常のトラフィックはポートを通過できます。

（注） CDP および STP は、Network Node Interface（NNI; ネットワーク ノード インターフェイス）でデフォルトでサポートされます。Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）上で、CDP および STP をイネーブルにできます。User Network Interface（UNI; ユーザ ネットワーク インターフェイス）では、CDP または STP はサポートされていません。

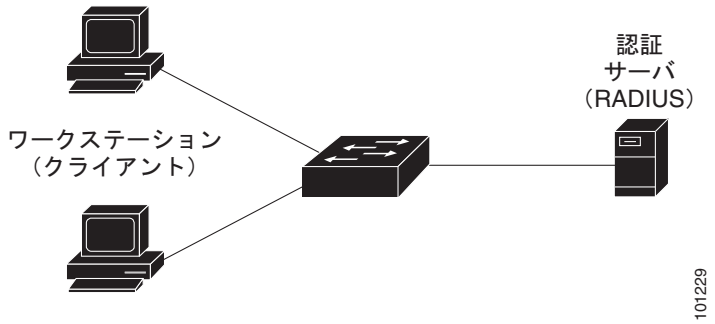
ここでは、802.1x ポートベース認証について説明します。

- 「デバイスの役割」（P.9-2）
- 「認証の開始とメッセージ交換」（P.9-3）
- 「許可ステートおよび無許可ステートのポート」（P.9-4）
- 「802.1x アカウンティング」（P.9-5）
- 「802.1x アカウンティングのアトリビュートと値のペア」（P.9-5）
- 「802.1x ホスト モード」（P.9-6）
- 「802.1x 準備状態チェック」（P.9-7）
- 「ポート セキュリティを含む 802.1x」（P.9-7）
- 「VLAN 割り当てを含む 802.1x」（P.9-8）
- 「802.1x ユーザ分散」（P.9-9）
- 「ネットワーク エッジ アクセス トポロジ（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ」（P.9-10）
- 「コモン セッション ID」（P.9-11）

デバイスの役割

802.1x ポートベース認証を使用すると、ネットワーク内のデバイスは図 9-1 のような特定の役割が割り当てられます。

図 9-1　802.1x デバイスの役割



- *クライアント*：LAN およびスイッチへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP オペレーティング システムなどで提供されるような、802.1x 準拠のクライアント ソフトウェアが稼動している必要があります （クライアントは、802.1x 規格の *サプリカント*になります）。

（注） Windows XP ネットワーク接続および IEEE 802.1x 認証の問題を解決するには、次の URL にアクセスして Microsoft Knowledge Base Article を参照してください。
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ*: 実際にクライアントの認証を行います。認証サーバは、クライアントの ID を確認し、クライアントの LAN およびスイッチ サービスへのアクセスを許可するかどうかをスイッチに通知します。スイッチはプロキシとして機能するので、認証サービスはクライアントにトランスペアレントです。このリリースでサポートされている認証サーバは、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）拡張機能を装備した RADIUS セキュリティ システムだけです。これは、Cisco Secure Access Control Server（ACS）バージョン 3.0 以上に対応しています。RADIUS は、RADIUS サーバと 1 つまたは複数の RADIUS クライアント間で安全な認証情報が交換されるクライアント/サーバ モデルで動作します。
- *スイッチ*（エッジ スイッチまたは無線アクセス ポイント）: クライアントの認証ステータスに基づいてネットワークへの物理アクセスを制御します。スイッチは、クライアントと認証サーバとの間の媒介（プロキシ）として機能し、クライアントに ID 情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには RADIUS クライアントが組み込まれています。RADIUS クライアントは、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの相互作用の役割を果たします。

  スイッチが EAPOL フレームを受信して認証サーバにリレーすると、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS 形式で再度カプセル化されます。EAP フレームはカプセル化の間は変更が行われず、認証サーバはネイティブのフレーム形式で EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、EAP フレームが残ります。これがイーサネット用にカプセル化されてクライアントに送信されます。

認証の開始とメッセージ交換

スイッチまたはクライアントは、認証を開始できます。**dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンク ステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチは、EAP 要求/ID フレームをクライアントに送信して ID を要求します。フレームの受信後、クライアントは EAP 応答/ID フレームで応答します。

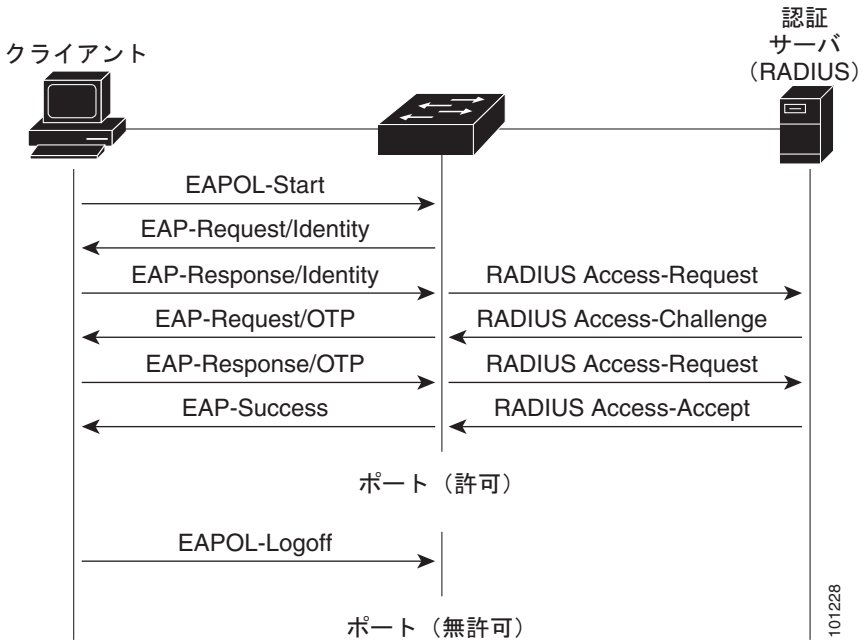
ただし、起動中にクライアントがスイッチから EAP 要求/ID フレームを受信しない場合は、クライアントは、EAPOL 開始フレームを送信して認証を開始できます。これにより、スイッチはクライアントの ID を要求するようになります。

（注）　ネットワーク アクセス デバイスで 802.1x がイネーブルになっていないかサポートされていない場合は、クライアントからの EAPOL フレームは廃棄されます。認証の開始を 3 回試行してもクライアントが EAP 要求/ID フレームを受信しない場合は、クライアントは、ポートが許可ステートであるものとしてフレームを送信します。許可ステートにあるポートは、事実上クライアントが正常に認証されたということを意味します。詳細については、「許可ステートおよび無許可ステートのポート」（P.9-4）を参照してください。

クライアントが自身の ID を提供すると、スイッチは媒介としての役割を開始し、認証が成功または失敗するまでクライアントと認証サーバとの間で EAP フレームを送受信します。認証に成功すると、スイッチのポートは許可された状態になります。詳細については、「許可ステートおよび無許可ステートのポート」（P.9-4）を参照してください。

特定の EAP フレーム交換は、使用される認証方式に依存します。図 9-2 に、RADIUS サーバで One Time Password（OTP; ワンタイム パスワード）認証方式を使用するクライアントによって開始されるメッセージ交換を示します。

図 9-2　メッセージ交換



許可ステートおよび無許可ステートのポート

スイッチ ポート ステートに応じて、スイッチはクライアントのネットワークへのアクセスを許可します。ポートは、*無許可*ステートで起動します。このステートでは、ポートは 802.1x、CDP、STP パケット以外の着信および発信トラフィックを許可しません。クライアントが正常に認証されると、ポートは*許可*ステートに移行し、そのクライアントへのすべてのトラフィックは通常のフローが許可されます。

802.1x をサポートしないクライアントが無許可の 802.1x ポートに接続している場合、スイッチはクライアントの ID を要求します。この場合、クライアントは要求に応答できないので、ポートは無許可ステートのままとなり、クライアントはネットワーク アクセスが許可されません。

対照的に、802.1x 対応クライアントが 802.1x 規格を実行していないポートに接続している場合、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答が得られなかった場合、クライアントは要求を一定の回数だけ送信します。応答が得られないので、クライアントはポートが許可ステートにあるものとしてフレームの送信を開始します。

ポートの許可ステートを制御するには、**dot1x port-control** インターフェイス コンフィギュレーション コマンドと次のキーワードを使用します。

- **force-authorized**：IEEE 802.1x 認証をディセーブルにして、認証情報の交換を要求せずにポートを許可ステートに移行させます。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これは、デフォルト設定です。
- **force-unauthorized**：ポートを無許可ステートのままにし、クライアントが認証を試みてもすべて無視します。スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto**：802.1x 認証をイネーブルにして、ポートに無許可ステートで開始させ、EAPOL フレームだけがポート経由で送受信できるようにします。ポートのリンク ステートがダウンからアップに移行するか、EAPOL 開始フレームを受信すると、認証プロセスが開始されます。スイッチは、クライアントの ID を要求し、クライアントと認証サーバ間で認証メッセージのリレーを開始します。スイッチはネットワークにアクセスしようとする各クライアントを、クライアントの MAC アドレスを使用して一意に識別します。

クライアントが正常に認証されると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントのフレームはすべてそのポート経由で送受信を許可されます。認証が失敗した場合は、ポートは無許可ステートのままですが、認証を再試行できます。認証サーバにアクセスできない場合、スイッチは要求を再送信できます。指定された試行回数のあとでもサーバから応答が得られない場合は、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフすると EAPOL ログオフ メッセージを送信します。これにより、スイッチ ポートは無許可ステートに移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ フレームを受信した場合は、ポートは無許可ステートに戻ります。

802.1x アカウンティング

802.1x 標準は、ネットワーク アクセスに対するユーザの許可および認証方法を定義しますが、ネットワークの使用状況を追跡するものではありません。802.1x アカウンティングは、デフォルトでディセーブルに設定されています。802.1x アカウンティングをイネーブルにすると、802.1x 対応ポートで次のアクティビティを監視できます。

- ユーザ認証の成功
- ユーザのログオフ
- リンク ダウンの発生
- 再認証の成功
- 再認証の失敗

スイッチは 802.1x アカウンティング情報をログに記録しません。代わりに、この情報を RADIUS サーバに送信します。RADIUS サーバはアカウンティング メッセージをログに記録するように設定されている必要があります。

802.1x アカウンティングのアトリビュートと値のペア

RADIUS サーバに送信された情報は、アトリビュートと値（AV）のペアという形式で表されます。AV ペアは、さまざまなアプリケーションにデータを提供します （たとえば、課金アプリケーションでは、パケットの Acct-Input-Octets または Acct-Output-Octets の情報が必要となることがあります）。

AV ペアを設定する必要はありません。これらは、802.1x アカウンティングに設定されるスイッチによって、自動的に送信されます。表 9-1 に、スイッチが送信する AV ペアを示します。

表 9-1　　アカウンティングの AV ペア

アトリビュート番号	AV ペア名
Attribute [1]	User-Name
Attribute [4]	NAS-IP-Address
Attribute [5]	NAS-Port
Attribute [6]	NAS-Port-Type
Attribute [8]	Framed-IP-Address
Attribute [25]	Class
Attribute [30]	Called-Station-ID
Attribute [31]	Calling-Station-ID

表 9-1　アカウンティングの AV ペア （続き）

アトリビュート番号	AV ペア名
Attribute [40]	Acct-Status-Type
Attribute [41]	Acct-Delay-Time
Attribute [42]	Acct-Input-Octets
Attribute [43]	Acct-Output-Octets
Attribute [44]	Acct-Session-ID
Attribute [45]	Acct-Authentic
Attribute [46]	Acct-Session-Time
Attribute [49]	Acct-Terminate-Cause

スイッチによって送信されている AV ペアを表示するには、**debug radius accounting** または **debug aaa accounting** の各特権 EXEC コマンドを入力します。このコマンドの詳細については、次の URL の『*Cisco IOS Debug Command Reference*』*Release 12.2* を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122debug/

AV ペアの詳細については、RFC 3580『IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

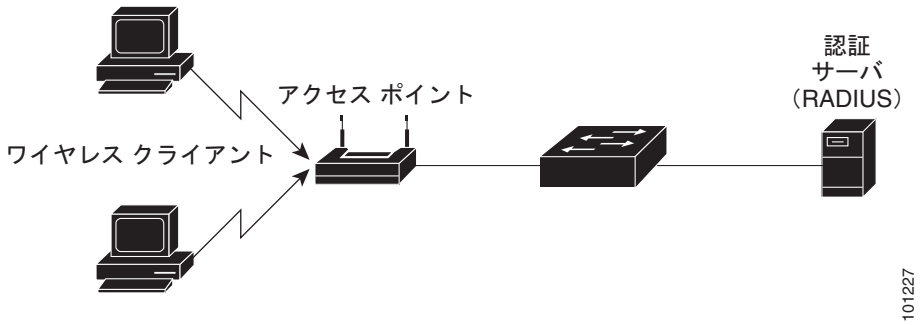
802.1x ホスト モード

802.1x ポートは、単一ホスト モードまたは複数ホスト モードに設定できます。単一ホスト モード（図 9-1（P.9-2）を参照）では、802.1x 対応のスイッチ ポートに接続できるクライアントは 1 台だけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信してクライアントを検出します。クライアントがログオフするか、別のクライアントに交換されると、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

複数ホスト モードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。図 9-3（P.9-7）は、無線 LAN における 802.1x ポートベース認証を表しています。このモードでは、接続ホストのいずれか 1 つだけが許可されれば、すべてのホストがネットワーク アクセスを許可されます。ポートが無許可になると（再認証が失敗するか、EAPOL ログオフ メッセージを受信する）、スイッチは、接続しているすべてのクライアントに対するネットワーク アクセスを拒否します。このトポロジでは、無線アクセス ポイントは、接続しているクライアントを認証する役割があり、スイッチに対してクライアントとして機能します。

複数ホスト モードがイネーブルの場合、802.1x をポートの認証に使用し、クライアントを含むすべての MAC アドレスへのネットワーク アクセスをポート セキュリティが管理します。

図 9-3　複数ホスト モードの例



802.1x 準備状態チェック

802.1x 準備状態チェックでは、すべてのスイッチ ポート上における 802.1x のアクティビティが監視され、802.1x がサポートされているポートに接続されたデバイスに関する情報が表示されます。この機能を使用すれば、スイッチ ポートに接続されたデバイスが 802.1x 対応であるかどうかを確認できます。802.1x の機能がサポートされていないデバイスに対しては、別の認証を使用します。

この機能が動作するのは、NOTIFY EAP 通知パケットを使用したクエリーがクライアント上のサプリカントによってサポートされている場合だけです。クライアントは、802.1x タイムアウト値の範囲内で応答する必要があります。

802.1x 準備状態チェックに関するスイッチの設定については、「802.1x 準備状態チェックの設定」（P.9-14）を参照してください。

ポート セキュリティを含む 802.1x

単一ホスト モードまたは複数ホスト モードのどちらかで、ポート セキュリティを含む 802.1x ポートを設定できます（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定する必要もあります）。ポート上のポート セキュリティと 802.1x をイネーブルにすると、802.1x がポートを認証し、ポート セキュリティがクライアントの MAC アドレスを含むすべての MAC アドレスについてネットワーク アクセスを管理します。この場合、802.1x ポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

たとえば、スイッチにおいて、802.1x とポート セキュリティの間には次のような相互作用があります。

- クライアントが認証され、ポート セキュリティ テーブルが満杯になっていない場合、クライアントの MAC アドレスがセキュア ホストのポート セキュリティ リストに追加されます。追加されると、ポートが通常どおりアクティブになります。

  クライアントが認証されてポート セキュリティが手動で設定された場合、セキュア ホスト テーブル内のエントリが保証されます（ポート セキュリティのスタティック エージングがイネーブルになっていない場合）。

  クライアントが認証されてもセキュリティ テーブルが満杯の場合は、セキュア違反が発生します。これは、セキュア ホストの最大数がスタティックに設定されているか、またはセキュア ホスト テーブルでのクライアントの有効期限が切れた場合に発生します。クライアントのアドレスの有効期限が切れた場合、そのクライアントのセキュア ホスト テーブルの位置は他のホストに取って代わられます。

最初の認証ホストによってセキュリティ違反が引き起こされた場合、ポートは errdisable となり、すぐにシャットダウンされます。

ポート セキュリティ違反モードは、セキュリティ違反の動作を判別します。詳細については、「セキュリティ違反」（P.23-10）を参照してください。

- **no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、802.1x クライアントのアドレスをポート セキュリティ テーブルから手動で削除した場合は、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを使用して 802.1x クライアントを再認証する必要があります。
- 802.1x クライアントがログオフすると、ポートが無許可ステートに移行し、クライアントのエントリを含むセキュア ホスト テーブル内のすべてのダイナミック エントリが消去されます。ここで通常の認証が実行されます。
- ポートが管理上の理由からシャットダウンされる場合、ポートは無許可ステートになりすべてのダイナミック エントリはセキュア ホスト テーブルから削除されます。
- **dot1x violation-mode** インターフェイス コンフィギュレーション コマンドを設定して、ポートが IEEE 802.1x 対応ポートに接続されている場合や、最大数の許可デバイスが認証されている場合に、ポートがシャットダウンされたり、Syslog エラーが生成されたり、または、新しいデバイスからのパケットが破棄されたりするようにできます。詳細については、「ポート単位の許可デバイスの最大数」（P.9-14）および、このリリースのコマンド リファレンスを参照してください。

スイッチのポート セキュリティをイネーブルにする方法の詳細については、「ポート セキュリティの設定」（P.23-8）を参照してください。

VLAN 割り当てを含む 802.1x

RADIUS サーバは、スイッチ ポートを設定するために VLAN 割り当てを送信します。RADIUS サーバのデータベースは、ユーザ名 /VLAN のマッピングを維持します。このマッピングでは、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てています。この機能を使用して、特定ユーザのネットワーク アクセスを制限できます。

スイッチと RADIUS サーバで設定されている場合、802.1x と VLAN 割り当てには次のような特性があります。

- RADIUS サーバが VLAN を割り当てていないか、または 802.1x 許可がディセーブルの場合、認証が成功したあとにポートはアクセス VLAN に設定されます。
- 802.1x 許可がイネーブルだが、RADIUS サーバからの VLAN 情報が有効でない場合には、ポートは無許可ステートを戻し、設定済みのアクセス VLAN 内に留まります。これにより、設定エラーによって不適切な VLAN 上にポートが突然現れることを防ぎます。

  設定エラーには、ルーテッド ポートへの VLAN の指定、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）VLAN ID などがあります。
- 802.1x 許可がイネーブルで RADIUS サーバからのすべての情報が有効の場合、ポートは認証が成功したあと指定した VLAN に配置されます。
- 802.1x ポートで複数ホスト モードがイネーブルの場合は、全てのホストが最初に認証されたホストと同じ VLAN（RADIUS サーバによって指定された）に配置されます。
- 802.1x とポート セキュリティがポート上でイネーブルの場合は、そのポートは RADIUS サーバによって割り当てられた VLAN に配置されます。
- 802.1x がポートでディセーブルの場合は、設定済みのアクセス VLAN に戻ります。

ポートが強制許可（force authorized）、強制無許可（force unauthorized）、無許可、シャットダウンのいずれかのステートの場合、そのポートは設定済みのアクセス VLAN に配置されます。

802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置された場合、ポートのアクセス VLAN 設定への変更は反映されません。

VLAN 割り当て機能付きの 802.1x は、トランク ポート、または VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）を使用したダイナミック アクセス ポート割り当てではサポートされていません。

VLAN 割り当てを設定するには、次の作業を実行します。

- キーワード **network** を使用して Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x をイネーブルにします （VLAN 割り当て機能は、アクセス ポートに 802.1x が設定されると自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル アトリビュートを割り当てます。RADIUS サーバは次のアトリビュートをスイッチに戻す必要があります。
  - [64] トンネル タイプ = VLAN
  - [65] トンネル メディア タイプ = 802
  - [81] トンネル プライベート グループ = VLAN 名または VLAN ID

  アトリビュート [64] は、値 *VLAN*（type 13）とします。アトリビュート [65] は、値 *802*（type 6）とします。アトリビュート [81] には、802.1x 認証ユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

トンネル アトリビュートの例については、「ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法」（P.8-29）を参照してください。

802.1x ユーザ分散

802.1x ユーザ分散を設定して、複数の異なる VLAN を超えて、同じグループ名を持つ各ユーザのロード バランシングができます。

各 VLAN は、RADIUS サーバによって提供されるか、任意の VLAN グループ名で、スイッチ CLI を介して設定されます。

- 1 つのユーザに対して複数の VLAN 名を送信するように RADIUS サーバを設定します。複数の VLAN 名を、ユーザに対する応答の一部として送信できます。802.1x ユーザ分散では、特定の VLAN 内のすべてのユーザを追跡し、許可済みユーザを最もユーザ数の少ない VLAN に移動することによって、ロード バランシングを実現します。
- 1 つのユーザに対して、1 つの VLAN グループ名を送信するように RADIUS サーバを設定します。その VLAN グループ名を、ユーザに対する応答の一部として送信できます。スイッチ CLI を使用して設定した複数の VLAN グループ名の中から、選択した VLAN グループ名を検索できます。その VLAN グループ名が発見されると、最もユーザが少ない VLAN を発見するために、その VLAN グループ名に属する、対応する VLAN が検索されます。対応する許可済みユーザが、その VLAN に移動されることによって、ロード バランシングが実現します。

（注） RADIUS サーバによって、VLAN-ID、VLAN 名、または VLAN グループのどんな組み合せでも、VLAN 情報を送信できます。

802.1x ユーザ分散の設定ガイドライン

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされていることを確認します。

- 1 つの VLAN グループに複数の VLAN をマッピングできます。
- VLAN を追加または削除することによって、VLAN グループを変更できます。
- VLAN グループ名から既存の VLAN を消去しても、その VLAN 内のいずれの認証済みポートも消去されることはありませんが、マッピングでは、既存の VLAN グループから削除されます。
- VLAN グループ名から最後の VLAN を消去すると、その VLAN グループは消去されます。
- ある VLAN グループにアクティブな VLAN がマッピングされていても、その VLAN グループを消去できます。VLAN グループを消去しても、そのグループ内のいずれかの VLAN において許可ステートにあるポートまたはユーザは消去されませんが、その VLAN グループに対する VLAN マッピングは消去されます。

詳細については、「802.1x ユーザ分散の設定」（P.9-24）を参照してください。

ネットワーク エッジ アクセス トポロジ（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ

Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）機能によって、ID を、ワイヤリング クローゼット（会議室など）の外部の領域に拡張できます。これにより、あらゆるタイプのデバイスに対して、ポート上での認証を許可できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することによって、スイッチを、他のスイッチに対するサプリカントとして動作するように設定できます。この設定は、スイッチがワイヤリング クローゼットの外部にあり、トランク ポートを介してアップストリーム スイッチに接続されているようなシナリオで有用です。802.1x スイッチ サプリカント機能を使用して設定したスイッチでは、アップストリーム スイッチによって認証が行われるので、接続の安全性が確保されます。

  サプリカント スイッチによる認証が成功すると、ポート モードがアクセスからトランクに変更されます。

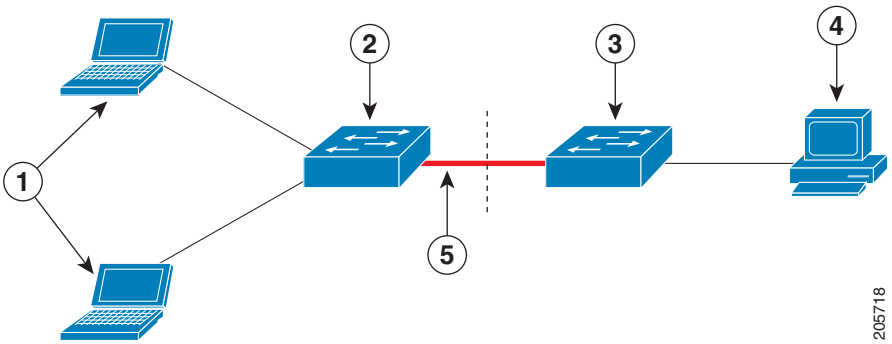
- アクセス VLAN をオーセンティケータ スイッチ上で設定すると、その VLAN は、認証が成功した後に、トランク ポートのネイティブ VLAN になります。

もう 1 つのサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイス上で、MDA またはマルチ認証モードをイネーブルにできます。マルチホスト モードは、オーセンティケータ スイッチ インターフェイスではサポートされていません。

NEAT がすべてのホスト モードで動作するように、サプリカント スイッチ上で、**dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを使用します。

- ホスト許可：（サプリカントを使用したスイッチに接続している）許可済みホストがネットワーク上で確実に許可されるようにします。各スイッチでは、図 9-4 に示すように、Client Information Signalling Protocol（CISP; クライアント情報シグナリング プロトコル）によって、サプリカント スイッチに接続している MAC アドレスがオーセンティケータ スイッチに送信されます。
- 自動イネーブル化：オーセンティケータ スイッチ上でトランク設定が自動的にイネーブルにされ、オーセンティケータ スイッチから来る、複数の VLAN からのユーザ トラフィックが許可されます。ACS で、cisco-av-pair を *device-traffic-class=switch* に設定します （これは、*group* または *user* 設定で設定できます）。

図 9-4　CISP を使用したオーセンティケータおよびサプリカント スイッチ



1	ワークステーション（クライアント）	2	サプリカント スイッチ（ワイヤリング クローゼットの外部）
3	オーセンティケータ スイッチ	4	Access Control Server（ACS）
5	トランク ポート		

ガイドライン

- NEAT ポートを、他の認証ポートと同じコンフィギュレーションで設定できます。サプリカント スイッチが認証を実行すると、スイッチ ベンダー固有アトリビュート（VSA）に基づいて、ポートモードが *アクセス*から *トランク*に変更されます （device-traffic-class=switch）。
- VSA によって、オーセンティケータ スイッチ ポート モードが、アクセスからトランクに変更され、802.1x トランクのカプセル化およびアクセス VLAN が、ネイティブ トランク VLAN に変換される場合に、イネーブルにされます。VSA によっては、サプリカント上でのポート設定は変更されません。
- ホスト モードを変更し、*また*、オーセンティケータ スイッチ ポート上で標準ポート設定を適用するには、スイッチ VSA ではなく、AutoSmart ポート ユーザ定義マクロを使用することも可能です。これにより、オーセンティケータ スイッチ ポート上のサポートされていない設定を削除し、ポート モードを *アクセス*から *トランク*に変更できます。詳細については、第 11 章「コマンド マクロの設定」を参照してください。

詳細については、「オーセンティケータおよび、NEAT を使用したサプリカント スイッチの設定」（P.9-25）を参照してください。

コモン セッション ID

認証マネージャでは、どの認証方法が使用されるのかに関わらず、クライアントのシングル セッション ID（コモン セッションと呼びます）が使用されます。この ID は、表示コマンドや MIB など、あらゆるレポート用途で使用されます。セッション ID は、セッション単位のすべての Syslog メッセージと共に表示されます。

セッション ID には、次のものがあります。

- Network Access Device（NAD; ネットワーク アクセス デバイス）の IP アドレス
- 単調に増加する一意の 32 ビット整数
- セッション開始タイム スタンプ（32 ビット整数）

この例では、show authentication コマンドの出力内でセッション ID がどのように表示されるのかを示します。この例におけるセッション ID は、160000050000000B288508E5 です。

```
Switch# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

これは、Syslog 出力内でのセッション ID の表示例です。この例におけるセッション ID も、160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

このセッション ID は、クライアントを特定するために、NAD、AAA サーバ、およびその他レポート分析アプリケーションによって使用されます。ID は自動的に表示されます。設定は不要です。

IEEE 802.1x 認証の設定

ここでは、次の設定情報について説明します。

- 「802.1x のデフォルト設定」（P.9-13）
- 「802.1x 設定時の注意事項」（P.9-13）
- 「802.1x 準備状態チェックの設定」（P.9-14）（任意）
- 「802.1x 認証の設定」（P.9-16）（必須）
- 「スイッチと RADIUS サーバ間通信を設定する方法」（P.9-17）（必須）
- 「定期的な再認証の設定」（P.9-18）（任意）
- 「手動によるポート接続クライアントの再認証」（P.9-19）（任意）
- 「待機時間の変更」（P.9-19）（任意）
- 「スイッチとクライアント間の再送信時間の変更」（P.9-20）（任意）
- 「スイッチとクライアント間のフレーム再送信回数の設定」（P.9-21）（任意）
- 「再認証回数の設定」（P.9-21）（任意）
- 「ホスト モードの設定」（P.9-22）（任意）
- 「802.1x 設定をデフォルト値にリセットする方法」（P.9-23）（任意）
- 「802.1x アカウンティングの設定」（P.9-23）（任意）
- 「802.1x アカウンティングの設定」（P.9-23）（任意）
- 「802.1x ユーザ分散の設定」（P.9-24）（任意）
- 「オーセンティケータおよび、NEAT を使用したサプリカント スイッチの設定」（P.9-25）（任意）

802.1x のデフォルト設定

表 9-2 に、802.1x のデフォルト設定を示します。

表 9-2　802.1x のデフォルト設定

機能	デフォルト設定
AAA	ディセーブル。
RADIUS サーバ • IP アドレス • UDP 認証ポート • 鍵	 • 指定なし。 • 1812. • 指定なし。
スイッチの 802.1x イネーブル ステート	ディセーブル。
ポート単位の 802.1x イネーブル ステート	ディセーブル（force-authorized）。 ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
定期的再認証	ディセーブル。
再認証試行間隔	3600 秒
再認証回数	2 回（ポートが未許可ステートになるまでにスイッチが認証プロセスを再開する回数）
待機時間	60 秒（クライアントとの認証交換が失敗したあと、スイッチが待機ステートにとどまる秒数）
再送信時間	30 秒（スイッチが、クライアントからの EAP 要求/ID フレームに対する応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（スイッチが、認証プロセスを再開するまでに EAP 要求/ID フレームを送信する回数）
ホスト モード	単一ホスト モード
クライアントのタイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが応答を待ち、クライアントに要求を再送信するまでの時間）
認証サーバのタイムアウト時間	30 秒（クライアントの応答を認証サーバにリレーするとき、スイッチが応答を待ち、サーバに応答を送信するまでの時間）。 このタイムアウト時間を変更するには、**dot1x timeout server-timeout** インターフェイス コンフィギュレーション コマンドを使用します。

802.1x 設定時の注意事項

802.1x 認証の設定時の注意事項は次のとおりです。

- 802.1x がイネーブルの場合、ポートは認証されたあとに他のレイヤ 2 またはレイヤ 3 機能がイネーブルになります。
- 802.1x プロトコルは、レイヤ 2 スタティック アクセス ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。

  - トランク ポート：トランク ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol [VQP]）ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
  - EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバーを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポート上のポートで 802.1x をイネーブルにできます。ただし、ポートが SPAN または RSPAN 宛先ポートとして削除されるまで 802.1x はディセーブルです。SPAN または RSPAN 送信元ポートでは、802.1x をイネーブルにできます。
- RSPAN VLAN または プライベート VLAN 以外のすべての VLAN を設定できます。
- VLAN 割り当て機能付きの 802.1x は、プライベート VLAN ポート、トランク ポート、または VMPS を使用したダイナミック アクセス ポート割り当てではサポートされていません。
- プライベート VLAN ポートでは 802.1x を設定できますが、ポート セキュリティとは同時に設定しないでください。
- **dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x をグローバルにイネーブルにする前に、802.1x と EtherChannel が設定されているインターフェイスで EtherChannel コンフィギュレーションを削除します。

ポート単位の許可デバイスの最大数

これは、802.1x 対応ポート上で許可されるデバイスの最大数です。

- 単一ホスト モードでは、アクセス VLAN 上で許可されるデバイスは 1 つだけです。ポートを音声 VLAN でも設定する場合、音声 VLAN を介してトラフィックを送受信可能な Cisco IP Phone の数に制限はありません。
- マルチホスト モードでは、ポート上で許可される 802.1x サプリカントは 1 つだけですが、アクセス VLAN 上で許可される非 802.1x ホストの数に制限はありません。音声 VLAN 上で許可されるデバイスの数に制限はありません。

802.1x 準備状態チェックの設定

802.1x 準備状態チェックでは、すべてのスイッチ ポート上における 802.1x のアクティビティが監視され、802.1x がサポートされているポートに接続されたデバイスに関する情報が表示されます。この機能を使用すれば、スイッチ ポートに接続されたデバイスが 802.1x 対応であるかどうかを確認できます。

802.1x 準備状態チェックは、802.1x 用に設定可能なすべてのポート上で許可されます。準備状態チェックは、**dot1x force-unauthorized** として設定されているポート上では使用できません。

スイッチ上で準備状態チェックをイネーブルにするには、次のガイドラインに従ってください。

- 準備状態チェックは、802.1x をスイッチ上でイネーブルにする前に使用するのが一般的です。
- インターフェイスを指定しないで **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタック上のすべてのポートがテストされます。

- 802.1x 対応ポート上で **dot1x test eapol-capable** コマンドを設定し、リンクが起動する際、ポートによって、接続されたクライアントに対し、その 802.1x 機能に関するクエリーが実行されます。クライアントが通知パケットによって応答する場合、そのクライアントは 802.1x 対応です。クライアントがタイムアウト時間内で応答すると、Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、そのクライアントは非 802.1x 対応です。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホストを処理するポート上（IP 電話に接続された PC など）で送信できます。Syslog メッセージは、タイマー時間内で準備状態チェックに応答するクライアントごとに生成されます。

スイッチ上で 802.1x 準備状態チェックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dot1x test eapol-capable** [**interface** *interface-id*]	スイッチ上で 802.1x 準備状態チェックをイネーブルにします。 （任意）*interface-id* には、IEEE 802.1x 準備状態のチェックを実行するポートを指定します。 **（注）** オプションの **interface** キーワードを省略すると、スイッチ上のすべてのインターフェイスがテストされます。
ステップ 1	**configure terminal**	（任意）グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot1x test timeout** *timeout*	（任意）EAPOL 応答を待機するために使用されるタイムアウトを設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。
ステップ 3	**end**	（任意）特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	（任意）変更したタイムアウト値を確認します。

次の例では、スイッチ上で準備状態チェックをイネーブルにしてポートにクエリーを実行する方法を示します。また、照会済みポートから受信した応答も示し、接続しているデバイスが 802.1x 対応であることを確認します。

```
switch# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

802.1x 違反モードの設定

802.1x ポートを、次の場合にシャットダウンされ、Syslog エラーを生成し、新しいデバイスからのパケットを破棄するように設定できます。

- デバイスが 802.1x 対応ポートに接続している
- デバイスに関して許可される最大数がポート上で許可されている

スイッチ上にセキュリティ違反動作を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定*されない*場合に使用されるデフォルトのリストを作成するには、キーワード **default** の後ろにデフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、キーワード **group radius** を入力して、認証用のすべての RADIUS サーバのリストを使用します。 **（注）** コマンドライン ヘルプ ストリングではその他のキーワードが表示されても、サポートされるのは **group radius** キーワードだけです。
ステップ 4	**interface** *interface-id*	クライアントに接続されたポートの中で、IEEE 802.1x 認証をイネーブルにするものを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access**	ポートをアクセス モードに設定します。
ステップ 6	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	違反モードを設定します。キーワードの意味は次のとおりです。 • **shutdown**：ポートをエラー ディセーブルにします。 • **restrict**：Syslog エラーを生成します。 • **protect**：トラフィックをポートに送信する新しいデバイスからのパケットを破棄します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show dot1x**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x 認証の設定

802.1x ポートベースの認証を設定するには、AAA をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。

VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

802.1x AAA プロセスは次のとおりです。

ステップ 1　ユーザがスイッチ上のポートに接続します。

ステップ 2　認証が実行されます。

ステップ 3　RADIUS サーバ設定に基づいて VLAN 割り当てが適切にイネーブルになります。

ステップ 4　スイッチが開始メッセージをアカウンティング サーバに送信します。

ステップ 5　必要に応じて再認証が実行されます。

ステップ 6　再認証結果に基づいて、スイッチが暫定的なアカウンティング アップデートをアカウンティング サーバに送信します。

ステップ 7　ユーザがポートから切断されます。

ステップ 8　スイッチが停止メッセージをアカウンティング サーバに送信します。

802.1x ポートベースの認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定*されない*場合に使用されるデフォルトのリストを作成するには、キーワード **default** の後ろにデフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、キーワード **group radius** を入力して、認証用のすべての RADIUS サーバのリストを使用します。 **（注）** コマンドライン ヘルプ ストリングではその他のキーワードが表示されても、サポートされるのは **group radius** キーワードだけです。
ステップ 4	**dot1x system-auth-control**	スイッチで 802.1x 認証をグローバルにイネーブルにします。
ステップ 5	**aaa authorization network** {**default**} **group radius**	（任意）VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。
ステップ 6	**interface** *interface-id*	クライアントに接続されたポートの中で、802.1x 認証をイネーブルにするものを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**dot1x port-control auto**	ポート上で 802.1x 認証をイネーブルにします。 機能の相互作用の詳細については、「802.1x 設定時の注意事項」（P.9-13）を参照してください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show dot1x**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチと RADIUS サーバ間通信を設定する方法

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、あるいは IP アドレスと特定の UDP ポート番号で識別します。IP アドレスと UDP ポート番号の組み合せにより、一意の識別子が作成され、これにより、サーバ上の同一の IP アドレスの複数の UDP ポートに RADIUS 要求を送信できます。同一の RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス（たとえば、認証）を設定している場合、あとから設定されたホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。RADIUS のホスト エントリは、設定された順序で試されます。

スイッチ上に RADIUS サーバ パラメータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	RADIUS サーバ パラメータを設定します。 *hostname* |*ip-address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1812 です。指定できる範囲は 0 ～ 65536 です。 **key** *string* には、スイッチと RADIUS サーバ上で稼動する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。 **（注）** 先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されるため、鍵は必ず **radius-server host** コマンド構文の最後の項目として設定してください。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。この鍵は、RADIUS デーモン上で使用する暗号と照合する必要があります。 RADIUS サーバを複数使用する場合は、このコマンドを繰り返し入力してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次の例は、IP アドレスが 172.20.39.46 のサーバを RADIUS サーバとして照合し、ポート 1612 を許可ポートとして使用し、暗号化鍵を RADIUS サーバ上の鍵と *rad123* に設定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

radius-server host グローバル コンフィギュレーション コマンドを使用すると、すべての RADIUS サーバに対してタイムアウト、再送信、および暗号化鍵の値をグローバルに設定できます。サーバ単位でこれらのオプションを設定する場合は、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバに対する設定」（P.8-29）を参照してください。

さらに、RADIUS サーバでいくつかの設定を行う必要があります。この設定とは、スイッチの IP アドレス、およびサーバとスイッチで共有するキー ストリングです。詳細については、RADIUS サーバのマニュアルを参照してください。

定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにして、その発生間隔を指定できます。再認証の間隔を指定しなかった場合は、再認証は 3600 秒ごとに行われます。

クライアントの定期的な再認証をイネーブルにして、再認証を試行する間隔（秒数）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x reauthentication**	デフォルトではディセーブルに設定されている定期的な再認証をイネーブルにします。
ステップ 4	**dot1x timeout reauth-period** *seconds*	再認証の間隔（秒）を指定します。 指定できる範囲は 1 ～ 65,535 秒で、デフォルトは 3600 秒です。 定期的な再認証がイネーブルに設定されている場合にだけ、このコマンドはスイッチの動作に影響します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

定期的な再認証をディセーブルにするには、**no dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの再認証試行間隔に戻すには、**no dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、定期的再認証をイネーブルにし、再認証を試行する間隔を 4000 秒に設定します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

手動によるポート接続クライアントの再認証

dot1x re-authenticate interface *interface-id* 特権 EXEC コマンドを使用すると、特定のポートに接続しているクライアントを手動でいつでも再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする場合は、「定期的な再認証の設定」（P.9-18）を参照してください。

次に、ポートに接続したクライアントを手動で再認証する方法を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet0/1
```

待機時間の変更

スイッチがクライアントを認証できなかった場合は、スイッチは一定時間アイドル状態を続けたあと、再試行します。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドを使用すると、アイドル時間を制御できます。クライアントが無効なパスワードを提供したため、クライアントの認証失敗が起こる可能性があります。デフォルトより小さい数値を入力することで、ユーザに対する応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

	コマンド	目的
ステップ 3	**dot1x timeout quiet-period** *seconds*	クライアントとの認証交換が失敗したあと、スイッチが待機ステートにある秒数を設定します。 指定できる範囲は 1 ～ 65535 秒で、デフォルトは 60 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの待機時間に戻すには、**no dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、スイッチ上の待機時間を 30 秒に設定します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

スイッチとクライアント間の再送信時間の変更

クライアントは、スイッチからの EAP 要求/ID フレームに、EAP 応答/ID フレームで応答します。スイッチはこの応答を受信しなかった場合、一定時間（再送信時間）待機してから、フレームを再送信します。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x timeout tx-period** *seconds*	スイッチがクライアントからの EAP 要求/ID フレームに対する応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒で、デフォルトは 30 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1xinterface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの再送信時間に戻すには、**no dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、スイッチがクライアントからの EAP 要求/ID フレームに対する応答を待ち、要求を再送信するまでの秒数を 60 秒に設定します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

スイッチとクライアント間のフレーム再送信回数の設定

スイッチとクライアント間の再送信時間の変更だけでなく、（応答を受信しなかった場合）認証プロセスを再開するまでに、スイッチがクライアントに EAP フレームを送信する回数を変更できます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチとクライアント間のフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count*	スイッチが、認証プロセスを再開するまでに EAP フレームをクライアントに送信する回数を設定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの再送信回数に戻すには、**no dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、認証プロセスを再開するまでに、スイッチが EAP 要求を送信する回数を 5 に設定します。

```
Switch(config-if)# dot1x max-req 5
```

再認証回数の設定

スイッチが、ポートが未許可ステートに変わるまでに認証プロセスを再始動する回数を変更できます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

	コマンド	目的
ステップ 3	**dot1x max-reauth-req** *count*	スイッチが、ポートが未許可ステートに変わるまでに認証プロセスを再始動する回数を設定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの再認証回数に戻すには、**no dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

```
Switch(config-if)# dot1x max-reauth-req 4
```

ホスト モードの設定

dot1x port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	複数のホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x host-mode multi-host**	802.1x 許可ポート上で、複数のホスト（クライアント）を許可します。 指定されたインターフェイスについて、**dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

dot1x host-mode single-host インターフェイス コンフィギュレーション コマンドを入力して、インターフェイスを、ポート上の単一ホストを許可するように設定します。

（注）　**dot1x host-mode multi-domain** インターフェイス コンフィギュレーション コマンドは、コマンドライン インターフェイスのヘルプには表示されますが、サポートされていません。インターフェイス上でこのコマンドを設定すると、インターフェイスがエラー ディセーブル ステートになります。

ポート上の複数ホストをディセーブルにするには、**no dot1x host-mode multi-host** インターフェイス コンフィギュレーション コマンドを使用します。

次に、802.1x をイネーブルにし、複数のホストを許可する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
```

```
Switch(config-if)# dot1x host-mode multi-host
```

802.1x 設定をデフォルト値にリセットする方法

802.1x 設定をデフォルト値にリセットするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	**dot1x default**	設定可能な 802.1x パラメータをデフォルト値にリセットします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x アカウンティングの設定

AAA システム アカウンティングと 802.1x アカウンティングをイネーブルにすることにより、ロギング用にシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。これにより、サーバはすべてのアクティブ 802.1x セッションが閉じていることを推測できます。

RADIUS は信頼性のない UDP トランスポート プロトコルを使用するため、ネットワークの状態が悪いとアカウンティング メッセージが消失する場合があります。設定されたアカウンティング要求の再送信回数を超えてもスイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、このシステム メッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

停止メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） 開始、停止、暫定的な更新メッセージ、およびタイム スタンプのロギングなどの、アカウンティング タスクを実行するように RADIUS サーバを設定する必要があります。この機能をオンにするには、RADIUS サーバのネットワーク設定タブにある「Update/Watchdog packets from this AAA client」のロギングをイネーブルにします。次に、RADIUS サーバのシステム設定タブの「CVS RADIUS Accounting」をイネーブルにします。

AAA をスイッチでイネーブルにしたあとで 802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

	コマンド	目的
ステップ 3	**aaa accounting dot1x default start-stop group radius**	すべての RADIUS サーバのリストを使用して 802.1x アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting system default start-stop group radius**	（任意）（すべての RADIUS サーバのリストを使用して）システム アカウンティングをイネーブルにして、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アカウンティング応答メッセージを受信しない RADIUS メッセージ数を表示するには、**show radius statistics** 特権 EXEC コマンドを使用します。

次に、802.1x アカウンティングを設定する例を示します。最初のコマンドは RADIUS サーバを設定し、1813 をアカウンティング用の UDP ポートに指定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

802.1x ユーザ分散の設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、グローバル コンフィギュレーションで次の手順を実行します。

	コマンド	目的
ステップ 1	**vlan group** *vlan-group-name* ***vlan-list*** *vlan-list*	VLAN グループを設定して、単一の VLAN または一連の VLAN をそのグループにマッピングします。
ステップ 2	**show vlan group all** *vlan-group-name*	設定を確認します。
ステップ 3	**no vlan group** ***vlan-group-name*** **vlan-list** ***vlan-list***	VLAN グループ設定、または VLAN グループ設定の要素を消去します。

次の例では、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループの設定と、指定した VLAN に対するマッピングを確認する方法を示します。

```
switch(config)# vlan group eng-dept vlan-list 10

switch(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
switch# show dot1x vlan-group all
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
hr-dept                         20
```

次の例では、VLAN を既存の VLAN グループに追加し、その VLAN が追加されたことを確認する方法を示します。

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
```

```
-------------                    --------------
eng-dept                         10,30
```

次の例では、VLAN グループから VLAN を削除する方法を示します。

```
switch# no vlan group eng-dept vlan-list 10
```

次の例では、VLAN グループからすべての VLAN を消去すると、その VLAN グループが消去されることを示します。

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

switch(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループを消去する方法を示します。

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

オーセンティケータおよび、NEAT を使用したサプリカント スイッチの設定

この機能を設定するには、ワイヤリング クローゼットの外部にある 1 つのスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続されていることが必要です。

概要については、「ネットワーク エッジ アクセス トポロジ（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ」（P.9-10）を参照してください。

（注） *cisco-av-pair* は、ACS 上で *device-traffic-class=switch* として設定する必要があります。これにより、サプリカントの認証が成功した後に、インターフェイスがトランクとして設定されます。

スイッチをオーセンティケータとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	ポート モードを**アクセス**に設定します。
ステップ 5	**authentication port-control auto**	ポート認証モードを自動に設定します。
ステップ 6	**dot1x pae authenticator**	インターフェイスを Port Access Entity（PAE）オーセンティケータとして設定します。
ステップ 7	**spanning-tree portfast**	単一のワークステーションまたはサーバに接続されたアクセス ポートで PortFast をイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id*	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチを 802.1x オーセンティケータとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

スイッチをサプリカントとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile*	802.1x 証明書プロファイルを作成します。これは、サプリカントとして設定されたポートに付加する必要があります。
ステップ 4	**username** *suppswitch*	ユーザ名を作成します。
ステップ 5	**password** *password*	新しいユーザ名のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast**	スイッチによってユニキャストまたはマルチキャスト パケットが受信されたときに、強制的にマルチキャスト EAPOL パケット*だけ*が送信されるように、そのスイッチを設定します。 これにより、すべてのホスト モードで NEAT がサプリカント スイッチ上で動作することも可能となります。
ステップ 7	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport trunk encapsulation dot1q**	ポートをトランク モードに設定します。
ステップ 9	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant**	インターフェイスを Port Access Entity（PAE）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name*	802.1x 証明書プロファイルをインターフェイスに付加します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show running-config interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

ASP を使用した NEAT の設定

スイッチ VSA ではなく、AutoSmart Ports ユーザ定義マクロを使用してオーセンティケータ スイッチを設定することも可能です。詳細については、第 11 章「コマンド マクロの設定」を参照してください。

802.1x 統計情報およびステータスの表示

すべてのポートの 802.1x 統計情報を表示するには、**show dot1x all statistics** 特権 EXEC コマンドを使用します。特定のポートの 802.1x 統計情報を表示するには、**show dot1x statistics interface** *interface-id* 特権 EXEC コマンドを使用します。

スイッチについて 802.1x 管理および動作のステータスを表示するには、**show dot1x all** 特権 EXEC コマンドを使用します。特定のポートの 802.1x 管理および動作のステータスを表示するには、**show dot1x interface** *interface-id* 特権 EXEC コマンドを使用します。

表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 10

インターフェイスの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにおける各種インターフェイスのタイプとその設定方法について説明します。

- 「インターフェイス タイプの概要」（P.10-1）
- 「インターフェイス コンフィギュレーション モードの使用方法」（P.10-8）
- 「イーサネット管理ポートの使用方法」（P.10-13）
- 「イーサネット インターフェイスの設定」（P.10-16）
- 「レイヤ 3 インターフェイスの設定」（P.10-27）
- 「システム MTU の設定」（P.10-29）
- 「インターフェイスのモニタおよびメンテナンス」（P.10-31）

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチのコマンド リファレンス、およびオンラインの『*Cisco IOS Interface Command Reference*』Release12.2 を参照してください。

インターフェイス タイプの概要

ここでは、各種インターフェイス タイプの設定に関する詳細情報が記載された章についても言及しながら、スイッチによってサポートされるこれらのインターフェイス タイプについて説明します。また、物理インターフェイス特性の設定手順についても説明します。

- 「UNI、NNI、および ENI の各ポート タイプ」（P.10-2）
- 「ポートベースの VLAN」（P.10-3）
- 「スイッチ ポート」（P.10-4）
- 「ルーテッド ポート」（P.10-5）
- 「スイッチ ポート」（P.10-4）
- 「スイッチ仮想インターフェイス」（P.10-6）
- 「EtherChannel ポート グループ」（P.10-7）
- 「デュアルパーパス ポート」（P.10-7）
- 「インターフェイスの接続」（P.10-8）

UNI、NNI、および ENI の各ポート タイプ

Cisco ME スイッチは、User-Network Interface（UNI; ユーザ ネットワーク インターフェイス）、Network Node Interface（NNI; ネットワーク ノード インターフェイス）、および Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）をサポートしています。UNI は通常、PC や Cisco IP Phone などのホストに接続されます。NNI は通常、ルータまたは別のスイッチに接続されます。ENI は、機能的には UNI と同じですが、設定により Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）、Link Layer Discovery Protocol（LLDP; リンク レイヤ検出プロトコル）、および EtherChannel の Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）または Port Aggregation Protocol（PAgP; ポート集約プロトコル）用のプロトコル制御パケットをサポートできます。デフォルトでは、10/100 ポートおよびデュアルパーパス ポートは UNI として設定され、Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）専用モジュール アップリンク ポートは NNI として設定されます。デフォルトで ENI として設定されるポートはありません。

（注）　Cisco ME 3400E-24TS-M スイッチでは、デフォルトで NNI として設定されるデュアルパーパス ポートがアップリンク ポートの役割を果たします。

メトロ アクセス イメージが実行されているスイッチ上では、同時に NNI として設定できるポートは 4 つまでです。メトロ IP アクセス イメージが実行されているスイッチ上では、設定できる NNI の数に制限はありません。スイッチ上のすべてのポートを UNI または ENI として設定することもできます。

UNI または ENI のデフォルト ステートは、スイッチを設定する場合に無許可のユーザが他のポートにアクセスするのを防止するため、管理上のダウンとなっています。トラフィックはこれらのポート間ではスイッチングされません。また、UNI または ENI に着信するすべてのトラフィックは、ユーザが別のユーザのプライベート ネットワークにアクセスするのを防止するため、NNI から発信される必要があります。スイッチ内でトラフィックを 2 つ以上の UNI または ENI により交換するのが適切であれば、この UNI および ENI はコミュニティ VLAN に割り当てられます。コミュニティ VLAN の設定手順については、第 12 章「VLAN の設定」を参照してください。

（注）　UNI または ENI のデフォルト ステートがシャットダウンである場合でも、**default interface** *interface-id* コマンドを入力すると、ポートはイネーブル ステートに変更されます。

NNI のデフォルト ステータスは管理上アップであり、サービス プロバイダーは初期設定時にリモート スイッチへのアクセスを許可されます。

ポートは、UNI から NNI または ENI へ再設定することも、NNI または ENI から UNI へ再設定することも可能です。別のインターフェイス タイプとして再設定されるポートは、現在のインターフェイス タイプの特性をすべて継承します。UNI または ENI であるポートを NNI に再設定した場合、そのポートがアクティブになるためには、あらかじめそのポートをイネーブルにしておく必要があります。

ポート タイプを UNI から ENI に変更しても、そのポートの管理ステートは影響を受けません。ステータスがシャットダウンである UNI は、ENI として再設定しても、そのステータスはシャットダウンのままです。また、非シャットダウン ステートにあるポートは、その非シャットダウン ステートが維持されます。Cisco ME スイッチ上の各ポートは常に、UNI、NNI、ENI のいずれかになります。

ポートベースの VLAN

VLAN は、ユーザの物理的な位置に関係なく、機能、チーム、またはアプリケーションによって論理的に分割されたスイッチド ネットワークです。VLAN の詳細については、第 12 章「VLAN の設定」を参照してください。ポートで受信したパケットが転送されるのは、その受信ポートと同じ VLAN に属するポートに限られます。異なる VLAN 上のネットワーク デバイスは、VLAN 間でトラフィックをルーティングするレイヤ 3 のデバイスがなければ、お互いに通信することができません。

VLAN パーティションはトラフィックに対する堅固なファイアウォールを VLAN 内で実現します。また、各 VLAN には固有の MAC アドレス テーブルがあります。VLAN が成立するのは、ローカル ポートが VLAN ID に関連付けられた場合、またはユーザが VLAN ID を作成した場合です。

サービス プロバイダー ネットワークの各カスタマーの VLAN を分離するため、Cisco ME スイッチでは UNI-ENI VLAN が使用されます。UNI-ENI VLAN により、スイッチ上の UNI または ENI と、カスタマーの VLAN に属する UNI または ENI が分離されます。UNI-ENI VLAN には 2 種類あります。

- UNI-ENI 独立 VLAN：これは、スイッチ上で作成されるすべての VLAN のデフォルト VLAN ステートです。同一の UNI-ENI 独立 VLAN に属するスイッチでは、UNI または ENI 間のローカル スイッチングが実行されません。
- UNI-ENI コミュニティ VLAN：同一の UNI コミュニティ VLAN に属するスイッチ上の UNI および ENI 間で、ローカル スイッチングが許可されます。UNI または ENI が同一カスタマーに属する場合に、ポート間でパケットをスイッチングするには、UNI-ENI コミュニティ VLAN として共通の VLAN を設定できます。

（注）　ローカル スイッチングは、同一コミュニティ VLAN の ENI および UNI との間で行われます。スパニング ツリーは UNI ではなく ENI でイネーブルに設定できるため、同一コミュニティ VLAN で ENI および UNI を設定する場合は注意が必要です。UNI は常に、フォワーディング ステートです。

UNI VLAN の詳細については、「UNI-ENI VLAN」（P.12-5）を参照してください。

VLAN を設定するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して、VLAN コンフィギュレーション モードを開始します。VLAN ID が 1 ～ 1005 の VLAN 設定は VLAN データベースに保存されます。拡張範囲 VLAN（VLAN ID が 1006 ～ 4094）は VLAN データベースに追加されません。VLAN の設定はスイッチの実行コンフィギュレーションに保存されます。また、**copy running-config startup-config** 特権 EXEC コマンドを実行することにより、スイッチのスタートアップ コンフィギュレーション ファイルにも保存できます。

switchport インターフェイス コンフィギュレーション コマンドを使用すると、VLAN にポートが追加されます。

- インターフェイスを特定します。
- トランクポートには、トランク特性を設定し、必要に応じて所属できる VLAN を定義します。
- アクセス ポートには、所属する VLAN を設定して定義します。
- トンネル ポートの場合は、カスタマー固有の VLAN タグ用に VLAN ID の設定と定義を行います。第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

スイッチ ポート

スイッチ ポートは、物理ポートに対応付けられたレイヤ 2 専用インターフェイスです。スイッチ ポートは 1 つまたは複数の VLAN に属しています。スイッチ ポートは、アクセス ポート、トランク ポート、プライベート VLAN ポート、またはトンネル ポートのいずれかになります。各ポートは、アクセス ポートまたはトランク ポートとして設定できます。プライベート VLAN ポートは、プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN に属するホストまたはプロミスキャス ポートとして設定します （NNI に限り、プロミスキャス ポートとして設定できます）。トンネル ポートは手動操作により、IEEE 802.1Q トランク ポートに接続した非対称リンクの一部として設定する必要があります。スイッチ ポートは、物理インターフェイスおよび対応レイヤ 2 プロトコルの管理に使用され、ルーティングやブリッジングの処理は行いません。

スイッチ ポートは、**switchport** インターフェイス コンフィギュレーション コマンドを使用して設定します。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにするには、no キーワードを指定した **switchport** コマンドを使用します。

（注）　レイヤ 3 モードのインターフェイスをレイヤ 2 モードにすると、その対象となったインターフェイスに関するそれまでの設定情報が消失することがあります。その場合、インターフェイスはデフォルト設定に戻ります。

アクセス ポート特性およびトランク ポート特性の詳細については、第 12 章「VLAN の設定」を参照してください。トンネル ポートの詳細については、第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

アクセス ポート

各アクセス ポートは、ただ 1 つの VLAN に属し、そのトラフィックを伝送します。トラフィックは、VLAN タギングのないネイティブ フォーマットで送受信されます。アクセス ポートに着信したトラフィックは、ポートに割り当てられた VLAN に属すると見なされます。アクセス ポートで IEEE 802.1Q タグ付きパケットを受信した場合、そのパケットは廃棄され、送信元アドレスは学習されません。また、VLAN 割り当てには IEEE 802.1X も使用されます。

サポートされているアクセス ポートは 2 種類です。

- スタティック アクセス ポートは、手動で VLAN に割り当てます。
- ダイナミック アクセス ポートの VLAN メンバーシップは、着信パケットを通じて学習されます。デフォルトでは、ダイナミック アクセス ポートはどの VLAN のメンバーでもなく、ポートとの間での転送はポートの VLAN メンバーシップが検出されたときにだけイネーブルになります。UNI は、イネーブルになるとすぐにパケット転送を開始します。スイッチのダイナミック アクセス ポートは、VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）によって VLAN に割り当てられます。VMPS には Catalyst 6500 シリーズ スイッチを使用できますが、VMPS サーバとしては Cisco ME スイッチを使用できません。VMPS のダイナミック アクセス ポートは、UNI および ENI に限りサポートされます。

トランク ポート

IEEE 802.1Q トランク ポートは複数の VLAN のトラフィックを搬送し、デフォルトでは VLAN データベース内のすべての VLAN のメンバーとなります。トランク ポートは、タグ付きトラフィックおよびタグなしトラフィックを同時にサポートします。IEEE 802.1Q トランク ポートには、デフォルトの Port VLAN ID（PVID; ポート VLAN ID）が割り当てられます。タグなしトラフィックはすべてデフォルト PVID のポート上を流れます。NULL VLAN ID を備えたタグなしトラフィックおよびタグ付

きトラフィックはすべて、デフォルト PVID のポートに属すると見なされます。発信ポートのデフォルト PVID と等しい VLAN ID を持つパケットは、タグなしで送信されます。それ以外のトラフィックはすべて、VLAN タグ付きで送信されます。

デフォルトでは、トランク ポートは複数の VLAN のメンバーですが、トランク ポートごとに VLAN の許可リストを設定することで、VLAN メンバーシップを制限できます。許可 VLAN のリストは、その他のポートには影響を与えませんが、対応トランク ポートには影響を与えます。デフォルトでは、存在しうる VLAN（VLAN ID が 1 ～ 4094）はすべて、許可リスト内にあります。トランク ポートは、VLAN がイネーブル ステートにある場合に限り、VLAN のメンバーとなります。

トランク ポートの詳細については、第 12 章「VLAN の設定」を参照してください。

トンネル ポート

トンネル ポートは IEEE 802.1Q トンネリングで使用されます。このトンネリングにより、サービス プロバイダー ネットワーク内のカスタマーのトラフィックを、同じ VLAN 番号を使用するその他のカスタマーから分離できます。サービス プロバイダー エッジ スイッチのトンネル ポートからカスタマーのスイッチの IEEE 802.1Q トランク ポートには非対称リンクを設定します。エッジ スイッチのトンネル ポートに入るパケットは、すでにカスタマーの VLAN で IEEE802.1Q タグが付けられていますが、さらに IEEE 802.1Q タグの別のレイヤ（メトロ タグと呼ばれる）でカプセル化されます。またこのパケットには、カスタマーごとにサービス プロバイダー ネットワーク内で一意の VLAN ID が含まれます。タグが二重に付いたパケットは、元のカスタマーの VLAN をその他のカスタマーの VLAN から分離した状態で、サービス プロバイダー ネットワークを通過します。発信インターフェイスおよびトンネル ポートでは、メトロ タグが削除され、カスタマーのネットワークの元の VLAN 番号が取得されます。

トンネル ポートは、トランク ポートまたはアクセス ポートにすることができず、それぞれのカスタマーに固有の VLAN に属す必要があります。

トンネル ポートの詳細については、第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

ルーテッド ポート

ルーテッド ポートは物理ポートであり、ルータ上にあるポートと同じように動作しますが、ルータに接続されている必要はありません。ルーテッド ポートは、アクセス ポートとは異なり、特定の VLAN に対応付けられていません。VLAN サブインターフェイスをサポートしない点を除けば、通常のルータ インターフェイスと同じように動作します。ルーテッド ポートは、レイヤ 3 ルーティング プロトコルで設定できます。ルーテッド ポートはレイヤ 3 インターフェイス専用で、Spanning-Tree Protocol（STP; スパニングツリー プロトコル）などのレイヤ 2 プロトコルはサポートしていません。

ルーテッド ポートを設定するには、**no switchport** インターフェイス コンフィギュレーション コマンドでインターフェイスをレイヤ 3 モードにします。次に、ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、**ip routing** および **router** *protocol* の各グローバル コンフィギュレーション コマンドを使用してルーティング プロトコルの特性を指定します。

（注）　**no switchport** インターフェイス コンフィギュレーション コマンドを実行すると、インターフェイスが一度シャットダウンしてから再度イネーブルになります。このとき、インターフェイスが接続しているデバイスについてのメッセージが表示されることがあります。レイヤ 2 モードのインターフェイスをレイヤ 3 モードにすると、その対象となったインターフェイスに関するそれまでの設定情報が消失する場合があります。

ソフトウェアに、設定できるルーテッド ポートの個数制限はありません。ただし、ハードウェアには限界があるため、この個数と設定されている他の機能の数との組み合せによっては、CPU パフォーマンスに影響する場合もあります。ハードウェアのリソース制限に達するとどうなるかについては、「レイヤ 3 インターフェイスの設定」（P.10-27）を参照してください。

IP ユニキャストおよびマルチキャストのルーティングおよびルーティング プロトコルの詳細については、第 36 章「IP ユニキャスト ルーティングの設定」および第 44 章「IP マルチキャスト ルーティングの設定」を参照してください。

（注）　フル レイヤ 3 ルーティングの場合は、スイッチにメトロ IP アクセス イメージをインストールする必要があります。

イーサネット管理ポート

イーサネット管理ポート（*Fa0 ポートまたは fastethernet0 ポートとも呼ばれる*）は、PC に接続できるレイヤ 3 ホスト ポートです。ネットワーク管理を行う場合には、スイッチ コンソール ポートの代わりにイーサネット管理ポートを使用できます。

詳細については、「イーサネット管理ポートの使用方法」（P.10-13）を参照してください。

スイッチ仮想インターフェイス

Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）は、スイッチ ポートの VLAN を、システムのルーティング機能またはブリッジング機能に対する 1 つのインターフェイスとして表します。1 つの VLAN に対応付けできるのは 1 つの SVI だけです。VLAN に SVI を設定する必要があるのは、VLAN 間でルーティングする場合、またはスイッチと IP ホストの接続を行う場合に限られます。デフォルトでは、リモート スイッチ管理が行えるように、デフォルト VLAN（VLAN 1）用に SVI が作成されます。追加の SVI は明示的に設定する必要があります。

（注）　インターフェイス VLAN 1 は削除できません。

SVI はシステムにしか IP ホスト接続を行いません。レイヤ 3 モードでは、SVI 全体にルーティングを設定できます。

スイッチは合計 1005 の VLAN（および SVI）をサポートしますが、ハードウェアには限界があるため、SVI とルーテッド ポートの数および設定されている他の機能の数との組み合せによっては、CPU のパフォーマンスに影響する場合もあります。ハードウェアのリソース制限に達するとどうなるかについては、「レイヤ 3 インターフェイスの設定」（P.10-27）を参照してください。

SVI は、VLAN インターフェイスに対する **vlan** インターフェイス コンフィギュレーション コマンドの初回実行時に作成されます。VLAN は、IEEE802.1Q カプセル化トランク上のデータ フレームに関連付けられた VLAN タグ、あるいはアクセス ポート用に設定された VLAN ID に対応します。トラフィックをルーティングするそれぞれの VLAN に対して VLAN インターフェイスを設定し、そのインターフェイスに IP アドレスを割り当ててください。詳細については、「手動での IP 情報の割り当て」（P.3-15）を参照してください。

（注）　物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

SVI は、さまざまなルーティング プロトコルをサポートします。IP ルーティング設定の詳細については、第 36 章「IP ユニキャスト ルーティングの設定」および第 44 章「IP マルチキャスト ルーティングの設定」を参照してください。

（注）　ルーテッド ポート（または SVI）は、スイッチ上にメトロ IP アクセス イメージがインストールされている場合に限りサポートされます。

EtherChannel ポート グループ

EtherChannel ポート グループは、複数のスイッチ ポートを 1 つのスイッチ ポートとして取り扱います。このようなポート グループは、スイッチ間、またはスイッチおよびサーバ間で広帯域接続を行う単一論理ポートとして動作します。EtherChannel では、チャネルのリンク全体でトラフィックのロード バランシングが行われます。EtherChannel 内のリンクに障害が発生した場合、そのリンクで搬送されていたトラフィックは、その他のリンクで搬送されます。複数のトランク ポートを 1 つの論理トランク ポートに、複数のアクセス ポートを 1 つの論理アクセス ポートに、複数のトンネル ポートを 1 つの論理トンネル ポートに、複数のルーテッド ポートを 1 つの論理ルーテッド ポートにまとめることができます。大半のプロトコルは、単一ポートまたは集約スイッチ ポートで動作し、ポート グループ内の物理ポートを認識しません。ただし、CDP、LACP、および PAgP は例外です。これらのプロトコルは、NNI または ENI の各物理ポート上でしか動作しません。

EtherChannel を設定する場合は、ポートチャネル論理インターフェイスを作成し、EtherChannel にインターフェイスを割り当てます。レイヤ 3 インターフェイスの場合は、**interface port-channel** グローバル コンフィギュレーション コマンドを使用して手動で論理インターフェイスを作成します。そのあと、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。レイヤ 2 インターフェイスの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用することで、ポートチャネル論理インターフェイスをダイナミックに作成します。このコマンドにより、物理ポートと論理ポートがバインドされます。詳細については、第 35 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

デュアルパーパス ポート

各デュアルパーパス ポートは、デュアル フロント エンド（RJ-45 コネクタおよび SFP モジュール コネクタ）を持つ単一のインターフェイスと見なされます。デュアル フロント エンドは、冗長インターフェイスではありません。スイッチによりアクティブになるのは、このペアの一方のコネクタだけです。

デフォルトでは、デュアルパーパス ポートは UNI、SFP 専用モジュール ポートは NNI です。デフォルトでは、最初にリンク アップするデュアルパーパス ポートのメディア タイプは、スイッチによりダイナミックに選択されます。ただし、**media-type** インターフェイス コンフィギュレーション コマンドを使用すれば、RJ-45 コネクタまたは SFP モジュール コネクタを手動で選択できます。デュアルパーパス ポート設定の詳細については、「デュアルパーパス ポートの設定」（P.10-22）を参照してください。

各デュアルパーパス ポートには 2 つの LED があります。1 つは SFP モジュール ポートのステータスを示し、もう 1 つは RJ-45 ポートのステータスを示します。ポート LED は、いずれかのコネクタがアクティブの場合にオンになります。LED の詳細については、ハードウェア インストレーション ガイドを参照してください。

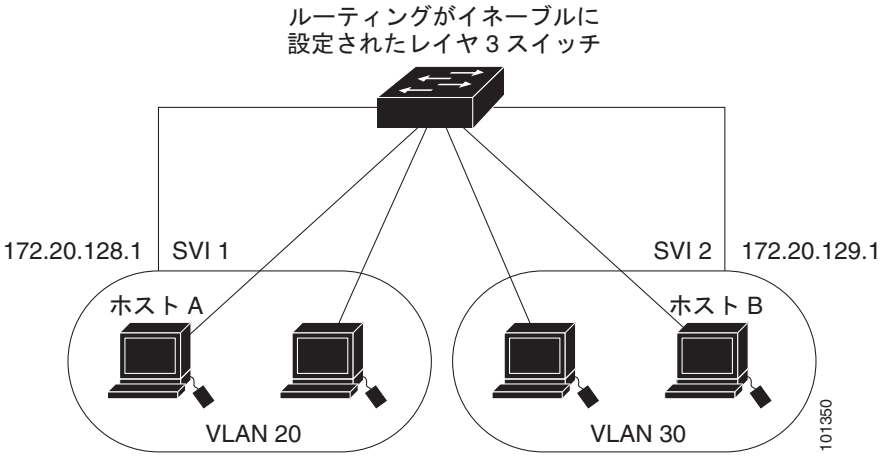
インターフェイスの接続

同一 VLAN 内のデバイスは、スイッチを介して直接通信できます。異なる VLAN のポートは、ルーティング デバイスを介さなければデータを交換できません。標準のレイヤ 2 スイッチを使用している場合、異なる VLAN のポートは、ルータを通じて情報を交換する必要があります。

デフォルトでは、Cisco ME スイッチは UNI または ENI の間で VLAN を分離します。UNI および ENI の間でトラフィックを交換するには、それらの UNI および ENI が NNI に変更されるか、または同じ UNI-ENI コミュニティ VLAN に割り当てられることが必要です。

ルーティングがイネーブルに設定されたスイッチを使用することにより、IP アドレスを割り当てた SVI で VLAN 20 および VLAN 30 の両方を設定すると、外部ルータを使用せずに、スイッチを介してパケットをホスト A からホスト B に直接送信できます（図 10-1 を参照）。

図 10-1　　スイッチと VLAN との接続



メトロ IP アクセス イメージが稼動しているスイッチ上では、ルーティングをイネーブルにできます。高いパフォーマンスを維持するため、可能な場合は常にスイッチ ハードウェアによって転送を行います。ただし、ハードウェア内をルーティングできるのは、イーサネット II カプセル化機能を備えた IP バージョン 4 パケットだけです。ルーティング機能は、すべての SVI およびルーテッド ポートでイネーブルにできます。スイッチは、IP トラフィックだけをルーティングします。SVI またはルーテッド ポートに IP ルーティング プロトコル パラメータとアドレス設定が 追加されていれば、これらのポートで受信した IP トラフィックはすべてルーティングされます。詳細については、第 36 章「IP ユニキャスト ルーティングの設定」、第 44 章「IP マルチキャスト ルーティングの設定」、および 第 45 章「MSDP の設定」を参照してください。

インターフェイス コンフィギュレーション モードの使用方法

スイッチは、次のインターフェイス タイプをサポートします。

- 物理ポート：スイッチ ポート、ルーテッド ポート、UNI、NNI、および ENI ポート
- VLAN：SVI
- ポート チャネル：EtherChannel インターフェイス

また、インターフェイスは範囲を指定して設定することもできます（「インターフェイスの範囲設定」（P.10-10）を参照）。

物理インターフェイス（ポート）を設定するには、インターフェイスのタイプ、モジュール番号、およびスイッチ ポート番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

- タイプ：10/100 Mbps イーサネット対応のファスト イーサネット（fastethernet または fa）、10/100/1000 Mbps イーサネット ポート対応のギガビット イーサネット（gigabitethernet または gi）、または SFP モジュール ギガビット イーサネット インターフェイス
- モジュール番号：スイッチ上のモジュール番号またはスロット番号（Cisco ME スイッチでは常に 0）
- ポート番号：スイッチ上のインターフェイス番号。ポート番号は、スイッチの正面に向かって左端のポートが常に 1 になります（fastethernet 0/1、gigabitethernet 0/1 など）。インターフェイス タイプが複数ある場合（たとえば 10/100 ポートと SFP モジュール ポート）、ポート番号はインターフェイス タイプが変わるごとに 1 から始まります（gigabitethernet 0/1 など）。

物理インターフェイスは、スイッチ上の位置を物理的に調べることにより識別できます。**show** 特権 EXEC コマンドを使用して、スイッチ上の特定のインターフェイスまたはすべてのインターフェイスに関する情報を表示することもできます。以降では、主に物理インターフェイスの設定手順について説明します。

インターフェイスの設定手順

次に説明するのは、すべてのインターフェイス設定プロセスに当てはまる一般的な手順です。

ステップ 1　特権 EXEC プロンプトで、次のように **configure terminal** コマンドを入力します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

ステップ 2　**interface** グローバル コンフィギュレーション コマンドを入力します。インターフェイス タイプおよびコネクタ番号を確認します。次の例では、ファスト イーサネット ポート 1 を選択しています。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)#
```

（注）　インターフェイス タイプとインターフェイス番号の間には、必ずしもスペースを入れる必要はありません。上記の例で言えば、**fastethernet 0/1**、**fastethernet0/1**、**fa 0/1**、**fa0/1** のいずれを指定してもかまいません。

ステップ 3　UNI または ENI を設定する場合は、**no shutdown** インターフェイス コンフィギュレーション コマンドを実行して、インターフェイスをイネーブルにします。

```
Switch(config-if)# no shutdown
```

ステップ 4　各 **interface** コマンドのあとに、そのインターフェイスで必要なインターフェイス コンフィギュレーション コマンドを続けて入力します。入力するコマンドにより、そのインターフェイスで稼動するプロトコルとアプリケーションが定義されます。別のインターフェイス コマンドまたは **end** を入力して特権 EXEC モードに戻ると、これらのコマンドがまとめてインターフェイスに適用されます。

interface range グローバル コンフィギュレーション コマンドまたは **interface range macro** グローバル コンフィギュレーション コマンドを使用すれば、インターフェイスを範囲で設定することもできます。範囲を指定して設定されたインターフェイスは、同じタイプでなければならず、機能オプションも同じものを設定する必要があります。

ステップ 5　インターフェイスを設定したら、「インターフェイスのモニタおよびメンテナンス」（P.10-31）に示した **show** 特権 EXEC コマンドでそのステータスを確認してください。

show interfaces 特権 EXEC コマンドを入力すると、スイッチ上の全インターフェイスまたはスイッチ用に設定されている全インターフェイスのリストが表示されます。さらに、デバイスがサポートする各インターフェイスまたは指定されたインターフェイスのレポートを出力できます。

インターフェイスの範囲設定

interface range グローバル コンフィギュレーション コマンドを使用すると、同じコンフィギュレーション パラメータを持つ複数のインターフェイスを設定できます。インターフェイス範囲設定モードを開始すると、入力されたコマンド パラメータはすべて、このモードを終了するまで、その範囲内の全インターフェイスに対するものと見なされます。

同じパラメータを持つインターフェイスを範囲で設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** {*port-range*}	設定するインターフェイス（VLAN または物理ポート）の範囲を指定し、インターフェイス範囲設定モードを開始します。 • **interface range** コマンドを使用すると、最大 5 つのポート範囲または定義済みのマクロを設定できます。 • *port-rang* に指定する複数のポート範囲をカンマで区切る場合は、エントリごとにインターフェイス タイプを入力し、カンマの前後にスペースを入れる必要があります。 • *port-range* に指定する複数のポート範囲をハイフンで区切る場合、インターフェイス タイプを再入力する必要はありませんが、ハイフンの前にはスペースを入れる必要があります。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4		通常のコンフィギュレーション コマンドを使用して、範囲内のすべてのインターフェイスにコンフィギュレーション パラメータを適用します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*]	範囲内のインターフェイスの設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

interface range グローバル コンフィギュレーション コマンドを使用するときは、次の注意事項に留意してください。

- *port-range* の有効なエントリは次のとおりです。
  - **vlan** *vlan-ID -vlan-ID*（VLAN ID は 1 ～ 4094）
  - **fastethernet** module/{first *port*} - {*last port*}（module は常に 0）
  - **gigabitethernet** module/{*first port*} - {*last port*}（module は常に 0）

– **port-channel** *port-channel-number - port-channel-number*（*port-channel-number* は 1 ～ 48）

（注）　**interface range** コマンドにポート チャネルを指定する場合、最初と最後のポート チャネル番号はアクティブなポート チャネルの番号とします。

- **interface range** コマンドは、**interface vlan** コマンドで設定された VLAN インターフェイスに対してだけ有効です。**show running-config** 特権 EXEC コマンドを実行すると、設定済みの VLAN インターフェイスを表示できます。**show running-config** コマンドにより表示されない VLAN インターフェイスには、**interface range** コマンドは使用できません。
- 指定された範囲に含まれるインターフェイスはすべて、同じタイプ（すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN）であることが必要ですが、1 つのコマンド内で複数の範囲を組み合せることはできます。

次の例は、**interface range** グローバル コンフィギュレーション コマンドを使用して、ポート 1 および 2 の速度を 100 Mbps に設定したものです。

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 - 2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# speed 100
```

この例では、カンマを使用して別のインターフェイス タイプ ストリングを追加し、ファスト インターネット ポート 1 ～ 3 のすべてと、ギガビット イーサネット ポート 1 および 2 の両方をイネーブルにし、IEEE 802.3 X フロー制御ポーズ フレームを受信できるようにしています。

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 - 3 , gigabitethernet0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

インターフェイス範囲モードで複数のコンフィギュレーション コマンドを入力した場合、各コマンドは入力された時点で実行されます。インターフェイス範囲モードを終了した時点で、コマンドがバッチ処理されるわけではありません。コマンドの実行中にインターフェイス範囲設定モードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスに対して実行されないことがあります。インターフェイス範囲設定モードは、コマンド プロンプトが再表示されるのを待ってから終了してください。

インターフェイス範囲マクロの設定と使用方法

インターフェイス範囲マクロを作成すると、設定用のインターフェイスの範囲を自動的に選択できます。**interface range macro** グローバル コンフィギュレーション コマンド ストリングでキーワード **macro** を使用するには、まず **define interface-range** グローバル コンフィギュレーション コマンドでマクロを定義する必要があります。

インターフェイス範囲マクロを定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**define interface-range** *macro_name interface-range*	インターフェイス範囲マクロを定義して NVRAM に保存します。 • *macro_name* は、最大 32 文字の文字列です。 • マクロには、カンマで区切ったインターフェイス範囲を 5 つまで指定できます。 • それぞれの *interface-range* は、同じポート タイプで構成されている必要があります。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**interface range macro** *macro_name*	*macro_name* という名前のインターフェイス範囲マクロに保存された値を使用して、設定するインターフェイス範囲を選択します。 この時点で、通常のコンフィギュレーション コマンドを使用して、定義済みマクロ内のすべてのインターフェイスに設定を適用できます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config | include define**	定義済みインターフェイス範囲マクロの設定を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

マクロを削除する場合は、**no define interface-range** *macro_name* グローバル コンフィギュレーション コマンドを使用します。

define interface-range グローバル コンフィギュレーション コマンドを使用するときは、次の注意事項に留意してください。

- *interface-range* の有効なエントリは次のとおりです。
  - **vlan** *vlan-ID -vlan-ID*（VLAN ID は 1 ～ 4094）
  - **fastethernet** module/{first *port*} - {*last port*}（module は常に 0）
  - **gigabitethernet** module/{*first port*} - {*last port*}（module は常に 0）
  - **port-channel** *port-channel-number - port-channel-number*（*port-channel-number* は 1 ～ 48）

（注） ポート チャネルにインターフェイス範囲を使用する場合、最初と最後のポート チャネル番号はアクティブなポート チャネルの番号でなければなりません。

- *interface-range* を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。たとえば、**gigabitethernet0/1 - 2** は範囲として有効ですが、**gigabitethernet0/1-2** は無効です。
- VLAN インターフェイスは、**interface vlan** コマンドで設定済みであることが必要です。**show running-config** 特権 EXEC コマンドを実行すると、設定済みの VLAN インターフェイスを表示できます。**show running-config** コマンドによって表示されない VLAN インターフェイスは、*interface-range* としては使用できません。
- 指定された範囲に含まれるインターフェイスはすべて、同じタイプ（すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN）であることが必要ですが、1 つのマクロ内で複数のインターフェイス タイプを組み合せることはできます。

次に、ポート 1 およびポート 2 を含む *enet_list* というインターフェイス範囲を定義して、マクロ設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet0/1 - 2
Switch(config)# end
Switch# show running-config | include define
define interface-range enet_list GigabitEthernet0/1 - 2
```

次に、*macro1* という複数インターフェイス マクロを作成して、範囲内のすべてのインターフェイスを VLAN に割り当てる例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# no shut
Switch(config-if-range)# end
```

次に、インターフェイス範囲マクロ *enet_list* に対するインターフェイス範囲設定モードを開始する例を示します。

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

次に、インターフェイス範囲マクロ *enet_list* を削除し、その処理を確認する例を示します。

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

イーサネット管理ポートの使用方法

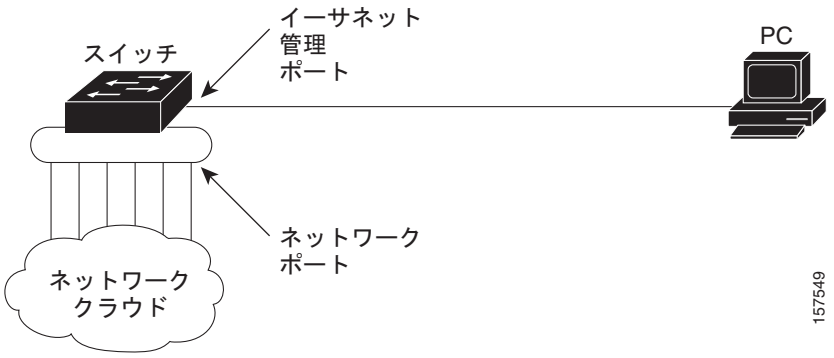
- 「イーサネット管理ポートの概要」（P.10-13）
- 「イーサネット管理ポート上でサポートされている機能」（P.10-15）
- 「イーサネット管理ポートの設定」（P.10-15）
- 「TFTP とイーサネット管理ポート」（P.10-15）

イーサネット管理ポートの概要

イーサネット管理ポート（*ポート Fa0 またはポート fastethernet0* とも呼ばれる）は、PC に接続できるレイヤ 3 ホスト ポートです。ネットワーク管理を行う場合には、スイッチ コンソール ポートの代わりにイーサネット管理ポートを使用できます。

PC をイーサネット管理ポートに接続する場合は、IP アドレスを割り当てる必要があります。図 10-2 は、イーサネット管理ポートと PC との接続方法を図示したものです。

図 10-2　スイッチの PC への接続



デフォルトでは、イーサネット管理ポートはイネーブルになっています。スイッチは、イーサネット管理ポートからネットワーク ポートへパケットをルーティングできず、ルーティングされてきたパケットをネットワーク ポートから受け取ることもできません。

イーサネット管理ポートはルーティングをサポートしていませんが、ポート上でルーティング プロトコルをイネーブルにすることが必要となる場合もあります。たとえば図 10-3 のように、PC がスイッチから 2 ホップ以上離れているため、2 つ以上のレイヤ 3 デバイスを経由しなければパケットが PC に到達できない場合には、イーサネット管理ポート上でルーティング プロトコルをイネーブルにする必要があります。

図 10-3　ルーティング プロトコルがイネーブルになったネットワークの例

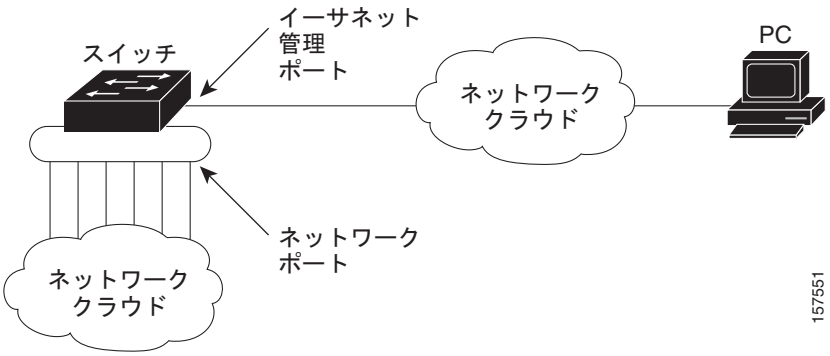


図 10-3 において、イーサネット管理ポートおよびネットワーク ポートが同じルーティング プロセスに対応付けられている場合、ルートは次のように伝播されます。

- イーサネット管理ポートからのルートは、ネットワーク ポートを経由してネットワークへ伝播される。
- ネットワーク ポートからのルートは、イーサネット管理ポートを経由してネットワークへ伝播される。

イーサネット管理ポートとネットワーク ポートの間ではルーティングがサポートされていないため、これらのポート間ではトラフィックの送受信は行えません。トラフィックの送受信が行われると、ポート間でデータ パケット ループが発生し、スイッチやネットワークの動作に不具合が生じます。イーサネット管理ポートとネットワーク ポートの間のルートを避け、ループを回避するためには、ルート フィルタを設定します。

イーサネット管理ポート上でサポートされている機能

イーサネット管理ポートでは、次の機能がサポートされています。

- パスワードを使用する Telnet
- TFTP
- セキュア シェル（SSH）
- DHCP ベースの自動設定
- SMNP（ENTITY-MIB および IF-MIB に限る）
- IP PING
- インターフェイス機能
- 速度：10 Mb/s、100 Mb/s、および自動ネゴシエーション
- デュプレックス モード：全二重、半二重、および自動ネゴシエーション
- ループバック検出
- CDP
- DHCP リレー エージェント
- IPv4 アクセス コントロール リスト（ACL）
- ルーティング プロトコル

注意　イーサネット管理ポート上で何らかの機能をイネーブルにする場合は、その機能がサポートされていることを事前に確認してください。イーサネット管理ポート上でサポートされていない機能は、設定しようとしても正常には機能しません。またその場合には、スイッチに障害が発生することがあります。

イーサネット管理ポートの設定

CLI でイーサネット管理ポートを指定するには、**fastethernet0** と入力します。

このポートをディセーブルにする場合は、**shutdown** インターフェイス コンフィギュレーション コマンドを使用します。このポートをイネーブルにする場合は、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用します。

PC へのリンク ステータスは、イーサネット管理ポートの LED で判別できます。リンクがアクティブの場合 LED は緑色に点灯し（オン）、リンクがダウンしている場合 LED は点灯しません（オフ）。POST のエラーが発生した場合 LED はオレンジ色に点灯します。

リンク ステータスを表示する場合は、**show interfaces fastethernet 0** 特権 EXEC コマンドを使用します。

TFTP とイーサネット管理ポート

表 1 のコマンドは、TFTP を使用してブートローダに設定ファイルをダウンロードまたはアップロードする際に使用します。

表 1　　ブートローダ コマンド

コマンド	説明
arp [*ip_address*]	パラメータ *ip_address* を指定しないでこのコマンドを入力すると、現在キャッシュされている ARP[1] テーブルが表示されます。 パラメータ *ip_address* を指定してこのコマンドを入力すると、ARP がイネーブルになり、指定した IP アドレスに MAC アドレスが関連付けられます。
mgmt_clr	イーサネット管理ポートに関する統計情報をクリアします。
mgmt_init	イーサネット管理ポートを起動します。
mgmt_show	イーサネット管理ポートに関する統計情報を表示します。
ping *host_ip_address*	指定したネットワーク ホストに ICMP ECHO_REQUEST パケットを送信します。
boot tftp:*/file-url ...*	実行可能イメージを TFTP サーバからロードして起動し、コマンドライン インターフェイスを開始します。 詳細については、このリリースのコマンド リファレンスを参照してください。
copy tftp:/*source-file-url* *filesystem*:/*destination-file-url*	TFTP サーバから指定した場所に Cisco IOS イメージをコピーします。 詳細については、このリリースのコマンド リファレンスを参照してください。

1. ARP = アドレス解決プロトコル。

イーサネット インターフェイスの設定

- 「イーサネット インターフェイスのデフォルト設定」（P.10-16）
- 「ポート タイプの設定」（P.10-18）
- 「インターフェイス速度とデュプレックス モードの設定」（P.10-19）
- 「デュアルパーパス ポートの設定」（P.10-22）
- 「IEEE 802.3X フロー制御の設定」（P.10-24）
- 「インターフェイスの自動 MDIX の設定」（P.10-25）
- 「インターフェイスに関する説明の追加」（P.10-26）

イーサネット インターフェイスのデフォルト設定

表 10-2 は NNI に対するイーサネット インターフェイスのデフォルト設定を、表 10-3 は、UNI および ENI に対するイーサネット インターフェイスのデフォルト設定をそれぞれまとめたものです。表に示されている VLAN パラメータの詳細については、第 12 章「VLAN の設定」を参照してください。また、ポートへのトラフィックの制御に関する詳細については、第 23 章「ポートベースのトラフィック制御の設定」を参照してください。

（注）　インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスが一度シャットダウンしてから

再度イネーブルになります。この場合、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにすると、その対象となったインターフェイスに関するそれまでの設定情報が消失することがあります。その場合、インターフェイスはデフォルト設定に戻ります。

表 10-2　NNI に対するイーサネットのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ 2 モードまたはスイッチング モード（**switchport** コマンド）。
許可 VLAN 範囲	VLAN 1 ～ 4094。
デフォルト VLAN（アクセス ポート用）	VLAN 1（レイヤ 2 インターフェイスに限る）。
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1（レイヤ 2 インターフェイスに限る）。
VLAN トランキング	スイッチ ポート モード アクセス（レイヤ 2 インターフェイスに限る）。
ポート イネーブル ステート	イネーブル。
ポート記述	定義なし。
Speed	自動ネゴシエーション。
デュプレックス モード	自動ネゴシエーション。
IEEE 802.3X フロー制御	フロー制御は **receive**: **off** に設定。送信されたパケットに対しては常に off。
EtherChannel	すべてのイーサネット ポートでディセーブル。第 35 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
ポート ブロッキング（不明のマルチキャスト トラフィックおよびユニキャスト トラフィック）	ディセーブル（ブロッキングされない）（レイヤ 2 インターフェイスに限る）。「ポート ブロッキングの設定」（P.23-7）を参照してください。
ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームの制御	ディセーブル。「ストーム制御のデフォルト設定」（P.23-3）を参照してください。
ポート セキュリティ	ディセーブル（レイヤ 2 インターフェイスに限る）。「ポート セキュリティのデフォルト設定」（P.23-10）を参照してください。
Port Fast	ディセーブル。「オプションのスパニング ツリー機能のデフォルト設定」（P.17-6）を参照してください。
自動 MDIX	イネーブル。
CDP	イネーブル。
VMPS	設定なし

表 10-3　UNI および ENI に対するイーサネットのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ 2 モードまたはスイッチング モード（**switchport** コマンド）。
許可 VLAN 範囲	VLAN 1 ～ 4094。
デフォルト VLAN（アクセス ポート用）	VLAN 1（レイヤ 2 インターフェイスに限る）。
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1（レイヤ 2 インターフェイスに限る）。
VLAN トランキング	スイッチ ポート モード アクセス（レイヤ 2 インターフェイスに限る）。
ダイナミック VLAN	イネーブル。
ポート イネーブル ステート	コンフィギュレーション ファイルが存在しない場合はディセーブル。

表 10-3　UNI および ENI に対するイーサネットのデフォルト設定 （続き）

機能	デフォルト設定
ポート記述	定義なし。
Speed	自動ネゴシエーション。
デュプレックス モード	自動ネゴシエーション。
IEEE 802.3X フロー制御	フロー制御は **receive**: **off** に設定。送信されたパケットに対しては常に off。
EtherChannel	すべてのイーサネット ポートでディセーブル。第 35 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
ポート ブロッキング（不明のマルチキャスト トラフィックおよびユニキャスト トラフィック）	ディセーブル（ブロッキングされない）（レイヤ 2 インターフェイスに限る）。「ポート ブロッキングの設定」（P.23-7）を参照してください。
ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームの制御	ディセーブル。「ストーム制御のデフォルト設定」（P.23-3）を参照してください。
ポート セキュリティ	ディセーブル（レイヤ 2 インターフェイスに限る）。「ポート セキュリティのデフォルト設定」（P.23-10）を参照してください。
自動 MDIX	イネーブル。

ポート タイプの設定

デフォルトでは、Cisco ME スイッチ上のすべての 10/100 ポートが UNI として設定され、SFP モジュール ポートが NNI として設定されます。ポート タイプを ENI に設定することもできます。ENI は、機能的には UNI と同じですが、設定により CDP、STP、LLDP、および EtherChannel の LACP および PAgP をサポートできます。

port-type インターフェイス コンフィギュレーション コマンドを使用すると、ポート タイプを変更できます。メトロ アクセス イメージが実行されているスイッチ上では、同時に NNI として設定できるポートは 4 つまでです。メトロ IP アクセス イメージが実行されているスイッチ上では、設定できる NNI の数に制限はありません。スイッチ上のすべてのポートを UNI または ENI として設定することもできます。

ポートを NNI から UNI または ENI に変更する場合、VLAN に割り当てられた設定（独立モードまたはコミュニティ モード）は継承されます。UNI-ENI 独立 VLAN および UNI-ENI コミュニティ VLAN の設定に関する詳細については、第 12 章「VLAN の設定」を参照してください。

ポートを NNI から UNI または ENI に変更した場合、あるいは UNI または ENI から NNI へ変更した場合、ポート タイプに特化した機能はすべてデフォルト設定に戻ります。STP、CDP、LLDP などのレイヤ 2 プロトコルでは、UNI および ENI に対するデフォルト設定はディセーブル（ただし ENI に対してはイネーブルにできる）、NNI に対するデフォルト設定はイネーブルです。

（注）　デフォルトの場合、スイッチは UNI および ENI 上ではキープアライブ メッセージを送信し、NNI 上では送信しません。ポート タイプを UNI または ENI から NNI、あるいは NNI から UNI または ENI に変更しても、キープアライブ ステータスに影響はありません。キープアライブ ステートをデフォルト設定から変更するには、[**no**] **keepalive** インターフェイス コンフィギュレーション コマンドを入力します。**keepalive** コマンドを引数なしで入力すると、キープアライブ パケットはデフォルトの時間間隔（10 秒）およびリトライ数（5）に基づいて送信されます。**no keepalive** コマンドを入力すると、インターフェイス上のキープアライブ パケットはディセーブルになります。

インターフェイスに対してポート タイプを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**port-type** {**eni** | **nni** | **uni**}	ポートを ENI、NNI、または UNI に変更します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id*	インターフェイスの IEEE 802.3X フロー制御設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

no port-type インターフェイス コンフィギュレーション コマンドまたは **default port-type** インターフェイス コンフィギュレーション コマンドを入力すると、ポートがデフォルト ステート（ファスト イーサネット ポートの場合は UNI、ギガビット イーサネット ポートの場合は NNI）に戻ります。

次に、ポートを UNI から NNI に変更し、その内容を実行コンフィギュレーションに保存する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# no shutdown
5d20h: %SYS-5-CONFIG_I: Configured from console by console
Switch(config-if)# end
Switch# copy running-config startup-config
```

インターフェイス速度とデュプレックス モードの設定

スイッチのイーサネット インターフェイスは、10 Mbps、100 Mbps、1000 Mbps のいずれかの速度、および全二重と半二重のどちらかのモードで動作します。全二重モードでは、2 つのステーションが同時にトラフィックを送受信できます。通常、10 Mbps ポートは半二重モードで動作します。つまり、ステーションはトラフィックの受信または送信のいずれかを交互に行います。

スイッチ モデルの中には、ファスト イーサネット（10/100 Mbps）ポート、ギガビット イーサネット（10/100/1000 Mbps）ポート、および SFP モジュールをサポートする SFP モジュール スロットを組み合せたものもあります。

ここでは、インターフェイス速度とデュプレックス モードの設定方法について説明します。

- 「速度およびデュプレックスの設定に関する注意事項」（P.10-19）
- 「インターフェイス速度およびデュプレックスに関するパラメータの設定」（P.10-20）

速度およびデュプレックスの設定に関する注意事項

インターフェイス速度とデュプレックス モードの設定時には、次の注意事項に留意してください。

- インターフェイス速度は、ファスト イーサネット（10/100 Mbps）ポートおよびギガビット イーサネット（10/100/1000 Mbps）ポート上で設定できます。ファスト イーサネット ポートは全二重モード、半二重モード、または自動ネゴシエーション モードに設定できます。ギガビット イーサ

ネット ポートは、全二重モードまたは自動ネゴシエーション モードに設定できます。ただし、ギガビット イーサネット ポートは、速度が 10 Mbps または 100 Mbps であれば半二重モードに設定することもできます。半二重モードは、1000 Mbps で動作するギガビット イーサネット ポートではサポートされていません。

- 1000 BASE-T SFP モジュールが SFP モジュール スロットに挿入されている場合を除き、SFP モジュール ポートの速度は設定できませんが、自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、速度を非ネゴシエーション（**nonegotiate**）に設定できます。

  ただし、1000BASE-T SFP モジュールが SFP モジュール スロットに挿入されている場合、速度は 10 Mbps、100 Mbps、1000 Mbps、または auto に設定できますが、**nonegotiate** には設定できません。

  100BASE-FX SFP モジュール上では、速度を **nonegotiate** に設定できません。

- SFP モジュール ポートではデュプレックス モードを設定できません。SFP モジュール ポートは、次の場合を除けば全二重モードで動作します。
  - Cisco 1000BASE-T SFP モジュールが SFP モジュール スロットに挿入されている場合は、デュプレックス モードを **auto** または **full** に設定できます。半二重モードは、**auto** 設定の場合にサポートされます。
  - Cisco 100BASE-FX SFP モジュールが SFP モジュール スロットに挿入されている場合は、デュプレックス モードを **half** または **full** に設定できます。キーワード **auto** は使用できませんが、100BASE-FX SFP モジュールでは、自動ネゴシエーションがサポートされていないため、インターフェイスを半二重モード（SFP モジュールのデフォルト）にすることができます。
- 回線の両端で自動ネゴシエーションがサポートされている場合は、デフォルトの自動ネゴシエーション（**auto**）に設定することを強く推奨します。
- 一方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしていない場合は、両方のインターフェイスでデュプレックスと速度を設定してください。ただし、サポートしている側では **auto** 設定を使用しないでください。
- STP がイネーブルになっている場合、ポートの再設定時には。スイッチがループの有無を調べるまでに 30 秒ほどかかることがあります。STP の再設定が行われている間、ポートの LED はオレンジ色に点灯します。Cisco ME スイッチの場合、NNI では STP がデフォルトでサポートされ、ENI では STP をイネーブルにできます。UNI では、STP はサポートされていません。

注意　インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再度イネーブルになる場合があります。

インターフェイス速度およびデュプレックスに関するパラメータの設定

物理インターフェイスに対して速度およびデュプレックス モードを設定するには、特権 EXEC モードで次の手順を実行します。

（注）　デュアルパーパス ポートでは、**media-type** インターフェイス コンフィギュレーション コマンドを入力してインターフェイスを変更すると、速度およびデュプレックス モードの設定が削除されます。これらのポートに対する速度設定およびデュプレックス モード設定の詳細については、「デュアルパーパス ポートの設定」（P.10-22）を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**speed** {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}	インターフェイスの適切な速度パラメータを入力します。 • **10**、**100**、**1000** のいずれかを入力し、インターフェイスの特定の速度を設定します。キーワード **1000** は、10/100/1000 Mbps ポートまたは 1000BASE-T SFP モジュールが挿入された SFP モジュール ポートに限り使用できます。 • **auto** を入力すると、インターフェイスは、接続されている装置と速度を自動ネゴシエーションできるようになります。キーワード **10**、**100**、**1000** のうちいずれかをキーワード **auto** と併用すると、ポートは指定された速度でだけ自動ネゴシエーションを行います。 • キーワード **nonegotiate** は、SFP モジュール ポートに限り使用できます。SFP モジュール ポートは 1000 Mbps でだけ稼動しますが、自動ネゴシエーションをサポートしていないデバイスに接続されている場合はネゴシエーションしないように設定できます。 **（注）** Cisco 1000BASE-T SFP モジュールが SFP モジュール スロットに挿入されている場合、その速度は、**10**、**100**、**1000**、**auto** のいずれかに設定できますが、**nonegotiate** には設定できません。
ステップ 5	**duplex** {**auto** | **full** | **half**}	インターフェイスのデュプレックス パラメータを入力します。 （10 Mbps または 100 Mbps でだけ動作しているインターフェイスに対して）半二重モードをイネーブルにします。1000 Mbps で動作しているインターフェイスは、半二重モードには設定できません。 速度が **auto** に設定されている場合、デュプレックス設定を行うことができます。 このコマンドは、次の例外を除き、SFP モジュール ポートでは使用できません。 • Cisco 1000BASE-T SFP モジュールが挿入されている場合は、デュプレックスを **auto** または **full** に設定できます。 • Cisco 100BASE-T SFP モジュールが挿入されている場合は、デュプレックスを **full** または **half** に設定できます。キーワード **auto** は使用できますが、インターフェイスは半二重モード（デフォルト）になります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id*	インターフェイス速度およびデュプレックス モードの設定を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスの速度およびデュプレックス モードをデフォルト設定（自動ネゴシエーション）に戻すには、**no speed** インターフェイス コンフィギュレーション コマンドおよび **no duplex** インターフェイス コンフィギュレーション コマンドを使用します。すべてのインターフェイス設定をデフォルトに戻すには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス速度を 10 Mbps に、10/100Mbps ポートのデュプレックス モードを半二重に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fasttethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

次に、10/100/1000 Mbps ポートでインターフェイス速度を 100 Mbps に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# speed 100
```

デュアルパーパス ポートの設定

スイッチ上の一部のポートはデュアルパーパス ポートであり、10/100/100 ポートまたは SFP モジュール ポートとして設定できます。各デュアルパーパス ポートは、デュアル フロント エンド（RJ-45 コネクタおよび SFP モジュール コネクタ）を持つ単一のインターフェイスと見なされます。

（注）　デュアルパーパス ポート（および SFP 専用モジュール ポート）は、10 Mps または 100 Mps で動作している場合でも、**system mtu jumbo** グローバル コンフィギュレーション コマンドにより設定されるフレーム サイズを使用します。

各デュアルパーパス ポートは、デュアル フロント エンド（RJ-45 コネクタおよび SFP モジュール コネクタ）を持つ単一のインターフェイスと見なされます。デュアル フロント エンドは、冗長インターフェイスではありません。スイッチによりアクティブになるのは、このペアの一方のコネクタだけです。

デフォルトでは、デュアルパーパス ポートは UNI、SFP 専用モジュール ポートは NNI です。

（注）　ただし、Cisco ME 3400E-24TS-M スイッチの場合、アップリンク ポートの役割を果たすデュアルパーパス ポートはデフォルトで NNI に設定されます。

スイッチでメトロ IP アクセス イメージが稼動している場合、NNI として設定できるポート数に制限はありません。スイッチでメトロ アクセス イメージが稼動している場合、NNI として設定できるポートは 4 つまでです。

デフォルトでは、最初にリンク アップするデュアルパーパス ポートのメディア タイプは、スイッチによりダイナミックに選択されます。ただし、**media-type** インターフェイス コンフィギュレーション コマンドを使用すれば、RJ-45 コネクタまたは SFP モジュール コネクタを手動で選択できます。**auto-select** モードで、銅線信号と光ファイバ信号の両方が同時に検出された場合、スイッチは SFP モードを優先します。

アクティブにするデュアルパーパスのメディア タイプを選択するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するデュアルパーパス ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**media-type** {**auto-select** | **rj45** | **sfp**}	アクティブ インターフェイスおよびデュアルパーパス ポートのメディア タイプを選択します。キーワードの意味は次のとおりです。 • **auto-select**：スイッチによりメディア タイプがダイナミックに選択されます。これはデフォルト設定です。リンクアップが実現されると、スイッチはアクティブなリンクがダウンするまで、他のタイプをディセーブルにします。アクティブ リンクが終了すると、スイッチはいずれかのリンクが確立されるまでの間、両方のタイプをイネーブルにします。auto-select モードでは、スイッチはいずれのタイプも速度とデュプレックスの自動ネゴシエーションに基づいて設定します（デフォルト）。 • **rj45**：スイッチでは SFP モジュール インターフェイスがディセーブルになります。ケーブルを SFP ポートに接続した場合、RJ-45 がダウンしているか切断されている場合でも、リンクを確立できません。このモードでは、デュアルパーパス ポートは 10/100/1000BASE-TX インターフェイスと同様に動作します。このインターフェイス タイプに合った速度とデュプレックスが設定できます。 • **sfp**：スイッチでは RJ-45 インターフェイスがディセーブルになります。ケーブルを RJ-45 ポートに接続した場合、SFP 側 がダウンしているか、SFP モジュールが存在していない場合でも、リンクを確立できません。搭載された SFP モジュール タイプに応じて、このインターフェイス タイプに合った速度とデュプレックスが設定できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **transceiver properties**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻す場合は、**no media-type** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイス タイプを変更すると、速度およびデュプレックスの設定は削除されます。スイッチでは、どちらのメディア タイプについても、速度およびデュプレックスの自動ネゴシエーションが行われるように設定されます（デフォルト）。**auto-select** を設定した場合、**speed** および **duplex** インターフェイス コンフィギュレーション コマンドは設定できません。

メディア タイプとして **sfp** または **rj45** を設定した場合、設定しなかったメディア タイプのインターフェイスにコネクタが接続され、設定したメディア タイプのインターフェイスにコネクタが接続されていない場合でも、設定しなかった方のメディア タイプはディセーブルになります。

メディア タイプが **auto-select** の場合、スイッチでは次の基準に基づいてタイプが選択されます。

（注）　SFP が*インストール*されるためには、その SFP に光ファイバ ケーブルまたは銅ケーブルが接続されている必要があります。

- 接続されているコネクタがただ 1 つの場合、このインターフェイスはアクティブとなり、メディアが削除されるかスイッチがリロードされるまではアクティブのままです。
- イネーブルなデュアルパーパス ポートに両方のタイプのメディアがインストールされている場合、スイッチは最初にインストールされたタイプに基づいてアクティブ リンクを選択します。
- デュアルパーパス ポートに両方のメディアがインストールされている場合に、スイッチがリロードされるか、またはポートがいったんディセーブル化されたあと **shutdown** インターフェイス コンフィギュレーション コマンドおよび **no shutdown** インターフェイス コンフィギュレーション コマンドにより再度イネーブル化されると、スイッチは SFP モジュール インターフェイスを優先します。

詳細については、コマンド リファレンスの **media-type** インターフェイス コンフィギュレーション コマンドを参照してください。

IEEE 802.3X フロー制御の設定

IEEE 802.3Z フロー制御により、接続しているイーサネット ポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止させることで、輻輳時のトラフィック レートを制御できます。あるポートで輻輳が発生し、トラフィックをそれ以上受信できない場合は、ポーズ フレームを送信して、その状況が解消されるまで送信を停止するようにもう一方のポートに通知します。送信側デバイスは、ポーズ フレームを受信するとデータ パケットの送信を停止します。これにより、輻輳によるデータ パケットの損失を防ぐことができます。

（注） ポートでは、ポーズ フレームを受信できますが、送信はできません。

flowcontrol インターフェイス コンフィギュレーション コマンドを使用して、ポーズ フレームの **receive**（受信）に対するインターフェイスの機能を **on**、**off**、または **desired** に設定します。デフォルトのステートは、**off** です。

desired に設定すると、インターフェイスは、フロー制御パケットを送信する必要のある接続済みデバイス、またはフロー制御パケットを送信する必要はないが送信可能な接続済みデバイスと連携して動作します。

デバイスに設定される IEEE 802.3X フロー制御には、次の規則が適用されます。

- **receive on**（または **desired**）：ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要のある、または送信できる接続デバイスと連携して動作できます。ポートはポーズ フレームを受信できます。
- **receive off**：IEEE 802.3X フロー制御は、どちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

（注） ローカル ポートおよびリモート ポートにおけるコマンドの設定とそれによる IEEE 802.3X フロー制御解決の詳細については、このリリースのコマンド リファレンスに記載されている **flowcontrol** インターフェイス コンフィギュレーション コマンドの項を参照してください。

インターフェイスでの IEEE 802.3X フロー制御を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**flowcontrol** {**receive**} {**on** | **off** | **desired**}	ポートに IEEE 802.3X フロー制御モードを設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id*	インターフェイスの IEEE 802.3X フロー制御設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IEEE 802.3X フロー制御をディセーブルにするには、**flowcontrol receive off** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートで IEEE 802.3X フロー制御をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)# end
```

インターフェイスの自動 MDIX の設定

自動 Media-Dependent Interface crossover（MDIX; メディア依存型インターフェイス クロスオーバー）がイネーブルになっているインターフェイスでは、必要なケーブル接続タイプ（ストレートまたはクロス）が自動的に検出され、接続が適切に設定されます。自動 MDIX 機能を使わずにスイッチを接続するには、サーバ、ワークステーション、ルータなどのデバイスにはストレート ケーブルを使用して接続し、その他のスイッチやリピータへはクロスケーブルを使用して接続する必要があります。自動 MDIX がイネーブルな場合は、他のデバイスへ接続にどちらかのタイプのケーブルを使用できます。また、インターフェイスに不正なケーブル接続があれば自動的に修正されます。ケーブル接続に関する要件の詳細については、ハードウェア インストレーション ガイドを参照してください。

自動 MDIX はデフォルトでイネーブルに設定されています。また、自動 MDIX がイネーブルの場合は、この機能を正常に動作させるために、インターフェイスの速度とデュプレックス モードを **auto** に設定する必要があります。自動 MDIX は、10/100 Mbps インターフェイスおよび 10/100/1000 Mbps インターフェイスのすべてと Cisco 10/100/1000BASE-T/TX SFP モジュール インターフェイス上でサポートされています。1000BASE-SX または LX SFP モジュール インターフェイス上ではサポートされていません。

表 10-4 は、自動 MDIX の各設定値と、それらの設定値の下でケーブル接続が正しい場合と不正な場合の各リンク ステートを示したものです。

表 10-4　　リンクの状態と自動 MDIX 設定

ローカル側の自動 MDIX	リモート側の自動 MDIX	正しいケーブル接続	不正なケーブル接続
点灯	点灯	リンクアップ	リンクアップ
点灯	消灯	リンクアップ	リンクアップ

表 10-4　リンクの状態と自動 MDIX 設定 （続き）

ローカル側の自動 MDIX	リモート側の自動 MDIX	正しいケーブル接続	不正なケーブル接続
消灯	点灯	リンクアップ	リンクアップ
消灯	消灯	リンクアップ	リンクダウン

インターフェイスでの自動 MDIX を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**speed auto**	接続されたデバイスと速度を自動ネゴシエーションするようにインターフェイスを設定します。
ステップ 5	**duplex auto**	接続されたデバイスとデュプレックス モードを自動ネゴシエーションするようにインターフェイスを設定します。
ステップ 6	**mdix auto**	インターフェイス上で自動 MDIX をイネーブルにします。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show controllers ethernet-controller** *interface-id* **phy**	インターフェイス上の自動 MDIX 機能の動作ステートを確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

自動 MDIX をディセーブルにする場合は、**no mdix auto** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

インターフェイスに関する説明の追加

インターフェイスの機能に関する説明を追加できます。説明は、**show configuration**、**show running-config**、および **show interfaces** の各特権 EXEC コマンドによる出力内に表示されます。

インターフェイスに関する説明を追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	説明を追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**description** *string*	インターフェイスに関する説明を追加します（最大 240 文字）。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **description** または **show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

説明を削除するには、**no description** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに関する説明を追加し、その説明を確認する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet0/2 description
Interface Status         Protocol Description
Gi 0/2    admin down     down     Connects to Marketing
```

レイヤ 3 インターフェイスの設定

レイヤ 3 インターフェイスをサポートするためには、スイッチ上でメトロ IP アクセス イメージが稼動している必要があります。Cisco ME スイッチは、次に示す 3 種類のレイヤ 3 インターフェイスをサポートしています。

- SVI：SVI は、トラフィックをルーティングするすべての VLAN に対して設定する必要があります。SVI は、**interface vlan** グローバル コンフィギュレーション コマンドのあとに VLAN ID を入力して作成します。SVI を削除するには、**no interface vlan** グローバル コンフィギュレーション コマンドを使用します。インターフェイス VLAN 1 は削除できません。

  （注）　物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。VLAN へのレイヤ 2 ポートの割り当てに関する詳細については、第 12 章「VLAN の設定」を参照してください。

- ルーテッド ポート：ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。
- レイヤ 3 EtherChannel ポート：ルーテッド ポートにより構成される EtherChannel インターフェイスです。

  EtherChannel ポート インターフェイスについては、第 35 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

レイヤ 3 スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。

スイッチに設定可能な SVI およびルーテッド ポートの個数について規定された制限はありません。ただし、ハードウェアには限界があるため、SVI およびルーテッド ポートの個数と、設定されている他の機能の個数の組み合せによっては、CPU の稼動率に影響する場合もあります。スイッチが最大限のハードウェア リソースを使用している場合にルーテッド ポートまたは SVI を作成しようとすると、次のような結果になります。

- 新たなルーテッド ポートを作成しようとすると、スイッチは、インターフェイスをルーテッド ポートに変換するための十分なリソースがないことを示すメッセージを表示し、そのインターフェイスはスイッチ ポートのままとなります。
- 拡張範囲の VLAN を作成しようとすると、エラー メッセージが生成され、拡張範囲の VLAN は拒否されます。
- スイッチが、ハードウェアのサポート可能な数を超える VLAN とルーテッド ポートが設定されたコンフィギュレーションを使って起動を試みた場合、VLAN は作成されますが、ルーテッド ポートはシャットダウンされ、スイッチはその原因がハードウェア リソースの不足にあるという内容のメッセージを送信します。

トラフィックをルーティングするレイヤ 3 インターフェイスにはすべて、IP アドレスが必要です。次に、インターフェイスをレイヤ 3 インターフェイスとして設定する手順およびインターフェイスに IP アドレスを割り当てる手順を示します。

（注） 物理ポートがレイヤ 2 モード（デフォルト）である場合は、**no switchport** インターフェイス コンフィギュレーション コマンドを実行してインターフェイスをレイヤ 3 モードにする必要があります。**no switchport** コマンドを実行すると、インターフェイスはいったんディセーブルになった後で、再度イネーブルになります。その際、インターフェイスが接続されているデバイスについてのメッセージが表示されることがあります。さらに、レイヤ 3 モードのインターフェイスをレイヤ 2 モードにすると、その対象となったインターフェイスに関するそれまでの設定情報が消失することがあります。その場合、インターフェイスはデフォルト設定に戻ります。

レイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** {{**fastethernet** | **gigabitethernet**} *interface-id*} | {**vlan** *vlan-id*} | {**port-channel** *port-channel-number*}	レイヤ 3 インターフェイスとして設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**no switchport**	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 5	**ip address** *ip_address subnet_mask*	IP アドレスおよび IP サブネットを設定します。
ステップ 6	**no shutdown**	インターフェイスをイネーブルにします。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*] **show ip interface** [*interface-id*] **show running-config interface** [*interface-id*]	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスの IP アドレスを削除するには、**no ip address** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをルーテッド ポートとして設定し、それに IP アドレスを割り当てる例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
```

システム MTU の設定

スイッチ上のすべてのインターフェイスで送受信されるフレームのデフォルトの Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズは、1500 バイトです。**system mtu** グローバル コンフィギュレーション コマンドを使用すると、10 Mbps または 100 Mbps で動作するすべてのインターフェイスの MTU サイズを拡張できます。また、**system mtu jumbo** グローバル コンフィギュレーション コマンドを使用すると、すべてのギガビット イーサネット インターフェイス上でジャンボ フレームをサポートできるように MTU サイズを拡張できます。**system mtu routing** グローバル コンフィギュレーション コマンドを使用すると、ルーテッド ポートの MTU サイズを変更できます。

（注）　システム MTU サイズを超えるルーティング MTU サイズは設定できません。システム MTU サイズを現在設定されているルーティング MTU サイズより小さい値に変更すると、設定変更は受け入れられますが、次にスイッチをリセットするまで適用されません。設定変更が有効になると、ルーティング MTU サイズは自動的にデフォルトの新しいシステム MTU サイズになります。

ギガビット イーサネット ポートは、**system mtu** コマンドの影響を受けません。ジャンボ フレームは、100BASE-FX SFP モジュールおよび 100BASE-BX SFP モジュールを含む 10/100 インターフェイス上ではサポートされないため、ファスト イーサネット ポートは **system mtu jumbo** コマンドの影響を受けません。**system mtu jumbo** コマンドを設定しなければ、**system mtu** コマンドの設定がすべてのギガビット イーサネット インターフェイスに適用されます。

MTU サイズは、個々のインターフェイスに 設定できません。スイッチ上のすべての 10/100 インターフェイスまたはすべてのギガビット イーサネット インターフェイスに対して設定されます。システム MTU サイズを変更した場合、新しい設定を有効にするには、スイッチをリセットする必要があります。**system mtu routing** コマンドは、スイッチをリセットしなくても有効になります。

（注）　システム MTU 設定は、NVRAM のスイッチ環境変数に保存され、スイッチをリロードするときに有効になります。**system mtu** コマンドおよび **system mtu jumbo** コマンドで入力した MTU 設定は、**copy running-config startup-config** 特権 EXEC コマンドを入力しても、スイッチ IOS コンフィギュレーション ファイルには保存されません。したがって、TFTP を使用し、バックアップ コンフィギュレーション ファイルで新しいスイッチを設定して、システム MTU をデフォルト以外の値にしたい場合、新しいスイッチ上で **system mtu** および **system mtu jumbo** を明示的に設定し、スイッチをリロードする必要があります。

スイッチの CPU で受信可能なフレーム サイズは、**system mtu** コマンドまたは **system mtu jumbo** コマンドで指定された値には関係なく、1998 バイトに制限されています。通常、転送されたフレームは CPU では受信されませんが、トラフィック制御用に送信されるトラフィック、SNMP、Telnet、ルーティング プロトコルなどでは、パケットが CPU に送信される場合があります。

スイッチはパケットを分割しないので、次のパケットをドロップします。

- *出力*インターフェイスでサポートされるパケット サイズより大きい、スイッチド パケット

- ルーティング MTU 値より大きいルーテッド パケット

たとえば、**system mtu** 値が 1998 バイトで **system mtu jumbo** 値が 5000 バイトである場合、1000 Mbps で動作するインターフェイスで受信可能なパケット サイズは、最大 5000 バイトです。ただし、1998 バイトより大きいパケットは、1000 Mbps で動作するインターフェイス上では受信できますが、その宛先インターフェイスが 10 Mbps または 100 Mbps で動作するインターフェイスである場合は廃棄されます。

ルーテッド パケットは、送信ポートで MTU チェックの対象となります。ルーテッド ポートで使用される MTU 値は、（**system mtu jumbo** 値ではなく）設定された **system mtu** 値から導出されます。つまり、ルーテッド MTU はどの VLAN のシステム MTU よりも大きくはなりません。ルーティング プロトコルでは、隣接関係とリンクの MTU をネゴシエーションする際にシステム MTU 値が使用されます。たとえば、Open Shortest Path First（OSPF）プロトコルでは、ピア ルータとの隣接関係を設定する前にこの MTU 値が使用されます。特定の VLAN のルーテッド パケットの MTU 値を表示する場合は、**show platform port-asic mvid** 特権 EXEC コマンドを使用します。

（注） レイヤ 2 ギガビット イーサネット インターフェイスが、10/100 インターフェイスより大きいサイズのフレームを受け取るように設定されている場合、レイヤ 2 ギガビット イーサネット インターフェイスに着信するジャンボ フレームとレイヤ 2 10/100 インターフェイスで発信されるジャンボ フレームは廃棄されます。

10/100 インターフェイスまたはギガビット イーサネット インターフェイスすべての MTU サイズを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**system mtu** *bytes*	（任意）10 Mbps または 100 Mbps で動作するスイッチのすべてのインターフェイスに対する MTU サイズを変更します。指定できる範囲は 1500 ～ 1998 バイトで、デフォルトは 1500 バイトです。
ステップ 3	**system mtu jumbo** *bytes*	（任意）スイッチのすべてのギガビット イーサネット インターフェイスに対する MTU サイズを変更します。指定できる範囲は 1500 ～ 9000 バイトで、デフォルトは 1500 バイトです。
ステップ 4	**system mtu routing** *bytes*	（任意）ルーテッド ポートのシステム MTU を変更します。指定できる範囲は 1500 ～システム MTU 値（すべてのポートにルーティング可能な最大 MTU 値）です。 これより大きなパケットは、受け入れられますがルーティングはされません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	コンフィギュレーション ファイルに設定を保存します。
ステップ 7	**reload**	オペレーティング システムをリロードします。

特定タイプのインターフェイスに対して許容範囲外の値を入力しても、その値は受け入れられません。

スイッチをリロードしたら、**show system mtu** 特権 EXEC コマンドを使用して設定を確認できます。

次は、ギガビット イーサネット ポートの最大パケット サイズを 1800 バイトに設定する方法を示した例です。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

次は、ギガビット イーサネット インターフェイスを範囲外の数値に設定しようとした場合の応答を示した例です。

```
Switch(config)# system mtu jumbo 25000
                                 ^
% Invalid input detected at '^' marker.
```

インターフェイスのモニタおよびメンテナンス

ここでは、インターフェイスのモニタおよびメンテナンスについて説明します。

- 「インターフェイス ステータスのモニタ」（P.10-31）
- 「インターフェイスおよびカウンタのクリアとリセット」（P.10-32）
- 「インターフェイスのシャットダウンおよび再起動」（P.10-33）

インターフェイス ステータスのモニタ

特権 EXEC プロンプトにコマンドを入力することによって、ソフトウェアおよびハードウェアのバージョン、設定、インターフェイスに関する統計情報など、インターフェイスのさまざまな情報が表示されます。表 10-5 に、このインターフェイス モニタ コマンドの一部を示します（特権 EXEC プロンプトで **show ?** コマンドを入力すると、**show** コマンドの全リストを表示できます）。これらのコマンドの詳細については、『*Cisco IOS Interface Command Reference*』*Release 12.2* を参照してください。

表 10-5　インターフェイス用の show コマンド

コマンド	目的
show interfaces [*interface-id*]	すべてのインターフェイスまたは特定のインターフェイスのステータスおよび設定を表示します。
show interfaces *interface-id* **status** [**err-disabled**]	インターフェイスのステータス、または errdisable ステートにあるインターフェイス リストを表示します。
show interfaces [*interface-id*] **switchport**	スイッチング モードの管理上および動作上のステータスを表示します。このコマンドを使用すると、ポートのモードがルーティング モードかスイッチング モードかを判別できます。
show interfaces [*interface-id*] **description**	1 つのインターフェイスまたはすべてのインターフェイスに関する説明とインターフェイスのステータスを表示します。
show ip interface [*interface-id*]	IP ルーティング用に設定されたすべてのインターフェイス、または指定されたインターフェイスの使用可能性に関するステータスを表示します。
show interface [*interface-id*] **stats**	インターフェイスのスイッチング パスによる入力パケットおよび出力パケットを表示します。

表 10-5　インターフェイス用の show コマンド （続き）

コマンド	目的
show interfaces [*interface-id]* **transceiver** [**detail** | **dom-supported-list** | **module** *number* | **properties** | **threshold-table**]	SFP モジュールの物理ステータスおよび動作ステータスを表示します。 • *interface-id :*（任意）指定した物理インターフェイスの設定およびステータスを表示します。 • **detail :**（任意）Digital Optical Monitoring（DoM; デジタル オプティカル モニタリング）対応トランシーバがスイッチに装備されている場合に、そのトランシーバに関する較正プロパティ（上限値、下限値、アラーム情報など）を表示します。 • **dom-supported-list :**（任意）サポートされているすべての DoM トランシーバをリスト表示します。 • **module** *number* **:**（任意）スイッチ上のモジュールのインターフェイスだけを表示します。指定できる範囲は 1 ～ 9 です。このオプションは、特定のインターフェイス ID を入力したときは利用できません。 • **properties :**（任意）インターフェイスの速度、デュプレックス、およびインライン パワーの設定を表示します。 • **threshold-table :**（任意）アラームおよび警告のしきい値テーブルを表示します。
show port-type [**eni** | **nni** | **uni**]	Cisco ME スイッチのインターフェイス タイプの情報を表示します。
show running-config interface [*interface-id*]	RAM に保存されたインターフェイスの実行コンフィギュレーションを表示します。
show version	ハードウェア構成、ソフトウェアのバージョン、コンフィギュレーション ファイルの名前とソース、およびブート イメージを表示します。
show controllers ethernet-controller *interface-id* **phy**	インターフェイス上の自動 MDIX 機能の動作ステートを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 10-6 に、カウンタのクリアとインターフェイスのリセットに使用できる特権 EXEC モードの **clear** コマンドを示します。

表 10-6　インターフェイス用の clear コマンド

コマンド	目的
clear counters [*interface-id*]	インターフェイスのカウンタをクリアします。
clear interface *interface-id*	インターフェイスに関するハードウェア ロジックをリセットします。
clear line [*number* | **console 0** | **vty** *number*]	非同期シリアル回線に関するハードウェア ロジックをリセットします。

show interfaces 特権 EXEC コマンドによって表示されたインターフェイス カウンタをクリアするには、**clear counters** 特権 EXEC コマンドを使用します。**clear counters** コマンドを実行すると、インターフェイスから現在のインターフェイス カウンタがすべてクリアされます。ただし、特定のインターフェイス番号から特定のインターフェイス タイプだけがクリアされるようにオプション引数が指定されている場合は除きます。

（注）　**clear counters** 特権 EXEC コマンドを実行しても、SNMP を使用して取得されたカウンタはクリアされません。クリアされるのは **show interface** 特権 EXEC コマンドで表示されるカウンタだけです。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定されたインターフェイスのすべての機能がディセーブルになり、使用不可能であることがすべてのモニタ コマンドの出力に表示されます。この情報は、すべてのダイナミック ルーティング プロトコルによって他のネットワーク サーバに伝達されます。ルーティング更新のときには、このインターフェイスは一切考慮されません。

インターフェイスをシャットダウンするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** {**vlan** *vlan-id*}	{{**fastethernet** | **gigabitethernet**} *interface-id*} | {**port-channel** *port-channel-number*}	設定するインターフェイスを選択します。
ステップ 3	**shutdown**	インターフェイスをシャットダウンします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。

インターフェイスをイネーブルにする場合は、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスがディセーブルになっていることを確認する場合は、**show interfaces** 特権 EXEC コマンドを使用します。ディセーブル化されたインターフェイスは、出力では *administratively down* と表示されます。

CHAPTER 11

コマンド マクロの設定

この章では、Cisco ME 3400E スイッチにコマンド マクロを設定して適用する方法について説明します。

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

- 「コマンド マクロの概要」（P.11-1）
- 「コマンド マクロの設定」（P.11-1）
- 「コマンド マクロの表示」（P.11-5）

コマンド マクロの概要

コマンド マクロは、共通の設定を保存および共有するのに便利な方法です。コマンド マクロを使用して、ネットワークのスイッチの位置に基づく機能および設定をイネーブルにしたり、ネットワーク上で大規模な設定配置を行ったりすることができます。

各コマンド マクロは、定義する CLI（コマンドライン インターフェイス）コマンドのセットです。コマンド マクロは、新しい CLI コマンドを含みません。既存の CLI コマンドの集合です。

インターフェイスで コマンド マクロを適用すると、マクロ内の CLI コマンドがこのインターフェイス上で設定されます。マクロがインターフェイスに適用されても、既存のインターフェイスの設定は失われません。新しいコマンドはインターフェイスに追加され、実行コンフィギュレーション ファイルに保存されます。

コマンド マクロの設定

新たにコマンド マクロを作成したり、ご使用のアプリケーションに特有の新しいマクロを作成したりする場合、既存のマクロをテンプレートとして使用することができます。マクロを作成して、スイッチ、スイッチ インターフェイスまたはインターフェイス範囲に適用することができます。

- 「コマンド マクロのデフォルト設定」（P.11-2）
- 「コマンド マクロ設定時の注意事項」（P.11-2）
- 「コマンド マクロの作成」（P.11-3）
- 「コマンド マクロの適用」（P.11-4）
- 「コマンド マクロの表示」（P.11-5）

コマンド マクロのデフォルト設定

イネーブルに設定されているコマンド マクロはありません。

コマンド マクロ設定時の注意事項

スイッチでマクロを設定するには、次の注意事項に従ってください。

- マクロを作成する際に、**exit** や **end** コマンド、または **interface** *interface-id* コマンドを使用してコマンド モードを変更しないでください。これらのコマンドを使用すると、**exit**、**end**、または **interface** *interface-id* に続くコマンドが異なるコマンド モードで実行されることがあります。
- マクロを作成する場合、すべての CLI コマンドは同じコンフィギュレーション モードになる必要があります。
- 一意の値の割り当てを必要とするマクロを作成する場合、**parameter** *value* キーワードを使用して、そのインターフェイスに固有の値を指定します。キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。
- マクロ名では、大文字と小文字が区別されます。たとえば、コマンド **macro name Sample-Macro** と **macro name sample-macro** は、2 つの別個のマクロとなります。
- 一部のマクロには、パラメータ値が必要なキーワードが含まれます。マクロで必要な値のリストを表示するには、**macro global apply** *macro-name* **?** グローバル コンフィギュレーション コマンド、または **macro apply** *macro-name* **?** インターフェイス コンフィギュレーション コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。
- マクロがスイッチまたはスイッチ インターフェイスにグローバルに適用されると、インターフェイス上の既存の設定はすべて保持されます。これは、差分設定を適用する場合に便利です。
- コマンドを追加または削除してマクロ定義を変更する場合、この変更は元のマクロが適用されているインターフェイスに反映されません。新しいコマンドまたは変更したコマンドを適用するには、更新したマクロをインターフェイスに再適用する必要があります。
- **macro global trace** *macro-name* グローバル コンフィギュレーション コマンドまたは **macro trace** *macro-name* インターフェイス コンフィギュレーション コマンドを使用して、構文または設定エラーを検索するためのマクロを適用してデバッグできます。構文エラーまたは設定エラーによりコマンドが失敗した場合、マクロは続けて残りのコマンドを適用します。
- CLI コマンドには、あるインターフェイス タイプに特有のものもあります。マクロが設定を受け入れないインターフェイスに適用された場合、マクロは構文チェックや設定チェックに失敗して、スイッチがエラー メッセージを返します。
- インターフェイス範囲にマクロを適用することは、単一のインターフェイスにマクロを適用するのと同じです。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。あるインターフェイスでマクロ コマンドが失敗した場合、残りのインターフェイスに適用されていきます。
- マクロをスイッチまたはスイッチ インターフェイスに適用する場合、マクロ名が自動的にスイッチまたはインターフェイスに追加されます。**show running-config** ユーザ EXEC コマンドを使用して、適用されたコマンドとマクロ名を表示できます。

- マクロを User Network Interface（UNI; ユーザ ネットワーク インターフェイス）または Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）に適用する場合、先にポートをイネーブルに設定する必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。

コマンド マクロの作成

コマンド マクロを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro name *macro-name*	マクロ定義を作成して、マクロ名を入力します。マクロ定義には、最大 3000 文字まで含めることができます。 1 行につき 1 つのコマンドで、マクロ コマンドを入力します。マクロを終了するには、**@** 文字を使用します。マクロ内でコメント テキストを入力するには、行の始めに **#** 文字を使用します。 （任意）キーワードの指定にヘルプ ストリングを使用することで、マクロ内にキーワードを定義できます。**#macro keywords** *word* を入力してマクロで使用できるキーワードを定義します。スペースで分離することで、最大で 3 つのヘルプ ストリング キーワードをマクロに入力できます。 マクロ名では、大文字と小文字が区別されます。たとえば、コマンド **macro name Sample-Macro** と **macro name sample-macro** は、2 つの別個のマクロとなります。 **exit** または **end** コマンドを使用したり、**interface** *interface-id* を使用してコマンド モードを変更することはしないでください。これは、**exit**、**end**、または **interface** *interface-id* に続くコマンドが、異なるコマンド モードで実行されてしまう可能性があります。最良の結果を得るには、マクロ内のすべてのコマンドが同じコンフィギュレーション モードである必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show parser macro** name *macro-name*	マクロが作成されたことを確認します。

macro name グローバル コンフィギュレーション コマンドの **no** 形式によって、マクロの定義だけが削除されます。マクロがすでに適用されているインターフェイスの設定には、影響はありません。

次に、スイッチポート アクセス VLAN とセキュア MAC アドレス数を定義するマクロを作成し、**# macro keywords** を使用して 2 つのヘルプ ストリング キーワードを含める例を示します。

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

コマンド マクロの適用

コマンド マクロを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**macro global** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	マクロで定義された各コマンドをスイッチに適用するには、**macro global apply** *macro-name* を入力します。構文または設定エラーを検索するためのマクロを適用しデバッグするには、**macro global trace** *macro-name* を指定します。 （任意）スイッチに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。 一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro global apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。
ステップ 3	**macro global description** *text*	（任意）スイッチに適用されるマクロについての説明を入力します。
ステップ 4	**interface** *interface-id*	（任意）インターフェイス コンフィギュレーション モードを開始して、マクロを適用するインターフェイスを指定します。
ステップ 5	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 6	**default interface** *interface-id*	（任意）指定したインターフェイスからすべての設定を消去します。
ステップ 7	**macro** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	マクロで定義された各コマンドをインターフェイスに適用するには、**macro apply** *macro-name* を入力します。構文または設定エラーを検索するためのマクロを適用しデバッグするには、**macro trace** *macro-name* を指定します。 （任意）インターフェイスに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。 一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。
ステップ 8	**macro description** *text*	（任意）インターフェイスに適用されるマクロについての説明を入力します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show parser macro description** [**interface** *interface-id*]	マクロがインターフェイスに適用されたことを確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

マクロ内の各コマンドの **no** バージョンを入力する場合だけ、グローバル マクロ適用コンフィギュレーションを削除できます。**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用すれば、インターフェイスで適用されたマクロの設定を削除できます。

次に、ユーザが作成した **snmp** というマクロを適用してホスト名アドレスを **test-server** に設定し、IP precedence 値を **7** に設定する例を示します。

```
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

次に、スイッチにマクロが適用された際にマクロ内の構文または設定エラーを検索するために、**macro global trace** グローバル コンフィギュレーション コマンドを使用して **snmp** というユーザ作成マクロをデバッグする例を示します。

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

次に、ユーザ作成の **desktop-config** と いうマクロを適用して設定を確認する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# macro apply desktop-config
Switch(config-if)# end
Switch# show parser macro description
Interface    Macro Description
---------------------------------------------------------------
Gi0/2      desktop-config
---------------------------------------------------------------
```

次に、**desktop-config** というユーザ作成マクロを適用して、VLAN 1 となっているところをすべて VLAN 25 に置き換える例を示します。

```
Switch(config-if)# macro apply desktop-config vlan 25
```

コマンド マクロの表示

コマンド マクロを表示するには、表 11-1 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 11-1　コマンド マクロを表示するコマンド

コマンド	目的
show parser macro	設定されたすべてのマクロを表示します。
show parser macro name *macro-name*	特定のマクロを表示します。
show parser macro brief	設定されたマクロ名を表示します。
show parser macro description [**interface** *interface-id*]	すべてのインターフェイスまたは特定のインターフェイスに関するマクロの説明を表示します。

CHAPTER 12

VLAN の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに、標準範囲の VLAN（仮想 LAN）（VLAN ID が 1 ～ 1005）および拡張範囲の VLAN（VLAN ID が 1006 ～ 4094）を設定する方法について説明します。VLAN メンバーシップ モード、VLAN コンフィギュレーション モード、VLAN トランク、VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）からのダイナミック VLAN 割り当てについても説明します。

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

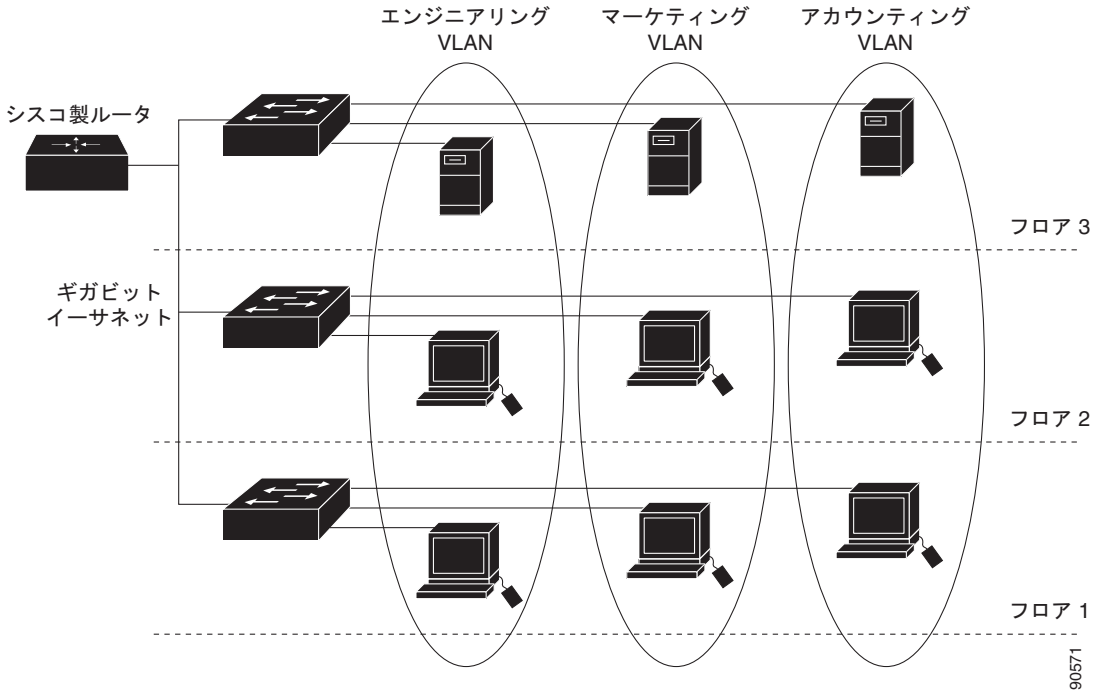
- 「VLAN の概要」（P.12-1）
- 「VLAN の作成および変更」（P.12-7）
- 「VLAN の表示」（P.12-15）
- 「VLAN トランクの設定」（P.12-15）
- 「VMPS の設定」（P.12-24）

VLAN の概要

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションによって論理的に分割されたスイッチド ネットワークです。VLAN は物理 VLAN と同じアトリビュートを備えていますが、エンド ステーションが物理的に同一の LAN セグメントにない場合でもグループ化できます。どのスイッチ ポートも VLAN に割り当てることができます。ユニキャスト、ブロードキャスト、およびマルチキャスト パケットは、VLAN 内のエンド ステーションにだけフォワーディングおよびフラッディングが行われます。各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に属さないステーション宛のパケットは、ルータを経由して伝送しなければなりません（図 12-1 を参照）。VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLAN ごとに独自のブリッジ MIB（管理情報ベース）情報があり、それぞれが独自にスパニング ツリーの実装をサポートします。第 15 章「STP の設定」を参照してください。

図 12-1 に、論理的に定義されたネットワークに分割した VLAN の例を示します。

図 12-1　論理的に定義されたネットワークとしての VLAN



VLAN は、多くの場合、IP サブネットワークと対応付けられます。たとえば、特定の IP サブネットのすべてのエンド ステーションを同一の VLAN に属させることがあります。スイッチ上のインターフェイス VLAN メンバーシップは、インターフェイスごとに手動で割り当てます。この方法で VLAN にスイッチ インターフェイスを割り当てることを、インターフェイスベースまたはスタティック VLAN メンバーシップと呼びます。

（注） スイッチは、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）をサポートしません。

VLAN 間のトラフィックは、ルーティングする必要があります。メトロ IP アクセス イメージを稼動しているスイッチは、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を使用して VLAN 間のトラフィックをルーティングできます。VLAN 間のトラフィックをルーティングするには、SVI を明示的に設定し、IP アドレスが割り当てられる必要があります。詳細については、「スイッチ仮想インターフェイス」（P.10-6）および「レイヤ 3 インターフェイスの設定」（P.10-27）を参照してください。

この章の内容は、次のとおりです。

- 「サポート対象の VLAN」（P.12-3）
- 「標準範囲 VLAN」（P.12-3）
- 「拡張範囲 VLAN」（P.12-4）
- 「VLAN ポート メンバーシップ モード」（P.12-4）
- 「UNI-ENI VLAN」（P.12-5）

サポート対象の VLAN

VLAN は、1 ～ 4094 の番号で識別されます。VLAN ID の 1002 ～ 1005 は、トークン リングおよび Fiber Distributed Data Interface（FDDI）VLAN 用です。1006 以上の VLAN ID は、拡張範囲 VLAN で、VLAN データベースには格納されません。

スイッチは合計 1005（標準範囲および拡張範囲）の VLAN をサポートしますが、ルーテッド ポート、SVI、その他の設定済み機能の個数によって、スイッチのハードウェアの使用は左右されます。

このスイッチは、Per-VLAN Spanning-Tree Plus（PVST+; VLAN 単位スパニング ツリー プラス）と最大 128 のスパニング ツリー インスタンスをサポートします。VLAN ごとに 1 つのスパニング ツリー インスタンスがサポートされます。

（注） デフォルトで、Network Node Interface（NNI; ネットワーク ノード インターフェイス）が、STP をサポートします。Enhanced Network Interfaces（ENI; 拡張ネットワーク インターフェイス）を設定して、STP をサポートします。User Network Interfaces（UNI; ユーザ ネットワーク インターフェイス）は STP をサポートせず、デフォルトでは常にフォワーディング ステートです。

スパニング ツリー インスタンスの数と VLAN 番号の詳細については、「VLAN 設定時の注意事項」（P.12-8）を参照してください。スイッチは、イーサネット ポート上での VLAN トラフィックの送信において、IEEE 802.1Q トランキングをサポートします。

標準範囲 VLAN

標準範囲 VLAN とは、VLAN ID が 1 ～ 1005 の VLAN のことです。VLAN 2 ～ 1001 の設定は、VLAN データベースで追加、変更、または削除できます （VLAN ID の 1 と 1002 ～ 1005 は、自動作成され、削除できません）。

VLAN ID が 1 ～ 1005 の設定はファイル *vlan.dat*（VLAN データベース）に保存され、**show vlan** 特権 EXEC コマンドを入力すると表示できます。*vlan.dat* ファイルはフラッシュ メモリに保存されています。

注意 *vlan.dat* ファイルを手動で削除しようとすると、VLAN データベースに不整合が生じるおそれがあります。VLAN 設定を変更する場合は、ここに記載されているコマンド、およびこのリリースのコマンド リファレンスを参照してください。

VLAN データベースに新しい標準範囲 VLAN を作成する場合、または VLAN データベース内の既存の VLAN を変更する場合、次のパラメータを設定できます。

- VLAN ID
- VLAN name
- VLAN タイプ（イーサネット、FDDI、FDDI Network Entity Title [NET]、Token Ring Bridge Relay Function [TrBRF; トークンリング ブリッジ リレー機能] または Token Ring Concentrator Relay Function [TrCRF; トークンリング コンセントレータ リレー機能]、トークン リング、トークン リングネット）

（注） スイッチは、イーサネット VLAN だけをサポートしています。FDDI およびトークン リング VLAN のパラメータを設定して、vlan.dat ファイルでの結果を表示できますが、これらのパラメータは使用されません。

- VLAN ステート（アクティブまたはサスペンド）
- VLAN の Maximum Transmission Unit（MTU; 最大伝送ユニット）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN の Spanning-Tree Protocol（STP; スパニング ツリープロトコル）タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号
- プライベート VLAN。VLAN は、プライマリまたはセカンダリ プライベート VLAN として設定できます。プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。
- RSPAN VLAN。リモート SPAN セッションに、VLAN を Remote Switched Port Analyzer（RSPAN）VLAN として設定します。RSPAN の詳細については、第 27 章「SPAN および RSPAN の設定」を参照してください。
- UNI-ENI VLAN コンフィギュレーション

拡張範囲 VLAN の場合、MTU、プライベート VLAN、RSPAN VLAN、および UNI-ENI VLAN パラメータに限り設定できます。

（注）　ここでは、これらのパラメータのほとんどについて設定の詳細は説明しません。VLAN 設定を制御するコマンドおよびパラメータの詳細については、このリリースのコマンド リファレンスを参照してください。

拡張範囲 VLAN

拡張範囲 VLAN（1006 ～ 4094 の範囲）を作成すると、サービス プロバイダーはインフラストラクチャをさらに多数のカスタマーに拡張できます。拡張範囲 VLAN ID は、VLAN ID を認めるどの **switchport** コマンドでも認められます。拡張範囲 VLAN の設定は、VLAN データベースには保存されませんが、スイッチの実行コンフィギュレーション ファイルに保存されます。また、**copy running-config startup-config** 特権 EXEC コマンドを使用するとスタートアップ コンフィギュレーション ファイルに設定を保存できます。

（注）　スイッチは 4094 の VLAN ID をサポートしますが、サポートされる VLAN の実数は 1005 です。

VLAN ポート メンバーシップ モード

VLAN に属するポートは、メンバーシップ モードを指定して設定します。メンバーシップ モードにより、ポートが搬送できるトラフィックの種類、および属することができる VLAN の数が決まります。表 12-1 に、各種メンバーシップ モードおよび特性を示します。

表 12-1　ポート メンバーシップ モード

メンバーシップ モード	VLAN メンバーシップの特性
スタティック アクセス	スタティック アクセス ポートは、1 つの VLAN だけに属し、手動でその VLAN に割り当てられます。 詳細については、「VLAN へのスタティックアクセス ポートの割り当て」（P.12-11）を参照してください。
トランク（IEEE 802.1Q）	トランク ポートは、拡張範囲 VLAN も含めて、デフォルトで全 VLAN のメンバーですが、許可 VLAN リストを設定することにより、メンバーシップを制限できます。 トランク ポートの設定の詳細については、「トランク ポートとしてのイーサネット インターフェイスの設定」（P.12-17）を参照してください。
ダイナミック アクセス	ダイナミック アクセス ポートは、1 つの VLAN（VLAN ID が 1 ～ 4094）だけに属し、VMPS によって動的に割り当てられます。たとえば、Catalyst 5000 または Catalyst 6500 シリーズ スイッチは VMPS として使用できますが、Cisco ME 3400E イーサネット アクセス スイッチは VMPS として使用できません。Cisco ME 3400E スイッチは、VMPS クライアントです。 **（注）**　UNI または ENI に限り、ダイナミック アクセス ポートにできます。 同じスイッチ上にダイナミック アクセス ポートとトランク ポートを設定できますが、ダイナミック アクセス ポートはエンド ステーションまたはハブに接続する必要があります。別のスイッチに接続してはなりません。 設定の詳細については、「VMPS クライアントのダイナミック アクセス ポートの設定」（P.12-27）を参照してください。
プライベート VLAN	プライベート VLAN ポートは、プライベート VLAN のプライマリまたはセカンダリ VLAN に属するホストまたはプロミスキャス ポートです。NNI に限り、プロミスキャス ポートとして設定できます。 プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。
トンネル（**dot1q-tunnel**）	トンネル ポートは、IEEE 802.1Q トンネリング用に使用され、サービス プロバイダー ネットワーク全体でカスタマー VLAN の整合性を維持します。トンネル ポートをサービス プロバイダー ネットワークのエッジ スイッチ上に設定し、カスタマー インターフェイスの IEEE 802.1Q トランク ポートに接続して、非対称リンクを作成します。トンネル ポートは、トンネリング専用の単一の VLAN に属します。 トンネル ポートの詳細については、第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

アクセス モードおよびトランク モードの定義およびその機能の詳細については、表 12-4（P.12-16）を参照してください。

VLAN にポートを割り当てると、スイッチは VLAN 単位で、ポートに対応するアドレスを学習して管理します。詳細については、「MAC アドレス テーブルの管理」（P.5-19）を参照してください。

UNI-ENI VLAN

Cisco ME スイッチは、カスタマー ネットワークとサービス プロバイダー ネットワークの境界であり、UNI および ENI によりネットワークのカスタマー側と接続されます。カスタマー トラフィックがサービス プロバイダー ネットワークで発信または着信する場合、このカスタマーの VLAN ID はその他の

カスタマーの VLAN ID から分離されている必要があります。この分離を行うには、プライベート VLAN を使用するなど、いくつか方法があります。Cisco ME スイッチ上では、この分離がデフォルトで UNI-ENI VLAN を使用して行われます。

UNI-ENI VLAN には 2 種類あります。

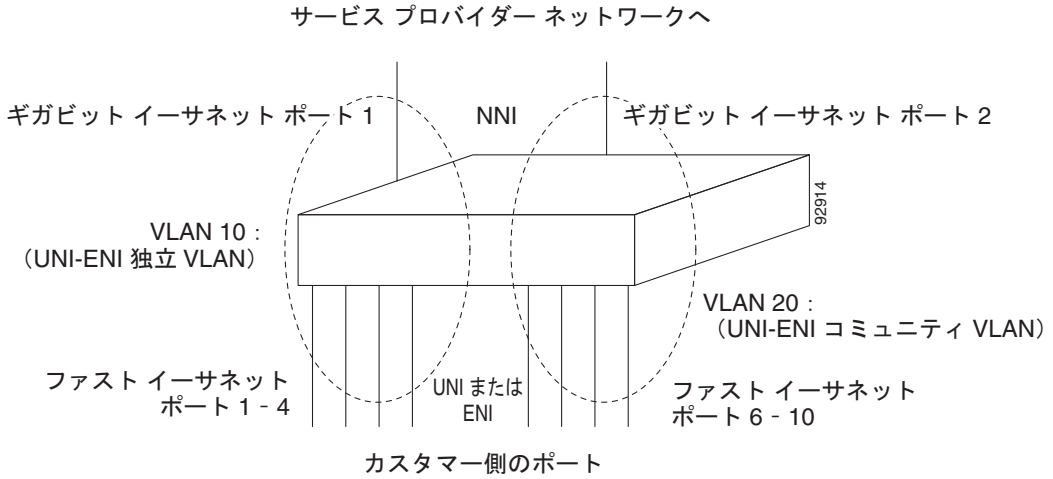
- UNI-ENI 独立 VLAN：これは、スイッチ上で作成されるすべての VLAN のデフォルト VLAN ステートです。同一の UNI-ENI 独立 VLAN に属するスイッチでは、UNI または ENI 間のローカル スイッチングが実行されません。この設定は、異なるカスタマーが同一スイッチの UNI または ENI に接続される場合のために設計されています。ただし、同一の UNI-ENI 独立 VLAN に属している場合でも、異なるスイッチ上の UNI または ENI 間では、スイッチングが許可されます。
- UNI-ENI コミュニティ VLAN：同一のコミュニティ VLAN に属するスイッチ上の UNI および ENI 間で、ローカル スイッチングが許可されます。UNI または ENI が同一カスタマーに属する場合に、ポート間でパケットをスイッチングするには、UNI-ENI コミュニティ VLAN として共通の VLAN を設定できます。UNI-ENI コミュニティ VLAN 内のポートと VLAN 外のポート間では、ローカル スイッチングは実行されません。スイッチでは、UNI-ENI コミュニティ VLAN の 8 つの UNI および ENI だけの組み合せをサポートします。

（注）　ローカル スイッチングは、同一コミュニティ VLAN の ENI および UNI との間で行われます。スパニング ツリーは UNI ではなく ENI でイネーブルに設定できるため、同一コミュニティ VLAN で ENI および UNI を設定する場合は注意が必要です。UNI は常に、フォワーディング ステートです。

NNI は、属している UNI-ENI VLAN のタイプの影響を受けません。VLAN タイプに関係なく、同一のスイッチまたは同一の VLAN に属する異なるスイッチ上の NNI 間、または NNI と UNI 間では、スイッチングが行われます。

図 12-2 の設定では、VLAN 10 が UNI-ENI 独立 VLAN で、VLAN 20 が UNI-ENI コミュニティ VLAN である場合、ローカル スイッチングは、ファスト イーサネット ポート 1 ～ 4 では実行されませんが、ファスト イーサネット ポート 6 ～ 10 では実行されます。VLAN 10 と VLAN 20 の両方の NNI は、同一の VLAN 内の UNI または ENI とパケットを交換できます。

図 12-2　Cisco ME スイッチの UNI-ENI 独立 VLAN および UNI コミュニティ VLAN



UNI または ENI は、アクセス ポート、トランク ポート、プライベート VLAN ポート、または IEEE 802.1Q トンネル ポートにできます。また、EtherChannel のメンバーにもできます。

IEEE 802.1Q トランク ポートとして設定されている UNI または ENI が UNI-ENI 独立 VLAN に属する場合、トランク上の VLAN は、異なるトランク ポートまたはアクセス ポート上の同一 VLAN ID と分離されます。トランク ポート上のその他の VLAN を、異なる タイプ（プライベート VLAN、UNI-ENI コミュニティ VLAN など）にできます。たとえば、UNI-ENI トランク ポート上の UNI アクセス ポートおよび 1 つの VLAN は、同じ UNI 独立 VLAN に属することができます。この場合、UNI アクセス ポートと UNI トランク ポート上の VLAN 間で分離が行われます。その他のアクセス ポートおよびトランク ポート上のその他の VLAN は、異なる VLAN に属するため、分離されます。

UNI、ENI、および NNI は常に、異なる VLAN 上のポートから分離されます。

VLAN の作成および変更

VLAN を作成して、いくつかのパラメータを変更するには、**vlan** グローバル コンフィギュレーション コマンドを入力して、VLAN コンフィギュレーション モードにアクセスします。さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバーシップ モードの定義、VLAN に対するポートの追加および削除を行います。このモードのコマンド実行結果は実行コンフィギュレーション ファイルに書き込まれ、**show running-config** 特権 EXEC コマンドを入力することによって表示できます。

ここでは、VLAN の設定情報について説明します。

- 「イーサネット VLAN のデフォルト設定」（P.12-7）
- 「VLAN 設定時の注意事項」（P.12-8）
- 「イーサネット VLAN の作成または変更」（P.12-9）
- 「VLAN へのスタティックアクセス ポートの割り当て」（P.12-11）
- 「内部 VLAN ID を指定した拡張範囲 VLAN の作成」（P.12-12）
- 「UNI-ENI VLAN の設定」（P.12-13）

スイッチ上の MAC アドレス テーブルのスペースをさらに効率的に管理するために、特定の VLAN で MAC アドレス学習をディセーブルにして、MAC アドレスを学習する VLAN を制御できます。詳細については、「VLAN 上での MAC アドレス学習のディセーブル化」（P.5-29）を参照してください。

イーサネット VLAN のデフォルト設定

スイッチは、イーサネット インターフェイスだけをサポートしています。表 12-2 に、イーサネット VLAN のデフォルト設定を示します。

（注）　拡張範囲 VLAN 上では、MTU サイズ、プライベート VLAN、リモート SPAN、および UNI-ENI VLAN 設定だけを変更できます。他のすべての特性は、デフォルト条件のままにしておく必要があります。

表 12-2　イーサネット VLAN のデフォルト値および範囲

パラメータ	デフォルト	範囲
VLAN ID	1	1 ～ 4094 （注）　拡張範囲 VLAN（VLAN ID が 1006 ～ 4094）は VLAN データベースに保存されません。
VLAN name	*VLANxxxx*、ここで *xxxx* は VLAN ID である 4 桁の数字（先頭の 0 を含む）	範囲なし
IEEE 802.10 SAID	100001（100000 + VLAN ID）	1 ～ 4294967294
MTU size	1500	1500 ～ 9198
Translational bridge 1	0	0 ～ 1005
Translational bridge 2	0	0 ～ 1005
VLAN state	active	アクティブ、中断
Remote SPAN	ディセーブル	イネーブル、ディセーブル
プライベート VLAN	設定なし	2 ～ 1001、1006 ～ 4094
UNI-ENI VLAN	UNI-ENI 独立 VLAN	2 ～ 1001、1006 ～ 4094 VLAN 1 は常に、UNI-ENI 独立 VLAN です。

VLAN 設定時の注意事項

ネットワーク内で VLAN を作成または変更するときは、次の注意事項に従ってください。

- スイッチは、1005 の VLAN をサポートします。
- 標準範囲の VLAN は、1 ～ 1001 の番号で識別されます。VLAN 番号の 1002 ～ 1005 は、トークン リングおよび Fiber Distributed Data Interface（FDDI）VLAN 用です。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは、FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを転送しません。
- VLAN 1 ～ 1005 の VLAN 設定は常に、VLAN データベースおよびスイッチの実行コンフィギュレーション ファイルに保存されます。
- VLAN 1006 ～ 4094（拡張範囲 VLAN）の設定オプションは、MTU、RSPAN VLAN、プライベート VLAN、および UNI-ENI VLAN に限定されます。拡張範囲 VLAN は、VLAN データベースに追加されません。

- STP は、デフォルトですべての VLAN 上の NNI に対してだけイネーブルです。ENI で STP を設定できます。同一 VLAN の NNI および ENI は、同一スパニング ツリー インスタンスにあります。128 のスパニング ツリー インスタンスが、このスイッチによってサポートされます。サポートされるスパニング ツリー インスタンスを超える数のアクティブ VLAN がスイッチに設定されている場合は、128 の VLAN でスパニング ツリーをイネーブルに設定できますが、残りの VLAN ではディセーブルに設定します。スイッチ上で使用可能なすべてのスパニング ツリー インスタンスをすでに使用している場合、VLAN をさらに 1 つ追加すると、そのスイッチ上にスパニング ツリーを実行しない VLAN が作成されます。（すべての VLAN を許可するための）スイッチのトランク ポートにデフォルトの許可リストが設定されていると、すべてのトランク ポートに新しい VLAN が割り当てられます。ネットワークのトポロジに応じて、新しい VLAN 内に阻止されないループが作成されることがあります。特に、複数の隣接スイッチでスパニング ツリー インスタンスをすべて使用してしまっている場合は、注意してください。このような事態を防ぐには、スパニング ツリー インスタンスの割り当てを使い切っているスイッチのトランク ポートに、許可リストを設定します。

  スイッチ上の VLAN 数がサポートされるスパニング ツリー インスタンス数を超える場合は、IEEE 802.1s Multiple STP（MSTP）をスイッチに設定して、複数の VLAN を単一のスパニング ツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 16 章「MSTP の設定」を参照してください。

  （注）　MSTP は、STP がイネーブルに設定されている NNI または ENI でだけサポートされています。

- スイッチ上の各ルーテッド ポートは、内部 VLAN を使用するために作成します。この内部 VLAN は拡張範囲 VLAN 番号を使用し、その内部 VLAN ID は拡張範囲 VLAN には使用できません。内部 VLAN として割り当て済みの VLAN ID を指定して拡張範囲 VLAN を作成すると、エラー メッセージが生成され、コマンドは拒否されます。
  - 内部 VLAN ID は拡張範囲の下部の方なので、拡張範囲 VLAN を作成するには最大の番号（4094）から始めて最小値（1006）へと動いて、内部 VLAN ID を使用する可能性を減らすことを推奨します。
  - 拡張範囲 VLAN を設定する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、どの VLAN が内部 VLAN として割り当てられているかを確認します。
  - 必要に応じて内部 VLAN に割り当てられたルーテッド ポートをシャットダウンします。これにより、内部 VLAN が解放され、拡張範囲 VLAN を作成してポートを再度イネーブルにし、別の VLAN を内部 VLAN として使用します。「内部 VLAN ID を指定した拡張範囲 VLAN の作成」（P.12-12）を参照してください。
- スイッチは合計 1005（標準範囲および拡張範囲）の VLAN をサポートしますが、ルーテッド ポート、SVI、その他の設定済み機能の個数によって、スイッチのハードウェアの使用は左右されます。拡張範囲の VLAN を作成しようとしたときに、使用可能なハードウェア リソースが不十分な場合は、エラー メッセージが生成され、拡張範囲の VLAN は拒否されます。

イーサネット VLAN の作成または変更

VLAN コンフィギュレーション モードにアクセスするには、VLAN ID を指定して **vlan** グローバル コンフィギュレーション コマンドを入力します。VLAN を新規に作成するには新しい VLAN ID を、既存の VLAN を変更するには、その VLAN ID を入力します。デフォルトの VLAN 設定（表 12-2 を参照）を使用するか、複数のコマンドを入力して VLAN を設定します。

（注）　拡張範囲 VLAN は、デフォルトの イーサネット VLAN 特性を使用し、変更可能なパラメータは、MTU、プライベート VLAN、RSPAN、および UNI-ENI VLAN 設定に限られます。

このモードで使用できるコマンドの詳細については、このリリースのコマンド リファレンスに記載されている **vlan** グローバル コンフィギュレーション コマンドを参照してください。設定が終了したら、設定が有効になるように VLAN コンフィギュレーション モードを終了する必要があります。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN ID 1 ～ 1005 の設定は常に、VLAN 番号および VLAN 名とともに VLAN データベース（valn.dat ファイル）およびスイッチの実行コンフィギュレーション ファイルに保存されます。拡張範囲 VLAN は VLAN データベースに保存されません。スイッチの実行コンフィギュレーション ファイルに保存されます。**copy running-config startup-config** 特権 EXEC コマンドを使用すると、スイッチのスタートアップ コンフィギュレーション ファイルに VLAN の設定を保存できます。

（注）　拡張範囲 VLAN を作成する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、VLAN ID が内部的に使用されていないことを確認します。VLAN ID が内部的に使用されている場合に、それを解放するには、「内部 VLAN ID を指定した拡張範囲 VLAN の作成」（P.12-12）を参照してから拡張範囲 VLAN を作成してください。

イーサネット VLAN を作成または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。VLAN を新規に作成するには新しい VLAN ID を、既存の VLAN を変更するには、その VLAN ID を入力します。このコマンドで使用できる VLAN ID の範囲は、1 ～ 4094 です。 （注）　新しく作成された VLAN は、デフォルトで UNI-ENI 独立 VLAN になります。
ステップ 3	**name** *vlan-name*	（任意および標準範囲 VLAN でだけサポート）VLAN の名前を入力します。VLAN 名を入力しない場合には、VLAN データベースのデフォルトとして、文字列 VLAN の後ろに先行 0 付きで *vlan-id* が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 です。
ステップ 4	**mtu** *mtu-size*	（任意）MTU サイズを変更します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	設定を確認します。**name** オプションは、VLAN ID 1 ～ 1005 に限り有効です。
ステップ 7	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

VLAN を削除するには、**no vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。VLAN 1 および VLAN 1002 ～ 1005 は削除できません。

注意　VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブな状態で）対応付けられたままとなります。

VLAN 名をデフォルト設定に戻すには、**no name**、または **no mtu** VLAN コンフィギュレーション コマンドを使用します。

次の例は、イーサネット VLAN 20 を作成し、*test20* と名前を付け、VLAN データベースに追加する方法を示しています。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

次の例は、すべてのデフォルト特性を備えた新しい拡張範囲 VLAN を作成し、config-vlan モードを開始し、スイッチのスタートアップ コンフィギュレーション ファイルに新しい VLAN を保存する方法を示しています。

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

VLAN へのスタティックアクセス ポートの割り当て

VLAN にスタティックアクセス ポートを割り当てられます。

（注）　存在しない VLAN にインターフェイスを割り当てると、新しく VLAN が作成されます （「イーサネット VLAN の作成または変更」（P.12-9）を参照）。

VLAN データベース内の VLAN にポートを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	VLAN に追加されるインターフェイスを入力します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport mode access**	ポート（レイヤ 2 アクセス ポート）の VLAN メンバーシップ モードを定義します。
ステップ 5	**switchport access vlan** *vlan-id*	VLAN にポートを割り当てます。指定できる VLAN ID は、1 ～ 4094 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface** *interface-id*	インターフェイスの VLAN メンバーシップ モードを確認します。
ステップ 8	**show interfaces** *interface-id* **switchport**	表示された *Administrative Mode* フィールドおよび *Access Mode VLAN* フィールドの設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスの設定をデフォルトに戻すには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。

次に、VLAN 2 のアクセス ポートとしてポートを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

内部 VLAN ID を指定した拡張範囲 VLAN の作成

内部 VLAN に割り当て済みの拡張範囲 VLAN ID を入力すると、エラー メッセージが表示され、拡張範囲 VLAN は拒否されます。内部 VLAN ID を手動で解放するには、内部 VLAN ID を使用しているルーテッド ポートを一時的にシャットダウンする必要があります。

内部 VLAN に割り当てられた VLAN ID を解放してその ID で拡張範囲 VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**show vlan internal usage**	スイッチが内部的に使用している VLAN ID を表示します。使用したい VLAN ID が内部 VLAN の場合は、その VLAN ID を使用しているルーテッド ポートが表示されます。そのポート番号をステップ 3 で入力してください。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	その VLAN ID を使用しているルーテッド ポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**shutdown**	ポートをシャットダウンして内部 VLAN ID を解放します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**vlan** *vlan-id*	新しい拡張範囲 VLAN ID を入力し、config-vlan モードを開始します。
ステップ 7	**exit**	config-vlan モードを終了してグローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ステップ 4 でシャットダウンしたルーテッド ポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**no shutdown**	ルーテッド ポートを再度イネーブルにします。新しい内部 VLAN ID が割り当てられます。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

UNI-ENI VLAN の設定

デフォルトでは、スイッチ上で設定されるすべての VLAN は、UNI-ENI 独立 VLAN です。VLAN 設定は、UNI-ENI コミュニティ VLAN、プライベート VLAN、または RSPAN VLAN の設定に変更できます。また、これらのいずれかの VLAN 設定をデフォルトの UNI-ENI 独立 VLAN に戻すこともできます。

設定時の注意事項

次に、UNI-ENI VLAN 設定時の注意事項について説明します。

- UNI-ENI 独立 VLAN は、NNI ポートに影響しません。
- UNI-ENI コミュニティ VLAN は従来の VLAN と同様ですが、設定できるのは最大 8 つの UNI および ENI の組み合せである点だけ異なります。
- VLAN タイプを変更するには、最初に **vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力して、VLAN コンフィギュレーション モードを開始します。
  - VLAN を UNI-ENI 独立 VLAN からプライベート VLAN に変更するには、**private-vlan** VLAN コンフィギュレーション モード コマンドを入力します。
  - UNI-ENI コミュニティ VLAN をプライベート VLAN に変更するには、**no uni-vlan** VLAN コンフィギュレーション モード コマンドを入力してまずコミュニティ VLAN のタイプを削除する必要があります。次に、**private-vlan** VLAN コンフィギュレーション コマンドを入力します。
  - VLAN を UNI-ENI 独立 VLAN から RSPAN VLAN に変更するには、**rspan-vlan** VLAN コンフィギュレーション モード コマンドを入力します。
  - UNI-ENI コミュニティ VLAN を RSPAN VLAN に変更するには、**no uni-vlan** VLAN コンフィギュレーション モード コマンドを入力してまずコミュニティ VLAN を削除する必要があります。次に、**rspan-vlan** VLAN コンフィギュレーション コマンドを入力します。
  - プライベート VLAN を UNI-ENI VLAN に変更するには、**no private-vlan** VLAN コンフィギュレーション モード コマンドを入力してまずプライベート VLAN のタイプを削除する必要があります。次に、**uni-vlan** VLAN コンフィギュレーション コマンドを入力します。
  - RSPAN VLAN を UNI-ENI VLAN に変更するには、**no rspan-vlan** VLAN コンフィギュレーション モード コマンドを入力してまず RSPAN VLAN のタイプを削除する必要があります。次に、**uni-vlan** VLAN コンフィギュレーション コマンドを入力します。
- スイッチでは、コミュニティ VLAN の合計 8 つの UNI および ENI をサポートします。9 つ以上の UNI および ENI が VLAN に属している場合は、VLAN を UNI-ENI コミュニティとして設定できません。
- すでに 8 つの UNI および ENI が指定されている UNI-ENI コミュニティ VLAN に UNI または ENI スタティック アクセス ポートを追加しようすると、設定が拒否されます。8 つの UNI または ENI が設定されている UNI-ENI コミュニティ VLAN に、UNI または ENI ダイナミック アクセス ポートを追加すると、ポートはエラー ディセーブル ステートになります。
- 同一コミュニティ VLAN に ENI および UNI を設定する場合は注意してください。ローカル スイッチングがコミュニティ VLAN の ENI および UNI の間で行われます、ENI はスパニング ツリーをサポートしますが、UNI はサポートしません。

UNI-ENI VLAN の設定

デフォルトでは、スイッチ上で作成されるすべての VLAN は、UNI-ENI 独立 VLAN です。この設定は、UNI-ENI コミュニティ VLAN、プライベート VLAN、または RSPAN VLAN に変更できます。プライベート VLAN または RSPAN VLAN の設定手順については、第 13 章「プライベート VLAN の設定」および 第 27 章「SPAN および RSPAN の設定」を参照してください。

UNI-ENI VLAN のタイプを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。VLAN を新規に作成するには新しい VLAN ID を、既存の VLAN を変更するには、その VLAN ID を入力します。デフォルトでは、VLAN は UNI-ENI 独立 VLAN です。 **（注）**　このコマンドで使用できる VLAN ID の範囲は、1 ～ 4094 です。
ステップ 3	**uni-vlan** {**community** | **isolated**}	UNI-ENI の VLAN タイプを設定します。 • デフォルトから UNI-ENI コミュニティ VLAN に変更するには、**community** を入力します。 • デフォルトの UNI-ENI 独立 VLAN に戻すには、**isolated** を入力します。 **（注）**　VLAN 1 は常に UNI-ENI 独立 VLAN です。VLAN 1 を UNI-ENI コミュニティ VLAN として設定できません。予約 VLAN 1002 ～ 1005 は、イーサネット VLAN です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show vlan uni-vlan** [**type**]	UNI-ENI の VLAN 情報を表示します。VLAN ID および UNI-ENI VLAN のタイプだけを参照するには、**type** を入力します（任意）。
ステップ 6	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

デフォルト（UNI-ENI 独立 VLAN）に戻るには、**no uni-vlan** VLAN コンフィギュレーション コマンドを使用します。**uni-vlan isolated** コマンドを入力すると、**uni-vlan** VLAN コンフィギュレーション コマンドを入力した場合と同じ結果になります。**show vlan** および **show vlan** *vlan-id* の各特権 EXEC コマンドでも、UNI-ENI VLAN 情報を表示できますが、UNI-ENI コミュニティ VLAN だけが表示されます。独立 VLAN およびコミュニティ VLAN の両方を表示するには、**show vlan uni-vlan type** コマンドを使用します。

VLAN の表示

拡張範囲 VLAN を含めてスイッチ上のすべての VLAN のリストを表示するには、**show vlan** 特権 EXEC コマンドを使用します。この表示には、VLAN ステータス、ポート、および設定情報が含まれます。表 12-3 に、VLAN モニタリング用のその他の特権 EXEC コマンドを示します。

表 12-3　VLAN モニタ コマンド

コマンド	目的
show interfaces [**vlan** *vlan-id*]	スイッチに設定されたすべてのインターフェイス、または指定されたインターフェイスの特性を表示します。
show vlan [**id** *vlan-id*]	スイッチのすべての、または指定された VLAN のパラメータを表示します。
show vlan [*vlan-name*] **uni-vlan type**	UNI-ENI 独立 VLAN または UNI-ENI コミュニティ VLAN を、VLAN 名で表示します。
show vlan uni-vlan	スイッチ上の UNI-ENI コミュニティ VLAN および関連付けられたポートを表示します。
show vlan uni-vlan type	スイッチ上の UNI-ENI 独立 VLAN および UNI-ENI コミュニティ VLAN を、VLAN ID で表示します。

show コマンドのオプションと出力フィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

VLAN トランクの設定

- 「トランキングの概要」（P.12-15）
- 「レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定」（P.12-17）
- 「トランク ポートとしてのイーサネット インターフェイスの設定」（P.12-17）
- 「トランク ポートの負荷分散の設定」（P.12-20）

トランキングの概要

トランクは、1 つまたは複数のイーサネット スイッチ インターフェイスと、ルータやスイッチといった他のネットワーキング デバイス間のポイントツーポイント リンクです。イーサネット トランクは 1 つのリンクを介して複数の VLAN トラフィックを搬送するので、VLAN をネットワーク全体に拡張することができます。スイッチは、IEEE 802.1Q 業界標準トランキング カプセル化をサポートします。

トランクを設定できるのは、1 つのイーサネット インターフェイスまたは 1 つの EtherChannel バンドルに対してです。EtherChannel の詳細については、第 35 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

イーサネット インターフェイスは、各種トランキング モードをサポートしています（表 12-4 を参照）。インターフェイスをトランキングまたは非トランキングとして設定できます。

- リンクをトランキングしない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用してトランキングをディセーブルにします。
- トランキングをイネーブルにするには、**switchport mode trunk** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスをトランクに変更します。

表 12-4　レイヤ 2 インターフェイス モード

モード	機能
switchport mode access	インターフェイス（アクセス ポート）は永続的な非トランキング モードになり、リンクを非トランク リンクに変換するようにネゴシエーションを行います。インターフェイスは、近接インターフェイスがトランク インターフェイスであるかどうかに関係なく、非トランク インターフェイスになります。これがデフォルトのモードです。
switchport mode trunk	インターフェイスは永続的なトランキング モードになり、近接リンクをトランク リンクに変換するようにネゴシエーションを行います。近接インターフェイスがトランク インターフェイスでなくても、インターフェイスはトランク インターフェイスになります。
switchport mode dot1q-tunnel	インターフェイスをトンネル（非トランキング）ポートとして設定し、IEEE 802.1Q トランク ポートと非対称リンクで接続されるようにします。IEEE 802.1Q トンネリングは、サービス プロバイダー ネットワーク全体でカスタマー VLAN の整合性を維持するのに使用されます。トンネル ポートについての詳細は、第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。
switchport mode private-vlan	インターフェイスをプライベート VLAN ホストまたはプロミスキャス ポートとして設定します（プロミスキャス ポートとして設定できるのは NNI だけです）。プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。

IEEE 802.1Q の設定に関する注意事項

IEEE 802.1Q トランクでは、ネットワークのトランキング方式に次の制約があります。

- IEEE 802.1Q トランクを使用して接続したシスコ製スイッチのネットワークでは、スイッチはトランク上で許可された VLAN ごとに 1 つのスパニング ツリー インスタンスを維持します。他社製のデバイスは、すべての VLAN に対して 1 つのスパニング ツリー インスタンスをサポートする場合があります。

  IEEE 802.1Q トランクを使用して他社製のデバイスにシスコ製スイッチを接続する場合、シスコ製スイッチは、トランクの VLAN のスパニング ツリー インスタンスを他社製 IEEE 802.1Q スイッチのスパニング ツリー インスタンスと結合します。ただし、各 VLAN のスパニング ツリー情報は、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離されたシスコ製スイッチによって維持されます。シスコ製スイッチを分離する他社製の IEEE 802.1Q スイッチ クラウドは、スイッチ間の 1 つのトランク リンクとして取り扱われます。

- IEEE 802.1Q トランクに対応するネイティブ VLAN が、トランク リンクの両端で一致していなければなりません。トランクの一方のネイティブ VLAN ともう一方のネイティブ VLAN が異なっていると、スパニング ツリー ループが発生する可能性があります。

- ネットワーク内のすべての VLAN でスパニング ツリーをディセーブルにしないまま、IEEE 802.1Q トランクのネイティブ VLAN でスパニング ツリーをディセーブルにすると、スパニング ツリー ループが発生する可能性があります。IEEE 802.1Q トランクのネイティブ VLAN でスパニング ツリーをイネーブルのままにしておくか、または、ネットワーク内のすべての VLAN でスパニング ツリーをディセーブルにしてください。また、ネットワークにループがないことを確認してから、スパニング ツリーをディセーブルにしてください。

レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

表 12-5 に、レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定を示します。

表 12-5　レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
インターフェイス モード	**switchport mode access**
許可 VLAN 範囲	VLAN 1 ～ 4094
デフォルト VLAN（アクセス ポート用）	VLAN 1
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1

トランク ポートとしてのイーサネット インターフェイスの設定

- 「他の機能との相互作用」（P.12-17）
- 「トランク上での許可 VLAN の定義」（P.12-18）
- 「タグなしトラフィック用ネイティブ VLAN の設定」（P.12-20）
- 「タグなしトラフィック用ネイティブ VLAN の設定」（P.12-20）

他の機能との相互作用

トランキングは、次のように他の機能と相互作用します。

- トランク ポートはセキュア ポートにできません。
- トランク ポートはトンネル ポートにできません。
- トランク ポートは EtherChannel ポート グループにまとめることができますが、グループ内のすべてのトランクは同じ設定にしておく必要があります。グループを初めて作成したときは、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次に示すパラメータのいずれかの設定を変更すると、スイッチは、入力された設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト
  - 各 VLAN の STP ポート プライオリティ。
  - STP PortFast の設定値。

（注）　デフォルトでは、STP は NNI でサポートされていますが、ENI ではイネーブルに設定する必要があります。UNI では STP はサポートされていません。

  - トランク ステータス：ポート グループ内の 1 つのポートがトランクでなくなった場合、すべてのポートがトランクでなくなります。
- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをトランクに変更しようとしても、ポート モードは変更されません。

トランク ポートの設定

IEEE 802.1Q トランク ポートとしてポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	トランキング用に設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport mode trunk**	インターフェイスをレイヤ 2 トランクとして設定します。
ステップ 5	**switchport access vlan** *vlan-id*	（任意）デフォルト VLAN を指定します。これは、インターフェイスがトランキングを停止した場合に使用されます。
ステップ 6	**switchport trunk native vlan** *vlan-id*	IEEE 802.1Q トランク用にネイティブ VLAN を指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** *interface-id* **switchport**	*Administrative Mode* フィールドに、インターフェイスのスイッチポート設定を表示します。
ステップ 9	**show interfaces** *interface-id* **trunk**	インターフェイスのトランク設定を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスの設定をデフォルトに戻すには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。トランキング インターフェイスのすべてのトランキング特性をデフォルトにリセットするには、**no switchport trunk** インターフェイス コンフィギュレーション コマンドを使用します。トランキングをディセーブルにするには、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用してポートをスタティックアクセス ポートとして設定します。

次に、VLAN 33 をネイティブ VLAN として、ポートを IEEE 802.1Q トランクとして設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 33
Switch(config-if)# end
```

トランク上での許可 VLAN の定義

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックの送受信を行います。各トランクで、すべての VLAN ID（1 ～ 4094）が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。トランクが伝送するトラフィックを制限するには、**switchport trunk allowed vlan remove** *vlan-list* インターフェイス コンフィギュレーション コマンドを使用して、許可リストから特定の VLAN を削除します。

（注）　VLAN 1 は、すべてのシスコ製スイッチ内のすべてのトランクポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を常にイネーブルにしておく必要がありました。VLAN 1 の最小化機能により、VLAN 1 を任意の個々の VLAN トランク リンクでディセーブルにして、ユーザ トラフィック（スパニング ツリー アドバタイズを含む）が VLAN 1 で送受信されないようにできます。これは、許可 VLAN リストから VLAN 1 を削除することにより、実行します。

スパニング ツリー ループまたはストームの危険性を減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除しても、インターフェイスは、VLAN 1 の Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）、Link Aggregation Control Protocol（LACP; リンク レイヤ検出プロトコル）などの管理トラフィックを送受信し続けます。

VLAN 1 がディセーブルなトランク ポートが非トランク ポートに変換された場合は、アクセス VLAN に追加されます。アクセス VLAN が 1 に設定されている場合、**switchport trunk allowed** 設定に関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルなすべての VLAN について、同じことが当てはまります。

トランクポートは、VLAN がイネーブルになっていて、かつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバーになることができます。

IEEE802.1Q トランクの許可リストを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 5	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*	（任意）トランク上で許可される VLAN のリストを設定します。 **add**、**all**、**except**、および **remove** の各キーワードの使用法については、このリリースのコマンド リファレンスを参照してください。 *vlan-list* パラメータは、1 ～ 4094 のうちいずれか 1 つの VLAN 番号か、値の小さい方を先にしてハイフンで区切られた 2 つの VLAN 番号で指定する一定範囲の VLAN です。カンマで区切られた VLAN パラメータやハイフンで指定された範囲の間には、スペースは入れないでください。 デフォルトではすべての VLAN が許可されています。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id* **switchport**	表示された *Trunking VLANs Enabled* フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

すべての VLAN の許可 VLAN リストをデフォルトに戻すには、**no switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用します。

次の例は、ポートの許可 VLAN リストから VLAN 2 を削除する方法を示しています。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

タグなしトラフィック用ネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、スイッチはタグなしトラフィックをポートに設定されたネイティブ VLAN に伝送します。ネイティブ VLAN は、デフォルトでは VLAN 1 です。

（注）　ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

IEEE 802.1Q 設定の詳細については、「IEEE 802.1Q の設定に関する注意事項」（P.12-16）を参照してください。

IEEE802.1Q トランクでネイティブ VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	IEEE 802.1Q トランクとして設定されているインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport trunk native vlan** *vlan-id*	トランク ポート上でタグなしトラフィックを送受信している VLAN を設定します。 *vlan-id* では、指定できる範囲は 1 ～ 4094 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport**	表示された *Trunking Native Mode VLAN* フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ネイティブ VLAN をデフォルトの VLAN 1 に戻すには、**no switchport trunk native vlan** インターフェイス コンフィギュレーション コマンドを使用します。

パケットの VLAN ID が送信ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで転送されます。同じでない場合、スイッチはそのパケットをタグ付きで転送します。

トランク ポートの負荷分散の設定

負荷分散により、スイッチに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、スイッチ間で 1 つのパラレル リンク以外のすべてのリンクをブロックします。負荷分散を行うと、トラフィックが属する VLAN に基づいて、リンク間でトラフィックが分割されます。

STP がイネーブルに設定されているトランクポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使用します。STP ポート プライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リンクを同じスイッチに接続する必要があります。STP パスコストを使用して負荷分散を設定する場合には、それぞれの負荷分散リンクを同じスイッチに、または 2 台の異なるスイッチに接続することができます。STP の詳細については、第 15 章「STP の設定」を参照してください。

STP ポート プライオリティによる負荷分散

同一スイッチ上の 2 つのポートがループを形成すると、スイッチが STP ポート プライオリティを使用してイネーブルになるポートとブロッキング ステートになるポートを決定します。パラレル STP トランク ポートにプライオリティを設定すると、そのポートは、特定の VLAN のすべてのトラフィックを搬送させることができます。VLAN に対するプライオリティがより高い（より小さい値）トランク ポートがその VLAN のトラフィックを伝送します。同じ VLAN に対してプライオリティのより低い（より大きい値）トランク ポートは、その VLAN に対してブロッキング ステートのままです。1 つのトランク ポートがその VLAN に関するすべてのトラフィックを送受信することになります。

図 12-3 に、サポート対象スイッチを接続する 2 つのトランクを示します。この例では、スイッチは次のように設定されています。

- VLAN 8 ～ 10 は、トランク 1 でポート プライオリティ 16 が割り当てられています。
- VLAN 3 ～ 6 は、トランク 1 でデフォルトのポート プライオリティ 128 のままです。
- VLAN 3 ～ 6 は、トランク 2 でポート プライオリティ 16 が割り当てられています。
- VLAN 8 ～ 10 は、トランク 2 でデフォルトのポート プライオリティ 128 のままです。

このように設定すると、トランク 1 が VLAN 8 ～ 10 のトラフィックを搬送し、トランク 2 が VLAN 3 ～ 6 のトラフィックを搬送します。アクティブ トランクで障害が起きた場合には、プライオリティのより低いトランクが引き継ぎ、すべての VLAN のトラフィックを搬送します。どのトランク ポート上でも、トラフィックの重複は発生しません。

図 12-3　　STP ポート プライオリティによる負荷分散

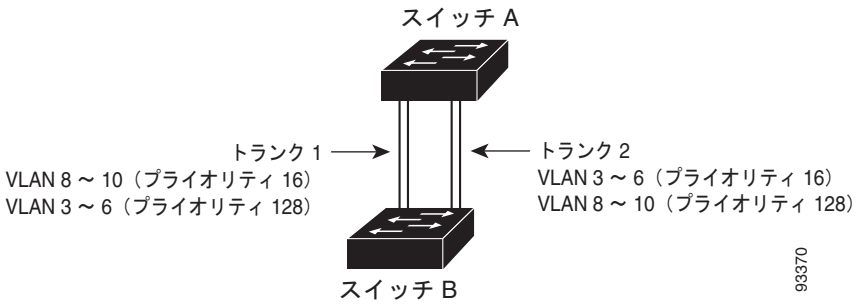


図 12-3 に示すネットワークを設定するには、スイッチ A で特権 EXEC モードで次の手順を実行します。インターフェイス番号には任意の数を使用できますが、表示されている番号はほんの一例であることに注意してください。

	コマンド	目的
ステップ 1	**show vlan**	参照された VLAN がスイッチ A に存在していることを確認します。存在しない場合、VLAN ID を入力して VLAN を作成します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface gigabitethernet 0/1**	トランク 1 インターフェイスとして設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**port-type {nni | eni}**	インターフェイスを NNI または ENI として設定します。UNI では、STP はサポートされていません。ポートを ENI として設定する場合、**spanning-tree** インターフェイス コンフィギュレーション コマンドを使用して、ポートの STP もイネーブルに設定する必要があります。
ステップ 5	**switchport mode trunk**	ポートをトランク ポートとして設定します。

	コマンド	目的
ステップ 6	**spanning-tree vlan 8-10 port-priority 16**	トランク 1 上の VLAN 8 ～ 10 にポート プライオリティ 16 を割り当てます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces gigabitethernet 0/1 switchport**	ポートの設定を確認します。
ステップ 9	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface gigabitethernet 0/2**	トランク 2 インターフェイスとして設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**port-type {nni | eni}**	インターフェイスを NNI または ENI として設定します。UNI では、STP はサポートされていません。ポートを ENI として設定する場合、**spanning-tree** インターフェイス コンフィギュレーション コマンドを使用して、ポートの STP もイネーブルに設定する必要があります。
ステップ 12	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 13	**spanning-tree vlan 3-6 port-priority 16**	トランク 2 上の VLAN 3 ～ 6 にポート プライオリティ 16 を割り当てます。
ステップ 14	**end**	特権 EXEC モードに戻ります。
ステップ 15	**show interfaces gigabitethernet 0/2 switchport**	ポートの設定を確認します。
ステップ 16	**show running-config**	設定を確認します。
ステップ 17	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ B で同じ手順を使用して、トランク 1 のトランク ポートで VLAN 8 ～ 10 のスパニング ツリー ポート プライオリティ を 16 にして設定し、トランク 2 のトランク ポートで VLAN 3 ～ 6 のスパニング ツリー ポート プライオリティ を 16 にして設定します。

STP パス コストによる負荷分散

トランクに異なるパス コストを設定し、各パス コストを異なる VLAN セットに対応付け、VLAN ごとに異なるポートをブロッキングすることにより、VLAN トラフィックを分担するようにパラレル トランクを設定できます。VLAN は、トラフィックを個別に保持し、リンクが失われても冗長性を維持します。

図 12-4 で、トランク ポート 1 および 2 は 100BASE-T ポートとして設定されています。次の VLAN パス コストが割り当てられています。

- VLAN 2 ～ 4 には、トランク ポート 1 でパス コスト 30 が割り当てられています。
- VLAN 8 ～ 10 は、トランク ポート 1 で 100BASE-T のデフォルトのパス コスト 19 のままになっています。
- VLAN 8 ～ 10 には、トランク ポート 2 でパス コスト 30 が割り当てられています。
- VLAN 2 ～ 4 は、トランク ポート 2 で 100BASE-T のデフォルトのパス コスト 19 のままになっています。

図 12-4　パス コストによってトラフィックが分散される負荷分散トランク

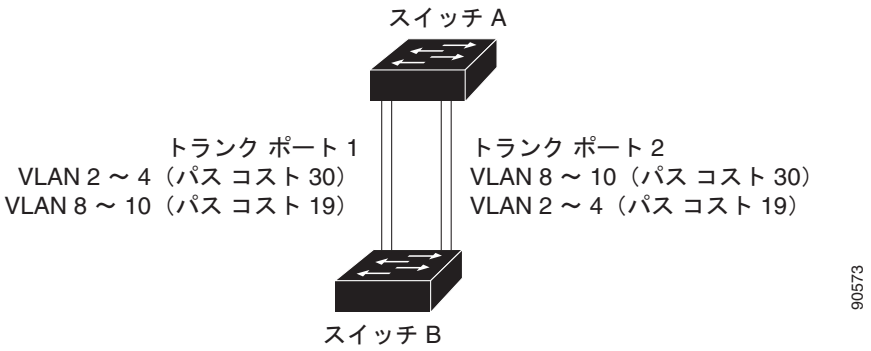


図 12-4 に示すネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface fastethernet0/1**	トランク ポート 1 として設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**port-type {nni | eni}**	インターフェイスを NNI または ENI として設定します。UNI では、STP はサポートされていません。ポートを ENI として設定する場合、**spanning-tree** インターフェイス コンフィギュレーション コマンドを使用して、ポートの STP もイネーブルに設定する必要があります。
ステップ 4	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface fastethernet0/2**	トランク ポート 2 として設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**port-type {nni | eni}**	インターフェイスを NNI または ENI として設定します。UNI では、STP はサポートされていません。ポートを ENI として設定する場合、**spanning-tree** インターフェイス コンフィギュレーション コマンドを使用して、ポートの STP もイネーブルに設定する必要があります。
ステップ 8	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config**	設定を確認します。表示で、ステップ 2 および 7 で設定されたインターフェイスはトランク ポートとして設定されていることを確認します。
ステップ 11	**show vlan**	スイッチ A で、VLAN 2 ～ 4 および 8 ～ 10 が設定されていることを確認します。設定されていない場合は、これらの VLAN を作成します。
ステップ 12	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**interface fastethernet0/1**	トランク ポート 2 でインターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**spanning-tree vlan 2-4 cost 30**	VLAN 2 ～ 4 に対し、スパニング ツリー パス コストを 30 に設定します。
ステップ 15	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**interface fastethernet0/2**	トランク ポート 2 でインターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 17	**spanning-tree vlan 8-10 cost 30**	VLAN 2 ～ 4 に対し、スパニング ツリー パス コストを 30 に設定します。
ステップ 18	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 19		スイッチ A に設定済みのその他のトランク インターフェイスに対してステップ 9 ～ 11 を繰り返し、VLAN 8、9、10 に対して、スパニング ツリー パス コストを 30 に設定します。
ステップ 20	**exit**	特権 EXEC モードに戻ります。
ステップ 21	**show running-config**	設定を確認します。表示内で、両方のトランク インターフェイスに対してパス コストが正しく設定されていることを確認します。
ステップ 22	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ B で同じ手順を使用して、トランク 1 のトランク ポートで VLAN 2 ～ 4 のパス コストを 30 にして設定し、トランク 2 のトランク ポートで VLAN 8 ～ 10 のパス コストを 30 にして設定します。

VMPS の設定

VLAN Query Protocol（VQP）は、ダイナミック アクセス ポートをサポートします。ダイナミック アクセス ポートは、永続的には VLAN に割り当てられませんが、ポート上で認識された MAC 送信元アドレスに基づいて VLAN に割り当てられます。

（注）　UNI および ENI に限り、ダイナミック アクセス ポートとして設定できます。NNI は VQP に参加できません。

スイッチは、不明の MAC アドレスを認識するたびに、VQP クエリーをリモート VMPS に送信します。クエリーには、新たに認識された MAC アドレスと認識元のポートが含まれます。VMPS は、ポートの VLAN 割り当てと一緒に応答を返します。このスイッチは VMPS サーバとしては使用できませんが、VMPS のクライアントとして動作し、VQP を介して VMPS と通信します。

- 「VMPS の概要」（P.12-24）
- 「VMPS クライアントのデフォルト設定」（P.12-26）
- 「VMPS 設定時の注意事項」（P.12-26）
- 「VMPS クライアントの設定」（P.12-26）
- 「VMPS のモニタ」（P.12-29）
- 「ダイナミック アクセス ポート VLAN メンバーシップのトラブルシューティング」（P.12-30）
- 「VMPS の構成例」（P.12-30）

VMPS の概要

クライアント スイッチは、新たなホストの MAC アドレスを受け取るたびに、VQP クエリーを VMPS に送信します。VMPS は、このクエリーを受信すると、自身のデータベースで MAC アドレス /VLAN 間のマッピングを検索します。サーバはこのマッピングと、サーバがオープン モードかセキュア モードであるかに基づいて応答を返します。セキュア モードでは、サーバは、違法なホストを検出すると、そのポートをシャットダウンします。オープン モードでは、サーバは単にポートへのホストのアクセスを拒否するだけです。

ポートが現在*未割り当て（unassigned）*の場合（つまり、まだ VLAN に割り当てられていない）、VMPS は次の応答のいずれかを返します。

- ホストがポート上で許可されている場合、VMPS は、割り当てられた VLAN 名を含み、ホストへのアクセスを許可する *VLAN 割り当て（vlan-assignment）*の応答をクライアントに送信します。
- ホストがポート上で許可されておらず、かつ、VMPS がオープン モードの場合、VMPS は*アクセス拒否（access-denied）*の応答を送信します。
- VLAN がポート上で許可されておらず、かつ、VMPS がセキュア モードの場合、VMPS は*ポート シャットダウン（port-shutdown）*の応答を送信します。

ポートがすでに VLAN 割り当てを持つ場合は、VMPS は次の応答のいずれかを返します。

- データベース内の VLAN がポート上の現在の VLAN と一致する場合、VMPS は*成功（success）*の応答を返し、ホストへのアクセスを許可します。
- データベースの VLAN とポート上の現在の VLAN が一致せず、かつ、ポート上にアクティブなホストがある場合、VMPS のセキュア モードに応じて、VMPS は*アクセス拒否*または*ポート シャットダウン*の応答を送信します。

VMPS から*アクセス拒否*の応答を受信したスイッチは、引き続き、そのホスト MAC アドレスとやり取りされるトラフィックをブロックします。また、スイッチは引き続きそのポート宛てのパケットをモニタし、新しいホスト アドレスを検出するたびに、VMPS にクエリーを送ります。VMPS から*ポート シャットダウン*の応答を受け取ったスイッチは、ポートをディセーブルにします。このポートは、CLI（コマンドライン インターフェイス）、または SNMP（簡易ネットワーク管理プロトコル）を使用して、手動で再びイネーブルにする必要があります。

ダイナミック アクセス ポート VLAN メンバーシップ

ダイナミック アクセス ポートは ID が 1 ～ 4094 の 1 つの VLAN にだけ属することができます。リンクがアクティブになっても、VMPS によって VLAN 割り当てが行われるまで、スイッチとこのポート間ではトラフィックの転送は行われません。VMPS はダイナミック アクセス ポートに接続された新しいホストの最初のパケットから送信元 MAC アドレスを受信し、VMPS データベースに登録されている VLAN とその MAC アドレスを照合します。

（注） UNI または ENI に限り、ダイナミック アクセス ポートにできます。

MAC アドレスと VMPS データベース内の VLAN が一致した場合には、VMPS がそのポートの VLAN 番号を送信します。クライアント スイッチがまだ設定されていない場合には、クライアント スイッチは、トランク ポートで VMPS から受信した最初の VTP パケットに指定されているドメイン名を使用します。クライアント スイッチがすでに設定されている場合には、VMPS へのクエリー パケットに自身のドメイン名を指定して、VLAN 番号を取得します。VMPS はパケットに指定されたドメイン名が自身のドメイン名と一致することを確認してから、要求を受け入れ、そのクライアント用に割り当てた VLAN 番号を使用してクライアントに応答します。一致しなかった場合、VMPS は（VMPS のセキュア モードの設定に応じて）要求を拒否するか、またはポートをシャットダウンします。

ダイナミック アクセス ポート上で複数のホスト（MAC アドレス）がアクティブになるのは、それらのホストがすべて同じ VLAN に属する場合に限られます。ただし、同一ポート上でアクティブのホストが 20 を超えると、VMPS はそのポートをシャットダウンします。

ダイナミック アクセス ポート上でリンクがダウンすると、そのポートは切り離された状態に戻り、VLAN から離脱します。このポートを介してオンラインになるホストは、VQP により再び VMPS のチェックを受けたあとに、ポートが VLAN に割り当てられます。

ダイナミック アクセス ポートは、直接ホストに接続できます。また、ネットワークへ接続することもできます。スイッチ上のポートあたり最大 20 の MAC アドレスが許可されます。ダイナミック アクセス ポートは 1 度に 1 つの VLAN にしか属せません。ただし、VLAN は認識された MAC アドレスに応じて時間の経過とともに変更することがあります。

VMPS クライアントのデフォルト設定

表 12-6 に、クライアント スイッチ上の VMPS およびダイナミック アクセス ポートのデフォルト設定を示します。

表 12-6　VMPS クライアントおよびダイナミック アクセス ポートのデフォルト設定

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認インターバル	60 分
VMPS サーバへの再試行回数	3
ダイナミック アクセス ポート	設定なし

VMPS 設定時の注意事項

ダイナミック アクセス ポート VLAN メンバーシップには、次の注意事項および制限事項があります。

- VMPS を先に設定してから、ダイナミック アクセス ポートとしてポートを設定する必要があります。
- IEEE 802.1X ポートは、ダイナミック アクセス ポートとして設定できません。ダイナミック アクセス（VQP）ポートで IEEE 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- トランク ポートをダイナミック アクセス ポートにできません。ただし、トランク ポートに対して **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力できます。この場合、スイッチは設定値を保持し、あとにポートがアクセス ポートとして設定された場合にはその設定値が適用されます。

  ダイナミック アクセスの設定を有効にするには、ポートのトランキングをオフにする必要があります。
- ダイナミック アクセス ポートは、モニタ ポートにできません。
- セキュア ポートは、ダイナミック アクセス ポートにできません。ダイナミックになる前にポートでのポート セキュリティをディセーブルにする必要があります。
- プライベート VLAN ポートは、ダイナミック アクセス ポートにできません。
- ダイナミック アクセス ポートは、EtherChannel グループのメンバーになれません。
- ポート チャネルは、ダイナミック アクセス ポートとして設定できません。

VMPS クライアントの設定

ダイナミック VLAN は VMPS（サーバ）を使用して設定します。スイッチは、VMPS クライアントにはできますが、VMPS サーバにはできません。

VMPS の IP アドレスの入力

スイッチをクライアントとして設定するには、最初にサーバの IP アドレスを入力する必要があります。VMPS の IP アドレスを入力するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vmps server** *ipaddress* **primary**	プライマリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。
ステップ 3	**vmps server** *ipaddress*	（任意）セカンダリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。 最大 3 つのセカンダリ サーバ アドレスを入力できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show vmps**	表示された *VMPS Domain Server* フィールドの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注） ダイナミック アクセス ポートを動作させるには、VMPS への IP 接続を確立する必要があります。VMPS の IP アドレスに ping し、応答の受信を確認することで、IP 接続をテストできます。

VMPS クライアントのダイナミック アクセス ポートの設定

注意 ダイナミック アクセス ポート VLAN メンバーシップは、エンド ステーション用、またはエンド ステーションに接続しているハブ用です。ダイナミック アクセス ポートを他のスイッチに接続すると、接続が切断される可能性があります。

VMPS クライアント スイッチにダイナミック アクセス ポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	エンド ステーションに接続されているスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。ポートは、UNI または ENI とします。
ステップ 3	**no shutdown**	ポートをイネーブルにします。
ステップ 4	**port-type** {**uni** | **eni**}	ポートを UNI または ENI として設定します。
ステップ 5	**switchport mode access**	ポートをアクセス モードに設定します。
ステップ 6	**switchport access vlan dynamic**	ダイナミック VLAN メンバーシップ適格としてポートを設定します。 ダイナミック アクセス ポートはエンド ステーションに接続されている必要があります。
ステップ 7	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	**show interfaces** *interface-id* **switchport**	表示された *Operational Mode* フィールドを確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスの設定をデフォルトに戻すには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。アクセス モードをスイッチのデフォルト VLAN にリセットするには、**no switchport access vlan** インターフェイス コンフィギュレーション コマンドを使用します。

VLAN メンバーシップの再確認

スイッチが VMPS から受信したダイナミック アクセス ポート VLAN メンバーシップの割り当てを確認するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**vmps reconfirm**	ダイナミック アクセス ポート VLAN メンバーシップを再確認します。
ステップ 2	**show vmps**	ダイナミック VLAN の再確認ステータスを調べます。

再確認インターバルの変更

VMPS クライアントは、VMPS から受信した VLAN メンバーシップ情報を定期的に再確認します。この再確認を行う間隔を分単位で設定できます。

再確認インターバルを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vmps reconfirm** *minutes*	ダイナミック VLAN メンバーシップを再確認する間隔を分単位で指定します。指定できる範囲は 1 ～ 120 です。デフォルトは 60 分です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vmps**	表示されている *Reconfirm Interval* フィールドのダイナミック VLAN の再確認ステータスを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

再試行回数の変更

スイッチが次のサーバにクエリー送信するまでに、VMPS との接続を試みる試行回数を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vmps retry** *count*	再試行回数を変更します。再試行回数は 1 ～ 10 回の範囲で指定できます。デフォルトは 3 回です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vmps**	表示された *Server Retry Count* フィールドを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

VMPS のモニタ

VMPS 情報を表示するには、**show vmps** 特権 EXEC コマンドを使用します。VMPS に関する次の情報が表示されます。

- VMPS VQP バージョン : VMPS との通信に使用される VQP のバージョン。スイッチは VQP バージョン 1 を使用する VMPS にクエリー送信をします。
- 再確認インターバル : VLAN と MAC アドレスとの割り当てを再確認するまでにスイッチが待機する時間（分単位）
- サーバ再試行回数 : VQP から VMPS にクエリーを再送信する回数。この回数だけ試行しても応答がない場合、スイッチはセカンダリ VMPS に対してクエリー送信を開始します。
- VMPS ドメイン サーバ : 設定されている VMPS の IP アドレス。スイッチは、*current* の指定があるサーバにクエリーを送信しています。*primary* と表示されたサーバがプライマリ サーバです。
- VMPS アクション : 最新の再確認試行の結果。再確認は、再確認インターバルとして設定された時間が経過すると自動的に行われます。また、**vmps reconfirm** 特権 EXEC コマンドを入力することによって、強制的に再確認できます。

次に、**show vmps** 特権 EXEC コマンドの出力例を示します。

```
Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         other
```

ダイナミック アクセス ポート VLAN メンバーシップのトラブルシューティング

VMPS は次の条件が発生したときに、ダイナミック アクセス ポートをシャットダウンします。

- VMPS がセキュア モードで、かつ、ホストにポートへの接続を許可しない場合。VMPS は、ホストがネットワークに接続しないように、ポートをシャットダウンします。
- 1 つのダイナミック アクセス ポート上に 20 を超えるアクティブ ホストが存在する場合

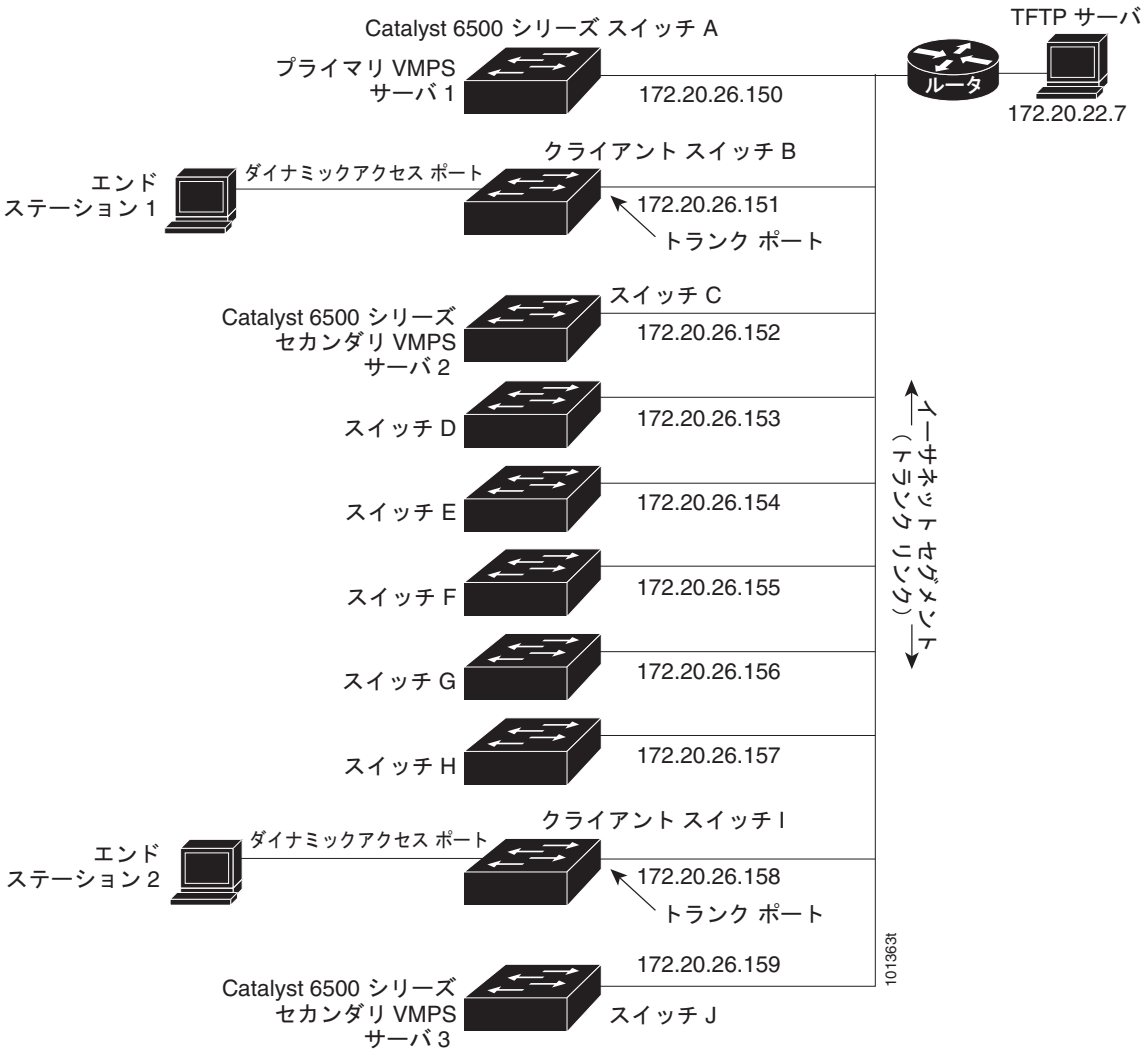
ディセーブルのダイナミック アクセス ポートを再度イネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドに続けて、**no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

VMPS の構成例

図 12-5 に、VMPS サーバ スイッチと、ダイナミック アクセス ポートの設定された VMPS クライアント スイッチで構成されるネットワークを示します。この例の前提条件は次のとおりです。

- VMPS サーバと VMPS クライアントは、それぞれ別個のスイッチです。
- Catalyst 6500 シリーズ スイッチ A がプライマリの VMPS サーバです。
- Catalyst 6500 シリーズ スイッチ C およびスイッチ J がセカンダリの VMPS サーバです。
- エンド ステーションは、クライアント、スイッチ B、およびスイッチ I に接続されます。
- データベース コンフィギュレーション ファイルは、IP アドレス 172.20.22.7 の TFTP サーバに保管されます。

図 12-5　ダイナミック ポート VLAN メンバーシップの構成



CHAPTER 13

プライベート VLAN の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにプライベート VLAN を設定する方法について説明します。

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

- 「プライベート VLAN の概要」（P.13-1）
- 「プライベート VLAN の設定」（P.13-6）
- 「プライベート VLAN のモニタリング」（P.13-16）

プライベート VLAN の概要

プライベート VLAN 機能は、サービス プロバイダーが VLAN を使用している場合に直面する 2 つの問題に対処します。

- スケーラビリティ：スイッチは最大 1005 のアクティブ VLAN をサポートします。サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

プライベート VLAN を使用することでスケーラビリティの問題に対処することができ、サービス プロバイダーにとっては IP アドレス管理上の利点が得られ、カスタマーに対してはレイヤ 2 セキュリティを提供できます。

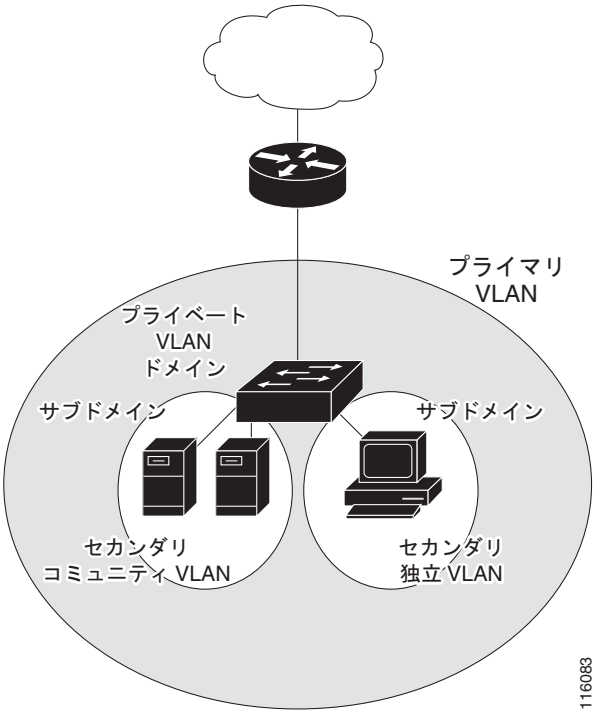
ここでは、プライベート VLAN の機能について説明します。

- 「プライベート VLAN およびプライベート VLAN ポートのタイプ」（P.13-2）
- 「プライベート VLAN での IP アドレッシング方式」（P.13-4）
- 「複数のスイッチにまたがるプライベート VLAN」（P.13-4）
- 「プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック」（P.13-5）
- 「プライベート VLAN と SVI」（P.13-6）

プライベート VLAN およびプライベート VLAN ポートのタイプ

プライベート VLAN では、通常の VLAN ドメインはサブドメインに分割されます。サブドメインは、*プライマリ* VLAN および*セカンダリ* VLAN という VLAN のペアで表されます。プライベート VLAN では複数の VLAN ペアを設定でき、各サブドメインにつき 1 ペアとなります。プライベート VLAN 内のすべての VLAN ペアは同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、あるサブドメインを別のサブドメインと区別します。図 13-1 を参照してください。

図 13-1　　プライベート VLAN ドメイン



セカンダリ VLAN には 2 種類あります。

- 隔離 VLAN：隔離 VLAN 内のポートは、レイヤ 2 レベルでは互いに通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルの他のコミュニティ内のポートとは通信できません。コミュニティ VLAN には、User Network Interface（UNI; ユーザネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）を最大 8 つ組み合せて指定できます。

プライベート VLAN では、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートには、次のタイプがあります。

- プロミスキャス：プロミスキャス ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト ポートなどの、すべてのインターフェイスと通信できます。

（注） プロミスキャス ポートは、Network Node Interface（NNI; ネットワーク ノード インターフェイス）とします。UNI または ENI は、プロミスキャス ポートとしては設定できません。

- 独立：独立ポートは、独立セカンダリ VLAN に属するホスト ポートです。これは、プロミスキャス ポートを除く、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN では、プロミスキャス ポートからのトラフィックを除く、独立ポートへのすべてのトラフィックをブロックします。独立ポートで受信されるトラフィックは、プロミスキャス ポートへだけ転送されます。
- コミュニティ：コミュニティ ポートは、コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN にある他のポートおよびプロミスキャス ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。最大 8 つの UNI と ENI を同一コミュニティ VLAN 内のコミュニティ ポートとすることができます。

（注）　トランク ポートは、通常の VLAN からのトラフィックを転送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも転送します。

プライマリおよびセカンダリ VLAN には次のような特性があります。

- プライマリ VLAN：プライベート VLAN にはプライマリ VLAN が 1 つだけあります。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、プロミスキャス ポートからの単一方向トラフィックのダウンストリームを、（独立およびコミュニティ）ホスト ポートおよび他のプロミスキャス ポートに転送します。
- 独立 VLAN：プライベート VLAN の独立 VLAN は 1 つだけです。独立 VLAN は、ホストからの単一方向トラフィック アップストリームをプロミスキャス ポートおよびゲートウェイへ転送するセカンダリ VLAN です。
- コミュニティ VLAN：コミュニティ VLAN は、コミュニティ ポートからのアップストリーム トラフィックをプロミスキャス ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートへ転送するセカンダリ VLAN です。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。コミュニティ VLAN は、UNI および ENI を組み合せて最大 8 つ指定できます。

（注）　またスイッチは、UNI-ENI 独立 VLAN および UNI-ENI コミュニティ VLAN サポートします。作成された VLAN は、デフォルトで UNI-ENI 独立 VLAN となります。UNI-ENI 独立 VLAN に属するスイッチの UNI および ENI 間では、トラフィックはスイッチングされません。UNI-ENI VLAN の詳細については、第 12 章「VLAN の設定」を参照してください。

プロミスキャス ポートが扱えるのは、1 つのプライマリ VLAN、1 つの独立 VLAN、および複数のコミュニティ VLAN だけです。レイヤ 3 ゲートウェイは通常プロミスキャス ポートを介してスイッチに接続されています。プロミスキャス ポートを使用すると、幅広いデバイスをプライベート VLAN へのアクセス ポートとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションからモニタしたりバックアップしたりするのに、プロミスキャス ポートを使用できます。

スイッチング環境では、個々のエンド ステーションまたはエンド ステーションの共通グループに、個別のプライベート VLAN と関連する IP サブネットを割り当てることができます。エンド ステーションがデフォルト ゲートウェイと対話する必要があるのは、プライベート VLAN 外部と通信する場合だけです。

プライベート VLAN を使用してエンド ステーションへのアクセスを次のように制御できます。

- エンド ステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。たとえば、エンド ステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択したエンド ステーション（たとえばバックアップ サーバなど）に接続された NNI をプロミスキャス ポートとして設定します。これにより、すべてのエンド ステーションがデフォルト ゲートウェイに接続できます。

プライマリ、独立、およびコミュニティ VLAN をプライベート VLAN をサポートする他のデバイスにトランキングすることで、プライベート VLAN を複数のデバイスに拡張できます。プライベート VLAN コンフィギュレーションのセキュリティを保って VLAN の他のユーザがプライベート VLAN に設定されないようにするには、プライベート VLAN ポートのないデバイスを含む、すべての中間デバイス内にプライベート VLAN を設定します。

プライベート VLAN での IP アドレッシング方式

各カスタマーに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

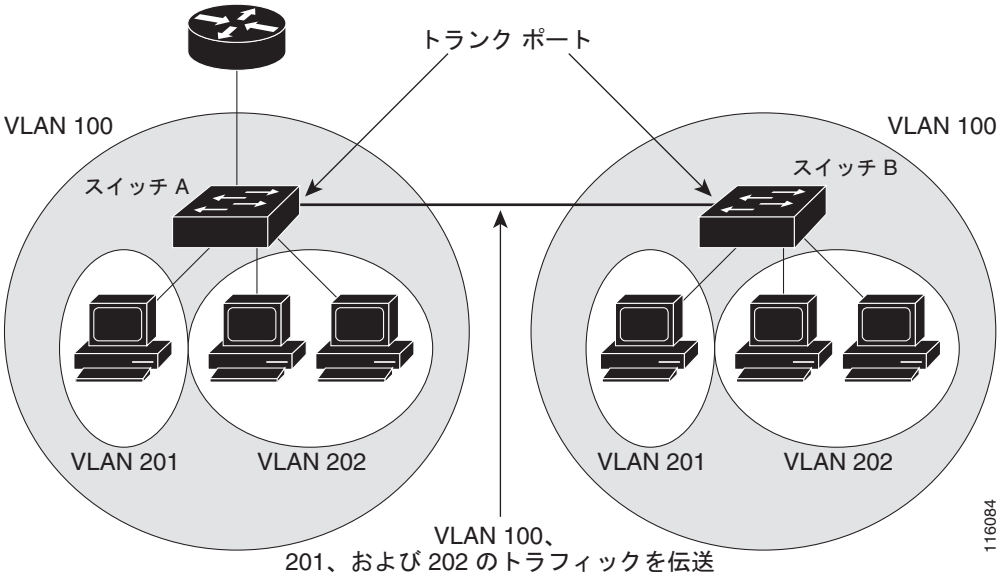
- カスタマーの VLAN にアドレス ブロックを割り当てると、未使用の IP アドレスが出てきます。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

これらの問題は、プライベート VLAN を使用することで軽減できます。この場合、プライベート VLAN 内のすべてのメンバーがプライマリ VLAN に割り当てられた共通アドレス空間を共有します。ホストはセカンダリ VLAN に接続され、Dynamic Host Configuration Protocol（DHCP）サーバがプライマリ VLAN に割り当てられたアドレス ブロックから IP アドレスを割り当てます。後続の IP アドレスは、同じプライマリ VLAN にある別のセカンダリ VLAN にあるカスタマー デバイスに割り当てることができます。新しいデバイスが追加されると、DHCP サーバはサブネット アドレスの大きなプールから次に使用できるアドレスをデバイスに割り当てます。

複数のスイッチにまたがるプライベート VLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチ全体に設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を隣接スイッチに伝送します。トランク ポートはプライベート VLAN を他の VLAN として扱います。複数のスイッチにまたがるプライベート VLAN の機能の場合、スイッチ A にある独立ポートからのトラフィックはスイッチ B にある独立ポートに到達しません。図 13-2 を参照してください。

図 13-2　複数のスイッチにまたがるプライベート VLAN



VLAN 100 = プライマリ VLAN
VLAN 201 = セカンダリ独立 VLAN
VLAN 202 = セカンダリ コミュニティ VLAN

レイヤ 2 ネットワークのすべてのスイッチ上のプライベート VLAN は、手動で設定する必要があります。ネットワーク内の一部のスイッチにプライマリおよびセカンダリ VLAN の関連を設定しない場合、これらのスイッチのレイヤ 2 データベースは統合されません。これにより、これらのスイッチにプライベート VLAN トラフィックの不要なフラッディングが発生する可能性があります。

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。プライベート VLAN では、プロミスキャス ポートはプライマリ VLAN のメンバーで、ホスト ポートはセカンダリ VLAN に属しています。セカンダリ VLAN はプライマリ VLAN に対応付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで互いに通信できます。

通常の VLAN では、ブロードキャストはその VLAN 内のすべてのポートに転送されます。プライベート VLAN ブロードキャスト転送は、次のようにブロードキャストを送信するポートに左右されます。

- 独立ポートはブロードキャストをプロミスキャス ポートまたはトランク ポートにだけ送信します。
- コミュニティ ポートは、すべてのプロミスキャス ポート、トランク ポート、および同じコミュニティ VLAN 内のポートにブロードキャストを送信します。
- プロミスキャス ポート（NNI だけ）は、プライベート VLAN のすべてのポート（他のプロミスキャス ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックは、プライベート VLAN 境界を越えて単一のコミュニティ VLAN 内にルーティングまたはブリッジされます。マルチキャスト トラフィックは、同じ独立 VLAN 内のポート間で転送されず、また別のセカンダリ VLAN 内のポート間でも転送されません。

プライベート VLAN と SVI

レイヤ 3 スイッチ（メトロ IP アクセス イメージが稼動するスイッチ）では、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）が VLAN のレイヤ 3 インターフェイスを表します。レイヤ 3 デバイスは、セカンダリ VLAN ではなくプライマリ VLAN を介してだけプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイスはプライマリ VLAN にだけ設定してください。レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

- アクティブ SVI を設定した VLAN をセカンダリ VLAN として設定しようとすると、SVI をディセーブルにするまで設定が許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 にマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされます。

プライマリ VLAN がセカンダリ VLAN に対応付けられていてマッピングされている場合、プライマリ VLAN 上の設定はセカンダリ VLAN SVI に伝播されます。たとえば、IP サブネットをプライマリ VLAN SVI に割り当てる場合、このサブネットはプライベート VLAN 全体の IP サブネット アドレスです。

プライベート VLAN の設定

- 「プライベート VLAN の設定手順」（P.13-6）
- 「デフォルトのプライベート VLAN 設定」（P.13-7）
- 「プライベート VLAN 設定時の注意事項」（P.13-7）
- 「プライベート VLAN への VLAN の設定と関連付け」（P.13-10）
- 「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」（P.13-12）
- 「プライベート VLAN プロミスキャス ポートとしてのレイヤ 2 インターフェイスの設定」（P.13-13）
- 「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」（P.13-15）

プライベート VLAN の設定手順

プライベート VLAN を設定するには、次の手順を実行します。

ステップ 1　プライマリおよびセカンダリ VLAN を作成してこれらを対応付けします。「プライベート VLAN への VLAN の設定と関連付け」（P.13-10）を参照してください。

（注）　VLAN がまだ作成されていない場合、プライベート VLAN 設定プロセスでこれを作成します。

ステップ 2　インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」（P.13-12）を参照してください。

ステップ 3　NNI をプロミスキャス ポートを設定し、プロミスキャス ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。「プライベート VLAN プロミスキャス ポートとしてのレイヤ 2 インターフェイスの設定」（P.13-13）を参照してください。

ステップ 4　VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI にマッピングします。「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」（P.13-15）を参照してください。

ステップ 5　プライマリ VLAN 設定を確認します。

デフォルトのプライベート VLAN 設定

プライベート VLAN は設定されていません。新たに作成された VLAN は、UNI-ENI 独立 VLAN になります。

プライベート VLAN 設定時の注意事項

プライベート VLAN 設定時の注意事項は、次のカテゴリに分けられます。

- 「セカンダリおよびプライマリ VLAN の設定」（P.13-7）
- 「プライベート VLAN ポート設定」（P.13-9）
- 「他の機能との間の制限」（P.13-10）

セカンダリおよびプライマリ VLAN の設定

プライベート VLAN の設定を行うときは、次の注意事項に従ってください。

- プライベート VLAN を設定するには、VLAN 設定モードを使用します。VLAN 設定の詳細については、「VLAN の作成および変更」（P.12-7）を参照してください。
- プライベート VLAN ポートが必要な各デバイスにプライベート VLAN を設定する必要があります。
- プライベート VLAN は、UNI-ENI VLAN にできません。
  - UNI-ENI 独立 VLAN（デフォルト）をプライベート VLAN に変更するには、**private-vlan** VLAN コンフィギュレーション コマンドを入力します。これにより、デフォルトの独立 VLAN 設定は上書きされます。
  - UNI-ENI コミュニティ VLAN をプライベート VLAN に変更するには、まず **no uni-vlan** VLAN コンフィギュレーション コマンドを入力して、デフォルトの UNI 独立 VLAN 設定に戻します。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリまたはセカンダリ VLAN に設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に属することができます。
- プライマリ VLAN には、1 つの隔離 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立またはコミュニティ VLAN には、これに対応付けられたプライマリ VLAN を 1 つだけ設定できます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行可能な Spanning-Tree Protocol（STP; スパニングツリー プロトコル）インスタンスは 1 つだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。

- プライベート VLAN で DHCP スヌーピングをイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにする場合、セカンダリ VLAN に伝播されます。セカンダリ VLAN に DHCP を設定する場合、その設定はプライマリ VLAN がすでに設定されていないと有効になりません。
- プライベート VLAN ポートで IP ソース ガードをイネーブルにするには、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN に別々の QoS（Quality of Service）設定を適用できます。
- スティッキ ARP について、スイッチでメトロ IP アクセス イメージが稼動している場合
  - スティッキ ARP エントリは、SVI およびレイヤ 3 インターフェイスで学習されるエントリです。これらのエントリは、期限切れになりません。
  - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属している SVI でだけサポートされます。
  - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、次のものでだけサポートされます。

    レイヤ 3 インターフェイス

    通常の VLAN に属している SVI

    プライベート VLAN に属している SVI

  ip sticky-arp *global* コンフィギュレーションおよび **ip sticky-arp** *interface* コンフィギュレーション コマンドの使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。
- プライマリおよびセカンダリ VLAN で VLAN マップを設定できます（「VLAN マップの設定」（P.32-30）を参照）。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内でレイヤ 2 を介して転送される場合、同じ VLAN マップが受信側と送信側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが受信側に適用されます。

  - ホスト ポートからプロミスキャス ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN に設定されている VLAN マップが適用されます。
  - プロミスキャス ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN に設定されている VLAN マップが適用されます。

  プライベート VLAN の特定の IP トラフィックをフィルタリングするには、VLAN マップをプライマリおよびセカンダリ VLAN の両方に適用します。
- スイッチでメトロ IP アクセス イメージが稼動している場合、ルータ ACL はプライマリ VLAN SVI 上でだけ適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN は、次の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能をサポートします。
  - プライベート VLAN を SPAN 送信元ポートとして設定できます。
  - VLAN-based SPAN（VSPAN）はプライマリ VLAN、独立 VLAN、およびコミュニティ VLAN で使用できます。また、送信または受信トラフィックを別々にモニタするために、1 つの VLAN でだけ SPAN を使用できます。

プライベート VLAN ポート設定

プライベート VLAN ポートの設定を行うときは、次の注意事項に従ってください。

- プロミスキャス ポートは NNI である必要があり、UNI および ENI はプロミスキャス ポートとして設定できません。
- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN 設定コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定した VLAN に割り当てられたレイヤ 2 アクセス ポートは、VLAN がプライベート VLAN 設定の一部の間は非アクティブになります。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- Port Aggregation Protocol（PAgP; ポート集約プロトコル）または Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）EtherChannel に属する NNI ポートは、プライベート VLAN ポートとして設定できません。ポートがプライベート VLAN 設定に含まれていると、ポートの EtherChannel 設定が非アクティブになります。
- 誤った設定による STP ループを発生させず、STP コンバージェンスを高速にするために、NNI 独立およびコミュニティ ホスト ポートで PortFast および Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガードをイネーブルにします（第 17 章「オプションのスパニング ツリー機能の設定方法」を参照）。イネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN ポートに BPDU ガード機能を適用します。PortFast および BPDU ガードをプロミスキャス ポートでイネーブルにしないでください。
- プライベート VLAN 設定で VLAN を削除した場合、VLAN に対応付けられたプライベート VLAN ポートが非アクティブになります。
- デバイスがトランクに接続されていてプライマリおよびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートを別のネットワーク デバイス上に設定できます。
- コミュニティ プライベート VLAN には、最大 8 つの UNI および ENI を含めることができます。9 つ以上の UNI および ENI を追加しようとした場合、設定は許可されません。9 つ以上の UNI および ENI の組み合せを含む VLAN をコミュニティ プライベート VLAN として設定しようとしても、設定は許可されません。

他の機能との間の制限

プライベート VLAN を設定する際、他の機能との間で次のような制限があることに留意してください。

（注）　エラー メッセージなしで設定が受け入れられていてもコマンドが機能しない場合があります。

- IGMP スヌーピングがスイッチでイネーブルの場合（デフォルト）、スイッチでサポートされるプライベート VLAN ドメインの数は 20 までです。
- プライベート VLAN は、UNI-ENI 独立 VLAN または UNI-ENI コミュニティ VLAN にはできません。UNI-ENI VLAN の詳細については、第 12 章「VLAN の設定」を参照してください。
- Remote SPAN（RSPAN; リモート SPAN）をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。SPAN の詳細については、第 27 章「SPAN および RSPAN の設定」を参照してください。
- 次のような機能が設定されているインターフェイスにプライベート VLAN ポートを設定しないでください。
  - ダイナミック アクセス ポート VLAN メンバーシップ
  - PAgP（NNI または ENI だけ）
  - LACP（NNI または ENI だけ）
  - マルチキャスト VLAN レジストレーション（MVR）
- プライベート VLAN ポートでは 802.1x ポートベース認証を設定できますが、このポートで、ポート セキュリティと同時に IEEE 802.1x を設定しないでください。
- プライベート VLAN ホストまたはプロミスキャス ポートは SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN 内のプロミスキャス ポートにスタティック MAC アドレスを設定した場合、同じスタティック アドレスをすべての関連セカンダリ VLAN に追加する必要があります。セカンダリ VLAN 内ホスト ポートにスタティック MAC アドレスを設定した場合、同じスタティック アドレスをすべての関連プライマリ VLAN に追加する必要があります。スタティック MAC アドレスをプライベート VLAN ポートから削除する際に、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要があります。

  （注）　プライベート LAN 上にある 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連 VLAN に複製されます。たとえば、セカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN に複製されます。元のダイナミック MAC アドレスが削除されたり期限が切れた場合、複製アドレスは MAC アドレス テーブルから削除されます。

- レイヤ 3 VLAN インターフェイスはプライマリ VLAN にだけ設定してください。

プライベート VLAN への VLAN の設定と関連付け

プライベート VLAN を設定するには、特権 EXEC モードで次の手順を行います。

（注）　**private-vlan** コマンドは VLAN コンフィギュレーション モードを終了するまで機能しません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定するか作成します。指定できる VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。 **（注）** VLAN が UNI-ENI コミュニティ VLAN として設定されている場合、**no uni-vlan** VLAN コンフィギュレーション コマンドを入力してから、プライベート VLAN を設定する必要があります。
ステップ 3	**private-vlan primary**	VLAN をプライマリ VLAN として指定します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**vlan** *vlan-id*	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定するか作成します。指定できる VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 6	**private-vlan isolated**	VLAN を独立 VLAN として指定します。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**vlan** *vlan-id*	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定するか作成します。指定できる VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。 **（注）** VLAN が UNI-ENI コミュニティ VLAN として設定されている場合、**no uni-vlan** VLAN コンフィギュレーション コマンドを入力してから、プライベート VLAN を設定する必要があります。
ステップ 9	**private-vlan community**	VLAN をコミュニティ VLAN として指定します。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**vlan** *vlan-id*	ステップ 3 で指定したプライマリ VLAN 用の VLAN コンフィギュレーション モードを開始します。
ステップ 12	**private-vlan association** [**add** | **remove**] *secondary_vlan_list*	セカンダリ VLAN をプライマリ VLAN に関連付けます。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show vlan private-vlan** [**type**] または **show interfaces status**	設定を確認します。
ステップ 15	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

セカンダリ VLAN をプライマリ VLAN に関連付ける際に、構文に関して次のことに留意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。
- *secondary_vlan_list* を入力するか、またはキーワード **add** を指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN を関連付けます。

- **remove** キーワードとともに *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN の関連付けを解除します。
- **private-vlan association** VLAN コンフィギュレーション コマンドは、VLAN コンフィギュレーション モードを終了しないかぎり、有効になりません。

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および VLAN 503 をコミュニティ VLAN として設定し、これらをプライベート VLAN 内で関連付けして、設定を確認する例を示します。VLAN 502 および VLAN 503 は、事前に UNI-ENI コミュニティ VLAN として設定されていると想定します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# no-uni vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no-uni vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
20      503       community
20      504       non-operational
```

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定し、これをプライマリおよびセカンダリ VLAN と関連付けるには、特権 EXEC モードで次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 2 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**switchport mode private-vlan host**	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 5	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id*	レイヤ 2 ポートをプライベート VLAN に関連付けます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport**	設定を確認します。
ステップ 8	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスをプライベート VLAN ホスト ポートとして設定し、これにプライベート VLAN ペアを関連付けて、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/22
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
Switch# show interfaces fastethernet0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501
<output truncated>
```

プライベート VLAN プロミスキャス ポートとしてのレイヤ 2 インターフェイスの設定

プロミスキャス ポートとして設定できるのは、NNI に限られます。レイヤ 2 インターフェイスをプライベート VLAN プロミスキャス ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、特権 EXEC モードで次の手順を実行します。

（注）　独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 2 インターフェイスを指定します。インターフェイスは、NNI である必要があります。 （注）　インターフェイスが UNI または ENI の場合は、プロミスキャス ポートとして設定する前に、**port-type nni** インターフェイス コンフィギュレーション コマンドを入力する必要があります。
ステップ 3	**switchport mode private-vlan promiscuous**	レイヤ 2 NNI ポートをプライベート VLAN プロミスキャス ポートとして設定します。
ステップ 4	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list*	プライベート VLAN プロミスキャス ポートをプライマリ VLAN と選択したセカンダリ VLAN にマッピングします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] **switchport**	設定を確認します。
ステップ 7	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 インターフェイスをプライベート VLAN プロミスキャス ポートとして設定した場合、構文に関して次のことに留意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- *secondary_vlan_list* を入力するか、またはキーワード **add** を指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN をプライベート VLAN プロミスキャス ポートにマッピングします。
- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライベート VLAN プロミスキャス ポートのマッピングを解除します。

次に、NNI をプライベート VLAN プロミスキャス ポートとして設定してそれをプライベート VLAN にマッピングする例を示します。インターフェイスは、プライマリ VLAN 20 のメンバーで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用してプライマリおよびセカンダリ VLAN とスイッチ上のプライベート VLAN ポートを表示します。

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング

スイッチでメトロ IP アクセス イメージが稼動していて、プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定してセカンダリ VLAN を SVI にマッピングできます。

（注）　独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングしてプライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *primary_vlan_id*	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して VLAN を SVI として設定します。指定できる VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 3	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list*	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 着信トラフィックのレイヤ 3 スイッチングを可能にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interface private-vlan mapping**	設定を確認します。
ステップ 6	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

（注）　**private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 を介してスイッチングされているプライベート VLAN トラフィックにだけ影響します。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際、構文について次の点に留意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- *secondary_vlan_list* を入力するか、またはキーワード **add** を指定した *secondary_vlan_list* を使用してセカンダリ VLAN をプライマリ VLAN にマッピングします。
- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。VLAN 10 では、プライベート VLAN 501 から 502 へのセカンダリ VLAN 着信トラフィックのルーティングが許可されます。

```
Switch# configure terminal
Switch(config)# interface vlan 10
```

```
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

プライベート VLAN のモニタリング

表 13-1 に、プライベート VLAN モニタ用の特権 EXEC コマンドを示します。

表 13-1　プライベート VLAN モニタリング コマンド

コマンド	目的
show interfaces status	所属する VLAN を含むインターフェイスのステータスを表示します。
show vlan private-vlan [type]	スイッチのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN インターフェイスのプライベート VLAN マッピングに関する情報を表示します。

次に、**show vlan private-vlan** コマンドからの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa0/1, Gi0/1, Gi0/2
10      502       community         Fa0/11, Fa0/12, Gi0/1
10      503       non-operational
```

CHAPTER 14

IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）では、多くの場合にイーサネットベースの共有インフラストラクチャである企業規模の接続に、プライベート ネットワークと同じセキュリティ、プライオリティ、信頼性、管理の容易さが提供されます。トンネリングは、サービス プロバイダーのネットワークを越えて複数のカスタマーのトラフィックを運び、その他のカスタマーのトラフィックに影響を与えずに、それぞれのカスタマーの VLAN（仮想 LAN）およびレイヤ 2 プロトコルの設定を維持する必要があるサービス プロバイダー用に設計された機能です。Cisco ME 3400E イーサネット アクセス スイッチは、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングをサポートします。また、トランクポート上での VLAN マッピング（または VLAN ID トランスレーション）もサポートしています。

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

- 「802.1Q トンネリングの概要」（P.14-1）
- 「802.1Q トンネリングの設定」（P.14-4）
- 「VLAN マッピングの概要」（P.14-8）
- 「VLAN マッピングの設定」（P.14-9）
- 「レイヤ 2 プロトコル トンネリングの概要」（P.14-13）
- 「レイヤ 2 プロトコル トンネリングの設定」（P.14-16）
- 「トンネリングおよびマッピング ステータスのモニタおよびメンテナンス」（P.14-24）

802.1Q トンネリングの概要

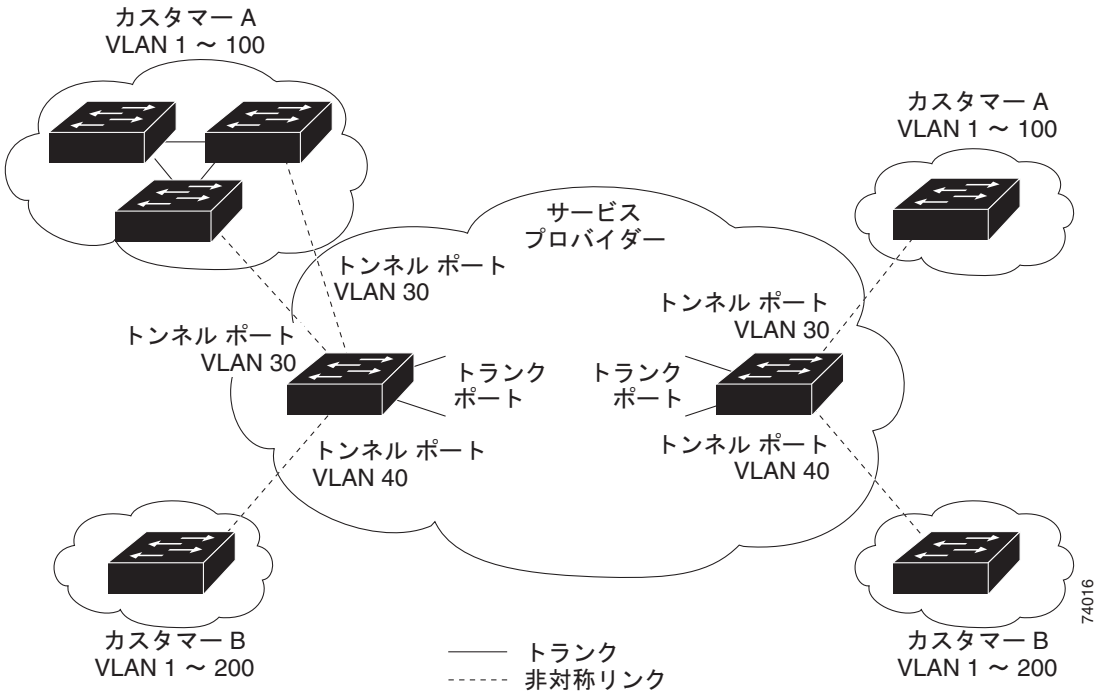
サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同じサービス プロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混在することがあります。それぞれのカスタマーに VLAN ID の固有の範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN 制限（4096）を簡単に越えてしまうことがあります。

サービス プロバイダーは、802.1Q トンネリング（QinQ）機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。カスタマーの VLAN ID（C-VLAN）は、同一 VLAN 内にあるように見えても保護され、さまざまなカスタマーのトラフィックは、サービス プロバイダー ネットワーク内で区別されます。802.1Q トンネリングを使用すると、VLAN 内の VLAN 階層を使用してタグ付きパケットにタグを再び付けることで、VLAN 容量が拡大します。802.1Q トンネリングをサポートするように設定したポートは、*トンネル ポート*と呼ばれます。トンネリングを設定する場合は、トンネリング専用の VLAN ID にトンネル ポートを割り当てます。それぞれのカスタマーには個別のサービス プロバイダー VLAN ID（S-VLAN）が必要ですが、その VLAN ID ではすべてのカスタマーの VLAN がサポートされます。トンネル ポートでの 802.1Q トンネリングの設定は、従来の *QinQ* と呼ばれます。

適切な VLAN ID で通常どおりにタグ付けされたカスタマーのトラフィックは、カスタマー デバイスの 802.1Q トランク ポートからサービス プロバイダー側のエッジ スイッチのトンネル ポートに発信されます。カスタマー デバイスおよびエッジ スイッチの間のリンクは、片方が 802.1Q トランク ポートとして設定され、もう一方がトンネル ポートとして設定されているので非対称です。それぞれのカスタマーに固有のアクセス VLAN ID には、トンネル ポート インターフェイスを割り当てます。図 14-1 を参照してください。

（注） デフォルトでは、スイッチ上に設定された VLAN は、User Network Interface-Enhanced Network Interface（UNI-ENI）独立 VLAN です。UNI-ENI 独立 VLAN では、スイッチ上で 802.1Q トンネリングされたアクセス ポートが相互に独立しています。**uni-vlan community** VLAN コンフィギュレーション コマンドを使用して、VLAN を UNI-ENI コミュニティ VLAN に変更すると、これらのポート間でローカル スイッチングが行われます。UNI-ENI VLAN の詳細については、第 12 章「VLAN の設定」を参照してください。

図 14-1　サービス プロバイダー ネットワークの 802.1Q トンネル ポート

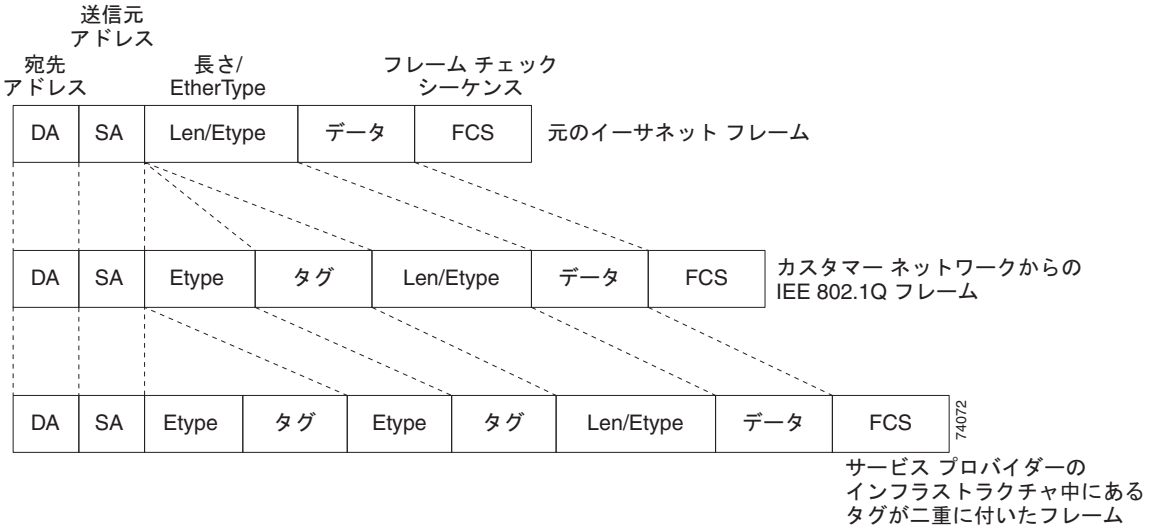


カスタマーのトランク ポートからサービス プロバイダー側のエッジ スイッチのトンネル ポートに発信されるパケットには、通常、適切な VLAN ID とともに 802.1Q タグが付いています。タグ付きパケットはスイッチ内にそのまま残り、トランク ポートからサービス プロバイダー ネットワークに発信されると、カスタマーに固有の VLAN ID を含む 802.1Q タグの別のレイヤ（*メトロタグ*）でカプセル化されます。カスタマーの元の 802.1Q タグは、カプセル化されたパケット内で保護されます。このため、サービス プロバイダー ネットワークに入るパケットには、カスタマーのアクセス VLAN ID を含む外部（メトロ）タグ、および着信トラフィックのものである内部 VLAN ID という、2 重のタグが付いています。

2 重タグ パケットがサービス プロバイダー コア スイッチの別のトランク ポートに入ると、スイッチがパケットを処理する間に外部タグが外されます。パケットが、そのコア スイッチの別のトランク ポートを出るとき、同じメトロ タグがパケットに再び追加されます。図 14-2 は、2 重タグ パケットのタグ構造を示しています。

（注） 着信したカプセル化パケットによってトランク ポートが errdisable に変更されるため、レイヤ 2 プロトコル設定をトランク ポートから削除します。発信カプセル化 VTP（CDP および STP）パケットは同じトランクでドロップされます。

図 14-2　元の（通常）イーサネット パケット、802.1Q イーサネット パケット、2 重タグ イーサネット パケットの形式



パケットがサービス プロバイダー出力スイッチのトランク ポートに入ると、スイッチがパケットを内部処理する間に外部タグは再び外されます。しかし、パケットがエッジ スイッチのトンネル ポートからカスタマー ネットワークに送信されるとき、メトロ タグは追加されません。パケットは通常の 802.1Q タグ フレームとして送信され、カスタマー ネットワーク内で元の VLAN 番号は保護されます。

図 14-1 では、カスタマー A に VLAN 30 が、カスタマー B に VLAN 40 が割り当てられています。エッジ スイッチのトンネル ポートに入る、802.1Q タグが付いたパケットには、サービス プロバイダー ネットワークに入るとき、VLAN ID 30 または 40 のどちらかを含む外部タグ、および VLAN 100 などの元の VLAN 番号を含む内部タグが付いて 2 重タグになります。カスタマー A とカスタマー B の両方が、それぞれのネットワーク内で VLAN 100 を含んでいても、外部タグが異なるので、トラフィックはサービス プロバイダー ネットワーク内で区別されます。それぞれのカスタマーは、その他のカスタマーが使用する VLAN 番号スペース、およびサービス プロバイダー ネットワークが使用する VLAN 番号スペースから独立した、独自の VLAN 番号スペースを制御します。

発信トンネル ポートでは、カスタマーのネットワーク上の元の VLAN 番号が回復されます。トンネリングおよびタグ付けを複数のレベルにすることもできますが、このリリースのスイッチでは 1 レベルだけがサポートされます。

カスタマー ネットワークから発信されるトラフィックにタグ（ネイティブ VLAN フレーム）が付いていない場合、そのパケットのブリッジまたはルートは通常パケットとして行われます。エッジ スイッチのトンネル ポートを通ってサービス プロバイダー ネットワークに入るすべてのパケットは、タグが付いていないか、802.1Q ヘッダーですでにタグが付いているかに関係なく、タグなしパケットとして扱われます。パケットは、802.1Q トランク ポートでサービス プロバイダー ネットワークを通じて送信される場合、メトロ タグ VLAN ID（トンネル ポートのアクセス VLAN に設定）でカプセル化されます。メトロ タグのプライオリティ フィールドは、トンネル ポートで設定されているインターフェイス Class of Service（CoS; サービス クラス）プライオリティに設定されます （設定されていない場合、デフォルトはゼロです）。

802.1Q トンネリングの設定

- 「802.1Q トンネリングのデフォルト設定」（P.14-4）
- 「802.1Q トンネリング設定時の注意事項」（P.14-4）
- 「802.1Q トンネリングおよびその他の機能」（P.14-6）
- 「802.1Q トンネリング ポートの設定」（P.14-7）

802.1Q トンネリングのデフォルト設定

デフォルトでは、デフォルト switchport モードが access であるため、802.1Q トンネルはディセーブルです。すべての 802.1Q トランク ポートにおける 802.1Q ネイティブ VLAN パケットのタグ付けもディセーブルです。デフォルトでは、スイッチ上の VLAN は UNI-ENI 独立 VLAN です。

802.1Q トンネリング設定時の注意事項

802.1Q トンネリングを設定する場合は、カスタマー デバイスおよびエッジ スイッチの間で非対称リンクを常に使用する必要があります。カスタマー デバイスのポートを 802.1Q トランク ポートに、エッジ スイッチのポートをトンネル ポートとして設定してください。

トンネリングに使用する VLAN だけにトンネル ポートを割り当ててください。

ネイティブ VLAN および Maximum Transmission Unit（MTU; 最大伝送ユニット）の設定要件については、次のセクションで説明します。

ネイティブ VLAN

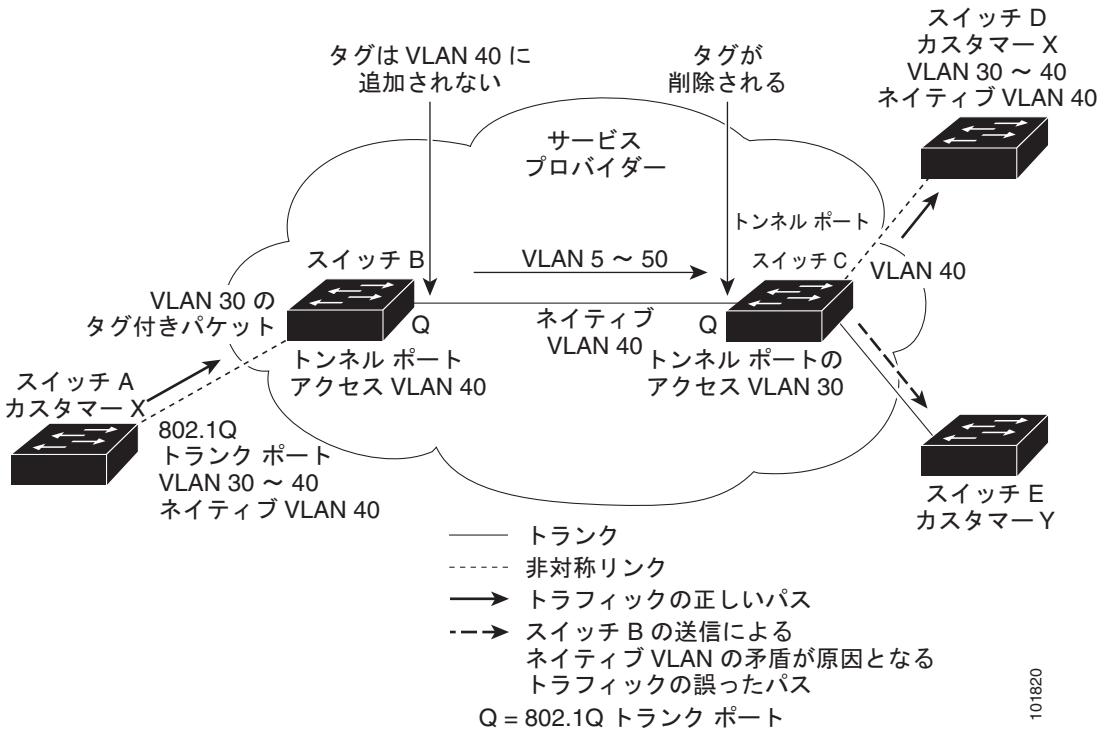
エッジ スイッチで 802.1Q トンネリングを設定する場合は、サービス プロバイダー ネットワークにパケットを送信するために、802.1Q トランク ポートを使用する必要があります。しかしサービス プロバイダー ネットワークのコアを通過するパケットは、802.1Q トランク、ISL（スイッチ間リンク）トランク、非トランキング リンクのいずれかで送信できます。コア スイッチで 802.1Q トランクを使用する場合、802.1Q トランクのネイティブ VLAN を、同一スイッチの非トランキング（トンネリング）ポートのネイティブ VLAN と照合させることはできません。ネイティブ VLAN のトラフィックに、802.1Q 送信トランク ポートでタグが付かないためです。

図 14-3 を参照してください。VLAN 40 は、サービス プロバイダー ネットワークの入力エッジ スイッチ（スイッチ B）において、カスタマー X からの 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属す、サービス プロバイダー ネットワークのスイッチ B の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN（VLAN 40）は、エッジ スイッチのトランク ポートのネイティブ VLAN（VLAN 40）と同じなので、トンネル ポートから受信したタグ付きパケットにメトロ タグは追加されません。パケットには VLAN 30 タグだけが付いて、サービス プロバイダー ネットワークで出力エッジ スイッチ（スイッチ C）のトランク ポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

この問題の解決方法は次のとおりです。

- サービス プロバイダー ネットワークのコア スイッチ間で ISL トランクを使用します。エッジ スイッチに接続されているカスタマー インターフェイスは 802.1Q トランクとしますが、コア レイヤのスイッチの接続には ISL トランクの使用を推奨します。Cisco ME スイッチでは、ISL トランクをサポートしていません。
- **vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用し、ネイティブ VLAN を含む、802.1Q トランクから発信されるすべてのパケットがタグ付けされるようにエッジ スイッチを設定します。すべての 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。
- エッジ スイッチのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲内でないことを確認します。たとえばトランク ポートが VLAN 100 ～ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

図 14-3　802.1Q トンネリングおよびネイティブ VLAN に潜在する問題



システム MTU

スイッチのトラフィックのデフォルト システム MTU は 1500 バイトです。**system mtu** グローバル コンフィギュレーション コマンドを使用すると、1500 バイトより大きいフレームをサポートするようにファスト イーサネット ポートを設定できます。**system mtu jumbo** グローバル コンフィギュレーション コマンドを使用すると、1500 バイトより大きいフレームをサポートするようにギガビット イーサネット ポートを設定できます。802.1Q トンネリング機能では、メトロ タグが追加されると、フレーム サイズが 4 バイト増加するので、スイッチ システム MTU サイズを最低 1504 バイトに増加して最大フレームを処理できるように、サービス プロバイダー ネットワークのすべてのスイッチを設定する必要があります。ギガビット イーサネット インターフェイスの最大許容システム MTU は 9000 バイトです。ファスト イーサネット インターフェイスの最大システム MTU は 1998 バイトです。

802.1Q トンネリングおよびその他の機能

802.1Q トンネリングはレイヤ 2 パケット スイッチングで適切に動作しますが、一部のレイヤ 2 機能およびレイヤ 3 スイッチングの間には非互換性があります。

（注） レイヤ 3 スイッチングは、スイッチ上でメトロ IP アクセス イメージが稼動している場合に限りサポートされます。

- トンネル ポートはルーテッド ポートにできません。
- 802.1Q トンネル ポートを含む VLAN では IP ルーティングがサポートされません。トンネル ポートから受信したパケットは、レイヤ 2 情報だけに基づいて転送されます。トンネル ポートを含む Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）でルーティングがイネーブルである場合、トンネル ポートから受信したタグなし IP パケットは、スイッチに認識されてルーティングされます。カスタマーは、ネイティブ VLAN でインターネットにアクセスできます。このアクセスが必要ない場合は、トンネル ポートを含む VLAN で SVI を設定しないでください。
- トンネル ポートでは IP Access Control List（ACL; アクセス コントロール リスト）がサポートされません。
- レイヤ 3 QoS（Quality Of Service）ACL およびレイヤ 3 に関連するその他の QoS 機能の情報は、トンネル ポートでサポートされません。MAC ベース QoS はトンネル ポートでサポートされます。
- 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- 802.1Q トンネル ポートでは、Unidirectional Link Detection（UDLD ; 単一方向リンク検出）がサポートされます。
- Port Aggregation Protocol（PAgP; ポート集約プロトコル）および Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）は、Network Node Interface（NNI; ネットワーク ノード インターフェイス）または Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）である 802.1Q トンネル ポート上でだけサポートされます。UNI では、PAgP および LACP をサポートしません。
- 802.1Q トンネル ポートでは、ループバック検出がサポートされます。
- 802.1Q トンネル ポートとして NNI または ENI ポートを設定すると、スパニングツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）フィルタリングはインターフェイスで自動的にイネーブルになり、Cisco Discovery Protocol（CDP）および Layer Link Discovery Protocol（LLDP）はインターフェイスで自動的にディセーブルになります。UNI では、BPDU フィルタリング、CDP、または LLDP をサポートしていません。

- UNI-ENI 独立 VLAN では、802.1Q トンネリングされたアクセス ポートは相互に独立していますが、UNI-ENI コミュニティ VLAN では、これらのポート間でローカル スイッチングが行われます。UNI-ENI VLAN の詳細については、第 12 章「VLAN の設定」を参照してください。

802.1Q トンネリング ポートの設定

802.1Q トンネル ポートとしてポート設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	トンネル ポートとして設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジ ポートである必要があります。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（ポート チャネル 1 ～ 48）が含まれます。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport access vlan** *vlan-id*	デフォルト VLAN を指定します。これは、インターフェイスがトランキングを停止した場合に使用されます。この VLAN ID は特定カスタマーに固有です。 **（注）** VLAN が UNI-ENI 独立 VLAN である場合、スイッチの UNI と ENI 間でのローカル スイッチングは行われません。VLAN が UNI-ENI コミュニティ VLAN である場合、ローカル スイッチングが許可されます。
ステップ 5	**switchport mode dot1q-tunnel**	802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vlan dot1q tag native**	（任意）すべての 802.1Q トランク ポートでネイティブ VLAN パケットのタグ付けをイネーブルにするようにスイッチを設定します。これを設定せず、カスタマー VLAN ID がネイティブ VLAN と同じである場合、トランク ポートはメトロ タグを適用せず、パケットは誤った宛先に送信される可能性があります。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** **show dot1q-tunnel**	802.1Q トンネリング用に設定したポートを表示します。 トンネリング モードになっているポートを表示します。
ステップ 10	**show vlan dot1q tag native**	802.1Q ネイティブ VLAN タグ付けステータスを表示します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

access のデフォルト状態にポートを戻すには、**no switchport mode dot1q-tunnel** インターフェイス コンフィギュレーション コマンドを使用します。ネイティブ VLAN パケットのタグ付けをディセーブルにするには、**no vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用します。

以下は、トンネル ポートとしてインターフェイスを設定してネイティブ VLAN パケットのタグ付けをイネーブルにし、設定を確認する方法の例です。この設定では、ギガビット イーサネット インターフェイス 2 に接続されているカスタマーの VLAN ID が VLAN 22 になっています。この VLAN は、デフォルトで UNI-ENI 独立 VLAN です。

```
Switch(config)# interface gigabitethernet0/2
```

```
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet0/2
dot1q-tunnel mode LAN Port(s)
------------------------------
Gi0/1

Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

VLAN マッピングの概要

S-VLAN を設定するもう 1 つの方法として、カスタマー ネットワークに接続しているトランク ポートに VLAN マッピング（または VLAN ID トランスレーション）を設定して、カスタマー VLAN をサービス プロバイダーの VLAN にマッピングします。ポートに入るパケットは、パケットのポート番号と元のカスタマー VLAN-ID（C-VLAN）に基づいて、サービス プロバイダーの VLAN（S-VLAN）にマッピングされます。

通常のメトロ展開では、カスタマー ネットワーク側の VLAN マッピングは UNI または ENI で行われます。ただし、ネットワーク ノート インターフェイス（NNI）で VLAN マッピングを設定できないわけではありません。

VLAN ID は受信時に S-VLAN にマッピングされるため、ME-3400E では、転送はすべて C-VLAN 情報ではなく S-VLAN 情報を使用して実行されます。

（注）　VLAN マッピングが設定されているポートに機能を設定する場合は常に、カスタマー VLAN-ID（C-VLAN）ではなく、S-VLAN（変換された VLAN）ID が使用されます。

VLAN マッピングが設定されているインターフェイスでは、指定された C-VLAN パケットはポートに入るとき、指定された S-VLAN にマッピングされます。パケットがポートから出る場合も同様に、カスタマー C-VLAN にマッピングが行われます。

スイッチは UNI トランク ポートにおける次の種類の VLAN マッピングをサポートします。

- One-to-One VLAN マッピング。ポートへの入出時に実行され、802.1Q タグの C-VLAN ID が S-VLAN ID にマッピングされます。他のすべての VLAN ID のパケットがドロップされるよう指定することもできます。
- 選択した QinQ は、UNI に入る指定のカスタマー VLAN を指定の S-VLAN ID にマッピングします。S-VLAN は、変更されない受信 C-VLAN に追加されます。他のすべての VLAN ID を転送するトラフィックがドロップされるよう指定することもできます。
- 従来の 802.1Q トンネリング（QinQ）は、ポートの 1 つの S-VLAN ID に対して C-VLAN ID への All-to-one バンドリングを実行します。S-VLAN は、変更されない受信 C-VLAN に追加されます。UNI を従来の QinQ の 802.1Q トンネルとして設定することも、またはより柔軟な実装のトランク ポートに選択した QinQ を設定することもできます。マッピングは、ポートの入出時に実行されます。ポートのすべてのパケットは指定の S-VLAN にバンドルされます。

（注）　タグなしパケットはトランク ネイティブ VLAN のスイッチに入り、マッピングされません。

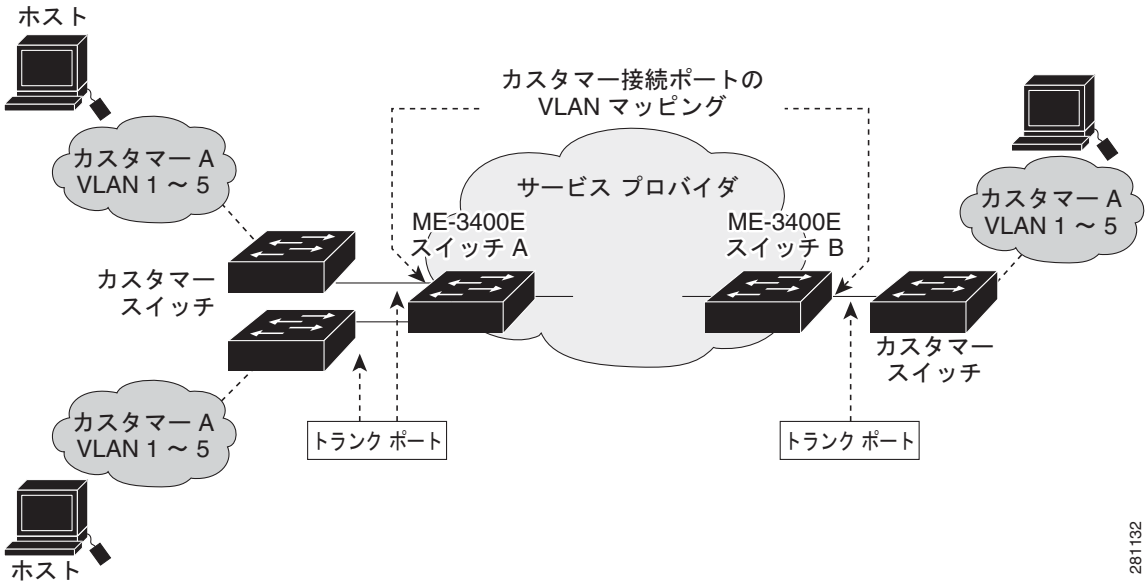
Quality of Service（QoS）については、スイッチは C-CoS または C-DSCP および S-CoS の間で柔軟なマッピングを行い、従来の QinQ によるトラフィックまたは選択した QinQ VLAN マッピングでは内部 CoS から外部 CoS にマッピングします。詳細については、「802.1Q トンネリング CoS マッピング」（P.34-10）を参照してください。

カスタマー VLAN のサービス プロバイダー VLAN へのマッピング

図 14-4 では、カスタマーがサービス プロバイダー ネットワークの両端の複数のサイトで同じ VLAN を使用する場合のトポロジを示します。サービス プロバイダーのバックボーンを通るパケットについて、カスタマー VLAN ID をサービス プロバイダー VLAN ID にマッピングします。カスタマー VLAN ID は、サービス プロバイダー バックボーンの一方の端で取得され、他のカスタマーサイトで使用されます。サービス プロバイダー ネットワークのそれぞれの側のカスタマー接続ポートで同じ VLAN マッピング セットを設定します。

One-to-One マッピング、従来の QinQ、または選択した QinQ を使用してカスタマー VLAN 1 ～ 5 をサービス プロバイダー VLAN にマッピングする設定手順については、例を参照してください。

図 14-4　　カスタマー VLAN のマッピング



VLAN マッピングの設定

- 「VLAN マッピングのデフォルト設定」（P.14-9）
- 「VLAN マッピング設定時の注意事項」（P.14-10）
- 「VLAN マッピングの設定」（P.14-10）

VLAN マッピングのデフォルト設定

デフォルトでは、VLAN マッピングは設定されていません。

VLAN マッピング設定時の注意事項

- 従来の QinQ では 802.1Q トンネル ポートを使用します。802.1Q トランク ポートには、One-to-One VLAN マッピングと選択した QinQ を設定します。
- カスタマー トラフィックが混在しないようにするためには、トランク ポートに従来の Q-in-Q を設定する場合、トランク ポートの許可 VLAN としてサービス プロバイダー S-VLAN ID を設定する必要があります。
- VLAN マッピングが設定された ME-3400E インターフェイスでは、スイッチに入るトラフィックで S-VLAN へのマッピングが行われます。そのため、VLAN マッピングが設定されているインターフェイスにその他の機能を設定する場合、VLAN マッピングとイーサネット E-LMI を設定する場合を除いて、S-VLAN ID を使用する必要があります。インターフェイスに E-LMI を設定する場合、C-VLAN を使用して **ethernet lmi ce-vlan map** *vlan-id* サービス インスタンス コンフィギュレーション モード コマンドを入力します。
- EtherChannel に VLAN マッピングを設定すると、マッピングはポート チャネルのすべてのポートに適用されます。
- ソース ポートがトンネル ポートとして設定されている、またはソース ポートに 1-to-2 マッピングが設定されている場合、SPAN 宛先ポートにカプセル化レプリケーションは設定できません。カプセル化レプリケーションは 1-to-1 VLAN マッピングでサポートされています。
- VLAN マッピングに使用するスイッチ リソースを決定するには、**show vlan mapping usage** または **show platform vlan mapping** 特権 EXEC コマンドを入力します。

VLAN マッピングの設定

次の手順では、トランク ポートに各種類の VLAN マッピングを設定する方法を示します。設定を確認するには、**show interfaces** *interface-id* **vlan mapping** または **show vlan mapping** の各特権 EXEC コマンドを入力します。これらのコマンドの構文については、「トンネリングおよびマッピング ステータスのモニタおよびメンテナンス」（P.14-24）を参照してください。ここで示すコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

One-to-One マッピング

One-to-One VLAN マッピングを設定して VLAN ID をサービス プロバイダーの VLAN ID にマッピングするには、特権 EXEC モードで次の手順を実行します。指定された C-VLAN ID と S-VLAN ID の組み合せが明示的にマッピングされていない限り、トラフィックがドロップされるよう指定するには **default drop** キーワードを使用できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	サービス プロバイダー ネットワークに接続するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。物理インターフェイスまたは EtherChannel ポート チャネルを入力できます。
ステップ 3	**switchport mode trunk**	インターフェイスをトランク ポートとして設定します。

	コマンド	目的
ステップ 4	**switchport vlan mapping** *vlan-id translated-id*	マッピングする VLAN ID を入力します。 • *vlan-id*：カスタマー ネットワークからスイッチに入るカスタマー VLAN ID（C-VLAN）。指定できる範囲は 1 ～ 4094 です。 • *translated-id*：割り当てられた VLAN ID（S-VLAN）。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**switchport vlan mapping default drop**	（任意）ステップ 4 で指定した VLAN に一致しない場合、ポートのすべてのパケットがドロップされるよう指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show vlan mapping**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN マッピング情報を削除するには、**no switchport vlan mapping** *vlan-id translated-id* コマンドを使用します。**no switchport vlan mapping all** を入力すると、すべてのマッピング情報が削除されます。

この例では、図 14-4 で示すように、カスタマー ネットワークの VLAN ID 1 ～ 5 をサービス プロバイダー ネットワークの VLAN ID 101 ～ 105 にマッピングする方法を示します。スイッチ A とスイッチ B のポートに次の同じ VLAN マッピング コマンドを設定します。その他の VLAN ID のトラフィックはドロップされます。

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping 1 101
Switch(config-if)# switchport vlan mapping 2 102
Switch(config-if)# switchport vlan mapping 3 103
Switch(config-if)# switchport vlan mapping 4 104
Switch(config-if)# switchport vlan mapping 4 105
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

前の例では、サービス プロバイダー ネットワークの入力側でカスタマー ネットワークの VLAN ID 1 ～ 5 は、サービス プロバイダー ネットワーク内の VLAN ID 101 ～ 105 にそれぞれマッピングされます。サービス プロバイダー ネットワークの出力側でサービス プロバイダー ネットワークの VLANs 101 ～ 105 は、カスタマー ネットワークの VLAN ID 1 ～ 5 にそれぞれマッピングされます。

トランク ポートの従来の QinQ

トランク ポートまたはデフォルトのトンネリングで従来の QinQ に VLAN マッピングを設定するには、特権 EXEC モードで次の手順を実行します。デフォルトでトンネリングを設定すると、ポートのすべてのパケットが、設定された S-VLAN にバンドルされます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	サービス プロバイダー ネットワークに接続するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。物理インターフェイスまたは EtherChannel ポート チャネルを入力できます。
ステップ 3	**switchport mode trunk**	インターフェイスをトランク ポートとして設定します。
ステップ 4	**switchport trunk allowed vlan** *vlan-id*	サービス プロバイダー ネットワークの外部 VLAN （S-VLAN）がインターフェイスで許可されるよう設定します。これは、次のステップで入力されるものと同じ外部 VLAN ID である必要があります。

	コマンド	目的
ステップ 5	**switchport vlan mapping default dot1q-tunnel** *outer vlan-id*	ポートに入るすべてのパケットが、指定された S-VLAN にバンドルされるよう、VLAN マッピングを設定します。 *outer-vlan-id*：サービス プロバイダー ネットワークの外部 VLAN ID（S-VLAN）を入力します。指定できる範囲は 1 ～ 4094 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id* **vlan mapping**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN マッピング設定を削除するには、**no switchport vlan mapping tunnel default** *outer vlan-id* コマンドを使用します。**no switchport vlan mapping all** を入力すると、すべてのマッピング情報が削除されます。

次の例では、ポートのすべてのトラフィックをバンドルして、S-VLAN ID が 100 のスイッチを出るようにする方法を示します。

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed 100
Switch(config-if)# switchport vlan mapping default dot1q-tunnel 100
Switch(config-if)# exit
```

トランク ポートの選択した QinQ

トランク ポートで、選択した QinQ に VLAN マッピングを設定するには、特権 EXEC モードで次の手順を実行します。One-to-One マッピングと選択した QinQ は同じインターフェイスに設定できますが、両方の設定で同じ C-VLAN ID を使用できない点に注意してください。指定された C-VLAN ID と S-VLAN ID の組み合せが明示的にマッピングされていない限り、トラフィックがドロップされるよう指定するには、キーワード **default drop** を使用できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	サービス プロバイダー ネットワークに接続するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。物理インターフェイスまたは EtherChannel ポート チャネルを入力できます。
ステップ 3	**switchport mode trunk**	インターフェイスをトランク ポートとして設定します。
ステップ 4	**switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id*	マッピングする VLAN ID を入力します。 • *vlan-id*：カスタマー ネットワークからスイッチに入るカスタマー VLAN ID（C-VLAN）。指定できる範囲は 1 ～ 4094 です。VLAN-ID の文字列を入力できます。 • *outer-vlan-id*：サービス プロバイダー ネットワークの外部 VLAN ID（S-VLAN）を入力します。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**switchport vlan mapping default drop**	（任意）ステップ 4 で指定した VLAN に一致しない場合、ポートのすべてのパケットがドロップされるよう指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show interfaces** *interface-id* **vlan mapping**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN マッピング設定を削除するには、**no switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id* コマンドを使用します。**no switchport vlan mapping all** を入力すると、すべてのマッピング情報が削除されます。

次の例では、ポートに選択した QinQ マッピングを設定して、C-VLAN ID が 1 ～ 5 のトラフィックが、S-VLAN ID が 100 であるスイッチに入るようにする方法を示します。その他の VLAN ID のトラフィックはドロップされます。

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping 1-5 dot1q-tunnel 100
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

レイヤ 2 プロトコル トンネリングの概要

サービス プロバイダー ネットワークを越えて接続されている、さまざまなサイトに散在するカスタマーは、さまざまなレイヤ 2 プロトコルを使用してトポロジをスケールし、すべてのリモート サイトおよびローカル サイトを含める必要があります。STP は適切に動作させる必要があり、すべての VLAN は、サービス プロバイダー ネットワークを越えたローカル サイトおよびすべてのリモート サイトを含む、適切なスパニングツリーを構築する必要があります。CDP では、隣接するシスコ製デバイスをローカル サイトおよびリモート サイトから検出する必要があります。VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）では、VTP に参加しているカスタマー ネットワークのすべてのサイトで矛盾しない VLAN 設定を提供する必要があります。

（注）　Cisco ME スイッチでは、VTP をサポートしていません。デフォルトでは、CDP および STP は NNI ではサポートされておらず、ENI でイネーブルにできます。ただし、レイヤ 2 プロトコル トンネリングはスイッチ上のすべてのポートでサポートされます。

プロトコル トンネリングがイネーブルである場合、サービス プロバイダー ネットワークの着信側のエッジ スイッチでは、特殊 MAC アドレスでレイヤ 2 プロトコル パケットがカプセル化され、サービス プロバイダー ネットワークを越えて送信されます。ネットワークのコア スイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、VTP のレイヤ 2 Protocol Data Unit（PDU; プロトコル データ ユニット）は、サービス プロバイダー ネットワークをまたがり、サービス プロバイダー ネットワークの発信側のカスタマー スイッチに配信されます。同一パケットは同じ VLAN のすべてのカスタマー ポートで受信され、次のような結果になります。

- それぞれのカスタマー サイトのユーザは STP を適切に実行でき、すべての VLAN では、ローカル サイトだけではなく、すべてのサイトからのパラメータに基づいて、正しいスパニングツリーが構築されます。
- CDP では、サービス プロバイダー ネットワークによって接続されているその他のシスコ製デバイスに関する情報が検出されて表示されます。
- VTP ではカスタマー ネットワーク全体で矛盾しない VLAN 設定が提供され、VTP をサポートするサービス プロバイダーを通してすべてのスイッチに伝播されます。

（注）　サードパーティ ベンダーとの相互運用性を提供するには、レイヤ 2 プロトコル トンネル バイパス機能を使用します。バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。バイパス モードを実装するには、出力トランク ポートでレイヤ 2 プロトコル トンネリングをイネーブルにします。トランク ポートでレイヤ 2 プロトコル トンネリングがイネーブルである場合、カプセル化されたトンネル MAC アドレスは削除され、プロトコル パケットには通常の MAC アドレスが割り当てられます。

レイヤ 2 プロトコル トンネリングは個別に使用できます。レイヤ 2 プロトコル トンネリングでは、802.1Q トンネリングを向上させることができます。802.1Q トンネリング ポートでプロトコル トンネリングをイネーブルにしていない場合、サービス プロバイダー ネットワークの受信側のリモート スイッチでは PDU を受信せず、STP、CDP、VTP を適切に実行できません。プロトコル トンネリングがイネーブル である場合、それぞれのカスタマー ネットワークのレイヤ 2 プロトコルは、サービス プロバイダー ネットワーク内で動作しているものから完全に区別されます。802.1Q トンネリングでサービス プロバイダー ネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマー スイッチでは、カスタマー VLAN が完全に認識されます。802.1Q トンネリングを使用しない場合は、アクセスまたはトランク ポートでカスタマー スイッチに接続し、サービス プロバイダーのアクセス ポートでトンネリングをイネーブルにすることで、レイヤ 2 プロトコル トンネリングをイネーブルにできます。

たとえば 図 14-5 の場合、カスタマー X には同一 VLAN に 4 つのスイッチがあり、サービス プロバイダー ネットワークで接続されています。ネットワークで PDU がトンネルされない場合、ネットワークの向こう側のスイッチでは、STP、CDP、VTP を適切に実行できません。たとえばカスタマー X、サイト 1 にあるスイッチの VLAN の STP では、サイト 2 のカスタマー X のスイッチに基づくコンバージェンス パラメータが考慮されずに、そのサイトにあるスイッチでスパニング ツリーが構築されます。これにより、図 14-6 のようなトポロジとなります。

図 14-5　レイヤ 2 プロトコル トンネリング

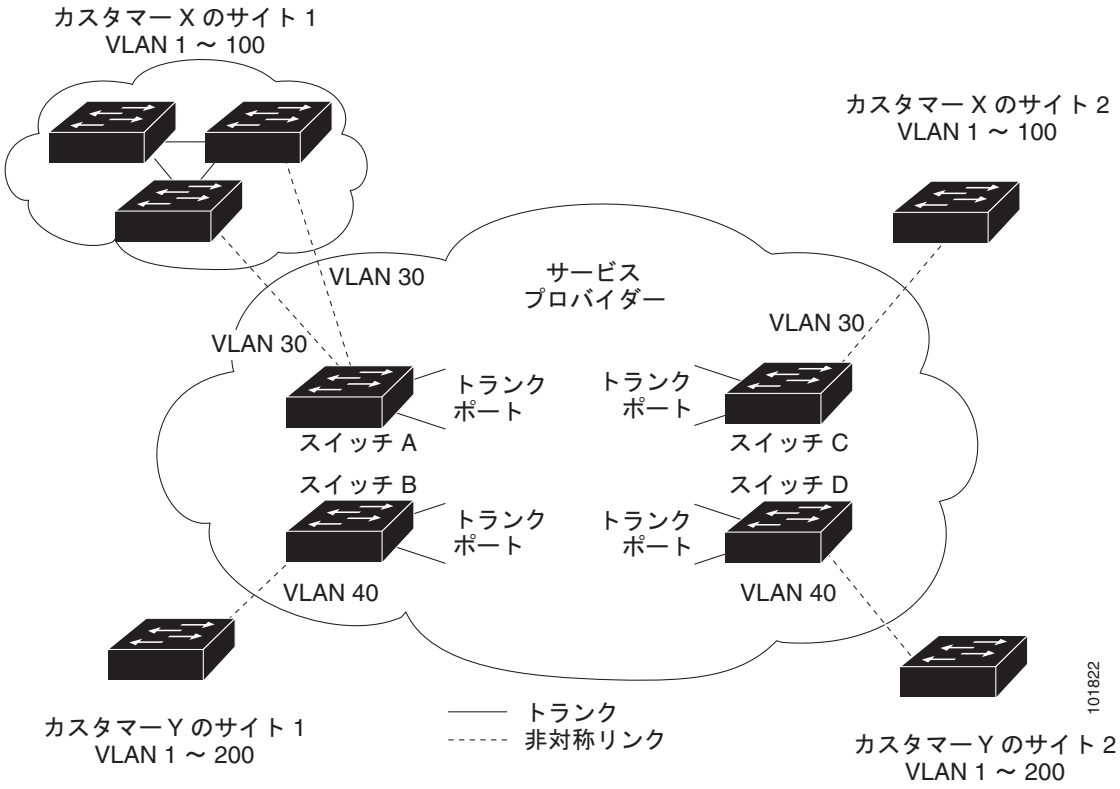
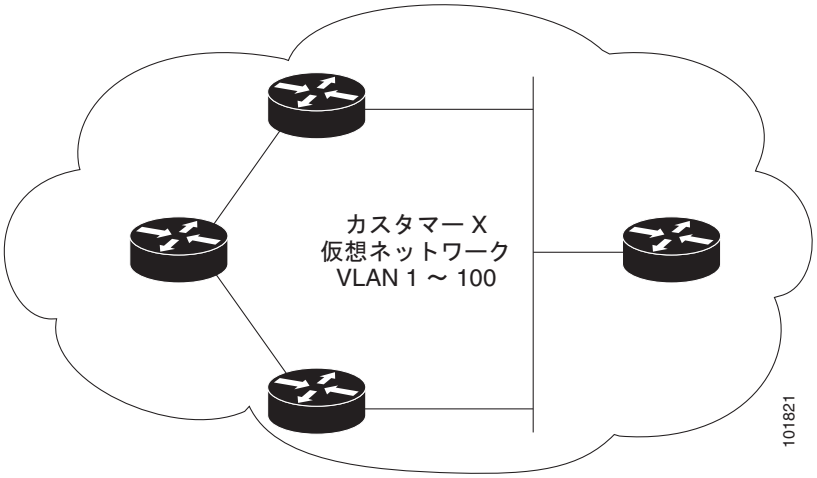


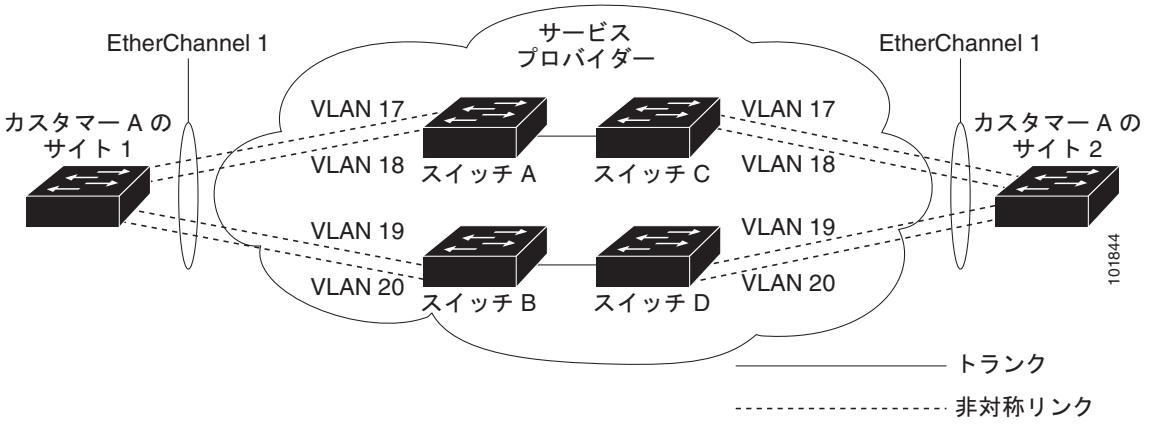
図 14-6　適切なコンバージェンスを含まないレイヤ 2 ネットワーク トポロジ



サービス プロバイダー ネットワークでは、レイヤ 2 プロトコル トンネリングを使用し、ポイントツーポイント ネットワーク トポロジをエミュレートして、EtherChannel の作成を向上させることができます。サービス プロバイダー スイッチでプロトコル トンネリング（PAgP または LACP）をイネーブルにすると、リモート カスタマー スイッチでは PDU が受信され、EtherChannel の自動作成をネゴシエーションできるようになります。

たとえば 図 14-7 の場合、カスタマー A には同一 VLAN に 2 つのスイッチがあり、サービス プロバイダー ネットワークで接続されています。ネットワークで PDU がトンネリングされると、ネットワークの向こう側のスイッチでは、専用回線を必要とせずに、EtherChannel の自動作成をネゴシエーションできます。手順については、「EtherChannel のレイヤ 2 トンネリングの設定」（P.14-20）を参照してください。

図 14-7　EtherChannel のレイヤ 2 プロトコル トンネリング



レイヤ 2 プロトコル トンネリングの設定

サービス プロバイダー ネットワークのエッジ スイッチで、カスタマーに接続されているポートにおいて、レイヤ 2 プロトコル トンネリングをプロトコルごとにイネーブルにできます。カスタマー スイッチに接続されているサービス プロバイダー エッジ スイッチでは、トンネリング処理が実行されます。エッジ スイッチ トンネル ポートは、カスタマーの 802.1Q トランク ポートに接続します。エッジ スイッチ アクセス ポートは、カスタマー アクセス ポートに接続します。カスタマー スイッチに接続されているエッジ スイッチでは、トンネリング処理が実行されます。

アクセス ポート、トンネル ポート、またはトランク ポートとして設定されているポートでは、レイヤ 2 プロトコル トンネリングをイネーブルにできます。スイッチでは、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングがサポートされます。ポイントツーポイント ネットワーク トポロジのエミュレートの場合は、PAgP、LACP、UDLD のプロトコルもサポートされます。スイッチでは、LLDP のレイヤ 2 プロトコル トンネリングがサポートされません。

注意　PAgP、LACP、UDLD プロトコル トンネリングでは、ポイントツーポイント トポロジのエミュレートだけが目的です。設定を間違えたことによりトンネリング パケットが多くのポートに送信されると、ネットワーク障害が発生する可能性があります。

レイヤ 2 プロトコルがイネーブルになっているポートでサービス プロバイダーの着信エッジ スイッチに入ったレイヤ 2 PDU が、トランク ポートからサービス プロバイダー ネットワークに出る場合、スイッチでは、カスタマー PDU 宛先 MAC アドレスが、周知のシスコ固有のマルチキャスト アドレス（01-00-0c-cd-cd-d0）で上書きされます。802.1Q トンネリングがイネーブルである場合、パケットにはタグが 2 重に付きます。外部タグはカスタマーのメトロ タグであり、内部タグはカスタマーの VLAN タグです。コア スイッチでは内部タグが無視され、同じメトロ VLAN のすべてのトランク ポートにパケットが転送されます。発信側のエッジ スイッチでは、適切なレイヤ 2 プロトコル情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのレイヤ 2 プロトコル対応アクセス

ポート、トンネル ポートおよびトランク ポートにパケットが転送されます。このため、レイヤ 2 PDU はそのまま残り、サービス プロバイダー インフラストラクチャを越えてカスタマー ネットワークの反対側に配信されます。

図 14-5 を参照してください。カスタマー X およびカスタマー Y が、それぞれアクセス VLAN 30 および 40 になっています。非対称リンクにより、サイト 1 のカスタマーは、サービス プロバイダー ネットワークのエッジ スイッチに接続されています。サイト 1 のカスタマー Y からスイッチ B に発信されたレイヤ 2 PDU（たとえば BPDU）は、周知の MAC アドレスが宛先 MAC アドレスになっている 2 重タグ パケットとしてインフラストラクチャに転送されます。この 2 重タグ パケットには、40 というメトロ VLAN タグ、および VLAN 100 などの内部 VLAN タグが付いています。2 重タグ パケットがスイッチ D に入ると、外部 VLAN タグ 40 が外されて周知の MAC アドレスがそれぞれのレイヤ 2 プロトコル MAC アドレスで置き換わり、パケットは、VLAN 100 の 1 重タグ フレームとしてサイト 2 のカスタマー Y に送信されます。

カスタマー スイッチのアクセス ポートまたはトランク ポートに接続されているエッジ スイッチのアクセス ポートでも、レイヤ 2 プロトコル トンネリングをイネーブルにできます。この場合は、カプセル化プロセスとカプセル開放プロセスが、前の段落で説明したものと同じですが、パケットはサービス プロバイダー ネットワークで 2 重タグになりません。カスタマー固有のアクセス VLAN タグの 1 重タグになります。

ここでは、次の設定情報について説明します。

- 「レイヤ 2 プロトコル トンネリングのデフォルト設定」（P.14-17）
- 「レイヤ 2 プロトコル トンネリング設定時の注意事項」（P.14-18）
- 「レイヤ 2 プロトコル トンネリングの設定」（P.14-19）
- 「EtherChannel のレイヤ 2 トンネリングの設定」（P.14-20）

レイヤ 2 プロトコル トンネリングのデフォルト設定

表 14-1 に、レイヤ 2 プロトコル トンネリングのデフォルト設定を示します。

表 14-1　レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
レイヤ 2 プロトコル トンネリング	ディセーブル。
シャットダウンしきい値	未設定
ドロップしきい値	未設定
CoS 値	インターフェイスに CoS 値が設定されている場合、その値を使用してレイヤ 2 プロトコル トンネリングに BPDU CoS 値を設定します。インターフェイス レベルで CoS 値が設定されていない場合、L2 プロトコル トンネリング BPDU の CoS マーキングのデフォルト値は 5 になります。これは、データ トラフィックには適用されません。

レイヤ 2 プロトコル トンネリング設定時の注意事項

以下は、レイヤ 2 プロトコル トンネリングの設定時の注意事項および動作特性です。

- スイッチでは、CDP、STP（Multiple STP [MSTP] を含む）、VTP のトンネリングがサポートされます。プロトコル トンネリングはデフォルトでディセーブルになっていますが、802.1Q トンネル ポート、アクセス ポート、またはトランク ポートでプロトコルごとにイネーブルにできます。
- サービス プロバイダー ネットワークの発信側のエッジ スイッチでは、適切なレイヤ 2 プロトコル情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのレイヤ 2 プロトコル対応トンネル ポート、アクセス ポート、トランク ポートにパケットが転送されます。
- サードパーティ ベンダー スイッチとの相互運用性のため、スイッチではレイヤ 2 プロトコルトンネル バイパス機能がサポートされます。バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。スイッチの入力ポートでレイヤ 2 プロトコル トンネルがイネーブルである場合は、出力トランク ポートにより、トンネリングされたパケットが特殊なカプセル化で転送されます。出力トランク ポートでもレイヤ 2 プロトコル トンネリングをイネーブルにすると、この動作がバイパスされて、スイッチによって、処理や修正が行われずに制御 PDU が転送されます。
- スイッチでは、ポイントツーポイント ネットワーク トポロジのエミュレートの場合、PAgP、LACP、UDLD のトンネリングがサポートされます。プロトコル トンネリングはデフォルトでディセーブルになっていますが、802.1Q トンネル ポート、アクセス ポート、またはトランク ポートでプロトコルごとにイネーブルにできます。
- PAgP トンネリングまたは LACP トンネリングの場合は、リンク障害検出を高速にするため、インターフェイスで UDLD もイネーブルにするよう推奨します。
- PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのレイヤ 2 プロトコル トンネリングでは、ループバック検出がサポートされません。
- 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- 独自の宛先 MAC アドレスでカプセル化された PDU が、レイヤ 2 トンネリングがイネーブルになっているトンネル ポート、アクセス ポート、またはトランク ポートから受信される場合、トンネル ポートは、ループを防止するためにシャットダウンされます。このポートは、プロトコル用に設定されたシャットダウンしきい値に達した場合にもシャットダウンされます。**shutdown** コマンドに続けて **no shutdown** コマンドを入力すると、ポートを再び手動でイネーブルにできます。errdisable recovery がイネーブルの場合は、指定された間隔で動作が再試行されます。
- カプセル化が解除された PDU だけがカスタマー ネットワークに転送されます。サービス プロバイダー ネットワーク上で動作しているスパニングツリー インスタンスでは、BPDU がトンネル ポートに転送されません。CDP パケットはトンネル ポートから転送されません。
- インターフェイスでプロトコル トンネリングがイネーブルの場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのシャットダウンしきい値やポートごとのシャットダウンしきい値を設定できます。制限を越えると、ポートはシャットダウンされます。QoS ACL およびポリシー マップをトンネル ポートで使用すると、BPDU レートを制限することもできます。
- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとの廃棄しきい値やポートごとの廃棄しきい値を設定できます。制限を越えると、ポートが PDU を受信するレートが廃棄しきい値未満になるまで、ポートで PDU が廃棄されます。
- トンネリングされた PDU（とくに STP BPDU）は、カスタマーの仮想ネットワークが正しく動作するためにすべてのリモート サイトに配信される必要があるので、同じトンネル ポートから受信されるデータ パケットよりも PDU のプライオリティをサービス プロバイダー ネットワーク内で高くできます。デフォルトの場合、PDU ではデータ パケットと同じ CoS 値が使用されます。

レイヤ 2 プロトコル トンネリングの設定

レイヤ 2 プロトコル トンネリング用にポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、トンネル ポートとして設定するインターフェイスを入力します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジ ポートである必要があります。有効なインターフェイスは、物理インターフェイスおよびポートチャネル論理インターフェイス（ポート チャネル 1 ～ 48）です。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport mode access** または **switchport mode dot1q-tunnel** または **switchport mode trunk**	アクセス ポート、802.1Q トンネル ポート、またはトランク ポートとしてインターフェイスを設定します。デフォルトのスイッチ ポート モードは、access です。
ステップ 5	**l2protocol-tunnel** [**cdp** | **stp** | **vtp**]	目的のプロトコルのプロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングは 3 つすべてのレイヤ 2 プロトコルでイネーブルになります。
ステップ 6	**l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] *value*	（任意）カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ～ 4096 です。デフォルトでは、しきい値 が設定されていません。 **（注）**　このインターフェイスで廃棄しきい値も設定する場合、シャットダウンしきい値は、廃棄しきい値以上とする必要があります。
ステップ 7	**l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *value*	（任意）カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスによってパケットが廃棄されます。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ～ 4096 です。デフォルトでは、しきい値 が設定されていません。 このインターフェイスでシャットダウンしきい値も設定する場合、廃棄しきい値は、シャットダウンしきい値以下でなければなりません。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**errdisable recovery cause l2ptguard**	（任意）インターフェイスを再びイネーブルにして再試行できるようにするため、レイヤ 2 最大レート エラーからの回復メカニズムを設定します。errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 10	**l2protocol-tunnel cos** *value*	（任意）トンネリングされたすべてのレイヤ 2 PDU の CoS 値を設定します。範囲は 0 ～ 7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。

	コマンド	目的
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show l2protocol**	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのプロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel** [**cdp** | **stp** | **vtp**] インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値および廃棄しきい値をデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] コマンドおよび **no l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] コマンドを使用します。

次は、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングを設定し、設定を確認する方法の例です。

```
Switch(config)# interface gigatethernet0/1
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
Port      Protocol Shutdown  Drop      Encapsulation Decapsulation Drop
                   Threshold Threshold Counter       Counter       Counter
-------   -------- --------- --------- ------------- ------------- -------------
Gi  0/1   cdp           1500      1000 2288          2282          0
          stp            1500       1000 116           13            0
          vtp            1500       1000 3             67            0
          pagp           ----       ---- 0             0             0
          lacp           ----       ---- 0             0             0
          udld           ----       ---- 0             0             0
```

EtherChannel のレイヤ 2 トンネリングの設定

レイヤ 2 ポイントツーポイント トンネリングを設定して EtherChannel の自動作成を容易にするには、サービス プロバイダー エッジ スイッチおよびカスタマー スイッチの両方を設定する必要があります。

サービス プロバイダー エッジ スイッチの設定

EtherChannel のレイヤ 2 プロトコル トンネリング用にサービス プロバイダー エッジ スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、トンネル ポートとして設定するインターフェイスを入力します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジ ポートである必要があります。有効なインターフェイスは物理インターフェイスです。

	コマンド	目的
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport mode dot1q-tunnel**	802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ 5	**l2protocol-tunnel point-to-point** [**pagp** | **lacp** | **udld**]	（任意）目的のプロトコルのポイントツーポイント プロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングは、3 つすべてのプロトコルでイネーブルになります。 **注意** ネットワーク障害を避けるため、ネットワークがポイントツーポイント トポロジになっていることを確認してから、PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのトンネリングをイネーブルにしてください。
ステップ 6	**l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*	（任意）カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ～ 4096 です。デフォルトでは、しきい値 が設定されていません。 **（注）** このインターフェイスで廃棄しきい値も設定する場合、シャットダウンしきい値は、廃棄しきい値以上とする必要があります。
ステップ 7	**l2protocol-tunnel drop-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*	（任意）カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスによってパケットが廃棄されます。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ～ 4096 です。デフォルトでは、しきい値 が設定されていません。 **（注）** このインターフェイスでシャットダウンしきい値も設定する場合、廃棄しきい値は、シャットダウンしきい値以下でなければなりません。
ステップ 8	**no cdp enable**	インターフェイスが NNI の場合、インターフェイス上で CDP をディセーブルにします。デフォルトでは、CDP は ENI 上でディセーブルに設定されています。UNI では、CDP をサポートしません。
ステップ 9	**spanning-tree bpdufilter enable**	インターフェイスが NNI または ENI の場合、インターフェイス上で BPDU フィルタリングをディセーブルにします。UNI は、STP PBDU フィルタリングをサポートしません。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**errdisable recovery cause l2ptguard**	（任意）インターフェイスを再びイネーブルにして再試行できるようにするため、レイヤ 2 最大レート エラーからの回復メカニズムを設定します。errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 12	**l2protocol-tunnel cos** *value*	（任意）トンネリングされたすべてのレイヤ 2 PDU の CoS 値を設定します。範囲は 0 ～ 7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show l2protocol**	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのポイントツーポイント プロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel** [**point-to-point** [**pagp** | **lacp** | **udld**]] インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値および廃棄しきい値をデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] コマンドおよび **no l2protocol-tunnel drop-threshold** [[**point-to-point** [**pagp** | **lacp** | **udld**]] コマンドを使用します。

カスタマー スイッチの設定

サービス プロバイダー エッジ スイッチを設定したら、特権 EXEC モードで次の手順を実行し、EtherChannel のレイヤ 2 プロトコル トンネリング用にカスタマー スイッチを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチ ポートにする必要があります。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport mode trunk**	インターフェイス上でトランキングをイネーブルにします。
ステップ 5	**udld enable**	インターフェイスの**通常**モードで UDLD をイネーブルにします。
ステップ 6	**channel-group** *channel-group-number* **mode desirable**	チャネル グループにインターフェイスを割り当て、インターフェイスが NNI または ENI である場合に PAgP モードに **desirable** を指定します。EtherChannel の設定の詳細については、第 35 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface port-channel** *port-channel number*	ポートチャネル インターフェイス モードを開始します。
ステップ 9	**shutdown**	インターフェイスをシャットダウンします。
ステップ 10	**no shutdown**	インターフェイスをイネーブルにします。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show l2protocol**	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**no switchport mode trunk**、**no udld enable**、**no channel group** *channel-group-number* **mode desirable** インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel の場合は、サービス プロバイダー エッジ スイッチおよびカスタマー スイッチをレイヤ 2 プロトコル トンネリング用に設定する必要があります （図 14-7（P.14-16）を参照）。

以下は、サービス プロバイダーのエッジ スイッチ 1 およびエッジ スイッチ 2 を設定する方法の例です。VLAN 17、18、19、20 はアクセス VLAN、ギガビット イーサネット インターフェイス 1 および 2 は PAgP および UDLD がイネーブルになっているポイントツーポイント トンネル ポート、廃棄しきい値は 1000、ファスト イーサネット インターフェイス 3 はトランク ポートです。

サービス プロバイダー エッジ スイッチ 1 の設定は次のとおりです。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport access vlan 17
```

```
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

サービス プロバイダー エッジ スイッチ 2 の設定は次のとおりです。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

次は、サイト 1 のカスタマー スイッチを設定する方法の例です。ファスト イーサネット インターフェイス 1、2、3、4 は 802.1Q トランキング用に設定されており、UDLD はイネーブル、EtherChannel グループ 1 はイネーブル、ポート チャネルはシャットダウンされたあとでイネーブルになって EtherChannel 設定がアクティブになります。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/4
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
```

```
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

トンネリングおよびマッピング ステータスのモニタおよびメンテナンス

表 14-2 は、802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングおよび VLAN マッピングのモニタとメンテナンスを行う特権 EXEC コマンドの説明です。

表 14-2　トンネリングのモニタおよびメンテナンスのためのコマンド

コマンド	目的
clear l2protocol-tunnel counters	レイヤ 2 プロトコル トンネリング ポートのプロトコル カウンタをクリアします。
show dot1q-tunnel	スイッチの 802.1Q トンネル ポートを表示します。
show dot1q-tunnel interface *interface-id*	特定インターフェイスがトンネル ポートであるかどうかを確認します。
show interfaces [**interface** *interface-id*] **vlan mapping**	すべてのインターフェイスまたは指定されたインターフェイスの VLAN マッピング情報を表示します。
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
show errdisable recovery	レイヤ 2 プロトコル トンネル エラー ディセーブル状態からの回復タイマーがイネーブルかどうかを確認します。
show l2protocol-tunnel interface *interface-id*	特定レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
show l2protocol-tunnel summary	レイヤ 2 プロトコルのサマリー情報だけを表示します。
show platform vlan mapping	プラットフォーム VLAN マッピング情報を表示します。
show vlan dot1q tag native	スイッチのネイティブ VLAN タグのステータスを表示します。
show vlan mapping [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスの VLAN マッピング情報を表示します。
show vlan mapping usage	VLAN マッピング専用のスイッチのハードウェア リソースの使用に関する情報を表示します。

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

CHAPTER 15

STP の設定

この章では、Cisco ME 3400E イーサネット アクセススイッチのポートベースの VLAN（仮想 LAN）に Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）を設定する方法について説明します。スイッチは、IEEE 802.1D 標準に基づく Per-VLAN Spanning-Tree Plus（PVST+; VLAN 単位スパニング ツリー プラス）プロトコルとシスコ独自の拡張機能、または IEEE 802.1w 標準に基づく Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルを使用します。Cisco ME スイッチでは、STP は Network Node Interface（NNI; ネットワーク ノード インターフェイス）上でデフォルトでイネーブルに設定されます。Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）上ではデフォルトでディセーブルになっていますが、イネーブルにできます。スイッチ上の User Network Interface（UNI; ユーザ ネットワーク インターフェイス）は STP に参加しません。STP がイネーブルにされていない UNI および ENI は、起動されるとすぐにトラフィックを転送します。

Multiple Spanning-Tree Protocol（MSTP; マルチ スパニング ツリー プロトコル）と複数の VLAN を同じスパニング ツリー インスタンスに対応付ける方法の詳細については、第 16 章「MSTP の設定」を参照してください。また、PortFast、ルート ガードなどの他のスパニング ツリー機能の詳細については、第 17 章「オプションのスパニング ツリー機能の設定方法」を参照してください。

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

この章で説明する内容は、次のとおりです。

- 「スパニング ツリー機能の概要」（P.15-1）
- 「スパニング ツリー機能の設定」（P.15-12）
- 「スパニング ツリー ステータスの表示」（P.15-24）

スパニング ツリー機能の概要

- 「STP の概要」（P.15-2）
- 「スパニング ツリー トポロジと BPDU」（P.15-3）
- 「ブリッジ ID、スイッチ プライオリティ、および拡張システム ID」（P.15-4）
- 「スパニング ツリー インターフェイスのステート」（P.15-5）
- 「スイッチまたはポートがルート スイッチまたはルート ポートになる方法」（P.15-8）
- 「スパニング ツリーおよび冗長接続」（P.15-9）
- 「スパニング ツリー アドレスの管理」（P.15-9）

- 「接続を維持するための有効期間の短縮」（P.15-9）
- 「スパニング ツリー モードとプロトコル」（P.15-10）
- 「スパニング ツリー インスタンスのサポート」（P.15-11）
- 「スパニング ツリーの相互運用性と下位互換性」（P.15-11）
- 「STP および IEEE 802.1Q トランク」（P.15-11）

設定の詳細については、「スパニング ツリー機能の設定」（P.15-12）を参照してください。

オプションのスパニング ツリー機能の詳細については、第 17 章「オプションのスパニング ツリー機能の設定方法」を参照してください。

STP の概要

STP は、ネットワーク内のループを防ぎながらパスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正常に動作するのは、任意の 2 つのステーション間にアクティブ パスが 1 つだけ存在する場合です。エンド ステーション間に複数のアクティブ パスがあると、ネットワーク内でループが発生する原因になります。ネットワークにループが存在すると、エンド ステーションが重複したメッセージを受信する可能性があります。また、スイッチが複数のレイヤ 2 インターフェイス上のエンド ステーション MAC（メディア アクセス制御）アドレスを学習する可能性もあります。このような状態ではネットワークが不安定になります。スパニング ツリーの動作はエンド ステーションにとってトランスペアレントであるため、エンド ステーション側では、1 つの LAN セグメントに接続されているのか、それとも複数のセグメントからなるスイッチド LAN に接続されているのかを認識できません。

STP は、スパニング ツリー アルゴリズムを使用して、冗長接続されたネットワークのいずれかのスイッチをスパニング ツリーのルートとして選択します。アルゴリズムは、アクティブ トポロジ内のポートの役割に基づいて各ポートに役割を割り当てることで、スイッチド レイヤ 2 ネットワークを経由する最適なループフリー パスを計算します。

- ルート：スパニング ツリー トポロジに対して選択されたフォワーディング ポート
- 指定：各スイッチド LAN セグメントに対して選択されたフォワーディング ポート
- 代替：スパニング ツリー内のルート ブリッジへの代替パスを提供するブロッキング ポート
- バックアップ：ループバック構成内のブロッキング ポート

（注）　Cisco ME 3400E スイッチでは、STP がイネーブルにされている NNI と ENI だけが STP に参加します。STP がイネーブルにされていないアクティブな UNI や ENI は、常にフォワーディング ステートです。この概要では、他のスイッチ上では STP ポートを任意のインターフェイスにできますが、Cisco ME スイッチ上では NNI または STP 対応の ENI に限られます。

すべてのポートで指定の役割またはバックアップの役割が設定されたスイッチは、ルート スイッチです。少なくとも *1* つのポートで指定の役割が設定されたスイッチを、指定スイッチと呼びます。

スパニング ツリーは、冗長データパスを強制的にスタンバイ（ブロック）ステートにします。スパニング ツリーの 1 つのネットワーク セグメントで障害が発生し、かつ冗長パスが存在する場合、STP アルゴリズムはスパニング ツリー トポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、定期的に Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）と呼ばれるスパニング ツリー フレームを送受信します。スイッチはこのようなフレームを転送せずに、フレームを使用してループフリー パスを構築します。BPDU には、スイッチおよび MAC アドレス、スイッチのプライオリティ、ポートのプライオリティ、パス コストなど、送信スイッチとそのポートに関する

情報が格納されています。スパニング ツリーは、この情報を使用して、スイッチド ネットワークのルート スイッチおよびルート ポート、さらに、各スイッチド セグメント用のルート ポートおよび指定ポートを選択します。

スイッチ上の 2 つのポートがループの一部になっている場合は、スパニング ツリー ポート プライオリティおよびパス コストの設定によって、フォワーディング ステートになるポートとブロッキング ステートになるポートが決まります。スパニング ツリー ポート プライオリティ値は、ネットワーク トポロジ内でのポートの位置を表すとともに、ポートがトラフィックを伝送するために適した位置にあるかどうかを表します。パス コスト値は、メディア速度を表します。

（注）　スイッチは、（接続がアップであることを確認するために）Small Form-factor Pluggable（SFP）モジュールがないインターフェイスにだけ、キープアライブ メッセージを送信します。

スパニング ツリー トポロジと BPDU

アクティブで安定したスイッチド ネットワークのスパニング ツリー トポロジは、次の要素によって決まります。

- 各スイッチの各 VLAN に対応付けられた固有のブリッジ ID（スイッチ プライオリティおよび MAC アドレス）
- ルート スイッチへのスパニング ツリー パス コスト
- 各レイヤ 2 STP 対応インターフェイスに関連付けられたポート ID（ポート プライオリティおよび MAC アドレス）

ネットワーク内のスイッチの電源がオンになっている場合、1 つ 1 つの各スイッチがルート スイッチとして機能します。各スイッチは、すべてのポートを介してコンフィギュレーション BPDU を送信します。または、Cisco ME スイッチの場合は STP 対応ポートだけを介して送信します。BPDU によってスパニング ツリー トポロジの通信と計算が行われます。各コンフィギュレーション BPDU には、次の情報が格納されています。

- 送信スイッチがルート スイッチとして識別するスイッチの一意のブリッジ ID
- ルートへのスパニング ツリー パス コスト
- 送信スイッチのブリッジ ID
- メッセージ有効期間
- 送信インターフェイスの識別子
- hello タイマー、転送遅延タイマー、および最大エージング プロトコル タイマーの値

スイッチは、*上位の*情報（低ブリッジ ID 値、低パス コスト値など）を持つコンフィギュレーション BPDU を受信すると、そのポートの情報を保存します。スイッチは、ルート ポートでこの BPDU を受信すると、そのスイッチが指定スイッチとなっているすべての接続 LAN に、この BPDU を更新メッセージと一緒に転送します。

スイッチは、現在ポートに保存されている情報よりも *下位の*情報が含まれたコンフィギュレーション BPDU を受信すると、その BPDU を廃棄します。スイッチが下位 BPDU の受信元 LAN の指定スイッチである場合、そのスイッチはそのポート用に保存されている最新情報の BPDU をその LAN に送信します。これによって下位の情報は廃棄され、優位の情報がネットワークを伝播します。

BPDU の交換により、次の処理が実行されます。

- ネットワーク内の 1 つのスイッチがルート スイッチとして選択されます（スイッチド ネットワーク内のスパニング ツリー トポロジの論理的な中心）。

各 VLAN で、スイッチ プライオリティの最も高い（プライオリティ値が最小の）スイッチが、ルート スイッチとして選択されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合は、VLAN 内で最小の MAC アドレスを持つスイッチがルート スイッチになります。表 15-1（P.15-4）に示すとおり、スイッチ プライオリティ値は、ブリッジ ID の最優位ビットを占めます。

- 各スイッチに 1 つルート ポートが選択されます（ルート スイッチを除く）。このポートは、そのスイッチからルート スイッチへパケットを転送するのに最適なパス（最も低コストのパス）となります。
- パス コストに基づいて、各スイッチからルート スイッチまでの最短距離が計算されます。
- LAN セグメントごとに指定スイッチが選択されます。指定スイッチは、その LAN からルート スイッチにパケットを転送するときに最もコストの低いパスを選びます。指定スイッチと LAN の接続に使用されるポートを指定ポートと呼びます。Cisco ME スイッチでは、特に STP がイネーブルにされている NNI または ENI にだけ適用されます。

スイッチド ネットワークの起点に関わらず、ルート スイッチに到達する必要のないパスはすべて、スパニング ツリー ブロッキング モードになります。

ブリッジ ID、スイッチ プライオリティ、および拡張システム ID

IEEE 802.1D 規格では、各スイッチには一意のブリッジ識別子（ブリッジ ID）を割り当てる必要があります。これによってルート スイッチが選択されます。各 VLAN は、PVST+ および Rapid PVST+ 搭載の異なる*論理ブリッジ*と見なされるので、各スイッチは、設定されている VLAN ごとに異なるブリッジ ID を備えている必要があります。スイッチ上の各 VLAN には一意の 8 バイト ブリッジ ID が割り当てられています。最上位の 2 バイトはスイッチのプライオリティに使用し、残りの 6 バイトは、スイッチの MAC アドレスとなっています。

スイッチは IEEE 802.1t スパニング ツリー拡張機能をサポートし、以前にスイッチのプライオリティが使用していたビットのいくつかは、現在 VLAN ID として使用されています。その結果、ブリッジ ID の固有性を維持しながら、スイッチ用に予約される MAC アドレスが少なくなり、サポートできる VLAN ID の範囲は大きくなっています。表 15-1 に示すように、以前スイッチのプライオリティが使用していた 2 バイトは、4 ビット プライオリティ値と、VLAN ID に等しい 12 ビット拡張システム ID に再割り当てされています。

表 15-1　スイッチ プライオリティ値および拡張システム ID

スイッチ プライオリティ値				拡張システム ID（VLAN ID と等価に設定）											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニング ツリーは、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニング ツリー MAC アドレスを使用して、各 VLAN の一意のブリッジ ID が重複しないようにします。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティを手動で設定する方法に影響が生じます。たとえば、スイッチ プライオリティ値を変更すると、スイッチがルート スイッチとして選択される可能性が変更されます。大きい値を設定すると可能性が減り、小さい値を設定すると可能性が増します。詳細については、「ルート スイッチの設定」（P.15-16）、「セカンダリ ルート スイッチの設定」（P.15-18）、および「VLAN のスイッチ プライオリティの設定」（P.15-21）を参照してください。

スパニング ツリー インターフェイスのステート

プロトコル情報がスイッチド LAN を通過するときに、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジの変更が発生します。STP ポートがスパニング ツリー トポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成される可能性があります。インターフェイスは、新しいトポロジ情報がスイッチド LAN 経由で伝達されるまで待機し、その後、フレーム転送を開始する必要があります。また、古いトポロジで転送されたフレームの存続時間を満了させることも必要です。

スパニング ツリーを使用するスイッチ上の各レイヤ 2 インターフェイスは、次のいずれかのステートで存在します。

- ブロッキング：インターフェイスはフレーム転送に参加しません。
- リスニング：インターフェイスがフレーム転送に参加する必要があるとスパニング ツリーが判断した場合に、ブロッキング ステート後最初に開始する移行ステートです。
- ラーニング：インターフェイスはフレーム転送に参加する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニング ツリーに参加していない状態です。ポートのシャットダウン、ポート上のリンク欠落、ポートで稼動するスパニング ツリー インスタンスが存在しないことなどが原因で、フレームを転送していない状態です。

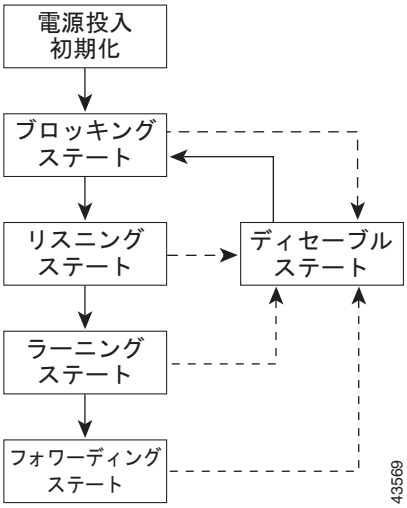
（注） Cisco ME スイッチ上では、UNI は常にフォワーディング ステートです。デフォルトの STP モードの ENI（ディセーブル）もフォワーディング ステートですが、ENI 上で STP をイネーブルにできます。

スパニング ツリーに参加するポートは、次のステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 15-1 に、インターフェイスがステートを移行する様子を示します。

図 15-1　スパニング ツリー インターフェイスのステート



スイッチの電源をオンにした場合、スパニング ツリーはデフォルトでイネーブルになり、Cisco ME スイッチ（と STP がイネーブルになっている各 ENI）のすべての NNI は、スパニング ツリーに参加する VLAN またはネットワークの他のスイッチのその他のポートと同様に、ブロッキング ステートおよびリスニングからラーニングへの移行ステートを経由します。スパニング ツリーは、各インターフェイスをフォワーディング ステートまたはブロッキング ステートで安定させます。

（注）　デフォルトで、UNI はシャット ダウンされていて、起動されるとすぐにトラフィックの転送を開始します。ポート上の STP を明確にイネーブルにしない限り、ENI は UNI と同じように機能します。

スパニング ツリー アルゴリズムによってレイヤ 2 スパニング ツリー インターフェイスがフォワーディング ステートになる場合には、次のプロセスが発生します。

1. インターフェイスはリスニング ステートになり、スパニング ツリーはインターフェイスをブロッキング ステートに移行するよう指示するプロトコル情報を待ちます。
2. スパニング ツリーは、転送遅延タイマーの満了を待ってインターフェイスをラーニング ステートに移行し、転送遅延タイマーをリセットします。
3. ラーニング ステートでは、インターフェイスは引き続きフレーム転送をブロックし、その間にスイッチは転送データベースのエンド ステーションのロケーション情報を学習します。
4. 転送遅延タイマーが満了すると、スパニング ツリーはインターフェイスをフォワーディング ステートに移行し、ここでラーニングとフレーム転送の両方がイネーブルになります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスは、フレーム転送に参加しません。初期化後、スイッチの各インターフェイスにまたは各スイッチ STP ポートに BPDU が送信されます。スイッチは最初、他のスイッチと BPDU を交換するまでルートとして動作します。この交換により、ネットワーク上のどのスイッチがルート（またはルート スイッチ）であるかが確定します。ネットワークにスイッ

チが 1 つしか存在しない場合は、BPDU 交換は行われず、転送遅延タイマーが満了し、インターフェイスはリスニング ステートに移行します。スイッチの初期化後、スパニング ツリーに参加しているインターフェイスは常にブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の処理を実行します。

- インターフェイスで受信したフレームを廃棄します。
- 別のインターフェイスから転送用にスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、レイヤ 2 インターフェイスがブロッキング ステートを経て移行する最初のステートです。このインターフェイスはフレーム転送に参加すべきであるとスパニング ツリーが判断した場合、インターフェイスはこのステートになります。

リスニング ステートのインターフェイスは、次の処理を実行します。

- インターフェイスで受信したフレームを廃棄します。
- 別のインターフェイスから転送用にスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレーム転送に参加する準備をしています。インターフェイスは、リスニング ステートからラーニング ステートへ移行します。

ラーニング ステートのインターフェイスは、次の処理を実行します。

- インターフェイスで受信したフレームを廃棄します。
- 別のインターフェイスから転送用にスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。インターフェイスは、ラーニング ステートからフォワーディング ステートへ移行します。

フォワーディング ステートのインターフェイスは、次の処理を実行します。

- インターフェイスで受信したフレームを受け入れ、転送します。
- 別のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ディセーブル ステートのレイヤ 2 インターフェイスは、フレーム転送やスパニング ツリーに参加しません。ディセーブル ステートのインターフェイスは、動作不能です。

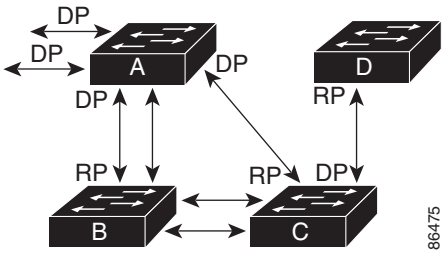
ディセーブルになったインターフェイスは、次の処理を実行します。

- インターフェイスで受信したフレームを廃棄します。
- 別のインターフェイスから転送用にスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU は受信しません。

スイッチまたはポートがルート スイッチまたはルート ポートになる方法

ネットワーク内のすべてのスイッチがデフォルトのスパニング ツリー設定でイネーブルな場合は、最小の MAC アドレスを持つスイッチがルート スイッチになります。図 15-2 では、スイッチ A がルート スイッチに選択されています。すべてのスイッチでスイッチ プライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるためです。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート ブリッジであるとはかぎりません。最適なスイッチのプライオリティを上げる（プライオリティの数値を小さくする）ことによって、そのスイッチがルート スイッチに設定すれば、最適なスイッチをルートとして持つ新しいスパニング ツリー トポロジを形成するよう、強制的に再計算させることができます。

図 15-2　　スパニング ツリー トポロジ



RP = ルート ポート
DP = 指定ポート

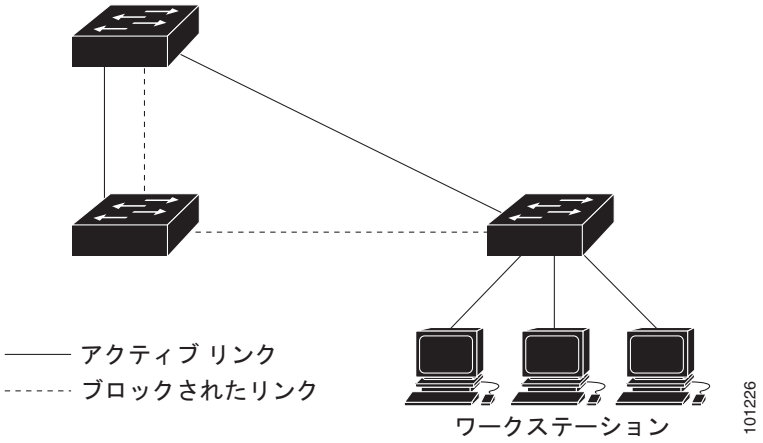
スパニング ツリー トポロジをデフォルトのパラメータに基づいて計算すると、スイッチド ネットワーク上の送信元から宛先エンド ステーションまでのパスが最適にならない可能性があります。たとえば、ルート ポートよりもプライオリティの高いインターフェイスに、より高速のリンクを接続すると、ルート ポートが変更されます。重要なのは、最も高速のリンクをルート ポートにすることです。

たとえば、スイッチ B の 1 つのポートがギガビット イーサネット リンクであり、同じスイッチの別のポート（10/100 リンク）がルート ポートになっていると仮定します。ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパニング ツリー ポート プライオリティをルート ポートよりも高く（数値を小さく）すれば、ギガビット イーサネット ポートが新しいルート ポートになります。

スパニング ツリーおよび冗長接続

図 15-3 に示すように、スパニング ツリーに参加する 2 つのスイッチ インターフェイスを別のデバイス、または 2 台の異なるデバイスに接続することにより、スパニング ツリーによる冗長バックボーンを作成できます。スパニング ツリーは、一方のインターフェイスを自動的にディセーブルにしますが、他方のインターフェイスに障害が発生すると、ディセーブルになっていたインターフェイスをイネーブルにします。一方のリンクが高速で、他方が低速の場合、常に低速の方のリンクがディセーブルになります。2 つのリンクの速度が同じ場合、ポート プライオリティとポート ID が加算され、値が小さいリンクがスパニング ツリーによってディセーブルにされます。

図 15-3　　スパニング ツリーおよび冗長接続



EtherChannel グループを使用して、スイッチ間に冗長リンクを設定することもできます。詳細については、第 35 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

スパニング ツリー アドレスの管理

IEEE 802.1D には、さまざまなブリッジ プロトコルが使用するマルチキャスト アドレスとして、0x00180C2000000 ～ 0x0180C2000010 の範囲のアドレスが 17 個規定されています。このアドレスはスタティック アドレスなので削除できません。

スパニング ツリー ステートに関係なく、各スイッチは 0x0180C2000000 ～ 0x0180C200000F のアドレス宛のパケットを受信しますが、転送は行いません。

スパニング ツリーがイネーブルな場合、スイッチの CPU は 0x0180C2000000 および 0x0180C2000010 宛のパケットを受信します。スパニング ツリーがディセーブルの場合は、スイッチは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するための有効期間の短縮

ダイナミック アドレスの有効期間のデフォルト値は 5 分（**mac address-table aging-time** グローバル コンフィギュレーション コマンドによるデフォルト設定）です。ただし、スパニング ツリーの再構成により、多数のステーション ロケーションが変更される場合があります。このようなステーションには、再構成中、5 分以上にわたって到達できないことがあるので、アドレス テーブルからステーション

アドレスを削除し、改めて学習できるように、アドレス有効期間が短縮されます。短縮された有効期間は、スパニング ツリーの再構成時には、転送遅延パラメータの値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN は独立したスパニング ツリー インスタンスなので、スイッチは VLAN 単位で有効期間を短縮します。ある VLAN でスパニング ツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスが有効期間短縮の対象になることがあります。他の VLAN のダイナミック アドレスは影響を受けず、スイッチで設定された有効期間がそのまま適用されます。

スパニング ツリー モードとプロトコル

STP がイネーブルにされているスイッチ NNI および ENI は、次のスパニング ツリー モードおよびプロトコルをサポートします。

- PVST+：このスパニング ツリー モードは、IEEE 802.1D 標準とシスコ独自の拡張機能に基づいています。これがデフォルトのスパニング ツリー モードであり、ほとんどのイーサネット ポート ベースの VLAN で使用されます。PVST+ は、スイッチがサポートする最大数の各 VLAN で稼動し、それぞれがネットワーク経由のループフリー パスを保持するように保証します。

  PVST+ は、それが稼動する VLAN にレイヤ 2 ロードバランシングを提供します。ネットワーク上で VLAN を使用して異なる論理トポロジを作成し、すべてのリンクが使用されるが、どのリンクもオーバーサブスクライブされないように保証できます。VLAN 上の各 PVST+ インスタンスは、単一のルート スイッチを持ちます。このルート スイッチは、ネットワーク内の他のすべてのスイッチに VLAN に関連するスパニング ツリー情報を伝播します。各スイッチがネットワークに関する同じ情報を持つため、このプロセスによってネットワーク トポロジは確実に維持されます。

- Rapid PVST+：このスパニング ツリー モードは、IEEE 802.1W 標準に基づく高速コンバージェンスを使用する点を除けば、PVST+ と同じです。これは、Cisco ME スイッチ NNI のデフォルトのスパニング ツリー モードです。Rapid PVST+ は、PVST+ と互換性があります。高速コンバージェンスを実現するため、Rapid PVST+ はトポロジ変更を受け取るとすぐに、動的に学習した MAC アドレス エントリをポート単位で削除します。対照的に、PVST+ は、動的に学習した MAC アドレス エントリに対して短いエージング タイムを使用します。

  Rapid PVST+ は、PVST+ と同じ設定（上記の点を除き）を使用するため、スイッチには最低限の設定を追加するだけで済みます。Rapid PVST+ の利点は、複雑な MSTP 設定を習得する必要もネットワークを再プロビジョンする必要もなく、大規模な PVST+ インストール ベースを Rapid PVST+ へ移行できる点です。Rapid PVST+ モードでは、各 VLAN がサポートできる最大数の専用のスパニング ツリー インスタンスを稼動します。

- MSTP：このスパニング ツリー モードは、IEEE 802.1 標準 に基づいています。複数の VLAN を同じスパニング ツリー インスタンスに対応付け、多数の VLAN をサポートするために必要なスパニング ツリー インスタンス数を削減できます。MSTP は、（IEEE802.1 W に基づいて）RSTP の上で稼動します。これは、転送遅延をなくし、ルート ポートと指定ポートを迅速にフォワーディング ステートに移行することで、スパニング ツリーの高速コンバージェンスに対応します。RSTP を使用せずに MSTP を稼動できません。

  MSTP の最も一般的な初期配備は、レイヤ 2 スイッチド ネットワークのバックボーンとディストリビューション レイヤへの配置です。詳細については、第 16 章「MSTP の設定」を参照してください。

サポートされるスパニング ツリー インスタンス数の詳細については、次のセクションを参照してください。

スパニング ツリー インスタンスのサポート

PVST+ または Rapid PVST+ モードでは、スイッチは最大 128 のスパニング ツリー インスタンスをサポートします。

MSTP モードでは、スイッチは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数は制限されていません。

スパニング ツリーの相互運用性と下位互換性

表 15-2 に、ネットワーク内でサポートされるスパニング ツリー モード間の相互運用性と互換性を示します。

表 15-2　PVST+、MSTP、Rapid PVST+ の相互運用性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり（制限付き）	あり（PVST+ に戻る）
MSTP	あり（制限付き）	あり	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	あり

MSTP と PVST+ が混在するネットワークでは、Common Spanning-Tree（CST）ルートが MST バックボーンの内部に存在している必要があります。PVST+ スイッチは複数の MST リージョンには接続できません。

ネットワークに Rapid PVST+ を稼動するスイッチと PVST+ を稼動するスイッチが含まれる場合は、Rapid PVST+ スイッチと PVST+ スイッチを異なるスパニング ツリー インスタンスに設定することを推奨します。Rapid PVST+ スパニング ツリー インスタンスでは、ルート スイッチは Rapid PVST+ スイッチでなければなりません。PVST+ インスタンスでは、ルート スイッチは PVST+ スイッチでなければなりません。PVST+ スイッチは、ネットワークのエッジに配置されている必要があります。

STP および IEEE 802.1Q トランク

VLAN トランクの IEEE 802.1Q 規格では、ネットワークのスパニング ツリー方式にいくつかの制約を課します。この規格では、トランク上で許可されたすべての VLAN に対してスパニング ツリー インスタンスは 1 つだけです。ただし、IEEE 802.1Q トランクを使用して接続したシスコ製スイッチで構成されたネットワークでは、スイッチはトランク上で許可された VLAN ごとに 1 つのスパニング ツリー インスタンスを維持します。

IEEE 802.1Q トランクを使用してシスコ製スイッチを他社製のデバイスに接続すると、シスコ製スイッチは PVST+ を使用してスパニング ツリーの相互運用性を実現します。Rapid PVST+ がイネーブルの場合は、スイッチは PVST+ の代わりに Rapid PVST+ を使用します。これにより、トランクの IEEE 802.1Q VLAN のスパニング ツリー インスタンスが他社製の 802.1Q スイッチのスパニング ツリー インスタンスと結合されます。

ただし、すべての PVST+ または Rapid PVST+ 情報は、他社製の 802.1Q スイッチ クラウドにより分離されたシスコ製スイッチによって維持されます。シスコ製スイッチを分離する他社製の 802.1Q スイッチ クラウドは、スイッチ間の 1 つのトランク リンクとして取り扱われます。

PVST+ は IEEE 802.1Q トランクで自動的にイネーブルに設定され、ユーザによる設定は必要ありません。アクセス ポートの外部スパニング ツリー動作は、PVST+ に影響されません。

IEEE 802.1Q トランクの詳細については、第 12 章「VLAN の設定」を参照してください。

スパニング ツリー機能の設定

- 「スパニング ツリーのデフォルト設定」（P.15-12）
- 「スパニング ツリーの設定時の注意事項」（P.15-13）
- 「ENI 上のスパニング ツリーをイネーブルにする」（P.15-14）（必須）
- 「スパニング ツリーのディセーブル化」（P.15-16）（任意）
- 「ルート スイッチの設定」（P.15-16）（任意）
- 「セカンダリ ルート スイッチの設定」（P.15-18）（任意）
- 「ポート プライオリティの設定」（P.15-18）（任意）
- 「パス コストの設定」（P.15-20）（任意）
- 「VLAN のスイッチ プライオリティの設定」（P.15-21）（任意）
- 「スパニング ツリー タイマーの設定」（P.15-22）（任意）

スパニング ツリーのデフォルト設定

表 15-3 に、スパニング ツリーのデフォルト設定を示します。

表 15-3　スパニング ツリーのデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 の NNI でイネーブルに設定されています。 ENI 上ではディセーブルです （UNI 上ではサポートされていません）。 詳細については、「スパニング ツリー インスタンスのサポート」（P.15-11）を参照してください。
スパニング ツリー モード	Rapid PVST+ Rapid PVST+ は、PVST および PVST+ と相互運用します。MSTP はディセーブルに設定されています。
スイッチ プライオリティ	32768.
スパニング ツリー ポート プライオリティ（インターフェイス単位で設定可能）	128.
スパニング ツリー ポート コスト（インターフェイス単位で設定可能）	1000 Mbps：4 100 Mbps：19 10 Mbps：100
スパニング ツリー ポート プライオリティ（VLAN 単位で設定可能）	128.

表 15-3　スパニング ツリーのデフォルト設定 （続き）

機能	デフォルト設定
スパニング ツリー ポート コスト（VLAN 単位で設定可能）	1000 Mbps：4 100 Mbps：19 10 Mbps：100
スパニング ツリー タイマー	Hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒

スパニング ツリーの設定時の注意事項

スパニング ツリー インスタンスよりも多くの VLAN が定義されている場合、STP ポート上で PVST+ または Rapid PVST+ をイネーブルにできるのは、スイッチあたり 128 の VLAN に限られます。残りの VLAN は、スパニング ツリーをディセーブルにした状態で動作します。ただし、MSTP を使用して複数の VLAN を同じスパニング ツリーに対応付けることができます。詳細については、第 16 章「MSTP の設定」を参照してください。

128 のスパニング ツリー インスタンスがすでに使用されている場合は、VLAN のいずれかで STP ポート上のスパニング ツリーをディセーブルにしてから、実行したい VLAN 上でスパニング ツリーをイネーブルにできます。特定の VLAN のスパニング ツリーをディセーブルにするには、**no spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。特定の VLAN 上のスパニング ツリーをイネーブルにするには、**spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

注意　スパニング ツリーを実行していないスイッチは、VLAN 上のスパニング ツリー インスタンスを実行しているその他のスイッチがループを切断できるように、受信した BPDU を転送します。したがって、ネットワーク内のすべてのループを阻止できるだけの十分な数のスイッチ上でスパニング ツリーを実行する必要があります。たとえば、VLAN のループごとに少なくとも 1 台のスイッチ上でスパニング ツリーが実行されていなければなりません。VLAN 内のすべてのスイッチでスパニング ツリーを稼動する必要はまったくありません。ただし、最小限のスイッチでスパニング ツリーを稼動している場合は、軽率にネットワークを変更すると、VLAN 内に別のループを引き起こし、結果としてブロードキャスト ストームが発生する可能性があります。

スイッチ上で使用可能なすべてのスパニング ツリー インスタンスをすでに使用している場合、VLAN をさらに 1 つ追加すると、そのスイッチ上にスパニング ツリーを実行しない VLAN が作成されます。スイッチのトランク ポートにデフォルトの許可リストが設定されていると、すべてのトランク ポートに新しい VLAN が割り当てられます。ネットワークのトポロジによっては、新しい VLAN で、切断されないループが作成されることがあります。特に、複数の隣接スイッチでスパニング ツリー インスタンスをすべて使用してしまっている場合は、注意してください。このような事態を防ぐには、スパニング ツリー インスタンスの割り当てを使い切っているスイッチのトランク ポートに、許可リストを設定します。多くの場合、許可リストの設定は不要です。ただし、許可リストを設定すると、ネットワークに VLAN を追加するときに、より多くの作業が必要になります。

スパニング ツリー コマンドは、VLAN スパニング ツリー インスタンスのコンフィギュレーションを決定します。スパニング ツリー インスタンスは、VLAN に STP ポート（STP がイネーブルの NNI または ENI）を割り当てるときに作成します。最後のポートが他の VLAN に移動すると、スパニング ツリー インスタンスは削除されます。スパニング ツリー インスタンスを作成する前に、スイッチおよびポートのパラメータを設定できます。このパラメータは、スパニング ツリー インスタンスの作成時に適用されます。

スイッチは PVST+、Rapid PVST+、MSTP をサポートしますが、アクティブにできるバージョンは 1 度に 1 つだけです （たとえば、すべての VLAN が PVST+ を稼動する、すべての VLAN が Rapid PVST+ を稼動する、またはすべての VLAN が MSTP を稼動する）。各種スパニング ツリー モードとそれらが相互に動作する方法の詳細については、「スパニング ツリーの相互運用性と下位互換性」（P.15-11）を参照してください。

注意　ループ ガードが機能するのは、ポイントツーポイント リンク上だけです。リンクの両端に、STP を実行しているデバイスを直接接続することを推奨します。

ME-3400E スイッチでは、STP がイネーブルになっている NNI または ENI 上で 1-to-1 VLAN マッピングがイネーブルにされ、STP インスタンスがスイッチ内のサービス プロバイダー VLAN（S-VLAN）に適用されます。

ENI 上のスパニング ツリーをイネーブルにする

デフォルトでは、スパニング ツリーはスイッチ上のすべての NNI 上でイネーブルに、ENI 上ではディセーブルにされています。ENI のスパニング ツリーをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する UNI または ENI インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに設定されています。
ステップ 4	**port-type eni**	ポートを ENI として設定します（設定されていない場合）。
ステップ 5	**spanning-tree**	インターフェイスでスパニング ツリーをイネーブルにします。VLAN の NNI とともに、インターフェイスはスイッチ スパニング ツリー インスタンスに所属します。 **（注）**　このコマンドは、ENI 上だけで表示されます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show spanning-tree interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ENI 上でスパニング ツリーをディセーブルにするには、**no spanning-tree** インターフェイス コマンドを入力します。

スパニング ツリー モードの変更

スイッチは、PVST+、Rapid PVST+、MSTP の 3 つのスパニング ツリー モードをサポートしています。デフォルトでは、スイッチはスパニング ツリーがイネーブルに設定されているすべての NNI および ENI 上で Rapid PVST+ プロトコルを使用します。

スパニング ツリー モードを変更するには、特権 EXEC モードで次の手順を実行します。デフォルト モードとは異なるモードをイネーブルにする場合に、次の手順を実行する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}	スイッチの STP ポート でスパニング ツリー モードを設定します。 • PVST+ をイネーブルにするには、**pvst** を選択します。 • MSTP（および、RSTP）をイネーブルにするには、**mst** を選択します。設定手順の詳細については、第 16 章「MSTP の設定」を参照してください。 • rapid PVST+（デフォルト設定）をイネーブルにするには、**rapid-pvst** を選択します。
ステップ 3	**interface** *interface-id*	（Rapid PVST+ モードの場合だけ推奨）設定する STP ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、スパニング ツリーがイネーブルになった物理 NNI または ENI、VLAN、および NNI または ENI のポート チャネルがあります。VLAN ID の範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。 **（注）** 物理インターフェイスが UNI の場合、スパニング ツリー リンクとして設定する前に、**port-type nni** インターフェイス設定コマンドを入力するか、ポートを ENI として設定し、ポート上のスパニング ツリーをイネーブルにする必要があります。「ENI 上のスパニング ツリーをイネーブルにする」（P.15-14）を参照してください。 インターフェイスが VLAN である場合は、VLAN のスパニング ツリーがイネーブルに設定されているポートだけがスパニング ツリーを実行します。 インターフェイスがポート チャネルである場合は、ポート チャネルのすべてのメンバーは、スパニング ツリーがイネーブルに設定されている NNI または ENI である必要があります。
ステップ 4	**spanning-tree link-type point-to-point**	（Rapid PVST+ モードの場合だけ推奨）このポートのリンク タイプをポイントツーポイントに指定します。 このポートをポイントツーポイント リンク経由でリモート ポートに接続し、ローカル ポートが指定ポートになった場合は、スイッチはリモート ポートとネゴシエーションして、迅速にローカル ポートをフォワーディング ステートに変更します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**clear spanning-tree detected-protocols**	（Rapid PVST+ モードの場合だけ推奨）スイッチ上の任意のポートが IEEE 802.1D レガシー スイッチ上のポートに接続されている場合は、スパニング ツリーを実行するスイッチ全体のプロトコル移行プロセスを再起動します。 指定スイッチがこのスイッチで Rapid PVST+ が稼動中であると検出した場合は、この手順は任意です。
ステップ 7	**show spanning-tree summary** および **show spanning-tree interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no spanning-tree mode** グローバル コンフィギュレーション コマンドを使用します。ポートをデフォルトのスパニング ツリー モード設定に戻すには、**no spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用します。

スパニング ツリーのディセーブル化

スパニング ツリーは、デフォルトで VLAN 1 および新規に作成されたすべての VLAN のすべての NNI で、「スパニング ツリー インスタンスのサポート」（P.15-11）に示したスパニング ツリーの限度を上限としてイネーブルに設定されています。スパニング ツリーはスイッチ上の ENI ではディセーブルに設定されていますが、インターフェイス単位でイネーブルに設定できます。スパニング ツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

注意　スパニング ツリーがディセーブルで、かつ、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

VLAN 単位でスパニング ツリーをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no spanning-tree vlan** *vlan-id*	*vlan-id* では、指定できる範囲は 1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スパニング ツリーを再度イネーブルにするには、**spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

ルート スイッチの設定

スイッチは、設定されたアクティブ VLAN ごとに 1 つずつ、独立したスパニング ツリー インスタンスを維持します。各インスタンスには、スイッチ プライオリティとスイッチ MAC アドレスからなるブリッジ ID が対応付けられています。各 VLAN で、最小のブリッジ ID を持つスイッチが、その VLAN のルート スイッチになります。

あるスイッチが特定の VLAN のルートになるよう設定するには、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値（32768）から大幅に小さい値に変更します。このコマンドを入力すると、ソフトウェアは、各 VLAN についてルート スイッチのスイッチ プライオリティをチェックします。拡張システム ID のサポートのため、スイッチは、指定された VLAN 上の自身のプライオリティを 24576 に設定します（この値によって、このスイッチが指定された VLAN のルートになる場合）。

指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（表 15-1（P.15-4）に示すように、4096 は、4 ビット スイッチ プライオリティ値の最下位ビットの値です）。

（注）　ルート スイッチにするのに必要な値が 1 未満の場合は、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドは失敗します。

拡張システム ID をサポートしないスイッチとサポートするスイッチの両方がネットワークに混在している場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはありません。拡張システム ID は、旧ソフトウェア実装の接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値を増やします。

（注）　各スパニング ツリー インスタンスのルート スイッチは、バックボーンまたはディストリビューション スイッチでなければなりません。アクセス スイッチをスパニング ツリー プライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ数）を指定するには、キーワード **diameter** を指定します。ネットワークの直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、STP のコンバージェンスに要する時間が大幅に短縮されます。キーワード **hello** を使用すると、自動的に計算された hello タイムを上書きできます。

（注）　スイッチをルート スイッチとして設定したあとに、**spanning-tree vlan** *vlan-id* **hello-time**、**spanning-tree vlan** *vlan-id* **forward-time**、および **spanning-tree vlan** *vlan-id* **max-age** の各グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは、推奨されていません。

指定された VLAN のルートになるようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定された VLAN のルートになるようにスイッチを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。 • （任意）**hello-time** *seconds* には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree detail**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

セカンダリ ルート スイッチの設定

スイッチをセカンダリ ルートとして設定すると、スイッチ プライオリティはデフォルト値（32768）から 28672 に変更されます。その結果、プライマリ ルート スイッチに障害が発生した場合に、このスイッチが、指定された VLAN のルート スイッチになる可能性が高くなります。ネットワーク上の他のスイッチはデフォルトのスイッチ プライオリティである 32768 を使用していると想定されるので、他のスイッチがルート スイッチになる可能性は低くなります。

このコマンドを複数のスイッチに実行して、複数のバックアップ ルート スイッチを設定できます。**spanning-tree vlan** *vlan-id* **root primary** グローバル コンフィギュレーション コマンドを使用して、プライマリ ルート スイッチの設定時と同じネットワーク直径と hello タイム値を設定します。

指定された VLAN のセカンダリ ルートになるようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定された VLAN のセカンダリ ルートになるようにスイッチを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。 • （任意）**hello-time** *seconds* には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。 プライマリ ルート スイッチの設定時と同じネットワーク直径および hello タイム値を使用します。「ルート スイッチの設定」（P.15-16）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree detail**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

ポート プライオリティの設定

ループが発生すると、スパニング ツリーは、ポート プライオリティを使用して、フォワーディング ステートにするスパニング ツリー ポートを選択します。STP に最初に選択させたいポートには高いプライオリティ値（小さい数値）を、最後に選択させたいポートには低いプライオリティ値（大きい数値）

を割り当てることができます。すべてのスパニング ツリー ポートが同じプライオリティ値を持つ場合、スパニング ツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。

スパニング ツリー ポートのポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 **（注）** 物理インターフェイスが UNI の場合、スパニング ツリー リンクとして設定する前に、**port-type nni** インターフェイス設定コマンドを入力するか、ポートを ENI として設定し、ポート上のスパニング ツリーをイネーブルにする必要があります。「ENI 上のスパニング ツリーをイネーブルにする」（P.15-14）を参照してください。 インターフェイスが VLAN である場合は、VLAN のスパニング ツリーがイネーブルに設定されているポートだけがスパニング ツリーを実行します。インターフェイスがポート チャネルである場合は、ポート チャネルのすべてのメンバーは、スパニング ツリーがイネーブルに設定されている NNI または ENI である必要があります。
ステップ 3	**spanning-tree port-priority** *priority*	スパニング ツリー ポートのポート プライオリティを設定します。 *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増えます。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 4	**spanning-tree vlan** *vlan-id* **port-priority** *priority*	VLAN のポート プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増えます。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show spanning-tree interface** *interface-id* または **show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注）　**show spanning-tree interface** *interface-id* 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能の状態にある場合に限られます。そうでない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認してください。

デフォルトのスパニング ツリー設定に戻すには、**no spanning-tree** [**vlan** *vlan-id*] **port-priority** インターフェイス コンフィギュレーション コマンドを使用します。スパニング ツリーのポート プライオリティを使用してトランク ポートに負荷分散を設定する方法については、「トランク ポートの負荷分散の設定」（P.12-20）を参照してください。

パス コストの設定

スパニング ツリー パス コストのデフォルト値は、インターフェイスのメディア速度と連動します（スパニング ツリーを実行するポートまたはスパニング ツリーを実行する複数のポートのポート チャネル）。ループが発生すると、スパニング ツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。STP に最初に選択させたいインターフェイスには小さいコスト値を、最後に選択させたいインターフェイスには大きいコスト値を割り当てることができます。すべての NNI（またはポート チャネル）が同じコスト値を使用している場合、スパニング ツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。

インターフェイスのコストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、NNI および STP 対応 ENI だけで構成される物理 NNI または STP 対応 ENI およびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。
ステップ 3	**spanning-tree cost** *cost*	インターフェイスのコストを設定します。 ループが発生すると、スパニング ツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストの値が小さいほど、高速で転送されます。 *cost* に指定できる範囲は 1 ～ 200000000 です。デフォルト値は、インターフェイスのメディア速度によって決まります。

	コマンド	目的
ステップ 4	**spanning-tree vlan** *vlan-id* **cost** *cost*	VLAN のコストを設定します。 ループが発生すると、スパニング ツリーはパス コストを使用して、フォワーディング ステートにするスパニング ツリー ポートを選択します。パス コストの値が小さいほど、高速で転送されます。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *cost* に指定できる範囲は 1 ～ 200000000 です。デフォルト値は、インターフェイスのメディア速度によって決まります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show spanning-tree interface** *interface-id* または **show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注）　**show spanning-tree interface** *interface-id* 特権 EXEC コマンドで情報が表示されるのは、リンクアップ動作可能の状態にあるポートに限られます。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

デフォルト設定に戻すには、**no spanning-tree** [**vlan** *vlan-id*] **cost** インターフェイス コンフィギュレーション コマンドを使用します。スパニング ツリー パス コスト使用してトランク ポートに負荷分散を設定する方法については、「トランク ポートの負荷分散の設定」（P.12-20）を参照してください。

VLAN のスイッチ プライオリティの設定

スイッチ プライオリティを設定し、そのスイッチがルート スイッチとして選択される可能性を高めることができます。

（注）　このコマンドは慎重に使用してください。通常、スイッチ プライオリティの変更には、**spanning-tree vlan** *vlan-id* **root primary**、および **spanning-tree vlan** *vlan-id* **root secondary** の各グローバル コンフィギュレーション コマンドの使用を推奨します。

VLAN のスイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **priority** *priority*	VLAN のスイッチ プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* に指定できる範囲は 0 ～ 61440 で、4096 ずつ増えます。デフォルトは 32768 です。数値が小さいほど、スイッチがルート スイッチとして選択される可能性が高くなります。 有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。それ以外の値はすべて拒否されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

スパニング ツリー タイマーの設定

表 15-4 に、スパニング ツリー全体のパフォーマンスに影響を与えるタイマーを示します。

表 15-4　スパニング ツリー タイマー

変数	説明
hello タイマー	スイッチが他のスイッチに hello メッセージをブロードキャストする頻度を指定します。
転送遅延タイマー	STP ポートが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を制御します。
最大エージング タイマー	STP ポートで受信したプロトコル情報が、スイッチに保管される時間を制御します。

次の項で、設定手順について説明します。

hello タイムの設定

hello タイムを変更することによって、ルート スイッチによるコンフィギュレーション メッセージが生成される間隔を設定できます。

（注）　このコマンドは慎重に使用してください。通常、hello タイムの変更には、**spanning-tree vlan** *vlan-id* **root primary**、および **spanning-tree vlan** *vlan-id* **root secondary** の各グローバル コンフィギュレーション コマンドの使用を推奨します。

VLAN の hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **hello-time** *seconds*	VLAN の hello タイムを設定します。hello タイムは、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔です。このメッセージはスイッチが動作中であることを意味します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

VLAN の転送遅延時間の設定

VLAN の転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **forward-time** *seconds*	VLAN の転送時間を設定します。転送遅延は、スパニング ツリーのラーニングおよびリスニング ステートからフォワーディング ステートに移行するまでに、スパニング ツリー ポートが待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 4 ～ 30 秒です。デフォルトは 15 秒です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

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

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

VLAN の最大エージング タイムの設定

VLAN の最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree vlan** *vlan-id* **max-age** *seconds*	VLAN の最大エージング タイムを設定します。最大エージング タイムは、再構成を行うまでに、スイッチがスパニング ツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 6 ～ 40 秒です。デフォルトは 20 秒です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

スパニング ツリー ステータスの表示

スパニング ツリー ステータスを表示するには、表 15-5 に示す特権 EXEC コマンドの 1 つまたは複数を使用します。

表 15-5　スパニング ツリー ステータスの表示に使用するコマンド

コマンド	目的
show spanning-tree active	アクティブなスパニング ツリー インターフェイスだけに関するスパニング ツリー情報を表示します。
show spanning-tree detail	インターフェイス情報の詳細なサマリーを表示します。

表 15-5　スパニング ツリー ステータスの表示に使用するコマンド （続き）

コマンド	目的
show spanning-tree interface *interface-id*	特定のスパニング ツリー インターフェイスのスパニング ツリー情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーまたは STP ステート セクションのすべての行を表示します。

clear spanning-tree [**interface** *interface-id*] 特権 EXEC コマンドを使用して、スパニング ツリー カウンタをクリアできます。

show spanning-tree 特権 EXEC コマンドのキーワードについては、このリリースのコマンド リファレンスを参照してください。

CHAPTER 16

MSTP の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに IEEE 802.1s Multiple Spanning-Tree Protocol（MSTP）のシスコ実装を設定する方法について説明します。Cisco ME スイッチで、スイッチ上の User Network Interface（UNI; ユーザ ネットワーク インターフェイス）は STP に参加せず、起動されるとただちにトラフィックを転送します。STP は、デフォルトで Network Node Interface（NNI; ネットワーク ノード インターフェイス）上でイネーブルにされており、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）上でもイネーブルにできます。STP が ENI 上でイネーブルにされていない場合、インターフェイスにより常にトラフィックが転送されます。

（注） Multiple Spanning-Tree（MST）は、先行標準の実装です。IEEE 標準のドラフト版に基づいています。

MSTP を使用すると、複数の VLAN（仮想 LAN）が同じスパニング ツリー インスタンスに対応付けられ、これにより、多数の VLAN をサポートするために必要なスパニング ツリー インスタンス数を削減できます。MSTP は、データ トラフィック用の複数のフォワーディング パスに対応し、ロード バランシングをイネーブルにします。MSTP を使用すると、1 つのインスタンス（フォワーディング パス）で障害が発生しても他のインスタンス（フォワーディング パス）は影響を受けないので、ネットワークのフォールト トレランスが向上します。MSTP の最も一般的な初期配置は、レイヤ 2 スイッチド ネットワークのバックボーンとディストリビューション レイヤへの配置です。この配置により、サービス プロバイダー環境で必要とされる可用性の高いネットワークが提供されます。

スイッチが MST モードの場合、IEEE 802.1w に基づく Rapid Spanning-Tree Protocol（RSTP）は自動的にイネーブルになります。RSTP は、明示的なハンドシェイクによってスパニング ツリーの高速コンバージェンスを提供します。これによって、IEEE 802.1D 転送遅延をなくし、ルート ポートと指定ポートを迅速にフォワーディング ステートへ移行します。

MSTP と RSTP はどちらも、スパニング ツリーのオペレーションを改善し、（オリジナルの）802.1D スパニング ツリー、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存の Cisco Per-VLAN Spanning-Tree Plus（PVST+）と Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）に基づく装置との下位互換性を維持します。PVST+ および Rapid PVST+ の詳細については、第 15 章「STP の設定」を参照してください。また、PortFast、UplinkFast、ルート ガードなどのその他のスパニング ツリー機能の詳細については、第 17 章「オプションのスパニング ツリー機能の設定方法」を参照してください。

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

- 「MSTP の概要」（P.16-2）
- 「RSTP の概要」（P.16-9）

- 「MSTP 機能の設定」（P.16-14）
- 「MST コンフィギュレーションおよびステータスの表示」（P.16-29）

MSTP の概要

MSTP は、高速コンバージェンスが可能な RSTP を使用し、複数の VLAN を 1 つのスパニング ツリー インスタンスにまとめます。各インスタンスのスパニング ツリー トポロジは、他のスパニング ツリー インスタンスの影響を受けません。このアーキテクチャによって、データ トラフィックに複数のフォワーディング パスが提供され、ロードバランシングが可能になり、また多数の VLAN をサポートするのに必要なスパニング ツリー インスタンスの数を減らすことができます。

- 「MST リージョン」（P.16-2）
- 「IST、CIST、および CST」（P.16-3）
- 「ホップ カウント」（P.16-6）
- 「境界ポート」（P.16-6）
- 「IEEE 802.1s の実装」（P.16-7）
- 「IEEE 802.1D STP との相互運用性」（P.16-9）

設定の詳細については、「MSTP 機能の設定」（P.16-14）を参照してください。

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定します。同じ MST コンフィギュレーションを持ち、相互接続されたスイッチの集合を MST リージョンといいます（図 16-1（P.16-4）を参照）。

各スイッチがどの MST リージョンに属しているかは、MST コンフィギュレーションによって決まります。MST コンフィギュレーションには、リージョン名、リビジョン番号、MST VLAN とインスタンスの割り当てマップが保存されています。スイッチにリージョンを設定するには、そのスイッチで **spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用して、MST コンフィギュレーション モードを開始します。このモードでは、**instance** MST コンフィギュレーション コマンドを使用して VLAN を MST インスタンスにマッピングし、**name** MST コンフィギュレーション コマンドでリージョン名を指定し、**revisions** MST コンフィギュレーション コマンドでリージョン番号を設定できます。

リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは RSTP Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニング ツリー インスタンスの数は最大 65 です。1 つの VLAN を同時に複数のスパニング ツリー インスタンスに割り当てることはできません。

IST、CIST、および CST

すべてのスパニング ツリー インスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 種類のスパニング ツリーを確立し、維持します。

- Internal Spanning-Tree（IST）は、1 つの MST リージョン内で稼動するスパニング ツリーです。

  各 MST リージョン内の MSTP は複数のスパニング ツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊インスタンスで、IST と呼ばれています。その他の MST インスタンスはすべて 1 ～ 4094 まで番号が付けられます。

  IST は、BPDU を送受信する唯一のスパニング ツリー インスタンスです。その他のスパニング ツリー インスタンス情報はすべて、MSTP BPDU 内でカプセル化される M レコードに格納されます。MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニング ツリー インスタンスをサポートするためにスイッチによる処理が必要な BPDU 数は大幅に減少します。

  同一リージョン内の MST インスタンスはすべて、同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ（ルート スイッチ ID、ルート パス コストなど）を持っています。デフォルトでは、すべての VLAN が IST に割り当てられています。

  MST インスタンスはリージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されていても、リージョン A の MST インスタンス 1 は、リージョン B の MST インスタンス 1 から独立しています。

- Common and Internal Spanning-Tree（CIST）は、各 MST リージョン内の IST の集合です。Common Spanning-Tree（CST）は MST リージョンとシングル スパニング ツリーを相互接続します。

  1 つのリージョン内で計算されたスパニング ツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w プロトコル、IEEE 802.1s プロトコル、および IEEE 802.1D プロトコルをサポートするスイッチ間で実行されるスパニング ツリー アルゴリズムによって形成されます。MST リージョン内の CIST は、リージョン外の CST と同じです。

詳細については、「MST リージョン内の動作」（P.16-3）および「MST リージョン間の動作」（P.16-4）を参照してください。

（注）　IEEE 802.1s 標準を実装すると、MST 実装に関連する一部の用語が変わります。この変更内容の概要については、表 16-1（P.16-5）を参照してください。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは IST マスターになります（図 16-1（P.16-4）を参照）。これは、リージョン内に存在して、最小のブリッジ ID および CST ルートへのパス コストが設定されたスイッチです。また、ネットワーク内にリージョンが 1 つしかない場合は、IST マスターも CST ルートになります。CST ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP スイッチの 1 つが IST マスターとして選択されます。

MSTP スイッチは初期化時に、自身が CST のルートおよび IST マスターであると宣言するため、CST ルートと IST マスターへのパス コストがいずれもゼロに設定された BPDU を送信します。スイッチはさらに MST インスタンスをすべて初期化し、自身がこれらすべてのインスタンスのルートであると宣言します。スイッチは、ポートに現在保存されているルート情報よりも優位のルート情報（小さいブリッジ ID、パス コストなど）を受信すると、IST マスターではなくなります。

初期化時は、リージョンに、それぞれが 独自の IST マスターを備えたサブリージョンが多数含まれる場合があります。スイッチは、優位の IST 情報を受信すると、古いサブリージョンから脱退して、真の IST マスターを含む可能性がある新しいサブリージョンに加入します。このようにして、真の IST マスターが含まれているサブリージョン以外のサブリージョンはすべて縮小します。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ IST マスターを承認する必要があります。したがって、そのリージョン内にある任意の 2 つのスイッチが、1 つの MST インスタンスに対するポートの役割を同期させるのは、共通の IST マスターに収束する場合だけです。

MST リージョン間の動作

ネットワーク内に複数のリージョンまたは IEEE 802.1D 準拠のレガシー スイッチが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP スイッチからなる CST を構築し、維持します。MST インスタンスは、リージョンの境界で IST と結合して CST になります。

IST は、リージョン内のすべての MSTP スイッチを接続し、CST のサブツリーとなります。CST は、スイッチド ドメイン全体を網羅し、サブツリーのルートが IST マスターとなります。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

図 16-1 は、3 つの MST リージョンと IEEE 802.1D 準拠のレガシー スイッチ（D）からなるネットワークを示しています。リージョン 1（A）の IST マスターは、CST ルートでもあります。リージョン 2（B）およびリージョン 3（C）の IST マスターは、CST 内にあるそれぞれのサブツリーのルートです。RSTP はすべてのリージョンで稼動しています。

図 16-1　MST リージョン、IST マスター、および CST ルート

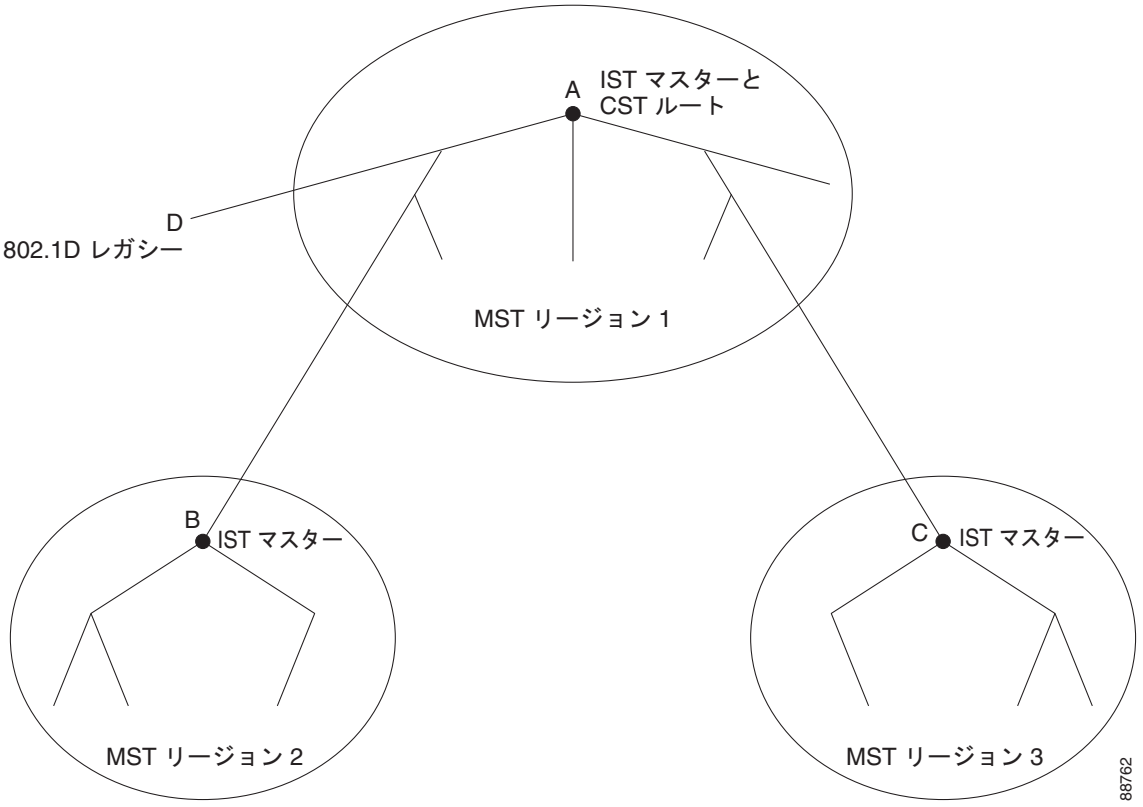


図 16-1 では、各リージョンのその他の MST インスタンスを示していません。MST インスタンスのトポロジは、同じリージョンの IST のトポロジとは異なる場合があることに注意してください。

BPDU を送受信するのは、CST インスタンスだけです。MST インスタンスは自身のスパニング ツリー情報を BPDU に追加して、近接スイッチと通信し、最終的なスパニング ツリー トポロジを計算します。したがって、BPDU 伝送に関連するスパニング ツリー パラメータ（hello タイム、転送時間、最大エージング タイム、最大ホップ数など）は、CST インスタンスでだけ設定されますが、その影響はすべての MST インスタンスに及びます。スパニング ツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または 802.1D STP BPDU を使用して、IEEE 802.1D 準拠のレガシー スイッチと通信します。MSTP スイッチ同士の通信には、MSTP BPDU が使用されます。

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の*内部*パラメータまたは*リージョン*パラメータを識別するように変更されました。このパラメータは、ネットワーク全体に関連する外部パラメータとは異なり、MST リージョン内だけで有効です。CIST はネットワーク全体にまたがる唯一のスパニング ツリー インスタンスなので、CIST パラメータでは、内部修飾子やリージョンの修飾子ではなく、外部修飾子が必要です。

- CIST ルートは、ネットワーク全体、つまり CIST にまたがる一意のインスタンスのルート スイッチです。
- CIST 外部ルート パス コストとは、CIST ルートのコストです。このコストは、MST リージョン内では変化しません。MST リージョンが CIST にとって単一のスイッチに見えることに注意してください。CIST 外部ルート パス コストは、このような仮想スイッチ、およびリージョンに属さないスイッチの間で計算されるルート パス コストです。
- CIST リージョナル ルートは、先行標準実装では IST マスターと呼ばれていました。CIST ルートがリージョン内にある場合は、CIST リージョナル ルートが CIST ルートになります。それ以外の場合は、リージョン内で CIST ルートに最も近いスイッチが CIST リージョナル ルートになります。CIST リージョナル ルートは、IST のルート スイッチとして動作します。
- CIST 内部ルート パス コストは、リージョン内の CIST リージョナル ルートのコストです。このコストは、IST（インスタンス 0）だけに関連します。

表 16-1 では、IEEE 標準およびシスコ先行標準の用語を比較します。

表 16-1　先行標準と標準の用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

ホップ カウント

IST と MST のインスタンスは、スパニング ツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。その代わり、ルートへのパス コスト、および IP Time to Live（TTL）メカニズムに似たホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST インスタンスに適用できます。ホップ カウントを設定すると、メッセージ エージ情報を設定するのと同様の結果が得られます（再構成の開始）。インスタンスのルート スイッチは、常にコストを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。この BPDU を受信したスイッチは、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準実装の場合、MST リージョンは境界ポートによって、RSTP を稼動するシングル スパニング ツリー リージョン、PVST+ または Rapid PVST+ を稼動するシングル スパニング ツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに接続されます。また境界ポートは LAN に接続されます。LAN の指定スイッチは、単一のスパニング ツリー スイッチまたは異なる MST コンフィギュレーションを持つスイッチのいずれかです。

（注）　Cisco ME スイッチでは、NNI または STP がイネーブルになった ENI だけが MST ポートとして指定できます。UNI は STP に参加しません。

IEEE 802.1s 標準には、境界ポートの定義がありません。IEEE 802.1Q-2002 標準では、ポートで受信可能な内部（同一リージョンからの）および外部の 2 種類のメッセージを識別します。メッセージが外部である場合は、CIST だけが受信します。CIST の役割がルートまたは代替ルートである場合、または外部 BPDU がトポロジ変更である場合、MST インスタンスに影響が及ぶことがあります。メッセージが内部である場合は、CIST が CIST 部分を受信し、それぞれの MST インスタンスがそれぞれの M レコードを受信します。シスコの先行標準実装では、外部メッセージを受信するポートが境界ポートとして扱われます。そのため、ポートが内部メッセージと外部メッセージの両方を受信することはありません。

MST リージョンには、スイッチと LAN の両方が含まれます。セグメントは、指定ポートのリージョンに属します。このため、セグメントの指定ポートと異なるリージョンのポートは境界ポートとなります。この定義では、リージョン内部の 2 つのポートが、異なるリージョンに属するポートとセグメントを共有し、内部メッセージと外部メッセージの両方をポートで受信できる可能性があります。

シスコの先行標準実装からの主な変更点は、指定ポートが、STP 互換モードで動作していないかぎり、境界ポートとして定義されないことです。

（注）　STP レガシー スイッチがセグメントに存在する場合、メッセージは常に外部と見なされます。

先行標準実装からのその他の変更として、RSTP またはレガシー IEEE 802.1Q スイッチに送信者スイッチ ID が含まれる場所へ CIST リージョナル ルート スイッチ ID フィールドが挿入されることが挙げられます。リージョン全体は、一貫した送信者スイッチ ID を近接スイッチに送信し、1 つの仮想スイッチのように動作します。図 16-1 の例では、A または B がセグメント用に指定されているかどうかに関係なく、スイッチ C はルートの送信者スイッチ ID が同一である BPDU を受信します。

IEEE 802.1s の実装

IEEE MST 標準のシスコ実装には、標準を満たすために必要な機能、および公表されている標準にまだ組み込まれていない先行標準の望ましい機能の一部が含まれます。

ポート役割命名の変更

境界という役割は最終 MST 標準には存在しませんが、その概念はシスコの実装で維持されています。ただし、リージョンの境界の MST インスタンス ポートは、対応する CIST ポートの状態に従わないことがあります。現在は次の 2 つのケースがあります。

- 境界ポートが CIST リージョナル ルートのルート ポートである場合：CIST インスタンス ポートが提案されて同期が取られている場合、対応するすべての MSTI ポートで同期化が行われ（フォワーディング ステートになっている）たときに限り、合意を返送してフォワーディング ステートに移行できます。MSTI ポートには、特別な *マスター*の役割が含まれます。
- 境界ポートが CIST リージョナル ルートのルート ポートでない場合：MSTI ポートは CIST ポートの状態と役割に従います。標準で提供される情報は少ないため、BPDU（M レコード）を受信しなくても MSTI ポートを交互にブロックできる理由を理解するのが困難な場合があります。このケースの場合、境界の役割は存在しませんが、**show** コマンドの出力の *type* 列ではポートが境界として識別されます。

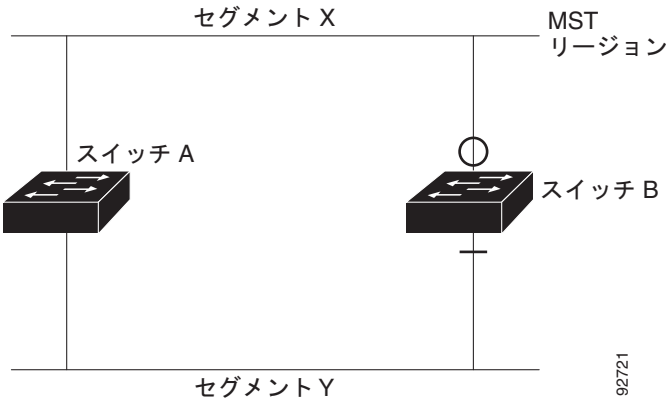
レガシー スイッチと標準スイッチ間の相互運用

先行標準スイッチの自動検出はエラーになることがありますが、インターフェイス コンフィギュレーション コマンドを使用すると、先行標準ポートを識別することができます。標準スイッチと先行標準スイッチの間ではリージョンを形成できませんが、CIST を使用する前に標準スイッチと先行標準スイッチを相互運用できます。この特定のケースでは、さまざまなインスタンスにおけるロード バランス機能だけが失われます。ポートが先行標準 BPDU を受信すると、CLI ではポート設定によってさまざまなフラグが表示されます。先行標準 BPDU 伝送用に設定されていないポートでスイッチが先行標準 BPDU を初めて受信したときには、syslog メッセージも表示されます。

図 16-2 ではこのシナリオの内容を図で表しています。A が標準スイッチ、B が先行標準スイッチであり、両方が同一リージョン内で設定されているとします。A が CIST のルート スイッチであり、B はセグメント X にルート ポート（BX）およびセグメント Y に代替ポート（BY）を含んでいます。セグメント Y がフラップし、BY のポートが 1 つの先行標準 BPDU の送信前に代替ポートになる場合、先行

標準スイッチが Y に接続されていることを AY は検出できず、標準 BPDU を送信し続けます。ポート BY はこのため境界に固定され、A と B の間ではロード バランスが不可能になります。同じ問題はセグメント X に存在しますが、B はトポロジ変更を転送することがあります。

図 16-2　　標準と先行標準スイッチの相互運用



（注） 標準と先行標準の MST 実装の間では、相互運用を最低限に抑えてください。

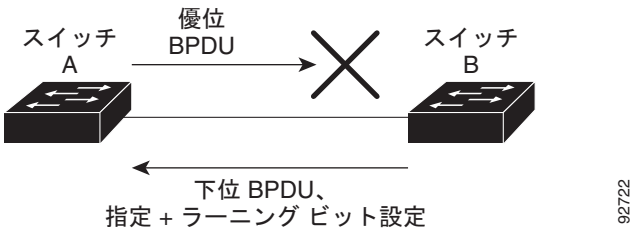
単一方向リンク障害の検出

IEEE MST 標準にはこの機能はありませんが、この Cisco IOS リリースには組み込まれています。ソフトウェアでは、受信 BPDU のポートの役割と状態が一貫しているかどうかがチェックされ、ブリッジング ループの原因となり得る単一方向リンク障害が検出されます。

指定ポートが矛盾を検出すると、その役割は維持されますが、接続に矛盾が生じた場合、ブリッジング ループを開始するよりも、接続を中断した方が好ましいので、廃棄ステートに戻します。

図 16-3 は、ブリッジング ループの原因となりやすい、単一方向リンク障害を表しています。スイッチ A はルート スイッチであり、その BPDU はスイッチ B へのリンクで失われました。RSTP と MST BPDU には、送信ポートの役割と状態が含まれています。スイッチ A はこの情報を使用して、送信した優位 BPDU にスイッチ B が反応しないこと、およびスイッチ B がルート スイッチではなく、指定スイッチであることを検出できます。その結果、スイッチ A はポートをブロックするので（またはブロックし続けるので）、ブリッジング ループが回避されます。

図 16-3　　単一方向リンク障害の検出



IEEE 802.1D STP との相互運用性

MSTP を稼動しているスイッチは、IEEE 802.1D レガシー スイッチとの相互運用を可能にする内蔵プロトコル移行メカニズムをサポートします。このスイッチは、IEEE 802.1D 準拠のレガシー コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信すると、そのポートでは IEEE 802.1D BPDU だけを送信します。また、MSTP スイッチは、レガシー BPDU、異なるリージョンに関連付けられている MST BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、スイッチは、IEEE 802.1D BPDU を受信しなくなっても、MSTP モードに自動的に戻ることはありません。レガシー スイッチが指定スイッチでないかぎり、レガシー スイッチがリンクから除去されたかどうかを検出できないからです。さらにスイッチは、接続先スイッチがリージョンに加入した場合に、引き続きポートに境界の役割を指定する可能性があります。プロトコル移行プロセスを再起動する（近接スイッチとの再ネゴシエーションを強制する）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー スイッチが RSTP スイッチであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP スイッチは、バージョン 0 コンフィギュレーションと Topology Change Notification（TCN; トポロジ変更通知）BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境界ポートは、指定スイッチが単一のスパニング ツリー スイッチ、または異なる MST コンフィギュレーションを持つスイッチである LAN に接続されます。

RSTP の概要

RSTP は、ポイントツーポイントの配線を利用して、スパニング ツリーの高速コンバージェンスを実現します。スパニング ツリーは 1 秒足らずで再構成されます（IEEE 802.1D スパニング ツリーのデフォルト設定では 50 秒かかります）。このことは、音声およびビデオなど遅延に影響されやすいトラフィックを転送するネットワークには重大です。

- 「ポートの役割およびアクティブ トポロジ」（P.16-9）
- 「高速コンバージェンス」（P.16-10）
- 「ポートの役割の同期化」（P.16-12）
- 「BPDU のフォーマットおよびプロセス」（P.16-12）

設定の詳細については、「MSTP 機能の設定」（P.16-14）を参照してください。

ポートの役割およびアクティブ トポロジ

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。「スパニング ツリー トポロジと BPDU」（P.15-3）で説明したように、RSTP は、IEEE 802.1D STP を構築して、最高のスイッチ プライオリティを持つ（プライオリティが最も小さい）スイッチをルート スイッチに選択します。RSTP はさらに、各ポートに次のいずれか 1 つの役割を割り当てます。

（注）　Cisco ME スイッチでは、NNI または STP がイネーブルになった ENI だけが RSTP ポートとして指定できます。UNI は STP に参加しません。

- ルート ポート：スイッチからルート スイッチにパケットを転送するのに最適なパス（最も低コストのパス）となります。

- 指定ポート：指定スイッチに接続します。これにより、LAN からルート スイッチにパケットを転送するときのパス コストが最小になります。指定スイッチと LAN の接続に使用されるポートを指定ポートと呼びます。
- 代替ポート：現在のルート ポートが提供したパスに替わるルート スイッチへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニング ツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンクによってループバックで同時接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合です。
- ディセーブル ポート：スパニング ツリーの動作において何も役割が与えられていません。

ルート ポートまたは指定ポートの役割を割り当てられたポートは、アクティブ トポロジの一部となります。代替ポートまたはバックアップ ポートの役割を割り当てられたポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルート ポートおよび指定ポートが即座にフォワーディング ステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート（802.1D のブロッキング ステートと同じ）になるように保証します。フォワーディング プロセスおよびラーニング プロセスの動作はポート ステートによって制御されます。表 16-2 に、IEEE 802.1D と RSTP のポート ステートの比較を示します。

表 16-2　ポート ステートの比較

動作ステータス	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートはアクティブ トポロジに含まれているか
イネーブル	ブロッキング	廃棄	含まれていない
イネーブル	リスニング	廃棄	含まれていない
イネーブル	ラーニング	ラーニング	含まれている
イネーブル	フォワーディング	フォワーディング	含まれている
ディセーブル	ディセーブル	廃棄	含まれていない

シスコの STP 実装製品で整合性を図るため、このマニュアルでは、ポートの*廃棄*ステートを*ブロッキング*と定義します。指定ポートは、リスニング ステートから開始します。

高速コンバージェンス

RSTP を使用すると、スイッチ、スイッチ ポート、または LAN に障害が発生しても、ただちに接続を回復できます。RSTP は、エッジ ポート、新しいルート ポート、およびポイントツーポイント リンクで接続されているポートに次のように高速コンバージェンスを提供します。

- エッジ ポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して、RSTP スイッチ上の 1 つのポートをエッジ ポートに設定すると、そのエッジ ポートは即座にフォワーディング ステートになります。エッジ ポートは PortFast イネーブル設定ポートと同じで、これをイネーブルにできるのは、単一のエンド ステーションに接続されているポート上だけです。
- ルート ポート：RSTP は、新しいルート ポートを選択すると、古いルート ポートをブロックして、新しいルート ポートをただちにフォワーディング ステートにします。
- ポイントツーポイント リンク：2 つのポートをポイントツーポイント リンクで接続し、ローカル ポートが指定ポートになると、その指定ポートは、提案合意ハンドシェイクを使用して、相手側ポートと高速移行をネゴシエーションし、ループのないトポロジを保証します。

（注）　Cisco ME スイッチでは、これらのポートは常に NNI または STP がイネーブルになった ENI となります。

図 16-4 では、スイッチ A とスイッチ B はポイントツーポイント リンクを通じて接続され、すべてのポートがブロッキング ステートになっています。スイッチ A のプライオリティ値がスイッチ B のプライオリティ値より小さい数値であるとします。この場合、スイッチ A はスイッチ B に提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）を送信し、スイッチ A 自身が指定スイッチになることを提案します。

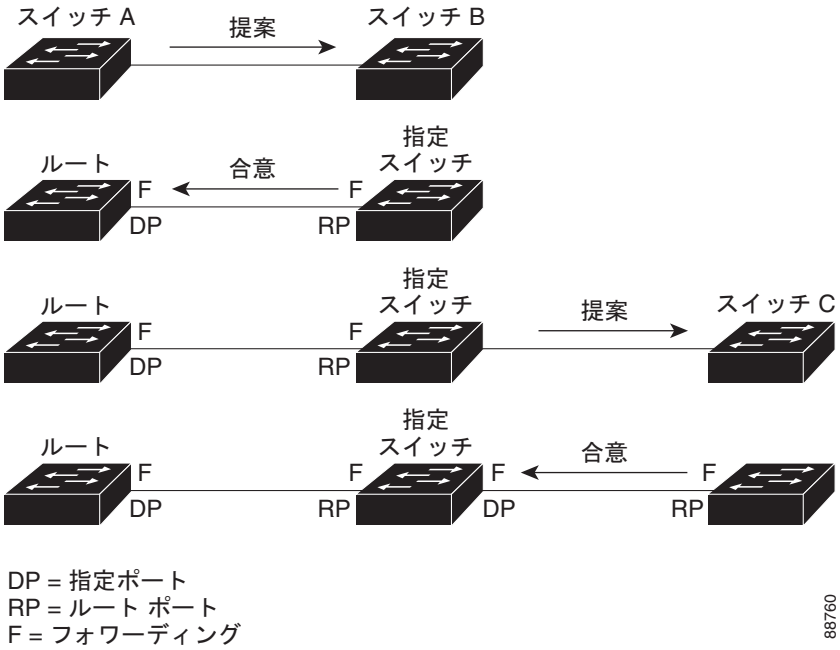
スイッチ B は、提案メッセージを受信すると、提案メッセージの受信ポートを新しいルート ポートに選択し、すべての非エッジ ポートをブロッキング ステートにします。さらに、新しいルート ポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

スイッチ A は、スイッチ B の合意メッセージを受信すると、ただちに自身の指定ポートをフォワーディング ステートにします。スイッチ B はその非エッジ ポートをすべてブロックし、またスイッチ A とスイッチ B はポイントツーポイント リンクで接続されているので、ネットワークにループは形成されません。

スイッチ C がスイッチ B に接続された場合も、同様のハンドシェイク メッセージが交換されます。スイッチ C はスイッチ B に接続されたポートをルート ポートとして選択し、両端のポートはただちにフォワーディング ステートに移行します。アクティブ トポロジにスイッチが追加されるたびに、このハンドシェイク プロセスが実行されます。ネットワークが収束すると、この提案合意ハンドシェイクがルートからスパニング ツリーのリーフへと進みます。

スイッチはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重ポートは共有接続と見なされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定で判断されたデフォルトの設定値を上書きできます。

図 16-4　高速コンバージェンスの提案/合意ハンドシェイク



ポートの役割の同期化

スイッチのポートの 1 つで提案メッセージが受信され、そのポートが新しいルート ポートに選択されると、RSTP は他のすべてのポートを新しいルートの情報に同期させます。

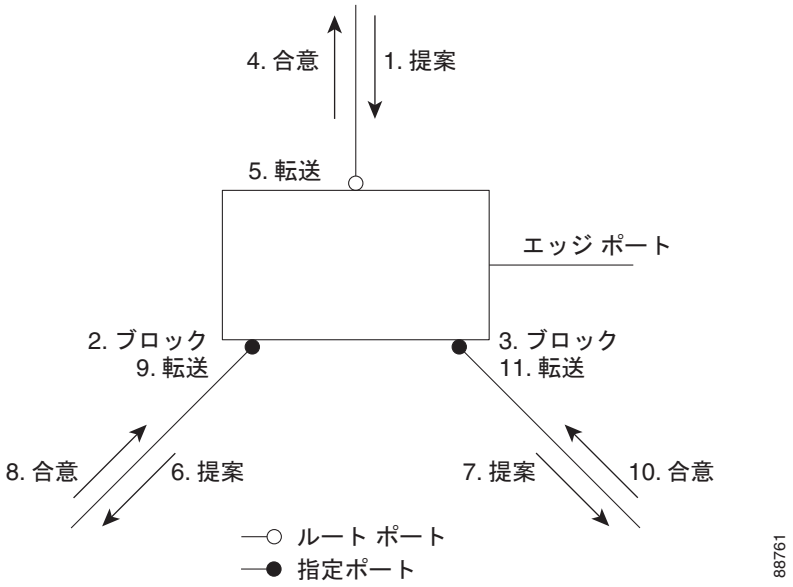
他のすべてのポートが同期化されている場合、スイッチはルート ポートで受信した上位のルート情報に同期化されます。スイッチ上の個々のポートは次の場合に同期化されます。

- ブロッキング ステートである場合
- エッジ ポートである場合（ネットワークのエッジとして設定されているポート）

指定 STP ポートがフォワーディング ステートであり、かつエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報で強制的に同期化されると、その指定ポートはブロッキング ステートになります。一般的に、RSTP がポートを新しいルート情報で強制的に同期化し、そのポートが上記のいずれの条件も満たしていない場合、ポートのステートはブロッキングに設定されます。

スイッチは、すべてのポートが同期化されたことを確認すると、そのルート ポートに対応する指定スイッチに合意メッセージを送信します。ポイントツーポイント リンクで接続されたスイッチがポートの役割について互いに合意すると、RSTP はポート ステートをただちにフォワーディング ステートに移行させます。図 16-5 は、この一連のイベントを示します。

図 16-5　高速コンバージェンス中のイベント シーケンス



BPDU のフォーマットおよびプロセス

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。表 16-3 に、RSTP のフラグ フィールドを示します。

表 16-3　RSTP BPDU フラグ

ビット	機能
0	トポロジの変更（TC）
1	提案
2–3:	ポートの役割
00	不明
01	代替ポート
10	ルート ポート
11	指定ポート
4	ラーニング
5	フォワーディング
6	合意
7	トポロジの変更の確認（TCA）

送信スイッチは、自身を LAN 上の指定スイッチにするために、RSTP BPDU に提案フラグを設定します。提案メッセージでは、ポートの役割は常に指定ポートに設定されます。

送信スイッチは、提案を受け入れる場合、RSTP BPDU に合意フラグを設定します。合意メッセージでは、ポートの役割は常にルート ポートに設定されます。

RSTP には個別の TCN BPDU はありません。トポロジの変更を示すには、トポロジ変更（TC）フラグが使用されます。ただし、802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニングとフォワーディングのフラグは、送信ポートのステートに応じて設定されます。

優位 BPDU 情報の処理

現在保存されているルート情報よりも優位のルート情報（小さいブリッジ ID、低パス コストなど）をポートが受信すると、RSTP は再構成を開始します。そのポートが新しいルート ポートとして提案され、選択されると、RSTP は他のすべてのポートを強制的に同期化します。

受信した BPDU が提案フラグの設定された RSTP BPDU である場合、スイッチは他のすべてのポートを同期化したあと、合意メッセージを送信します。BPDU が 802.1D BPDU である場合、スイッチは提案フラグを設定せずに、そのポートの転送遅延タイマーを開始します。新しいルート ポートはフォワーディング ステートに移行するのに 2 倍の転送遅延時間を必要とします。

ポートで上位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる場合、RSTP はそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。指定ポートは、転送遅延タイマーが満了するまで提案フラグの設定された BPDU の送信を続けます。タイマーが満了すると、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

指定ポートの役割フラグが設定された下位の BPDU（そのポートに現在保存されている値より大きいブリッジ ID、高いパス コストなど）を指定ポートが受信した場合、その指定ポートは、ただちに現在の自身の情報を応答します。

トポロジの変更

ここでは、スパニング ツリー トポロジの変更処理について、RSTP と IEEE 802.1D の違いを説明します。

- 検出：IEEE 802.1D はブロッキングとフォワーディングの間でステートの移行があると、*必ず*トポロジの変更が生じますが、RSTP ではトポロジの変更が生じるのは、ブロッキングからフォワーディングにステートが移行する場合*だけ*です（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジ ポートでステートが変更されても、トポロジの変更は生じません。RSTP スイッチは、トポロジの変更を検出すると、TC 通知の送信元ポートを除き、すべての非エッジ ポート上の学習済みの情報をフラッシュします。
- 通知：IEEE 802.1D は、TCN BPDU を使用しますが、RSTP は使用しません。ただし、802.1D との相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。
- 確認：RSTP スイッチは、指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信した場合、TCA ビットが設定された 802.1D コンフィギュレーション BPDU で応答します。ただし、802.1D スイッチに接続されたルート ポートで TC 時間タイマー（802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

  この処理は、IEEE 802.1D スイッチをサポートする目的でだけ必要とされます。RSTP BPDU では、TCA ビットは設定されません。
- 伝播：RSTP スイッチは、指定ポートまたはルート ポートを介して別のスイッチから TC メッセージを受信すると、自身のすべての非エッジ ポート、指定ポート、およびルート ポート（受信ポートを除く）にトポロジの変更を伝播します。スイッチは、これらの全ポートの TC 時間タイマーを開始し、これらのポート上で学習した情報をフラッシュします。
- プロトコルの移行：IEEE 802.1D スイッチとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で選択的に送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU を送信する最小時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコル タイプは無視します。

  スイッチはポートの移行遅延タイマーが満了したあとに IEEE 802.1D BPDU を受信した場合、IEEE 802.1D スイッチに接続されていると想定し、IEEE 802.1D BPDU だけの使用を開始します。ただし、RSTP スイッチが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了したあとに RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

MSTP 機能の設定

- 「MSTP のデフォルト設定」（P.16-15）
- 「MSTP 設定時の注意事項」（P.16-15）
- 「MST リージョンの設定の指定および MSTP のイネーブル設定」（P.16-16）（必須）
- 「ルート スイッチの設定」（P.16-18）（任意）
- 「セカンダリ ルート スイッチの設定」（P.16-19）（任意）
- 「ポート プライオリティの設定」（P.16-20）（任意）
- 「パス コストの設定」（P.16-22）（任意）
- 「スイッチ プライオリティの設定」（P.16-23）（任意）
- 「hello タイムの設定」（P.16-24）（任意）

- 「転送遅延時間の設定」（P.16-24）（任意）
- 「最大エージング タイムの設定」（P.16-25）（任意）
- 「最大ホップ カウントの設定」（P.16-25）（任意）
- 「リンク タイプの指定による高速移行の保証」（P.16-26）（任意）
- 「ネイバ タイプの指定」（P.16-27）（任意）
- 「プロトコル移行プロセスの再起動」（P.16-28）（任意）

MSTP のデフォルト設定

表 16-4 に、MSTP のデフォルト設定を示します。

表 16-4　MSTP のデフォルト設定

機能	デフォルト設定
スパニング ツリー モード	Rapid PVST+（PVST+ と MSTP はディセーブル）
スイッチ プライオリティ（CIST ポート単位で設定可能）	32768.
スパニング ツリー ポート プライオリティ（CIST ポート単位で設定可能）	128.
スパニング ツリー ポート コスト（CIST ポート単位で設定可能）	1000 Mbps：4 100 Mbps：19 10 Mbps：100
hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

サポートされるスパニング ツリー インスタンス数の詳細については、「スパニング ツリー インスタンスのサポート」（P.15-11）を参照してください。

MSTP 設定時の注意事項

- Cisco ME スイッチでは、MSTP は STP がイネーブルにされた NNI または ENI でだけ稼動します。**spanning-tree** インターフェイス コンフィギュレーションコマンドを入力して、ENI で STP をイネーブルにできます。UNI は、MSTP に参加しません。
- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- 2 つ以上のスイッチを同じ MST リージョンに設置するには、その 2 つのスイッチに同じ VLAN/インスタンス マップ、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- スイッチは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数は制限されていません。

- PVST+、Rapid PVST+、MSTP がサポートされますが、アクティブにできるバージョンは一度に 1 つだけです （たとえば、すべての VLAN が PVST+ を稼動する、すべての VLAN が Rapid PVST+ を稼動する、またはすべての VLAN が MSTP を稼動する）。詳細については、「スパニング ツリーの相互運用性と下位互換性」（P.15-11）を参照してください。推奨するトランク ポート設定の詳細については、「他の機能との相互作用」（P.12-17）を参照してください。
- CLI（コマンドライン インターフェイス）または SNMP サポートを通じて、MST リージョン内の各スイッチで MST コンフィギュレーション（リージョン名、リビジョン番号、および VLAN/インスタンス間のマッピング）を手動で設定することは可能です。
- ネットワーク内の冗長パスでロードバランシングを機能させるには、すべての VLAN/インスタンス間マッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。
- PVST+ クラウドと MST クラウド間、または Rapid PVST+ クラウドと MST クラウド間でロードバランシングを実現するには、すべての MST 境界ポートがフォワーディング ステートでなければなりません。そのためには、MST クラウドの IST マスターが CST のルートを兼ねている必要があります。MST クラウドが複数の MST リージョンで構成されている場合は、MST リージョンの 1 つに CST ルートが含まれており、他のすべての MST リージョンにおいて、MST クラウドに含まれているルートへのパスの方が、PVST+ クラウドまたは Rapid PVST+ クラウド経由のパスよりも優れている必要があります。クラウド内のスイッチを手動で設定しなければならない場合もあります。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。

MST リージョンの設定の指定および MSTP のイネーブル設定

2 台以上のスイッチを同じ MST リージョンに設置するには、その 2 つのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは RSTP BPDU を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニング ツリー インスタンスの数は最大 65 です。1 つの VLAN を同時に複数のスパニング ツリー インスタンスに割り当てることはできません。

MST リージョンの設定を指定し、MSTP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst configuration**	MST コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**instance** *instance-id* **vlan** *vlan-range*	VLAN を MST インスタンスに対応付けます。 • *instance-id* に指定できる範囲は 0 ～ 4094 です。 • **vlan** *vlan-range* に指定できる範囲は 1 ～ 4094 です。 VLAN を MST インスタンスにマッピングする場合、そのマッピングはインクリメンタルです。コマンドに指定した VLAN 範囲が、以前にマッピングした VLAN 範囲に対し追加または削除されます。 VLAN 範囲を指定する場合は、ハイフンを使用します。たとえば、**instance 1 vlan 1-63** と入力すると、VLAN の 1 ～ 63 が MST インスタンス 1 にマッピングされます。 VLAN を列挙する場合は、カンマを使用します。たとえば、**instance 1 vlan 10, 20, 30** と入力すると、VLAN 10、20、30 が MST インスタンス 1 にマッピングされます。
ステップ 4	**name** *name*	コンフィギュレーション名を指定します。*name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。
ステップ 5	**revision** *version*	コンフィギュレーション リビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
ステップ 6	**show pending**	入力した設定を表示して、確認します。
ステップ 7	**exit**	変更を適用し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**spanning-tree mode mst**	MSTP をイネーブルにします。RSTP もイネーブルになります。 **注意** スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが以前のモードのために停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と Rapid PVST+ の両方、または MSTP と PVST+ の両方は、同時に稼動できません。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config**	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの MST リージョン コンフィギュレーションに戻すには、**no spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用します。VLAN インスタンス マップをデフォルトの設定に戻すには、**no instance** *instance-id* [**vlan** *vlan-range*] MST コンフィギュレーション コマンドを使用します。デフォルトの名前に戻すには、**no name** MST コンフィギュレーション コマンドを使用します。デフォルトのリビジョン番号に戻すには、**no revision** MST コンフィギュレーション コマンドを使用します。Rapid PVST+ を再度イネーブルにするには、**no spanning-tree mode**、または **spanning-tree mode pvst** グローバル コンフィギュレーション コマンドを使用します。

次の例では、MST コンフィギュレーション モードを開始して VLAN 10 ～ 20 を MST インスタンス 1 にマッピングし、リージョンに *region1* と名前を付けて、構成リビジョンを 1 に設定します。変更確認前の構成を表示して変更を適用し、グローバル コンフィギュレーション モードに戻る方法を示します。

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
```

```
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  --------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

ルート スイッチの設定

スイッチは、マッピングした VLAN グループのスパニング ツリー インスタンスを維持します。各インスタンスには、スイッチ プライオリティとスイッチ MAC アドレスからなるブリッジ ID が対応付けられています。VLAN グループの場合は、最小のブリッジ ID を持つスイッチがルート スイッチになります。

あるスイッチがルート スイッチになるように設定するには、**spanning-tree mst** *instance-id* **root** グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値（32768）から極めて小さいプライオリティ値に変更します。これにより、そのスイッチが指定されたスパニング ツリー インスタンスのルート スイッチになることができます。このコマンドを入力すると、スイッチは、ルート スイッチのスイッチ プライオリティをチェックします。拡張システム ID をサポートするため、スイッチは、指定インスタンスの固有のプライオリティを 24576 に設定します（この値によって、このスイッチが指定されたスパニング ツリー インスタンスのルート スイッチになる場合）。

指定インスタンスのルート スイッチに、24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 小さい値に設定します（表 15-1（P.15-4）に示すように、4096 は、4 ビット スイッチ プライオリティ値の最下位ビットの値です）。

拡張システム ID をサポートしないスイッチとサポートするスイッチの両方がネットワークに混在している場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはありません。拡張システム ID は、旧ソフトウェア実装の接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値を増やします。

各スパニング ツリー インスタンスのルート スイッチは、バックボーンまたはディストリビューション スイッチでなければなりません。アクセス スイッチをスパニング ツリー プライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ数）を指定するには、キーワード **diameter** を指定します。ネットワークの直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、STP のコンバージェンスに要する時間が大幅に短縮されます。キーワード **hello** を使用すると、自動的に計算された hello タイムを上書きできます。

（注）　スイッチをルート スイッチとして設定したあとに、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

スイッチをルート スイッチに設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst** *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	スイッチをルート スイッチとして設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 の場合のみ使用できます。 • （任意）**hello-time** *seconds* には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst** *instance-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **root** グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

拡張システム ID をサポートするスイッチをセカンダリルートとして設定すると、スイッチ プライオリティはデフォルト値（32768）から 28672 に変更されます。その結果、プライマリ ルート スイッチに障害が発生した場合に、このスイッチが、指定されたインスタンスのルート スイッチになる可能性が高くなります。ネットワーク上の他のスイッチはデフォルトのスイッチ プライオリティである 32768 を使用していると想定されるので、他のスイッチがルート スイッチになる可能性は低くなります。

このコマンドを複数のスイッチに実行して、複数のバックアップ ルート スイッチを設定できます。**spanning-tree mst** *instance-id* **root primary** グローバル コンフィギュレーション コマンドを使用して、プライマリ ルート スイッチの設定時と同じネットワーク直径と hello タイム値を設定してください。

スイッチをセカンダリ ルート スイッチに設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst** *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	スイッチをセカンダリ ルート スイッチとして設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 の場合のみ使用できます。 • （任意）**hello-time** *seconds* には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。 プライマリ ルート スイッチの設定時と同じネットワーク直径および hello タイム値を使用します。「ルート スイッチの設定」（P.16-18）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst** *instance-id*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **root** グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生した場合、MSTP はポート プライオリティを使用して、フォワーディング ステートにする STP ポートを選択します。最初に選択させる STP ポートには高いプライオリティ（小さい数値）を与え、最後に選択させる STP ポートには低いプライオリティ（大きい数値）を付けます。すべてのインターフェイスが同じプライオリティ値を使用している場合、MSTP はインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。

インターフェイスの MSTP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、スパニング ツリーがイネーブルになった物理 NNI または ENI、VLAN、および NNI または ENI のポート チャネルがあります。VLAN ID の範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。 **（注）** 物理インターフェイスが UNI の場合、MST ポート プライオリティを設定する前に、**port-type nni** インターフェイス コンフィギュレーション コマンドを入力するか、ポートを ENI として設定し、そのポートでスパニング ツリーをイネーブルにする必要があります。「ENI 上のスパニング ツリーをイネーブルにする」（P.15-14）を参照してください。 インターフェイスが VLAN である場合は、VLAN のスパニング ツリーがイネーブルに設定されているポートだけがスパニング ツリーを実行します。 インターフェイスがポート チャネルである場合は、ポート チャネルのすべてのメンバーは、スパニング ツリーがイネーブルに設定されている NNI または ENI である必要があります。
ステップ 3	**spanning-tree mst** *instance-id* **port-priority** *priority*	ポート プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高くなります。 プライオリティ値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree mst interface** *interface-id* または **show spanning-tree mst** *instance-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注） **show spanning-tree mst interface** *interface-id* 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能の状態にある場合に限られます。そうでない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認してください。

インターフェイスをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **port-priority** インターフェイス コンフィギュレーション コマンドを使用します。

パス コストの設定

MSTP パス コストのデフォルト値は、STP ポートのメディア速度から派生します。ループが発生すると、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたい STP ポートには小さいコスト値を、最後に選択させたい STP ポートには大きいコスト値を割り当てることができます。すべてのインターフェイスが同じコスト値を使用している場合、MSTP はインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。

インターフェイスの MSTP コストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、スパニング ツリーがイネーブルになった物理 NNI または ENI、VLAN、および NNI または ENI のポート チャネルがあります。VLAN ID の範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。 **（注）** 物理インターフェイスが UNI の場合、MST ポート プライオリティを設定する前に、**port-type nni** インターフェイス コンフィギュレーション コマンドを入力するか、ポートを ENI として設定し、そのポートでスパニング ツリーをイネーブルにする必要があります。「ENI 上のスパニング ツリーをイネーブルにする」（P.15-14）を参照してください。 インターフェイスが VLAN である場合は、VLAN のスパニング ツリーがイネーブルに設定されているポートだけがスパニング ツリーを実行します。 インターフェイスがポート チャネルである場合は、ポート チャネルのすべてのメンバーは、スパニング ツリーがイネーブルに設定されている NNI または ENI である必要があります。
ステップ 3	**spanning-tree mst** *instance-id* **cost** *cost*	コストを設定します。 ループが発生すると、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストの値が小さいほど、高速で転送されます。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *cost* に指定できる範囲は 1 ～ 200000000 です。デフォルト値は、インターフェイスのメディア速度によって決まります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

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

（注）　**show spanning-tree mst interface** *interface-id* 特権 EXEC コマンドで情報が表示されるのは、リンクアップ動作可能の状態にあるポートに限られます。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

インターフェイスをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **cost** インターフェイス コンフィギュレーション コマンドを使用します。

スイッチ プライオリティの設定

スイッチ プライオリティを設定し、そのスイッチがルート スイッチとして選択される可能性を高めることができます。

（注）　このコマンドは慎重に使用してください。通常、スイッチ プライオリティの変更には、**spanning-tree mst** *instance-id* **root primary**、および **spanning-tree mst** *instance-id* **root secondary** グローバル コンフィギュレーション コマンドの使用を推奨します。

スイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst** *instance-id* **priority** *priority*	スイッチ プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* に指定できる範囲は 0 ～ 61440 で、4096 ずつ増えます。デフォルトは 32768 です。数値が小さいほど、スイッチがルート スイッチとして選択される可能性が高くなります。 プライオリティ値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。それ以外の値はすべて拒否されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

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

スイッチをデフォルト設定に戻すには、**no spanning-tree mst** *instance-id* **priority** グローバル コンフィギュレーション コマンドを使用します。

hello タイムの設定

hello タイムを変更することによって、ルート スイッチによるコンフィギュレーション メッセージが生成される間隔を設定できます。

（注）　このコマンドは慎重に使用してください。通常、hello タイムの変更には、**spanning-tree mst** *instance-id* **root primary**、および **spanning-tree mst** *instance-id* **root secondary** グローバル コンフィギュレーション コマンドの使用を推奨します。

すべての MST インスタンスの hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst hello-time** *seconds*	すべての MST インスタンスの hello タイムを設定します。hello タイムは、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔です。このメッセージはスイッチが動作中であることを意味します。 *seconds* に指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst hello-time** グローバル コンフィギュレーション コマンドを使用します。

転送遅延時間の設定

すべての MST インスタンスの転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst forward-time** *seconds*	すべての MST インスタンスの転送時間を設定します。転送遅延は、スパニング ツリーのラーニングおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 *seconds* に指定できる範囲は 4 ～ 30 秒です。デフォルトは 15 秒です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst forward-time** グローバル コンフィギュレーション コマンドを使用します。

最大エージング タイムの設定

すべての MST インスタンスの最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst max-age** *seconds*	すべての MST インスタンスの最大エージング タイムを設定します。最大エージング タイムは、再構成を行うまでに、スイッチがスパニング ツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 秒です。デフォルトは 20 秒です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用します。

最大ホップ カウントの設定

すべての MST インスタンスの最大ホップ カウントを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree mst max-hops** *hop-count*	BPDU が廃棄され、ポートに維持されていた情報が期限切れになるまでの、リージョン内でのホップ数を指定します。 *hop-count* に指定できる範囲は 1 ～ 255 です。デフォルトは 20 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree mst**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst max-hops** グローバル コンフィギュレーション コマンドを使用します。

リンク タイプの指定による高速移行の保証

2 つの STP ポートをポイントツーポイント リンクで接続し、ローカル ポートが指定ポートになると、RSTP は提案合意ハンドシェイクを使用して、相手側ポートと高速移行をネゴシエーションし、ループのないトポロジを保証します（「高速コンバージェンス」（P.16-10）を参照）。

リンク タイプは、デフォルトで、インターフェイスのデュプレックス モードによって制御されます。全二重ポートはポイントツーポイント接続と見なされ、半二重ポートは共有接続と見なされます。MSTP が稼動しているリモート スイッチ上の 1 つのポートと物理的にポイントツーポイントで接続されている半二重リンクが存在する場合は、リンク タイプのデフォルト設定値を変更して、フォワーディング ステートへの高速移行をイネーブルにできます。

デフォルトのリンク タイプ値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、スパニング ツリーがイネーブルになった物理 NNI または ENI、VLAN、および NNI または ENI のポート チャネルがあります。VLAN ID の範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。 **（注）** 物理インターフェイスが UNI の場合、MST ポート プライオリティを設定する前に、**port-type nni** インターフェイス コンフィギュレーション コマンドを入力するか、ポートを ENI として設定し、そのポートでスパニング ツリーをイネーブルにする必要があります。「ENI 上のスパニング ツリーをイネーブルにする」（P.15-14）を参照してください。 インターフェイスが VLAN である場合は、VLAN のスパニング ツリーがイネーブルに設定されているポートだけがスパニング ツリーを実行します。 インターフェイスがポート チャネルである場合は、ポート チャネルのすべてのメンバーは、スパニング ツリーがイネーブルに設定されている NNI または ENI である必要があります。
ステップ 3	**spanning-tree link-type point-to-point**	ポートのリンク タイプをポイントツーポイントに指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree mst interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポートをデフォルト設定に戻すには、**no spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用します。

ネイバ タイプの指定

トポロジには、先行標準対応のデバイスと IEEE 802.1s 標準対応のデバイスの両方を含めることができます。デフォルトでは、ポートは自動的に先行標準デバイスを検出しますが、標準 BPDU と先行標準 BPDU の両方を受信できます。デバイスとそのネイバに不一致が存在すると、CIST だけがインターフェイスで動作します。

先行標準 BPDU だけを送信するようにポートを設定できます。ポートが STP 互換モードになっていても、すべての show コマンドで先行標準フラグが表示されます。

デフォルトのリンク タイプ値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、スパニング ツリーがイネーブルになった物理 NNI または ENI、VLAN、および NNI または ENI のポート チャネルがあります。VLAN ID の範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。 **（注）** 物理インターフェイスが UNI の場合、MST ポート プライオリティを設定する前に、**port-type nni** インターフェイス コンフィギュレーション コマンドを入力するか、ポートを ENI として設定し、そのポートでスパニング ツリーをイネーブルにする必要があります。「ENI 上のスパニング ツリーをイネーブルにする」（P.15-14）を参照してください。 インターフェイスが VLAN である場合は、VLAN のスパニング ツリーがイネーブルに設定されているポートだけがスパニング ツリーを実行します。 インターフェイスがポート チャネルである場合は、ポート チャネルのすべてのメンバーは、スパニング ツリーがイネーブルに設定されている NNI または ENI である必要があります。
ステップ 3	**spanning-tree mst pre-standard**	ポートが先行標準 BPDU だけを送信することを指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree mst interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポートをデフォルト設定に戻すには、**no spanning-tree mst prestandard** インターフェイス コンフィギュレーション コマンドを使用します。

プロトコル移行プロセスの再起動

MSTP を稼動しているスイッチは、802.1D レガシー スイッチとの相互運用を可能にする内蔵プロトコル移行メカニズムをサポートします。このスイッチは、802.1D 準拠のレガシー コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信すると、そのポートでは 802.1D BPDU だけを送信します。また、MSTP スイッチは、レガシー BPDU、異なるリージョンに関連付けられている MST BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、スイッチは、802.1D BPDU を受信しなくなっても、MSTP モードに自動的に戻ることはありません。レガシー スイッチが指定スイッチでないかぎり、レガシー スイッチがリンクから除去されたかどうかを検出できないからです。さらにスイッチは、接続先スイッチがリージョンに加入した場合に、引き続きポートに境界の役割を指定する可能性があります。

スイッチのプロトコル移行プロセスを再起動する（近接スイッチとの再ネゴシエーションを強制する）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

特定のインターフェイスに対してプロトコル移行プロセスを再起動するには、**clear spanning-tree detected-protocols interface** *interface-id* 特権 EXEC コマンドを使用します。

MST コンフィギュレーションおよびステータスの表示

スパニング ツリー ステータスを表示するには、表 16-5 に示す特権 EXEC コマンドの 1 つまたは複数を使用します。

表 16-5　MST ステータスを表示するためのコマンド

コマンド	目的
show spanning-tree mst configuration	MST リージョンの設定を表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれる MD5 ダイジェストを表示します。
show spanning-tree mst *instance-id*	指定インスタンスの MST 情報を表示します。
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。

show spanning-tree 特権 EXEC コマンドのキーワードについては、このリリースのコマンド リファレンスを参照してください。

CHAPTER 17

オプションのスパニング ツリー機能の設定方法

この章では、Cisco ME 3400E イーサネット アクセス スイッチにオプションのスパニング ツリー機能を設定する方法について説明します。スイッチで Per-VLAN Spanning-Tree Plus（PVST+; VLAN 単位スパニング ツリー プラス）が稼動している場合は、これらの機能をすべて設定できます。スイッチが Multiple Spanning-Tree Protocol（MSTP; マルチ スパニング ツリー プロトコル）または Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルを稼動している場合は、明記した機能だけを設定できます。Cisco ME スイッチでは、STP は Network Node Interface（NNI; ネットワーク ノード インターフェイス）上でデフォルトでイネーブルに設定されます。Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）上ではデフォルトでディセーブルになっていますが、イネーブルにできます。スイッチ上の User Network Interface（UNI; ユーザ ネットワーク インターフェイス）は STP に参加しません。STP がイネーブルにされていない UNI および ENI は、起動されるとすぐにトラフィックを転送します。

PVST+ および Rapid PVST+ を設定する方法の詳細については、第 15 章「STP の設定」を参照してください。また、MSTP および複数の VLAN を同じスパニング ツリー インスタンスにマッピングする方法の詳細については、第 16 章「MSTP の設定」を参照してください。

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

- 「オプションのスパニング ツリー機能の概要」（P.17-1）
- 「オプションのスパニング ツリー機能の設定方法」（P.17-5）
- 「スパニング ツリー ステータスの表示」（P.17-12）

オプションのスパニング ツリー機能の概要

- 「PortFast の概要」（P.17-2）
- 「BPDU ガードの概要」（P.17-3）
- 「BPDU フィルタリングの概要」（P.17-3）
- 「EtherChannel ガードの概要」（P.17-4）
- 「ルート ガードの概要」（P.17-4）
- 「ループ ガードの概要」（P.17-5）

PortFast の概要

PortFast を使用することにより、アクセス ポートまたはトランク ポートとして設定された STP ポートは、ブロッキング ステートから、リスニングおよびラーニング ステートを経由することなく、直接にフォワーディング ステートになります。

（注）　デフォルトでは、STP は NNI 上でイネーブルに設定され、ENI 上ではディセーブルに設定されます。UNI では、STP はサポートされていません。ポートが UNI の場合、ポート タイプを NNI または ENI に変更し、**port-type {nni | eni}** インターフェイス コンフィギュレーション コマンドを入力することで、ポートを STP ポートとして設定できます。ENI では、ポートを STP ポートとして設定するには、**spanning-tree** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

単一のワークステーションまたはサーバに接続された STP ポート上で PortFast を使用すると、スパニング ツリーが収束するのを待たずにデバイスをただちにネットワークに接続できます（図 17-1 を参照）。

単一のワークステーションまたはサーバに接続されている STP ポートは Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信しません。PortFast がイネーブルに設定されている STP ポートは、スイッチを再起動すると、通常のスパニング ツリー ステータスの変化をたどります。

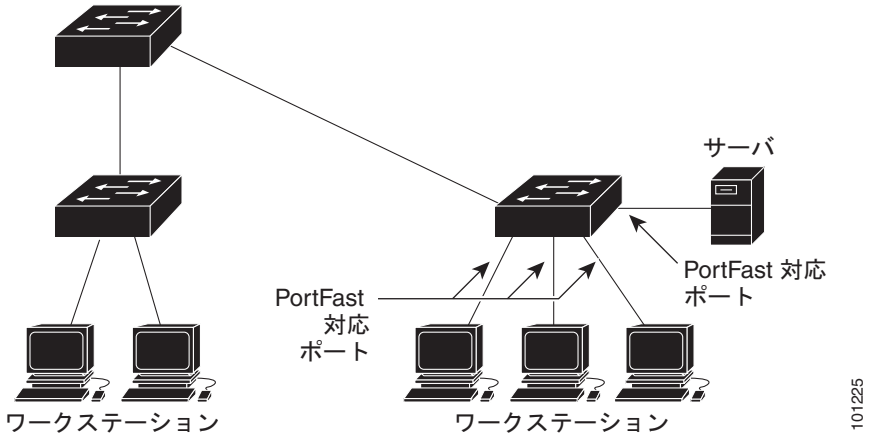
（注）　PortFast の目的は、インターフェイスがスパニング ツリーのコンバージェンスを待つ時間を最小限にすることです。したがって、エンド ステーションに接続された STP ポートで使用した場合に限り有効になります。別のスイッチに接続しているインターフェイスで PortFast をイネーブルにした場合は、スパニング ツリー ループが発生する危険性が生じます。

UNI は、通常カスタマー側のポートで、サービス プロバイダーのスパニング ツリーには参加しません。ただし、カスタマー側のポートを ENI として設定し、スパニング ツリーをイネーブルにすると、ポート上のルート ガードを設定しない限り、ENI がスパニング ツリー ルート ポートとなる場合があります。「ルート ガードの概要」（P.17-4）を参照してください。STP がイネーブルに設定されているカスタマー側の ENI は、サービス プロバイダー側の NNI と同じスパニング ツリーに参加します。

（注）　カスタマー側の ENI 上の STP をイネーブルにする場合、注意して使用してください。

spanning-tree portfast インターフェイス コンフィギュレーション コマンドまたは **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

図 17-1　PortFast 対応インターフェイス



BPDU ガードの概要

BPDU ガード機能はスイッチ全体でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできますが、いくつかの相違点があります。

グローバル レベルでは、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用することにより、PortFast 対応 STP ポートで BPDU ガードをイネーブルにできます。任意の BPDU が Port Fast 動作ステータスの STP ポート上で受信された場合、スパニング ツリーはこの STP ポートをシャット ダウンします。有効な設定では、PortFast 対応 STP ポートは BPDU を受信しません。PortFast がイネーブルに設定されているポートが BPDU を受信するということは、認可されていないデバイスの接続など、無効な設定が存在することを示しており、BPDU ガード機能によってインターフェイスは errdisable ステートになります。

インターフェイス レベルでは、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用することにより、PortFast 機能をイネーブルにせずに、任意の STP ポートで BPDU ガードをイネーブルにできます。STP ポートが BPDU を受信すると、そのポートは errdisable ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。

BPDU ガード機能をスイッチ全体またはインターフェイスでイネーブルにできます。

BPDU フィルタリングの概要

BPDU フィルタリング機能はスイッチ全体でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできますが、いくつかの相違点があります。

グローバル レベルでは、**spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用することにより、PortFast イネーブル設定 STP ポートで BPDU フィルタリングをイネーブルにできます。このコマンドは、PortFast 稼動ステート インターフェイスが BPDU できないようにします。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのポートに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。PortFast イネーブル設定 STP ポート上で BPDU が受信された場合、そのインターフェイスは PortFast 稼動ステータスを解除され、BPDU フィルタリングはディセーブルになります。

インターフェイス レベルでは、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用することにより、PortFast 機能をイネーブルにせずに、任意の STP ポートで BPDU フィルタリングをイネーブルにできます。このコマンドにより、インターフェイスは BPDU を送受信できなくなります。

注意　STP ポート上で BPDU フィルタリングをイネーブルにすると、STP ポート上でスパニング ツリーをディセーブルにしたのと同じ結果になり、スパニング ツリー ループが発生する可能性があります。

スイッチ全体または STP ポートに対して、BPDU フィルタリング機能をイネーブルにできます。

EtherChannel ガードの概要

EtherChannel ガードを使用して、スイッチと接続デバイス間の誤った EtherChannel の設定を検出できます。スイッチ STP ポートが EtherChannel に設定された場合に設定ミスが発生しますが、他のデバイスのインターフェイスはそうではありません。また、チャネル パラメータが EtherChannel の両端で異なっている場合も設定ミスが発生します。EtherChannel 設定時の注意事項については、「EtherChannel 設定時の注意事項」（P.35-10）を参照してください。

スイッチが設定ミスを検出すると、EtherChannel ガードがスイッチ STP ポート を errdisable ステートにして、エラー メッセージを表示します。

この機能は、**spanning-tree etherchannel guard misconfig** グローバル コンフィギュレーション コマンドを使用してイネーブルにできます。

ルート ガードの概要

サービス プロバイダー（SP）のレイヤ 2 ネットワークには、SP が所有するスイッチ以外への接続が多く含まれている場合があります。このようなトポロジでは、図 17-2 に示すように、スパニング ツリーが再構成され、*カスタマーのスイッチ*がルート スイッチとして選択される可能性があります。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチのインターフェイス上で、ルート ガード機能を設定します。スパニング ツリー計算によりカスタマー ネットワークのインターフェイスがルート ポートとして選択された場合、ルート ガード機能はそのインターフェイスを root-inconsistent（ブロック）ステートに変更し、カスタマー スイッチがルート スイッチにならないように、またルートへのパスを提供しないようにします。

サービス プロバイダー ネットワークの外側のスイッチがルート スイッチになると、インターフェイスはブロックされ（root-inconsistent ステートになるので）、スパニング ツリーによって新しいルート スイッチが選択されます。カスタマーのスイッチがルート スイッチになることはなく、ルートへのパスに含まれることもありません。

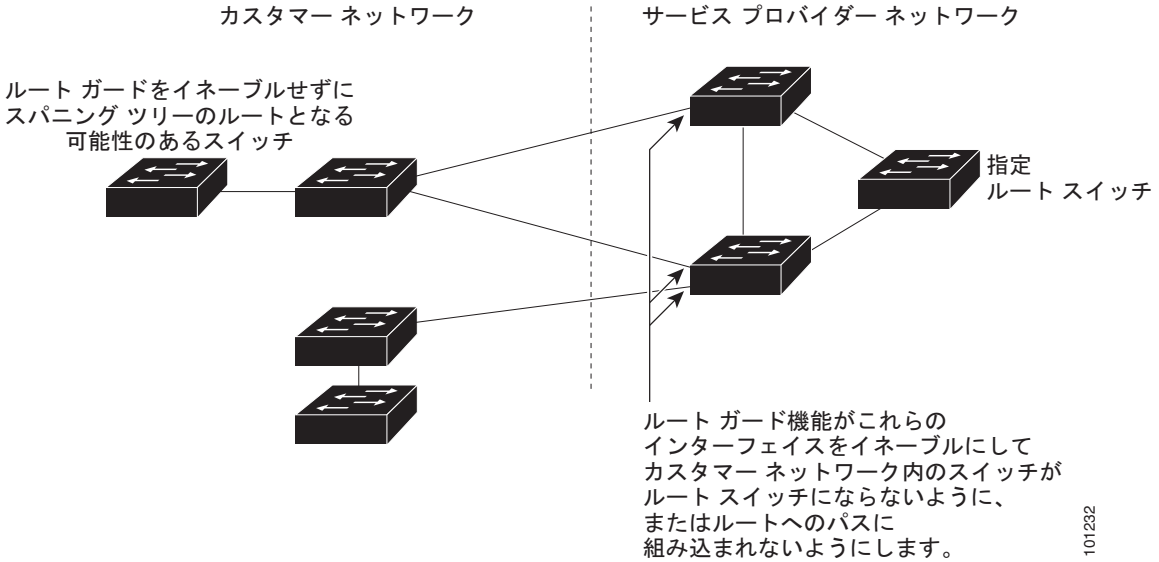
そのスイッチが Multiple Spanning-Tree（MST）モードで動作している場合、ルート ガード機能によって、そのインターフェイスは強制的に指定ポートになります。ルート ガードにより、Internal Spanning-Tree（IST）インスタンス内の境界ポートがブロックされた場合、そのインターフェイスはすべての MST インスタンスでブロックされます。境界ポートは、指定スイッチが 802.1D スイッチまたは異なる MST リージョン コンフィギュレーションを持つスイッチである LAN に接続されたインターフェイスです。

1 つのインターフェイスでルート ガードをイネーブルにすると、そのインターフェイスが属するすべての VLAN にルート ガードが適用されます。VLAN をグループにまとめて MST インスタンスにマッピングすることができます。

この機能は、**spanning-tree guard root** インターフェイス コンフィギュレーション コマンドを使用してイネーブルにできます。

注意　ルート ガード機能を誤って使用すると、接続が切断されることがあります。

図 17-2　SP ネットワークにおけるルート ガード



ループ ガードの概要

ループ ガードを使用すると、障害による単方向リンクが原因で、代替ポートまたはルート ポートが指定ポートになるのを防止できます。この機能は、スイッチド ネットワーク全体で設定すると、大きな効果が得られます。ループ ガードは、代替ポートおよびルート ポートが指定ポートになるのを防ぎます。したがって、スパニング ツリーはルート ポートまたは代替ポートで BPDU を送信しません。

この機能は、**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドを使用してイネーブルにできます。

スイッチが PVST+ モードまたは Rapid PVST+ モードで動作している場合、ループ ガードは、代替ポートおよびルート ポートが指定ポートになるのを防ぎます。スパニング ツリーはルート ポートまたは代替ポート上で BPDU を送信しません。

スイッチが MST モードで動作している場合、非境界ポートで BPDU が送信されないのは、すべての MST インスタンスにおいて、そのインターフェイスがループ ガードによりブロックされている場合だけです。境界ポートでは、ループ ガードによってすべての MST インスタンスのインターフェイスがブロックされます。

オプションのスパニング ツリー機能の設定方法

- 「オプションのスパニング ツリー機能のデフォルト設定」（P.17-6）
- 「オプションのスパニング ツリー機能の設定時の注意事項」（P.17-6）
- 「PortFast のイネーブル化」（P.17-6）（任意）
- 「BPDU ガードのイネーブル化」（P.17-8）（任意）

- 「BPDU フィルタリングのイネーブル化」（P.17-9）（任意）
- 「EtherChannel ガードのイネーブル化」（P.17-10）（任意）
- 「ルート ガードのイネーブル化」（P.17-11）（任意）
- 「ループ ガードのイネーブル化」（P.17-12）（任意）

オプションのスパニング ツリー機能のデフォルト設定

表 17-1 に、オプションのスパニング ツリー機能のデフォルト設定を示します。スイッチ上の STP に参加するのは、NNI または STP がイネーブルに設定されている ENI に限られます。STP 対応に設定されていない UNI および ENI は、常にフォワーディング ステートです。

表 17-1　オプションのスパニング ツリー機能のデフォルト設定

機能	デフォルト設定
PortFast、BPDU フィルタリング、BPDU ガード	グローバルにディセーブル（STP ポート単位で個別に設定されていない場合）
EtherChannel ガード	グローバルにイネーブル
ルート ガード	すべての STP ポートでディセーブルになっています。
ループ ガード	すべての STP ポートでディセーブルになっています。

オプションのスパニング ツリー機能の設定時の注意事項

スイッチで PVST+、Rapid PVST+、または MSTP を実行している場合、PortFast、BPDU ガード、BPDU フィルタリング、EtherChannel ガード、ルート ガード、またはループ ガードを設定できます。

任意のスパニング ツリー コンフィギュレーション コマンドは、UNI または STP がイネーブルに設定されていない ENI ではサポートされていません。

PortFast のイネーブル化

PortFast 機能がイネーブルに設定された STP ポートは、標準の転送遅延時間を待たずに直接スパニング ツリーのフォワーディング ステートに移行されます。

注意　PortFast を使用するのは、単一のエンド ステーションをアクセス ポートまたはトランク ポートに接続する場合*だけ*にしてください。スイッチまたはハブに接続するインターフェイスでこの機能をイネーブルにすると、スパニング ツリーがネットワーク ループを検出または阻止できなくなり、そのためにブロードキャスト ストームやアドレス学習の障害が起こる可能性があります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動していれば、この機能をイネーブルにできます。

PortFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する STP インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスが UNI である場合、Port Fast をイネーブルにする前に、次のようにポート タイプを NNI または ENI に変更して STP をイネーブルにする必要があります。 • **port-type nni** インターフェイス コンフィギュレーション コマンドを入力し、ポートを STP がデフォルトでイネーブルに設定されている NNI に変更します。 • または、**port-type eni** および **spanning-tree** の各インターフェイス コンフィギュレーション コマンドを入力してポートを ENI STP ポートとして設定します。
ステップ 3	**spanning-tree portfast** [**trunk**]	単一のワークステーションまたはサーバに接続されたアクセス ポートで PortFast をイネーブルにします。キーワード **trunk** を指定することにより、トランク ポートで PortFast をイネーブルにすることができます。 **（注）** トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポートで動作しません。 **注意** トランク ポートで PortFast をイネーブルにする前に、そのトランク ポートとワークステーションまたはサーバの間のネットワークにループがないことを確認してください。 デフォルトでは、PortFast はすべての STP ポートでディセーブルに設定されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree interface** *interface-id* **portfast**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注） **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用すると、すべての非トランキング STP ポート上で PortFast 機能をグローバルにイネーブルにできます。

PortFast 機能をディセーブルにするには、**spanning-tree portfast disable** インターフェイス コンフィギュレーション コマンドを使用します。

BPDU ガードのイネーブル化

Port Fast がイネーブルに設定されているポート上（Port Fast が動作可能な状態のポート）で BPDU ガードをグローバルにイネーブルにすると、スパニング ツリーはポート上で実行を継続します。BPDU を受け取るまではアップのままになります。

有効な設定では、PortFast 対応インターフェイスは BPDU を受信しません。PortFast 対応インターフェイスが BPDU を受信した場合は、認可されていないデバイスの接続などのような無効な設定が存在することを示しており、BPDU ガード機能によってインターフェイスは errdisable ステートになります。インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。

注意　PortFast は、エンド ステーションに接続する STP ポートに限って設定します。そうしないと、偶発的なトポロジ ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

spanning-tree bpduguard enable インターフェイス コンフィギュレーション コマンドを使用すると、PortFast 機能をイネーブルにしなくても、任意の STP ポートで BPDU ガードをイネーブルにすることができます。インターフェイスが BPDU を受信すると、そのポートは errdisable ステートになります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動していれば、BPDU ガード機能をイネーブルにできます。

BPDU ガード機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree portfast bpduguard default**	BPDU ガードをグローバルにイネーブルにします （デフォルトでは、BPDU ガードはディセーブルに設定されています)。 **（注）** グローバルに BPDU ガードをイネーブルにする場合、STP ポートでだけイネーブルになります。このコマンドは、STP を実行していないポートでは無効です。
ステップ 3	**interface** *interface-id*	エンド ステーションに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスが UNI である場合、Port Fast をイネーブルにする前に、次のようにポート タイプを NNI または ENI に変更して STP をイネーブルにする必要があります。 • **port-type nni** インターフェイス コンフィギュレーション コマンドを入力し、ポートを STP がデフォルトでイネーブルに設定されている NNI に変更します。 • または、**port-type eni** および **spanning-tree** の各インターフェイス コンフィギュレーション コマンドを入力してポートを ENI STP ポートとして設定します。
ステップ 4	**spanning-tree portfast**	PortFast 機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BPDU ガードをディセーブルにするには、グローバル コンフィギュレーション コマンドを使用します。**no spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用します。

spanning-tree bpduguard enable インターフェイス コンフィギュレーション コマンドを STP ポートで使用すると、**no spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドの設定を上書きできます。

BPDU フィルタリングのイネーブル化

PortFast がイネーブルに設定されている STP ポートでグローバルに BPDU フィルタリングをイネーブルにすると、PortFast 稼動ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。PortFast イネーブル設定 STP ポート上で BPDU が受信された場合、そのインターフェイスは PortFast 稼動ステータスを解除され、BPDU フィルタリングはディセーブルになります。

注意　PortFast は、エンド ステーションに接続する STP ポートに限って設定します。そうしないと、偶発的なトポロジ ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

spanning-tree bpdufilter enable インターフェイス コンフィギュレーション コマンドを使用すると、PortFast 機能をイネーブルにせずに、任意の STP ポートで BPDU フィルタリングをイネーブルにできます。このコマンドにより、STP ポートは BPDU を送受信できなくなります。

注意　STP ポート上で BPDU フィルタリングをイネーブルにすると、STP ポート上でスパニング ツリーをディセーブルにしたのと同じ結果になり、スパニング ツリー ループが発生する可能性があります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動していれば、BPDU フィルタリング機能をイネーブルにできます。

BPDU フィルタリング機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree portfast bpdufilter default**	BPDU フィルタリングをグローバルにイネーブルにします （デフォルトでは、BPDU フィルタリングはディセーブルに設定されています)。 **（注）** グローバルに BPDU フィルタリングをイネーブルにする場合、STP ポートでだけイネーブルになります。このコマンドは、STP を実行していない UNI または ENI では無効です。
ステップ 3	**interface** *interface-id*	エンド ステーションに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスが UNI である場合、Port Fast をイネーブルにする前に、次のようにポート タイプを NNI または ENI に変更して STP をイネーブルにする必要があります。 • **port-type nni** インターフェイス コンフィギュレーション コマンドを入力し、ポートを STP がデフォルトでイネーブルに設定されている NNI に変更します。 • または、**port-type eni** および **spanning-tree** の各インターフェイス コンフィギュレーション コマンドを入力してポートを ENI STP ポートとして設定します。
ステップ 4	**spanning-tree portfast**	PortFast 機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BPDU フィルタリングをディセーブルにするには、**no spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用します。

spanning-tree bpdufilter enable インターフェイス コンフィギュレーション コマンドを STP ポートで使用すると、**no spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドの設定を上書きできます。

EtherChannel ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が動作している場合に EtherChannel の誤設定を検出するように EtherChannel ガードをイネーブルにできます。

EtherChannel ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**spanning-tree etherchannel guard misconfig**	EtherChannel ガードをイネーブルにします。

	コマンド	目的
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree summary**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EtherChannel ガード機能をディセーブルにするには、**no spanning-tree etherchannel guard misconfig** グローバル コンフィギュレーション コマンドを使用します。

EtherChannel の誤設定によりどのスイッチ STP ポートがディセーブルであるかを示すには、**show interfaces status err-disabled** 特権 EXEC コマンドを使用します。リモート デバイスでは、**show etherchannel summary** 特権 EXEC コマンドを入力して EtherChannel 設定を確認できます。

設定を修正後、**shutdown** および **no shutdown** の各インターフェイス コンフィギュレーション コマンドを、誤設定したポートチャネル インターフェイスに入力します。

ルート ガードのイネーブル化

1 つの STP ポートでルート ガードをイネーブルにすると、そのポートが属するすべての VLAN にルート ガードが適用されます。

（注）　ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動していれば、この機能をイネーブルにできます。

インターフェイス上でルート ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスが UNI である場合、ルート ガードをイネーブルにする前に、次のようにポート タイプを NNI または ENI に変更して STP をイネーブルにする必要があります。 • **port-type nni** インターフェイス コンフィギュレーション コマンドを入力し、ポートを STP がデフォルトでイネーブルに設定されている NNI に変更します。 • または、**port-type eni** および **spanning-tree** の各インターフェイス コンフィギュレーション コマンドを入力してポートを ENI STP ポートとして設定します。
ステップ 3	**spanning-tree guard root**	STP ポートでルート ガードをイネーブルに設定します。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルに設定されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。

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

ルート ガードをディセーブルにするには、**no spanning-tree guard** インターフェイス コンフィギュレーション コマンドを使用します。

ループ ガードのイネーブル化

ループ ガードを使用すると、障害による単方向リンクが原因で、代替ポートまたはルート ポートが指定ポートになるのを防止できます。この機能は、スイッチド ネットワーク全体で設定すると、大きな効果が得られます。ループ ガードが機能するのは、スパニング ツリーによってポイントツーポイントと見なされた STP ポート上だけです。

（注）　ループ ガードとルート ガードは、同時にイネーブルにできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動していれば、この機能をイネーブルにできます。

ループ ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**show spanning-tree active** または **show spanning-tree mst**	代替インターフェイスまたはルート ポートを確認します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default**	ループ ガードをイネーブルにします。デフォルトでは、ループ ガードはディセーブルに設定されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ループ ガードをグローバルにディセーブルにするには、**no spanning-tree loopguard default** グローバル コンフィギュレーション コマンドを使用します。**spanning-tree guard loop** インターフェイス コンフィギュレーション コマンドを NNI で使用すると、**no spanning-tree loopguard default** グローバル コンフィギュレーション コマンドの設定を上書きすることができます。

スパニング ツリー ステータスの表示

スパニング ツリー ステータスを表示するには、表 17-2 に示す特権 EXEC コマンドの 1 つまたは複数を使用します。

表 17-2　スパニング ツリー ステータスを表示するためのコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスだけに関するスパニング ツリー情報を表示します。
show spanning-tree detail	インターフェイス情報の詳細なサマリーを表示します。
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーまたはスパニング ツリー ステート セクションのすべての行を表示します。

clear spanning-tree [**interface** *interface-id*] 特権 EXEC コマンドを使用して、スパニング ツリー カウンタをクリアできます。

show spanning-tree 特権 EXEC コマンドのキーワードについては、このリリースのコマンド リファレンスを参照してください。

CHAPTER 18

レジリエント イーサネット プロトコルの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに Resilient Ethernet Protocol（REP; レジリエント イーサネット プロトコル）を設定する方法について説明します。REP はシスコ独自のプロトコルで、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）の代替プロトコルとして、ネットワーク ループを制御、リンク障害に対応、コンバージェンス時間を改善します。REP は、それぞれのセグメントに接続されているポートのグループを制御してセグメントがブリッジング ループを作成するのを防ぎ、セグメント内のリンク障害に対応します。REP は、より複雑なネットワークを構築するための基盤を提供、VLAN ロード バランシングをサポートします。

この章で説明する内容は、次のとおりです。

- 「REP の概要」（P.18-1）
- 「REP の設定」（P.18-6）
- 「REP のモニタリング」（P.18-15）

REP の概要

REP セグメントは、互いに接続しているポートのチェーンで、セグメント ID が設定されています。各セグメントは、標準（非エッジ）セグメント ポートと、2 つのユーザ設定のエッジ ポートで構成されています。同じセグメント内では、1 つのスイッチあたりのポートは 2 つまでで、各セグメント ポートの外部ネイバーは 1 つだけです。セグメントは共有メディアを経由できますが、どのリンクでも同じセグメントに属することができるポートは 2 つだけです。REP は、レイヤ 2 トランク インターフェイスでだけサポートされます。

図 18-1 に、4 つのスイッチに分散する 6 つのポートで構成されたセグメントの例を示します。ポート E1 とポート E2 はエッジ ポートとして設定されます。すべてのポートが動作可能である場合（左側のセグメント）、斜線が示すように、単一ポートがブロックされます。右側のダイアグラムで示されているように、ネットワーク障害がある場合、ブロックされたポートがフォワーディング ステートに戻り、ネットワークの崩壊を最低限にくいとめます。

図 18-1　REP オープン セグメント

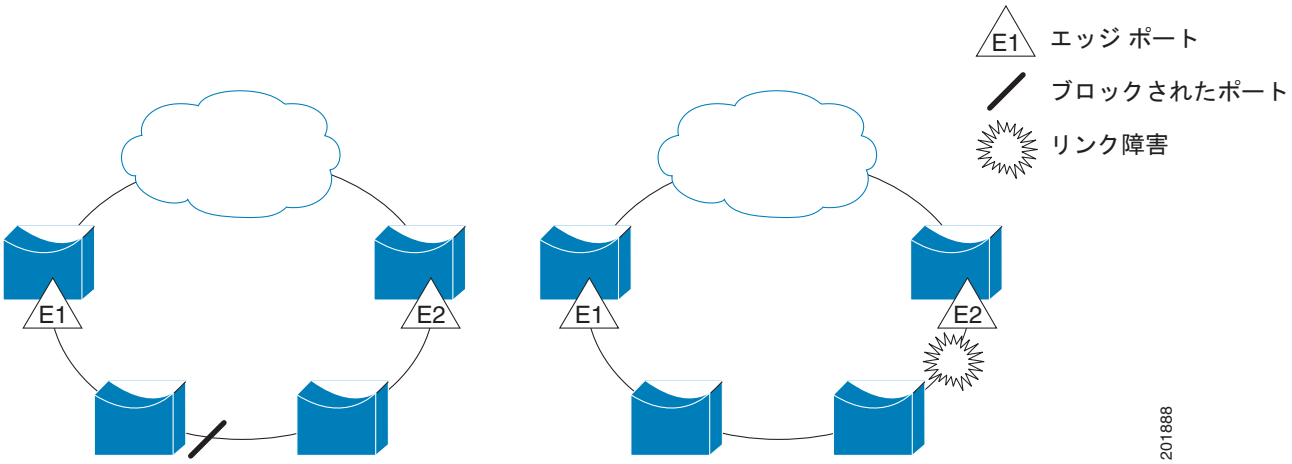
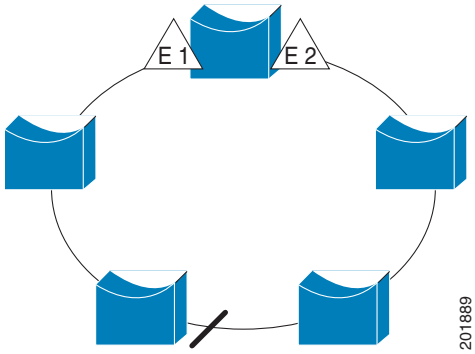


図 18-1 に示されたセグメントはオープン セグメントです。2 つのエッジ ポート間には接続がありません。REP セグメントはブリッジング ループの原因とならないため、セグメント エッジを安全に任意のネットワークに接続できます。セグメント内のスイッチに接続するすべてのホストには、エッジ ポートを経由する残りのネットワークへの接続が 2 種類可能ですが、常にアクセス可能な接続は 1 つだけです。障害によりホストが通常のゲートウェイにアクセスできない場合、他のゲートウェイを経由して接続できるよう、REP がすべてのポートのブロックを解除します。

図 18-2 に示すような、両方のエッジ ポートが同じスイッチにあるセグメントは、リングセグメントです。この設定の場合、セグメント経由でエッジ ポート同士が接続しています。この設定により、セグメント内の任意の 2 つのスイッチ間に冗長接続を作成できます。

図 18-2　REP リングセグメント



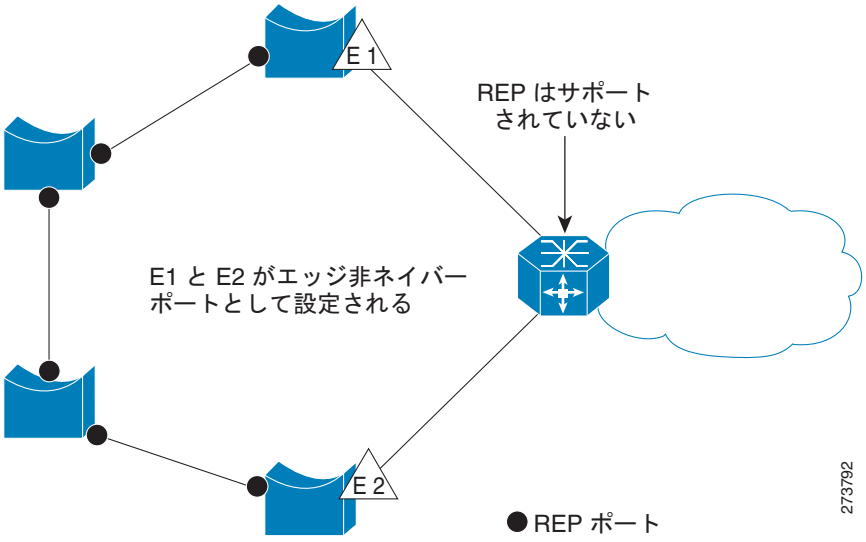
REP セグメントには、次の 3 つの特性があります。

- セグメント内のすべてのポートが動作可能である場合、1 つのポート（*代替*ポートと呼ばれる）が各 VLAN でブロックされた状態になります。
- VLAN にロード バランシングが設定されている場合、セグメント内の 2 つのポートが VLAN のブロックされた状態を制御します。
- セグメント内の 1 つまたは複数のポートが動作可能でなく、リンク障害の原因となる場合、すべてのポートがすべての VLAN のトラフィックを転送し、接続を確保します。
- リンク障害が発生すると、代替ポートのブロックがただちに解除されます。リンク障害が復旧した場合、ネットワークの崩壊が最小限になるよう、VLAN ごとに論理的にブロックされたポートが選択されます。

REP セグメントに基づくことにより、ほとんどの種類のネットワークが構築できます。また、REP は、プライマリ エッジ ポートで制御され、セグメント内の任意のポートで発生する VLAN ロード バランシングもサポートします。

アクセスのリング型トポロジでは、図 18-3 で示すように隣接スイッチが REP をサポートしない場合があります。この場合、非 REP 側ポート（E1 および E2）をエッジ非ネイバー ポートとして設定できます。これらのポートはエッジ ポートのすべてのプロパティを継承し、STP または REP のトポロジ変更通知を集約スイッチに送信するよう設定するなど、任意のエッジ ポートと同じように設定できます。この場合、送信される STP topology change notice（TCN; STP トポロジ変更通知）は、Multiple Spanning-Tree（MST; 複数のスパニング ツリー）STP メッセージです。

図 18-3　　エッジ非ネイバー ポート



REP には、次の制限事項があります。

- 各セグメント ポートを設定する必要があります。設定が正しくないと、ネットワークでフォワーディング ループを引き起こす場合があります。
- REP は、セグメント内の障害の起きたポートを 1 つだけ管理できます。REP セグメント内で複数のポートに障害が発生した場合、ネットワーク接続性が失われます。
- 冗長性のあるネットワークに REP だけを設定する必要があります。冗長性のないネットワークに REP を設定すると、接続性が失われます。

リンク完全性

REP は、エンドツーエンド ポーリング メカニズムを使用して、リンク完全性を確認することはありません。ローカルのリンク障害の検出を実行します。REP Link Status Layer（LSL; リンク ステータス レイヤ）は、REP 認識ネイバーを検出して、セグメント内の接続性を確立します。ネイバーが検出されるまで、インターフェイス上の VLAN はすべてブロックされます。ネイバーが特定されると、REP は代替ポートとなるネイバー ポートおよびトラフィックを転送するポートを決定します。

セグメントの各ポートには、一意のポート ID があります。ポート ID の形式は、スパニング ツリー アルゴリズムで使用されている ID の形式と類似しており、MAC アドレス（ネットワークで一意）に関連付けられているポート番号（ブリッジ上で一意）です。セグメント ポートがアクティブになると、LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。同じセグメント内のネイバーとスリーウェイ ハンドシェイクを実行した後、ポートが動作可能であると宣言されます。

次の場合、セグメント ポートは動作可能となりません。

- 同じセグメント ID を持つネイバーがない。
- 同じセグメント ID を持つネイバーが複数ある。
- ネイバーがローカル ポートをピアとして認識していない。

各ポートは、すぐ隣のネイバーとの隣接関係を作成します。ネイバーの隣接関係が作成されると、ポートは、セグメントのブロックされたポートを代替ポートとして決定するようネゴシエーションします。その他すべてのポートのブロックが解除されます。デフォルトでは、REP パケットは BPDU クラスの MAC アドレスに送信されます。パケットは シスコのマルチキャスト アドレスにも送信できます。シスコのマルチキャスト アドレスは、セグメントに障害がある場合、Blocked Port Advertisement（BPA）メッセージを送信する場合にだけ使用されます。パケットは、REP を実行していないデバイスによって廃棄されます。

高速コンバージェンス

REP は物理リンク ベースで動作し、VLAN 単位ベースで動作しないため、全 VLAN で必要な hello メッセージは 1 つだけとなり、プロトコルの負荷が低減します。所定のセグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許可 VLAN を設定することを推奨します。ソフトウェアでメッセージをリレーすることによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッディングすることもできます。これらのメッセージは Hardware Flood Layer（HFL）で動作し、REP セグメントだけではなくネットワーク全体ににフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体で専用の管理 VLAN を設定することにより、これらのメッセージのフラッディングを制御できます。

ファイバ インターフェイスのコンバージェンス復旧時間は、200 の VLAN が設定されているローカル セグメントで推定 200 ミリ秒未満です。VLAN ロード バランシングのコンバージェンスは 300 ミリ秒以下です。

VLAN ロード バランシング

REP セグメント内の一方のエッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。プライマリ エッジ ポートの方が、セグメント内の VLAN ロード バランシングに常に参加します、REP VLAN バランシングは、設定した代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックして実行されます。VLAN ロード バランシングを設定する場合、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

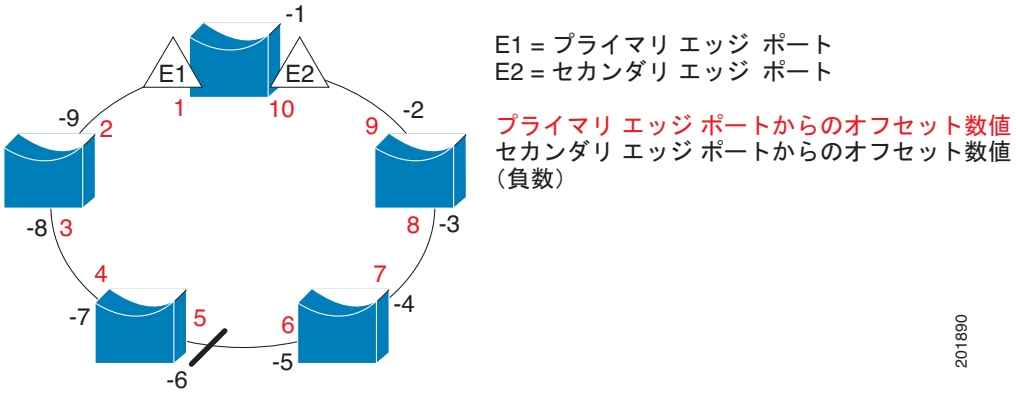
- インターフェイスのポート ID を入力する。セグメント内のポート ID を識別するには、ポートの **show interface rep detail** インターフェイス コンフィギュレーション コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力する。これにより、エッジ ポートのダウンストリーム ネイバー ポートが識別されます。ネイバー オフセット番号の範囲は、-256 ～ +256 で、値 0 は無効です。プライマリ エッジ ポートのオフセット番号は 1 です。1 を超える正の整数はプライマリ エッジ ポートのダウンストリーム ネイバーを示します。負の数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

（注） プライマリ（またはセカンダリ）エッジ ポートからポートのダウンストリーム位置を特定して、プライマリ エッジ ポートのオフセット番号を設定します。番号 1 はプライマリ エッジ ポート自体のオフセット番号であるため、オフセット番号 1 は入力しないでください。

図 18-4 に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートである場合の、セグメントのネイバー オフセット番号を示します。リング内側の赤い番号は、プライマリ エッジ ポートからのオフセット番号、リング外側の黒い番号はセカンダリ エッジ ポートからのオフセット番号です。正のオフセット番号（プライマリ エッジ ポートからのダウンストリーム位置）または負のオフセット番号（セカンダリ エッジ ポートからのダウンストリーム位置）のいずれかにより、（プライマリ エッジ ポートを除く）全ポートを識別できます。E2 がプライマリ エッジ ポートになると、オフセット番号が 1 となり、E1 が -1 となります。

- キーワード **preferred** を入力し、**rep segment** *segment-id* **preferred** インターフェイス コンフィギュレーション コマンドで優先的な代替ポートとしてすでに設定されているポートを選択します。

図 18-4　　セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN ロード バランシングを設定する際に、次の 2 つの方法のいずれかでトリガーも設定する必要があります。

- 手動で設定する。プライマリ エッジ ポートのあるスイッチ上で **rep preempt segment** *segment-id* 特権 EXEC コマンドを入力することにより、手動で VLAN ロード バランシングをいつでもトリガーできます。
- **rep preempt delay** *seconds* インターフェイス コンフィギュレーション コマンドを入力してプリエンプト遅延時間を設定する。リンク障害が発生して復旧すると、設定されたプリエンプション期間が経過した後に VLAN ロード バランシングが開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが最初からもう一度開始されることに注意してください。

（注） VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および復旧によってトリガーされるまで、動作は開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信し、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリ エッジ ポートで受信されると、ネットワークに反映され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

また、セグメント内の特定のポートに対して、すべての VLAN をブロックするように設定できます。VLAN ロード バランシングを開始するのはプライマリ エッジ ポートだけですが、セグメントが両端でエッジ ポートによって終端されていない場合は開始できません。プライマリ エッジ ポートは、ローカル VLAN ロード バランシングの設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。ロード バランシング設定を変更する場合、プライマリ エッジ ポートで **rep preempt segment** コマンドを再度待機する、またはポート障害および復旧の後で新規設定を実行する前に設定済プリエンプト遅延期間を待機します。エッジ ポートを通常のセグメント ポートに変更した場合でも、VLAN ロード バランシングの既存のステータスは変更されません。新規エッジ ポートを設定すると、新規トポロジ設定になる場合があります。

スパニング ツリー インタラクション

REP は STP または Flex Link 機能と対話はしませんが、共存は可能です。セグメントに属しているポートがスパニング ツリーの制御から削除されると、STP BPDU がセグメント ポートで受け入れられないか、送信されなくなります。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するために、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数が最小限になるように隣接するポートを設定します。各セグメントには常に、ブロックされたポートが含まれているので、セグメントが複数になればブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジ ポートの場所まで両方向に設定されたら、エッジ ポートを設定します。

REP ポート

REP セグメント内のポートは、障害、オープン、代替となります。

- 通常セグメント ポートとして設定されているポートは、障害ポートとして開始されます。
- ネイバーとの隣接関係が決定すると、ポートは代替ポート ステートに移行して、インターフェイスの全 VLAN をブロックします。ブロックされたポートのネゴシエーションが発生し、セグメントが安定すると、ブロックされたポートの 1 つは代替ロールのままになり、他のすべてのポートがオープン ポートとなります。
- リンク内に障害が発生すると、すべてのポートが障害ステートになります。代替ポートが障害通知を受信すると、オープン ステートに移行し、すべての VLAN を転送します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更があるわけではありません。エッジ ポートを通常のセグメント ポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングでは、セグメントに 2 つのエッジ ポートを設定する必要があります。

スパニング ツリー ポートとして再設定されたセグメント ポートは、スパニング ツリー設定に従って再起動します。デフォルトでは、これが指定ブロッキング ポートとなります。PortFast が設定されている場合、または STP がディセーブルの場合、ポートはフォワーディング ステートになります。

REP の設定

セグメントとはチェーン状に相互接続されているポートの集合で、セグメント ID が設定されています。REP セグメントを設定するには、REP 管理 VLAN を設定（またはデフォルト VLAN 1 を使用）し、次にインターフェイス コンフィギュレーション モードを使用してポートをセグメントに追加します。2 つのエッジ ポートをセグメント内に設定します。一方がプライマリ エッジ ポートになると、もう一方はデフォルトでセカンダリ エッジ ポートになります。1 つのセグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチ上のポートなど、セグメント内で 2 つのポートをプライマリ

エッジ ポートに設定しても、REP が選択してどちらかをセグメントのプライマリ エッジ ポートとして機能させます。また、オプションで、Segment Topology Change Notice（STCN; セグメント トポロジ変更通知）および VLAN ロード バランシングを送信する場所を設定することもできます。

- 「REP のデフォルト設定」（P.18-7）
- 「REP 設定時の注意事項」（P.18-7）
- 「REP 管理 VLAN の設定」（P.18-9）
- 「REP インターフェイスの設定」（P.18-10）
- 「VLAN ロード バランシングの手動によるプリエンプションの設定」（P.18-14）
- 「REP の SNMP トラップの設定」（P.18-14）

REP のデフォルト設定

REP はすべてのインターフェイス上でディセーブルです。イネーブルにする場合、エッジ ポートとして設定されていなければ、インターフェイスは通常セグメント ポートとなります。

REP をイネーブルにする場合、STCN の送信はディセーブルとなり、すべての VLAN がブロックされ、管理 VLAN が VLAN 1 になります。

VLAN ロード バランシングがイネーブルの場合、デフォルトは手動によるプリエンプションで、遅延タイマーはディセーブルとなります。VLAN ロード バランシングが設定されていない場合、手動によるプリエンプション後のデフォルトでは、プライマリ エッジ ポートで全 VLAN がブロックされます。

REP 設定時の注意事項

REP を設定する場合は、次の注意事項に従ってください。

- まず、1 つのポートを設定し、セグメント数とブロックされたポートの数が最小限となるように隣接ポートを設定することをお勧めします。
- 外部ネイバーが設定されておらずセグメント内で 3 つ以上のポートに障害が発生した場合、1 つのポートがデータ パスのフォワーディング ステートになり、設定時の接続性を維持する役割となります。**show rep interface** 特権 EXEC コマンド出力では、このポートのポート ロールは *Fail Logical Open* と表示されます。他の障害ポートのポート ロールは *Fail No Ext Neighbor* と表示されます。障害ポートに外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行し、代替ポート選択メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままとなります。
- REP ポートは、レイヤ 2 トランク ポートである必要があります。
- telnet 接続を経由して REP を設定する場合は注意してください。別の REP インターフェイスがメッセージを送信して VAN のブロック解除するまで、REP はすべての VLAN をブロックするため、REP インターフェイスを介してスイッチがアクセスする Telnet セッションで REP をイネーブルにすると、スイッチへの接続が失われる場合があります。
- 同じセグメントやインターフェイスでは、REP と STP または REP と Flex Link を実行できません。
- STP ネットワークを REP セグメントに接続する場合は、接続がセグメント エッジで実行されていることを確認してください。エッジで実行されていない STP 接続は、STP が REP セグメントを実行しないため、ブリッジング ループが発生する場合があります。すべての STP BPDU は、REP インターフェイスで削除されます。
- 同じ許可 VLAN セットでセグメント内のすべてのトランク ポートを設定する必要があります。そうでない場合、設定ミスが発生します。

- REP ポートは以下の規則に従います。
  - スイッチ上の REP ポート数に制限はなし。ただし同じ REP セグメントに属することができるのは、スイッチ上の 2 つのポートだけです。
  - セグメント内のスイッチ上に 1 つのポートだけが設定されている場合、そのポートがエッジ ポートとなる。
  - 同じセグメント内のスイッチに 2 つのポートがある場合、両方のポートがエッジ ポートになるか、両方のポートが通常セグメント ポートになるか、一方が通常ポートで他方がエッジ非ネイバー ポートになる。スイッチ上のエッジ ポートおよび通常セグメント ポートは同じセグメントに属することはできません。
  - スイッチ上の 2 ポートが同じセグメントに属していて、一方がエッジ ポートとして設定され、他方が通常セグメント ポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われる。
- REP インターフェイスがアクティブ化されブロックされたステートになり、ブロック解除しても安全であると通知されるまではブロックされたステートのままになります。接続が突然失われることがないよう、このことに注意する必要があります。
- REP は、ネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコ マルチキャスト アドレスに送信された BPA メッセージは、管理 VLAN で送信されます。デフォルトでは VLAN 1 です。
- ネイバーから Hello メッセージを受け取るまで REP インターフェイスがアップ状態のままである時間を設定できます。**rep lsl-age-time**r *value* インターフェイス コンフィギュレーション コマンドを使用して、時間を 120 ～ 10000 ミリ秒に設定できます。次に、LSL Hello タイマーはエージング タイマーの値を 3 で割った値に設定されます。通常の操作では、3 つの LSL Hello メッセージが、ピア スイッチのエージング タイマーの期限が経過して Hello メッセージを検索する前に送信されます。
  - Cisco IOS リリース 12.2(52)SE では、LSL エージング タイマーの範囲が 3000 ～ 10000 ミリ秒（増分 500 ミリ秒）から 120 ～ 10000 ミリ秒（増分 40 ミリ秒）に変わりました。REP 隣接デバイスが Cisco IOS リリース 12.2(52)SE 以降を稼動していない場合、デバイスが以前の範囲外の値を受け入れないため、短い時間の範囲を設定する必要があります。
  - EtherChannel ポート チャネル インターフェイスは、1000 ミリ秒未満の LSL エージング タイマーの値をサポートしていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示され、コマンドが拒否されます。
- REP ポートは、これらのポート タイプのいずれかには設定できません。
  - SPAN 宛先ポート
  - プライベート VLAN ポート
  - トンネル ポート
  - アクセス ポート
- REP ポートは、ネットワーク ノード インターフェイス（NNI）である必要があります。ユーザ ネットワーク インターフェイス（UNI）または拡張ネットワーク インターフェイス（ENI）を REP ポートにはできません。
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別ポートではサポートされていません。
- スイッチごとの REP セグメント数は最大 64 です。

REP 管理 VLAN の設定

リンク障害用のソフトウェアまたはロード バランシング中の VLAN ブロッキング通知のソフトウェアでの、メッセージのリレーによる遅延を回避するために、REP はハードウェア フラッド レイヤ（HFL）で通常のマルチキャスト アドレスにフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。ドメイン全体で管理 VLAN を設定することにより、これらのメッセージのフラッディングを制御できます。

REP 管理 VLAN を設定する場合には、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1。
- スイッチとセグメントで 1 つの管理 VLAN だけが可能。ただし、これはソフトウェアによって強制されません。
- 管理 VLAN は RSPAN VLAN にできない。

REP 管理 VLAN を設定するには、特権 EXEC モードを開始し、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rep admin vlan** *vlan-id*	管理 VLAN を指定します。指定できる範囲は 2 ～ 4094 です。デフォルトは VLAN 1 です。管理 VLAN を 1 に設定するには、**no rep admin vlan** グローバル コンフィギュレーション コマンドを実行します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show interface** [*interface-id*] **rep detail**	REP インターフェイスのいずれか 1 つの設定を確認します。
ステップ 5	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、管理 VLAN を VLAN 100 として設定し、REP インターフェイスの 1 つに **show interface rep detail** コマンドを入力して設定を確認する例を示します。

```
Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end

Switch# show interface gigabitethernet0/1 rep detail
GigabitEthernet0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
```

```
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

REP インターフェイスの設定

REP 動作は、各セグメント インターフェイスでイネーブルにし、セグメント ID を特定する必要があります。このステップは必須であり、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリ エッジ ポートおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

インターフェイス上で REP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**port-type nni**	ポートをネットワーク ノード インターフェイス（NNI）として設定します。
ステップ 4	**switchport mode trunk**	インターフェイスをレイヤ 2 トランク ポートとして設定します。

	コマンド	目的
ステップ 5	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]	インターフェイス上で REP をイネーブルにし、セグメント番号を特定します。指定できるセグメント ID の範囲は 1 ～ 1024 です。オプション キーワードが利用可能です。 **（注）** 各セグメントに 1 つのプライマリ エッジ ポートを含む、2 つのエッジ ポートを設定する必要があります。 • **edge** を入力して、ポートをエッジ ポートとして設定します。**edge** をキーワード **primary** なしで入力し、ポートをセカンダリ エッジ ポートとして設定します。各セグメントのエッジ ポートは 2 つだけです。 • （任意）**no-neighbor** を入力して、外部 REP ネイバーがないポートをエッジ ポートとして設定します。ポートはエッジ ポートのすべてのプロパティを継承します。それらのプロパティを任意のエッジ ポートと同じように設定できます。 • （任意）エッジ ポート上で、**primary** を入力してポートをプライマリ エッジ ポートとして設定し、VLAN ロード バランシングを設定できます。 **（注）** 各セグメントのプライマリ エッジ ポートは 1 つだけ設定可能ですが、2 つの異なるスイッチにエッジ ポートを設定してキーワード **primary** を両方のスイッチに入力しても、その設定は許可されます。ただし、REP はセグメント プライマリ エッジ ポートとして 1 つのポートだけを選択します。**show rep topology** 特権 EXEC コマンドを入力して、セグメントのプライマリ エッジ ポートを特定できます。 • （任意）**preferred** を入力して、ポートが優先代替ポートであるか、VLAN ロード バランシングの優先ポートであるかを設定します。 **（注）** ポートを優先に設定しても、代替ポートになるわけではありません。同等に可能性のあるポートより若干可能性が高くなるだけです。通常、以前障害が発生したポートが代替ポートとなります。
ステップ 6	**rep stcn** {**interface** *interface-id* | **segment** *id-list* | **stp**}	（任意）STCN を送信するよう、エッジ ポートを設定します。 • **interface** *interface-id* を入力し、STCN を受信するための物理インターフェイスまたはポート チャネルを指定します。 • **segment** *id-list* を入力して、STCN を受信する 1 つまたは複数のセグメントを特定します。指定できる範囲は 1 ～ 1024 です。 • **stp** を入力して、STCN を STP ネットワークに送信します。

	コマンド	目的
ステップ 7	**rep block port** {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**}	（任意）プライマリ エッジ ポートに VLAN ロード バランシングを設定し、REP 代替ポートを特定して、代替ポートでブロックされるように VLAN を設定します。 • **id** *port-id* を入力して、ポート ID で代替ポートを特定します。セグメント内の各ポートにポート ID が自動的に生成されます。**show interface** *interface-id* **rep** [**detail**] 特権 EXEC コマンドを入力し、インターフェイス ポート ID を表示できます。 • *neighbor_offset* 番号を入力し、代替ポートをエッジ ポートからのダウンストリーム ネイバーとして特定します。指定できる範囲は -256 ～ 256 で、負の数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。値 **0** は無効です。**-1** を入力して、セカンダリ エッジ ポートを代替ポートとして特定します。ネイバー オフセット番号の例については、図 18-4 (P.18-5) を参照してください。 **（注）** このコマンドはプライマリ エッジ ポート（オフセット番号 1）で入力するため、オフセット値 1 代替ポートを特定することはありません。 • **preferred** を入力して、すでに VLAN ロード バランシングの優先代替ポートとして特定されている通常セグメント ポートを選択します。 • **vlan** *vlan-list* を入力し、1 つの VLAN または VLAN の範囲をブロックします。 • **vlan all** を入力して、すべての VLAN をブロックします。 **（注）** このコマンドは、REP プライマリ エッジ ポート上にだけ入力します。
ステップ 8	**rep preempt delay** *seconds*	（任意）リンク障害および復旧後に自動的に VLAN ロード バランシングをトリガーする場合、このコマンドを入力して、プリエンプト時間遅延を設定する必要があります。時間遅延の範囲は 15 ～ 300 秒です。デフォルトは、時間遅延のない手動によるプリエンプションです。 **（注）** このコマンドは、REP プライマリ エッジ ポート上にだけ入力します。
ステップ 9	**rep lsl-age-timer** *value*	（任意）ネイバーから Hello メッセージを受け取るまで REP インターフェイスがアップのままになる時間（ミリ秒）を設定します。指定できる範囲は 120 ～ 10000 ミリ秒（増分 40 ミリ秒）で、デフォルトは 5000 ミリ秒（5 秒）です。 **（注）** 隣接デバイスが Cisco IOS リリース 12.2(52)SE 以降を稼動していない場合、指定できる値は 3000 ～ 10000 ミリ秒（増分 500 ミリ秒）となります。 EtherChannel ポート チャネル インターフェイスは、1000 ミリ秒未満の LSL エージング タイマーの値をサポートしていません。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	**show interface** [*interface-id*] **rep** [**detail**]	REP インターフェイスの設定を確認します。
ステップ 12	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各コマンドの **no** 形式を入力します。**show rep topology** 特権 EXEC コマンドを入力して、セグメント内のプライマリ エッジ ポートであるポートを確認します。

次に、インターフェイスをセグメント 1 のプライマリ エッジ ポートに設定し、STCN をセグメント 2 ～ 5 に送信、代替ポートを ポート ID 0009001818D68700 のポートとして設定して、セグメント ポート障害および復旧後のプリエンプション遅延 60 秒後にすべての VLAN をブロックする例を示します。インターフェイスは、ネイバーからの Hello メッセージを受信するまで 6000 ミリ秒間アップ状態であるよう設定されます。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end
```

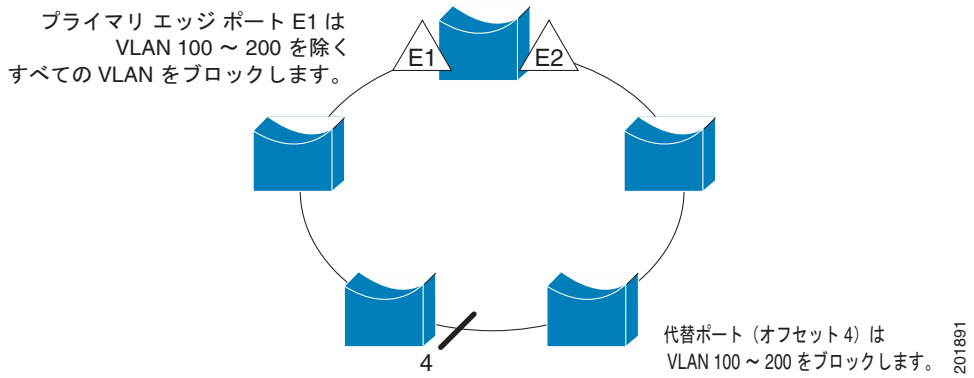
次に、インターフェイスに外部 REP ネイバーがない場合に同じ設定を行う方法の例を示します。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
```

図 18-5 に、VLAN ブロッキング コンフィギュレーションを設定する例を示します。代替ポートは、ネイバー オフセット番号 4 のネイバーです。手動によるプリエンプションのあと、VLAN 100 ～ 200 がこのポートでブロックされ、その他のすべての VLAN がプライマリ エッジ ポート E1（ギガビット イーサネット ポート 0/1）でブロックされます。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

図 18-5　VLAN ブロッキングの例



VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリ エッジ ポートで **rep preempt delay** *seconds* インターフェイス コンフィギュレーション コマンドを入力せず、プリエンプション時間遅延を設定するには、デフォルトで、セグメントで VLAN ロード バランシングを手動でトリガーします。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了していることを確認してください。**rep preempt segment** *segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する場合があるため、コマンドの実行前に確認メッセージが表示されます。

セグメント上で手動により VLAN ロード バランシングをトリガーするには、特権 EXEC モードを開始し、セグメント プライマリ エッジ ポートのあるスイッチのセグメント上で次の手順を実行します。

	コマンド	目的
ステップ 1	**rep preempt segment** *segment-id*	手動でセグメント上の VLAN ロード バランシングをトリガーします。 実行前にコマンドを確認する必要があります。
ステップ 2	**show rep topology**	REP トポロジ情報を表示します。

REP の SNMP トラップの設定

リンク動作ステータス変更およびポート ロール変更について SNMP サーバに通知するため、REP 固有のトラップを送信するようにスイッチを設定できます。REP トラップを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp mib rep trap-rate** *value*	スイッチで REP トラップの送信をイネーブルにし、1 秒あたりのトラップの送信数を設定します。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 です（制限はなく、トラップは発生するたびに送信されます）。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	REP トラップの設定を確認します。
ステップ 5	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

トラップを削除するには、**no snmp mib rep trap-rate** グローバル コンフィギュレーション コマンドを入力します。

次に、1 秒あたり 10 の割合で REP トラップを送信するようにスイッチを設定する例を示します。

```
Switch(config)# snmp mib rep trap-rate 10
```

REP のモニタリング

REP を監視するには、表 18-1 に示す特権 EXEC コマンドを使用します。

表 18-1　REP モニタリング コマンド

コマンド	目的
show interface [*interface-id*] **rep** [**detail**]	指定のインターフェイスまたはすべてのインターフェイスの REP 設定およびステータスを表示します。
show rep topology [**segment** *segment_id*] [**archive**] [**detail**]	セグメントに含まれるプライマリ エッジポートおよびセカンダリ エッジ ポートなど、1 つのセグメントまたはすべてのセグメントの REP トポロジ情報を表示します。

CHAPTER 19

Flex Link および MAC アドレス テーブル移行更新機能の設定

この章では、Flex Link の設定方法について説明します。これは、Cisco ME 3400E スイッチ上のインターフェイスのペアで、相互バックアップに使用します。また、MAC（メディア アクセス制御）アドレス テーブル移行更新機能の設定についても説明します。これは、Flex Link 双方向高速コンバージェンス機能とも呼ばれます。

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

この章で説明する内容は、次のとおりです。

- 「Flex Link および MAC アドレス テーブル移行更新機能の概要」（P.19-1）
- 「Flex Link および MAC アドレス テーブル移行更新機能の設定」（P.19-8）
- 「Flex Link および MAC アドレス テーブル移行更新機能のモニタリング」（P.19-15）

Flex Link および MAC アドレス テーブル移行更新機能の概要

- 「Flex Link」（P.19-1）
- 「VLAN Flex Link のロード バランシングおよびサポート」（P.19-2）
- 「Flex Link マルチキャスト高速コンバージェンス」（P.19-3）
- 「MAC アドレス テーブル移行更新」（P.19-7）

Flex Link

Flex Link は、レイヤ 2 インターフェイス（スイッチポートまたはポート チャネル）のペアで、1 つのインターフェイスがもう一方のバックアップとして機能するように設定されています。この機能は、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）の代替ソリューションとして提供され、ユーザが STP をオフにしても、基本的なリンク冗長性は確保されます。Flex Link は、通常、カスタマーがスイッチで STP の実行を望まないサービス プロバイダーまたは企業のネットワークに設定されます。スイッチが STP を実行中の場合、STP がすでにリンク レベルの冗長性またはバックアップを提供しているので Flex Link の設定は必要ありません。

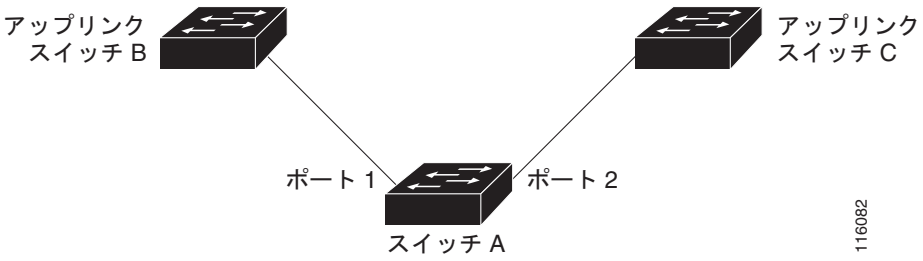
（注）　STP は、Network Node Interface（NNI; ネットワーク ノード インターフェイス）上で、デフォルトでイネーブルに設定されています。Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）ではディセーブルに設定されていますが、イネーブルにできます。STP は、User Network Interface（UNI; ユーザネットワーク インターフェイス）ではサポートされていません。

別のレイヤ 2 インターフェイスを Flex Link またはバックアップ リンクとして割り当てることで、1 つのレイヤ 2 インターフェイス（アクティブ リンク）に Flex Link を設定します。リンクの 1 つがアップでトラフィックを転送しているときはもう一方のリンクがスタンバイ モードで、もう一方のリンクがシャット ダウンした場合にトラフィックの転送を開始できるように準備しています。どの時点でも、1 つのインターフェイスだけがリンクアップ ステートでトラフィックを転送しています。プライマリ リンクがシャットダウンすると、スタンバイ リンクがトラフィックの転送を開始します。アクティブ リンクがアップに戻ると、スタンバイ モードになりトラフィックを転送しません。STP は Flex Link インターフェイスでディセーブルです。

図 19-1 では、スイッチ A のポート 1 およびポート 2 がアップリンク スイッチ B およびアップリンク スイッチ C に接続されています。これらのスイッチは Flex Link として設定されているので、どちらかのインターフェイスがトラフィックを転送し、もう一方のインターフェイスはスタンバイ モードになります。ポート 1 がアクティブ リンクになる場合、ポート 1 とスイッチ B との間でトラフィックの転送を開始し、ポート 2 とスイッチ C との間のリンク（バックアップ リンク）ではトラフィックは転送されません。ポート 1 がダウンした場合はポート 2 がアップし、トラフィックをスイッチ C に転送し始めます。ポート 1 は、再びアップになってもスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィック転送を続けます。

また、トラフィック転送に優先ポートを指定して、プリエンプト メカニズムを設定するように選択できます。たとえば図 19-1 では、Flex Link ペアをプリエンプト モードで設定できます。このシナリオでは、ポート 1 がバック アップ状態になったあと、ポート 1 の帯域幅がポート 2 よりも大きい場合、ポート 1 は 60 秒後に転送を開始し、ポート 2 はスタンバイになります。これは、**switchport backup interface preemption mode bandwidth** および **switchport backup interface preemption delay** インターフェイス コンフィギュレーション コマンドを入力することによって、実行されます。

図 19-1　　Flex Link 設定例



プライマリ（転送）リンクがダウンした場合、トラップがネットワーク管理ステーションに通知します。スタンバイ リンクがダウンした場合、トラップがユーザに通知します。

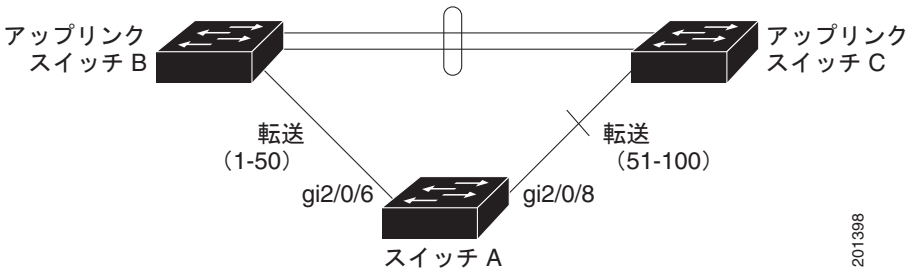
Flex Link はレイヤ 2 ポートおよびポート チャネルでだけサポートされ、VLAN やレイヤ 3 ポートではサポートされません。

VLAN Flex Link のロード バランシングおよびサポート

VLAN Flex Link のロード バランシングにより、両方のポートが相互に排他的な VLAN のトラフィックを同時に転送するように、Flex Link ペアを設定できます。たとえば、Flex Link ポートが 1 ～ 100 の VLAN に設定されている場合、最初の 50 個の VLAN のトラフィックを 1 つのポートで転送し、残り

のトラフィックを他のポートで転送することができます。1 つのポートに障害が発生した場合、もう 1 つのアクティブなポートがすべてのトラフィックを転送します。障害が発生したポートが稼動状態に戻ると、優先 VLAN のトラフィックの転送が再開されます。このように、冗長性の提供とは別に、この Flex Link ペアは、ロード バランシングに使用できます。また、Flex Link VLAN のロード バランシングでは、アップリンク スイッチが制限されません。

図 19-2　　VLAN Flex Link ロード バランシングの設定例



Flex Link マルチキャスト高速コンバージェンス

Flex Link マルチキャスト高速コンバージェンスを使用すれば、Flex Link に障害が発生した後のマルチキャスト トラフィック コンバージェンス時間が短縮されます。この機能は、次のソリューションの組み合せで実装します。

- 「他の Flex Link ポートの mrouter ポートとしての学習」（P.19-3）
- 「IGMP レポートの生成」（P.19-4）
- 「IGMP レポートの通過許可」（P.19-4）

他の Flex Link ポートの mrouter ポートとしての学習

一般的なマルチキャスト ネットワークでは、VLAN ごとにクエリアが存在します。ネットワークのエッジに配置されたスイッチには、クエリーを受信する Flex Link ポートの 1 つが用意されています。また、Flex Link ポートでは、どの時点においても、常に転送が実行されます。

クエリーを受信するポートが、スイッチに *mrouter* ポートとして追加されます。mrouter ポートは、スイッチによって学習されるすべてのマルチキャスト グループの一部です。切り替え後、クエリーは、別の Flex Link ポートによって受信されます。次に、別の Flex Link ポートが mrouter ポートとして学習されます。切り替え後、マルチキャスト トラフィックは、別の Flex Link ポートを通るようになります。トラフィックのコンバージェンスを高速化するために、片方の Flex Link ポートが mrouter ポートとして学習されると必ず、両方の Flex Link ポートが mrouter ポートとして学習されます。両方の Flex Link ポートは、常にマルチキャスト グループの一部となります。

通常の動作モードでは、両方の Flex Link ポートはグループの一部ですが、バックアップ ポート上のすべてのトラフィックはブロックされます。そのため、通常のマルチキャスト データ フローは、バックアップ ポートを mrouter ポートとして追加しても影響を受けません。切り替えが発生すると、バックアップ ポートのブロックが解除され、トラフィックのフローが許可されます。この場合、バックアップ ポートのブロックが解除されると同時に、アップストリーム マルチキャスト データが通過します。

IGMP レポートの生成

切り替え後にバックアップ リンクが起動しても、アップストリームの新しいディストリビューション スイッチでは、マルチキャスト データの転送は開始されません。ブロックされている Flex Link ポートに接続されているアップストリーム ルータ上のポートが、いずれのマルチキャスト グループの一部でもないからです。バックアップ リンクがブロックされているため、マルチキャスト グループのレポートは、ダウンストリーム スイッチによって転送されることはありません。データは、このポートがマルチキャスト グループを学習するまで通過しません。学習が行われるのは、このポートがレポートを受信した後だけです。

一般クエリーが受信されるとレポートがホストによって送信され、通常のシナリオでは、一般クエリーが 60 秒以内に送信されます。バックアップ リンクが転送を開始すると、ダウンストリーム スイッチは、マルチキャスト データのコンバージェンスを高速化するために、一般クエリーを待つことなく、このポート上のすべての学習済みグループのプロキシ レポートを即座に送信します。

IGMP レポートの通過許可

マルチキャスト トラフィック コンバージェンスを最小限のロスで実現するには、Flex Link アクティブ リンクがダウンする前に、冗長データパスを設定する必要があります。そのためには、Flex Link バックアップ リンク上で IGMP レポート パケットだけに通過を許可します。これらの通過を許可された IGMP レポート メッセージは、アップストリーム配信ルータによって処理され、その結果、マルチキャスト データ トラフィックは、バックアップ インターフェイスに転送されます。バックアップ インターフェイス上のすべての着信トラフィックは、アクセス スイッチの入力で破棄されるので、ホストによって受信されるマルチキャスト トラフィックが重複することはありません。Flex Link アクティブ リンクに障害が発生すると同時に、アクセス スイッチでは、バックアップ リンクからのトラフィックの受信が開始されます。このスキームの唯一の欠点は、ディストリビューション スイッチ間のリンク、および、ディストリビューション スイッチとアクセス スイッチとの間のバックアップ リンク上の帯域幅が消費されるということです。この機能はデフォルトでディセーブルになっており、**switchport backup interface** *interface-id* **multicast fast-convergence** コマンドを使用して設定できます。

この機能が切り替え時にイネーブルになっていても、スイッチでは、フォワーディング ポートになったバックアップ ポート上にプロキシ レポートは生成されません。

設定例

次に、Flex Link が GigabitEthernet 0/11 および GigabitEthernet 0/12 上で設定されているときに、他の Flex Link ポートを mrouter ポートとして学習する設定例を示します。この例では、**show interfaces switchport backup** コマンドの出力を示しています。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface Gi0/12
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

次の出力は、VLAN 1 および VLAN 401 のクエリアを示しています。これらのクエリーは、GigabitEthernet 0/11 を介してスイッチに到達しています。

```
Switch# show ip igmp snooping querier
Vlan    IP Address      IGMP Version       Port
-----------------------------------------------------------
1       1.1.1.1         v2                 Gi0/11
401     41.41.41.1      v2                 Gi0/11
```

これは、VLAN 1 および VLAN 401 に対する **show ip igmp snooping mrouter** コマンドの出力です。

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
1       Gi1/0/11(dynamic), Gi0/12(dynamic)
401     Gi1/0/11(dynamic), Gi0/12(dynamic)
```

同様に、両方の Flex Link ポートは、学習済みグループの一部です。この例では、GigabitEthernet 0/10 が VLAN 1 におけるレシーバー / ホストであり、2 つのマルチキャスト グループを対象とします。

```
Switch# show ip igmp snooping groups
Vlan    Group       Type    Version     Port List
------------------------------------------------------------------------
1       228.1.5.1   igmp    v2          Gi0/11, Gi0/12, Gi0/10
1       228.1.5.2   igmp    v2          Gi0/11, Gi0/12, Gi0/10
```

ホストが一般クエリーに応答すると、スイッチが、すべての mrouter ポート上のこのレポートを転送します。この例では、ホストによって、グループ 228.1.5.1 のレポートが送信されると、GigabitEthernet 0/11 上でだけ転送が行われます。バックアップ ポート GigabitEthernet 0/12 がブロックされているためです。アクティブ リンクである GigabitEthernet 0/11 がダウンすると、バックアップ ポートである GigabitEthernet 0/12 で転送が開始されます。

このポートで転送が開始されると同時に、スイッチが、ホストの代わりに、グループ 228.1.5.1 および 228.1.5.2 のプロキシ レポートを送信します。アップストリーム ルータによって各グループが学習され、マルチキャスト データの転送が開始されます。これは、Flex Link のデフォルトの動作です。ユーザが、**switchport backup interface gigabitEthernet 0/12 multicast fast-convergence** コマンドを使用して高速コンバージェンスを設定すると、この動作は変更されます。次に、この機能をオンにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet0/11
Switch(config-if)# switchport backup interface gigabitEthernet0/12 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active                Interface             Backup Interface State
------------------------------------------------------------------------
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

次の出力は、VLAN 1 および VLAN 401 のクエリアを示しています。これらのクエリーは、GigabitEthernet 0/11 を介してスイッチに到達しています。

```
Switch# show ip igmp snooping querier
Vlan       IP Address      IGMP Version   Port
-----------------------------------------------------------
1          1.1.1.1         v2             Gi0/11
```

```
401         41.41.41.1      v2              Gi0/11
```

これは、VLAN 1 および VLAN 401 に対する **show ip igmp snooping mrouter** コマンドの出力です。

```
Switch# show ip igmp snooping mrouter
Vlan        ports
----        -----
1           Gi0/11(dynamic), Gi0/12(dynamic)
401         Gi0/11(dynamic), Gi0/12(dynamic)
```

同様に、両方の Flex Link ポートは学習済みグループの一部です。この例では、GigabitEthernet 0/10 が VLAN 1 におけるレシーバー / ホストであり、2 つのマルチキャスト グループを対象とします。

```
Switch# show ip igmp snooping groups
Vlan    Group       Type    Version     Port List
------------------------------------------------------------------------
1       228.1.5.1   igmp    v2          Gi0/11, Gi0/12, Gi0/10
1       228.1.5.2   igmp    v2          Gi1/0/11, Gi0/12, Gi0/10
```

ホストが一般クエリーに応答するときは必ず、スイッチが、すべての mrouter ポート上のこのレポートを転送します。コマンドライン ポートを介してこの機能をオンにし、GigabitEthernet 0/11 上のスイッチによってレポートが転送されると、そのレポートはバックアップ ポート GigabitEthernet 0/12 に対しても通過を許可されます。アップストリーム ルータによって各グループが学習され、マルチキャスト データの転送が開始されます。GigabitEthernet 0/12 はブロックされているので、このデータは入力時に破棄されます。アクティブ リンクである GigabitEthernet 0/11 がダウンすると、バックアップ ポートである GigabitEthernet 0/12 で転送が開始されます。マルチキャスト データは、アップストリーム ルータによってすでに転送されているので、プロキシレ ポートを送信する必要はありません。レポートに対してバックアップ ポートへの通過を許可することによって、冗長マルチキャスト パスが設定されているので、マルチキャスト トラフィック コンバージェンスにかかる時間は極めて短くなっています。

MAC アドレス テーブル移行更新

MAC アドレス テーブル移行更新機能により、プライマリ（転送）リンクがダウンし、スタンバイ リンクがトラフィックの転送を開始した場合に、双方向の高速コンバージェンスが提供されます。

図 19-3 では、スイッチ A はアクセス スイッチで、スイッチ A のポート 1 および 2 は Flex Link ペアを介してアップリンク スイッチ B およびアップリンク スイッチ D と接続されています。ポート 1 がトラフィックを転送し、ポート 2 はバックアップ ステートです。PC からサーバへのトラフィックは、ポート 1 からポート 3 に転送されます。PC の MAC アドレスは、スイッチ C 上のポート 3 で学習されます。サーバから PC へのトラフィックは、ポート 3 からポート 1 に転送されます。

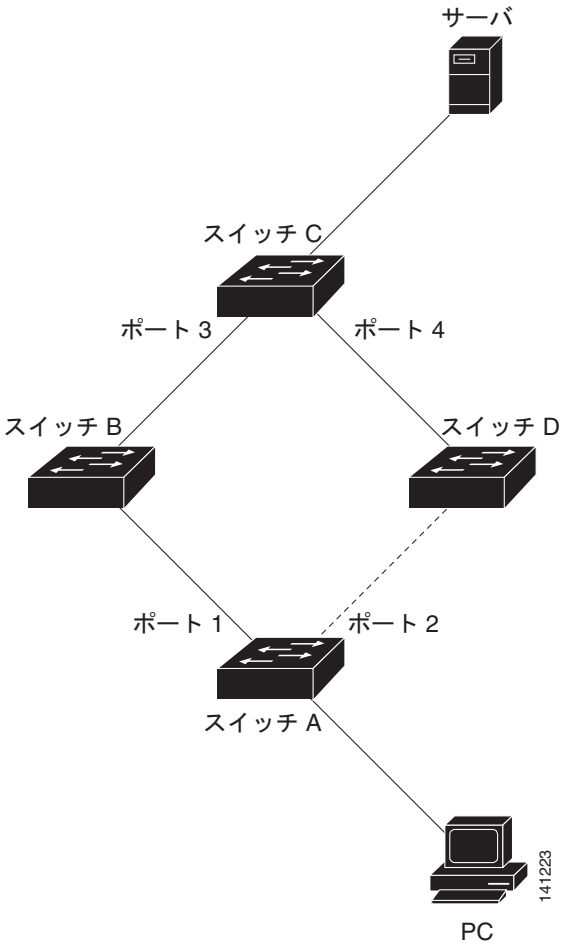
MAC アドレス テーブル移行更新機能が設定されていない場合にポート 1 がダウンすると、ポート 2 がトラフィックの転送を開始します。ただし、スイッチ C はポート 3 を介してサーバから PC へのトラフィックの転送を一時的に維持します。また、ポート 1 がダウンしているため、PC はトラフィックを受け取りません。スイッチ C がポート 3 上の PC の MAC アドレスを削除し、ポート 4 上で再学習すると、ポート 2 を介してサーバから PC にトラフィックを転送できます。

図 19-3 のスイッチで、MAC アドレス テーブル移行更新機能が設定されていて、イネーブルの場合に、ポート 1 がダウンすると、ポート 2 が PC からサーバへのトラフィックの転送を開始します。スイッチは、ポート 2 から MAC アドレス テーブル移行更新パケットを送信します。スイッチ C はポート 4 でこのパケットを受け取り、ただちにポート 4 上で PC の MAC アドレスを学習します。これにより、再コンバージェンス時間が短縮されます。

アクセス スイッチであるスイッチ A が、MAC アドレス テーブル移行更新メッセージを*送信する*ように設定できます。また、アップリンク スイッチ B、C、および D が、MAC アドレス テーブル移行更新メッセージを*受け取り*、処理するように設定できます。スイッチ C が、スイッチ A からの MAC アドレス テーブル移行更新メッセージを受け取ると、スイッチ C はポート 4 で PC の MAC アドレスを学習します。スイッチ C は、PC の転送テーブルのエントリを含む MAC アドレス テーブルを更新します。

スイッチ A が、MAC アドレス テーブル更新を待機する必要はありません。スイッチによってポート 1 における障害が検出されると、ただちに、新しいフォワーディング ポートであるポート 2 からのサーバ トラフィックの転送が開始されます。この変更は 100 ミリ秒（ms）内に行われます。PC はスイッチ A に直接接続されており、接続ステータスは変更されません。スイッチ A が、MAC アドレス テーブル内の PC エントリを更新する必要はありません。

図 19-3　MAC アドレス テーブル移行更新の例



Flex Link および MAC アドレス テーブル移行更新機能の設定

- 「デフォルト設定」（P.19-8）
- 「設定時の注意事項」（P.19-9）
- 「Flex Link の設定」（P.19-10）
- 「Flex Link での VLAN ロード バランシングの設定」（P.19-12）
- 「MAC アドレス テーブル移行更新機能の設定」（P.19-13）

デフォルト設定

Flex Link は設定されておらず、バックアップ インターフェイスは定義されていません。

プリエンプト モードはオフです。

プリエンプト遅延は 35 秒です。

Flex Link VLAN ロード バランシングが設定されていません。

MAC アドレス テーブル移行更新機能は、スイッチで設定されていません。

設定時の注意事項

Flex Link の設定時には、次の注意事項に従ってください。

- 最大で 16 のバックアップ リンクを設定できます。
- アクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスは、1 つのアクティブ リンクに対してのみバックアップ リンクになれます。アクティブ リンクは別の FLex Link ペアに属することはできません。
- いずれのリンクも EtherChannel に属するポートにはなれません。ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルと物理インターフェイスを Flex Link として設定でき、ポート チャネルまたは物理インターフェイスをアクティブ リンクにできます。
- バックアップ リンクはアクティブ リンクと同じタイプ（ファスト イーサネット、ギガビット イーサネット、またはポート チャネル）にする必要はありません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の FLex Link を似たような特性で設定する必要があります。
- STP は Flex Link ポートでディセーブルです。スイッチ上で STP が設定されている場合でも、Flex Link は STP が設定されているすべての VLAN の STP に参加しません。STP が実行されていない場合、設定されているトポロジでループがないかを確認してください。

（注） STP を使用できるのは、NNI または ENI 上だけです。

Flex Link 機能に VLAN ロード バランシングを設定するには、次の注意事項に従ってください。

- Flex Link VLAN ロード バランシングでは、バックアップ インターフェイスで優先 VLAN を選択する必要があります。
- 同じ Flex Link のインターフェイス ペアに、プリエンプト メカニズムと VLAN ロード バランシングの両方は設定できません。

MAC アドレス テーブル移行更新機能の設定時には、次の注意事項に従ってください。

- アクセス スイッチでこの機能をイネーブルにして設定すると、MAC アドレス テーブル移行更新を*送信*できます。
- アップリンク スイッチでこの機能をイネーブルにして設定すると、MAC アドレス テーブル移行更新を*受信*できます。

Flex Link の設定

Flex Link のペアを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、ネットワーク NNI はイネーブルに設定されています。
ステップ 4	**switchport backup interface** *interface-id*	物理レイヤ 2 インターフェイス（ポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interface** [*interface-id*] **switchport backup**	設定を確認します。
ステップ 7	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスをバックアップ インターフェイスに設定して設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# no shutdown
Switch(conf-if)# switchport backup interface fastethernet0/2
Switch(conf-if)# end
Switch# show interface switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------------------------
FastEthernet0/1         FastEthernet0/2         Active Up/Backup Standby
FastEthernet0/3         FastEthernet0/4         Active Up/Backup Standby
Port-channel1           GigabitEthernet0/1      Active Up/Backup Standby
```

Flex Link のペアにプリエンプト スキームを設定するには、インターフェイス コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネル範囲は 1 ～ 48 です。

	コマンド	目的
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport backup interface** *interface-id*	物理レイヤ 2 インターフェイス（ポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 5	**switchport backup interface** *interface-id* **preemption mode** {**forced** | **bandwidth** | **off**}	Flex Link のインターフェイス ペアに、プリエンプト メカニズムおよびプリエンプト遅延を設定します。プリエンプトは、次のように設定できます。 • **forced**：アクティブ インターフェイスは常に、バックアップをプリエンプトします。 • **bandwidth**：より高い帯域幅を持つインターフェイスが常に、アクティブ インターフェイスとして動作します。 • **off**：アクティブからバックアップへのプリエンプトは発生しません。
ステップ 6	**switchport backup interface** *interface-id* **preemption delay** *delay-time*	特定のポートが別のポートをプリエンプトするまでの遅延時間を設定します。 **（注）** 遅延時間の設定は、forced および bandwidth モードだけで機能します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show interface** [*interface-id*] **switchport backup**	設定を確認します。
ステップ 9	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、バックアップ インターフェイス ペアに対して、プリエンプト モードを *forced* として設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2 preemption mode forced
Switch(conf-if)# switchport backup interface gigabitethernet0/2 preemption delay 50
Switch(conf-if)# end

Switch# show interface switchport backup detail
Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet0/1 GigabitEthernet0/2 Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2)
Mac Address Move Update Vlan : auto
```

Flex Link での VLAN ロード バランシングの設定

Flex Link に VLAN ロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport backup interface** *interface-id* **prefer vlan** *vlan-range*	物理レイヤ 2 インターフェイス（または、ポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定し、インターフェイス上で実行される VLAN を指定します。VLAN ID の範囲は 1 ～ 4094 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] **switchport backup**	設定を確認します。
ステップ 7	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次の例では、VLAN 1 ～ 50、60、および 100 ～ 120 がスイッチに設定されています。

```
Switch(config)# interface gigabitEthernet 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

両方のインターフェイスが起動している場合、gigabitethernet port 0/8 が VLAN 60 および 100 ～ 120 のトラフィックを転送し、gigabitethernet port 0/6 が VLAN 1 ～ 50 のトラフィックを転送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は Flex Link ペアのピア インターフェイスに移動します。この例では、gigabitethernet port 0/6 がダウンした場合、gigabitethernet port 0/8 が Flex Link ペアのすべての VLAN を移動します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス 0/6 が起動する場合、このインターフェイスで優先される VLAN がピア インターフェイス 0/8 でブロックされ、0/6 で転送されます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet 0/3       FastEthernet 0/4       Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode  : off
Bandwidth : 10000 Kbit (Fa 0/3), 100000 Kbit (Fa0/4)
Mac Address Move Update Vlan : auto
```

MAC アドレス テーブル移行更新機能の設定

ここでは、次の情報について説明します。

- スイッチの MAC アドレス テーブル移行更新の送信設定
- スイッチの MAC アドレス テーブル移行更新の受信設定

MAC アドレス テーブル移行更新を送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**switchport backup interface** *interface-id* または **switchport backup interface** *interface-id* **mmu primary vlan** *vlan-id*	物理レイヤ 2 インターフェイス（ポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。MAC アドレス テーブル移行更新の VLAN は、インターフェイス上で最も小さい VLAN ID です。 物理レイヤ 2 インターフェイス（またはポート チャネル）を設定して、MAC アドレス テーブル移行更新の送信に使用される、インターフェイス上の VLAN ID を指定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 5	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**mac address-table move update transmit**	プライマリ リンクがダウンして、スイッチがスタンバイ リンクを介してトラフィックの転送を開始する場合に、アクセス スイッチをイネーブルにして、ネットワーク内の他のスイッチに MAC アドレス テーブル移行更新を送信するようにします。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show mac address-table move update**	設定を確認します。
ステップ 9	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブル移行更新機能をディセーブルにするには、**no mac address-table move update transmit** インターフェイス コンフィギュレーション コマンドを使用します。MAC アドレス テーブル移行更新情報を表示するには、**show mac address-table move update** 特権 EXEC コマンドを使用します。

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次に、設定を確認する例を示します。

```
Switch# show mac-address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
```

```
Xmt last interface : None
```

MAC アドレス テーブル移行更新メッセージを受信して、処理するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table move update receive**	スイッチをイネーブルにして、MAC アドレス テーブル移行更新を受信して、処理するようにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table move update**	設定を確認します。
ステップ 5	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブル移行更新機能をディセーブルにするには、**no mac address-table move update receive** コンフィギュレーション コマンドを使用します。MAC アドレス テーブル移行更新情報を表示するには、**show mac address-table move update** 特権 EXEC コマンドを使用します。

次に、スイッチが MAC アドレス テーブル移行更新メッセージを受信して処理するよう設定する例を示します。

Flex Link および MAC アドレス テーブル移行更新機能のモニタリング

表 19-1 に、Flex Link 設定のモニタリング用の特権 EXEC コマンドを示します。

表 19-1　Flex Link モニタリングするためのコマンド

コマンド	目的
show interface [*interface-id*] **switchport backup**	あるインターフェイス用に設定された Flex Link バックアップ インターフェイス、またはスイッチ上で設定されたすべての Flex Link と、各アクティブおよびバックアップ インターフェイスの状態（アップまたはスタンバイ モード）を表示します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

CHAPTER 20

DHCP 機能および IP ソース ガードの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチ上における、DHCP スヌーピング機能、Option 82 データ挿入機能、および DHCP サーバ ポートベース アドレス割り当て機能の設定方法について説明します。また、IP ソース ガード機能の設定方法についても説明します。

(注) この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』*Release 12.2* の「DHCP Commands」を参照してください。

- 「DHCP 機能の概要」（P.20-1）
- 「DHCP 機能の設定」（P.20-7）
- 「DHCP スヌーピング情報の表示」（P.20-15）
- 「DHCP サーバ ポートベース アドレス 割り当て」（P.20-16）
- 「DHCP サーバ ポートベース アドレス 割り当ての設定」（P.20-16）
- 「DHCP サーバ ポートベース アドレス 割り当ての表示」（P.20-19）
- 「IP ソース ガードの概要」（P.20-20）
- 「IP ソース ガードの設定」（P.20-22）
- 「IP ソース ガード情報の表示」（P.20-30）

DHCP 機能の概要

DHCP は、中央のサーバからホストの IP アドレスをダイナミックに割り当てるために、LAN 環境で広範囲に使用されています。この機能により、IP アドレス管理のオーバーヘッドを著しく軽減できます。また、DHCP により、IP アドレスをホストに永続的に割り当てる必要がなくなり、ネットワークに接続しているホストだけが IP アドレスを使用するので、制限のある IP アドレス スペースの節約に役立ちます。

- 「DHCP サーバ」（P.20-2）
- 「DHCP リレー エージェント」（P.20-2）
- 「DHCP スヌーピング」（P.20-2）
- 「Option 82 データ挿入」（P.20-3）
- 「Cisco IOS DHCP サーバ データベース」（P.20-6）
- 「DHCP スヌーピング バインディング データベース」（P.20-6）

DHCP クライアントの詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「*IP Addressing and Services*」の章の「*Configuring DHCP*」を参照してください。

DHCP サーバ

DHCP サーバは、スイッチまたはルータにある指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、管理します。DHCP サーバが要求された設定パラメータをデータベースから DHCP クライアントに付与できない場合、その要求はネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに転送されます。

DHCP リレー エージェント

DHCP リレー エージェントは、DHCP パケットをクライアントとサーバ間で転送するレイヤ 3 デバイスです。リレー エージェントは、クライアントとサーバが同じ物理サブネット上にない場合に、両者間で要求と応答の転送を行います。リレー エージェント転送は、IP データグラムがネットワーク間で透過的にスイッチングされる通常のレイヤ 2 転送とは異なります。リレー エージェントは DHCP メッセージを受信し、新しい DHCP メッセージを生成して出力インターフェイスで送信します。

DHCP スヌーピング

DHCP スヌーピングは、DHCP のセキュリティ機能で、信頼できない DHCP メッセージをフィルタリングし、DHCP スヌーピング バインディング データベース（DHCP スヌーピング バインディング テーブル）を構築し、維持することで、ネットワーク セキュリティを提供します。このデータベースの詳細については、「DHCP スヌーピング情報の表示」（P.20-15）を参照してください。

DHCP スヌーピングは、信頼できないホストと DHCP サーバ間でファイアウォールに似た機能を果たします。エンドユーザに接続する信頼できないインターフェイスと、DHCP サーバまたは他のスイッチに接続する信頼できるインターフェイスとを区別するのに DHCP スヌーピングを使用します。

（注）　DHCP スヌーピングが正常に機能するために、すべての DHCP サーバを信頼できるインターフェイスを介してスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、ネットワークまたはファイアウォールの外で受信されたメッセージです。サービス プロバイダー環境で DHCP スヌーピングを使用する場合、信頼できないメッセージは、カスタマーのスイッチなど、サービス プロバイダー ネットワークにないデバイスから送信されたものです。不明なデバイスからのメッセージは、トラフィック攻撃の送信元の可能性があるので、信頼できません。

DHCP スヌーピング バインディング データベースには MAC（メディア アクセス制御）アドレス、IP アドレス、リース時間、バインディング タイプ、VLAN（仮想 LAN）番号、およびスイッチ上のローカルにある信頼できないインターフェイスに対応するインターフェイス情報があります。これには、信頼できるインターフェイスに相互接続しているホストに関する情報はありません。

サービス プロバイダー ネットワークでは、信頼できるインターフェイスは同じネットワーク内のデバイスのポートに接続されています。信頼できないインターフェイスは、ネットワーク内の信頼できないインターフェイスまたはそのネットワークにはないデバイス上のインターフェイスに接続されています。

スイッチが信頼できないインターフェイス上でパケットを受信し、そのインターフェイスが属する VLAN で DHCP スヌーピングがイネーブルの場合、スイッチは送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスとを比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットを廃棄します。

スイッチは、次のような状況が発生した場合に DHCP パケットを廃棄します。

- DHCPOFFER、DHCPACK、DHCPNAK、または DHCPLEASEQUERY パケットなどの、DHCP サーバからのパケットがネットワークまたはファイアウォールの外で受信された場合
- パケットが信頼できないインターフェイスで受信され、送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合
- DHCP スヌーピング バインディング データベースにある MAC アドレスを持つ DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージをスイッチが受信するものの、バインディング データベース内のインターフェイス情報が、メッセージが受信されたインターフェイスと一致しない場合
- DHCP リレー エージェントが 0.0.0.0 でないリレー エージェント IP アドレスが含まれる DHCP パケットを転送するか、またはリレー エージェントが Option 82 情報が含まれるパケットを信頼できないポートに転送する場合

DHCP スヌーピングをサポートする集約スイッチが DHCP Option 82 情報の挿入元のエッジ スイッチに接続されている場合、パケットが信頼できないインターフェイスに着信したときに、Option 82 情報が含まれるパケットは廃棄されます。DHCP スヌーピングがイネーブル化されているときに、パケットが信頼できないポートに着信した場合、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを取得せず、完全な DHCP スヌーピング バインディング データベースを構築できません。

信頼できないインターフェイスを介して集約スイッチをエッジ スイッチに接続できるときに、**ip dhcp snooping information option allowed-trust** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スイッチから送信された Option 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチ インターフェイスを介して接続されたホストのバインディングを取得します。スイッチが、ホストが接続されている信頼できない入力インターフェイス上で Option 82 情報を含むパケットを受信する場合は、集約スイッチ上で、ダイナミック ARP 検査や IP ソース ガードなどの DHCP セキュリティ機能をイネーブルにできます。集約スイッチに接続されたエッジ スイッチのポートは、信頼できるインターフェイスとして設定する必要があります。

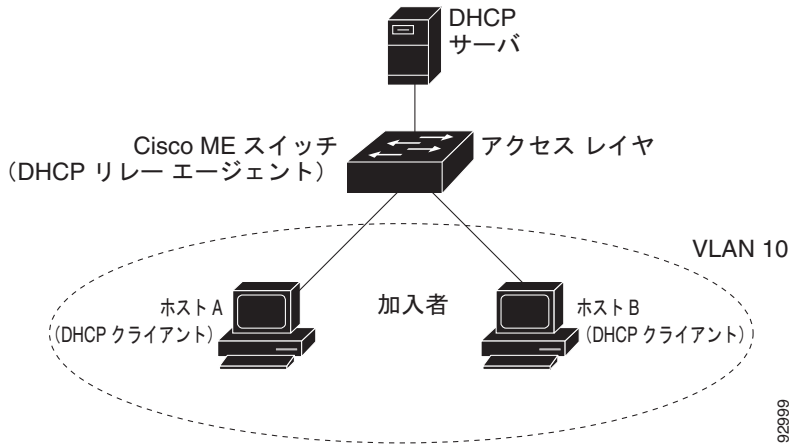
Option 82 データ挿入

住宅地のメトロポリタン イーサネット アクセス環境では、DHCP により、多数の加入者への IP アドレスの割り当てを集中管理できます。スイッチで DHCP Option 82 機能がイネーブルの場合は、（MAC アドレスの他に）ネットワークへの接続に使用されるスイッチ ポートにより、加入者デバイスを識別します。加入者 LAN の複数のホストは、アクセス スイッチ上の同一ポートに接続でき、一意に識別されます。

（注）　DHCP Option 82 機能は、DHCP スヌーピングがグローバルにイネーブルで、この機能を使用している加入者デバイスが割り当てられている VLAN にある場合にだけサポートされます。

図 20-1 は、中央集中型 DHCP サーバが、アクセス レイヤでスイッチに接続している加入者に IP アドレスの割り当てを行うメトロポリタン イーサネット ネットワークの例です。DHCP クライアントおよびこれに対応する DHCP サーバは、同じ IP ネットワークまたはサブネット上には存在しないため、DHCP リレー エージェント（Cisco ME スイッチ）は、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間の DHCP メッセージを転送するように、ヘルパー アドレスを使用して設定されます。

図 20-1　メトロポリタン イーサネット ネットワークの DHCP リレー エージェント



スイッチで DHCP スヌーピング情報 Option 82 をイネーブルにすると、次の一連のイベントが発生します。

- ホスト（DHCP クライアント）は、DHCP 要求を生成して、ネットワーク上にブロードキャストします。
- スイッチが DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションは、スイッチの MAC アドレスで、回線 ID サブオプションは、パケットの受信ポートの識別子である **vlan-mod-port** です。リモート ID および回線 ID も設定できます。これらのサブオプションの設定については、「DHCP スヌーピングおよび Option 82 のイネーブル化」（P.20-12）を参照してください。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバで、パケットを受信します。サーバが Option 82 対応の場合は、リモート ID、回線 ID、またはその両方を使用して、IP アドレスを割り当てて、単一のリモート ID または回線 ID に割り当てることができる IP アドレス数を制限するなど、ポリシーの実装を行います。また、DHCP サーバは、DHCP 応答に含まれるオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチでは、リモート ID あるいは回線 ID フィールドを調べて、自身が挿入した Option 82 データであることを確認します。スイッチは Option 82 フィールドを削除して、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

デフォルトのサブオプション設定で、前述の一連のイベントが発生した場合、図 20-2 内にある次のフィールドの値は変更されません。

- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ

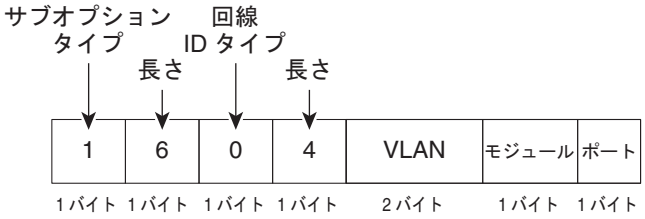
- リモート ID タイプ
- 回線 ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります たとえば 24 の 10/100 ポートおよび Small Form-factor Pluggable（SFP）モジュール スロットを含むスイッチでは、ポート 3 がファスト イーサネット 0/1 ポート、ポート 4 がファスト イーサネット 0/2 ポートのようになります。ポート 27 は SFP モジュール スロット 0/1 などのようになります。

図 20-2 に、デフォルトのサブオプション設定が使用されている場合の、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力される場合にこれらのパケット形式を使用します。

図 20-2　　サブオプション パケット形式

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット

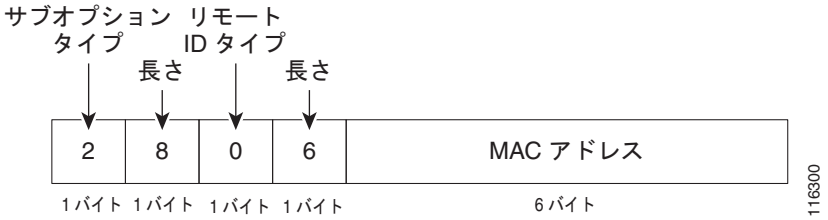


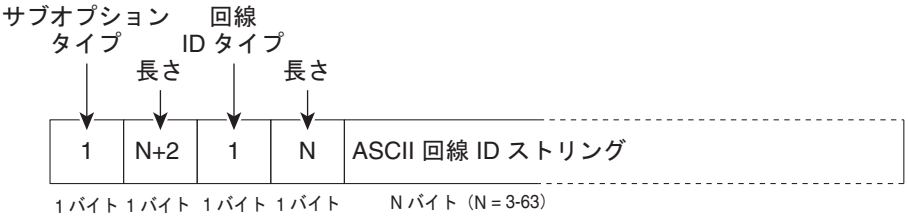
図 20-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット形式を示します。スイッチは、DHCP スヌーピングをグローバルにイネーブルにして、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力する場合に、これらのパケット形式を使用します。

パケット内のこれらのフィールドの値は、リモート ID および回線 ID サブオプションを設定すると、デフォルト値から変更されます。

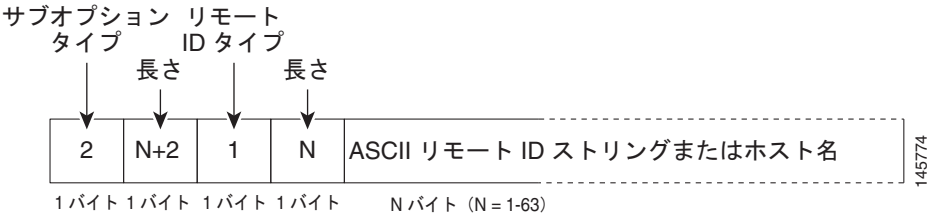
- 回線 ID サブオプション フィールド
  - 回線 ID タイプは 1 です。
  - 設定するストリング長に応じて、長さの値を変えられます。
- リモート ID サブオプション フィールド
  - リモート ID タイプは 1 です。
  - 設定するストリング長に応じて、長さの値を変えられます。

図 20-3　　ユーザ設定のサブオプション パケット形式

回線 ID サブオプション フレーム フォーマット（ユーザ設定のストリング）：



リモート ID サブオプション フレーム フォーマット（ユーザ設定のストリング）：



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、*アドレス バインディング*、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスは手動で割り当てることが可能で、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることもできます。手動および自動アドレスバインディングの詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「Configuring DHCP」の章を参照してください。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングがイネーブルの場合、スイッチは DHCP スヌーピング バインディング データベースを使用して信頼できないインターフェイスに関する情報を保存します。データベースには、8192 のバインディングを含めることができます。

各データベース エントリ（*binding*）には、IP アドレス、関連 MAC アドレス、およびリース時間（16 進数表記）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN があります。データベース エージェントは設定された場所にあるファイルにバインディングを保存します。各エントリの最後は、エントリに関連性のあるすべてのバイトが含まれる *checksum* 値です。各エントリは 72 バイトで、そのあとにスペースとチェックサム値が続きます。

スイッチをリロードしたときにバインディングを維持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP 検査または IP ソース ガードがイネーブルに設定されていて、DHCP スヌーピング バインディング データベースにダイナミック バインディングがある場合、スイッチの接続が切断されます。エージェントがディセーブルで、DHCP スヌーピングだけがイネーブルの場合、スイッチの接続は切断されませんが、DHCP スヌーピングでは DCHP スプーフィング攻撃を防止できないことがあります。

リロードしたとき、スイッチは DHCP スヌーピング バインディング データベースを構築するため、バインディング ファイルを読み込みます。スイッチは、データベース変更時にファイルを更新することにより、ファイルの内容を維持します。

スイッチが新しいバインディングを学習したり、バインディングを消失したりした場合には、スイッチはデータベース内のエントリを迅速に更新します。スイッチは、バインディング ファイル内のエントリも更新します。ファイルを更新する頻度は、設定可能な遅延に基づいて更新され、更新はバッチ処理されます。指定された時間（write-delay および abort-timeout 値によって設定）でファイルが更新されない場合、更新は中止されます。

バインディングのあるファイルのフォーマットは次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

ファイル内の各エントリはチェックサム値でタグ付けされていて、スイッチはファイルの読み取り時にこの値を使用してエントリを確認します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連したエントリを、前のファイル更新に関連したエントリと区別するものです。

バインディング ファイルの例は次のとおりです。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Fa1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Fa1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Fa1/0/4 584a38f0
END
```

スイッチが開始されて計算されたチェックサム値が保存されているチェックサム値と等しい場合、スイッチはバインディング ファイルからエントリを読み取ってバインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合にスイッチはエントリを無視します。

- スイッチがエントリを読み取って計算されたチェックサム値が保存されているチェックサム値と異なる場合。エントリとその後続のものが無視されます。
- エントリがリース時間を超過した場合（リース時間が超過してもスイッチはバインディング エントリを削除しない場合があります）
- エントリ内のインターフェイスがシステムに存在しない場合
- インターフェイスがルーテッド インターフェイスか DHCP スヌーピング信頼インターフェイスの場合

DHCP 機能の設定

- 「DHCP のデフォルト設定」（P.20-8）
- 「DHCP スヌーピング設定時の注意事項」（P.20-8）
- 「DHCP サーバの設定」（P.20-10）

- 「DHCP リレー エージェントの設定」（P.20-10）
- 「パケット転送アドレスの指定」（P.20-10）
- 「DHCP スヌーピングおよび Option 82 のイネーブル化」（P.20-12）
- 「プライベート VLAN での DHCP スヌーピングのイネーブル化」（P.20-14）
- 「Cisco IOS DHCP サーバ データベースのイネーブル化」（P.20-14）
- 「DHCP スヌーピング バインディング データベース エージェントのイネーブル化」（P.20-14）

DHCP のデフォルト設定

表 20-1 に、DHCP のデフォルト設定を示します。

表 20-1　DHCP のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル。設定が必要です。[1]
DHCP リレー エージェント	イネーブル[2]
DHCP パケット転送アドレス	設定なし
リレー エージェント情報のチェック	イネーブル（無効なメッセージは廃棄）[2]
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置き換えます。[2]
グローバルにイネーブルにされた DHCP スヌーピング	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
信頼できない入力インターフェイスでパケットを受信するための DHCP スヌーピング オプション[3]	ディセーブル
DHCP スヌーピング制限レート	設定なし
DHCP スヌーピングの信頼	信頼されない
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピング MAC アドレス検証	イネーブル
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル。設定が必要です。 **（注）** スイッチは、DHCP サーバとして設定されているデバイスだけから、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル。設定が必要です。宛先が設定されている場合にだけ、この機能は有効です。

1. スイッチは、DHCP サーバとして設定された場合にだけ DHCP 要求に応答します。
2. スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）に設定されている場合にだけ DHCP パケットをリレーします。
3. この機能は、スイッチが、エッジ スイッチから送信された Option 82 情報を含むパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

- スイッチでは、DHCP スヌーピングをグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN 上でイネーブルになるまで、アクティブではありません。

- スイッチで DHCP スヌーピングをグローバルでイネーブルにする前に、DHCP サーバおよび DHCP リレー エージェントとして機能しているデバイスが設定されていて、イネーブルであることを確認してください。
- スイッチで DHCP スヌーピングをグローバルにイネーブルにすると、スヌーピングがディセーブルになるまで、次の Cisco IOS コマンドを使用できません。次のコマンドを入力すると、スイッチはエラー メッセージを返し、設定は適用されません。
  - **ip dhcp relay information check** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information policy** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information trust-all** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information trusted** インターフェイス コンフィギュレーション コマンド
- スイッチに DHCP スヌーピング オプション情報を設定する前に、DHCP サーバとして機能するデバイスが設定されていることを確認します。たとえば、DHCP サーバが割り当てたり排除したりできる IP アドレスを指定する、またはデバイスに DHCP オプションを設定する必要があります。
- スイッチ上に多数の回線 ID を設定する場合は、NVRAM（不揮発性 RAM）またはフラッシュ メモリに対して長い文字列が与える影響について考慮してください。サーキット ID 設定がその他のデータと組み合わされた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、エラー メッセージが表示されます。
- スイッチに DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスが設定されていることを確認します。たとえば、DHCP サーバが割り当てたり排除したりできる IP アドレスを指定する、デバイスに DHCP オプションを設定する、または DHCP データベース エージェントを設定する必要があります。
- DHCP リレー エージェントがイネーブルであるものの、DHCP スヌーピングがディセーブルの場合、DHCP Option 82 データ挿入機能はサポートされません。
- スイッチ ポートが DHCP サーバに接続されている場合、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力してポートを trusted に設定します。
- スイッチ ポートが DHCP クライアントに接続されている場合、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力してポートを untrusted に設定します。
- DHCP スヌーピング バインディング データベースを設定する際は、次の注意事項に従ってください。
  - NVRAM およびフラッシュ メモリのストレージ容量に制限があるので、バインディング ファイルは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存することを推奨します。
  - ネットワーク ベース URL（TFTP や FTP（ファイル転送プロトコル）など）の場合、スイッチが設定した URL のバインディング ファイルにバインディングを書き込む前に、その URL で空のファイルを作成しておく必要があります。先にサーバで空のファイルを作成する必要があるかどうかを判断するには、TFTP サーバのマニュアルを参照してください。一部の TFTP サーバはこの方法では設定できません。
  - データベースのリース時間を正確にするには、Network Time Protocol（NTP）をイネーブルにして、設定することを推奨します。詳細については、「NTP の設定」（P.5-4）を参照してください。
  - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容を書き込みます。
- 信頼できないデバイスが接続された集約スイッチに、**ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。

- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力することにより、DHCP スヌーピングの統計情報を表示できます。また、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力することにより、スヌーピングの統計情報カウンタをクリアできます。

（注）　RSPAN VLAN 上では Dynamic Host Configuration Protocol（DHCP）スヌーピングをイネーブルにしないでください。DHCP スヌーピングが RSPAN VLAN 上でイネーブルになっていると、DHCP パケットが RSPAN 宛先ポートに到達しない可能性があります。

DHCP サーバの設定

スイッチは、DHCP サーバとして機能させることもできます。デフォルトでは、Cisco IOS DHCP サーバおよびリレー エージェント機能は、スイッチ上でイネーブルになっていますが、設定が行われていません。このため、これらの機能は動作しません。

スイッチを DHCP サーバとして設定するときの手順については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Addressing and Services」の章の「Configuring DHCP」を参照してください。

DHCP リレー エージェントの設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service dhcp**	スイッチ上で DHCP リレー エージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP リレー エージェントをディセーブルにするには、**no service dhcp** グローバル コンフィギュレーション コマンドを使用します。

次の手順については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Addressing and Services」の章の「*Configuring DHCP*」を参照してください。

- リレー エージェント情報のチェック（確認）
- リレー エージェント転送ポリシーの設定

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにあり、スイッチでメトロ IP アクセス イメージが稼動している場合、スイッチを **ip helper-address** *address* インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的な規則は、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで

使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにできます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id*	VLAN ID を入力してスイッチの仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** *ip-address subnet-mask*	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 4	**ip helper-address** *address*	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバ アドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにできます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface range** *port-range* または **interface** *interface-id*	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス レンジ コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**no shutdown**	必要な場合に、インターフェイスをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interfaces（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 8	**switchport mode access**	ポートの VLAN メンバーシップ モードを定義します。
ステップ 9	**switchport access vlan** *vlan-id*	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP パケット転送アドレスを削除するには、**no ip helper-address** *address* インターフェイス コンフィギュレーション コマンドを使用します。

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp snooping**	DHCP スヌーピングをグローバルにイネーブルにします。
ステップ 3	**ip dhcp snooping vlan** *vlan-range*	VLAN または VLAN 範囲で、DHCP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力できます。これらはスペースで区切ります。
ステップ 4	**ip dhcp snooping information option**	スイッチをイネーブルにして、DHCP サーバへの DHCP 要求メッセージの DHCP リレー情報（Option 82 フィールド）を挿入または削除します。これは、デフォルト設定です。
ステップ 5	**ip dhcp snooping information option format remote-id [string** *ASCII-string* **| hostname]**	（任意）リモート ID サブオプションを設定します。 リモート ID は次のように設定できます。 • 最大 63 の ASCII 文字（スペースなし）の文字列 • スイッチの設定済みのホスト名 **（注）** ホスト名が 63 文字以上の場合は、リモート ID 設定で 63 文字に切り捨てられます。 デフォルトのリモート ID は、スイッチの MAC アドレスです。
ステップ 6	**ip dhcp snooping information option allowed-untrusted**	（任意）スイッチがエッジ スイッチに接続された集約スイッチである場合に、エッジ スイッチから送信された Option 82 情報を含む着信 DHCP スヌーピング パケットをスイッチが受信できるようにします。 デフォルトはディセーブルです。 **（注）** このコマンドを入力する必要があるのは、信頼できるデバイスに接続された集約スイッチだけです。
ステップ 7	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 9	**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id string** [**override**] *ASCII-string*	（任意）指定されたインターフェイスの回線 ID サブオプションを設定します。 1 ～ 4094 の範囲の VLAN ID を使用して、VLAN およびポートの識別子を指定します。デフォルトの回線 ID は、ポートの識別子で、**vlan-mod-port** フォーマットです。 回線 ID は、3 ～ 63 の ASCII 文字（スペースなし）の文字列になるよう設定できます。 （任意）加入者情報を定義するうえで、TLV 形式で挿入された回線 ID サブオプションが不要な場合は、キーワード **override** を使用します。
ステップ 10	**ip dhcp snooping trust**	（任意）インターフェイスを trusted または untrusted と設定します。信頼されないクライアントからメッセージを受信するようにインターフェイスを設定するには、キーワード **no** を使用します。デフォルトでは、信頼されません。
ステップ 11	**ip dhcp snooping limit rate** *rate*	（任意）インターフェイスが受信できる毎秒ごとの DHCP パケット数を設定します。指定できる範囲は 1 ～ 2048 です。デフォルトでは、レート制限は設定されていません。 **（注）** 信頼されないレート制限を毎秒 100 パケット以下にすることを推奨します。信頼できるインターフェイスでレート制限を設定した場合、ポートが、DHCP スヌーピングをイネーブルにしている複数の VLAN に割り当てられたトランク ポートであれば、レート制限値を上げる必要があります。
ステップ 12	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**ip dhcp snooping verify mac-address**	（任意）信頼できないポートで受信された DHCP パケット内の送信元 MAC アドレスが、パケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケット内のクライアント ハードウェア アドレスと一致することを確認します。
ステップ 14	**end**	特権 EXEC モードに戻ります。
ステップ 15	**show running-config**	設定を確認します。
ステップ 16	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用します。VLAN または VLAN 範囲で DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、**no ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。エッジ スイッチから送信された Option 82 情報を含む着信 DHCP スヌーピング パケットを廃棄するように集約スイッチを設定するには、**no ip dhcp snooping information option allowed-untrusted** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 10 で DHCP スヌーピングをグローバルにイネーブルにし、ポート上でレート制限を毎秒 100 パケットに設定する方法を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

プライベート VLAN での DHCP スヌーピングのイネーブル化

プライベート VLAN で DHCP スヌーピングをイネーブルにできます。DHCP スヌーピングがイネーブルの場合、設定はプライマリ VLAN および関連付けられているセカンダリ VLAN の両方に伝播します。DHCP スヌーピングがプライマリ VLAN でイネーブルの場合、セカンダリ VLAN でもイネーブルに設定されています。

DHCP スヌーピングがすでにプライマリ VLAN に設定されていて DHCP スヌーピングをセカンダリ VLAN とは異なるように設定した場合、セカンダリ VLAN の設定は有効になりません。プライマリ VLAN に DHCP スヌーピングを設定する必要があります。プライマリ VLAN に DHCP スヌーピングが設定されていない場合は、VLAN 200 などのセカンダリ VLAN に DHCP スヌーピングを設定するときに、次のメッセージが表示されます。

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not take
effect on secondary vlan 200. DHCP Snooping configuration on secondary vlan is derived
from its primary vlan.
```

show ip dhcp snooping 特権 EXEC コマンド出力には、プライマリおよびセカンダリ プライベート VLAN を含む、DHCP スヌーピングがイネーブルのすべての VLAN が表示されています。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「Configuring DHCP」の章にある「DHCP Configuration Task List」を参照してください。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp snooping database** {**flash:**/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** | **rcp:**//*user*@*host*/*filename*}| **tftp:**//*host*/*filename*	次の形式のいずれかを使用して、データベース エージェントまたはバインディング ファイル用の URL を指定します。 • **flash:**/*filename* • **ftp:**//*user*:*password*@*host*/*filename* • **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** • **rcp:**//*user*@*host*/*filename* • **tftp:**//*host*/*filename*
ステップ 3	**ip dhcp snooping database timeout** *seconds*	バインディング データベースが変更されたあとのデータベースの転送プロセスを停止する時間を指定します。 指定できる範囲は 0 ～ 86400 です。無制限を指定する場合、0 を使用します。デフォルトは 300 秒（5 分）です。

	コマンド	目的
ステップ 4	**ip dhcp snooping database write-delay** *seconds*	バインディング データベースが変更されたあとの転送が遅延する期間を指定します。 指定できる範囲は 15 ～ 86400 秒です。デフォルトは 300 秒（5 分）です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*	（任意）DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。指定できる *vlan-id* の範囲は 1 ～ 4904 です。*seconds* の範囲は 1 ～ 4294967295 秒です。 追加する各エントリにこのコマンドを入力します。 **（注）**　このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 7	**show ip dhcp snooping database** [**detail**]	DHCP スヌーピング バインディング データベース エージェントのステータスと統計情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

データベース エージェントおよびバインディング ファイルの使用を停止するには、**no ip dhcp snooping database** グローバル コンフィギュレーション コマンドを使用します。タイムアウトまたは遅延値をリセットするには、**ip dhcp snooping database timeout** *seconds* または **ip dhcp snooping database write-delay** *seconds* グローバル コンフィギュレーション コマンドを使用します。

DHCP スヌーピング バインディング データベース エージェントの統計情報を消去するには、**clear ip dhcp snooping database statistics** 特権 EXEC コマンドを使用します。データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

DHCP スヌーピング バインディング データベースからエントリを削除するには、**no ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* 特権 EXEC コマンドを使用します。削除する各エントリにこのコマンドを入力します。

DHCP スヌーピング情報の表示

DHCP スヌーピング情報を表示するには、表 20-2 に示す、1 つまたは複数の特権 EXEC コマンドを使用します。

表 20-2　DHCP 情報を表示するためのコマンド

コマンド	目的
show ip dhcp snooping	スイッチの DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	バインディング テーブルとも呼ばれる DHCP スヌーピング バインディング データベースの中から、動的に設定されたバインディングだけを表示します。[1]
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報をサマリー形式または詳細形式で表示します。
show ip source binding	ダイナミックおよびスタティックに設定されたバインディングを表示します。

1. DHCP スヌーピングがイネーブルで、インターフェイスがダウン ステートに変更された場合、スイッチは手動で設定されたバインディングを削除しません。

DHCP サーバ ポートベース アドレス 割り当て

DHCP サーバ ポートベース アドレス割り当ては、DHCP が、付加されたデバイス クライアント ID またはクライアント ハードウェア アドレスに関わらず、イーサネット スイッチ ポート上で同じ IP アドレスを維持できるようにする機能です。

イーサネット スイッチをネットワーク内に配置すると、それらのスイッチによって、直接接続されたデバイスに対する接続が提供されます。工場のような一部の環境では、あるデバイスに障害が発生した場合、交換デバイスが、既存のネットワーク内で即座に動作する必要があります。現在の DHCP 実装では、DHCP がその交換デバイスに対して同じ IP アドレスを提供するという保証はありません。コントロール、モニタリング、およびその他のソフトウェアでは、各デバイスに関連付けられた IP アドレスは変わらないと見なされます。デバイスが交換された場合、DHCP クライアントが変わったとしても、アドレス割り当ては変わらないままである必要があります。

DHCP サーバ ポートベース アドレス割り当て機能を設定すると、ポート上で受信された DHCP メッセージ内でクライアント ID またはクライアント ハードウェア アドレスが変更されていても、同じ IP アドレスがその同じ接続ポートに対して常に提供されるようになります。DHCP プロトコルでは、DHCP パケット内のクライアント ID オプションによって DHCP クライアントが認識されます。クライアント ID オプションを持っていないクライアントは、クライアント ハードウェア アドレスによって識別されます。この機能を設定すると、インターフェイスのポート名によって、クライアント ID またはハードウェア アドレスが上書きされ、実際の接続ポイント、つまりスイッチ ポートがクライアント ID になります。

どんな場合でも、同じポートに対してイーサネット ケーブルを接続することによって、同じ IP アドレスが DHCP を介して付加されたデバイスに割り当てられます。

DHCP サーバ ポートベース アドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけであり、サードパーティのサーバではサポートされていません。

DHCP サーバ ポートベース アドレス 割り当ての設定

- 「ポートベース アドレス割り当てのデフォルト設定」（P.20-16）
- 「ポートベース アドレス割り当て設定のガイドライン」（P.20-16）
- 「DHCP サーバ ポートベース アドレス 割り当てのイネーブル化」（P.20-17）

ポートベース アドレス割り当てのデフォルト設定

デフォルトでは、DHCP サーバ ポートベース アドレス割り当てはディセーブルに設定されています。

ポートベース アドレス割り当て設定のガイドライン

次に、DHCP ポートベース アドレス割り当て設定に関するガイドラインを示します。

- ポートごとに割り当てられる IP アドレスは 1 つだけです。
- **clear ip dhcp binding** グローバル コンフィギュレーション コマンドを使用しても、予約済みアドレス（事前割り当て）は消去できません。
- 事前割り当てアドレスは、通常のダイナミック IP アドレス割り当てからは自動的に除外されます。事前割り当てアドレスは、ホスト プール内では使用できませんが、DHCP アドレス プールごとに複数のアドレスを事前に割り当てることが可能です。

- DHCP プールから事前設定予約への割り当てを制限するには（予約されていないアドレスはクライアントに提供されず、他のクライアントには DHCP プールのサービスが提供されません）、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

DHCP サーバ ポートベース アドレス 割り当てのイネーブル化

ポートベース アドレス割り当てをグローバルにイネーブルにし、インターフェイス上で加入者 ID をグローバルに生成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp use subscriber-id client-id**	DHCP サーバを、加入者 ID がすべての着信 DHCP メッセージにおけるクライアント ID としてグローバルに使用されるように設定します。
ステップ 3	**ip dhcp subscriber-id interface-name**	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイス上で設定された加入者 ID は、このコマンドよりも優先されます。
ステップ 4	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip dhcp server use subscriber-id client-id**	DHCP サーバを、加入者 ID がインターフェイス上のすべての着信 DHCP メッセージにおけるクライアント ID として使用されるように設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ上で DHCP ポートベース アドレス割り当てをイネーブルにした後、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスを事前に割り当て、それらのアドレスをクライアントに関連付けます。DHCP プールから事前に設定された予約への割り当てを制限するには、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。ネットワークに含まれているアドレスやプール範囲にあるアドレスでも、予約されていないアドレスはクライアントに提供されず、他のクライアントには DHCP プールのサービスが提供されません。ユーザはこのコマンドを使用して、DHCP プールを装備した 1 組のスイッチが共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視するように設定できます。

IP アドレスを事前に割り当て、そのアドレスを、インターフェイス名によって識別されるクライアントに対して関連付けるには、特権 EXEC モードで、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *poolname*	DHCP プール コンフィギュレーション モードを開始し、DHCP プールの名前を定義します。プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 3	**network** *network-number* [*mask* | */prefix-length*]	DHCP アドレス プールのサブネット ネットワーク番号およびサブネット マスクを指定します。
ステップ 4	**address** *ip-address* **client-id** *string* [**ascii**]	インターフェイス名によって特定される DHCP クライアントの IP アドレスを予約します。 *string* : ASCII 値または 16 進数値で指定できます。
ステップ 5	**reserved-only**	（任意）DHCP アドレス プール内の予約済みアドレスだけを使用します。デフォルトでは、プール アドレスは制限されません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip dhcp pool**	DHCP プール設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP ポートベース アドレス割り当てをディセーブルにするには、**no ip dhcp use subscriber-id client-id** グローバル コンフィギュレーション コマンドを使用します。加入者 ID の自動生成をディセーブルにするには、**no ip dhcp subscriber-id interface-name** グローバル コンフィギュレーション コマンドを使用します。インターフェイス上の加入者 ID をディセーブルにするには、**no ip dhcp server use subscriber-id client-id** インターフェイス コンフィギュレーション コマンドを使用します。

DHCP プールから IP アドレス予約を削除するには、**no address** *ip-address* **client-id** *string* DHCP プール コンフィギュレーション コマンドを使用します。アドレス プールを制限なしに変更するには、**no reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

次の例では、加入者 ID が自動的に生成されています。また、DHCP メッセージ内のクライアント ID フィールドは DHCP サーバによってすべて無視され、その代わりに、加入者 ID が使用されています。加入者 ID は、インターフェイスの短い名前と、IP アドレス 10.1.1.7 が事前に割り当てられたクライアントに基づいています。

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id “Et1/0” ascii
<output truncated>
```

次に、事前に割り当てられたアドレスが DHCP 内で正しく予約されている例を示します。

```
Switch# show ip dhcp pool dhcppool
Pool dhcp pool:
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 0
 Excluded addresses : 4
 Pending event : none
 1 subnet is currently in the pool:
 Current index   IP address range         Leased/Excluded/Total
 10.1.1.1        10.1.1.1 - 10.1.1.254     0     / 4 / 254
 1 reserved address is currently in the pool
 Address         Client
 10.1.1.7 Et1/0
```

DHCP サーバ ポートベース アドレス割り当て機能の設定の詳細については、Cisco.com の [Search] フィールドに *Cisco IOS IP Addressing Services* と入力して、Cisco IOS ソフトウェア マニュアルにアクセスしてください。マニュアルは次の URL でもアクセスできます。

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

DHCP サーバ ポートベース アドレス 割り当ての表示

DHCP サーバ ポートベース アドレス割り当て情報を表示するには、表 20-3 に示す、1 つまたは複数の特権 EXEC コマンドを使用します。

表 20-3　DHCP ポートベース アドレス割り当て情報を表示するためのコマンド

コマンド	目的
show interface *interface-id*	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバ上のアドレス バインディングを表示します。

IP ソース ガードの概要

IPSG は、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックを制限するセキュリティ機能で、DHCP スヌーピング バインディング データベースと手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることで、実現しています。IP ソース ガードを使用して、ホストがネイバの IP アドレスを使用しようとする場合のトラフィック攻撃を回避できます。

DHCP スヌーピングが信頼できないインターフェイスでイネーブルの場合に IP ソース ガードをイネーブルにできます。IPSG がインターフェイスでイネーブルになったあと、スイッチは、DHCP スヌーピングで許可された DHCP パケットを除く、インターフェイスで受信されたすべての IP トラフィックをブロックします。ポート Access Control List（ACL; アクセス制御リスト）はインターフェイスに適用されます。ポート ACL により、IP 送信元バインディング テーブル内の送信元 IP アドレスの IP トラフィックだけを許可し、その他のトラフィックを拒否できます。

（注）　ポート ACL は同じインターフェイスに影響を与えるいずれのルータ ACL または VLAN マップよりも優先されます。

IP 送信元バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP 送信元バインディング）があります。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルの場合にだけ IP 送信元バインディング テーブルを使用します。

IP ソース ガードは、アクセス ポートやトランク ポートなどのレイヤ 2 ポートでだけサポートされます。IP ソース ガードを、送信元 IP フィルタリングや送信元 IP および MAC アドレス フィルタリングとともに設定できます。

ここでは、次の情報について説明します。

- 「送信元 IP アドレス フィルタリング」（P.20-20）
- 「送信元 IP および MAC アドレス フィルタリング」（P.20-21）
- 「スタティック ホスト用 IP ソース ガード」（P.20-21）

送信元 IP アドレス フィルタリング

IP ソース ガードがこのオプションでイネーブルの場合、IP トラフィックは送信元 IP アドレスに基づいてフィルタリングされます。送信 IP アドレスが DHCP スヌーピング バインディング データベースのエントリまたは IP 送信元バインディング テーブル内のバインディングと一致した場合、スイッチは IP トラフィックを転送します。

DHCP スヌーピング バインディングまたはスタティック IP 送信元バインディングがインターフェイスで追加、変更、削除された場合、スイッチは IP 送信元バインディングを変更してポート ACL を修正し、ポート ACL をインターフェイスに適用します。

（DHCP スヌーピングで動的に学習されたか手動で設定された）IP 送信元バインディングが設定されていないインターフェイスで IP ソース ガードをイネーブルにする場合、スイッチはインターフェイス上のすべての IP トラフィックを拒否するポート ACL を作成し、適用します。IP ソース ガードをディセーブルにする場合、スイッチはポート ACL をインターフェイスから削除します。

送信元 IP および MAC アドレス フィルタリング

IP ソース ガードがこのオプションでイネーブルの場合、IP トラフィックは送信元 IP アドレスおよび MAC アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP アドレスおよび MAC アドレスが IP 送信元バインディング テーブルのエントリと一致する場合にトラフィックを転送します。

IP ソース ガードと送信元 IP および MAC アドレス フィルタリングがイネーブルの場合、スイッチは IP および非 IP トラフィックをフィルタリングします。IP または非 IP パケットの送信元 MAC アドレスが有効な IP 送信元バインディングと一致する場合、スイッチはパケットを転送します。スイッチは、DHCP パケットを除く他のすべてのタイプのパケットを廃棄します。

スイッチは、ポート セキュリティを使用して送信元 MAC アドレスをフィルタリングします。ポート セキュリティ違反の発生時にインターフェイスをシャット ダウンできます。

スタティック ホスト用 IP ソース ガード

（注）　アップリンク ポートまたはトランク ポート上ではスタティック ホスト用 IP source guard（IPSG; IP ソース ガイド）は使用しないでください。

スタティック ホスト用 IPSG によって、IPSG 機能を非 DHCP およびスタティックな環境に拡張できます。旧 IPSG では、DHCP スヌーピングによって作成されたエントリを使用して、スイッチに接続されたホストを検証していました。有効な DHCP バインディング エントリを持たないホストから受信したトラフィックはすべて破棄されます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。DHCP スヌーピング バインディング データベースと手動で設定された IP ソース バインディングに基づいてトラフィックがフィルタリングされます。旧バージョンの IPSG では、IPSG が動作するのに DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしに IPSG が動作します。スタティック ホスト用 IPSG では、IP デバイス トラッキング テーブルのエントリに基づいて、ポート ACL がインストールされます。スイッチでは、ARP 要求またはその他の IP パケットに基づいてスタティック エントリが作成され、指定されたポートの有効なホストのリストが維持されます。指定されたポートにトラフィックを送信することを許可するホストの数も指定できます。これは、レイヤ 3 におけるポート セキュリティに相当します。

スタティック ホスト用 IPSG では、ダイナミック ホストもサポートされています。ダイナミック ホストによって、IP DHCP スヌーピング テーブル内に存在する DHCP 割り当て済み IP アドレスが受信されると、同じエントリが、IP デバイス トラッキング テーブルによって学習されます。**show ip device tracking all** EXEC コマンドを入力すると、IP デバイス トラッキング テーブルにエントリが ACTIVE として表示されます。

（注）　複数のネットワーク インターフェイスを持つ IP ホストの中には、一部の無効なパケットをネットワーク インターフェイスに送信可能なものもあります。無効なパケットには、ホストの別のネットワーク インターフェイスの IP アドレスまたは MAC アドレスが、送信元アドレスとして含まれています。無効なパケットが原因で、スタティック ホスト用 IPSG がそのホストに接続し、無効な IP アドレスまたは MAC アドレス バインディングを学習し、有効なバインディングを拒否してしまう可能性があります。対応するオペレーティング システムとネットワーク インターフェイスのベンダーに相談して、ホストが無効なパケットを送信するのを防いでください。

スタティック ホスト用 IPSG では、ACL ベースのスヌーピング メカニズムを介して IP または MAC バインディングが動的に取得されます。IP または MAC バインディングは、ARP および IP パケットによって、スタティック ホストから取得されます。これらのパケットは、デバイス トラッキング データベースに保存されます。指定されたポート上で動的に取得されるか、スタティックに設定された IP アドレスの数が上限に達すると、新しい IP アドレスを持つパケットはすべてハードウェアによって破棄されます。何らかの理由により移動または撤去されたホストを解決するために、スタティック ホスト用 IPSG では、IP デイバス トラッキングによって、学習された IP アドレス バインディングが動的にエージング アウトされます。この機能は、DHCP スヌーピングと共に使用できます。DHCP とスタティック ホストへ接続されているポート上で、複数のバインディングが確立されます。たとえば、バインディングが、デバイス トラッキング データベースと、DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガードの設定

- 「デフォルトの IP ソース ガードの設定」（P.20-22）
- 「IP ソース ガード設定時の注意事項」（P.20-22）
- 「IP ソース ガードのイネーブル化」（P.20-23）

デフォルトの IP ソース ガードの設定

デフォルトでは、IP ソース ガードはディセーブルに設定されています。

IP ソース ガード設定時の注意事項

IP ソース ガードの設定時の注意事項は次のとおりです。

- 非ルーテッド ポートでだけスタティック IP バインディングを設定できます。**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドをルーテッド インターフェイスに入力した場合、このエラー メッセージが表示されます。

  ```
  Static IP source binding can only be configured on switch port.
  ```

- IP ソース ガードと送信元 IP フィルタリングがインターフェイスでイネーブルの場合、DHCP スヌーピングは、VLAN が所属するアクセス VLAN でイネーブルでなければなりません。
- 複数の VLAN があるトランク インターフェイスで IP ソース ガードがイネーブルで、DHCP スヌーピングがすべての VLAN でイネーブルの場合、送信元 IP アドレス フィルタがすべての VLAN に適用されます。

（注）　IP ソース ガードがイネーブルでトランク インターフェイス上の VLAN で DHCP スヌーピングがイネーブルまたはディセーブルの場合、スイッチが適切にトラフィックをフィルタリングできません。

- IP ソース ガードを、送信元 IP および MAC アドレス フィルタリングによってイネーブルにする場合、DHCP スヌーピングおよびポート セキュリティがインターフェイスでイネーブルでなければなりません。また、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力し、DHCP サーバが Option 82 をサポートできるようにする必要があります。IP ソース ガードが MAC アドレス フィルタリング上でイネーブルの場合、DHCP ホストの MAC アドレスは、ホストがリースを許可されるまで学習されません。パケットをサーバからホストに転送する場合、DHCP スヌーピングは、Option 82 のデータを使用してホストポートを識別します。
- プライベート VLAN が設定されているインターフェイスで IP ソース ガードを設定する場合、ポート セキュリティはサポートされません。
- IP ソース ガードは EtherChannel でサポートされません。
- IEEE 802.1X ポートベース認証がイネーブルである場合、IP ソース ガードの機能をイネーブルにできます。
- Ternary CAM（TCAM）エントリ数が最大数を超えた場合、CPU の使用量が増加します。

IP ソース ガードのイネーブル化

インターフェイス上で IP ソース ガードをイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip verify source** または **ip verify source port-security**	IP ソース ガードと送信元 IP アドレス フィルタリングをイネーブルにします。 IP ソース ガードと送信元 IP および MAC アドレス フィルタリングをイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して IP ソース ガードとポート セキュリティの両方をイネーブルにする場合は、次の 2 つの注意事項があります。 • DHCP サーバで Option 82 をサポートしていないと、クライアントには IP アドレスが割り当てられません。 • DHCP パケットの MAC アドレスは、セキュア アドレスとして学習されません。スイッチが DHCP 以外のデータ トラフィックを受信した場合にだけ、DHCP クライアントの MAC アドレスはセキュア アドレスとして学習されます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **inteface** *interface-id*	スタティック IP 送信元バインディングを追加します。 各スタティック バインディングに対してこのコマンドを入力します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip verify source** [**interface** *interface-id*]	すべてのインターフェイスまたは特定のインターフェイスに対して IP ソース ガード設定を表示します。
ステップ 9	**show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**inteface** *interface-id*] [**vlan** *vlan-id*]	スイッチ、特定の VLAN、または特定のインターフェイス上の IP 送信元バインディングを表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ソース ガードおよび送信元 IP アドレス フィルタリングをディセーブルにするには、**no ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

スタティック IP 送信元バインディング エントリを削除するには、**no ip source** グローバル コンフィギュレーション コマンドを使用します。

次に、IP ソース ガードと送信元 IP および MAC フィルタリングを VLAN 10 および VLAN 11 でイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet0/1
Switch(config)# end
```

スタティック ホスト用 IP ソース ガードの設定

- 「レイヤ 2 アクセス ポート上におけるスタティック ホスト用 IP ソース ガードの設定」（P.20-24）
- 「プライベート VLAN ホスト ポート上におけるスタティック ホスト用 IP ソース ガードの設定」（P.20-28）

レイヤ 2 アクセス ポート上におけるスタティック ホスト用 IP ソース ガードの設定

（注）　スタティック ホスト用 IPSG を動作させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。IP デバイス トラッキングをグローバルにイネーブルにしないか、あるいは、そのインターフェイス上で IP デバイス トラッキングの最大値を設定しないで、ポート上でこのコマンドだけを設定する場合、スタティック ホストを使用した IPSG によって、そのインターフェイスからのすべての IP トラフィックが拒否されます。この要件は、プライベート VLAN ホスト ポート上でのスタティック ホストを使用した IPSG にも適用されます。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking**	IP ホスト テーブルをオンにして、IP デバイス トラッキングをグローバルにイネーブルにします。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	ポートを access に設定します。
ステップ 5	**switchport access vlan** *vlan-id*	このポートの VLAN を設定します。
ステップ 6	**ip verify source tracking port-security**	MAC アドレス フィルタリングを使用してスタティック ホスト用 IPSG をイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して IP ソース ガードとポート セキュリティの両方をイネーブルにするときは、次の 2 つの注意事項があります。 • DHCP サーバで Option 82 をサポートしていないと、クライアントには IP アドレスが割り当てられません。 • DHCP パケットの MAC アドレスは、セキュア アドレスとして学習されません。スイッチが DHCP 以外のデータ トラフィックを受信した場合にだけ、DHCP クライアントの MAC アドレスはセキュア アドレスとして学習されます。
ステップ 7	**ip device tracking maximum** *number*	IP デバイス トラッキング テーブルがポート上で許可するスタティック IP の数の最大限度を確立します。指定できる範囲は 1 ～ 10 です。最大数は 10 です。 （注）　**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 8	**switchport port-security**	（任意）このポートのポート セキュリティをアクティブにします。
ステップ 9	**switchport port-security maximum** *value*	（任意）このポートの MAC アドレスの最大値を確立します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	**show ip verify source** *interface* interface-id	設定を確認し、スタティック ホスト用 IPSG 許可 ACL を表示します。
ステップ 12	**show ip device track all [active | inactive] count**	スイッチ インターフェイス上における指定されたホストの IP と MAC バインディングを表示することによって、設定を確認します。 • **all active**：アクティブな IP または MAC バインディング エントリだけを表示します。 • **all inactive**：非アクティブな IP または MAC バインディング エントリだけを表示します。 • **all**：アクティブおよび非アクティブな IP または MAC バインディング エントリを表示します。

次に、インターフェイス上の、スタティック ホストを使用した IPSG を停止する例を示します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

次に、ポート上の、スタティック ホストを使用して IPSG をイネーブルにする例を示します。

```
Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security
```

次に、レイヤ 2 アクセス ポート上で IP フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、インターフェイス Gi0/3 上の有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip trk       active       40.1.1.24                           10
Gi0/3      ip trk       active       40.1.1.20                           10
Gi0/3      ip trk       active       40.1.1.21                           10
```

次に、レイヤ 2 アクセス ポート上で IP-MAC フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、インターフェイス Gi0/3 上の有効な IP-MAC バインディングを確認し、このインターフェイス上のバインディングの数が最大値に達したことを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Gi0/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Gi0/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Gi0/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Gi0/3      ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  1
```

次の例では、すべてのインターフェイスの、すべての IP または MAC バインディング エントリを表示しています。CLI では、すべてのアクティブおよび非アクティブなエントリが表示されます。ホストがインターフェイス上で学習されると、その新しいエントリが ACTIVE としてマークされます。同じホストがそのインターフェイスから切断され、異なるインターフェイスに接続されると、そのホストが検知されると同時に新しい IP または MAC バインディング エントリが ACTIVE として表示されます。以前のインターフェイス上の、このホストの古いエントリは、INACTIVE としてマークされます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

次の例では、すべてのインターフェイスの、すべてのアクティブな IP または MAC バインディング エントリを表示しています。

```
Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
```

次の例では、すべてのインターフェイスの、すべての非アクティブな IP または MAC バインディング エントリを表示しています。このホストは、最初に GigabitEthernet 0/1 上で学習されてから、次に GigabitEthernet 0/2 に移動されました。GigabitEthernet 0/1 上で学習された IP または MAC バインディング エントリは、INACTIVE としてマークされています。

```
Switch# show ip device tracking all inactive
IP Device Tracking = Enabled
```

```
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

次の例では、すべてのインターフェイスの、すべての IP デバイス トラッキング ホスト エントリの数を表示しています。

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
-----------------------------------------------------------------------
  Interface           Maximum Limit           Number of Entries
-----------------------------------------------------------------------
Gi0/3                  5
```

プライベート VLAN ホスト ポート上におけるスタティック ホスト用 IP ソース ガードの設定

（注）　スタティック ホスト用 IPSG を動作させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。IP デバイス トラッキングをグローバルにイネーブルにしないか、あるいは、そのインターフェイス上で IP デバイス トラッキングの最大値を設定しないで、ポート上でこのコマンドだけを設定する場合、スタティック ホストを使用した IPSG によって、そのインターフェイスからのすべての IP トラフィックが拒否されます。この要件は、レイヤ 2 アクセス ポート上でのスタティック ホストを使用した IPSG にも適用されます。

レイヤ 2 アクセス ポート上で、IP フィルタを使用してスタティック ホスト用 IPSG を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id1*	VLAN コンフィギュレーション モードを開始します。
ステップ 3	**private-vlan primary**	プライベート VLAN ポート上でプライマリ VLAN を確立します。
ステップ 4	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 5	**vlan** *vlan-id2*	別の VLAN の コンフィギュレーション VLAN モードを開始します。
ステップ 6	**private-vlan isolated**	プライベート VLAN ポート上で独立 VLAN を確立します。
ステップ 7	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 8	**vlan** *vlan-id1*	コンフィギュレーション VLAN モードを開始します。

	コマンド	目的
ステップ 9	**private-vlan association 201**	独立プライベート VLAN ポート上で、VLAN を関連付けます。
ステップ 10	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 11	**interface fastEthernet** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**switchport mode private-vlan host**	（任意）ポートをプライベート VLAN ホストとして確立します。
ステップ 13	**switchport private-vlan host-association** *vlan-id1 vlan-id2*	（任意）このポートを対応するプライベート VLAN に関連付けます。
ステップ 14	**ip device tracking maximum** *number*	IP デバイス トラッキング テーブルがポート上で許可するスタティック IP の最大数を確立します。 最大数は 10 です。 （注）　スタティック ホスト用 IPSG を動作させるには、**ip device tracking maximum** *number* インターフェイス コマンドをグローバルに設定する必要があります。
ステップ 15	**ip verify source tracking [port-security]**	このポート上で MAC アドレス フィルタリングを使用してスタティック ホストの IPSG をアクティブ化します。
ステップ 16	**end**	コンフィギュレーション インターフェイス モードを終了します。
ステップ 17	**show ip device tracking all**	設定を確認します。
ステップ 18	**show ip verify source interface** *interface-id*	IP ソース ガードの設定を確認します。スタティック ホストの IPSG 許可 ACL を表示します。

次に、プライベート VLAN ホスト ポート上で IP フィルタを使用してスタティック ホスト用 IPSG をイネーブルにする例を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int gigabitethernet0/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface             STATE
-----------------------------------------------------------------------
40.1.1.24       0000.0000.0304  200  FastEthernet0/3       ACTIVE
```

```
40.1.1.20       0000.0000.0305  200  FastEthernet0/3        ACTIVE
40.1.1.21       0000.0000.0306  200  FastEthernet0/3        ACTIVE
40.1.1.22       0000.0000.0307  200  FastEthernet0/3        ACTIVE
40.1.1.23       0000.0000.0308  200  FastEthernet0/3        ACTIVE
```

出力には、インターフェイス Fa0/3 上で学習された 5 つの有効な IP-MAC バインディングが表示されています。プライベート VLAN の場合、バインディングはプライマリ VLAN ID に関連付けられます。そのため、この例では、プライマリ VLAN ID 200 が、テーブル内に表示されています。

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/3      ip trk       active       40.1.1.23                           200
Fa0/3      ip trk       active       40.1.1.24                           200
Fa0/3      ip trk       active       40.1.1.20                           200
Fa0/3      ip trk       active       40.1.1.21                           200
Fa0/3      ip trk       active       40.1.1.22                           200
Fa0/3      ip trk       active       40.1.1.23                           201
Fa0/3      ip trk       active       40.1.1.24                           201
Fa0/3      ip trk       active       40.1.1.20                           201
Fa0/3      ip trk       active       40.1.1.21                           201
Fa0/30/3      ip trk       active       40.1.1.22                           201
```

出力には、プライマリおよびセカンダリの両方の VLAN 上に 5 つの有効な IP-MAC バインディングが存在していることが表示されます。

IP ソース ガード情報の表示

IP ソース ガード情報を表示するには、表 20-4 に示す、1 つまたは複数の特権 EXEC コマンドを使用します。

表 20-4　IP ソース ガード情報を表示するためのコマンド

コマンド	目的
show ip source binding	スイッチの IP 送信元バインディングを表示します。
show ip verify source	スイッチの IP ソース ガード設定を表示します。

CHAPTER 21

ダイナミック ARP 検査の設定

この章では、Cisco ME 3400E スイッチにダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査を設定する方法について説明します。この機能により、同じ VLAN（仮想 LAN）内の他のポートの無効な ARP 要求や応答を信頼しないようにして、スイッチでの悪意のある攻撃を回避できます。

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

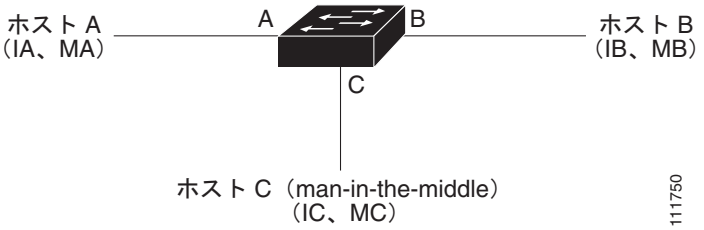
- 「ダイナミック ARP 検査の概要」（P.21-1）
- 「ダイナミック ARP 検査の設定」（P.21-5）
- 「ダイナミック ARP 検査情報の表示」（P.21-15）

ダイナミック ARP 検査の概要

ARP では、IP アドレスを MAC（メディア アクセス制御）アドレスにマッピングすることでレイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現しています。たとえば、ホスト B がホスト A に情報を送信しようとしていて、ARP キャッシュ内にホスト A の MAC アドレスがないとします。ホスト B は、ブロードキャスト ドメイン内のすべてのホストに対してブロードキャスト メッセージを生成し、ホスト A の IP アドレスに関連する MAC アドレスを取得します。ブロードキャスト ドメイン内のすべてのホストは ARP 要求を受信し、ホスト A は MAC アドレスで応答します。ただし、ARP 要求を受信しなくても ARP がホストからの余計な応答を許可するために、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生する可能性があります。攻撃のあと、攻撃下にあるデバイスからのすべてのトラフィックは攻撃者のコンピュータを介してルータ、スイッチ、またはホストに流れていきます。

悪意のあるユーザは、サブネットに接続されているシステムの APR キャッシュをポイズニングし、サブネット上の他のホストへ向かうトラフィックを代行受信することで、ネットワーク上のレイヤ 2 ネットワークに接続されているホスト、スイッチ、ルータを攻撃します。図 21-1 は、ARP キャッシュ ポイズニングの例です。

図 21-1　ARP キャッシュ ポイズニング



ホスト A、B、C は、インターフェイス A、B、C 上のスイッチに接続されていて、すべてが同じサブネット上にあります。IP アドレスおよび MAC アドレスは括弧内に示してあります。たとえば、ホスト A は IP アドレス IA と MAC アドレス MA を使用しています。ホスト A は、ホスト B と IP レイヤで通信を行う必要がある場合、ARP 要求をブロードキャストし、IP アドレス IB に関連する MAC アドレスを取得します。スイッチおよびホスト B は、ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を含むホストの ARP バインディングを ARP キャッシュに入力します（たとえば IP アドレス IA が MAC アドレス MA にバインドされます）。ホスト B が応答すると、スイッチとホスト A は、IP アドレス IB と MAC アドレス MB が関連付けられているホストの ARP バインディングを持つ ARP キャッシュを読み込みます。

ホスト C は、IP アドレス IA（または IB）と MAC アドレス MC が関連付けられているホストのバインディングを持つ偽造 ARP 応答をブロードキャストすることで、スイッチ、ホスト A、ホスト B の ARP キャッシュをポイズニングできます。ポイズニングされた ARP キャッシュのあるホストは、IA または IB 向けのトラフィックの宛先 MAC アドレスとして MAC アドレス MC を使用します。つまりホスト C がそのトラフィックを代行受信します。ホスト C は IA および IB に関連付けられた本当の MAC アドレスを知っているので、代行受信したトラフィックを正しい MAC アドレスを宛先として使用することで、それらのホストに転送できるのです。ホスト C は、ホスト A からホスト B へのトラフィック ストリームに割り込んで、一般的な *man-in-the-middle* 攻撃を行います。

ダイナミック ARP 検査は、ネットワーク内の ARP パケットを検査するセキュリティ機能です。この検査では、無効な IP と MAC アドレスのバインディングを持つ ARP パケットを代行受信し、記録して、廃棄します。この機能により、ある種の man-in-the-middle 攻撃からネットワークを保護できます。

ダイナミック ARP 検査により、有効な ARP 要求および応答だけが、リレーされることが保証されます。スイッチは次のアクティビティを実行します。

- 信頼できないポート上のすべての ARP 要求および応答を代行受信します。
- ローカル ARP キャッシュの更新前、またはパケットが適切な宛先に転送される前に、代行受信された各パケットに有効な IP と MAC アドレスのバインディングがあるかを確認します。
- 無効な ARP パケットを廃棄します。

ダイナミック ARP 検査は、信頼できるデータベースである DHCP スヌーピング バインディング データベースに保存されている、有効な IP と MAC アドレスのバインディングに基づいて、ARP パケットの有効性を判断します。このデータベースは、DHCP スヌーピングが VLAN およびスイッチでイネーブルの場合に、DHCP スヌーピングによって構築されます。ARP パケットが信頼できるインターフェイスで受信される場合、スイッチはチェックなしにパケットを転送します。信頼できないインターフェイスでは、スイッチは有効な場合にだけパケットを転送します。

ip arp inspection vlan *vlan-range* グローバル コンフィギュレーション コマンドを使用して VLAN 単位でダイナミック ARP 検査をイネーブルにできます。設定の詳細については、「DHCP 環境でのダイナミック ARP 検査の設定」（P.21-7）を参照してください。

非 DHCP 環境では、ダイナミック ARP 検査は、スタティックに設定された IP アドレスを持つホストのユーザ設定 ARP Access Control List（ACL; アクセス コントロール リスト）に対して、ARP パケットを検証できます。ARP ACL は、**arp access-list** *acl-name* グローバル コンフィギュレーション コマ

ンドを使用して定義されます。設定の詳細については、「非 DHCP 環境の ARP ACL の設定」（P.21-9）を参照してください。スイッチは、廃棄されたパケットを記録します。ログ バッファの詳細については、「廃棄されたパケットのロギング」（P.21-5）を参照してください。

パケット内の IP アドレスが無効か、または ARP パケットの本体にある MAC アドレスがイーサネット ヘッダーで指定されているアドレスと一致しない場合に、ARP パケットを廃棄するようにダイナミック ARP 検査を設定できます。**ip arp inspection validate** {**[src-mac]** **[dst-mac]** **[ip]**} グローバル コンフィギュレーション コマンドを使用します。詳細については、「妥当性チェックの実行」（P.21-13）を参照してください。

インターフェイス信頼状態およびネットワーク セキュリティ

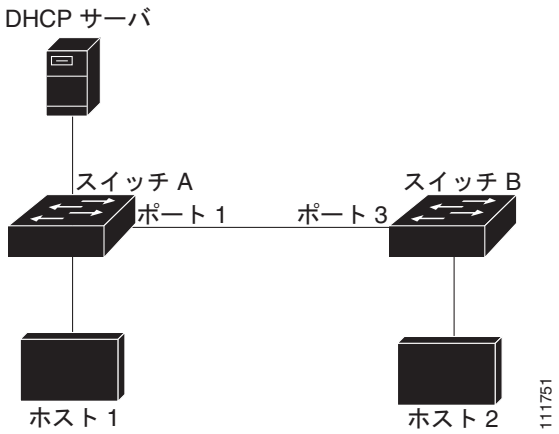
ダイナミック ARP 検査は、信頼状態とスイッチ上の各インターフェイスとを関連付けます。信頼できるインターフェイスに着信したパケットは、すべてのダイナミック ARP 検査の検証チェックを迂回し、信頼できないインターフェイスに着信したパケットはダイナミック ARP 検査の検証プロセスで処理されます。

一般的なネットワーク設定では、ホスト ポートに接続するすべてのスイッチ ポートを untrusted に設定し、スイッチに接続しているすべてのスイッチ ポートを trusted に設定します。このような設定では、指定したスイッチからネットワークに入ったすべての ARP パケットがセキュリティ チェックを迂回します。VLAN またはネットワーク内のその他の場所でその他の検証を行う必要はありません。信頼設定を **ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用して設定します。

注意　信頼状態は慎重に設定してください。インターフェイスを信頼すべきときに untrusted と設定すると、接続が切断される可能性があります。

図 21-2 では、スイッチ A およびスイッチ B の両方が、ホスト 1 およびホスト 2 のそれぞれを含む VLAN でダイナミック ARP 検査を実行しているとします。ホスト 1 およびホスト 2 がスイッチ A に接続している DHCP サーバから IP アドレスを取得すると、スイッチ A だけがホスト 1 の IP アドレスと MAC アドレスのペアをバインドします。このため、スイッチ A およびスイッチ B の間のインターフェイスが信頼できない場合、ホスト 1 からの ARP パケットはスイッチ B によって廃棄されます。ホスト 1 およびホスト 2 の間の接続は失われます。

図 21-2　ダイナミック ARP 検査がイネーブルである VLAN での ARP パケット検証



実際にインターフェイスを信頼できない場合にインターフェイスを信頼できるように設定してしまうと、ネットワークにセキュリティ ホールが残ってしまいます。スイッチ A でダイナミック ARP 検査が動作していない場合、ホスト 1 は簡単にホスト B の ARP キャッシュをポイズニングできます（スイッチ間のリンクが trusted に設定されている場合はホスト 2 も可能）。この状態は、スイッチ B がダイナミック ARP 検査を実行していても発生します。

ダイナミック ARP 検査は、ダイナミック ARP 検査を実行しているスイッチに接続している（信頼できないインターフェイス上の）ホストがネットワーク内の他のホストの ARP キャッシュをポイズニングしないようにするものです。ただし、ダイナミック ARP 検査では、ネットワークの他の部分にあるホストでは、ダイナミック ARP 検査を実行しているスイッチに接続しているホストのキャッシュに対するポイズニングは回避されません。

VLAN 内にあるスイッチの中で、ダイナミック ARP 検査を実行しているものとしていないものがある場合、そのようなスイッチに接続しているインターフェイスを untrusted に設定します。ただし、ダイナミック ARP 検査を実行していないスイッチからのパケットのバインディングを検証するには、ARP ACL を使用してダイナミック ARP 検査を実行するようにスイッチを設定します。そのようなバインディングをレイヤ 3 で判別できない場合、ダイナミック ARP 検査を実行しているスイッチを、ダイナミック ARP 検査を実行していないスイッチから分離します。設定の詳細については、「非 DHCP 環境の ARP ACL の設定」（P.21-9）を参照してください。

（注）　DHCP サーバおよびネットワークの設定により、VLAN 内のすべてのスイッチにある指定した ARP パケットを検査できない場合があります。

ARP パケットのレート制限

スイッチの CPU はダイナミック ARP 検査妥当性チェックを実行するので、着信 ARP パケットの数は、DoS 攻撃を受けないようにレート制限されています。デフォルトで、信頼できないインターフェイスのレートは、1 秒あたり 15 パケット（pps）です。信頼できるインターフェイスはレート制限されません。**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用してこの設定を変更できます。

着信 ARP パケットのレートが設定された制限を超えた場合、スイッチはポートを errdisable ステートにします。ユーザが介入するまでポートは errdisable ステートのままになります。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用して、指定したタイムアウト期間の経過後にポートがこのステートから自動的に回復するように errdisable 回復をイネーブルにできます。

設定の詳細については、「着信 ARP パケットのレート制限」（P.21-11）を参照してください。

ARP ACL と DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP 検査では、有効な IP と MAC アドレスのバインディングのリスト用に DHCP スヌーピング バインディング データベースを使用します。

ARP ACL は DHCP スヌーピング バインディング データベース内のエントリよりも優先度が高くなります。**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して ACL を設定した場合、スイッチは ACL だけを使用します。スイッチは最初に ARP パケットとユーザ定義の ARP ACL を比較します。ARP ACL が ARP パケットを拒否した場合、DHCP スヌーピングによって読み込まれたデータベースに有効なバインディングがあっても、スイッチもパケットを拒否します。

廃棄されたパケットのロギング

スイッチがパケットを廃棄する際に、ログ バッファにエントリを配置してレート制限ベースでシステム メッセージを生成します。メッセージの生成後、スイッチはエントリをログ バッファから削除します。各ログ エントリには、受信 VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスなどのフロー情報が含まれています。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数、およびシステム メッセージを生成するのに指定した間隔で必要となるエントリ数を設定します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用してロギングされるパケットのタイプを指定できます。設定の詳細については、「ログ バッファの設定」（P.21-14）を参照してください。

ダイナミック ARP 検査の設定

- 「デフォルトのダイナミック ARP 検査の設定」（P.21-5）
- 「ダイナミック ARP 検査の設定時の注意事項」（P.21-6）
- 「DHCP 環境でのダイナミック ARP 検査の設定」（P.21-7）（DHCP 環境で必須）
- 「非 DHCP 環境の ARP ACL の設定」（P.21-9）（非 DHCP 環境で必須）
- 「着信 ARP パケットのレート制限」（P.21-11）（任意）
- 「妥当性チェックの実行」（P.21-13）（任意）
- 「ログ バッファの設定」（P.21-14）（任意）

デフォルトのダイナミック ARP 検査の設定

表 21-1 に、デフォルトのダイナミック ARP 検査の設定を示します。

表 21-1　デフォルトのダイナミック ARP 検査の設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブル。
インターフェイス信頼状態	すべてのインターフェイスが信頼できない。
着信 ARP パケットのレート制限	このレートは、信頼できないインターフェイス上で 15 pps に設定されています。ただし、1 台のホストが 1 秒間に 15 台の新規ホストに接続できるスイッチド ネットワークであると仮定しています。 信頼できるすべてのインターフェイスでは、レートは無制限です。 バースト インターバルは 1 秒に設定されています。
非 DHCP 環境の ARP ACL	ARP ACL は定義されません。
妥当性チェック	どの検証も実行されません。

表 21-1　デフォルトのダイナミック ARP 検査の設定 （続き）

機能	デフォルト設定
ログ バッファ	ダイナミック ARP 検査がイネーブルの場合、すべての拒否または廃棄 ARP パケットがログされます。 ログ内のエントリ数は 32 です。 システム メッセージの数は 1 秒あたり 5 つに制限されています。 ロギングレート インターバルは 1 秒です。
VLAN 単位ロギング	拒否または廃棄されたすべての ARP パケットがログされます。

ダイナミック ARP 検査の設定時の注意事項

- ダイナミック ARP 検査は着信セキュリティ機能で、発信チェックは実行しません。
- ダイナミック ARP 検査は、ダイナミック ARP 検査をサポートしていないスイッチや、この機能をイネーブルにしていないスイッチに接続されたホストでは有効ではありません。
man-in-the-middle 攻撃が単一のレイヤ 2 ブロードキャスト ドメインに限定されているため、ダイナミック ARP 検査チェックのあるドメインとチェックのないドメインとを分離します。この処置により、ダイナミック ARP 検査をイネーブルにしたドメイン内のホストの ARP キャッシュが保護されます。
- 着信 ARP 要求と ARP 応答内の IP と MAC アドレスのバインディングを確認する場合、ダイナミック ARP 検査は DHCP スヌーピング バインディング データベース内のエントリに依存します。IP アドレスがダイナミックに割り当てられている ARP パケットを許可するために、DHCP スヌーピングをイネーブルにしていることを確認します。設定の詳細については、第 20 章「DHCP 機能および IP ソース ガードの設定」を参照してください。

  DHCP スヌーピングがディセーブルの場合または非 DHCP 環境では、ARP ACL を使用してパケットを許可または拒否します。
- ダイナミック ARP 検査は、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポートでサポートされています。

（注）　RSPAN VLAN 上では、ダイナミック ARP 検査をイネーブルにしないでください。RSPAN VLAN 上でダイナミック ARP 検査をイネーブルにすると、ダイナミック ARP 検査パケットが、RSPAN 宛先ポートに到達しなくなる可能性があります。

- 物理ポートとチャネル ポートの信頼状態が一致した場合にだけ、物理ポートは EtherChannel ポート チャネルに加入できます。そうでない場合、物理ポートはポート チャネル内で停止したままになります。ポート チャネルは、チャネルに最初に加入した物理ポートの信頼状態を継承します。その結果、最初の物理ポートの信頼状態はチャネルの信頼状態と一致する必要がありません。

  逆にいえば、ポート チャネルの信頼状態を変更した場合、スイッチはチャネルを構成するすべての物理ポートの信頼状態を新規に設定します。
- ポート チャネルの動作レートは、チャネル内のすべての物理ポートを累積したものです。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定した場合、チャネル上に集約される全インターフェイスで合計 400 pps を受信します。EtherChannel ポートの着信 ARP パケットのレート

は、全チャネル メンバーからのパケットの着信レートを合計したものです。チャネルポート メンバーの着信 ARP パケットのレートを検査したあとに、EtherChannel ポートのレート制限を設定します。

物理ポート上の着信パケットのレートは、物理ポート設定ではなくポートチャネル設定に対してチェックされます。ポート チャネルのレート制限設定は、物理ポートの設定からは独立しています。

EtherChannel が設定レートよりも多くの ARP パケットを受信する場合、（すべての物理ポートを含む）チャネルは errdisable ステートになります。

- 着信トランク ポート上の ARP パケットのレートを制限していることを確認します。集約を反映して、複数のダイナミック ARP 検査対応 VLAN でパケットを処理するために、トランク ポートを高めのレートに設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用してレートを無制限にできます。1 つの VLAN でレート制限が高いと、ソフトウェアがポートを errdisable ステートにするときに、他の VLAN が DoS 攻撃を受けるおそれがあります。
- スイッチ上でダイナミック ARP 検査をイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーが無効になります。その結果、すべての ARP トラフィックが CPU に送信されます。

DHCP 環境でのダイナミック ARP 検査の設定

この手順は、2 つのスイッチがこの機能をサポートしている場合にダイナミック ARP 検査を設定する方法について説明します。図 21-2（P.21-3）で示しているように、ホスト 1 はスイッチ A に接続していて、ホスト 2 はスイッチ B に接続しています。両方のスイッチが、ホストが位置する VLAN 1 でダイナミック ARP 検査を実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同じ DHCP サーバから IP アドレスを取得します。したがって、スイッチ A にはホスト 1 およびホスト 2 のバインディングがあり、スイッチ B にはホスト 2 のバインディングがあります。

（注）　着信 ARP 要求と ARP 応答内の IP と MAC アドレスのバインディングを確認する場合、ダイナミック ARP 検査は DHCP スヌーピング バインディング データベース内のエントリに依存します。IP アドレスがダイナミックに割り当てられている ARP パケットを許可するために、DHCP スヌーピングをイネーブルにしていることを確認します。設定の詳細については、第 20 章「DHCP 機能および IP ソース ガードの設定」を参照してください。

1 つのスイッチだけがダイナミック ARP 検査をサポートしている場合の、この機能の設定の詳細については、「非 DHCP 環境の ARP ACL の設定」（P.21-9）を参照してください。

ダイナミック ARP 検査を設定するには、特権 EXEC モードで次の手順を行います。この手順を両方のスイッチで実行する必要があります。この手順は必須です。

	コマンド	目的
ステップ 1	**show cdp neighbors**	スイッチ間の接続を確認します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ip arp inspection *vlan*** *vlan-range*	ダイナミック ARP 検査を VLAN 単位でイネーブルにします。デフォルトで、ダイナミック ARP 検査はすべての VLAN でディセーブルに設定されています。 *vlan-range* では、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定します。指定できる範囲は 1 ～ 4094 です。 両方のスイッチに同じ VLAN ID を指定します。
ステップ 4	**interface** *interface-id*	他のスイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 6	**ip arp inspection trust**	スイッチ間の接続を trusted に設定します。 デフォルトでは、すべてのインターフェイスが untrusted です。 スイッチは、信頼できるインターフェイス上にある他のスイッチから受信した ARP パケットをチェックしません。単純にパケットを転送するだけです。 信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。スイッチは、無効なパケットを廃棄し、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。詳細については、「ログ バッファの設定」（P.21-14）を参照してください。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip arp inspection interfaces** **show ip arp inspection vlan** *vlan-range*	ダイナミック ARP 検査の設定を確認します。
ステップ 9	**show ip dhcp snooping binding**	DHCP バインディングを確認します。
ステップ 10	**show ip arp inspection statistics vlan** *vlan-range*	ダイナミック ARP 検査の統計情報をチェックします。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ダイナミック ARP 検査をディセーブルにするには、**no ip arp inspection vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。ポートを untrusted の状態に戻すには、**no ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

次は、VLAN 1 のスイッチ A でダイナミック ARP 検査を設定する方法の例です。スイッチ B でも同様の手順を実行します。

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境の ARP ACL の設定

この手順は、図 21-2（P.21-3）で示すスイッチ B がダイナミック ARP 検査または DHCP スヌーピングをサポートしていない場合に、ダイナミック ARP 検査を設定する方法を示しています。

スイッチ A のポート 1 を trusted に設定すると、スイッチ A およびホスト 1 はスイッチ B またはホスト 2 から攻撃される可能性があるため、セキュリティ ホールができてしまいます。この可能性をなくすため、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL を設定して VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックでなく、スイッチ A で ACL 設定を適用できない場合は、レイヤ 3 でスイッチ B とスイッチ A を分離し、ルータを使用してその間でパケットをルーティングする必要があります。

スイッチ A で ARP ACL を設定するには、特権 EXEC モードで次の手順を実行します。この手順は、非 DHCP 環境で必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**arp access-list** *acl-name*	ARP ACL を定義し、ARP アクセスリスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセス リストは定義されていません。 **（注）** ARP アクセス リストの最後には、暗黙の **deny ip any mac any** コマンドがあります。
ステップ 3	**permit ip host** *sender-ip* **mac host** *sender-mac* [**log**]	指定したホスト（ホスト 2）からの ARP パケットを許可します。 • *sender-ip* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。 • （任意）Access Control Entry（ACE; アクセス制御エントリ）が一致した場合にログバッファ内のパケットをログするために **log** を指定します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドをキーワード **matchlog** とともに設定した場合、一致も記録されます。詳細については、「ログ バッファの設定」（P.21-14）を参照してください。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 5	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]	ARP ACL を VLAN に適用します。デフォルトで、どの VLAN にも ARP ACL が定義されていません。 • *arp-acl-name* には、ステップ 2 で作成した ACL 名を指定します。 • *vlan-range* には、スイッチおよびホストが含まれる VLAN を指定します。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットを廃棄するために、**static** を指定します。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、パケットを拒否する明示的な拒否が ACL 内にないことを意味し、パケットが ACL 内の句に一致しないと DHCP バインディングがパケットの許可または拒否を決定します。 IP および MAC アドレスのバインディングだけを含む ARP パケットが ACL と比較されます。パケットは、アクセス リストが許可した場合にだけ許可されます。
ステップ 6	**interface** *interface-id*	スイッチ B に接続されたスイッチ A インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 8	**no ip arp inspection trust**	スイッチ B に接続しているスイッチ A インターフェイスを untrusted として設定します。 デフォルトでは、すべてのインターフェイスが untrusted です。 信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。スイッチは、無効なパケットを廃棄し、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。詳細については、「ログ バッファの設定」（P.21-14）を参照してください。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show arp access-list** [*acl-name*] **show ip arp inspection vlan** *vlan-range* **show ip arp inspection interfaces**	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ARP、ACL を削除するには、**no arp access-list** グローバル コンフィギュレーション コマンドを使用します。VLAN に付加されている ARP ACL を削除するには、**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。

次に、*host2* という ARP ACL を設定し、ホスト 2（IP アドレスが 1.1.1.1 で MAC アドレスが 0001.0001.0001）からの ARP パケットを許可し、ACL を VLAN 1 に適用し、スイッチ A のポート 1 を untrusted に設定する例を示します。

```
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no ip arp inspection trust
```

着信 ARP パケットのレート制限

スイッチの CPU はダイナミック ARP 検査妥当性チェックを実行するので、着信 ARP パケットの数は、DoS 攻撃を受けないようにレート制限されています。

着信 ARP パケットのレートが設定された制限を超えた場合、スイッチはポートを errdisable ステートにします。指定したタイムアウト期間の経過後、ポートがこのステートから自動的に回復するように errdisable 回復をイネーブルにしないと、ポートは errdisable ステートのままになります。

（注）　インターフェイスにレート制限を設定しない場合、インターフェイスの信頼状態の変更によって、レート制限がその信頼状態のデフォルト値に変更されます。レート制限を設定すると、インターフェイスはその信頼状態が変更された場合でも設定されたレート制限を維持します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

トランク ポートおよび EtherChannel ポートのレート制限の設定時の注意事項については、「ダイナミック ARP 検査の設定時の注意事項」（P.21-6）を参照してください。

着信 ARP パケットのレートを制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レート制限を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] | **none**}	インターフェイス上の着信 ARP 要求および応答のレートを制限します。 デフォルトのレートは信頼できないインターフェイスで 15 pps、信頼できるインターフェイスで無制限です。バースト インターバルは 1 秒に設定されています。 キーワードの意味は次のとおりです。 • **rate** *pps* では、1 秒間に処理される着信パケットの上限数を指定します。指定できる範囲は 0 ～ 2048 pps です。 • （任意）**burst interval** *seconds* では、高いレートの ARP パケットについてインターフェイスがモニタされる累積期間を秒単位で指定します。範囲は 1 ～ 15 です。 • **rate none** では、処理可能な着信 ARP パケットの上限を指定しません。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**errdisable recovery cause arp-inspection interval** *interval*	（任意）ダイナミック ARP 検査の errdisable ステートからのエラー回復をイネーブルにします。 デフォルトで、回復はディセーブルで、回復間隔は 300 秒です。 **interval** *interval* では、errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。
ステップ 7	**exit**	特権 EXEC モードに戻ります。
ステップ 8	**show ip arp inspection interfaces** **show errdisable recovery**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのレート制限設定に戻すには、**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。ダイナミック ARP 検査のエラー回復をディセーブルにするには、**no errdisable recovery cause arp-inspection** グローバル コンフィギュレーション コマンドを使用します。

妥当性チェックの実行

ダイナミック ARP 検査では、無効な IP/MAC アドレス バインディングのある ARP パケットを代行受信し、記録し、廃棄します。宛先 MAC アドレス、発信者 IP アドレスおよび対象 IP アドレス、送信元 MAC アドレスで追加チェックを実施するようにスイッチを設定できます。

着信 ARP パケットで特定のチェックを実施するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}	着信 ARP パケットで特定のチェックを実行します。デフォルトで、チェックは実行しません。 キーワードの意味は次のとおりです。 • **src-mac** では、ARP ボディ内の発信者 MAC アドレスに対して、イーサネット ヘッダーの送信元 MAC アドレスをチェックします。この検証は、ARP 要求と ARP 応答に両方に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、廃棄されます。 • **dst-mac** では、ARP 形式の対象 MAC アドレスに対して、イーサネット ヘッダーの宛先 MAC アドレスを検査します。この検証は、ARP 応答に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、廃棄されます。 • **ip** では、無効で予期しない IP アドレスの ARP 形式をチェックします。0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスがこれに該当します。発信者 IP アドレスは ARP 要求および応答すべてでチェックされ、対象 IP アドレスは ARP 応答でだけチェックされます。 少なくとも 1 つのキーワードを指定する必要があります。各コマンドは、以前のコマンドの設定を上書きします。たとえば、あるコマンドが **src** および **dst mac** 検証をイネーブルにし、2 番めのコマンドが IP 検証だけをイネーブルにした場合、2 番めのコマンドによって **src** および **dst mac** 検証はディセーブルになります。
ステップ 3	**exit**	特権 EXEC モードに戻ります。
ステップ 4	**show ip arp inspection vlan** *vlan-range*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

チェックをディセーブルにするには、**no ip arp inspection validate** [**src-mac**] [**dst-mac**] [**ip**] グローバル コンフィギュレーション コマンドを使用します。転送、廃棄、MAC 検証失敗、および IP 検証失敗パケットの統計情報を表示するには、**show ip arp inspection statistics** 特権 EXEC コマンドを使用します。

ログ バッファの設定

スイッチがパケットを廃棄する際に、ログ バッファにエントリを配置してレート制限ベースでシステム メッセージを生成します。メッセージの生成後、スイッチはエントリをログ バッファから削除します。各ログ エントリには、受信 VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスなどのフロー情報が含まれています。

ログバッファ エントリは、複数のパケットを表示できます。たとえば、インターフェイスが同じ ARP パラメータを持つ VLAN 上で多くのパケットを受信する場合、スイッチはパケットをログ バッファ内の 1 つのエントリに結合して、エントリの単一のシステム メッセージを生成します。

ログ バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに [--] が表示されます。このエントリに関してそれ以外の統計情報は表示されません。このエントリを表示で見る場合、ログ バッファ内のエントリ数を増やすか、ロギング レートを増やします。

ログ バッファを設定するには、特権 EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip arp inspection log-buffer** {**entries** *number* | **logs** *number* **interval** *seconds*}	ダイナミック ARP 検査ロギング バッファを設定します。 デフォルトで、ダイナミック ARP 検査がイネーブルの場合、拒否または廃棄 ARP パケットがログされます。ログ エントリ数は、32 です。システム メッセージの数は 1 秒あたり 5 つに制限されています。ロギングレート インターバルは 1 秒です。 キーワードの意味は次のとおりです。 • **entries** *number* では、バッファ内に記録されるエントリ数を指定します。指定できる範囲は 0 ～ 1024 です。 • **logs** *number* **interval** *seconds* では、指定した間隔でシステム メッセージを生成するためのエントリ数を指定します。 **logs** *number* に指定できる範囲は 0 ～ 1024 です。値を 0 に設定すると、エントリはログ バッファに配置されますが、システム メッセージが生成されません。 指定できる **interval** *seconds* の範囲は 0 ～ 86400 秒（1 日）です。値を 0 に設定すると、システム メッセージがただちに生成されます（ログ バッファは常に空になります）。 0 の間隔設定は、ログ設定 0 を上書きします。 **logs** および **interval** の設定は、相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合は、X を Y で割って（X/Y）求められたシステム メッセージ数が 1 秒間に送信されます。それ以外の場合は、Y を X で割って（Y/X）求められた間隔（秒）で 1 つのシステム メッセージが送信されます。

	コマンド	目的
ステップ 3	**ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	記録されるパケットのタイプを VLAN 単位で制御します。デフォルトで、すべての拒否および廃棄パケットが記録されます。用語 *logged* は、エントリはログ バッファに置かれてシステム メッセージが生成されることを意味します。 キーワードの意味は次のとおりです。 • *vlan-range* では、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定します。指定できる範囲は 1 ～ 4094 です。 • **acl-match matchlog** では、ACR ロギング設定に基づいたパケットを記録します。このコマンドでキーワード **matchlog** を指定し、**permit** または **deny** ARP アクセスリスト コンフィギュレーション コマンドでキーワード **log** を指定した場合、ACL で許可または拒否された ARP パケットが記録されます。 • **acl-match none** では、ACL と一致するパケットを記録しません。 • **dhcp-bindings all** では、DHCP バインディングと一致するパケットがすべて記録されます。 • **dhcp-bindings none** では、DHCP バインディングと一致するパケットが記録されません。 • **dhcp-bindings permit** では、DHCP バインディング許可パケットを記録します。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**show ip arp inspection log**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのログ バッファ設定に戻すには、**no ip arp inspection log-buffer** {**entries** | **logs**} グローバル コンフィギュレーション コマンドを使用します。デフォルトの VLAN ログ設定に戻すには、**no ip arp inspection vlan** *vlan-range* **logging** {**acl-match** | **dhcp-bindings**} グローバル コンフィギュレーション コマンドを使用します。ログ バッファをクリアするには、**clear ip arp inspection log** 特権 EXEC コマンドを使用します。

ダイナミック ARP 検査情報の表示

ダイナミック ARP 検査情報を表示するには、表 21-2 に示す特権 EXEC コマンドを使用します。

表 21-2　ダイナミック ARP 検査情報を表示するためのコマンド

コマンド	説明
show arp access-list [*acl-name*]	ARP ACL の詳細情報を表示します。

表 21-2　ダイナミック ARP 検査情報を表示するためのコマンド（続き）

コマンド	説明
show ip arp inspection interfaces [*interface-id*]	指定されたインターフェイスまたはすべてのインターフェイスに関して信頼状態と ARP パケットのレート制限を表示します。
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。VLAN を指定しない場合、または範囲を指定しない場合は、ダイナミック ARP 検査がイネーブル（アクティブ）である VLAN の情報だけが表示されます。

ダイナミック ARP 検査統計情報を消去するには、表 21-3 に示す特権 EXEC コマンドを使用します。

表 21-3　ダイナミック ARP 検査の統計情報を消去または表示するためのコマンド

コマンド	説明
clear ip arp inspection statistics	ダイナミック ARP 検査の統計情報を消去します。
show ip arp inspection statistics [**vlan** *vlan-range*]	指定した VLAN の転送パケット、廃棄パケット、MAC 確認エラー パケット、IP 確認エラー パケット、ACL の許可および拒否パケット、DHCP 許可および拒否パケットの統計情報が表示されます。VLAN を指定しない場合、または範囲を指定しない場合は、ダイナミック ARP 検査がイネーブル（アクティブ）である VLAN の情報だけが表示されます。

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インスペクション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

ダイナミック ARP 検査ロギング情報を消去するには、表 21-4 に示す特権 EXEC コマンドを使用します。

表 21-4　ダイナミック ARP 検査のロギング情報を消去または表示するためのコマンド

コマンド	説明
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファを消去します。
show ip arp inspection log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

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

CHAPTER 22

IGMP スヌーピングおよび MVR の設定

この章では、ローカル Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングを応用した Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）など、Cisco ME 3400E イーサネット アクセス スイッチ上で IGMP スヌーピングを設定する方法について説明します。また、IGMP フィルタリングを使用して、マルチキャスト グループ メンバシップを制御する手順、および IGMP スロットリング アクションを設定する手順についても説明します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのスイッチ コマンド リファレンス、および『*Cisco IOS IP Command Reference, Volume 3 of 3:Multicast*』*Release 12.2* の「IP Multicast Routing Commands」を参照してください。

- 「IGMP スヌーピングの概要」（P.22-1）
- 「IGMP スヌーピングの設定」（P.22-7）
- 「IGMP スヌーピング情報の表示」（P.22-15）
- 「MVR の概要」（P.22-17）
- 「MVR の設定」（P.22-19）
- 「MVR 情報の表示」（P.22-25）
- 「IGMP フィルタリングおよび IGMP スロットリングの設定」（P.22-25）
- 「IGMP フィルタリングおよび IGMP スロットリングの設定の表示」（P.22-30）

（注） IGMP スヌーピングや MVR などの機能を利用して IP マルチキャスト グループ アドレスを管理したり、スタティック IP アドレスを使用したりできます。

IGMP スヌーピングの概要

レイヤ 2 スイッチでは、IGMP スヌーピングを使用してレイヤ 2 インターフェイスをダイナミックに設定することにより、マルチキャスト トラフィックのフラッディングを抑制できるよう、マルチキャスト トラフィックが IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。IGMP スヌーピングでは、その名前が示すとおり、LAN スイッチによってホストとルータの間の IGMP 伝送がスヌーピングされ、マルチキャスト グループとメンバー ポートの追跡が行われます。スイッチは、特定のマルチキャスト グループのホストから IGMP レポートを受け取ると、転送テーブル

エントリにホストのポート番号を追加します。また、ホストから IGMP Leave Group メッセージを受け取ると、テーブル エントリからホスト ポートを削除します。さらに、マルチキャスト クライアントから IGMP メンバシップ レポートを受信しない場合、定期的にエントリを削除します。

（注）　IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャスト ルータは定期的に一般クエリーをすべての VLAN に送信します。このマルチキャスト トラフィックを必要とするすべてのホストは、Join 要求を送信し、これによって転送テーブルのエントリに追加されます。IGMP Join 要求の送信元である各グループについて、IGMP スヌーピング IP マルチキャスト転送テーブルの VLAN ごとに 1 つのエントリが作成されます。

スイッチは、MAC（メディア アクセス制御）アドレスベース グループでなく、IP マルチキャスト グループベースのブリッジングをサポートします。マルチキャスト MAC アドレスベース グループが設定されている場合に、設定中の IP アドレスが設定済みの MAC アドレス、または予約済みマルチキャスト MAC アドレス（224.0.0.xxx の範囲）に変換されると（エイリアスが作成されると）、コマンド エラーになります。スイッチでは IP マルチキャスト グループが使用されるため、アドレスのエイリアスに関する問題は発生しません。

IGMP スヌーピングを通じて学習する IP マルチキャスト グループは、ダイナミックです。ただし、**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用すれば、マルチキャスト グループをスタティックに設定できます。マルチキャスト グループ アドレスのグループ メンバシップをスタティックに設定すると、その設定は IGMP スヌーピングによるどの自動操作よりも優先されます。マルチキャスト グループ メンバシップのリストは、ユーザ側で定義した設定と IGMP スヌーピングにより学習された設定の両方で構成されます。

マルチキャスト トラフィックはルーティングの必要がないので、マルチキャスト インターフェイスを持たないサブネット内でも IGMP スヌーピングがサポートされるように IGMP スヌーピング クエリアを設定できます。IGMP スヌーピング クエリアの詳細については、「IGMP スヌーピング クエリアの設定」（P.22-13）を参照してください。

ポート スパニング ツリー、ポート グループ、または VLAN ID が変更された場合、VLAN 上のこのポートから IGMP スヌーピングにより学習されたマルチキャスト グループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

- 「IGMP バージョン」（P.22-2）
- 「マルチキャスト グループへの参加」（P.22-3）
- 「マルチキャスト グループからの脱退」（P.22-5）
- 「即時脱退」（P.22-6）
- 「IGMP の設定可能な Leave タイマー」（P.22-6）
- 「IGMP レポート抑制」（P.22-6）

IGMP バージョン

このスイッチでは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 がサポートされています。これらのバージョンは、スイッチ上で相互運用できます。たとえば、IGMP スヌーピングがイネーブルになっている IGMPv2 スイッチでは、ホストから IGMPv3 レポートを受信した場合、IGMPv3 レポートをマルチキャスト ルータに転送できます。

（注）　スイッチは、宛先マルチキャスト MAC アドレスだけに基づいた IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスまたはプロキシ レポートに基づくスヌーピングは、サポートしていません。

IGMPv3 スイッチは、IGMPv1 スイッチおよび IGMPv2 スイッチでのスヌーピング機能および IGMPv3 メンバシップ レポート メッセージのサポートを含む、Basic IGMPv3 Snooping Support（BISS）をサポートします。BISS が適用されることで、ネットワークに IGMPv3 ホストが含まれる場合、マルチキャスト トラフィックのフラッディングが抑制されます。また、IGMPv2 ホストまたは IGMPv1 ホストの IGMP スヌーピング機能とほぼ同じポート セットへトラフィックが制限されます。

（注）　IGMP フィルタリングまたは MVR を実行しているスイッチでは、IGMPv3 の Join メッセージおよび Leave メッセージはサポートされません。

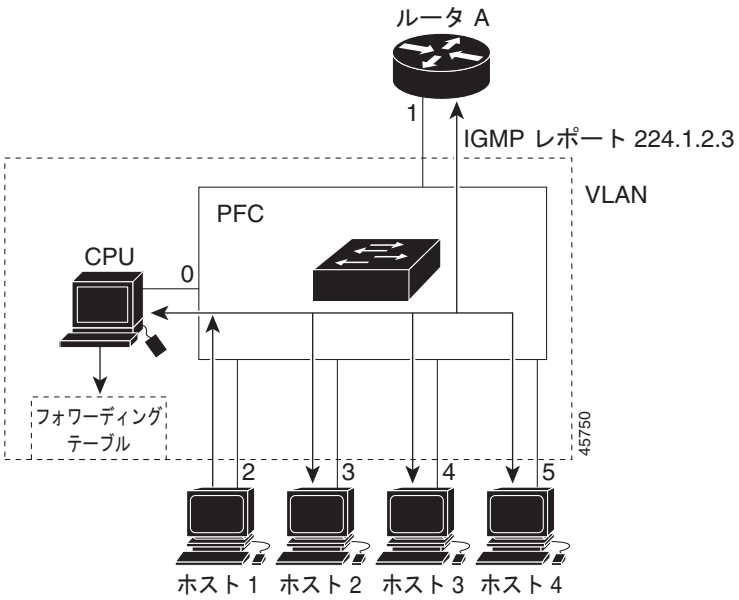
IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行しているデバイスとの間でメッセージの送受信を行うことができます。IGMPv3 および IGMP を含む SSM の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtssm5t.htm

マルチキャスト グループへの参加

スイッチに接続されたホストが IP マルチキャスト グループに参加する場合、このホストが IGMP バージョン 2 クライアントであれば、参加する IGMP マルチキャスト グループを指定して、非請求の IGMP Join メッセージを送信します。また、スイッチはルータから一般クエリーを受信すると、VLAN 内のすべてのポートにそのクエリーを転送します。マルチキャスト グループに参加しようとする IGMP バージョン 1 またはバージョン 2 のホストは、スイッチに Join メッセージを送信して応答します。グループのマルチキャスト転送テーブル エントリがまだ作成されていない場合は、スイッチの CPU により作成されます。また CPU では、Join メッセージを受信したインターフェイスの転送テーブル エントリへの追加も行われます。そのインターフェイスに関連付けられているホストは、マルチキャスト グループのマルチキャスト トラフィックを受信します。図 22-1 を参照してください。

図 22-1　最初の IGMP Join メッセージ



ルータ A からスイッチに送信された一般クエリーは、さらにスイッチから同じ VLAN のすべてのメンバーであるポート 2 ～ 5 に転送されます。ホスト 1 はマルチキャスト グループ 224.1.2.3 に参加し、このグループに IGMP メンバシップ レポート（IGMP Join メッセージ）をマルチキャストしようとします。スイッチの CPU は、IGMP レポート内の情報を使用して、ホスト 1 およびルータに接続されたポート番号を含む転送テーブル エントリを設定します（表 22-1 を参照）。

表 22-1　IGMP スヌーピング転送テーブル

宛先アドレス	パケット タイプ	Ports
224.1.2.3	IGMP	1, 2

スイッチのハードウェアは、IGMP 情報パケットをマルチキャスト グループの他のパケットと区別できます。スイッチング エンジンでは、テーブル内の情報に従って、IGMP パケットではない 224.1.2.3 マルチキャスト IP アドレス宛のフレームが、ルータおよびグループに参加しているホストに送信されます。

別のホスト（たとえばホスト 4）が同じグループに非請求の IGMP Join メッセージを送信する場合（図 22-2 を参照）、CPU はそのメッセージを受信し、転送テーブルにホスト 4 のポート番号を追加します（表 22-2 を参照）。ただし、転送テーブルにより指定される IGMP メッセージの送信先は CPU に限られるため、スイッチの他のポートにメッセージがフラッディングされることはありません。既知のマルチキャスト トラフィックはグループには転送されますが、CPU には転送されません。

図 22-2　2 番めのホストのマルチキャスト グループへの参加

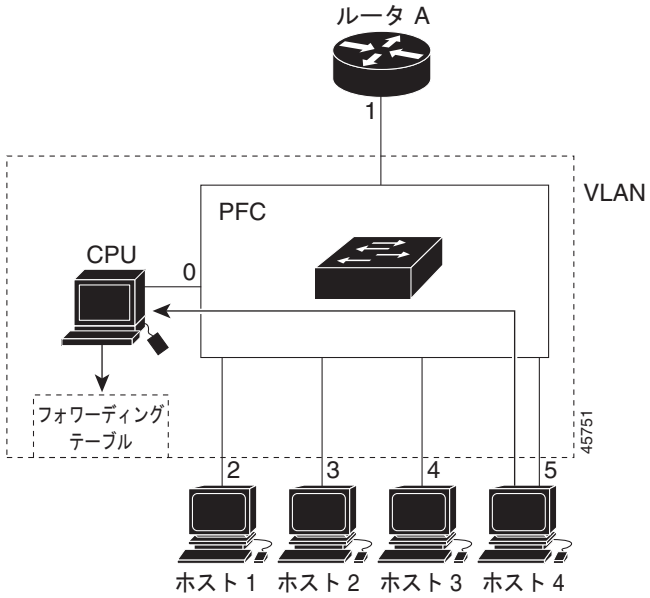


表 22-2　アップデートされた IGMP スヌーピング転送テーブル

宛先アドレス	パケット タイプ	Ports
224.1.2.3	IGMP	1, 2, 5

マルチキャスト対応ルータ ポートは、各レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。スイッチは、次のいずれか 1 つの方式でそれらのポートを学習します。

- IGMP クエリーおよび Protocol Independent Multicast（PIM）パケットのスヌーピング
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャスト ルータ ポートへのスタティックな接続

マルチキャスト グループからの脱退

ルータは定期的にマルチキャスト一般クエリーを送信し、スイッチはこのクエリーを VLAN のすべてのポートを通じて転送します。このクエリーを必要とするホストがこれに応答します。VLAN にマルチキャスト トラフィックを必要とするホストが少なくとも 1 つ存在すれば、ルータは引き続き VLAN にマルチキャスト トラフィックを転送します。スイッチがマルチキャスト グループ トラフィックを転送するのは、IGMP スヌーピングによって維持されている、IP マルチキャスト グループの転送テーブルにリストされているホストに限られます。

ホストは、マルチキャスト グループを脱退する場合、メッセージを送信せずに脱退することも、Leave メッセージを送信して脱退することもできます。スイッチは、ホストから Leave メッセージを受信すると、グループ固有のクエリーを送出して、そのインターフェイスに接続しているその他のデバイスが、特定のマルチキャスト グループのトラフィックを必要としているかどうかを学習します。次に、その MAC グループの転送テーブルをアップデートして、そのグループのマルチキャスト トラフィックを必要とするホストだけが転送テーブルにリストされるようにします。ルータは、VLAN からのレポートを受信しなかった場合は、IGMP キャッシュからその VLAN のグループを削除します。

即時脱退

即時脱退をサポートしているのは、IGMP バージョン 2 のホストだけです。

IGMP スヌーピングの即時脱退処理機能を使用すると、スイッチは、グループ固有のクエリーをインターフェイスに送信することなく、転送テーブルから Leave メッセージを送信したインターフェイスを削除できます。VLAN インターフェイスは、最初の Leave メッセージで指定されたマルチキャスト グループのマルチキャスト ツリーから削除されます。即時脱退処理によって、複数のマルチキャスト グループを同時に使用する場合でも、スイッチド ネットワーク上のすべてのホストに対して最適な帯域幅管理を行えます。

（注）　即時脱退処理機能は、各ポートに 1 つのホストしか接続されていない VLAN 上に限って使用してください。ポートに複数のホストが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のホストが誤って廃棄される可能性があります。

設定手順については、「IGMP 即時脱退のイネーブル化」（P.22-10）を参照してください。

IGMP の設定可能な Leave タイマー

ホストが現在も特定のマルチキャスト グループを必要としているかどうかを判別するため、スイッチがグループ固有のクエリーを送信してから待機する時間を設定できます。IGMP 脱退応答時間は、100 ～ 5000 ミリ秒の間で設定できます。このタイマーは、グローバルに設定できるほか、VLAN ごとに設定することもできます。グローバル設定は、脱退時間の VLAN 設定によって上書きされます。

設定手順については、「IGMP Leave タイマーの設定」（P.22-10）を参照してください。

IGMP レポート抑制

（注）　IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは IGMP レポート抑制を使用して、マルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求のみが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートのみを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。

マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

IGMP レポート抑制がディセーブルの場合は、すべての IGMP レポートがマルチキャスト ルータに転送されます。設定手順については、「IGMP レポート抑制のディセーブル化」（P.22-15）を参照してください。

IGMP スヌーピングの設定

IGMP スヌーピングを使用すると、スイッチは、IGMP パケットを検証できるほか、その内容に基づいて転送に関する判断を行えます。

- 「IGMP スヌーピングのデフォルト設定」（P.22-7）
- 「IGMP スヌーピングのイネーブル化またはディセーブル化」（P.22-7）
- 「マルチキャスト ルータ ポートの設定」（P.22-8）
- 「グループに参加するホストのスタティックな設定」（P.22-9）
- 「IGMP 即時脱退のイネーブル化」（P.22-10）
- 「IGMP Leave タイマーの設定」（P.22-10）
- 「TCN 関連コマンドの設定」（P.22-11）
- 「IGMP スヌーピング クエリアの設定」（P.22-13）
- 「IGMP レポート抑制のディセーブル化」（P.22-15）

IGMP スヌーピングのデフォルト設定

表 22-3 は、IGMP スヌーピングのデフォルト設定をまとめたものです。

表 22-3　IGMP スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブル
マルチキャスト ルータ	設定なし
マルチキャスト ルータの学習（スヌーピング）方式	PIM
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	設定なし
TCN[1] フラッド クエリー カウント	2
TCN クエリー請求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	イネーブル

1. TCN = Topology Change Notification（トポロジ変更通知）

IGMP スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IGMP スヌーピングはスイッチ上でグローバルにイネーブル化されています。グローバルにイネーブル化またはディセーブル化されている IGMP スヌーピングは、すべての既存 VLAN インターフェイスでもイネーブル化またはディセーブル化されます。IGMP スヌーピングは、すべての VLAN においてデフォルトでイネーブルになっていますが、VLAN 単位でイネーブルおよびディセーブルに設定することもできます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングに優先します。グローバル スヌーピングがディセーブルになっている場合、VLAN スヌーピングはイネーブルにできません。グローバル スヌーピングがイネーブルの場合は、VLAN スヌーピングをイネーブルまたはディセーブルのどちらにも設定できます。

スイッチ上で IGMP スヌーピングをグローバルにイネーブル化するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping**	すべての既存 VLAN インターフェイスで IGMP スヌーピングをグローバルにイネーブル化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

すべての VLAN インターフェイスで IGMP スヌーピングをグローバルにディセーブルにする場合は、**no ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。

VLAN インターフェイスで IGMP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id*	VLAN インターフェイスで IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 **（注）** VLAN スヌーピングをイネーブルにするには、事前に IGMP スヌーピングをグローバルにイネーブル化する必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN インターフェイスで IGMP スヌーピングをディセーブルにするには、指定された VLAN 番号について **no ip igmp snooping vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

マルチキャスト ルータ ポートの設定

マルチキャスト ルータ ポートを追加する（マルチキャスト ルータにスタティック接続を追加する）には、スイッチ上で **ip igmp snooping vlan mrouter** グローバル コンフィギュレーション コマンドを使用します。

（注） マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

マルチキャスト ルータへのスタティック接続をイネーブルに設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	マルチキャスト ルータの VLAN ID とインターフェイスをマルチキャスト ルータに指定します。 • 指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping mrouter** [**vlan** *vlan-id*]	VLAN インターフェイスで IGMP スヌーピングがイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN からマルチキャスト ルータ ポートを削除するには、**no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト ルータへのスタティック接続をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet0/2
Switch(config)# end
```

グループに参加するホストのスタティックな設定

ホストまたはレイヤ 2 ポートは通常、マルチキャスト グループにダイナミックに参加しますが、インターフェイスでホストをスタティックに設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id*	マルチキャスト グループのメンバーとしてレイヤ 2 ポートをスタティックに設定します。 • *vlan-id* には、マルチキャスト グループの VLAN ID を指定します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。 • *ip-address* には、グループ IP アドレスを指定します。 • *interface-id* にはメンバー ポートを指定します。物理インターフェイスまたはポート チャネル（1 ～ 48）を指定できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show ip igmp snooping groups**	メンバー ポートおよび IP アドレスを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

マルチキャスト グループからレイヤ 2 ポートを削除する場合は、**no ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、ポートでホストをスタティックに設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet0/1
Switch(config)# end
```

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルにすると、スイッチは、ポート上で IGMP バージョン 2 Leave メッセージを検出した時点でそのポートを削除します。即時脱退機能を使用するのは、VLAN の各ポートにレシーバーが 1 つ存在する場合だけです。

（注）　即時脱退は、IGMP バージョン 2 のホストに限ってサポートされています。

IGMP 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **immediate-leave**	VLAN インターフェイス上で IGMP 即時脱退をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping vlan** *vlan-id*	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN 上で IGMP 即時脱退をディセーブルにする場合は、**no ip igmp snooping vlan** *vlan-id* **immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 で IGMP 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

IGMP Leave タイマーの設定

IGMP Leave タイマーを設定するときは、次の注意事項に従ってください。

- 脱退時間は、グローバルに設定することも、VLAN ごとに設定することもできます。
- VLAN で脱退時間を設定すると、グローバル設定は無効となります。
- デフォルトの脱退時間は 1000 ミリ秒です。

- IGMP の設定可能な脱退時間は、IGMP バージョン 2 を実行しているホストに限りサポートされています。
- ネットワークの実際の脱退遅延時間は通常、設定した脱退時間になります。ただし、リアルタイムの CPU 負荷条件、ネットワーク遅延、インターフェイスを介して送信されたトラフィック量によっては、実際の脱退時間と設定した脱退時間に若干の誤差が生じることがあります。

IGMP の設定可能な Leave タイマーをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping last-member-query-interval** *time*	IGMP Leave タイマーをグローバルに設定します。指定できる範囲は 100 ～ 32768 ミリ秒です。デフォルト値は 1000 秒です。
ステップ 3	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time*	（任意）IGMP 脱退時間を VLAN インターフェイス上で設定します。指定できる範囲は 100 ～ 32768 ミリ秒です。 **（注）** VLAN で脱退時間を設定すると、グローバルに設定したタイマーは無効となります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping**	（任意）設定した IGMP 脱退時間を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP Leave タイマーをグローバルにリセットしてデフォルト設定に戻す場合は、**no ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

設定した IGMP 脱退時間設定を特定の VLAN から削除する場合は、**no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

TCN 関連コマンドの設定

ここでは、TCN イベント中にフラッディングされたマルチキャスト トラフィックの制御方法について説明します。

- 「TCN イベント後のマルチキャスト フラッディング時間の制御」（P.22-11）
- 「フラッディング モードからの回復」（P.22-12）
- 「TCN イベント中のマルチキャスト フラッディングのディセーブル化」（P.22-13）

TCN イベント後のマルチキャスト フラッディング時間の制御

ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用すると、TCN イベント後にマルチキャスト トラフィックがフラッディングされる時間を制御できます。このコマンドにより、TCN イベント後にマルチキャスト データ トラフィックが フラッディングされる間の一般クエリー数を設定します。TCN イベントが発生するのは、クライアントの位置が変更され、レシーバーの位置は同じポートのままブロッキングからフォワーディングに変更された場合や、ポートが Leave メッセージを送信せずにダウンした場合などです。

ip igmp snooping tcn flood query count コマンドを使用して TCN フラッディング クエリー数を 1 に設定した場合、フラッディングは一般クエリーを 1 つ受信した時点で停止します。カウントを 7 に設定すると、TCN イベントによるマルチキャスト トラフィックのフラッディングは、7 つの一般的クエリーを受信するまで継続します。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

TCN フラッディング クエリー数を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping tcn flood query count** *count*	マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ～ 10 です。デフォルトのフラッディング クエリー数は 2 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	TCN 設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

フラッディング クエリー数をデフォルト値に戻す場合は、**no ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。

フラッディング モードからの回復

トポロジ変更が発生すると、スパニング ツリーのルートはグループ マルチキャスト アドレス（0.0.0.0.）を使用して特別な IGMP Leave メッセージ（グローバル Leave とも呼ぶ）を送信します。ただし、**ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドをイネーブルにしている場合、スイッチはスパニング ツリーのルートであるかどうかに関係なく、グローバル Leave メッセージを送信します。ルータはこの特別な Leave メッセージを受信すると、ただちに一般クエリーを送信します。これにより、TCN イベント中にフラッディング モードからの回復処理が迅速に行われます。このコンフィギュレーション コマンドがイネーブルかディセーブルかに関わらず、スイッチがスパニング ツリーのルートである場合は常に、Leave メッセージが送信されます。デフォルトでは、クエリー請求はディセーブルに設定されています。

スイッチがスパニング ツリーのルートであるかどうかに関係なく、スイッチによるグローバル Leave メッセージの送信をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping tcn query solicit**	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP 脱退メッセージ（グローバル脱退）を送信します。デフォルトでは、クエリー請求はディセーブルに設定されています。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	TCN 設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

クエリー請求をデフォルトに戻すときは、**no ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。

TCN イベント中のマルチキャスト フラッディングのディセーブル化

スイッチが TCN を受信すると、2 つの一般的なクエリーが受信されるまで、マルチキャスト トラフィックはすべてのポートに対してフラッディングします。異なるマルチキャスト グループに参加している接続ホストを持つポートがスイッチに多数ある場合、フラッディングがリンクの容量を超過し、パケット損失を招くことがあります。**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用すると、この動作を制御できます。

インターフェイスのマルチキャスト フラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 4	**no ip igmp snooping tcn flood**	スパニング ツリー TCN イベント中のマルチキャスト トラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイスのマルチキャスト フラッディングはイネーブルに設定されています。
ステップ 5	**exit**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping**	TCN 設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスでマルチキャスト フラッディングを再度イネーブルにするには、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP スヌーピング クエリアの設定

IGMP スヌーピング クエリアを設定するときは、次の注意事項に従ってください。

- グローバル コンフィギュレーション モードで VLAN を設定します。
- VLAN インターフェイス上に IP アドレスを設定します。イネーブルの場合、IGMP スヌーピング クエリアは IP アドレスをクエリー送信元アドレスとして使用します。
- VLAN インターフェイスに IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されているグローバル IP アドレスの使用を試みます。グローバル IP アドレスが指定されていない場合は、IGMP スヌーピング クエリアは（存在する場合）VLAN Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）IP アドレスの使用を試みます。SVI IP アドレスがない場合は、スイッチはスイッチに設定されている使用可能な最初の IP アドレスを使用します。使用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピング クエリアは、スイッチで使用可能な IP アドレスが見つからなければ、IGMP 一般クエリーの生成を行いません。
- IGMP スヌーピング クエリアは、IGMP バージョン 1 および 2 をサポートしています。

- 管理上のイネーブルの場合、IGMP スヌーピング クエリアはネットワーク内でマルチキャスト ルータを検出すると非クエリア ステートに移行します。
- 管理上のイネーブルの場合、IGMP スヌーピング クエリアは次の条件下にあるときは操作上のディセーブル ステートに移行します。
  - IGMP スヌーピングが VLAN でディセーブルに設定されている。
  - PIM が、対応する VLAN の SVI でイネーブルに設定されている。

VLAN の IGMP スヌーピング クエリア機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping querier**	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 3	**ip igmp snooping querier** *ip_address*	（任意）IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 **（注）** スイッチ上で IP アドレスを検出できない場合、IGMP スヌーピング クエリアは IGMP 一般クエリーを生成しません。
ステップ 4	**ip igmp snooping querier query-interval** *interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
ステップ 5	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*]	（任意）TCN クエリアの間隔を設定します。指定できる数の範囲は 1 ～ 10 です。指定できる間隔の範囲は 1 ～ 255 秒です。
ステップ 6	**ip igmp snooping querier timer expiry** *timeout*	（任意）IGMP クエリアの期限が切れるまでの時間を設定します。指定できる範囲は 60 ～ 300 秒です。
ステップ 7	**ip igmp snooping querier version** *version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip igmp snooping vlan** *vlan-id*	（任意）VLAN インターフェイスで IGMP スヌーピング クエリアがイネーブルになっていることを確認します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

IGMP レポート抑制のディセーブル化

（注）　IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

IGMP レポート抑制は、デフォルトではイネーブルに設定されています。この機能がイネーブルになると、スイッチはマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけ転送します。レポート抑制がディセーブルの場合は、すべての IGMP レポートがマルチキャスト ルータに転送されます。

IGMP レポート抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ip igmp snooping report-suppression**	IGMP レポート抑制をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	IGMP レポート抑制がディセーブルであることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP レポート抑制を再びイネーブルにする場合は、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。

IGMP スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの IGMP スヌーピング情報を表示できます。IGMP スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

IGMP スヌーピング情報を表示するには、表 22-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 22-4　IGMP スヌーピング情報を表示するためのコマンド

コマンド	目的
show ip igmp snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN のスヌーピング設定情報を表示します。 （任意）単一の VLAN に関する情報を表示するには、**vlan** *vlan-id* を使用します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ip igmp snooping groups [**count** |**dynamic** [**count**] | **user** [**count**]]	スイッチまたは特定のパラメータに関するマルチキャスト テーブル情報を表示します。 • **count**：実際のエントリではなく、指定されたコマンド オプションに対するエントリの総数を表示します。 • **dynamic**：IGMP スヌーピングを通して学習されたエントリを表示します。 • **user**：ユーザが設定したマルチキャスト エントリに限って表示します。
show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user** [**count**]]	マルチキャスト VLAN または VLAN の特定のパラメータに関するマルチキャスト テーブル情報を表示します。 • *vlan-id*：VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • **count**：実際のエントリではなく、指定されたコマンド オプションに対するエントリの総数を表示します。 • **dynamic**：IGMP スヌーピングを通して学習されたエントリを表示します。 • *ip_address*：指定されたグループ IP アドレスを持つマルチキャスト グループの特性を表示します。 • **user**：ユーザが設定したマルチキャスト エントリに限って表示します。
show ip igmp snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習された、または手動で設定されたマルチキャスト ルータ インターフェイスに関する情報を表示します。 **（注）** IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらはダイナミックに学習されるインターフェイスです。 （任意）単一の VLAN に関する情報を表示するには、**vlan** *vlan-id* を使用します。
show ip igmp snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した IGMP クエリー メッセージの IP アドレスおよび着信ポートに関する情報を表示します。 （任意）単一の VLAN に関する情報を表示するには、**vlan** *vlan-id* を使用します。
show ip igmp snooping querier [**vlan** *vlan-id*] **detail**	VLAN 内で直前に受信した IGMP クエリー メッセージの IP アドレスおよび着信ポートに関する情報と、VLAN 内の IGMP スヌーピング クエリアの設定および動作ステートを表示します。

これらのコマンドのキーワードおよびオプションの詳細については、このリリースのコマンド リファレンスを参照してください。

MVR の概要

MVR は、イーサネット リングベースのサービス プロバイダー ネットワークで、マルチキャスト トラフィックを広範囲に配信するアプリケーション（サービス プロバイダー ネットワークでの複数の TV チャネルのブロードキャストなど）用に設計された機能です。MVR により、ポート上の参加者は、ネットワーク全般のマルチキャスト VLAN のマルチキャスト ストリームに対して参加または脱退を設定できます。これにより、各参加者が別々の VLAN に属しながら、ネットワーク上で 1 つのマルチキャスト VLAN を共有できます。MVR を使用すると、マルチキャスト VLAN 内でマルチキャスト ストリームを継続的に送信しながら、帯域幅およびセキュリティを確保するために、参加者 VLAN からストリームを隔離できます。

MVR では、参加者ポートが、IGMP の Join メッセージまたは Leave メッセージを送信することによって、マルチキャスト ストリームに参加またはマルチキャスト ストリームから脱退（Join または Leave）することを前提にしています。これらのメッセージは、イーサネット接続の IGMP バージョン 2 互換ホストから発信できます。MVR は IGMP スヌーピングの基本メカニズムで動作しますが、2 つの機能は相互に独立して動作します。それぞれ、他方の動作に影響を与えることなくイネーブルまたはディセーブルにできます。ただし、IGMP スヌーピングと MVR がともにイネーブルの場合、MVR は、MVR 上で設定されたマルチキャスト グループからの Join メッセージおよび Leave メッセージに対してだけ対応します。それ以外のマルチキャスト グループからの Join メッセージおよび Leave メッセージは、IGMP スヌーピングによって管理されます。

スイッチの CPU は、MVR IP マルチキャスト ストリームおよびスイッチ転送テーブル上の関連 IP マルチキャスト グループを識別し、IGMP メッセージを代行受信します。また、レシーバーが送信元とは別の VLAN に属する場合でも、参加者をマルチキャスト ストリームのレシーバーとしてテーブルに追加したりテーブルから削除したりするように転送テーブルを書き換えます。この転送動作により、さまざまな VLAN 間で伝送されるトラフィックが選択的に許可されます。

スイッチの MVR 動作は、互換モードまたはダイナミック モードに設定できます。

- 互換モードの場合、MVR ホストが受信したマルチキャスト データは、ポートの MVR ホスト メンバシップに関係なく、すべての MVR データ ポートに転送されます。マルチキャスト データは、IGMP レポートまたは MVR スタティック設定を使用して、MVR ホストが参加したレシーバー ポートにだけ転送されます。また、MVR ホストから受信した IGMP レポートは、スイッチに設定された MVP データ ポートからは転送されません。
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは MVR スタティック設定を使用して、MVR ホストが参加した MVR データ ポートおよびクライアント ポートからだけ転送されます。MVR ホストから受信した IGMP レポートは、スイッチ内のすべての MVR データ ポートからも転送されます。これにより、スイッチが互換モードで動作している場合と異なり、MVR データ ポート リンクで不要な帯域幅が使用されなくなります。

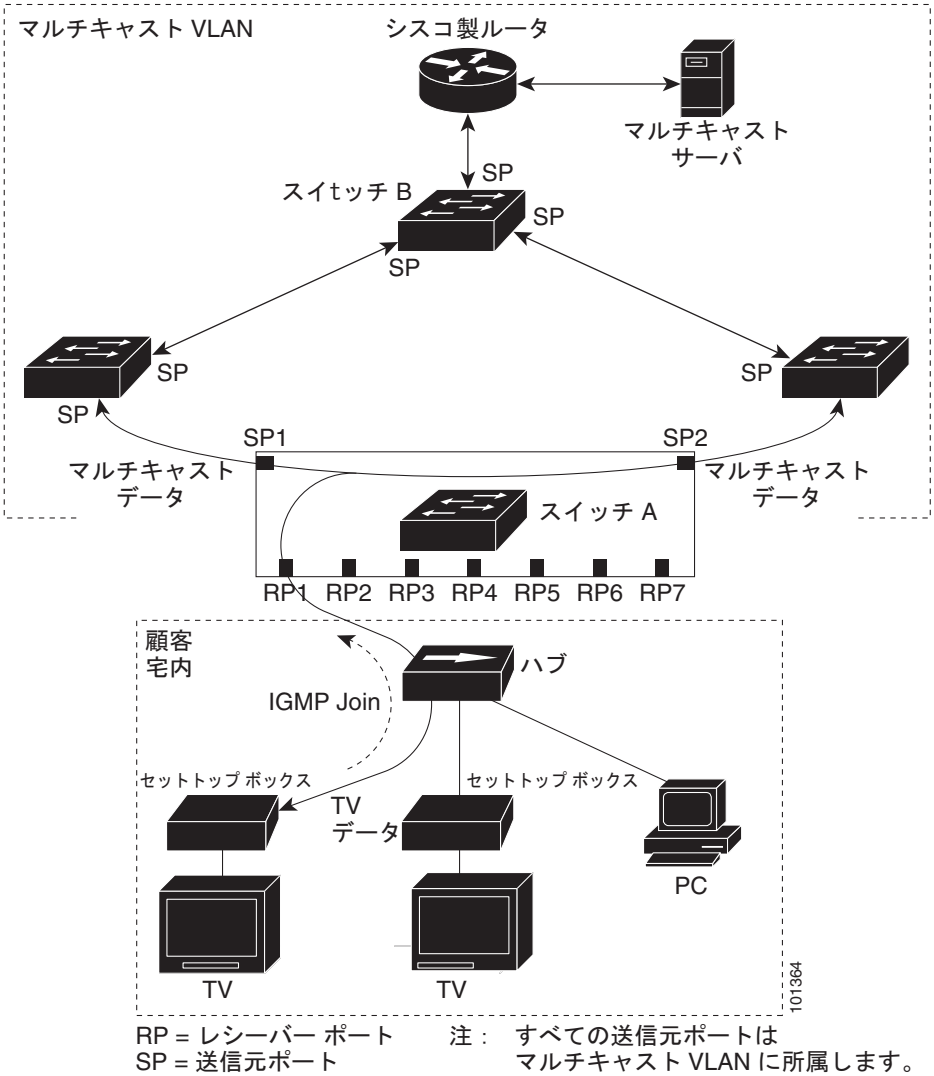
MVR に参加するのは、レイヤ 2 ポートだけです。ポートは MVR レシーバー ポートとして設定する必要があります。各スイッチでサポートされる MVR マルチキャスト VLAN は 1 つだけです。

マルチキャスト TV アプリケーションでの MVR の使用方法

マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備した TV で、マルチキャスト ストリームを受信できます。MVR のレシーバー ポートとして設定されたスイッチ ポートである各参加者ポートには、セットトップ ボックスまたは PC を複数接続できます。図 22-3 は設定例です。セットトップ ボックスまたは PC には、DHCP によって IP アドレスが割り当てられます。参加者がチャネルを選択すると、セットトップ ボックスまたは PC では、対応するマルチキャストに参加するために、スイッチ A に対して IGMP レポートが送信されます。IGMP レポートが設定済み IP マルチキャスト グループ アドレスの 1 つに一致した場合、スイッチの CPU は、ハードウェアのアドレス テーブルを変更し、指定されたマルチキャスト ストリームをマルチキャスト VLAN から受信した場合

にそのマルチキャスト ストリームを転送する宛先として、このレシーバー ポートと VLAN をアドレス テーブルに追加します。マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを、MVR 送信元ポートと呼びます。

図 22-3　　MVR の例



RP = レシーバー ポート
SP = 送信元ポート

注：　すべての送信元ポートは
マルチキャスト VLAN に所属します。

参加者がチャネルを変更するか、TV をオフにすると、セットトップ ボックスからマルチキャスト ストリームの IGMP Leave メッセージが送信されます。スイッチの CPU は、レシーバー ポートの VLAN を介して、MAC ベースの一般クエリーを送信します。このグループに参加している他のセットトップ ボックスが VLAN 内に存在する場合、そのセットトップ ボックスはクエリーで指定された最大応答時間内に応答しなければなりません。応答を受信しない場合、CPU はこのグループの転送宛先からレシーバー ポートを除外します。

即時脱退機能がイネーブルになっていない場合、スイッチはレシーバー ポートの参加者から IGMP Leave メッセージを受信すると、そのポートに IGMP クエリーを送信して IGMP グループ メンバシップ レポートを待ちます。設定された時間内にレポートが届かないと、レシーバー ポートがマルチキャスト グループ メンバシップから削除されます。即時脱退機能がイネーブルになっている場合、IGMP Leave メッセージを受信したレシーバー ポートからは IGMP クエリーは送信されません。Leave メッ

セージの受信後ただちに、マルチキャスト グループ メンバシップからレシーバー ポートが削除されるので、脱退のための待ち時間が短縮されます。即時脱退機能は、1 つの受信デバイスを接続したレシーバー ポートに限ってイネーブルにしてください。

MVR では、各 VLAN に属する複数の参加者に対して TV チャネルのマルチキャスト トラフィックを重複して送信する必要がありません。すべてのチャネルに対するマルチキャスト トラフィックが、VLAN トランクで一度に送信されます（マルチキャスト VLAN に限る）。IGMP の Leave メッセージおよび Join メッセージは、参加者ポートが割り当てられている VLAN 内で送信されます。これらのメッセージにより、レイヤ 3 デバイス（スイッチ B）上でマルチキャスト VLAN のマルチキャスト トラフィック ストリームがダイナミックに登録されます。アクセス レイヤ スイッチ（スイッチ A）は、マルチキャスト VLAN から別の VLAN 上の参加者ポートにトラフィックが転送されるように転送動作を変更し、2 つの VLAN 間で伝送されるトラフィックを選択的に許可します。

IGMP レポートは、マルチキャスト データと同じ IP マルチキャスト グループ アドレスに送信されます。スイッチ A の CPU は、レシーバー ポートからの IGMP の Join メッセージおよび Leave メッセージをすべて取り込み、MVR モードに基づいて、送信元（アップリンク）ポートのマルチキャスト VLAN に転送する必要があります。

MVR の設定

- 「MVR のデフォルト設定」（P.22-19）
- 「MVR 設定時の注意事項および制限事項」（P.22-20）
- 「MVR グローバル パラメータの設定」（P.22-20）
- 「アクセス ポート上での MVR の設定」（P.22-22）
- 「トランク ポート上での MVR の設定」（P.22-23）

MVR のデフォルト設定

表 22-5 は、MVR のデフォルト設定をまとめたものです。

表 22-5　MVR のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位でディセーブル
マルチキャスト アドレス	設定なし
クエリー応答時間	0.5 秒
マルチキャスト VLAN	VLAN 1
モード	互換
インターフェイス（ポート単位）のデフォルト	レシーバーおよび送信元のどちらのポートでもない
即時脱退	すべてのポートでディセーブル

MVR 設定時の注意事項および制限事項

- スイッチのレシーバー ポートはそれぞれ別々の VLAN に属していてもかまいませんが、マルチキャスト VLAN には属することができません。
- レシーバー ポートとしては、トランク ポートまたはアクセス ポートを設定できます。
- MVR モードが互換に設定されている（デフォルト）場合、設定できる MVR グループの最大数は 512 です。
- MVR モードがダイナミックに設定されている場合、各スイッチ上で設定できるマルチキャスト エントリ（MVR グループ アドレス）の最大数は 2000 です。同時にアクティブにできるマルチキャスト ストリームの最大数（受信できる TV チャネルの最大数）は 512 です。この上限に達するすると、「*ハードウェアで規定されたグループ数の上限に達しました*」という内容のメッセージが生成されます。ただし、ポート上に IGMP Join が存在する場合、または **mvr vlan** *vlan-id* **group** *ip-address* インターフェイス コンフィギュレーション コマンドを使用してポートがグループに参加するよう設定した場合は、ハードウェア エントリが発生します。
- 各スイッチ上に設定できるマルチキャスト エントリ（MVR グループ アドレス）の最大数（受信できる TV チャネルの最大数）は 512 です。
- 送信元 VLAN で受信されレシーバー ポートから送信される MVR マルチキャスト データの Time To Live（TTL; 存続可能時間）は、スイッチを通過するたびに値が 1 ずつ減少します。
- スイッチの MVR では、MAC マルチキャスト アドレスではなく IP マルチキャスト アドレスが使用されるため、スイッチ上ではエイリアスが設定された IP マルチキャスト アドレスを使用できます。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス（224.0.0.xxx 範囲内）を設定する必要はありません。
- プライベート VLAN ポートには MVR を設定しないでください。
- スイッチ上でマルチキャスト ルーティングがイネーブルの場合、MVR はサポートされません。MVR がイネーブルの場合にマルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにすると、MVR がディセーブルになり、警告メッセージが表示されます。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの場合に、MVR をイネーブルにしようとすると、MVR をイネーブルにする操作が取り消され、エラーメッセージが表示されます。
- MVR はスイッチで IGMP スヌーピングと共存できます。
- MVR レシーバー ポートで受信された MVR データは、MVR 送信元ポートには転送されません。
- MVR では、IGMPv3 メッセージはサポートされていません。
- Cisco IOS リリース 12.2(52)SE を使用するときは、**mvr ringmode flood** グローバル コンフィギュレーション コマンドを入力することで、メンバーとして検出されたポートにリング トポロジにおけるデータ フォワーディングを制限し、マルチキャスト ルータ ポートへのフォワーディングを排除できます。これにより、MVR マルチキャスト トラフィックの転送方向とユニキャスト トラフィックの転送方向が逆の場合でも、リング環境でユニキャスト トラフィックが廃棄されるのを回避できます。

MVR グローバル パラメータの設定

デフォルト設定を使用する場合には、オプションの MVR パラメータを設定する必要はありません。デフォルトのパラメータ値を変更する場合（MVR VLAN を除く）は、先に MVR をイネーブルにする必要があります。

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

MVR パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	**mvr group** *ip-address* [*count*]	スイッチ上に IP マルチキャスト アドレスを設定します。または、*count* パラメータを使用して、連続した MVR グループ アドレスを設定します。count に指定できる値の範囲は 1 ～ 2000 です。ただし、MVR モードが互換に設定されている場合、スイッチ上に設定できる連続した MVR グループ アドレスの最大数は 512 です。モードがダイナミックに設定されている場合、作成できる MVR グループの最大数は 2000 です。デフォルトは 1 です。 このアドレス宛のマルチキャスト データは、スイッチ上のすべての送信元ポート、およびこのマルチキャスト アドレス上のデータを受信するように設定されているすべてのレシーバー ポートに送信されます。各マルチキャスト アドレスは、1 つの TV チャネルに対応付けられます。
ステップ 4	**mvr querytime** *value*	（任意）マルチキャスト グループ メンバシップからレシーバー ポートを削除するまでに、そのレシーバー ポートで IGMP レポート メンバシップを待機する最大待機時間を指定します。値は、1/10 秒単位で指定します。指定できる範囲は 1 ～ 100 で、デフォルトは 5/10、つまり 0.5 秒です。
ステップ 5	**mvr vlan** *vlan-id*	（任意）マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートはこの VLAN に属する必要があります。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。デフォルトは VLAN 1 です。
ステップ 6	**mvr mode** {**dynamic** | **compatible**}	（任意）MVR の動作モードを指定します。 • **dynamic**：送信元ポートでのダイナミック MVR メンバシップを使用可能にします。MVR グループの最大数を 2000 に設定する場合は、モードを **dynamic**（ダイナミック）に設定する必要があります。 • **compatible**：Catalyst 3500 XL スイッチおよび Catalyst 2900 XL スイッチを使用できるようになり、送信元ポートでは IGMP ダイナミック Join が使用できなくなります。 デフォルトのモードは **compatible**（互換）です。
ステップ 7	**mvr ringmode flood**	（任意）アクセス リングに対する MVR リングモード フラッディングをイネーブルにします。このコマンドを入力すると、ユニキャスト トラフィックが廃棄されないよう、リング環境内の出力ポートでトラフィック フローを制御できます。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mvr** or **show mvr members**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻す場合は、**no mvr** [**mode** | **group** *ip-address* | **querytime** | **vlan**] グローバル コンフィギュレーション コマンドを使用します。

次に示すのは、MVR をイネーブルにし MVR グループ アドレスを設定した上で、クエリー時間を 1 秒（10 × 1/10）に、MVR マルチキャスト VLAN を VLAN 22 に、MVR モードをダイナミックにそれぞれ設定した例です。

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(config)# end
```

show mvr members 特権 EXEC コマンドを使用すると、スイッチ上の MVR マルチキャスト グループ アドレスを確認できます。

アクセス ポート上での MVR の設定

（注）　アクセス ポートおよびトランク ポートの詳細については、第 10 章「インターフェイスの設定」を参照してください。

アクセス ポート上にレイヤ 2 MVR インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	**interface** *interface-id*	設定するレイヤ 2 ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5	**mvr type** {**source** | **receiver**}	MVR ポートを次のいずれかに設定します。 • **source**：マルチキャスト データを送受信するアップリンク ポートを送信元ポートとして設定します。参加者は、送信元ポートに直接接続できません。スイッチ上の送信元ポートはすべて 1 つのマルチキャスト VLAN に属します。 • **receiver**：ポートが参加者ポートで、マルチキャスト データの受信だけを行う場合には、そのポートをレシーバー ポートとして設定します。このポートでデータを受信するためには、スタティックな設定、または IGMP の Join メッセージおよび Leave メッセージによりこのポートがマルチキャスト グループのメンバーになる必要があります。レシーバー ポートはマルチキャスト VLAN に属することはできません。 デフォルト設定は非 MVR ポートです。非 MVR ポートに MVR 特性で設定しようとすると、操作は無効になります。

	コマンド	目的
ステップ 6	**mvr vlan** *vlan-id* **group** [*ip-address*]	（任意）マルチキャスト VLAN および IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するように、ポートをスタティックに設定します。グループのメンバーとしてスタティックに設定されたポートは、スタティックに削除されるまではグループ メンバーのままです。 **（注）** 互換モードでは、このコマンドはレシーバー ポートにだけ適用されます。ダイナミック モードでは、レシーバー ポートおよび送信元ポートに適用されます。 レシーバー ポートは、IGMP の Join メッセージおよび Leave メッセージによって、マルチキャスト グループにダイナミックに参加することもできます。
ステップ 7	**mvr immediate**	（任意）ポート上の MVR の即時脱退機能をイネーブルにします。 **（注）** このコマンドはレシーバー ポートにだけ適用されます。この機能は単一の受信デバイスが接続されているレシーバー ポート上に限りイネーブルにしてください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mvr** **show mvr interface** または **show mvr members**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻す場合は、**no mvr** [**type** | **immediate** | **vlan** *vlan-id* | **group**] インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをレシーバー ポートとして設定したうえで、マルチキャスト グループ アドレスに送信されたマルチキャスト トラフィックを受信するようにそのポートをスタティックに設定し、ポートに即時脱退機能を設定して、結果を確認する方法を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config)# end
Switch# show mvr interface
Port    Type            Mode            VLAN    Status          Immediate Leave
----    ----            ----            ----    -------         ---------------
Gia0/2  RECEIVER        Trunk           201     ACTIVE/DOWN     DISABLED
```

トランク ポート上での MVR の設定

トランク ポートを MVR レシーバー ポートとして設定するには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的
ステップ 3	**interface** *interface-id*	設定するレイヤ 2 ポートを入力し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk**	トランキング モードを無条件に TRUNK に設定します。 **（注）** トランク ポートを MVR レシーバー ポートとして設定する場合、送信元ポートは NNI として設定し、MVR トランク レシーバー ポートは UNI または ENI として設定することを推奨します。
ステップ 5	**mvr type receiver**	トランク ポートが MVR レシーバー ポートとして使用されるよう指定します。
ステップ 6	**mvr vlan** ***source****-vlan-id* **receiver vlan** *receiver-vlan-id*	MVR VLAN から受信した MVR トラフィックが、レシーバー VLAN により認識されたトランク上の VLAN に配信されるよう、このトランク ポートをイネーブルにします。
ステップ 7	**mvr vlan** *vlan-id* **group** *ip-address* **receiver** ***vlan****-id*	（任意）トランク ポートをレシーバー VLAN 上のグループのスタティック メンバーとして設定します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mvr** **show mvr interface** **show mvr members**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、ポートを MVR トランク レシーバー ポートとして設定し、それを VLAN に割り当てたあと、グループのスタティック メンバーとなるように設定して、その結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface fastethernet 0/10
Switch(config)# switchport mode trunk
Switch(config)# mvr type receiver
Switch(config)# mvr vlan 100 receiver vlan 201
Switch(config)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
Switch(config)# end
Switch# show mvr interface

To return the interface to its default settings, use the no mvr [type | immediate | vlan
vlan-id | group] interface configuration command.
```

MVR 情報の表示

スイッチまたは指定されたインターフェイスの MVR 情報を表示できます。MVR 設定を表示するには、特権 EXEC モードで表 22-6 のコマンドを実行します。

表 22-6　MVR 情報を表示するためのコマンド

コマンド	目的
show mvr	スイッチの MVR ステータスと MVR 値を表示します。具体的には、MVR がイネーブルであるかディセーブルであるか、マルチキャスト VLAN、マルチキャスト グループの最大数（512）および現在の数（0 ～ 512）、クエリー応答時間、および MVR モードが表示されます。
show mvr interface [*interface-id*] [**members** [**vlan** *vlan*-**id**]]	すべての MVR インターフェイスおよびそれぞれの MVR 設定を表示します。 特定のインターフェイスを入力すると、次の情報が表示されます。 • Type：RECEIVER（レシーバー）または SOURCE（送信元） • Mode：アクセスまたはトランク • VLAN：送信元ポートの MVR VLAN およびレシーバー ポートのレシーバー VLAN • Status：次のいずれかになります。 – ACTIVE は、ポートが VLAN に含まれていることを意味します。 – UP/DOWN はポートが転送中か非転送中のどちらかであることを意味します。 – INACTIVE はポートがどの VLAN にも属していないことを意味します。 • Immediate Leave：イネーブルまたはディセーブル キーワード **members** を指定すると、このポートのすべてのマルチキャスト グループ メンバーが表示されます。また、VLAN 識別子を指定すると、VLAN のすべてのマルチキャスト グループ メンバーが表示されます。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show mvr members [*ip-address*]	任意の IP マルチキャスト グループまたは指定された IP マルチキャスト グループ IP アドレスのメンバーであるすべてのレシーバー ポートおよび送信元ポートを表示します。

IGMP フィルタリングおよび IGMP スロットリングの設定

一部の環境（たとえば、メトロポリタンまたは Multiple-Dwelling Unit [MDU; 集合住宅] インストレーション）では、スイッチ ポート上のユーザが所属可能な複数のマルチキャスト グループを管理する必要があります。この機能により、契約やサービス計画のタイプに基づいて IP/TV などのマルチキャスト サービスの配信を制御できます。また、スイッチ ポート上のユーザが所属できるマルチキャスト グループの数を制限することもできます。

IGMP フィルタリング機能を使用すると、IP マルチキャスト プロファイルを設定しそれを個々のスイッチ ポートに対応付けることにより、ポート単位でマルチキャスト参加をフィルタリングできます。IGMP プロファイルには 1 つまたは複数のマルチキャスト グループを格納できます。また、IGMP プロファイルによって、このグループへのアクセスを許可するか拒否するかを指定できます。マルチキャスト グループへのアクセスを拒否する IGMP プロファイルがスイッチ ポートに適用された場合、IP マルチキャスト トラフィックのストリームを要求する IGMP 参加レポートは廃棄され、そのポートでは該当グループからの IP マルチキャスト トラフィックを受信できません。フィルタリング アクションに

よってマルチキャスト グループへのアクセスが許可された場合、ポートからの IGMP レポートが転送され、通常の処理が行われます。レイヤ 2 インターフェイスが参加できる IGMP グループの最大数を設定することもできます。

IGMP フィルタリングが制御するのは、Join レポートや Leave レポートなど、グループ固有のクエリー リポートやメンバシップ レポートだけです。一般的な IGMP クエリーは制御しません。IGMP フィルタリングは、IP マルチキャスト トラフィックの転送指示機能には関係しません。フィルタリング機能によって行われる処理は、マルチキャスト トラフィックの転送に IGMP を使用した場合でも MVR を使用した場合でも同じです。

IGMP フィルタリングは、IP マルチキャスト グループ アドレスをダイナミックに学習する場合にだけ適用されます。IP マルチキャスト グループ アドレスをスタティックに設定する場合には適用されません。

IGMP スロットリング機能により、レイヤ 2 インターフェイスが参加できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定されており、かつ IGMP スヌーピング転送テーブルに最大数のエントリが含まれ、さらにインターフェイスが IGMP Join レポートを受信する場合は、IGMP レポートを廃棄するか、またはランダムに選択されたマルチキャスト エントリを受信 IGMP レポートに置き換えるようインターフェイスを設定できます。

（注）　IGMP フィルタリングを実行しているスイッチでは、IGMPv3 の Join メッセージおよび Leave メッセージはサポートされません。

ここでは、次の設定情報について説明します。

- 「IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定」（P.22-26）
- 「IGMP プロファイルの設定」（P.22-27）（任意）
- 「IGMP プロファイルの適用」（P.22-28）（任意）
- 「IGMP グループの最大数の設定」（P.22-28）（任意）
- 「IGMP スロットリング アクションの設定」（P.22-29）（任意）

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

表 22-7 は、IGMP フィルタリングのデフォルト設定をまとめたものです。

表 22-7　IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタリング	適用なし
IGMP グループの IGMP 最大数	最大値は設定なし
IGMP プロファイル	定義なし
IGMP プロファイル アクション	範囲アドレスを拒否

転送テーブルにグループの最大数のエントリがある場合、デフォルトの IGMP スロットリング アクションとして IGMP レポートは拒否されます。設定時の注意事項については、「IGMP スロットリング アクションの設定」（P.22-29）を参照してください。

IGMP プロファイルの設定

IGMP プロファイルを設定するには、プロファイル番号を指定した **ip igmp profile** グローバル コンフィギュレーション コマンドを使用して、IGMP プロファイル コンフィギュレーション モードを開始し、IGMP プロファイルを作成します。このモードでは、ポートからの IGMP Join 要求をフィルタリングするために使用する IGMP プロファイルのパラメータを指定できます。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- **deny**：一致するアドレスを拒否します（デフォルト設定）。
- **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、デフォルト設定に戻します。
- **permit**：一致するアドレスを許可します。
- **range**：プロファイルに対する IP アドレスの範囲を指定します。単独の IP アドレスを指定できるほか、開始アドレスおよび終了アドレスによりアドレスの範囲を指定することもできます。

デフォルトでは、スイッチには IGMP プロファイルは設定されていません。プロファイルの設定時に、**permit** と **deny** のどちらのキーワードも指定されていない場合は、デフォルトで IP アドレスの範囲へのアクセスが拒否されます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp profile** *profile number*	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。プロファイル番号の範囲は 1 ～ 4,294,967,295 です。
ステップ 3	**permit** | **deny**	（任意）IP マルチキャスト アドレスへのアクセスに対するアクションとして許可または拒否を設定します。アクションが設定されていない場合は、プロファイルのデフォルト設定によりアクセスは拒否されます。
ステップ 4	**range** *ip multicast address*	アクセスが制御される IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力する場合は、最小値の IP マルチキャスト アドレス、スペース、最大値の IP マルチキャスト アドレスの順で入力します。 **range** コマンドを繰り返し使用することで、複数のアドレスまたはアドレス範囲を入力できます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp profile** *profile number*	プロファイル設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、**no range** *ip multicast address* IGMP プロファイル コンフィギュレーション コマンドを使用します。

次に、単独の IP マルチキャスト アドレスに対するアクセスを許可する IGMP プロファイル 4 を作成し、その設定を確認する例を示します。アクションが拒否（デフォルト）である場合、**show ip igmp profile** の出力にはそのアクションは表示されません。

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
```

```
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

IGMP プロファイルの適用

IGMP プロファイルの定義に従ってアクセスを制御するには、**ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用して該当するインターフェイスにプロファイルを適用します。IGMP プロファイルを適用できるのは、レイヤ 2 アクセス ポートだけです。IGMP プロファイルはルーテッド ポートや SVI には適用できません。また、EtherChannel ポート グループに属するポートにも適用できません。1 つのプロファイルを複数のインターフェイスに適用することもできますが、各インターフェイスに適用できるプロファイルは 1 つだけです。

スイッチ ポートに IGMP プロファイルを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。このインターフェイスには、EtherChannel ポート グループに属していないレイヤ 2 ポートを指定する必要があります。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp filter** *profile number*	指定した IGMP プロファイルをこのインターフェイスに適用します。指定できる範囲は 1 ～ 4294967295 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスからプロファイルを削除するには、**no ip igmp filter** *profile number* インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

IGMP グループの最大数の設定

ip igmp max-groups インターフェイス コンフィギュレーション コマンドを使用すると、レイヤ 2 インターフェイスが参加できる IGMP グループの最大数を設定できます。最大数をデフォルト（制限なし）に戻すには、このコマンドの **no** 形式を使用します。

この制限が適用されるのはレイヤ 2 ポートだけです。ルーテッド ポートや SVI には IGMP グループの最大数は設定できません。また、このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポート グループに属するポート上では使用できません。

転送テーブルの IGMP グループの最大数を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。このインターフェイスには、EtherChannel グループまたは EtherChannel インターフェイスに属していないレイヤ 2 ポートを指定できます。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp max-groups** *number*	インターフェイスが参加できる IGMP グループの最大数を設定します。指定できる範囲は 0 ～ 4294967294 です。デフォルトでは、最大値は設定されません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

最大グループ数の制限を削除し、デフォルト設定（最大値なし）に戻すには、**no ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが参加できる IGMP グループ数を 25 に制限する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

IGMP スロットリング アクションの設定

レイヤ 2 インターフェイスが参加可能な IGMP グループの最大数を設定したら、**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドを使用して、既存のグループを IGMP レポートが受信された新しいグループに置き換えるようにインターフェイスを設定できます。デフォルト設定（IGMP Join レポートを廃棄）に戻すには、このコマンドの **no** 形式を使用します。

IGMP スロットリング アクションを設定する場合には、次の注意事項に従ってください。

- この制限事項は、レイヤ 2 ポートに対してだけ適用されます。また、このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポート グループに属するポート上では使用できません。
- グループ数の上限設定がデフォルト（最大値なし）に設定されている場合は、**ip igmp max-groups action** {**deny** | **replace**} コマンドを入力しても処理は行われません。
- インターフェイスが転送テーブルにマルチキャスト エントリを追加したあとで、スロットリング アクションおよび最大グループ制限を設定すると、スロットリング アクションに応じて、転送テーブルのエントリは無効になるかまたは削除されます。
  - スロットリング アクションを **deny** に設定すると、すでに転送テーブルにあったエントリは削除されず無効になります。これらのエントリが無効になり、エントリの最大数が転送テーブルにある場合、スイッチはインターフェイスで次に受信した IGMP レポートを廃棄します。
  - スロットリング アクションを **replace** に設定した場合は、すでに転送テーブルにあったエントリは削除されます。エントリの最大数が転送テーブルにある場合、スイッチはランダムに選択されたエントリを受信された IGMP レポートに置き換えます。

スイッチが転送テーブルのエントリを削除しないようにするには、インターフェイスがエントリを転送テーブルに追加する前に、IGMP スロットリング アクションを設定します。

転送テーブルにエントリの最大数があるときに、スロットリング アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。このインターフェイスには、EtherChannel グループまたは EtherChannel インターフェイスに属していないレイヤ 2 ポートを指定できます。このインターフェイスには、トランク ポートを指定できません。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp max-groups action** {**deny** | **replace**}	インターフェイスが IGMP レポートを受信し、かつ最大数のエントリが転送テーブルにある場合に、インターフェイスが実行するアクションを指定します。 • **deny**：レポートを廃棄します。 • **replace**：既存のグループを IGMP レポートが受信された新しいグループに置き換えます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのアクション（レポートを廃棄）に戻す場合は、**no ip igmp max-groups action** インターフェイス コンフィギュレーション コマンドを使用します。

次に、転送テーブル内に最大数のエントリが存在する場合に、テーブルでランダムに選択されたマルチキャスト エントリを削除し、転送テーブルに IGMP グループを追加するようにポートを設定する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp max-groups action replace
Switch(config-if)# end
```

IGMP フィルタリングおよび IGMP スロットリングの設定の表示

IGMP プロファイルの特性を表示できます。また、スイッチのすべてのインターフェイスまたは指定したインターフェイスの IGMP プロファイルおよび最大グループ数設定を表示できます。さらには、スイッチ上のすべてのインターフェイスおよび特定のインターフェイスの IGMP スロットリング設定を表示することもできます。

IGMP フィルタリングおよび IGMP スロットリングの設定を表示するには、表 22-8 に記載された特権 EXEC コマンドを使用します。

表 22-8　IGMP フィルタリングおよび IGMP スロットリングの設定を表示するためのコマンド

コマンド	目的
show ip igmp profile [*profile number*]	指定されている IGMP プロファイル、またはスイッチ上で定義されているすべての IGMP プロファイルを表示します。
show running-config [**interface** *interface-id*]	指定されたインターフェイスまたはスイッチ上のすべてのインターフェイスの設定を表示します。インターフェイスが参加できる IGMP グループの最大数（設定されている場合）やインターフェイスに適用されている IGMP プロファイルなどがこれに含まれます。

CHAPTER 23

ポートベースのトラフィック制御の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにポートベースのトラフィック制御機能を設定する方法について説明します。

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

- 「ストーム制御の設定」（P.23-1）
- 「保護ポートの設定」（P.23-5）
- 「ポート ブロッキングの設定」（P.23-7）
- 「ポート セキュリティの設定」（P.23-8）
- 「ポートベースのトラフィック制御設定の表示」（P.23-18）

ストーム制御の設定

- 「ストーム制御の概要」（P.23-1）
- 「ストーム制御のデフォルト設定」（P.23-3）
- 「ストーム制御およびしきい値レベルの設定」（P.23-3）

ストーム制御の概要

ストーム制御は、LAN 上のトラフィックが、いずれかの物理インターフェイスのブロードキャスト、マルチキャスト、またはユニキャストのストームによって混乱しないようにします。LAN ストームは、パケットが LAN にフラッディングした場合に発生するもので、過剰なトラフィックが生み出され、ネットワーク パフォーマンスが低下します。プロトコルスタック実装内またはネットワーク設定内のエラーは、ストームの原因となる場合があります。

ストーム制御（トラフィック抑制）は、インターフェイスからスイッチング バスへ流れるパケットをモニタし、そのパケットがユニキャスト、マルチキャスト、ブロードキャストのいずれであるかを判別します。スイッチは、1 秒のタイム インターバル内で受信した指定されたタイプのパケットの数をカウントして、事前定義されている抑制レベルのしきい値とその測定値を比較します。

ストーム制御では、次のうちいずれかの手法を使用してトラフィック アクティビティを測定します。

- ブロードキャスト、マルチキャスト、ユニキャストのいずれかのトラフィックで使用できる帯域幅で、ポートで利用可能な総帯域幅に対するパーセンテージ

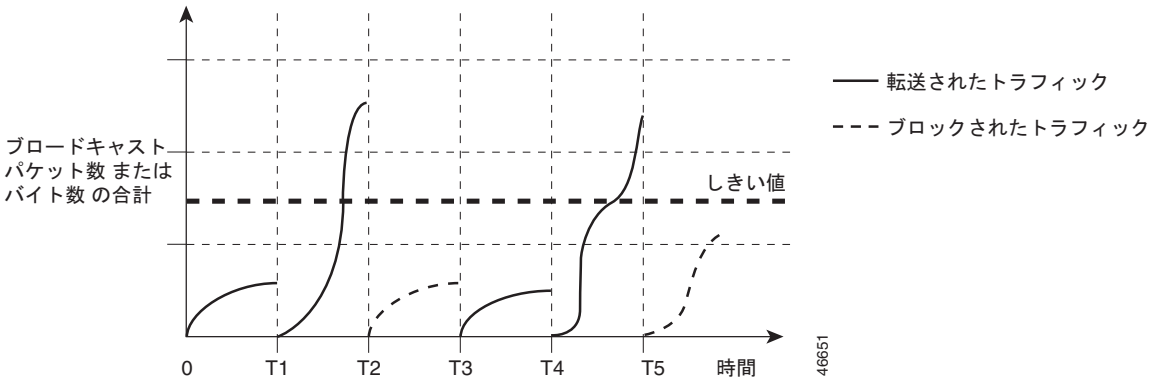
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レート（pps）
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レート（bps）

それぞれの手法では、上限しきい値に達すると、トラフィックがポートでブロックされます。トラフィック レートが下限しきい値（指定されている場合）未満に下がるまでポートはブロック状態のままとなり、下限しきい値未満に下がると、通常転送が再開されます。下限抑制レベルを指定していない場合、トラフィック レートが上限抑制レベル未満に下がるまで、スイッチではすべてのトラフィックがブロックされます。一般的には、レベルを上げると、ブロードキャスト ストームに対する保護の効果が小さくなります。

（注）　マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどのコントロール トラフィック以外のマルチキャスト トラフィックすべてがブロックされます。ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

図 23-1 のグラフは、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。この例は、マルチキャストおよびユニキャスト トラフィックにも適用できます。この例では、転送されているブロードキャスト トラフィックが、タイム インターバル T1 ～ T2 間および T4 ～ T5 間で設定されたしきい値を上回っています。特定のトラフィックの量がしきい値を上回ると、そのタイプのすべてのトラフィックは次の一定時間にわたり、廃棄されます。したがって、ブロードキャスト トラフィックは T2 および T5 のあとのインターバルではブロックされています。次のタイム インターバル（たとえば T3）では、ブロードキャスト トラフィックがしきい値を上回らなければ、再度転送されます。

図 23-1　　ブロードキャスト ストーム制御の例



ストーム制御の抑制レベルと 1 秒のタイム インターバルの組み合せにより、ストーム制御アルゴリズムの動作が制御されます。しきい値が高いほど、通過できるパケットが多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値が 0.0 であれば、ポートのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがすべてブロックされます。

（注）　パケットは均一の間隔で着信するわけではないため、トラフィック アクティビティを測定する 1 秒のタイム インターバルを設けることによって、ストーム制御の動作に影響を与える可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御のデフォルト設定

デフォルトでは、スイッチ インターフェイスでユニキャスト、ブロードキャスト、およびマルチキャスト ストーム制御はディセーブルです（抑制レベルは 100% です）。

ストーム制御およびしきい値レベルの設定

ポートでストーム制御を設定し、特定タイプのトラフィックで使用するしきい値レベルを入力します。

（注） ME 3400E スイッチでは、ストーム制御機能が小さなフレームを適切に処理できるようにするため、スイッチのストーム制御カウンタが小さいフレームで増加するように追加の設定を行う必要はありません。

ただし、ハードウェアの制約や、さまざまなサイズのパケットがカウントされる動作のため、しきい値の割合には誤差が生じます。着信トラフィックを構成するパケットのサイズによっては、実際のしきい値は、数 % 程度、設定されたレベルと異なる場合があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御およびしきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}	ブロードキャスト、マルチキャスト、ユニキャストのいずれかのストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルです。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、ユニキャストのいずれかのトラフィックの上限しきい値レベルを帯域幅のパーセンテージ（小数点以下第 2 位まで）で指定します。上限しきい値に達すると、ポートではトラフィックがブロックされます。指定できる範囲は **0.00 ～ 100.00** です。 • （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージ（小数点以下第 2 位まで）で指定します。この値は、上限抑制値より小さいまたは等しい必要があります。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は **0.00 ～ 100.00** です。 しきい値を最大値（100%）に設定すると、トラフィックは制限されません。しきい値を 0.0 に設定すると、ブロードキャスト、マルチキャスト、ユニキャストのすべてのトラフィックがそのポートでブロックされます。 • **bps** *bps* には、ブロードキャスト、マルチキャスト、ユニキャストのいずれかのトラフィック用に上限しきい値レベルを 1 秒あたりのビット数単位（小数点以下第 1 位まで）で指定します。上限しきい値に達すると、ポートではトラフィックがブロックされます。指定できる範囲は **0.0** ～ 10000000000.0 です。 • （任意）*bps-low* には、下限しきい値レベルを 1 秒あたりのビット数単位（小数点以下第 1 位まで）で指定します。上限しきい値レベル以下にしてください。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。指定できる範囲は **0.0** ～ 10000000000.0 です。 • **pps** *pps* には、ブロードキャスト、マルチキャスト、ユニキャストのいずれかのトラフィック用に上限しきい値レベルを 1 秒あたりのパケット数単位（小数点以下第 1 位まで）で指定します。上限しきい値に達すると、ポートではトラフィックがブロックされます。指定できる範囲は **0.0** ～ 10000000000.0 です。 • （任意）*pps-low* には、下限しきい値レベルを 1 秒あたりのパケット数単位（小数点以下第 1 位まで）で指定します。上限しきい値レベル以下にしてください。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。指定できる範囲は **0.0** ～ 10000000000.0 です。 BPS 設定および PPS 設定には、しきい値が大きくなる場合、k、m、g などのメートル法の単位を使用できます。

	コマンド	目的
ステップ 5	**storm-control action** {**shutdown** | **trap**}	ストームが検出されたときに実行する処理を指定します。デフォルトでは、トラフィックがフィルタリングされてトラップが送信されません。 • ストーム中にポートを errdisable にするには、キーワード **shutdown** を選択します。 • ストームが検出されたときに SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、キーワード **trap** を選択します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]	指定したトラフィック タイプについてインターフェイスに設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御設定が表示されます。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ストーム制御をディセーブルにするには、**no storm-control** {**broadcast** | **multicast** | **unicast**} **level** インターフェイス コンフィギュレーション コマンドを使用します。

以下は、上限抑制レベルを 87 %、下限抑制レベルを 65 % にしてポートでユニキャスト ストーム制御をイネーブルにする方法の例です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control unicast level 87 65
```

次の例は、ポートのブロードキャスト アドレス ストーム制御を 20 % のレベルでイネーブルにする方法を示します。ブロードキャスト トラフィックが、トラフィック ストーム制御インターバルでポートの使用可能帯域幅全体の 20 % という設定レベルを超えると、トラフィック ストーム制御インターバルが終了するまでスイッチはすべてのブロードキャスト トラフィックを廃棄します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

保護ポートの設定

一部のアプリケーションでは、同一スイッチ上のポート間でトラフィックがレイヤ 2 で転送されないようにすることにより、あるネイバによって生成されたトラフィックを別のネイバが認識しないようにする必要があります。このような環境では、保護ポートを使用すれば、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換は行われません。

（注）　NNI のデフォルトは非保護ポートです。UNI および ENI はポート独立を行うため、UNI および ENI ポート上では、保護ポートを使用できません。ポート タイプの詳細については、「UNI、NNI、および ENI の各ポート タイプ」（P.10-2）を参照してください。

保護ポートには次のような機能があります。

- 保護ポートは、他の保護ポートにユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、PIM パケットなどの制御トラフィックのみが転送されます。保護ポート間を通過するすべてのデータ トラフィックはレイヤ 3 装置を介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおり行われます。

ここでは、次の設定情報について説明します。

- 「保護ポートのデフォルト設定」（P.23-6）
- 「保護ポートの設定時の注意事項」（P.23-6）
- 「保護ポートの設定」（P.23-6）

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されていません。

保護ポートの設定時の注意事項

保護ポートは、NNI として設定される物理インターフェイス（ギガビット イーサネット ポート 1 など）または EtherChannel グループ（port-channel 5 など）のいずれにも設定できます。特定のポート チャネルについて保護ポートをイネーブルにすると、ポート チャネル グループ内の全ポートで保護ポートがイネーブルになります。

プライベート VLAN（仮想 LAN）ポートを保護ポートとして設定しないでください。保護ポートをプライベート VLAN ポートとして設定しないでください。プライベート VLAN の独立ポートは、他の独立ポートやコミュニティ ポートにトラフィックを転送しません。プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。

保護ポートの設定

ポートを保護ポートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、NNI である必要があります。 **（注）**　デフォルトでは、UNI および ENI は保護ポートです。
ステップ 3	**switchport protected**	インターフェイスを保護ポートとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートをディセーブルにするには、**no switchport protected** インターフェイス コンフィギュレーション コマンドを使用します。

次に、保護ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

次に、保護ポートとして FastEthernet ポートを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# port-type NNI
Switch(config-if)# no shutdown
Switch(config-if)# switchport protected
Switch(config-if)# end
```

ポート ブロッキングの設定

デフォルトでは、宛先 MAC（メディア アクセス制御）アドレスが不明のパケットは、すべてのポートからフラッディングされます。不明のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上の問題が発生することがあります。不明のユニキャストまたはマルチキャスト トラフィックがポート間で転送されないようにするため、不明のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにポート（保護ポートまたは非保護ポート）をブロックできます。

（注）　マルチキャスト トラフィックでは、ポート ブロッキング機能は、純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 情報を含むマルチキャスト パケットはブロックされません。

ここでは、次の設定情報について説明します。

- 「ポート ブロッキングのデフォルト設定」（P.23-7）
- 「インターフェイスでのフラッディング トラフィックのブロック」（P.23-7）

ポート ブロッキングのデフォルト設定

デフォルトでは、ポートから送信される不明のマルチキャストおよびユニキャスト トラフィックのフラッディングはブロックされません。これらのトラフィックは、すべてのポートにフラッディングされます。

インターフェイスでのフラッディング トラフィックのブロック

（注）　インターフェイスは物理インターフェイスまたは EtherChannel グループに設定できます。特定のポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

インターフェイスから送信されるユニキャストおよびレイヤ 2 マルチキャスト パケットのフラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport block multicast**	ポートからの不明マルチキャストの転送をブロックします。 （注）　純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 情報を含むマルチキャスト パケットはブロックされません。
ステップ 5	**switchport block unicast**	ポートからの不明ユニキャストの転送をブロックします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id* **switchport**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

トラフィックがブロックされず、ポート上で標準転送が行われるデフォルト状態にインターフェイスを戻すには、**no switchport block** {**multicast** | **unicast**} インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上でユニキャストおよびレイヤ 2 マルチキャスト フラッディングをブロックする例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

ポート セキュリティの設定

ポート セキュリティ機能を使用すると、ポートへのアクセスが許可されたステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは、定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレスを 1 つに制限し、1 つだけ割り当てると、そのポートに接続されたワークステーションでは、ポートの全帯域幅が保証されます。

セキュア ポートとして設定されたポートのセキュア MAC アドレスが最大数に達した場合に、ポートにアクセスしようとするステーションの MAC アドレスが、識別されたどのセキュア MAC アドレスとも異なるときは、セキュリティ違反が発生します。また、あるセキュア ポートで設定または学習されたセキュア MAC アドレスを持つステーションが別のセキュア ポートにアクセスしようとすると、違反のフラグが立てられます。

ここでは、次の概要および設定情報について説明します。

- 「ポート セキュリティの概要」（P.23-9）
- 「ポート セキュリティのデフォルト設定」（P.23-10）
- 「ポート セキュリティ設定時の注意事項」（P.23-11）
- 「ポート セキュリティのイネーブル化と設定」（P.23-12）
- 「ポート セキュリティ エージングのイネーブル化と設定」（P.23-15）
- 「ポート セキュリティおよびプライベート VLAN」（P.23-17）

ポート セキュリティの概要

- 「セキュア MAC アドレス」（P.23-9）
- 「セキュリティ違反」（P.23-10）

セキュア MAC アドレス

1 つのポートで許可されるセキュア アドレスの最大数を設定するには、**switchport port-security maximum** *value* インターフェイス コンフィギュレーション コマンドを使用します。

（注）　インターフェイスにすでに設定されているセキュア アドレス数よりも小さい値を最大値に設定しようとすると、コマンドは拒否されます。

スイッチは、次のタイプのセキュア MAC アドレスをサポートします。

- スタティック セキュア MAC アドレス：**switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーションを使用して手動で設定します。これらはアドレス テーブルに格納され、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス：動的に設定されます。これらはアドレス テーブルにだけ格納され、スイッチが再起動するときに削除されます。
- *固定*セキュア MAC アドレス：動的に学習されるか、または手動で設定します。これらはアドレス テーブルに格納され、実行コンフィギュレーションに追加されます。これらのアドレスがコンフィギュレーション ファイルに保存されている場合は、スイッチを再起動するときに、インターフェイスがアドレスを動的に再設定する必要はありません。

*固定学習*をイネーブルにすると、ダイナミック MAC アドレスを固定セキュア MAC アドレスに変換し、それらを実行コンフィギュレーションに追加するように、インターフェイスを設定できます。固定学習をイネーブルにするには、**switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、インターフェイスはすべてのダイナミック セキュア MAC アドレス（固定学習がイネーブルになる前に動的に学習されたアドレスを含む）を、固定セキュア MAC アドレスに変換します。すべての固定セキュア MAC アドレスが、実行コンフィギュレーションに追加されます。

固定セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチの再起動時に使用されるスタートアップ コンフィギュレーション）に、自動的には格納されません。コンフィギュレーション ファイルに固定セキュア MAC アドレスが保存されている場合は、スイッチを再起動するときに、インターフェイスはこれらのアドレスを再学習する必要がありません。スティッキ セキュア アドレスが保存されていない場合は、アドレスは失われます。

スティッキ ラーニングをディセーブルにした場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって設定されます。この数字はアクティブな SDM テンプレートによって決められます。第 7 章「SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。

セキュリティ違反

セキュリティ違反とは、次のいずれかの状況が発生したときです。

- セキュア MAC アドレスが最大数までアドレス テーブルに追加され、アドレス テーブルにない MAC アドレスを持つステーションが、インターフェイスにアクセスしようとした場合
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで認識された場合

違反発生時の対処方法に関して、次の 3 つの違反モードのいずれかにインターフェイスを設定できます。

- protect：セキュア MAC アドレスの数がポートに許容された最大限度に達した場合、十分な数のセキュア MAC アドレスを削除して最大限度以下にするか、またはアドレスの最大許容数を増やすまで、不明の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反が起こっても、ユーザには通知されません。

（注）　トランク ポートには protect 違反モードを設定しないでください。保護モードでは、ポートが最大制限に達していなくても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。

- protect：セキュア MAC アドレスの数がポートに許容された最大限度に達した場合、十分な数のセキュア MAC アドレスを削除して最大限度以下にするか、またはアドレスの最大許容数を増やすまで、不明の送信元アドレスを持つパケットは廃棄されます。このモードでは、セキュリティ違反が起こった場合、ユーザに通知されます。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。
- shutdown：ポート セキュリティ違反が発生すると、インターフェイスは errdisable ステートになって、ただちにシャットダウンし、ポート LED が消灯します。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが errdisable ステートになった場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを変更できます。また、**shutdown** および **no shut down** の各インターフェイス コンフィギュレーション コマンドを入力することにより、ポートを手動でイネーブルに戻すこともできます。これがデフォルトのモードです。

表 23-1 に、違反モード、およびポート セキュリティのインターフェイスを設定した場合の動作を示します。

表 23-1　セキュリティ違反モードの動作

違反モード	トラフィックの転送[1]	SNMP トラップの送信	Syslog メッセージの送信	エラー メッセージの表示[2]	違反カウンタの増加	ポートのシャットダウン
protect	不可	不可	不可	不可	不可	不可
restrict	不可	あり	あり	不可	あり	不可
shutdown	不可	あり	あり	不可	あり	あり

1. 送信元アドレスが不明なパケットは、十分な数のセキュア MAC アドレスが削除されるまで、廃棄されます。
2. 手動で設定したアドレスがセキュリティ違反の原因となる場合には、エラー メッセージが表示されます。

ポート セキュリティのデフォルト設定

表 23-2 に、インターフェイスに対するポート セキュリティのデフォルト設定を示します。

表 23-2　ポート セキュリティのデフォルト設定

機能	デフォルト設定
ポート セキュリティ	ポートでディセーブル
固定アドレス学習	ディセーブル。
ポート単位のセキュア MAC アドレスの最大数	1.
違反モード	shutdown です。セキュア MAC アドレスの最大数を超過すると、ポートはシャットダウンします。
ポート セキュリティのエージング	ディセーブル。エージング タイムは 0 です。 スタティック エージングはディセーブルです。 タイプは absolute です。

ポート セキュリティ設定時の注意事項

- ポート セキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートはダイナミック アクセス ポートにできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートは、Fast EtherChannel やギガビット EtherChannel ポート グループに属することができません。
- セキュア ポートは、プライベート VLAN ポートにできません。
- トランク ポートにポート セキュリティが設定され、データ トラフィックのアクセス VLAN および音声トラフィックの音声 VLAN に割り当てられている場合、**switchport voice** および **switchport priority extend** の各インターフェイス コンフィギュレーション コマンドは無効です。

  接続されたデバイスで同じ MAC アドレスを使用し、アクセス VLAN の IP および音声 VLAN の IP を要求した場合、アクセス VLAN だけに IP アドレスが割り当てられます。
- インターフェイスのセキュア アドレスの最大値として入力した値が古い値よりも大きい場合は、新しい値が古い設定値よりも優先します。新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングはサポートしていません。

表 23-3 は、ポート セキュリティとその他のポートベース機能の互換性をまとめたものです。

表 23-3　ポート セキュリティとその他のスイッチ機能の互換性

ポートのタイプまたはポート上の機能	ポート セキュリティとの互換性
トランク ポート	あり
ダイナミックアクセス ポート（switchport access vlan-dynamic interface conifiguration コマンドで設定される Vlan Query Protocol [VQP]）	不可
ルーテッド ポート	不可
SPAN 送信元ポート	あり
SPAN 宛先ポート	不可
EtherChannel	不可

表 23-3　ポート セキュリティとその他のスイッチ機能の互換性 （続き）

ポートのタイプまたはポート上の機能	ポート セキュリティとの互換性
トンネリング ポート	あり
保護ポート	あり
802.1X ポート	あり
プライベート VLAN ポート	不可
IP ソース ガード	あり
ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査	あり
Flex Link	あり

ポート セキュリティのイネーブル化と設定

ポートへのアクセスが許可されたステーションの MAC アドレスを制限および識別する方法でインターフェイスへの入力を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport mode** {**access** | **trunk**}	インターフェイス スイッチポート モードを access または trunk に設定します。デフォルト モード（dynamic auto）のインターフェイスは、セキュア ポートとしては設定できません。
ステップ 5	**switchport port-security**	インターフェイスでポート セキュリティをイネーブルにします。
ステップ 6	**switchport port-security** [**maximum** *value* [**vlan** *vlan-list* | **access**]	（任意）インターフェイスについてセキュア MAC アドレスの最大数を設定します。スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって設定されます。この値は、アクティブな SDM テンプレートによって決まります。第 7 章「SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-list*：トランク ポートで、VLAN 範囲（ハイフンで区切る）または一連の VLAN（カンマで区切る）に関する VLAN 単位の最大値を設定できます。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 • **access**：アクセス ポートで、アクセス VLAN として VLAN を指定します。

	コマンド	目的
ステップ 7	**switchport port-security violation** {**protect** | **restrict** | **shutdown**}	（任意）違反モード（セキュリティ違反検出時の対処方法）を次のいずれかで設定します。 • **protect**：セキュア MAC アドレスの数がポートの最大許容値に達した場合、十分な数のセキュア MAC アドレスを削除して最大限度以下にするか、または使用可能な最大アドレス数を増加させるまで、不明の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反が起こっても、ユーザには通知されません。 **（注）** トランク ポート上に保護モードを設定することは推奨されません。保護モードでは、ポートが最大制限に達していなくても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。 • **restrict**：セキュア MAC アドレスの数がポートの許容限度に達した場合、十分な数のセキュア MAC アドレスを削除するか、またはアドレスの最大許容数を増加させるまで、不明の送信元アドレスを持つパケットは廃棄されます。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown**：セキュリティ違反が発生すると、インターフェイスが errdisable ステートになり、ポート LED が消灯します。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。 **（注）** セキュア ポートが errdisable ステートになった場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを使用することにより、ステートを変更できます。また、**shutdown** および **no shutdown** の各インターフェイス コンフィギュレーション コマンドを入力することにより、手動でポートをイネーブルに戻すこともできます。
ステップ 8	**switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access**}}]	（任意）インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用してセキュア MAC アドレスの最大数を入力できます。最大数より少ないセキュア MAC アドレス数を設定すると、残りの MAC アドレスは動的に学習されます。 **（注）** このコマンドを入力したあとに固定学習をイネーブルにすると、動的に学習されたセキュア アドレスが固定セキュア MAC アドレスに変換されて、実行コンフィギュレーションに追加されます。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポートでは、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しないと、ネイティブ VLAN が使用されます。 • **access**：アクセス ポートで、アクセス VLAN として VLAN を指定します。
ステップ 9	**switchport port-security mac-address sticky**	（任意）インターフェイスで固定学習をイネーブルにします。

	コマンド	目的
ステップ 10	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access**}]	（任意）固定セキュア MAC アドレスを入力します。必要に応じて、このコマンドを繰り返し入力します。設定したセキュア MAC アドレス数が最大値より小さい場合、残りの MAC アドレスは動的に学習され、固定セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。 **（注）** このコマンドを入力する前に固定学習をイネーブルにしておかないと、エラー メッセージが表示され、固定セキュア MAC アドレスを入力できません。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポートでは、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しないと、ネイティブ VLAN が使用されます。 • **access**：アクセス ポートで、アクセス VLAN として VLAN を指定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show port-security**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルトの非セキュア ポートに戻すには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。固定学習がイネーブルの場合にこのコマンドを入力すると、固定学習アドレスは実行コンフィギュレーション内に残りますが、アドレス テーブルからは削除されます。ここで、すべてのアドレスが動的に学習されます。

インターフェイスのセキュア MAC アドレス数をデフォルトに戻すには、**no switchport port-security maximum** *value* インターフェイス コンフィギュレーション コマンドを使用します。違反モードをデフォルトの shutdown モードに戻すには、**no switchport port-security violation** {**protocol** | **restrict**} インターフェイス コンフィギュレーション コマンドを使用します。

固定学習をディセーブルにするには、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを実行します。インターフェイスは固定セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。ただし、固定 MAC アドレスを含む設定がすでに保存されている場合は、**no switchport port-security mac-address sticky** コマンドを入力したあとに再び設定を保存する必要があります。保存しない場合スイッチを再起動すると固定アドレスが復元されます。

MAC アドレス テーブルからセキュアなアドレスをすべて削除したり、スイッチまたはインターフェイス上の特定のタイプ（設定済み、ダイナミック、または固定）のセキュア アドレスをすべて削除したりするには、**clear port-security** {**all** | **configured** | **dynamic** | **sticky**} 特権 EXEC コマンドを使用します。

アドレス テーブルから特定のセキュア MAC アドレスを削除するには、**no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用します。

アドレス テーブルから特定のインターフェイスに関するダイナミック セキュア アドレスをすべて削除するには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドのあとに、**switchport port-security** コマンドを入力して、インターフェイスのポート セキュリティをイネーブルに戻します。**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、固定セキュア MAC アドレスをダイナミック セキュア MAC アドレスに変換してから、**no switchport port-security** コマンドを入力すると、手動で設定されたセキュア アドレスを除き、インターフェイス上のすべてのセキュア アドレスが削除されます。

no switchport port-security mac-address *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、アドレス テーブルから設定済みのセキュア MAC アドレスを削除する必要があります。

次の例では、ポートでポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する方法を示します。デフォルトは違反モードで、スタティック セキュア MAC アドレスは設定されていません。また、固定学習がイネーブルに設定されています。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 にスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、ポート上で固定ポート セキュリティをイネーブルにして、データ VLAN に MAC アドレスを手動で設定し、セキュア アドレスの最大合計数を 10 に設定する例を示します。

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security maximum 10 vlan access
```

ポート セキュリティ エージングのイネーブル化と設定

ポート セキュリティ エージングを使用すると、ポート上の全セキュア アドレスにエージング タイムを設定できます。ポートごとに 2 種類のエージングがサポートされています。

- absolute：ポートのセキュア アドレスは、指定のエージング タイムの経過後、削除されます。
- inactivity：ポートのセキュア アドレスが削除されるのは、指定したエージング タイムの間、そのセキュア アドレスが非アクティブであった場合だけです。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュア ポートでデバイスの削除や追加を実行でき、しかもポートのセキュア アドレスの数を制限できます。また、セキュア アドレスのエージングをポート単位でイネーブルまたはディセーブルに設定できます。

ポート セキュリティ エージングを設定するには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}	セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにするか、またはエージング タイムやタイプを設定します。 **（注）** スイッチでは、固定セキュア アドレスのポート セキュリティ エージングをサポートしません。 このポートに、スタティックに設定されたセキュア アドレスのエージングをイネーブルにするには、**static** を入力します。 *time* には、このポートのエージング タイムを指定します。指定できる範囲は 0 ～ 1440 分です。 **type** には、次のキーワードのいずれかを 1 つ選択します。 • **absolute**：エージング タイプを absolute に設定します このポートのセキュア アドレスはすべて、指定した 時間（分単位）が経過すると期限切れになり、セキュア アドレス リストから削除されます。 • **inactivity**：エージングのタイプを inactivity に設定します。このポートのセキュア アドレスが期限切れになるのは、指定した時間中にセキュア送信元アドレスからのデータ トラフィックを受信しなかった場合だけです。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show port-security** [**interface** *interface-id*] [**address**]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポート上のすべてのセキュア アドレスに対してポート セキュリティ エージングをディセーブルにするには、**no switchport port-security aging time** インターフェイス コンフィギュレーション コマンドを使用します。スタティックに設定されたセキュア アドレスに対してだけエージングをディセーブルにするには、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートのセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

次に、このインターフェイスに設定されたセキュア アドレスのエージングをイネーブルにし、エージング タイプを inactivity に、エージング タイムを 2 分に設定する例を示します。

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

設定したコマンドを確認するには、**show port-security interface** *interface-id* 特権 EXEC コマンドを入力します。

ポート セキュリティおよびプライベート VLAN

ポート セキュリティでは、管理者がポートで学習された MAC アドレスの数を制限するか、またはポートで学習できる MAC アドレスを定義できます。

PVLAN ホストおよびプロミスキャス ポートにポート セキュリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport mode private-vlan {host | promiscuous}	インターフェイスでプライベート VLAN をイネーブルにします。
ステップ 4	**switchport port-security**	インターフェイスでポート セキュリティをイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show port-security** [**interface** *interface-id*] [**address**]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

```
Switch(config)# interface GigabitEthernet0/8
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```

（注） ポート セキュリティとプライベート VLAN の両方が設定されているポートは、セキュア PVLAN ポートと呼ぶ場合があります。セキュア PVLAN ポートでセキュアなアドレスが学習される場合、同じプライマリ VLAN に属しているほかのセキュア PVLAN ポートでは、同じセキュア アドレスを学習できません。ただし、アンセキュアな PVLAN ポートで学習されるアドレスは、同じプライマリ VLAN に属しているセキュア PVLAN ポートで学習できます。

ホスト ポートで学習されるセキュア アドレスは、対応付けられたプライマリ VLAN に自動的に複製されます。同様に、プロミスキャス ポートで学習されるセキュア アドレスは、対応付けられたすべてのセカンダリ VLAN に自動的に複製されます。スタティック アドレス（mac-address-table static コマンドを使用）は、セキュア ポートではユーザ設定できません。

ポートベースのトラフィック制御設定の表示

show interfaces *interface-id* **switchport** 特権 EXEC コマンドを使用すると、（各種の特性とともに）インターフェイスのトラフィック抑制および制御の設定が表示されます。**show storm-control** および **show port-security** 特権 EXEC コマンドを使用すると、それぞれストーム制御とポート セキュリティ設定が表示されます。

トラフィック制御情報を表示するには、表 23-4 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 23-4　トラフィック制御のステータスおよび設定を表示するためのコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定したポートについて、管理ステータスまたは動作ステータスを表示します（ポート ブロッキング、ポート保護設定など）。
show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**]	すべてのインターフェイスまたは指定したインターフェイスについて、指定したトラフィック タイプ（指定されていない場合はブロードキャスト トラフィック）のストーム制御抑制レベルを表示します。
show port-security [**interface** *interface-id*]	スイッチまたは指定したインターフェイスのポートのセキュリティ設定を表示します。各インターフェイスのセキュア MAC アドレスの最大数、インターフェイスのセキュア MAC アドレス数、発生したセキュリティ違反数、違反モードなどが含まれます。
show port-security [**interface** *interface-id*] **address**	すべてのスイッチ インターフェイスまたは指定したインターフェイスについて、設定されたすべてのセキュア MAC アドレスと、各アドレスのエージング情報を表示します。
show port-security interface *interface-id* **vlan**	指定したインターフェイスの VLAN ごとに設定されたセキュア MAC アドレス数を表示します。

CHAPTER 24

CDP の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに Cisco Discovery Protocol（CDP; シスコ検出プロトコル）を設定する方法について説明します。

（注） この章で使用されるコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンス、および『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* の「System Management Commands」を参照してください。

- 「CDP の概要」（P.24-1）
- 「CDP の設定」（P.24-2）
- 「CDP のモニタリングおよびメンテナンス」（P.24-5）

CDP の概要

CDP は、すべてのシスコ製デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データリンク層）上で動作するデバイス ディスカバリ プロトコルです。これにより、ネットワーク管理アプリケーションは、既知デバイスに近接しているシスコのデバイスを検出できます。ネットワーク管理アプリケーションは、CDP によって、下位レイヤのトランスペアレント プロトコルが稼動する近接デバイスのデバイス タイプおよび SNMP（簡易ネットワーク管理プロトコル）エージェント アドレスを学習できます。この機能によって、アプリケーションから近接デバイスに SNMP クエリーを送信できます。

CDP は、Subnetwork Access Protocol（SNAP）をサポートしているすべてのメディアで稼動します。CDP がデータリンク層でしか稼動しないため、異なるネットワーク レイヤ プロトコルをサポートする 2 つのシステムは、相互に学習できます。

（注） Cisco ME スイッチ上では、CDP が、Network Node Interface（NNI; ネットワーク ノード インターフェイス）上ではデフォルトでイネーブルになっており、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）上ではデフォルトでディセーブルになっています。User Network Interface（UNI; ユーザ ネットワーク インターフェイス）ではサポートされていません。

CDP を設定した各デバイスは、マルチキャスト アドレスに対して定期的にメッセージを送信し、SNMP メッセージを受信できるアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信デバイスで CDP 情報を廃棄せずに保持しておく時間を表す Time To Live（TTL）、つまりホールドタイム情報も含まれます。各デバイスは、他のデバイスから送信されたメッセージのリスニングも行って近接デバイスについて学習します。

スイッチは CDP バージョン 2 をサポートします。

CDP の設定

- 「CDP のデフォルト設定」（P.24-2）
- 「CDP 特性の設定」（P.24-2）
- 「CDP のディセーブル化およびイネーブル化」（P.24-3）
- 「インターフェイスでの CDP のディセーブル化およびイネーブル化」（P.24-4）

CDP のデフォルト設定

表 24-1 に、CDP のデフォルト設定を示します。

表 24-1　　CDP のデフォルト設定

機能	デフォルト設定
CDP グローバル ステート	イネーブル。
CDP インターフェイス ステート	NNI 上でだけイネーブルです。ENI 上ではディセーブルです。 **（注）**　UNI 上では CDP はサポートされていません。
CDP タイマー（パケット アップデート頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

CDP 特性の設定

CDP のアップデート頻度、廃棄するまでに情報を保持する時間、およびバージョン 2 アドバタイズ送信の有無を設定できます。

CDP タイマー、ホールドタイム、およびアドバタイズのタイプを設定するには、特権 EXEC モードで次の手順を実行します。

（注）　ステップ 2 ～ 4 はすべて任意なので、順序不同で実行できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp timer** *seconds*	（任意）CDP アップデートの伝送頻度を秒単位で設定します。 指定できる範囲は 5 ～ 254 秒で、デフォルトは 60 秒です。
ステップ 3	**cdp holdtime** *seconds*	（任意）このデバイスから送信された情報を受信デバイスが廃棄するまで保持する時間を指定します。 指定できる範囲は 10 ～ 255 秒で、デフォルトは 180 秒です。
ステップ 4	**cdp advertise-v2**	（任意）バージョン 2 アドバタイズを送信するように CDP を設定します。 これがデフォルトの状態になります。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show cdp**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻す場合は、CDP コマンドの **no** 形式を使用します。

次に、CDP 特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

CDP の **show** コマンドの詳細については、「CDP のモニタリングおよびメンテナンス」（P.24-5）を参照してください。

CDP のディセーブル化およびイネーブル化

デフォルトでは、CDP は NNI 上でイネーブルに設定されています。ENI 上ではデフォルトでディセーブルになっていますが、イネーブルにはできません。

（注）　シスコ製デバイス（Cisco IP Phone など）は定期的に、接続されたデバイスと CDP メッセージを交換します。CDP をディセーブルにすると、デバイスの接続が中断されます。

CDP デバイス ディスカバリ機能をグローバルにディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no cdp run**	CDP をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

ディセーブル化されている CDP をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp run**	ディセーブル化されている CDP をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

次に、ディセーブル化されている CDP をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```

インターフェイスでの CDP のディセーブル化およびイネーブル化

CDP 情報の送受信を行う NNI 上では、CDP はデフォルトでイネーブルに設定されています。ENI 上で CDP をイネーブルにできますが、UNI 上ではサポートされていません。ポートで CDP をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 **（注）** インターフェイスが UNI の場合は、CDP を設定する前に、**port-type nni** または **port-type eni** インターフェイス コンフィギュレーション コマンドを入力する必要があります。デフォルトでは、CDP は、NNI 上ではイネーブルに、ENI 上ではディセーブルに設定されています。
ステップ 3	**no cdp enable**	インターフェイスの CDP をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポート上でディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	CDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 **（注）** インターフェイスが UNI の場合は、CDP を設定する前に、**port-type nni** または **port-type eni** インターフェイス コンフィギュレーション コマンドを入力する必要があります。デフォルトでは、CDP は、NNI 上ではイネーブルに、ENI 上ではディセーブルに設定されています。
ステップ 3	**cdp enable**	ディセーブルになっているインターフェイスの CDP をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、ポート上でディセーブル化されている CDP をイネーブルにする手順を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# cdp enable
Switch(config-if)# end
```

次に、UNI を ENI に変更し、ポート上の CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type eni
Switch(config-if)# cdp enable
Switch(config-if)# end
```

CDP のモニタリングおよびメンテナンス

ご使用のデバイスの CDP をモニタおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは複数実行します。

コマンド	説明
clear cdp counters	トラフィックのカウンタをゼロにリセットします。
clear cdp table	ネイバに関する CDP テーブルの情報を削除します。
show cdp	送信頻度、送信されたパケットのホールドタイムなどのグローバル情報を表示します。
show cdp entry *entry-name* [**protocol** | **version**]	特定のネイバに関する情報を表示します。 アスタリスク（*）を入力してすべての CDP ネイバを表示することも、情報が必要なネイバの名前を入力することもできます。 また、指定したネイバ上でイネーブルになっているプロトコルに関する情報、またはデバイス上で動作するソフトウェアのバージョンに関する情報だけを表示することもできます。
show cdp interface [*interface-id*]	CDP がイネーブル化されているインターフェイスに関する情報を表示します。 表示する情報に関して、インターフェイスの表示を制限できます。
show cdp neighbors [*interface-id*] [**detail**]	デバイスのタイプ、インターフェイスのタイプおよび番号、ホールドタイム設定、機能、プラットフォーム、ポート ID など、ネイバに関する情報を表示します。 特定のインターフェイスのネイバ情報だけを表示することも、より詳細な情報を表示することもできます。
show cdp traffic	CDP カウンタ（送受信されたパケット数、チェックサム エラーなど）を表示します。

CHAPTER 25

LLDP および LLDP-MED の設定

この章では、Cisco ME 3400E スイッチに Link Layer Discovery Protocol（LLDP）および LLDP Media Endpoint Discovery（LLDP-MED）を設定する方法について説明します。

（注） この章で使用されるコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンス、および『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* の「System Management Commands」を参照してください。

この章で説明する内容は、次のとおりです。

- 「LLDP および LLDP-MED の概要」（P.25-1）
- 「LLDP および LLDP-MED の設定」（P.25-3）
- 「LLDP および LLDP-MED のモニタおよびメンテナンス」（P.25-7）

LLDP および LLDP-MED の概要

- 「LLDP の概要」（P.25-1）
- 「LLDP-MED の概要」（P.25-2）

LLDP の概要

Cisco Discovery Protocol（CDP; シスコ検出プロトコル）は、すべてのシスコ製デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス ディスカバリ プロトコルです。CDP により、ネットワーク管理アプリケーションは、ネットワークに接続している他のシスコ製デバイスを自動的に検出し、これらのデバイスについて学習します。

他社製デバイスをサポートし、他のデバイス間での相互運用性を可能にするために、スイッチは IEEE 802.1AB Link Layer Discovery Protocol（LLDP; リンク レイヤ検出プロトコル）をサポートしています。LLDP は、ネットワーク デバイスが自身の情報をネットワーク上の他のデバイスにアドバタイズするために使用する近隣探索プロトコルです。このプロトコルがデータリンク層で稼動するため、異なるネットワーク レイヤ プロトコルを実行する 2 つのシステムは、相互に学習できます。

LLDP は、近接デバイスを検出するために使用する一連のアトリビュートをサポートします。これらのアトリビュートは、Type（タイプ）、Length（長さ）、および Value（値）の記述が含まれているため、TLV と呼ばれます。LLDP がサポートされているデバイスでは、TLV を使用して、近接デバイスに情報を送受信できます。設定情報、デバイスの機能、およびデバイス ID などの詳細情報を、このプロトコルを使用してアドバタイズできます。

デフォルトでは、LLDP は Network Node Interface（NNI; ネットワーク ノード インターフェイス）ではイネーブルに設定されています。Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）ではディセーブルに設定されていますが、イネーブルにできます。LLDP は、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）ではサポートされていません。

スイッチは、次の基本的な管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述の TLV
- システム名の TLV
- システムの説明
- システム機能の TLV
- 管理アドレスの TLV

次の組織的に固有な LLDP TLV も、LLDP-MED をサポートするためにアドバタイズされます。

- ポート VLAN ID TLV（IEEE 802.1 で組織的に固有な TLV）
- MAC/PHY コンフィギュレーション / ステータス TLV（IEEE 802.3 で組織的に固有な TLV）

LLDP-MED の概要

LLDP for Media Endpoint Devices（LLDP-MED）は、IP Phone などのエンドポイント デバイスとスイッチなどのネットワーク デバイスの間で動作する LLDP の拡張機能です。LLDP-MED は特に Voice over IP（VoIP）アプリケーションをサポートし、機能検出、ネットワーク ポリシー、Power over Ethernet（PoE）、およびコンポーネント管理のための TLV を追加します。

LLDP-MED は次の TLV をサポートします。

- LLDP-MED 機能の TLV

  LLDP-MED エンドポイントにより、接続されたデバイスがサポートする機能を決定し、デバイスでイネーブルになっている機能を決定できるようにします。

- ネットワーク ポリシーの TLV

  ネットワーク接続デバイスとエンドポイントの両方で、VLAN の設定とそのポート上の特定のアプリケーションに関連するレイヤ 2 およびレイヤ 3 のアトリビュートをアドバタイズできるようにします。たとえば、スイッチは、使用すべき VLAN 番号を電話機に通知することができます。電話機は、任意のスイッチに接続してその VLAN 番号を取得してから、コール制御との通信を開始できます。

- 電源管理の TLV

  LLDP-MED エンドポイントとネットワーク接続デバイスの間の高度な電源管理を可能にします。スイッチと電話機により、デバイスの電源を投入する方法、電源の優先順位、およびデバイスが必要とする電力の量など、電源に関する情報を伝達できるようにします。

- コンポーネント管理の TLV

  エンドポイントにより、エンドポイントの詳細なコンポーネント情報（ハードウェアのリビジョン番号、ファームウェアのバージョン、ソフトウェアのバージョン、シリアル番号、メーカー名、モデル名、資産 ID TLV など）をスイッチに送信できるようにします。

- ロケーションの TLV

  スイッチからエンドポイント デバイスへロケーション情報を提供します。所在地の TLV は次の情報を送信できます。

  - 都市ロケーション情報

都市の住所情報と郵便番号情報を提供します。都市ロケーション情報の例には、地名、番地、郵便番号などがあります。

– ELIN ロケーション情報

発信者のロケーション情報を提供します。ロケーションは Emergency Location Identifier Number（ELIN; 緊急ロケーション識別番号）によって決定されます。この番号は、緊急通報を最寄りの Public Safety Answering Point（PSAP）にルーティングする電話番号で、PSAP はこの番号を使用して通報者にコールバックできます。

LLDP および LLDP-MED の設定

- 「LLDP のデフォルト設定」（P.25-3）
- 「LLDP 特性の設定」（P.25-4）
- 「グローバルでの LLDP のディセーブル化およびイネーブル化」（P.25-4）
- 「インターフェイスでの LLDP のディセーブル化およびイネーブル化」（P.25-5）
- 「LLDP-MED TLV の設定」（P.25-6）

LLDP のデフォルト設定

表 25-1 に、LLDP のデフォルト設定を示します。デフォルト設定を変更するには、LLDP グローバル コンフィギュレーションおよび LLDP インターフェイス コンフィギュレーションのコマンドを使用します。

表 25-1　　LLDP のデフォルト設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット アップデート頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP TLV 選択	すべての TLV の送受信がディセーブルです。
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	Network Node Interface（NNI; ネットワーク ノード インターフェイス）でイネーブル、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）でディセーブル、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）では未サポート
LLDP 送信	NNI でイネーブル ENI でディセーブル UNI で未サポート
LLDP-MED TLV 選択	すべての LLDP-MED TLV の送信がディセーブル

LLDP 特性の設定

LLDP のアップデート頻度、廃棄するまでに情報を保持する時間、および初期化遅延時間を設定できます。送受信する LLDP TLV および LLDP-MED TLV も選択できます。

これらの特性を設定するには、特権 EXEC モードで次の手順を実行します。

（注）　ステップ 2 ～ 5 はすべて任意なので、順序不同で実行できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lldp holdtime** *seconds*	（任意）このデバイスから送信された情報を受信デバイスが廃棄するまで保持する時間を指定します。 指定できる範囲は 0 ～ 65535 秒で、デフォルトは 120 秒です。
ステップ 3	**lldp reinit**	（任意）任意のインターフェイスでの LLDP 初期化の遅延時間を秒単位で指定します。 指定できる範囲は 2 ～ 5 秒で、デフォルトは 2 秒です。
ステップ 4	**lldp timer** *seconds*	（任意）LLDP アップデートの伝送頻度を秒単位で設定します。 指定できる範囲は 5 ～ 65534 秒で、デフォルトは 30 秒です。
ステップ 5	**lldp tlv-select**	（任意）送信または受信する LLDP TLV を指定します。
ステップ 6	**lldp med-tlv-select**	（任意）送信または受信する LLDP-MED TLV を指定します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各 LLDP コマンドの **no** 形式を使用します。

次に、LLDP 特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config)# lldp timer 30
Switch(config)# end
```

LLDP の **show** コマンドの詳細については、「LLDP および LLDP-MED のモニタおよびメンテナンス」（P.25-7）を参照してください。

グローバルでの LLDP のディセーブル化およびイネーブル化

デフォルトでは LLDP はグローバルにディセーブルに設定されており、NNI ではイネーブルに設定されています。デフォルトでは ENI でディセーブルに設定されていますが、インターフェイスごとにイネーブルに設定できます。LLDP は UNI ではサポートしません。

LLDP をグローバルにディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2	**no lldp run**	LLDP をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

ディセーブル化されている LLDP-MED をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lldp run**	LLDP をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

次に、LLDP をグローバルにディセーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# no lldp run
Switch(config)# end
```

次に、LLDP をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

インターフェイスでの LLDP のディセーブル化およびイネーブル化

LLDP 情報の送受信をサポートするすべての NNI では、LLDP はデフォルトでディセーブルに設定されています。ENI ではデフォルトでディセーブルに設定されていますが、**lldp transmit** および **lldp receive** インターフェイス コンフィギュレーション コマンドを入力してイネーブルに設定できます。LLDP は UI ではサポートしません。

（注）　インターフェイスがトンネル ポートとして設定されている場合、LLDP は自動的にディセーブルになります。

インターフェイスの LLDP をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	LLDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。**lldp** コマンドを利用するには、インターフェイスは NNI または ENI でなければなりません。
ステップ 3	**no lldp transmit**	インターフェイスで LLDP パケットを送信しません。
ステップ 4	**no lldp receive**	インターフェイスで LLDP パケットを受信しません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ディセーブル化されている LLDP をインターフェイス上でイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。LLDP は NNI および ENI でだけサポートします。UNI ではサポートしません。必要に応じて、**port-type** {**eni** | **nni**} インターフェイス コンフィギュレーション コマンドを使用してポート タイプを変更します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルに設定します。デフォルトでは、NNI はイネーブルに、ENI および UNI はディセーブルに設定されています。
ステップ 4	**lldp transmit**	インターフェイスで LLDP パケットを送信します。
ステップ 5	**lldp receive**	インターフェイスで LLDP パケットを受信します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上で LLDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type nni
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```

LLDP-MED TLV の設定

デフォルトでは、スイッチは、LLDP-MED パケットをエンドポイント デバイスから受信するまで、LLDP パケットだけを送信します。その後、MED TLV とともに LLDP パケットを送信します。LLDP-MED のエントリが古くなると、ふたたび LLDP パケットだけを送信します。

lldp インターフェイス コンフィギュレーション コマンドを使用して、表 25-2 に示された TLV を送信しないようにインターフェイスを設定できます。

表 25-2　LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED コンポーネント管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

インターフェイスの TLV をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	LLDP-MED TLV を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no lldp med-tlv-select** ***tlv***	ディセーブルにする TLV を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスの TLV をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	LLDP-MED TLV を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**lldp med-tlv-select** ***tlv***	イネーブルにする TLV を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上でディセーブル化されている TLV をイネーブルにする手順を示します。

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```

LLDP および LLDP-MED のモニタおよびメンテナンス

ご使用のデバイスの LLDP および LLDP-MED をモニタおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは複数実行します。

コマンド	説明
clear lldp counters	トラフィックのカウンタをゼロにリセットします。
clear lldp table	ネイバに関する LLDP テーブルの情報を削除します。
show lldp	送信頻度、送信されたパケットのホールドタイム、インターフェイス上での LLDP 初期化の遅延時間などのグローバル情報を表示します。
show lldp entry *entry-name*	特定のネイバに関する情報を表示します。 アスタリスク（*）を入力してすべてのネイバを表示することも、情報が必要なネイバの名前を入力することもできます。
show lldp interface [*interface-id*]	LLDP がイネーブル化されているインターフェイスに関する情報を表示します。 表示する情報に関して、インターフェイスの表示を制限できます。

コマンド	説明
show lldp neighbors [*interface-id*] [**detail**]	デバイスのタイプ、インターフェイスのタイプおよび番号、ホールドタイム設定、機能、ポート ID など、ネイバに関する情報を表示します。 特定のインターフェイスのネイバ情報だけを表示することも、より詳細な情報を表示することもできます。
show lldp traffic	LLDP カウンタ（送受信されたパケット数、廃棄されたパケット数、認識されない TLV の数など）を表示します。

CHAPTER 26

UDLD の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに UniDirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルを設定する方法について説明します。

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

- 「UDLD の概要」（P.26-1）
- 「UDLD の設定」（P.26-3）
- 「UDLD ステータスの表示」（P.26-7）

UDLD の概要

UDLD は、光ファイバまたはツイストペア イーサネット ケーブルで接続されたデバイスが、ケーブルの物理構成をモニタしたり、単一方向リンクの存在を検出することを可能にするレイヤ 2 プロトコルです。プロトコルが正常に単一方向リンクを識別してディセーブルにするためには、接続されたすべてのデバイスが UDLD をサポートする必要があります。UDLD は、単一方向リンクを検出すると、対象となるポートをディセーブルにして警告します。単一方向リンクは、スパニング ツリー トポロジのループなど、さまざまな問題を引き起こすことがあります。

動作モード

UDLD は、2 つの動作モードをサポートしています。ノーマル モード（デフォルト）とアグレッシブ モードです。標準モードでは、UDLD は光ファイバ接続で誤って接続されたポートによる単一方向リンクを検出できます。アグレッシブ モードでも、UDLD は光ファイバおよびツイストペア リンクの一方向のトラフィック、および光ファイバ リンクで誤って接続されたポートによる、単一方向リンクを検出できます。

標準モードおよびアグレッシブ モードで、UDLD はレイヤ 1 メカニズムと連動して、リンクの物理ステータスを学習します。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバの ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

単一方向リンクが発生するのは、ローカル デバイスが送信したトラフィックをネイバが受信するのに対して、ネイバから送信されたトラフィックをローカル デバイスが受信しない場合です。

標準モードで、UDLD は、光ファイバ ポートのファイバ ストランドが誤って接続されて、レイヤ 1 メカニズムがこの誤った接続を検出できない場合の単一方向リンクを検出します。ポートは適切に接続されているが、トラフィックが一方向の場合、この状態を検出するよう想定されているレイヤ 1 メカニズムが検出しないため、UDLD では単一方向リンクを検出しません。この場合、論理リンクは不明となり、UDLD はポートをディセーブルにしません。

UDLD が標準モードのときに、1 組のファイバ ストランドの 1 つが切断され、自動ネゴシエーションがアクティブの場合、レイヤ 1 メカニズムがリンクの物理的問題を検出したため、リンクは維持されません。この場合、UDLD は何の処理も行わず、論理リンクは不明となります。

アグレッシブ モードでは、UDLD は、以前の検出方法で単一方向リンクを検出します。また、アグレッシブ モードの UDLD は、2 つのデバイス間での障害が許されない、ポイントツーポイントリンク上での単一方向リンクも検出できます。また、次のいずれかの問題がある場合も単一方向リンクを検出できます。

- 光ファイバまたはツイストペア リンクで、ポートの 1 つがトラフィックの送受信が不可能な場合
- 光ファイバまたはツイストペア リンクで、ポートの 1 つがダウン状態で、他のインターフェイスはアップである場合
- ケーブルのファイバ ストランドの 1 つが、切断されている場合

このような場合、UDLD は影響されるポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD hello パケットの存在は、リンクのヘルスを保証するハートビートと見なされます。逆にハート ビートの損失は、双方向リンクを再確立できない場合に、リンクをシャットダウンする必要があることを意味します。

レイヤ 1 から見てケーブルの両方のファイバ ストランドが正常に動作していれば、アグレッシブ モードの UDLD は、それらのファイバ ストランドが正しく接続されているかどうか、トラフィックが正しいネイバ間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で動作するので、この判別は自動ネゴシエーションでは不可能です。

単一方向リンクの検出方法

UDLD は、次の 2 つのメカニズムで動作します。

- 近接データベースのメンテナンス

  UDLD は、すべてのアクティブ ポートで hello パケット（別名アドバタイズまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバについて学習し、各デバイスがネイバに関しての最新情報を維持できるようにします。

  スイッチは hello メッセージを受信すると、エージングタイム（ホールドタイムまたは Time to Live [TTL]）が満了するまで、情報をキャッシュします。古いキャッシュ エントリの期限満了までに新しい hello メッセージを受信した場合、スイッチは古いエントリを新しいものと置き換えます。

  UDLD の稼動中にポートをディセーブルにしたり、ポートで UDLD をディセーブルにしたり、もしくはスイッチをリセットした場合はいつでも、設定変更によって影響を受けたポートの既存のキャッシュ エントリがすべて消去されます。UDLD は 1 つまたは複数のメッセージを送信して、ネイバに、ステータス変更によって影響を受けたキャッシュの部分をフラッシュするよう通知します。このメッセージは、キャッシュの同期を維持するためのものです。

- イベント駆動型検出およびエコー

  UDLD は、検出メカニズムとしてエコーを使用しています。UDLD デバイスが新しいネイバについて学習するか、または非同期ネイバから再同期要求を受信すると、接続側で検出ウィンドウを再起動してエコー メッセージを返信します。すべての UDLD ネイバで同じ動作をするので、エコーの送信側は返信エコーの受信を予測します。

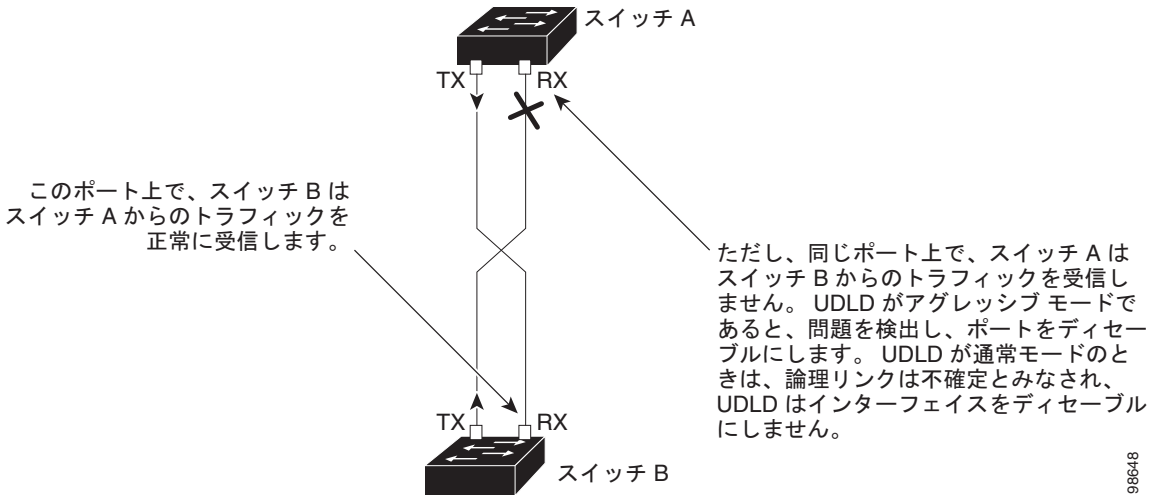
検出ウィンドウが終了して有効な応答メッセージを受信しなかった場合、UDLD モードに応じて、リンクはシャットダウンします。UDLD が標準モードのときは、リンクは不明と見なされ、シャットダウンされません。UDLD がアグレッシブ モードのときは、リンクは単一方向であると見なされ、ポートはディセーブルになります。

標準モードの UDLD がアドバタイズ フェーズまたは検出フェーズにあり、すべてのネイバ キャッシュ エントリが無効である場合、UDLD はリンクアップ シーケンスを再起動して、同期していない可能性のあるネイバとの同期化を再度行います。

ポートのすべてのネイバが、アドバタイズまたは検出フェーズのいずれかで無効であるときに、アグレッシブ モードをイネーブルにした場合、UDLD はリンクアップ シーケンスを再起動して、同期していない可能性のあるネイバとの同期化を再度行います。高速メッセージ列のあと、リンク ステートがまだ不明の場合は、UDLD がポートをシャットダウンします。

図 26-1 に、単一方向リンク状態の例を示します。

図 26-1　　UDLD による単一方向リンク検出



UDLD の設定

- 「UDLD のデフォルト設定」（P.26-4）
- 「設定時の注意事項」（P.26-4）
- 「UDLD のグローバルなイネーブル化」（P.26-5）
- 「インターフェイスでの UDLD のイネーブル化」（P.26-5）
- 「UDLD によりディセーブル化されたインターフェイスのリセット」（P.26-6）

UDLD のデフォルト設定

表 26-1 に、UDLD のデフォルト設定を示します。

表 26-1　UDLD のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ ポートでディセーブル
ポート別の UDLD イネーブル ステート（ツイストペア [銅] メディア用）	すべての イーサネット 10/100 および 1000BASE-TX ポートでディセーブル
UDLD アグレッシブ モード	ディセーブル

設定時の注意事項

- UDLD は Asynchronous Transfer Mode（ATM; 非同期転送モード）ポートではサポートされていません。
- UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合は、このポートは単一方向リンクを検出できません。
- モード（標準またはアグレッシブ）を設定するときは、リンクの両側で同じモードが設定されていることを確認してください。

注意　ループ ガードが機能するのは、ポイントツーポイント リンク上だけです。リンクの両端に、STP を実行しているデバイスを直接接続することを推奨します。

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは標準モードで UDLD をイネーブルにし、スイッチの光ファイバ ポートすべてに設定可能なメッセージ タイマーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*}	（任意）UDLD モードを指定します。 • **aggressive** : すべての光ファイバ ポート上で、アグレッシブ モードで UDLD をイネーブルにします。 • **enable** : スイッチのすべての光ファイバ ポート上で、標準モードで UDLD をイネーブルにします。UDLD は、デフォルトでディセーブルに設定されています。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定より優先されます。 アグレッシブ モードおよび標準モードの詳細については、「動作モード」（P.26-1）を参照してください。 • **message time** *message-timer-interval* : アドバタイズ フェーズにあり、双方向であると検出されているポート上で、UDLD プローブ メッセージの間隔を設定します。指定できる範囲は 7 ～ 90 秒です。 （注）　このコマンドは、光ファイバ ポートに対してだけ有効です。他のポート タイプで UDLD をイネーブルにするには、**udld** インターフェイス コンフィギュレーション コマンドを使用します。詳細については、「インターフェイスでの UDLD のイネーブル化」（P.26-5）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show udld**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

UDLD をグローバルにディセーブルにするには、**no udld enable** グローバル コンフィギュレーション コマンドを使用して、すべての光ファイバ ポート上で UDLD 標準モードをディセーブルにします。すべての光ファイバ ポート上で UDLD アグレッシブ モードをディセーブルにするには、**no udld aggressive** グローバル コンフィギュレーション コマンドを使用します。

インターフェイスでの UDLD のイネーブル化

ポート上で、アグレッシブ モードまたは標準モードで UDLD をイネーブルにするか、または UDLD をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	UDLD をイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 4	**udld port** [**aggressive**]	UDLD は、デフォルトでディセーブルに設定されています。 • **udld port** : 指定したポート上で、標準モードで UDLD をイネーブルにします。 • **udld port aggressive** : 指定したポート上で、アグレッシブ モードで UDLD をイネーブルにします。 （注）　指定された光ファイバ ポート上で UDLD をディセーブルにするには、**no udld port** インターフェイス コンフィギュレーション コマンドを使用します。 アグレッシブ モードおよび標準モードの詳細については、「動作モード」（P.26-1）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show udld** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

UDLD によりディセーブル化されたインターフェイスのリセット

UDLD によってディセーブル化されたすべてのポートをリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**udld reset**	UDLD によってディセーブル化されたすべてのポートをリセットします。
ステップ 2	**show udld**	設定を確認します。

次のコマンドを使用してポートを起動することもできます。

- **shutdown** インターフェイス コンフィギュレーション コマンドのあとに **no shutdown** インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再起動します。
- **no udld** {**aggressive** | **enable**} **グローバル コンフィギュレーションのあとに udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再びイネーブルになります。
- **no udld port** インターフェイス コンフィギュレーション コマンドのあとに **udld port** [**aggressive**] インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイバ ポートが再びイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを実行すると、UDLD errdisable ステートから自動的に回復するためのタイマーがイネーブルになります。また、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドを実行すると、UDLD errdisable ステートから回復する時間が指定されます。

UDLD ステータスの表示

指定したポートまたはすべてのポートの UDLD ステータスを表示するには、**show udld** [*interface-id*] 特権 EXEC コマンドを使用します。

コマンド出力のフィールドの詳細ついては、このリリースのコマンド リファレンスを参照してください。

CHAPTER 27

SPAN および RSPAN の設定

この章では、Cisco ME 3400E イーサネット スイッチに Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN）を設定する方法について説明します。

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

- 「SPAN および RSPAN の概要」（P.27-1）
- 「SPAN および RSPAN の設定」（P.27-9）
- 「SPAN および RSPAN ステータスの表示」（P.27-24）

SPAN および RSPAN の概要

ポートまたは VLAN（仮想 LAN）を通過するネットワーク トラフィックを分析するには、SPAN または RSPAN を使用して、そのスイッチの別のポート、またはネットワーク アナライザなどのモニタリング デバイスやセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポートまたは送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、分析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングに影響を与えません。宛先ポートを SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外のトラフィックを、宛先ポートが受信または転送することはありません。

SPAN を使用して監視できるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされるトラフィックは監視できません。たとえば、着信トラフィックを監視している場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックは監視できません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは監視できます。

SPAN または RSPAN 宛先ポートを使用すると、ネットワーク セキュリティ デバイスからトラフィックを送信できます。たとえば、Cisco Intrusion Detection System（IDS; 侵入検知システム）センサ装置を宛先ポートに接続した場合、IDS デバイスは TCP リセット パケットを送信して疑わしい攻撃者の TCP セッションを停止させることができます。

ここでは、次の概要について説明します。

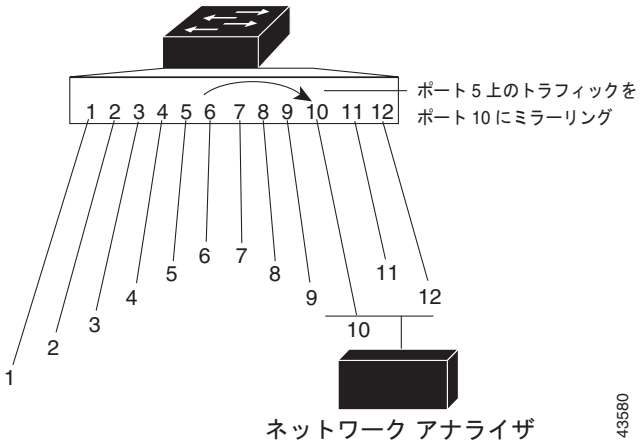
- 「ローカル SPAN」（P.27-2）
- 「Remote SPAN」（P.27-2）
- 「SPAN および RSPAN の概念と用語」（P.27-3）

- 「SPAN および RSPAN の他の機能との相互作用」（P.27-8）

ローカル SPAN

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートあるいは 1 つまたは複数の VLAN から宛先ポートに送信されるトラフィックをコピーして、分析します。たとえば、図 27-1 では、ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされています。ポート 10 のネットワーク アナライザは、ポート 5 に物理的に接続しなくても、ポート 5 からすべてのネットワーク トラフィックを受信します。

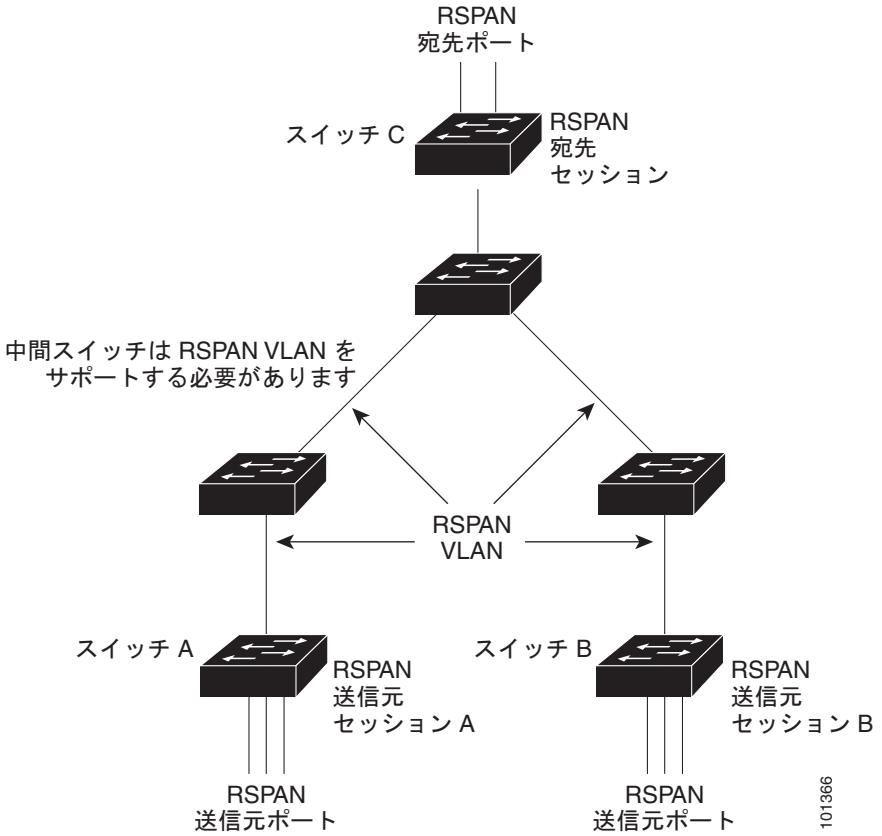
図 27-1　　単一スイッチでのローカル SPAN の設定例



Remote SPAN

RSPAN を使用すると、異なるスイッチ上で送信元ポート、送信元 VLAN、宛先ポートがサポートされるため、ネットワーク内で複数のスイッチの Remote Monitoring（RMON）がイネーブルになります。図 27-2 に、スイッチ A およびスイッチ B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN を監視する宛先セッションに転送されます。各 RSPAN 送信元スイッチでは、RSPAN 送信元としてポートまたは VLAN のいずれかを設定する必要があります。宛先は常に物理ポートになります（スイッチ C を参照）。

図 27-2　RSPAN の設定例



SPAN および RSPAN の概念と用語

ここでは、SPAN および RSPAN の設定に関連する概念と用語について説明します。

SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1 つまたは複数のポート、あるいは 1 つまたは複数の VLAN 上でトラフィックを監視し、監視したトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN（すべて単一のネットワーク デバイス上にある）の対応付けです。ローカル SPAN には、送信元セッションおよび宛先セッションが個別に設定されません。ローカル SPAN セッションはユーザが指定した入力および出力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は 1 つまたは複数の RSPAN 送信元セッション、1 つの RSPAN VLAN、および複数の RSPAN 宛先セッションで構成されます。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、送信元ポートまたは送信元 VLAN のセットを RSPAN VLAN と関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN と関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームの転送先を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを介して宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットから VLAN タギングを除去し、宛先ポートに送ります。RSPAN 宛先セッションの目的は、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットをユーザにコピーして、分析することです。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。RSPAN 送信元セッションと宛先セッションを分離する中間スイッチを配置することもできます。これらのスイッチには RSPAN の実行機能は不要ですが、RSPAN VLAN の要件を満たす必要があります（「RSPAN VLAN」（P.27-8）を参照）。

SPAN セッションでのトラフィックの監視には、次のような制限があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- スイッチは、最大 2 つの送信元セッション（ローカル SPAN および RSPAN 送信元セッション）をサポートします。同じスイッチで、ローカル SPAN 送信元セッション および RSPAN 送信元セッションの両方を実行できます。スイッチは合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、設定できる宛先ポートは最大で 64 です。
- 個別のまたは重複する SPAN 送信元ポートと VLAN の集合を使用して、2 つの独立した SPAN または RSPAN 送信元セッションを設定できます。スイッチでメトロ IP アクセス イメージが稼動している場合は、スイッチド ポートおよびルーテッド ポートの両方を SPAN 送信元および SPAN 宛先として設定できます。
- SPAN セッションは、スイッチの正常な動作を妨げません。ただし、SPAN の宛先がオーバーサブスクライブ型ポートである場合（たとえば 100 Mbps ポートを監視する 10 Mbps ポートなど）、パケットが廃棄されるか、または消失する可能性があります。
- RSPAN がイネーブルの場合、監視中の各パケットは 2 回伝送されます。1 回は標準トラフィックとして、もう 1 回は監視されたパケットとしてです。したがって、多数のポートまたは VLAN を監視すると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上でも SPAN セッションを設定できます。宛先ポートと、1 つまたは複数の送信元ポートまたは VLAN をイネーブルにしないかぎり、SPAN セッションはアクティブになりません。
- スイッチの単一セッション内では、ローカル SPAN と RSPAN を併用できません。つまり、RSPAN 送信元セッションにローカル宛先ポートを設定したり、RSPAN 宛先セッションにローカル送信元ポートを設定したり、同じスイッチ上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

監視対象トラフィック

SPAN セッションは、次のトラフィック タイプを監視できます。

- 受信（RX）SPAN：受信（または入力）SPAN の目的は、スイッチが変更または処理を行う前に送信元インターフェイスまたは VLAN が受信したすべてのパケットをできるかぎり多く監視することです。送信元が受信した各パケットのコピーがその SPAN セッションの宛先ポートに送信されます。

  Differentiated Services Code Point（DSCP）の変更など、ルーティングまたは QoS（Quality of Service）が原因で変更されるパケットは、変更前にコピーされます。

受信処理中にパケットを廃棄する可能性のある機能は、入力 SPAN には無効です。宛先ポートは、実際の着信パケットが廃棄された場合でも、パケットのコピーを受信します。これらの機能には、標準および拡張 IP 入力 Access Control List（ACL; アクセス コントロール リスト）、入力 QoS ポリシング、VLAN ACL、出力 QoS ポリシングなどがあります。

- 送信（TX）SPAN：送信（または出力）SPAN の目的は、スイッチによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできるかぎり多く監視することです。送信元から送信された各パケットのコピーは、その SPAN セッションに対応する宛先ポートに送信されます。コピーは、パケットの変更後送信されます。

  ルーティングが原因で変更されたパケット（Time to Live [TTL]、MAC [メディア アクセス制御] アドレス、QoS 値の変更など）は、宛先ポートで（変更されて）コピーされます。

  送信処理中にパケットを廃棄する可能性のある機能は、SPAN 用のコピーにも影響を与えます。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングなどがあります。

- 双方向：1 つの SPAN セッションで、単一のポートまたは VLAN の送信パケットと受信パケットを両方監視できます。これはデフォルト設定です。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。通常、SPAN は Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）などの Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）パケットおよびレイヤ 2 プロトコルを監視しません。ただし、宛先ポートを設定するときにキーワード **encapsulation replicate** を入力すると、次のように変更されます。

- 送信ポートの場合と同じカプセル化設定（タグなしまたは IEEE 802.1Q）を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットが監視されます。

したがって、カプセル化レプリケーションがイネーブル化されたローカル SPAN セッションでは、タグなし、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在する場合があります。

スイッチが輻輳すると、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットが廃棄されることがあります。一般に、これらの特性は相互に依存しません。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因で監視されないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スイッチ輻輳が原因で廃棄された出力パケットは、出力 SPAN からも廃棄されます。

SPAN の設定によっては、同じ送信元パケットの複数のコピーが SPAN 宛先ポートに送信される場合があります。たとえば、ポート A では RX 監視用に、ポート B では TX 監視用に、双方向（RX と TX）SPAN セッションが設定されているとします。パケットがポート A を介してスイッチに着信し、ポート B にスイッチングされると、着信パケットと発信パケットの両方が宛先ポートに送信されます。このため、両方のパケットは同じものになります（レイヤ 3 書き換えが行われない場合には、パケット変更のため異なるパケットになります）。

送信元ポート

送信元ポート（別名*監視対象ポート*）は、ネットワーク トラフィック分析のために監視するスイッチド ポートまたはルーテッド ポートです。1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向で監視できます。スイッチは、任意の数の送信元ポート（スイッチで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートします。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数は最大 2 つ（ローカルまたは RSPAN）であるため、単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートには、次の特性があります。

- 複数の SPAN セッションで監視できます。
- 各送信元ポートに、監視する方向（入力、出力、両方）を設定できます。
- すべてのタイプのポート（EtherChannel、ファスト イーサネット、ギガビット イーサネット、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）、Network Node Interface（NNI; ネットワーク ノード インターフェイス）、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）を送信元ポートに設定できます
- EtherChannel 送信元の場合は EtherChannel 全体で、または物理ポートがポート チャネルに含まれている場合は物理ポート上で個別に、トラフィックを監視できます。
- 送信元ポートを、ルーテッド ポート、アクセス ポート、またはトランク ポートにすることができます。
- 宛先ポートに指定できません。
- 送信元ポートは同じ VLAN 内にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートを監視できます。

送信元 VLAN

VLAN-based SPAN（VSPAN）では、1 つまたは複数の VLAN のネットワーク トラフィックを監視できます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスは VLAN ID で指定され、トラフィックはその VLAN のすべてのポートで監視されます。

VLAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向で監視できます。
- 指定されたポートでは、監視対象の VLAN 上のトラフィックだけが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、監視されません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、監視中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN は使用できません。
- 監視できるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとして監視する場合、デフォルトでは、トランク上でアクティブなすべての VLAN が監視されます。VLAN フィルタリングを使用すれば、トランク送信元ポートでの SPAN トラフィックの監視を特定の VLAN に制限できます。

- VLAN フィルタリングは、トランク ポートにだけ適用されます。
- VLAN フィルタリングはポートベース セッションにだけ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、リスト内のこれらの VLAN だけがトランク ポートで監視されます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにだけ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートまたは VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名*監視側ポート*）が必要です。

宛先ポートには、次の特性があります。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチになければなりません。RSPAN セッションの場合、宛先ポートは RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションだけを実行するスイッチには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先ポートの設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。
- EtherChannel グループに含まれていたポートが宛先ポートとして設定されている場合、そのポートはグループから削除されます。スイッチでメトロ IP アクセス イメージが稼動していて、ポートがルーテッド ポートであった場合、そのポートはルーテッド ポートではなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにはできません。
- 送信元ポートには指定できません。
- EtherChannel グループまたは VLAN にはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。このポートでは、SPAN セッションに必要なトラフィック以外の送信は行われません。宛先ポートでは着信トラフィックの学習または転送は行われません。
- 入力トラフィックの転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、監視されません。
- スイッチの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートでは、VLAN タギングおよびカプセル化に関する動作が異なります。

- ローカル SPAN では、宛先ポートにキーワード **encapsulation replicate** が指定されている場合、各パケットに元のカプセル化が使用されます（タグなし、または IEEE 802.1Q）。**encapsulation dot1q** が指定されている場合、パケットは IEEE 802.1Q カプセル化により表示されます。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブル化されたローカル SPAN セッションの出力に、タグなし、または IEEE 802.1Q タグ付きパケットが混在する場合があります。
- RSPAN の場合、元の VLAN ID は RSPAN VLAN ID で上書きされるため、失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN 送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には次の特殊な特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上だけです。
- RSPAN VLAN は、**remote-span** VLAN コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
  - VLAN を UNI-ENI 独立 VLAN（デフォルト）から RSPAN VLAN に変更するには、**rspan-vlan** VLAN コンフィギュレーション モード コマンドを入力します。
  - UNI-ENI コミュニティ VLAN を RSPAN VLAN に変更するには、**no uni-vlan** VLAN コンフィギュレーション モード コマンドを入力してまずコミュニティ VLAN を削除する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。

（注）　NNI はデフォルトで STP をサポートし、ENI の STP をイネーブルにできます。UNI では、STP はサポートされていません。

- RSPAN VLAN は、プライベート VLAN のプライマリまたはセカンダリ VLAN にできません。

通常は、ネットワークに複数の RSPAN VLAN を配置し、同時にそれぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションから RSPAN セッションにパケットを送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN を監視したり、ユーザにトラフィックを送信することもできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN の他の機能との相互作用

SPAN は次の機能と相互作用します。

- ルーティング：メトロ IP アクセス イメージを稼動しているスイッチでは、SPAN はルーテッド トラフィックを監視リングしません。RSPAN が監視するのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックは監視しません。たとえば、VLAN が受信監視され、スイッチが別の VLAN から監視対象 VLAN にトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。
- STP：宛先ポートの SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は、RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。ただし、STP は、NNI または ENI 上でだけサポートされ、UNI は STP に参加しません。
- CDP：SPAN 宛先ポートは、SPAN セッションがアクティブな間は CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。NNI ではデフォルトで CDP をイネーブルにし、ENI で CDP をイネーブルにできます。UNI は CDP に参加しません。

- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定値は、いつでも変更できます。ただし、宛先ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、SPAN 宛先設定を削除しないかぎり有効になりません。送信元ポートの VLAN メンバーシップまたはトランク設定の変更はただちに有効になり、個々の SPAN セッションは、それに応じて自動的に調整されます。
- EtherChannel：EtherChannel グループを送信元ポートに設定できますが、SPAN 宛先ポートには設定できません。グループを SPAN 送信元として設定すると、グループ全体が監視対象となります。

  監視対象 EtherChannel グループに物理ポートを追加すると、新しいポートが SPAN 送信元ポートリストに追加されます。監視対象 EtherChannel グループからポートを削除すると、SPAN 送信元ポート リストから自動的に削除されます。

  EtherChannel グループに属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とできます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータは監視されます。ただし、EtherChannel グループに属する物理ポートを SPAN 宛先ポートに設定した場合は、EtherChannel グループから削除されます。SPAN セッションからポートが削除されると、EtherChannel グループに復帰します。EtherChannel グループから削除されたポートはグループのメンバーに残りますが、*非アクティブ*または*サスペンド* ステートになります。

  EtherChannel グループに属する物理ポートが宛先ポートであり、かつ、EtherChannel グループが送信元である場合、ポートは EtherChannel グループおよび監視対象ポートのリストから削除されます。
- マルチキャスト トラフィックを監視できます。送信側および受信側ポートのモニタリングの場合は、未編集パケットが 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト パケットが送信される回数は反映されません。
- プライベート VLAN ポートは、SPAN 宛先ポートにはなれません。
- セキュア ポートは SPAN 宛先ポートにできません。

  SPAN セッションでは、宛先ポートで入力転送がイネーブルの場合、出力を監視しているポートでポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力を監視しているどのポートでもポート セキュリティをイネーブルにしないでください。
- IEEE 802.1X ポートは SPAN 送信元ポートにできます。SPAN 宛先ポートで IEEE 802.1X をイネーブルにできますが、SPAN 宛先として削除するまでは IEEE 802.1X はディセーブルに設定されます。

  SPAN セッションでは、宛先ポートで受信転送がイネーブルの場合、送信を監視しているポートで IEEE 802.1X をイネーブルにしないでください。RSPAN 送信元セッションでは、送信を監視しているどのポートでも IEEE802.1X をイネーブルにしないでください。

SPAN および RSPAN の設定

- 「SPAN および RSPAN のデフォルト設定」（P.27-9）
- 「ローカル SPAN の設定」（P.27-10）
- 「RSPAN の設定」（P.27-17）

SPAN および RSPAN のデフォルト設定

表 27-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 27-1　SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN のステート（SPAN および RSPAN）	ディセーブル。
監視する送信元ポートのトラフィック	受信トラフィックと送信トラフィックの両方（**both**）
カプセル化タイプ（宛先ポート）	ネイティブ形式（タグなしパケット）
入力転送（宛先ポート）	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN が監視されます。
RSPAN VLAN	設定なし。デフォルトの VLAN タイプは、UNI-ENI 独立 VLAN です。

ローカル SPAN の設定

- 「SPAN 設定時の注意事項」（P.27-10）
- 「ローカル SPAN セッションの作成」（P.27-11）
- 「ローカル SPAN セッションの作成および入力トラフィックの設定」（P.27-14）
- 「フィルタリングする VLAN の指定」（P.27-16）

SPAN 設定時の注意事項

- スイッチごとに、2 つのローカル SPAN セッションまたは RSPAN 送信元セッションの合計を設定できます。スイッチでは、合計で 66 の SPAN セッション（ローカル RSPAN 送信元および RSPAN 宛先）を設定できます。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、または一定範囲のポートまたは VLAN のトラフィックを監視できます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートは送信元ポートにできません。また、送信元ポートは宛先ポートにできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定できません。
- スイッチ ポートを SPAN 宛先ポートに設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象のトラフィックだけです。
- SPAN コンフィギュレーション コマンドを入力しても、設定済みの SPAN パラメータは削除されません。設定された SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、キーワード **encapsulation replicate** またはキーワード **encapsulation dot1q** が指定されている場合、SPAN 宛先ポートを経由する発信パケットには元のカプセル化ヘッダー（タグなし、または IEEE 802.1Q）が付加されます。これらのキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。RSPAN 宛先ポートの場合、発信パケットはタグなしです。
- ディセーブルに設定されているポートは、送信元または宛先ポートにはできますが、SPAN 機能は、宛先ポートおよび 1 つまたは複数の送信元ポートまたは送信元 VLAN がイネーブルになるまでは起動しません。

- キーワード **filter vlan** を使用すると、特定の VLAN に対して SPAN トラフィックを制限できます。監視対象がトランク ポートの場合、このキーワードで指定された VLAN 上のトラフィックだけが監視されます。デフォルトでは、トランク ポートのすべての VLAN が監視されます。
- 1 つの SPAN セッション内で送信元 VLAN を混在させたり、VLAN をフィルタリングできません。

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元（監視対象）ポートまたは VLAN、および宛先（監視側）ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* の範囲は、1 ～ 66 です。 すべての SPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべての RSPAN セッションを削除するには **remote** を指定します。

	コマンド	目的
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 *session_number* の範囲は、1 ～ 66 です。 *interface-id* には、監視する送信元ポートまたは送信元 VLAN を指定します。 • 送信元 *interface-id* には、監視する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。*有効なポートチャネル番号は 1 ～ 48* です。 • *vlan-id* には、監視する送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 **（注）** 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN の併用はできません。 （任意）[**,** | **-**]：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、SPAN は送受信両方のトラフィックを監視します。 • **both**：送受信両方のトラフィックを監視します。これはデフォルト設定です。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。 **（注）** **monitor session** *session_number* **source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation**{**dot1q** | **replicate**}]	SPAN セッションおよび宛先ポート（監視側ポート）を指定します。 *session_number* には、ステップ 3 で入力したセッション番号を指定します。 **（注）** ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）IEEE 802.1Q カプセル化の場合は **encapsulation dot1q** を、または **encapsulation replicate** を入力して、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するよう指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 **（注）** **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除する場合は、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式では、キーワード **encapsulation replicate** は無視されます。

次に、SPAN セッション 1 を設定し、送信元ポートから宛先ポートへのトラフィックを監視する例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、双方向トラフィックを送信元ギガビット イーサネット ポート 1 から宛先ギガビット イーサネット ポート 2 へミラーリングして、カプセル化方式を維持します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
encapsulation replicate
Switch(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元である、ポート 1 を削除する例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1
Switch(config)# end
```

次に、双方向監視用に設定された、ポート 1 での受信トラフィック監視をディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1 rx
```

ポート 1 での受信トラフィックの監視はディセーブルになりますが、このポートから送信されるトラフィックは引き続き監視されます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ～ 3 に属するすべてのポートで受信トラフィックを監視するように SPAN セッション 2 を設定し、監視されたトラフィックをスイッチ 1 の宛先ギガビット イーサネット ポート 2 に送信する例を示します。この設定は、VLAN 10 に属するすべてのポートですべてのトラフィックを監視するように変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

ローカル SPAN セッションの作成および入力トラフィックの設定

SPAN セッションを作成して送信元ポート、送信元 VLAN、および宛先ポートを指定し、ネットワーク セキュリティ デバイス（Cisco IDS センサ装置など）用の宛先ポート上の入力トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

（注）　入力トラフィックに関連性のないキーワードの詳細については、「ローカル SPAN セッションの作成」（P.27-11）を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（監視対象ポート）を指定します。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged**] **vlan** *vlan-id*}]	SPAN セッション、宛先ポート、パケット カプセル化、入力側 VLAN、およびカプセル化を指定します。 *session_number* には、ステップ 3 で入力したセッション番号を指定します。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （任意）**[,** | **-]** : 一連のまたは一定範囲のインターフェイスを指定します。カンマまたはハイフンの前後にはスペースを入力します。 （任意）IEEE 802.1Q カプセル化の場合は **encapsulation dot1q** を、または **encapsulation replicate** を入力して、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するよう指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 宛先ポートで入力トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** に次のキーワードを指定して入力します。 • **dot1q** *:* IEEE 802.1Q カプセル化を使用し、デフォルト VLAN として指定された VLAN を設定して、着信パケットを転送します。 • **untagged** *:* タグなしカプセル化 タイプを使用し、デフォルト VLAN として指定された VLAN を設定して、着信パケットを転送します。 • **vlan** *vlan-id* : デフォルト VLAN です。**dot1q** または **untagged** のいずれも指定しない場合、デフォルトでタグなしパケットが転送されます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除する場合は、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式では、encapsulation および ingress オプションは無視されます。

次に、SPAN セッション 2 の既存の設定を削除し、送信元ギガビット イーサネット ポート 1 に送信されたトラフィックを監視するように SPAN セッション 2 を設定し、このトラフィックを送信元ポートと同じ出力カプセル化タイプを使用して宛先ギガビット イーサネット ポート 2 に送信し、IEEE 802.1Q カプセル化およびデフォルト入力 VLAN として VLAN 6 を使用する着信転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress dot1q vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* の範囲は、1 ～ 66 です。 すべての SPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべての RSPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id*	送信元ポート（監視対象ポート）および SPAN セッションの特性を指定します。 *session_number* の範囲は、1 ～ 66 です。 *interface-id* には、監視する送信元ポートを指定します。指定されたインターフェイスが、トランク ポートとして設定されている必要があります。
ステップ 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* には、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* では、指定できる範囲は 1 ～ 4094 です。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して一定範囲の VLAN を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**dot1q** | **replicate**}]}	SPAN セッションおよび宛先ポート（監視側ポート）を指定します。 *session_number* には、ステップ 3 で入力したセッション番号を指定します。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （任意）**[,** | **-]**：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）**encapsulation dot1q** または **encapsulation replicate** を入力して、IEEE 802.1Q カプセル化または宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するよう指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN を監視するには、**no monitor session** *session_number* **filter** ローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定を削除し、ギガビット イーサネット トランク ポート 2 での受信トラフィックを監視するように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および VLAN 9 のトラフィックだけを宛先ギガビット イーサネット ポート 1 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet0/1
Switch(config)# end
```

RSPAN の設定

- 「RSPAN 設定時の注意事項」（P.27-17）
- 「RSPAN VLAN としての VLAN の設定」（P.27-18）
- 「RSPAN 送信元セッションの作成」（P.27-19）
- 「RSPAN 宛先セッションの作成」（P.27-20）
- 「RSPAN 宛先セッションの作成および入力トラフィックの設定」（P.27-21）
- 「フィルタリングする VLAN の指定」（P.27-23）

RSPAN 設定時の注意事項

- RSPAN には、「SPAN 設定時の注意事項」（P.27-10）のすべての項目が当てはまります。
- RSPAN VLAN には特殊なプロパティがあるので、RSPAN VLAN として使用する VLAN をネットワーク上にいくつか確保しておき、これらの VLAN にはアクセス ポートを割り当てないでください。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択してフィルタリングまたは監視できます。これらの ACL は、RSPAN 送信元スイッチ内の RSPAN VLAN 上で指定します。
- RSPAN の設定では、送信元ポートと宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- RSPAN は BPDU パケット モニタリングその他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにだけ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生するのを防ぐため、参加しているすべてのスイッチで VLAN リモート SPAN 機能がサポートされていることを確認してください。
- RSPAN VLAN 上のアクセス ポートは、非アクティブ ステートになります。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として組み込まれます。また、RSPAN VLAN を SPAN セッションの送信元にすることもできます。ただし、スイッチはセッション間にわたるトラフィックを監視しないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。
- 任意の VLAN を RSPAN VLAN として設定するには、次の条件を満たす必要があります。
  - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
  - 参加するすべてのスイッチが RSPAN をサポートしている。
  - RSPAN VLAN で、MAC アドレス ラーニング がイネーブルである。

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。

RSPAN VLAN としての VLAN の設定

RSPAN セッション用の RSPAN VLAN に設定する VLAN を新規に作成します。RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。送信元スイッチと宛先スイッチ、およびすべての中間スイッチで RSPAN VLAN を設定する必要があります。

RSPAN トラフィックのフローを効率化するために、RSPAN トラフィックを送信する必要のないすべてのトランクから、RSPAN VLAN を手動で削除してください。

RSPAN VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ～ 1001 および 1006 ～ 4094 です。 **（注）** RSPAN VLAN は、VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングや FDDI VLAN 専用）にできません。 UNI-ENI コミュニティ VLAN の VLAN ID を入力する場合、**no uni-vlan** VLAN コンフィギュレーション コマンドを入力してコミュニティ VLAN のタイプを削除する必要があります。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN から SPAN の特性を削除して、UNI-ENI 独立 VLAN に変換するには、**no remote-span** VLAN コンフィギュレーション コマンドを使用します。

次に、RSPAN VLAN 901 を作成する例を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを開始し、監視対象の送信元および宛先 RSPAN VLAN を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の RSPAN 設定を削除します。 *session_number* の範囲は、1 ～ 66 です。 すべての RSPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべての RSPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	RSPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 *session_number* の範囲は、1 ～ 66 です。 RSPAN セッションの送信ポートまたは送信元 VLAN を入力します。 • *interface-id* には、監視する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。*有効なポートチャネル番号は 1 ～ 48* です。 • *vlan-id* には、監視する送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 **（注）** 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN の併用はできません。 （任意）[**,** | **-**]：一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送受信両方のトラフィックを送信します。 • **both**：送受信両方のトラフィックを監視します。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。
ステップ 4	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先 RSPAN VLAN を指定します。 *session_number* には、ステップ 3 で定義した番号を入力します。 *vlan-id* には、監視する送信元 RSPAN VLAN を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除する場合は、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session** *session_number* **destination remote vlan** *vlan-id コマンドを使用します。*

次に、セッション 1 の既存の RSPAN 設定を削除し、複数の送信元インターフェイスを監視するように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 1 source interface port-channel 12
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは別のスイッチ（送信元セッションが設定されていないスイッチ）に設定します。

スイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id*	送信元スイッチで作成された RSPAN VLAN の VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。 **（注）** VLAN が UNI-ENI コミュニティ VLAN として設定される場合、**no uni-vlan** VLAN コンフィギュレーション コマンドを入力してコミュニティ VLAN のタイプを削除する必要があります。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として識別します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の RSPAN 設定を削除します。 *session_number* の範囲は、1 ～ 66 です。 すべての RSPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべての RSPAN セッションを削除するには **remote** を指定します。
ステップ 6	**monitor session** *session_number* **source remote vlan** *vlan-id*	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 *session_number* の範囲は、1 ～ 66 です。 *vlan-id* には、監視する送信元 RSPAN VLAN を指定します。

	コマンド	目的
ステップ 7	**monitor session** *session_number* **destination interface** *interface-id*	RSPAN セッションおよび宛先インターフェイスを指定します。 *session_number* には、ステップ 6 で定義した番号を入力します。 （注）　RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスには物理インターフェイスを指定する必要があります。 （注）　**encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されていますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除する場合は、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから宛先ポートを削除するには、**no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session** *session_number* **source remote vlan** *vlan-id コマンドを使用します。*

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet0/1
Switch(config)# end
```

RSPAN 宛先セッションの作成および入力トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、ネットワーク セキュリティ デバイス（Cisco IDS センサ装置など）用の宛先ポート上の入力トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

（注）　入力トラフィックに関連しないキーワードの詳細については、「RSPAN 宛先セッションの作成」（P.27-20）を参照してください。この手順では、RSPAN VLAN が設定してあると想定しています。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。

	コマンド	目的
ステップ 3	**monitor session** *session_number* **source remote vlan** *vlan-id*	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 *session_number* の範囲は、1 ～ 66 です。 *vlan-id* には、監視する送信元 RSPAN VLAN を指定します。
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**ingress** {**dot1q vlan** *vlan-id* **| untagged vlan** *vlan-id* **| vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケット カプセル化、入力側 VLAN、およびカプセル化を指定します。 *session_number* には、ステップ 4 で定義した番号を入力します。 **（注）** RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスには物理インターフェイスを指定する必要があります。 **（注）** **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されていますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 （任意）**[, | -]** : 一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 宛先ポートで入力トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** に次のキーワードを指定して入力します。 • **dot1q vlan** *vlan-id* : IEEE 802.1Q カプセル化を使用し、デフォルト VLAN として指定された VLAN を設定して、着信パケットを転送します。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id* : タグなしカプセル化タイプを使用し、デフォルト VLAN として指定された VLAN を設定して、着信パケットを転送します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RSPAN セッションを削除する場合は、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。RSPAN セッションから宛先ポートを削除するには、**no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。このコマンドの **no** 形式では、ingress オプションは無視されます。

次に、VLAN 901 を RSPAN セッション 2 の送信元リモート VLAN に設定し、ギガビット イーサネット送信元ポート 2 を宛先インターフェイスとして設定し、VLAN 6 がデフォルト入力 VLAN として設定されたインターフェイス上で入力転送をイネーブルにする例を示します。

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* の範囲は、1 ～ 66 です。 すべての SPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべての RSPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id*	送信元ポート（監視対象ポート）および SPAN セッションの特性を指定します。 *session_number* の範囲は、1 ～ 66 です。 *interface-id* には、監視する送信元ポートを指定します。指定されたインターフェイスが、トランク ポートとして設定されている必要があります。
ステップ 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* には、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* では、指定できる範囲は 1 ～ 4094 です。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して一定範囲の VLAN を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 *session_number* には、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* には、監視対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN を監視するには、**no monitor session** *session_number* **filter vlan** グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 での受信トラフィックを監視するように RSPAN セッション 2 を設定し、VLAN 2 ～ 5 および VLAN 9 のトラフィックだけを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 2 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

SPAN および RSPAN ステータスの表示

現在の SPAN または RSPAN 設定を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。**show running-config** 特権 EXEC コマンドを使用すれば、設定された SPAN セッションまたは RSPAN セッションを表示することもできます。

CHAPTER 28

RMON の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに Remote Monitoring（RMON）を設定する方法について説明します。

RMON は、RMON 準拠コンソール システムおよびネットワーク プローブ間で交換可能な一連の統計および機能を定義する標準モニタリング仕様です。RMON により、ネットワーク障害診断、プランニング、およびパフォーマンス調整情報に関する総合的な機能を使用できます。

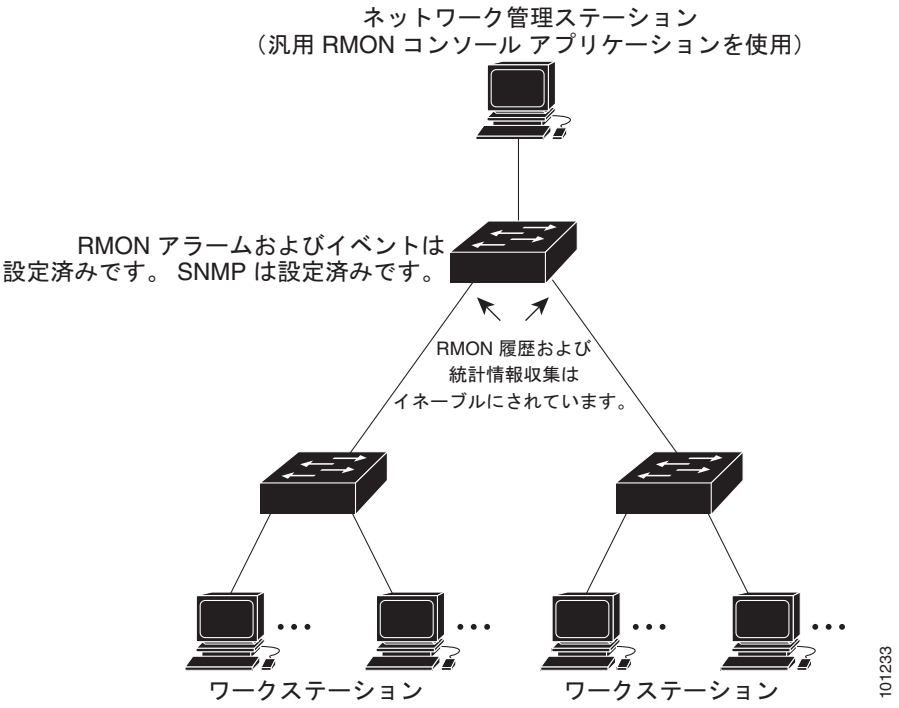
（注） この章で説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* の「System Management Commands」を参照してください。

- 「RMON の概要」（P.28-1）
- 「RMON の設定」（P.28-2）
- 「RMON ステータスの表示」（P.28-6）

RMON の概要

RMON は、Internet Engineering Task Force（IETF）標準モニタ仕様で、各種ネットワーク エージェントおよびコンソール システムがネットワーク モニタ データを交換できるようにします。RMON 機能をスイッチの SNMP（簡易ネットワーク管理プロトコル）エージェントとともに使用すると、接続された LAN セグメント上のスイッチ間を流れるすべてのトラフィックをモニタできます（図 28-1 を参照）。

図 28-1　RMON の例



スイッチは次の RMON グループをサポートします（RFC 1757 で定義）。

- 統計情報（RMON グループ 1）：イーサネット統計情報（スイッチ タイプおよびサポートされるインターフェイスに応じて、ファスト イーサネットおよびギガビット イーサネット統計情報など）を収集します。
- 履歴（RMON グループ 2）：イーサネット ポートに関する統計情報の履歴グループ（スイッチ タイプおよびサポートされるインターフェイスに応じて、ファスト イーサネットおよびギガビット イーサネット統計情報など）を指定されたポーリング インターバルで収集します。
- アラーム（RMON グループ 3）：指定されたインターバルの間、特定の MIB（管理情報ベース）オブジェクトをモニタし、指定された値（上限しきい値）でアラームをトリガーし、別の値（下限しきい値）でアラームをリセットします。アラームはイベントでも使用できます。アラームでイベントをトリガーすることで、ログ エントリや SNMP トラップを生成できます。
- イベント（RMON グループ 9）：アラームによってイベントがトリガーされた場合の処置を指定します。この処置により、ログ エントリや SNMP トラップを生成できます。

このソフトウェア リリースでサポートされているスイッチは RMON データ処理用にハードウェア カウンタを使用しているので、モニタがより効率的になり、ほとんど処理能力を必要としません。

（注）　64-bit カウンタは、RMON アラームではサポートされていません。

RMON の設定

- 「RMON のデフォルト設定」（P.28-3）
- 「RMON アラームおよびイベントの設定」（P.28-3）（必須）

- 「インターフェイスでのグループ履歴統計情報の収集」（P.28-5）（任意）
- 「インターフェイスでのグループ イーサネット統計情報の収集」（P.28-5）（任意）

RMON のデフォルト設定

RMON はデフォルトでディセーブルに設定されています。アラームやイベントは設定されていません。

RMON アラームおよびイベントの設定

CLI（コマンドライン インターフェイス）または SNMP 互換 Network Management Station（NMS; ネットワーク管理ステーション）を使用することにより、スイッチを RMON 対応に設定できます。NMS 上で汎用 RMON コンソール アプリケーションを使用し、RMON のネットワーク管理機能を利用してください。また、RMON MIB オブジェクトにアクセスするようにスイッチの SNMP を設定する必要があります。詳細については、第 30 章「SNMP の設定」を参照してください。

（注）　64-bit カウンタは、RMON アラームではサポートされていません。

RMON アラームおよびイベントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rmon alarm** *number variable interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]	MIB オブジェクトに対してアラームを設定します。 • *number* には、アラーム番号を指定します。指定できる範囲は 1 ～ 65535 です。 • *variable* には、モニタする MIB オブジェクトを指定します。 • *interval* には、MIB 変数をアラームがモニタする時間を秒単位で指定します。指定できる範囲は 1 ～ 4294967295 秒です。 • 各 MIB 変数を直接テストする場合は、キーワード **absolute** を指定します。MIB 変数のサンプル間の変動をテストする場合は、キーワード **delta** を指定します。 • *value* には、アラームをトリガーする数値とアラームをリセットする数値を指定します。上限しきい値および下限しきい値の範囲は、-2147483648 ～ 2147483647 です。 • （任意）*event-number* には、上限または下限しきい値の限度を超過したときにトリガーされるイベント番号を指定します。 • （任意）**owner** *string* には、アラームの所有者を指定します。

	コマンド	目的
ステップ 3	**rmon event** *number* [**description** *string*] [**log**] [**owner** *string*] [**trap** *community*]	RMON イベント テーブルに RMON イベント番号に対応付けられたイベントを追加します。 • *number* には、イベント番号を指定します。指定できる範囲は 1 ～ 65535 です。 • （任意）**description** *string* には、イベントの説明を指定します。 • （任意）イベントがトリガーされたときに RMON ログ エントリを生成するには、キーワード **log** を使用します。 • （任意）**owner** *string* には、このイベントの所有者を指定します。 • （任意）**trap** *community* には、このトラップに使用される SNMP コミュニティ ストリングを入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アラームをディセーブルにするには、設定したアラームごとに **no rmon alarm** *number* グローバル コンフィギュレーション コマンドを実行します。設定したアラームを一度にすべてディセーブルにはできません。イベントをディセーブルにするには、**no rmon event** *number* グローバル コンフィギュレーション コマンドを使用します。アラームおよびイベントとその相互作用の詳細については、RFC 1757 を参照してください。

MIB オブジェクトに対してアラームを設定できます。次に、**rmon alarm** コマンドを使用して RMON アラーム番号 10 を設定する例を示します。このアラームは、アラームがディセーブルになるまで、MIB 変数 *ifEntry.20.1* を 20 秒ごとに 1 回モニタし、変数の上昇または下降の変化をチェックします。*ifEntry.20.1* 値が 15 以上の MIB カウンタの増加を示した場合（たとえば 100000 から 100015）、アラームがトリガーされます。アラームは次にイベント番号 1 をトリガーします。イベントの設定には、**rmon event** コマンドを使用します。設定可能なイベントはログ エントリまたは SNMP トラップです。*ifEntry.20.1* 値の変化が 0 ずつの場合、アラームはリセットされ、再度トリガーできます。

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0 owner jjohnson
```

次に、**rmon event** コマンドを使用して RMON イベント番号 1 を作成する例を示します。イベントは *High ifOutErrors* として定義され、アラームによってイベントがトリガーされるときにログ エントリが生成されます。ユーザ *jjones* は、このコマンドによってイベント テーブルに作成された行を所有します。この例でも、イベントがトリガーされたときに SNMP トラップが生成されます。

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones
```

インターフェイスでのグループ履歴統計情報の収集

最初に RMON アラームおよびイベントを設定し、収集情報を表示する必要があります。

インターフェイス上でグループ履歴統計情報を収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	履歴を収集するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 4	**rmon collection history** *index* [**buckets** *bucket-number*] [**interval** *seconds*] [**owner** *ownername*]	指定されたバケット数および時間に関して履歴収集をイネーブルにします。 • *index* には、統計情報を収集する RMON グループを指定します。指定できる範囲は 1 ～ 65535 です。 • （任意）**buckets** *bucket-number* には、統計情報の RMON 収集履歴グループに関して、希望の最大バケット数を指定します。指定できる範囲は 1 ～ 65535 です。デフォルトは 50 です。 • （任意）**interval** *seconds* には、各ポーリング サイクルの秒数を指定します。指定できる範囲は 1 ～ 3600 です。デフォルトは 1800 秒です。 • （任意）**owner** *ownername* には、統計情報の RMON グループの所有者名を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**show rmon history**	スイッチ履歴テーブルの内容を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

履歴収集をディセーブルにするには、**no rmon collection history** *index* インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスでのグループ イーサネット統計情報の収集

インターフェイスでグループ イーサネット統計情報を収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	統計情報を収集するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**rmon collection stats** *index* [**owner** *ownername*]	インターフェイスでの RMON 統計情報収集をイネーブルにします。 • *index* には、統計情報の RMON グループを指定します。指定できる範囲は 1 ～ 65535 です。 • （任意）**owner** *ownername* には、統計情報の RMON グループの所有者名を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**show rmon statistics**	スイッチ統計情報テーブルの内容を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

グループ イーサネット統計情報の収集をディセーブルにするには、**no rmon collection stats** *index* インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、所有者 *root* の RMON 統計情報を収集する方法を示します。

```
Switch(config)# interface fastethernet0/1
Switch(config)# no shutdown
Switch(config-if)# rmon collection stats 2 owner root
```

RMON ステータスの表示

RMON ステータスを表示するには、表 28-1 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 28-1　RMON ステータスを表示するためのコマンド

コマンド	目的
show rmon	一般の RMON 統計情報を表示します。
show rmon alarms	RMON アラーム テーブルを表示します。
show rmon events	RMON イベント テーブルを表示します。
show rmon history	RMON 履歴テーブルを表示します。
show rmon statistics	RMON 統計情報テーブルを表示します。

これらの表示のフィールドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* の「System Management Commands」を参照してください。

CHAPTER 29

システム メッセージ ロギングの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにシステム メッセージ ロギングを設定する方法について説明します。

（注） この章で説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* を参照してください。

この章で説明する内容は、次のとおりです。

- 「システム メッセージ ロギングの概要」（P.29-1）
- 「システム メッセージ ロギングの設定」（P.29-2）
- 「ロギング設定の表示」（P.29-13）

注意 高い頻度でメッセージをコンソールにロギングすることにより、CPU 使用率が高くなり、スイッチの動作に悪影響を与える可能性があります。

システム メッセージ ロギングの概要

デフォルトでは、システム メッセージおよび **debug** 特権 EXEC コマンドの出力はロギング プロセスに送信されます。ロギング プロセスは、ロギング バッファ、端末回線、UNIX Syslog サーバといったさまざまな宛先へのロギング メッセージの配信を、設定に応じて制御します。ロギング プロセスはコンソールにもメッセージを送信します。

（注） Syslog フォーマットは、4.3 BSD UNIX と互換性があります。

ロギング プロセスがディセーブルになっている場合、メッセージはコンソールにだけ送信されます。メッセージは生成された時点で送信されるので、メッセージとデバッグ出力には、プロンプトまたは他のコマンドからの出力が各所に挿入されます。メッセージがコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定し、コンソールに表示されるメッセージのタイプとそれぞれの宛先を制御できます。ログ メッセージにタイムスタンプを設定したり、Syslog 送信元アドレスを設定して、リアルタイムでのデバッグおよび管理を強化できます。表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

ロギングされたシステム メッセージにアクセスするには、スイッチの CLI（コマンドライン インターフェイス）を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチ ソフトウェアは Syslog メッセージを内部バッファに保存します。

システム メッセージをリモートでモニタするには、Syslog サーバ上でログを表示するか、または Telnet あるいはコンソール ポートを通じてスイッチにアクセスします。

システム メッセージ ロギングの設定

- 「システム ログ メッセージ形式」（P.29-2）
- 「システム メッセージ ロギングのデフォルト設定」（P.29-3）
- 「メッセージ ロギングのディセーブル化」（P.29-4）（任意）
- 「メッセージ出力先デバイスの設定」（P.29-5）（任意）
- 「ログ メッセージの同期化」（P.29-6）（任意）
- 「ログ メッセージのタイムスタンプのイネーブル化およびディセーブル化」（P.29-7）（任意）
- 「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」（P.29-8）（任意）
- 「メッセージの重大度の定義」（P.29-8）（任意）
- 「履歴テーブルおよび SNMP に送信される Syslog メッセージの制限」（P.29-10）（任意）
- 「設定変更ロギングのイネーブル化」（P.29-10）（任意）
- 「UNIX Syslog サーバの設定」（P.29-11）（任意）

システム ログ メッセージ形式

システム ログ メッセージには、最大 80 文字とパーセント記号（%）が使用され、そのあとにオプションのシーケンス番号とタイムスタンプ情報（設定されている場合）が続きます。メッセージは次のフォーマットで表示されます。

seq no:timestamp: %facility-severity-MNEMONIC:description

メッセージのパーセント記号よりも前の部分は、**service sequence-numbers**、**service timestamps log datetime**、**service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]、または **service timestamps log uptime** グローバル コンフィギュレーション コマンドの設定に応じて異なります。

表 29-1 に、Syslog メッセージの要素を示します。

表 29-1　システム ログ メッセージ要素

要素	説明
seq no（シーケンス番号）:	**service sequence-numbers** グローバル コンフィギュレーション コマンドが設定されている場合に限り、シーケンス番号を付けてログ メッセージにスタンプを押します。 詳細については、「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」（P.29-8）を参照してください。
timestamp（タイムスタンプ）形式： *mm/dd hh:mm:ss* または *hh:mm:ss*（稼動時間が短い場合） または *d h*（稼動時間が長い場合）	メッセージまたはイベントの日時。この情報が表示されるのは、**service timestamps log [datetime | log]** グローバル コンフィギュレーション コマンドが設定されている場合に限られます。 詳細については、「ログ メッセージのタイムスタンプのイネーブル化およびディセーブル化」（P.29-7）を参照してください。
facility（ファシリティ）	メッセージが参照するファシリティ（SNMP、SYS など）を示します。サポートされているファシリティのリストについては、表 29-4（P.29-13）を参照してください。
severity（重大度）	メッセージの重大度を示す 0 ～ 7 の 1 桁のコード。重大度については、表 29-3（P.29-9）を参照してください。
MNEMONIC（ニーモニック）	一意にメッセージを記述する文字列。
description	レポート対象のイベントに関する詳細情報を含む文字列。

次に、スイッチ システム メッセージの一部の例を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

システム メッセージ ロギングのデフォルト設定

表 29-2 に、システム メッセージ ロギングのデフォルト設定を示します。

表 29-2　システム メッセージ ロギングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル。
コンソール重大度	Debugging（および数値的に下位のレベル。表 29-3（P.29-9）を参照）
ロギング ファイル設定	ファイル名の指定なし。
ロギング バッファ サイズ	4096 バイト。

表 29-2　システム メッセージ ロギングのデフォルト設定 （続き）

機能	デフォルト設定
ロギング履歴サイズ	1 メッセージ。
タイムスタンプ	ディセーブル。
同期ロギング	ディセーブル。
ロギング サーバ	ディセーブル。
Syslog サーバ IP アドレス	設定なし。
サーバ ファシリティ	Local7（表 29-4（P.29-13）を参照）
サーバ重大度	informational（および数値的に下位のレベル。表 29-3（P.29-9）を参照）

メッセージ ロギングのディセーブル化

メッセージ ロギングは、デフォルトでイネーブルに設定されています。コンソール以外の宛先へメッセージを送信するには、メッセージ ロギングをイネーブルに設定する必要があります。イネーブルに設定されている場合、ログ メッセージはロギング プロセスに送信され、この結果、指定された場所に、メッセージを生成したプロセスとは非同期でメッセージがロギングされます。

メッセージ ロギングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no logging console**	メッセージ ロギングをディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** または **show logging**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ロギング プロセスをディセーブルにすると、スイッチの処理速度が低下します。コンソールにメッセージが書き込まれるのを待ってからプロセスを続行するためです。ロギング プロセスがディセーブルになると、メッセージの生成後ただちにコンソールに表示されます。コマンド出力の途中に表示されることもあります。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージの表示に影響を与えます。このコマンドがイネーブルの場合は、Return キーを押さないかぎりメッセージが表示されません。詳細については、「ログ メッセージの同期化」（P.29-6）を参照してください。

ディセーブルにしたメッセージ ロギングを再度イネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

メッセージ出力先デバイスの設定

メッセージ ロギングがイネーブルになっている場合、コンソール以外の特定の場所へもメッセージを送信できます。メッセージを受信する場所を指定するには、特権 EXEC モードで、次のコマンドを 1 つまたは複数使用します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging buffered** [*size*]	スイッチの内部バッファにメッセージをロギングします。デフォルトのバッファ サイズは 4096 です。指定できる範囲は 4096 ～ 2147483647 バイトです。 スイッチに障害が発生すると、フラッシュ メモリに保存されていないログは失われます。ステップ 4 を参照してください。 **（注）** その他のタスク用メモリが不足する可能性があるので、バッファ サイズを大きく設定しないようにしてください。スイッチ上の空きプロセッサ メモリを表示するには、**show memory** 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値です。バッファ サイズを最大値に設定*しない*でください。
ステップ 3	**logging** *host*	UNIX Syslog サーバ ホストにメッセージをロギングします。 *host* には、Syslog サーバとして使用するホストの名前または IP アドレスを指定します。 ロギング メッセージを受信する Syslog サーバのリストを作成するには、複数回このコマンドを実行します。 Syslog サーバの設定手順の詳細については、「UNIX Syslog サーバの設定」（P.29-11）を参照してください。
ステップ 4	**logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]	フラッシュ メモリ内のファイルにログ メッセージを保存します。 • *filename* には、ログ メッセージのファイル名を入力します。 • （任意）*max-file-size* には、ロギング ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。デフォルトは 4096 バイトです。 • （任意）*min-file-size* には、ロギング ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。デフォルトは 2048 バイトです。 • （任意）*severity-level-number* | *type* には、ロギング重大度またはロギング タイプを指定します。指定できる 重大度の範囲は 0 ～ 7 です。ロギング タイプ キーワードのリストは、表 29-3（P.29-9）を参照してください。デフォルトでは、ログ ファイルは debugging メッセージおよび数値的に下位のレベルを受信します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**terminal monitor**	現在のセッション中に、メッセージをコンソール以外の端末にロギングします。 端末パラメータ設定コマンドはローカルに設定されていますが、セッションの終了後は無効になります。セッションごとにこのステップを実行し、デバッグ メッセージを表示する必要があります。

	コマンド	目的
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

logging buffered グローバル コンフィギュレーション コマンドは、内部バッファにロギング メッセージをコピーします。バッファは循環するので、バッファが満杯になると新しいメッセージで古いメッセージが上書きされます。バッファにロギングされているメッセージを表示するには、**show logging** 特権 EXEC コマンドを使用します。最初に表示されるのは、バッファ内で最も古いメッセージです。バッファの内容を消去するには、**clear logging** 特権 EXEC コマンドを使用します。

コンソールへのロギングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。ファイルへのロギングをディセーブルにするには、**no logging file** [*severity-level-number* | *type*] グローバル コンフィギュレーション コマンドを使用します。

ログ メッセージの同期化

非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を、送信請求デバイス出力および特定のコンソール ポート回線または仮想端末回線のプロンプトと同期させることができます。重大度に基づいて、非同期に出力するメッセージのタイプを特定したり、端末の非同期メッセージを廃棄する前に、これらを保存するバッファの最大数を設定することもできます。

非送信請求メッセージと **debug** コマンド出力の同期ロギングをイネーブルにすると、送信請求デバイス出力の表示または印刷後に、非送信請求デバイス出力がコンソールに表示または印刷されます。非送信請求メッセージと **debug** コマンド出力は、ユーザに入力を求めるプロンプトが表示されたのち、コンソールに表示されます。非送信請求メッセージと **debug** コマンド出力が、送信請求デバイス出力およびプロンプトに挿入されることはありません。非送信請求メッセージが表示されると、コンソールはユーザ プロンプトを再表示します。

同期ロギングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number* [*ending-line-number*]	メッセージの同期ロギング用に設定する回線を指定します。 • スイッチのコンソール ポートを経由して行う設定には、キーワード **console** を使用します。 • 同期ロギングをイネーブルにする vty 回線を指定するには、**line vty** *line-number* コマンドを使用します。Telnet セッションを経由して行う設定には、vty 接続を使用します。指定できる回線番号の範囲は 0 ～ 15 です。 次のように入力すると、16 の vty 回線すべての設定を同時に変更できます。 **line vty 0 15** また、現在の接続に使用している 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。 **line vty 2** このコマンドを入力すると、ライン コンフィギュレーション モードに変わります。

	コマンド	目的
ステップ 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*]	メッセージの同期ロギングをイネーブルにします。 • （任意）**level** *severity-level* には、メッセージの重大度を指定します。設定値以上の重大度を持つメッセージは、非同期で出力されます。数値が低いほど重大度が高く、数値が高いほど重大度が低くなります。デフォルト値は 2 です。 • （任意）**level all** を指定すると、重大度に関係なく、すべてのメッセージが非同期で出力されます。 • （任意）**limit** *number-of-buffers* には、新しいメッセージを廃棄する前に、端末用のキューに入れられるバッファ数を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 20 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

非送信請求メッセージおよびデバッグ出力の同期をディセーブルにするには、**no logging synchronous** [**level** *severity-level* | **all**] [**limit** *number-of-buffers*] ライン コンフィギュレーション コマンドを使用します。

ログ メッセージのタイムスタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにタイムスタンプは付加されません。

ログ メッセージのタイムスタンプをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service timestamps log uptime** または **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	ログのタイム スタンプをイネーブルにします。 最初のコマンドはログ メッセージのタイム スタンプをイネーブルにし、システムが再起動してからの時間を示します。 2 番めのコマンドは、ログ メッセージのタイム スタンプをイネーブルにします。選択したオプションに応じて、現地のタイムゾーンに基づく日付と時刻（ミリ秒）、タイムゾーン名をタイム スタンプに入れることができます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デバッグおよびログ メッセージの両方のタイム スタンプをディセーブルにするには、**no service timestamps** グローバル コンフィギュレーション コマンドを使用します。

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のロギング出力の一部の例を示します。

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のロギング出力の一部の例を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージが同じタイム スタンプを持つ可能性があるので、シーケンス番号を表示すると確実に 1 つのメッセージを参照できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

ログ メッセージのシーケンス番号をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service sequence-numbers**	シーケンス番号をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

シーケンス番号をディセーブルにするには、**no service sequence-numbers** グローバル コンフィギュレーション コマンドを使用します。

次に、シーケンス番号をイネーブルにした場合のロギング出力の一部の例を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

メッセージの重大度の定義

メッセージの重大度（表 29-3 を参照）を指定すると、選択したデバイスに表示されるメッセージを限定できます。

メッセージの重大度を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging console** *level*	コンソールにロギングされるメッセージを制限します。 デフォルトでは、コンソールは debugging メッセージおよび数値的に下位のレベルを受信します（表 29-3（P.29-9）を参照）。
ステップ 3	**logging monitor** *level*	端末回線にロギングされるメッセージを制限します。 デフォルトでは、端末は debugging メッセージおよび数値的に下位のレベルを受信します（表 29-3（P.29-9）を参照）。

	コマンド	目的
ステップ 4	**logging trap** *level*	Syslog サーバにロギングされるメッセージを制限します。 デフォルトでは、Syslog サーバは informational メッセージおよび数値的に下位のレベルを受信します（表 29-3（P.29-9）を参照）。 Syslog サーバの設定手順の詳細については、「UNIX Syslog サーバの設定」（P.29-11）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** または **show logging**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注）　*level* を指定すると、そのレベルと数値的に下位レベルのメッセージが出力先に表示されます。

コンソールへのロギングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのロギングをディセーブルにするには、**no logging monitor** グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのロギングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを使用します。

表 29-3 に、キーワード *level* について説明します。また、対応する UNIX Syslog 定義も重大度の高い順に示します。

表 29-3　メッセージ ロギングの level キーワード

level キーワード	レベル	説明	Syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	ただちに処置が必要	LOG_ALERT
critical	2	クリティカル	LOG_CRIT
errors	3	エラー	LOG_ERR
warnings	4	警告	LOG_WARNING
notifications	5	正常だが、要注意	LOG_NOTICE
informational	6	通知目的だけのメッセージ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアでは、これ以外に 4 つのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ。**warnings** から **emergencies** のレベルで表示されます。これらのメッセージは、スイッチの機能低下を示します。誤動作から回復する方法については、このリリースに対応するシステム メッセージ ガイドを参照してください。
- **debug** コマンドからの出力。**debugging** レベルで表示されます。デバッグ コマンドを使用するのは、通常 Technical Assistance Center だけです。
- インターフェイスの起動または停止の移行およびシステムの再起動メッセージ。**notifications** レベルで表示されます。このメッセージは単なる情報です。スイッチの機能に影響はありません。

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP（簡易ネットワーク管理プロトコル）ネットワーク管理ステーションに送信する Syslog メッセージのトラップをイネーブルにしている場合は、送信されるメッセージのレベルおよびスイッチの履歴テーブルに保存されるメッセージのレベルを変更できます。履歴テーブルに保存されるメッセージ数を変更することもできます。

SNMP トラップが宛先に到達する保証がないため、メッセージは履歴テーブルに保存されます。デフォルトでは、Syslog トラップがイネーブルになっていない場合でも、**warning** レベルと数値的に下位レベル（表 29-3（P.29-9）を参照）の 1 つのメッセージが、履歴テーブルに保存されます。

レベルと履歴テーブル サイズのデフォルト設定を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging history** *level*[1]	履歴ファイルに保存され、SNMP サーバに送信される Syslog メッセージのデフォルト レベルを変更します。 キーワード *level* のリストについては、表 29-3（P.29-9）を参照してください。 デフォルトでは、**warnings**、**errors**、**critical**、**alerts**、および **emergencies** メッセージが送信されます。
ステップ 3	**logging history size** *number*	履歴テーブルに保存できる Syslog メッセージの数を指定します。 デフォルトでは、1 つのメッセージが保存されます。指定できる範囲は 0 ～ 500 メッセージです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

1. キーワード level および重大度については、表 29-3 を参照してください。SNMP で使用する場合は、重大度レベルの値は 1 ずつ大きくなります。たとえば、emergencies は 0 ではなく 1、critical は 2 ではなく 3 です。

履歴テーブルが満杯のとき（**logging history size** グローバル コンフィギュレーション コマンドで指定されたメッセージ エントリの最大数を格納しているとき）は、最も古いメッセージ エントリがテーブルから削除され、新しいメッセージ エントリが保存されます。

Syslog メッセージのロギングをデフォルト レベルに戻すには、**no logging history** グローバル コンフィギュレーション コマンドを使用します。履歴テーブルのメッセージ数をデフォルト値に戻すには、**no logging history size** グローバル コンフィギュレーション コマンドを使用します。

設定変更ロギングのイネーブル化

コンフィギュレーション ロギングをイネーブルにすると、CLI（コマンドライン インターフェイス）による設定変更を追跡できます。**logging enable** 設定変更ロギング コンフィギュレーション コマンドを入力すると、セッション、ユーザ、および設定を変更するために入力されたコマンドがログに記録されます。コンフィギュレーション ログのサイズは、1 ～ 1000 エントリの範囲で設定できます（デフォルトは 100 です）。**no logging enable** コマンドを入力してロギングをディセーブルにし、**logging enable** コマンドで再びイネーブルにすることにより、いつでもログを消去できます。

すべてのコンフィギュレーション ログまたは指定されたパラメータのログを表示するには、**show archive log config** {**all** | *number* [*end-number*] | **user** *username* [**session** *number*] *number* [*end-number*] | **statistics**} [**provisioning**] 特権 EXEC コマンドを使用します。

デフォルトでは、コンフィギュレーション ロギングはディセーブルです。

コマンドの詳細については、次の URL で『*Cisco IOS Configuration Fundamentals and Network Management Command Reference*』*Release 12.3 T* を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a8086.html#wp1114989

コンフィギュレーション ロギングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	archive	アーカイブ コンフィギュレーション モードを開始します。
ステップ 3	**log config**	設定変更ロギング コンフィギュレーション モードを開始します。
ステップ 4	**logging enable**	設定変更ロギングをイネーブルにします。
ステップ 5	**logging size** *entries*	（任意）コンフィギュレーション ログに保持されるエントリ数を設定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 100 です。 **（注）** コンフィギュレーション ログが満杯になると、新しいエントリが追加されるたびに、最も古いログが削除されます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show archive log config**	コンフィギュレーション ログを表示して、設定を確認します。

次に、設定変更ロギングをイネーブルにして、ログのエントリ数を 500 に設定する例を示します。

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

次にコンフィギュレーション ログの出力例を示します。

```
Switch# show archive log config all
 idx   sess           user@line      Logged command
   38     11   unknown user@vty3     |no aaa authorization config-commands
   39     12   unknown user@vty3     |no aaa authorization network default group radius
   40     12   unknown user@vty3     |no aaa accounting dot1x default start-stop group
radius
   41     13   unknown user@vty3     |no aaa accounting system default
   42     14           temi@vty4     |interface GigabitEthernet4/0/1
   43     14           temi@vty4     | switchport mode trunk
   44     14           temi@vty4     | exit
   45     16           temi@vty5     |interface FastEthernet5/0/1
   46     16           temi@vty5     | switchport mode trunk
   47     16           temi@vty5     | exit
```

UNIX Syslog サーバの設定

次に、UNIX サーバの Syslog デーモンを設定し、UNIX システム ロギング ファシリティを定義する方法について説明します。

UNIX Syslog デーモンへのメッセージのロギング

UNIX Syslog サーバにシステム ログ メッセージを送信するには、事前に UNIX サーバで Syslog デーモンを設定する必要があります。この手順は任意です。

ルート（root）としてログインし、次の手順を実行します。

（注）　UNIX Syslog デーモンの最近のバージョンには、デフォルトでネットワークからの Syslog パケットを受信しないものがあります。使用しているシステムが該当する場合は、UNIX の **man syslogd** コマンドを使用し、リモート Syslog メッセージのロギングをイネーブルにするために Syslog コマンド ラインに追加または削除する必要のあるオプションを判別してください。

ステップ 1　ファイル /etc/syslog.conf に次のような行を追加します。

```
local7.debug /usr/adm/logs/cisco.log
```

キーワード **local7** は、使用するロギング ファシリティを指定します。ファシリティの詳細については、表 29-4（P.29-13）を参照してください。キーワード **debug** は、Syslog レベルを指定します。重大度の詳細については、表 29-3（P.29-9）を参照してください。Syslog デーモンは、重大度がこのレベル以上であるメッセージを、次のフィールドで指定されているファイルに送信します。ファイルが先に作成されていて、Syslog デーモンが書き込み権限を持っていることが必要となります。

ステップ 2　UNIX のシェル プロンプトで次のコマンドを入力し、ログファイルを作成します。

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

ステップ 3　Syslog デーモンが新しい変更を読み取っていることを確認します。

```
$ kill -HUP `cat /etc/syslog.pid`
```

詳細については、ご使用の UNIX システムの **man syslog.conf** コマンドおよび **man syslogd** コマンドを参照してください。

UNIX システム ロギング ファシリティの設定

外部のデバイスにシステム ログ メッセージを送信すると、スイッチはそのメッセージがどの UNIX Syslog ファシリティから発信されたかを識別します。

UNIX システム ファシリティのメッセージ ロギングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging** *host*	IP アドレスを入力し、UNIX Syslog サーバ ホストにメッセージをロギングします。 ロギング メッセージを受信する Syslog サーバのリストを作成するには、複数回このコマンドを実行します。

	コマンド	目的
ステップ 3	**logging trap** *level*	Syslog サーバにロギングされるメッセージを制限します。 デフォルトでは、Syslog サーバは informational メッセージおよびこれより下位のメッセージを受信します。キーワード *level* については、表 29-3（P.29-9）を参照してください。
ステップ 4	**logging facility** *facility-type*	Syslog ファシリティを設定します。キーワード *facility-type* については、表 29-4（P.29-13）を参照してください。 デフォルトは **local7** です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Syslog サーバを削除するには、**no logging** *host* グローバル コンフィギュレーション コマンドを使用し、Syslog サーバの IP アドレスを指定します。Syslog サーバへのロギングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを実行します。

表 29-4 に、ソフトウェアでサポートされている UNIX システム ファシリティを示します。このファシリティの詳細については、ご使用の UNIX オペレーティング システムのオペレータ向けマニュアルを参照してください。

表 29-4　ロギング facility-type キーワード

facility-type キーワード	説明
auth	許可システム
cron	cron ファシリティ
daemon	システム デーモン
kern	カーネル
local0 ～ 7	ローカルに定義されたメッセージ
lpr	ライン プリンタ システム
mail	メール システム
news	USENET ニュース
sys9 ～ 14	システムが使用
syslog	システム ログ
user	ユーザ プロセス
uucp	UNIX 間コピー システム

ロギング設定の表示

ロギング設定およびログ バッファの内容を表示するには、**show logging** 特権 EXEC コマンドを使用します。この出力内のフィールドについては、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* を参照してください。

CHAPTER 30

SNMP の設定

この章では、Cisco ME 3400E イーサネット アクセススイッチで SNMP（簡易ネットワーク管理プロトコル）を設定する方法について説明します。

（注）

この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスおよび『*Cisco IOS Network Management Command Reference*』*Release 12.4* を参照してください。URL は次のとおりです。
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html
MIB（管理情報ベース）一括統計情報データ収集およびプロセス MIB の設定のためのコマンドの詳細については『*Cisco IOS Commands Master List*』*Release 12.4* を参照してください。URL は次のとおりです。
http://www.cisco.com/en/US/products/ps6350/products_product_indices_list.html

- 「SNMP の概要」（P.30-1）
- 「SNMP の設定」（P.30-7）
- 「SNMP ステータスの表示」（P.30-24）

SNMP の概要

SNMP はアプリケーション レイヤ プロトコルで、マネージャとエージェント間の通信用メッセージ形式を規定します。SNMP システムは、SNMP マネージャ、SNMP エージェント、および MIB（管理情報ベース）で構成されます。SNMP マネージャは、CiscoWorks などの Network Management System（NMS; ネットワーク管理システム）の一部に組み入れることができます。エージェントおよび MIB はスイッチ上で動作します。スイッチに SNMP を設定するには、マネージャとエージェント間の関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャは、この変数の値を要求または変更できます。マネージャは、エージェントから値を取得したり、エージェントに値を保管することもできます。エージェントは、デバイス パラメータおよびネットワーク データに関する情報の保管場所である MIB からデータを収集します。また、エージェントはマネージャから要求されるデータ取得または設定に対応します。

エージェントは、非送信請求トラップをマネージャに送信します。トラップとは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップには、不正なユーザ認証、再起動、リンクのステータス（アップまたはダウン）、MAC（メディア アクセス制御）アドレス追跡、TCP 接続の切断、ネイバとの接続の切断、その他重要なイベントがあります。

スイッチは Cisco Data Collection MIB をサポートしませんが、CLI（コマンドライン インターフェイス）を使用して、選択した MIB データを特定の NMS ステーションに定期的に転送できます。このリリース以降では、Cisco Process MIB CPU しきい値テーブルの設定もできます。

ここでは、次の概要について説明します。

- 「SNMP のバージョン」（P.30-2）
- 「SNMP マネージャの機能」（P.30-3）
- 「SNMP エージェントの機能」（P.30-4）
- 「SNMP コミュニティ ストリング」（P.30-4）
- 「SNMP による MIB 変数へのアクセス」（P.30-4）
- 「SNMP 通知」（P.30-5）
- 「SNMP ifIndex MIB オブジェクト値」（P.30-6）
- 「MIB データの収集および転送」（P.30-6）

SNMP のバージョン

このソフトウェア リリースでは、次の SNMP バージョンをサポートしています。

- SNMPv1：SNMP、完全インターネット標準（RFC1157 に定義）
- SNMPv2C は、SNMPv2Classic のパーティ ベース管理およびセキュリティ フレームワークを SNMPv2C のコミュニティ ストリング ベース管理フレームワークに置き換えるもので、SNMPv2Classic の一括検索を保持しながら、エラー処理が改良されています。機能は次のとおりです。
  - SNMPv2：SNMP のバージョン 2、インターネット標準ドラフト（RFC1902 ～ 1907 に定義）
  - SNMPv2C：SNMPv2 に対応するコミュニティストリングベース管理フレームワーク、実験的インターネット プロトコル（RFC 1901 に定義）
- SNMPv3：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に定義された相互運用可能な標準ベース プロトコルです。SNMPv3 はネットワーク経由でパケットの認証および暗号化を行い、デバイスへの安全なアクセスを実現します。次のセキュリティ機能が組み込まれています。
  - メッセージ整合性：パケットが送信中に不正に変更されないようにします。
  - 認証：メッセージの送信元が有効かどうかを判別します。
  - 暗号化：パッケージの内容をスクランブルし、不正送信元に読み取られないようにします。

（注）　暗号化を選択する場合は、キーワード **priv** を指定します。このキーワードは、暗号化ソフトウェア イメージがインストールされている場合だけ使用できます。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティは、IP アドレスの Access Control List（ACL; アクセス コントロール リスト）とパスワードによって定義されています。

SNMPv2C には、一括検索メカニズムと管理ステーションへのより詳細なエラー メッセージ報告機能が組み込まれています。一括検索メカニズムは表や大量の情報を検索し、必要なラウンドトリップ数を最小限にします。SNMPv2C の改良されたエラー処理には、各種のエラー状況を区別する拡張エラー コードが組み込まれています。エラー状況は、SNMPv1 の単一のエラー コードを使用してレポートされます。SNMPv2C のエラー リターン コードが、エラー タイプをレポートします。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を備えています。セキュリティ モデルは、ユーザおよびそのユーザが所属するグループに対して設定する認証方法です。セキュリティ レベルは、1 つのセキュリティ モデルの中で許可されるセキュリティのレベルを表します。セキュリティ モデルとセキュリティ レベルの組み合せによって、SNMP パケットを処理するときに使用するセキュリティ メカニズムが決まります。使用可能なセキュリティ モデルは SNMPv1、SNMPv2C、および SNMPv3 です。

表 30-1 に、セキュリティ モデルおよびセキュリティ レベルをさまざまに組み合せた場合の特性を示します。

表 30-1　SNMP セキュリティ モデルおよびレベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	不可	認証にコミュニティ ストリングの照合を使用します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	不可	認証にコミュニティ ストリングの照合を使用します。
SNMPv3	noAuthNoPriv	ユーザ名	不可	認証にユーザ名の照合を使用します。
SNMPv3	authNoPriv	MD5（Message Digest 5）または SHA（Secure Hash Algorithm）	不可	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行います。
SNMPv3	authPriv（暗号ソフトウェア イメージが必要）	MD5 または SHA	DES（Data Encryption Standard）または AES（Advanced Encryption Standard）	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行います。 次の暗号化アルゴリズムで USM（User-based Security Model）を指定できます。 • CBC-DES（DES-56）標準に基づいて、認証に加えて DES（56 ビット）暗号化を提供します。 • 3DES 168 ビット暗号化 • AES 128 ビット、192 ビット、256 ビット暗号化

管理ステーションがサポートする SNMP のバージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、SNMPv3 のいずれかによる通信をサポートするようにソフトウェアを設定できます。

SNMP マネージャの機能

SNMP マネージャは MIB 情報を使用し、表 30-2 に示す動作を実行します。

表 30-2　SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[1]
get-bulk-request[2]	テーブルの複数行など、大きなデータブロックを取得します。小さなデータブロックを何回も送信する必要はありません。

表 30-2　SNMP の動作 （続き）

動作	説明
get-response	NMS から送られる get-request、get-next-request、および set-request に応答します。
set-request	特定の変数に値を格納します。
trap	イベントの発生時に、SNMP エージェントから SNMP マネージャに送られる、非送信請求メッセージです。

1. この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索し、必要な変数を検出します。
2. **get-bulk** コマンドが機能するのは SNMPv2 以降に限られます。

SNMP エージェントの機能

SNMP エージェントは、次のように SNMP マネージャの要求に応答します。

- MIB 変数の取得：SNMP エージェントは、NMS からの要求に応答してこの機能を開始します。エージェントは、要求された MIB 変数の値を取得し、その値で NMS に応答します。
- MIB 変数の設定：SNMP エージェントは、NMS からのメッセージに応答してこの機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

また、SNMP エージェントは非送信請求トラップ メッセージを送信し、エージェントで重要なイベントが発生したことを NMS に通知します。トラップ条件の例には、ポートまたはモジュールが起動または停止した場合、スパニングツリー トポロジの変更が発生した場合、認証障害が発生した場合などがあります。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは MIB オブジェクトへのアクセスを認証し、内蔵パスワードとして機能します。NMS がスイッチにアクセスするには、NMS 上のコミュニティ ストリングの定義が、スイッチ上の 3 つのコミュニティ ストリングの定義と 1 つまたは複数一致する必要があります。

コミュニティ ストリングは、次のいずれかのアトリビュートを持ちます。

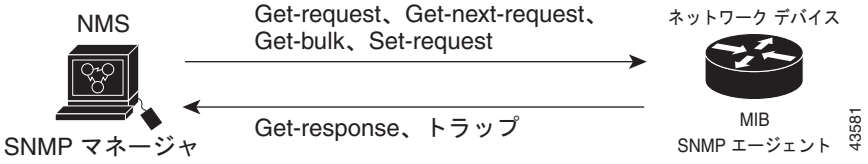
- read-only（RO）：許可した管理ステーションに、コミュニティ ストリングを除く MIB 内のオブジェクトすべてに対する読み取りアクセス権を与えます。ただし、書き込みアクセスは許可しません。
- read-write（RW）：許可した管理ステーションに、MIB 内のオブジェクトすべてに対する読み取りおよび書き込みアクセス権を与えます。ただし、コミュニティ ストリングへのアクセスは許可しません。

SNMP による MIB 変数へのアクセス

NMS の一例は、CiscoWorks ネットワーク管理ソフトウェアです。CiscoWorks 2000 ソフトウェアは、スイッチの MIB 変数を使用してデバイスの変数を設定し、ネットワーク上のデバイスに対するポーリングを実行して特定の情報を入手します。ポーリング結果は、グラフ形式で表示されます。この結果を分析して、ネットワーク間の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイスの設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 30-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対してトラップ（特定イベントの通知）を送信し、SNMP マネージャはトラップを受信してそれを処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンクステータス（アップまたはダウン）、MAC アドレス追跡などに関する条件を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送られる MIB 関連のクエリーに応答します。

図 30-1　　SNMP ネットワーク



サポートされている MIB とそのアクセス方法については、付録 A「サポートされている MIB」を参照してください。

SNMP 通知

SNMP を使用すると、スイッチは特定のイベントが発生したときに SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文内に、トラップまたはインフォームを選択するオプションが指定されていない場合、キーワード *traps* はトラップまたはインフォーム、あるいはその両方を表します。SNMP 通知をトラップまたはインフォームのどちらで送信するかを指定するには、**snmp-server host** コマンドを使用します。

（注）　SNMPv1 はインフォームをサポートしていません。

レシーバーはトラップの受信時に確認応答を送信しないため、トラップは信頼性が低く、送信側はトラップが受信されたかどうかを判別できません。SNMP マネージャはインフォーム要求を受信すると、SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）を使用してメッセージを確認します。送信側が応答を受信しない場合は、インフォーム要求を再送信します。このため、インフォームの方がトラップよりも目的の宛先に到達する可能性が高くなります。

インフォームはトラップよりも信頼性が高いため、スイッチおよびネットワーク内のリソースの消費量も多くなります。送信後すぐに廃棄されるトラップと異なり、インフォーム要求は応答を受信するか、または要求が時間切れになるまでメモリ内に保持されます。トラップの送信は 1 回限りですが、インフォームは何回も再送信されたり、再試行されることがあります。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなります。トラップおよびインフォームを使用する場合は信頼性とリソースのどちらを重視するかの選択が必要となります。SNMP マネージャですべての通知を受信することが重要な場合はインフォーム要求を使用し、ネットワーク トラフィックまたはスイッチのメモリが重要で、通知が必要ない場合は、トラップを使用します。

SNMP ifIndex MIB オブジェクト値

NMS では、IF-MIB によって interface index（ifIndex）オブジェクト値の生成および割り当てが行われます。この値は、物理または論理インターフェイスを識別する 0 より大きな一意の数です。スイッチが再起動するか、スイッチ ソフトウェアがアップグレードされても、スイッチはインターフェイスで同じ値を使用します。たとえば、スイッチがポート 2 に 10003 の ifIndex 値を割り当てる場合、この値はスイッチの再起動後も変わりません。

スイッチはインターフェイスに ifIndex 値を割り当てるときに、表 30-3 に記載されている値の 1 つを使用します。

表 30-3　ifIndex 値

インターフェイス タイプ	ifIndex 範囲
SVI[1]	1 ～ 4999
EtherChannel	5000 ～ 5012
ループバック	5013 ～ 5077
トンネル	5078 ～ 5142
物理（ギガビット イーサネットまたは SFP[2] モジュール インターフェイスなど）	10000 ～ 14500
null	14501

1. SVI = Switch Virtual Interface：スイッチ仮想インターフェイス
2. SFP = Small Form-Factor Pluggable

（注）　スイッチが範囲内の値を順番に使用するとは限りません。

MIB データの収集および転送

MIB データをデバイスから特定の NMS に定期的に転送するように設定するには、複数の MIB からのデータをリストにグループ化し、ポーリング インターバルを設定します。リスト内のすべての MIB オブジェクトは特定のインターバルでポーリングされ、データは、設定された転送インターバルで特定の NMS に転送されます。定期的なデータの収集および転送のメカニズムは、*bulk-statistics* 機能と呼ばれます。

一括統計情報を設定するには、bulk-statistics オブジェクト リストを使用して、モニタする SNMP オブジェクト タイプと、収集するオブジェクトのインスタンスを指定する bulk-statistics スキーマを指定します。一連の Object Identifier（OID; オブジェクト ID）を使用して、MIB、MIB テーブル、MIB オブジェクト、およびオブジェクト インデックスを指定できます。

- bulk-statistics オブジェクト リストは、ユーザが指定した名前により識別される同じ MIB インデックスを共有するユーザ指定の一連の MIB オブジェクトです。
- bulk-statistics スキーマは、ユーザが指定した名前により識別され、オブジェクト リストの名前、オブジェクト リスト内のオブジェクトのために取得されるインスタンス、およびポーリング インターバルが含まれています。

収集するデータを設定すると、収集されたすべてのデータにより、1 つの仮想の bulk-statistics ファイルが作成されます。ファイルを NMS（FTP、RCP、または TFTP）に転送する方法、ファイルを転送する頻度（デフォルトは 30 分）、およびセカンダリ宛先（プライマリ NMS が使用できない場合）を指定できます。転送インターバルの時間は、収集インターバルの時間でもあります。収集インターバルが

終了したあと、bulk-statistics ファイルはフリーズされ、新しいローカルの bulk-statistics ファイルが新しいデータを保存するために作成されます。フリーズしたファイルは指定された宛先に転送されたあと、削除されます（ファイルを指定した期間メモリ内に保存するようにデバイスを設定していない場合）。転送が失敗した場合に SNMP 通知を NMS に送信し、ローカル デバイスに Syslog メッセージを入力するように、スイッチを設定できます。

SNMP の設定

- 「SNMP のデフォルト設定」（P.30-7）
- 「SNMP 設定時の注意事項」（P.30-7）
- 「SNMP エージェントのディセーブル化」（P.30-8）
- 「コミュニティ ストリングの設定」（P.30-9）
- 「SNMP グループおよびユーザの設定」（P.30-10）
- 「SNMP 通知の設定」（P.30-13）
- 「エージェント コンタクトおよびロケーションの設定」（P.30-18）
- 「SNMP 経由で使用する TFTP サーバの制限」（P.30-18）
- 「MIB データ収集および転送の設定」（P.30-19）
- 「Cisco Process MIB CPU しきい値テーブルの設定」（P.30-22）
- 「MIB データ収集および転送の設定」（P.30-19）

SNMP のデフォルト設定

表 30-4　SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル[1]。
SNMP トラップ レシーバー	設定なし。
SNMP トラップ	TCP 接続のトラップ（**tty**）を除いてイネーブルなし
SNMP バージョン	**version** キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを指定しない場合、デフォルトは **noauth**（noAuthNoPriv）セキュリティ レベルです。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

1. スイッチが起動してスタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドがない場合、これがデフォルトです。

SNMP 設定時の注意事項

スイッチが起動してスイッチのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドがある場合、SNMP エージェントはイネーブルです。

SNMP *グループは*、SNMP ユーザを SNMP ビューにマッピングするテーブルです。SNMP *ユーザ*は、SNMP グループのメンバーです。SNMP *ホスト*は、SNMP トラップ動作の受信側です。SNMP *エンジン ID* は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP を設定する場合の注意事項は次のとおりです。

- SNMP グループを設定する場合は、通知ビューを指定しないでください。**snmp-server host** グローバル コンフィギュレーション コマンドを使用すると、ユーザ用の通知ビューが自動生成され、そのユーザに関連付けられたグループに追加されます。グループの通知ビューを変更すると、そのグループに関連付けられたすべてのユーザに影響を与えます。通知ビューを設定する時期については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。
- リモート ユーザを設定するには、ユーザが所属するデバイスのリモート SNMP エージェントの IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドで **remote** オプションを指定し、SNMP エンジン ID を設定してください リモート エージェントの SNMP エンジン ID およびユーザ パスワードは、認証およびプライバシ ダイジェストを計算するために使用されます。リモート エンジン ID を先に設定しないと、コンフィギュレーション コマンドは失敗します。
- SNMP インフォームを設定する場合は、SNMP データベース内のリモート エージェントの SNMP エンジン ID を設定してから、プロキシ要求またはインフォームを送信する必要があります。
- ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な悪影響を及ぼします。（コマンドラインから入力した）ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて MD5 または SHA セキュリティ ダイジェストに変換されます。コマンドライン パスワードはそのあと、RFC 2274 の要求に従って破棄されます。この破棄が原因で、エンジン ID の値が変更されると、SNMPv3 ユーザのセキュリティ ダイジェストが無効になるので、**snmp-server user** *username* グローバル コンフィギュレーション コマンドを使用して SNMP ユーザを再設定しなければなりません。同様に、エンジン ID が変更された場合は、コミュニティ ストリングを再設定する必要があります。

SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no snmp-server**	SNMP エージェントの動作をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

no snmp-server グローバル コンフィギュレーション コマンドは、デバイス上で実行されているすべてのバージョン（バージョン 1、バージョン 2C、およびバージョン 3）をディセーブルにします SNMP をイネーブルにする特定の Cisco IOS コマンドはありません。最初に入力する **snmp-server** グローバル コンフィギュレーション コマンドによって、SNMP のすべてのバージョンがイネーブルになります。

コミュニティ ストリングの設定

SNMP マネージャとエージェント間の関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングはパスワードと同様に機能し、スイッチのエージェントへのアクセスを許可します。任意で、ストリングに関連付けられた次の特性を 1 つまたは複数指定できます。

- エージェントへアクセスするコミュニティ ストリングの使用が許可されている、SNMP マネージャの IP アドレスに関するアクセス リスト
- MIB ビュー。指定のコミュニティがアクセス可能な全 MIB オブジェクトのサブセットを定義します。
- コミュニティがアクセス可能な MIB オブジェクトの読み取りおよび書き込み権限、または読み取り専用権限

スイッチ上でコミュニティ ストリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-name or number*]	コミュニティ ストリングを設定します。 **（注）** @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定するとき、@ 記号を SNMP コミュニティ ストリングの一部として使用しないでください。 • *string* には、パスワードのように機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の文字数で、1 つまたは複数のコミュニティ ストリングを設定できます。 • （任意）**view** には、コミュニティがアクセス可能なビュー レコードを指定します。 • （任意）許可した管理ステーションに MIB オブジェクトを検索させる場合は読み取り専用（**ro**）、MIB オブジェクトを検索して変更させる場合は読み取り / 書き込み（**rw**）を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトへの読み取り専用アクセスを許可します。 • （任意）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 の範囲で標準の IP アクセス リスト番号を入力します。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	（任意）ステップ 2 で標準の IP アクセス リスト番号を指定した場合は、リストを作成して必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、エージェントへアクセスするコミュニティ ストリングの使用が許可されている SNMP マネージャの IP アドレスを入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注） SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティに対するコミュニティ ストリングをヌル ストリングに設定します（コミュニティ ストリングに値を入力しない）。

特定のコミュニティ ストリングを削除するには、**no snmp-server community** *string* グローバル コンフィギュレーション コマンドを使用します。

次に、SNMP にストリング *comaccess* を割り当て、読み取り専用アクセスを許可し、IP アクセス リスト 4 がコミュニティ ストリングを使用してスイッチの SNMP エージェントにアクセスするよう指定する方法を示します。

```
Switch(config)# snmp-server community comaccess ro 4
```

SNMP グループおよびユーザの設定

スイッチ上のローカルまたはリモート SNMP サーバ エンジンに、識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする SNMP サーバ グループを設定し、SNMP グループに新規ユーザを追加できます。

スイッチ上で SNMP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}	SNMP のローカル コピーまたはリモート コピーのいずれかの名前を設定します。 • *engineid-string* は、SNMP のコピー名を含む 24 文字の ID ストリングです。後続の値がゼロの場合、エンジン ID に 24 文字すべてを指定する必要はありません。後続値がすべてゼロとなる位置まで、エンジン ID の一部を指定します。たとえば、123400000000000000000000 のエンジン ID を設定する場合は、**snmp-server engineID local 1234** と入力します。 • **remote** を選択した場合は、SNMP のリモート コピーが格納されたデバイスの *ip-address*、および任意でリモート デバイス上でデータの格納に使用する UDP ポートを指定します。デフォルトは 162 です。

	コマンド	目的
ステップ 3	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	リモート デバイスに新規の SNMP グループを設定します。 • *groupname* には、グループ名を指定します。 • セキュリティ モデルを指定します。 – **v1** は、使用可能なセキュリティ モデルのうち、安全性が最も低いモデルです。 – **v2c** は、2 番めに安全性が低いモデルです。このモデルを使用すると、インフォームおよび整数を標準の 2 倍の幅で伝送できます。 – **v3** は、最も安全性が高いモデルで、認証レベルを選択する必要があります。 **auth**：MD5 および SHA パケット認証をイネーブルにします。 **noauth**：noAuthNoPriv セキュリティ レベルをイネーブルにします。キーワードを指定しない場合は、このレベルがデフォルトです。 **priv**：Data Encryption Standard（DES; データ暗号化規格）パケット暗号化（別名 *プライバシ*）をイネーブルにします。 **（注）** キーワード **priv** は、暗号ソフトウェア イメージがインストールされている場合だけ使用できます。 • （任意）**read** *readview* には、エージェントの内容表示だけが可能なビューの名前を示すストリング（64 文字以下）を指定して、入力します。 • （任意）**write** *writeview* には、データを入力してエージェントの内容を設定するビューの名前を示すストリング（64 文字以下）を指定して、入力します。 • （任意）**notify** *notifyview* には、通知、インフォーム、またはトラップを指定するビューの名前を示すストリング（64 文字以下）を指定して、入力します。 • （任意）**access** *access-list* には、アクセス リストの名前を示すストリング（64 文字以下）を指定して、入力します。

	コマンド	目的
ステップ 4	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]} [*priv* {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]	SNMP グループの新規ユーザを追加します。 • *username* は、エージェントに接続されたホスト上のユーザ名です。 • *groupname* は、ユーザが関連付けられているグループの名前です。 • ユーザが属するリモート SNMP エンティティおよびホスト名を指定する場合は、**remote** を入力します。このエンティティの IP アドレスを指定する場合は、さらにオプションの UDP ポート番号を指定します。デフォルトは 162 です。 • SNMP バージョン番号（**v1**、**v2c**、または **v3**）を入力します。**v3** を入力する場合は、次のオプションを使用します。 – **encrypted** は、パスワードが暗号化形式で表示されるように指定します。キーワード **v3** を指定している場合だけこのキーワードが使用可能です。 – **auth** は、認証レベル設定セッションです。HMAC-MD5-96（**md5**）または HMAC-SHA-96（**sha**）認証レベルのいずれかを指定でき、パスワード ストリング *auth-password*（64 文字以下）が必要となります。 • **v3** を入力し、スイッチが暗号ソフトウェア イメージを実行している場合、プライベート（**priv**）暗号化アルゴリズムとパスワード ストリング *priv-password*（64 文字以下）も設定できます。 – **priv** は、USM（User-based Security Model）を指定します。 – **des** は、56 ビット DES アルゴリズムの使用を指定します。 – **3des** は、168 ビット DES アルゴリズムの使用を指定します。 – **aes** は、DES アルゴリズムの使用を指定します。128 ビット、192 ビット、または 256 ビット暗号化のいずれかを選択する必要があります。 • （任意）**access** *access-list* には、アクセス リストの名前を示すストリング（64 文字以下）を指定して、入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。 **（注）** **auth** | **noauth** | **priv** モード設定の SNMPv3 情報を表示するには、**show snmp user** 特権 EXEC コマンドを入力する必要があります。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生した場合に、スイッチが生成するシステム アラートです。デフォルトでトラップ マネージャは定義されていないため、トラップは送信されません。スイッチには、無制限にトラップ マネージャを設定できます。

（注）　多くのコマンドは、コマンド構文内でワード *traps* を使用します。トラップまたはインフォームを選択するオプションがコマンド内に指定されていない場合、キーワード **traps** はトラップまたはインフォーム、あるいはその両方を表します。SNMP 通知をトラップまたはインフォームのどちらで送信するかを指定するには、**snmp-server host** グローバル コンフィギュレーション コマンドを使用します。

表 30-5 に、サポートされているスイッチのトラップ（通知タイプ）を示します。これらのトラップの一部または全部をイネーブルにし、トラップ マネージャがトラップを受信するように設定できます。

表 30-5　スイッチの通知タイプ

通知タイプのキーワード	説明
bgp	Border Gateway Protocol（BGP）状態変化トラップを生成。このオプションは、メトロ IP アクセス イメージがインストールされている場合に限り使用できます。
bridge	STP ブリッジ MIB トラップを生成。
bulkstat collection transfer	データ収集またはデータ転送が失敗した場合、または bulkstats ファイルが最大サイズに達した場合にトラップを生成。
config	SNMP 設定の変更時にトラップを生成。
copy-config	SNMP コピー設定の変更時にトラップを生成。
cpu threshold	CPU しきい値超過時にトラップを生成。
entity	SNMP エンティティの変更時にトラップを生成。
envmon	環境モニタ トラップを生成。ファン、シャットダウン、ステータス、電源装置、温度の環境トラップの一部またはすべてをイネーブルにできます。
イーサネット	SNMP イーサネット トラップを生成。
flash	SNMP FLASH 通知を生成。
hsrp	Hot Standby Router Protocol（HSRP）の変更時にトラップを生成。
ipmulticast	IP マルチキャスト ルーティングの変更時にトラップを生成。
mac-notification	MAC アドレス通知のトラップを生成。
msdp	Multicast Source Discovery Protocol（MSDP）の変更時にトラップを生成。
ospf	Open Shortest Path First（OSPF）変更時にトラップを生成。シスコ固有のエラー、リンク ステート アドバタイズメント、レート リミット、再送信、状態変化のトラップの一部またはすべてをイネーブルにできます。
pim	Protocol-Independent Multicast（PIM）の変更時にトラップを生成。無効な PIM メッセージ、ネイバの変更、rendezvous point（RP; ランデブー ポイント）マッピングの変更のトラップの一部またはすべてをイネーブルにできます。
port-security	SNMP ポート セキュリティ トラップを生成。秒当たりの最大トラップ レートを設定することもできます。指定できる範囲は 0 ～ 1000 で、デフォルトは 0（レート制限なし）です。 （注）　通知タイプ **port-security** を使用してトラップを設定する場合、まずポート セキュリティ トラップを設定し、そのあとポート セキュリティ トラップ レートを設定します。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate** *rate*
rtr	SNMP Response Time Reporter（RTR）に対してトラップを生成
snmp	認証、コールド スタート、ウォーム スタート、リンク アップ、リンク ダウン時の SNMP タイプ通知のトラップを生成

表 30-5　スイッチの通知タイプ （続き）

通知タイプのキーワード	説明
storm-control	SNMP ストーム制御のトラップを生成。分当たりの最大トラップ レートを設定することもできます。指定できる範囲は 0 ～ 1000 で、デフォルトは 0 です（無制限、発生するたびにトラップを送信）。
stpx	SNMP STP 拡張 MIB トラップを生成
syslog	SNMP Syslog トラップを生成
tty	TCP 接続時にトラップを生成。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバーシップの変更時にトラップを生成
vlancreate	SNMP VLAN 作成トラップを生成
vlandelete	SNMP VLAN 削除トラップを生成

（注）　**flash insertion**、**flash removal**、**fru-ctrl**、および **vtp** の各キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。**snmp-server enable informs** グローバル コンフィギュレーション コマンドは、サポートされていません。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr* **informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

表 30-5 に示す通知タイプを受信する場合は、特定のホストに対して **snmp-server host** グローバル コンフィギュレーション コマンドを実行します。

ホストにトラップまたはインフォームを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server engineID remote** *ip-address engineid-string*	リモート ホストのエンジン ID を指定します。
ステップ 3	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]}	ステップ 2 で作成したリモート ホストに対応する SNMP ユーザを設定します。 （注）　アドレスに対してリモート ユーザを設定する場合は、最初にそのリモート ホストのエンジン ID を設定する必要があります。設定しない場合、エラー メッセージが表示され、コマンドが実行されません。
ステップ 4	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	SNMP グループを設定します。

	コマンド	目的
ステップ 5	**snmp-server host** *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [*notification-type*]	SNMP トラップ動作の受信側を指定します。 • *host-addr* には、ホスト（対象となる受信デバイス）の名前またはインターネット アドレスを指定します。 • （任意）SNMP インフォームをホストに送信する場合は、**informs** を入力します。 • （任意）SNMP トラップをホストに送信する場合は、**traps**（デフォルト）を入力します。 • （任意）SNMP **Version**（**1**、**2c**、または **3**）を指定します。SNMPv1 はインフォームをサポートしていません。 • （任意）バージョン 3 の場合は、認証レベル（**auth**、**noauth**、または **priv**）を選択します。 **（注）** キーワード **priv** は、暗号ソフトウェア イメージがインストールされている場合だけ使用できます。 • *community-string* では、**version 1** または **version 2c** を指定した場合、通知作業で送信されるパスワードと同様のコミュニティ ストリングを入力します。**version 3** を指定した場合、SNMPv3 ユーザ名を入力します。 **（注）** @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定するとき、@ 記号を SNMP コミュニティ ストリングの一部として使用しないでください。 • （任意）*notification-type* には、表 30-5（P.30-14）に示されているキーワードを使用します。タイプが指定されていない場合、すべての通知が送信されます。
ステップ 6	**snmp-server enable traps** *notification-types*	トラップまたはインフォームを送信するスイッチをイネーブルにし、送信する通知タイプを指定します。通知タイプの一覧については、表 30-5（P.30-14）を参照するか、または **snmp-server enable traps ?** を入力します。 複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。 **（注）** 通知タイプ **port-security** を使用してトラップを設定する場合、まずポート セキュリティ トラップを設定し、そのあとポート セキュリティ トラップ レートを設定します。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate** *rate*
ステップ 7	**snmp-server trap-source** *interface-id*	（任意）送信元インターフェイスを指定します。これにより、トラップ メッセージ用の IP アドレスが設定されます。このコマンドを実行すると、インフォーム用の送信元 IP アドレスも設定されます。
ステップ 8	**snmp-server queue-length** *length*	（任意）各トラップ ホストのメッセージ キュー長を設定します。指定できる値の範囲は 1 ～ 1000 です。デフォルト値は 10 です。
ステップ 9	**snmp-server trap-timeout** *seconds*	（任意）トラップ メッセージの再送信間隔を定義します。指定できる値の範囲は 1 ～ 1000 秒で、デフォルトは 30 秒です。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	**show running-config**	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

snmp-server host コマンドは、通知を受信するホストを指定します。**snmp-server enable trap** コマンドは、指定された通知（トラップまたはインフォーム用）のメカニズムをグローバルにイネーブルにします。インフォームを受信するホストをイネーブルにするには、ホストに対して **snmp-server host informs** コマンドを設定し、**snmp-server enable traps** コマンドを使用してインフォームをグローバルにイネーブルにする必要があります。

トラップを受信するように指定されたホストを削除する場合は、**no snmp-server host** *host* グローバル コンフィギュレーション コマンドを使用します。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。インフォームをディセーブルにするには、**no snmp-server host informs** グローバル コンフィギュレーション コマンドを使用します。特定のトラップ タイプをディセーブルにするには、**no snmp-server enable traps** *notification-types* グローバル コンフィギュレーション コマンドを使用します。

CPU しきい値通知のタイプと値の設定

CPU しきい値通知のタイプと値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**process cpu threshold type** {**total** | **process** | **interrupt**} **rising** *percentage* **interval** *seconds* [**falling** *fall-percentage* **interval** *seconds*]	CPU しきい値通知のタイプと値を設定します。 • **total**：通知タイプを total CPU utilization に設定します。 • **process**：通知タイプを CPU process utilization に設定します。 • **interrupt**：通知タイプを CPU interrupt utilization に設定します。 • **rising** *percentage*：CPU リソースのパーセンテージ（1 ～ 100）。設定されたインターバルを超えると、CPU しきい値通知を送信します。 • **interval** *seconds*：CPU しきい値超過の時間（単位は秒、5 ～ 86400）。条件を満たす場合、CPU しきい値通知を送信します。 • **falling** *fall-percentage*：CPU リソースのパーセンテージ（1 ～ 100）。使用度合いが設定されたインターバルのレベルを下回ったときに、CPU しきい値通知を送信します。 この値は、**rising** *percentage* 値以下でなければなりません。指定されていない場合、**falling** *fall-percentage* 値は **rising** *percentage* 値と同じです。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。 **（注）** **auth** | **noauth** | **priv** モード設定の SNMPv3 情報を表示するには、**show snmp user** 特権 EXEC コマンドを入力する必要があります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server contact** *text*	システム コンタクト ストリングを設定します。 次に例を示します。 `snmp-server contact Dial System Operator at beeper 21555.`
ステップ 3	**snmp-server location** *text*	システム ロケーション ストリングを設定します。 次に例を示します。 `snmp-server location Building 3/Room 222`
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP 経由で使用する TFTP サーバの制限

SNMP を経由してコンフィギュレーション ファイルの保存およびロードに使用する Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバを、アクセス リストに指定されたサーバに限定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server tftp-server-list** *access-list-number*	SNMP を経由してコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リスト内のサーバに限定します。 *access-list-number* には、1 ～ 99 および 1300 ～ 1999 の範囲で標準の IP アクセス リスト番号を入力します。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、スイッチへのアクセスが許可された TFTP サーバの IP アドレスを入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MIB データ収集および転送の設定

ここでは、MIB データ収集のための基本的な設定について説明します。詳細については、『*Periodic MIB Data Collection and Transfer Mechanism*』フィーチャ モジュールを参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a008014c77d.html

bulk-statistics オブジェクト リストおよびスキーマ オプションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp mib bulkstat object-list** *list-name*	SNMP bulk-statistics オブジェクト リストを定義し、bulk-statistics object-list 設定モードを開始します。
ステップ 3	**add** {*object-name* | *oid*}	bulk-statistics オブジェクト リストに MIB オブジェクトを追加します。 • *object-name* には、リストに追加する MIB オブジェクトの名前を入力します。オブジェクト名は、Interfaces MIB または Cisco Committed Access Rate MIB からだけ入力できます。 • *oid* には、リストに追加する MIB オブジェクトのオブジェクト ID を入力します。 オブジェクト リスト内のすべてのオブジェクトは同じ MIB インデックス内になければなりませんが、同じ MIB テーブルに属している必要はありません。モニタする、すべてのオブジェクトが追加されるまで、このコマンドを繰り返します。

	コマンド	目的
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**snmp mib bulkstat schema** *schema-name*	SNMP 一括統計情報スキーマに名前を付け、bulk-statistics スキーマ設定モードを開始します。
ステップ 6	**object-list** *list-name*	このスキーマに含める bulk-statistics オブジェクト リストを指定します。オブジェクト リストは、スキーマごとに 1 つだけ指定します。複数の **object-list** コマンドが入力された場合、最新のコマンドが以前のコマンドを上書きします。
ステップ 7	**instance** {**exact** | **wild**} {**interface** *interface-id* | **oid** *oid*}	このスキーマ内のオブジェクトにインスタンス情報を指定します。スキーマごとに **instance** コマンドを 1 つだけ入力します。複数の **instance** コマンドが入力された場合、最新のコマンドが以前のコマンドを上書きします。 • オブジェクト リストに付加された特定のインスタンスが完全な OID である場合、**exact** を入力します。 • 指定された OID のすべてのサブインデックスがそのスキーマに属している場合、**wild** を入力します。 • **interface** *interface-id* を入力して、インスタンス OID ではなく、インスタンス ID を指定します。 • **oid***oid* を入力して、スキーマのインスタンス OID を指定します。
ステップ 8	**poll interval** *interval*	スキーマで指定されたオブジェクト インスタンスからのデータ収集のタイム インターバルを分単位で設定します。指定できる範囲は 1 ～ 20000 分で、デフォルトは 5 分です。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、bulk-statistics オブジェクト リストおよびスキーマを設定します。

```
Switch(config)# snmp mib bulkstat object-list ifMIB
Switch(config-bulk-objects)# add 1.3.6.1.2.1.2.1.2.2.2.1.11
Switch(config-bulk-objects)# add ifName
Switch(config-bulk-objects)# exit
Switch(config)# snmp mib bulkstat schema testschema
Switch(config-bulk-sc)# object-list ifMIB
Switch(config-bulk-sc)# instance wild oil 1
Switch(config-bulk-sc)# poll-interval 1
Switch(config-bulk-sc)# exit
```

bulk-statistics 転送オプションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp mib bulkstat transfer** *transfer-id*	転送設定を名前で特定し、bulk-statistics 転送コンフィギュレーション モードを開始します。
ステップ 3	**buffer-size** *bytes*	（任意）bulk-statistics データ ファイルの最大サイズ（バイト）を指定します。指定できる範囲は 1024 ～ 2147483647 バイトで、デフォルトは 2048 バイトです。
ステップ 4	**format** {**bulkBinary** | **bulkASCII** | **schemaASCII**}	（任意）bulk-statistics データ ファイルのフォーマットを指定します。デフォルトは **schemaASCII** です。

	コマンド	目的
ステップ 5	**schema** *schema-name*	転送する bulk-statistics スキーマを指定します。必要な数のスキーマに対し、このコマンドを繰り返します。複数のスキーマを転送設定に対応付けることができます。
ステップ 6	**transfer-interval** *minutes*	（任意）転送を試みる前に、システムが MIB データを収集する時間の長さを指定します。有効な範囲は 1 ～ 2147483647 分で、デフォルトは 30 分です。転送インターバルは、収集インターバルと同じです。
ステップ 7	**url primary** *URL*	bulk-statistics ファイルを転送する先の NMS（ホスト）および転送に使用するプロトコル（FTP、RCP、または TFTP）を指定します。オプションで、**url secondary** コマンドを入力して、バックアップの転送先も指定できます。
ステップ 8	**retry** *number*	（任意）再送信の回数を指定します。指定できる範囲は 1 ～ 100 で、デフォルトは 0（再送信しない）です。
ステップ 9	**retain** *minutes*	（任意）bulk-statistics ファイルをシステム メモリに保管する時間を指定します。有効な範囲は 0 ～ 20000 分で、デフォルトは 0（転送が成功するとファイルはすぐに削除される）です。
ステップ 10	**enable**	設定のための bulk-statistics データの収集および転送プロセスを開始します。定期的な収集および転送を開始するには、このコマンドを入力する必要があります。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show mib bulk transfer**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

収集プロセスを停止するには、**no enable** 転送コンフィギュレーション コマンドを入力します。動作を再開するには、再び **enable** コマンドを入力します。**enable** コマンドでプロセスを再開するたびに、データは新しい bulk-statistics ファイルに収集されます。

次に、bulk-statistics の転送を設定し、収集プロセスをイネーブルにする例を示します。

```
Switch(config)# snmp mib bulkstat transfer testtransfer
Switch(config-bulk-tr)# format schemaASCII
Switch(config-bulk-tr)# buffer-size 2147483647
Switch(config-bulk-tr)# schema testschema1
Switch(config-bulk-tr)# schema testschema2
Switch(config-bulk-tr)# transfer-interval 1
Switch(config-bulk-tr)# url primary tftp://host/folder/bulkstat1
Switch(config-bulk-tr)# retain 20
Switch(config-bulk-tr)# retry 2
Switch(config-bulk-tr)# enable
Switch(config-bulk-tr)# exit
```

show snmp mib bulk transfer 特権 EXEC コマンドを入力し、設定された転送オプションを表示します。

Cisco Process MIB CPU しきい値テーブルの設定

CLI を使用して、Cisco Process MIB CPU しきい値テーブルを設定できます。

（注）　Cisco Process MIB CPU しきい値テーブルの設定のためのコマンドの詳細については、『*Cisco IOS Commands Master List*』*Release 12.4* を参照してください。URL は次のとおりです。
http://www.cisco.com/en/US/products/ps6350/products_product_indices_list.html

CPU しきい値テーブルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**process cpu statistics limit entry-percentage** *number* [**size** *seconds*]	プロセス エントリの制限および CPU 利用率の統計情報の履歴テーブルのサイズを設定します。 • **entry-percentage** *number* では、履歴テーブルの一部になるためにプロセスが使用しなければならない CPU 利用率（1 ～ 100%）を入力します。 • （任意）**size** *seconds* では、CPU 統計情報を履歴テーブルに保存する時間を秒単位で設定します。指定できる値の範囲は 5 ～ 86400 秒で、デフォルトは 600 秒です。
ステップ 3	**process cpu threshold type** {**total** | **process** | **interrupt**} **rising** *percentage* **interval** *seconds* [**falling** *percentage* **interval** *seconds*]	CPU しきい値通知のタイプと値を設定します。 • **threshold type** を **total** CPU utilization、CPU **process** utilization、または CPU **interrupt** utilization に設定します。 • **rising** *percentage* では、超過したときに CPU しきい値通知をトリガーする CPU リソースのパーセンテージ（1 ～ 100）を入力します。 • **interval** *seconds* では、CPU しきい値通知をトリガーするために必要な CPU しきい値超過の期間を秒単位（5 ～ 86400）で入力します。デフォルト値は 5 秒です。 • （任意）使用が設定されたインターバルのレベルを下回ったときに、CPU しきい値通知をトリガーする **falling** *percentage* **interval** *seconds* を設定します。パーセンテージは、上限パーセンテージと等しいか、またはそれ以下である必要があります。デフォルトでは、下限パーセンテージは上限パーセンテージと同じ値です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。この設定では、コミュニティストリング *public* を使用してすべてのオブジェクトに読み取り専用権限でアクセスするように SNMP マネージャを許可します。この設定により、スイッチがトラップを送信することはありません。

```
Switch(config)# snmp-server community public
```

次に、コミュニティ ストリング *public* を使用して、すべてのオブジェクトに読み取り専用権限でアクセスするように SNMP マネージャを許可する例を示します。このスイッチは、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に、それぞれ MAC 通知トラップを送信します。コミュニティ ストリング *public* がトラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps mac-notification
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、コミュニティ ストリング *comaccess* を使用するアクセス リスト 4 のメンバーに、すべてのオブジェクトへの読み取り専用アクセス権を許可する例を示します。その他の SNMP マネージャは、オブジェクトへのアクセス権がありません。コミュニティ ストリング *public* を使用し、SNMPv2C によって SNMP 認証失敗トラップがホスト *cisco.com* に送信されます。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されています。スイッチは最初の行により、すでにイネーブルになっているトラップ以外にエンティティ MIB トラップの送信もイネーブルになります。2 行めはこれらのトラップの宛先を指定し、ホスト **cisco.com** に対する以前の *snmp-server host* コマンドを無効にします。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、スイッチがコミュニティ ストリング *public* を使用し、すべてのトラップをホスト *myhost.cisco.com* に送信できるように設定する例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザがグローバル コンフィギュレーション モードを開始した際に、ユーザ名とリモート ホストを関連付けて **auth**（authNoPriv）認証レベル インフォームを送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

次の例では、SNMP 通知をイネーブルにして、定期的な MIB データ収集および転送メカニズムの転送ステータスに関する情報を提供する方法を示します（一括統計情報）。

```
Switch(config)# snmp-server enable traps bulkstat
Switch(config)# snmp-server host 192.180.1.27 informs version 2 public bulkstat
```

次の例では、SNMP 通知をイネーブルにして、Cisco Process MIB CPU しきい値テーブルに関する情報を提供する方法を示します。

```
Switch(config)# snmp-server enable traps cpu threshold
Switch(config)# snmp-server host 192.180.1.27 informs version 2 public cpu
```

SNMP ステータスの表示

不正なコミュニティ ストリング エントリ、エラー、および要求された変数を含む、SNMP 入出力の統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。また、SNMP 情報の表示には、表 30-6 に記載されているその他の特権 EXEC コマンドも使用できます。この出力内のフィールドについては、『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* を参照してください。

表 30-6　SNMP 情報を表示するためのコマンド

機能	デフォルト設定
show snmp	SNMP の統計情報を表示します。
show snmp engineID [**local** | **remote**]	デバイス上に設定されているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp mib bulk transfer	定期的な MIB データ収集および転送メカニズム（一括統計情報機能）により生成されたファイルの転送ステータスを表示します。
show snmp pending	保留中の SNMP 要求を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブル内の各 SNMP ユーザ名に関する情報を表示します。 （注）　**auth** | **noauth** | **priv** モードの SNMPv3 設定情報を表示するには、このコマンドを使用する必要があります。この情報は、**show running-config** 出力には表示されません。

CHAPTER 31

Embedded Event Manager の設定

Embedded Event Manager（EEM）は、Cisco IOS デバイス内部におけるイベント検出および回復の、分散方式およびカスタマイズ方式のアプローチです。EEM は、イベントを監視し、監視対象イベントが発生したり、何らかのしきい値に達したりしたときに、通知や、対処、またはその他の EEM アクションを実行する機能を備えています。発生時に実行するイベントおよび実行するアクションは、EEM ポリシーによって定義します。

この章では EEM の設定方法、および、EEM を使用して Cisco ME 3400E イーサネット アクセス スイッチを監視および管理する方法について説明します。この章で使用するコマンドの構文および使用方法の詳細については、このリリースのスイッチ コマンド リファレンスおよび『*Cisco IOS Network Management Command Reference*』を参照してください。EEM マニュアル セット全体については、『*Cisco IOS Network Management Configuration Guide*』に記載されているマニュアルを参照してください。

- *Embedded Event Manager の概要*
  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html
- *Cisco IOS CLI を使用した Embedded Event Manager ポリシーの作成*
  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_cli.html
- *Tcl を使用した Embedded Event Manager ポリシーの作成*
  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html

この章で説明する内容は、次のとおりです。

- 「Embedded Event Manager の概要」（P.31-1）
- 「Embedded Event Manager の設定」（P.31-6）
- 「Embedded Event Manager 情報の表示」（P.31-8）

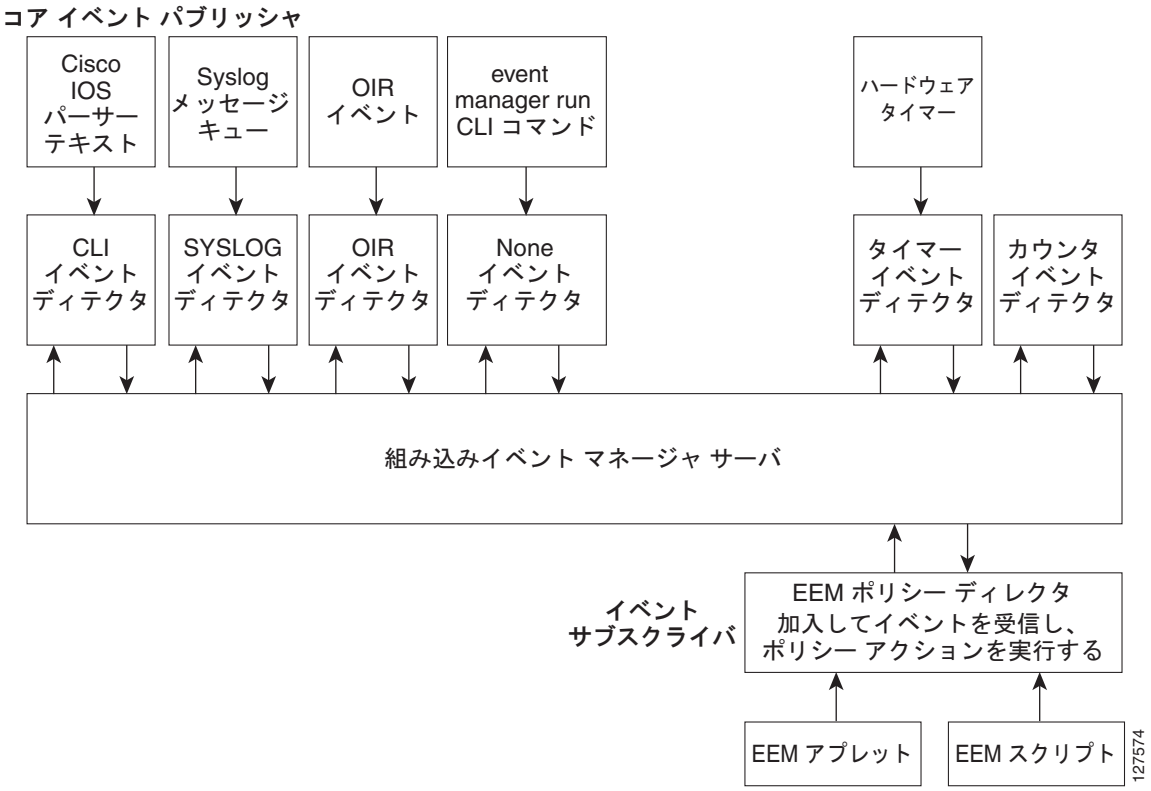
Embedded Event Manager の概要

Embedded Event Manager（EEM）では、主要なシステム イベントが監視され、次に、set ポリシーを介してそれらのイベントに対応したアクションが実行されます。このポリシーは、プログラミングされたスクリプトであり、これを使用し、指定した一連の発生イベントに基づいてアクションを起動するためのスクリプトをカスタマイズできます。このスクリプトにより、カスタム シスログや Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップの生成、CLI コマンドの起動、フェールオーバーの強制などの各種アクションが生成されます。すべてのイベント管理がスイッチ

から管理できるわけではなく、またスイッチと外部ネットワーク管理デバイス間の通信に問題がある場合もあります。これらのことから、EEM のイベント管理機能は便利です。自動回復アクションがスイッチを再起動することなく実行されれば、ネットワークのアベイラビリティは向上します。

図 31-1 に、EEM サーバ、コア イベント パブリッシャ（イベント ディテクタ）、およびイベント サブスクライバ（ポリシー）との間の関係を示します。イベント パブリッシャは、イベント サブスクライバによって提供されるイベント仕様との一致が存在するときに、イベントをスクリーニングします。イベントが発生すると、イベント ディテクタによって、EEM サーバに対して通知されます。システムの現在の状態と、特定のイベントに関してポリシー内で指定されたアクションに基づいて、EEM ポリシーによって回復が実行されます。

図 31-1　Embedded Event Manager コア イベント ディテクタ



EEM 配置の例については、『*EEM Configuration for Cisco Integrated Services Router Platforms Guide*』を参照してください。

ここでは、次の概要について説明します。

- 「イベント ディテクタ」（P.31-3）
- 「Embedded Event Manager のアクション」（P.31-4）
- 「Embedded Event Manager ポリシー」（P.31-4）
- 「Embedded Event Manager の環境変数」（P.31-5）
- 「EEM 3.2」（P.31-5）

イベント ディテクタ

イベント ディテクタと呼ばれる EEM ソフトウェア プログラムによって、EEM イベントが発生するタイミングが決定されます。各イベント ディテクタはそれぞれ別個のシステムであり、監視されるエージェント（SNMP など）と、アクションを実装できる EEM ポリシーとの間のインターフェイスとなります。

EEM では、次のイベント ディテクタが使用可能です。

- アプリケーション特有のイベント ディテクタ：あらゆる EEM ポリシーによるイベントの発行を可能にします。
- IOS CLI イベント ディテクタ：CLI を介して入力されたコマンドに基づいてポリシーを生成します。
- Generic Online Diagnostics（GOLD）イベント ディテクタ：指定したカードおよびサブカード上で GOLD 障害イベントが検出されたときにイベントを発行します。
- カウンタ イベント ディテクタ：名前付きカウンタが指定されたしきい値を超えたときにイベントを発行します。
- インターフェイス カウンタ イベント ディテクタ：指定されたインターフェイス用の汎用 Cisco IOS インターフェイス カウンタが定義されたしきい値を超えたときにイベントを発行します。しきい値は、絶対値としても増分値としても指定できます。たとえば、増分値を 50 に設定すると、インターフェイス カウンタが 50 増加するたびにイベントが発行されます。

  このディテクタでは、エントリ値および終了値の変化率に基づいたインターフェイスに関するイベントも発行されます。
- イベントディテクタなし：**event manager run** CLI コマンドによって EEM ポリシーが実行されたときにイベントを発行します。EEM は、ポリシー自体の内部のイベント仕様に基づいて、ポリシーをスケジューリングおよび実行します。**event manager run** コマンドが実行される前に、EEM ポリシーを手動で特定および登録する必要があります。
- 活性挿抜イベント ディテクタ：ハードウェアの挿入または取り外し（OIR）イベントが発生したときにイベントを発行します。
- Remote Procedure Call（RPC; リモート プロシージャ コール）イベント ディテクタ：Secure Shell（SSH; セキュア シェル）を使用した暗号化接続を介してスイッチの外部から EEM ポリシーを起動し、Simple Object Access Protocol（SOAP）データ符号化を使用して XML ベースのメッセージを交換します。また、EEM ポリシーを実行してから、SOAP XML 形式の応答内の出力を取得します。
- SNMP イベント ディタクタ：次の場合に、標準 SNMP MIB オブジェクトの監視とイベントの生成を可能にします。
  - オブジェクトが、指定した値に一致するか、指定したしきい値を超える。
  - 期間の開始時における監視対象 Object Identifier（OID; オブジェクト ID）値と、イベント発行時における実際の OID 値の違いである SNMP デルタ値が、指定値と一致する。
- SNMP 通知イベント ディテクタ：SNMP トラップ、およびスイッチによって受信される通知メッセージを代行受信します。このイベントは、着信メッセージが指定値に一致するか、定義されたしきい値を超えたときに生成されます。
- シスログ イベント ディテクタ：正規表現パターン マッチのためのシスログ メッセージのスクリーニングを可能にします。選択したメッセージをさらに限定し、特定の発生回数を指定した時間内にロギングすることを要求できます。指定したイベント基準が満たされると、設定したポリシー アクションがトリガーされます。
- タイマー イベント ディテクタ：次のイベントを発行します。

  - 指定した絶対日付時刻が発生するときに Absolute-Time-of-Day タイマーがイベントを発行します。
  - タイマーがゼロに向けてカウント ダウンするときにカウントダウン タイマーがイベントを発行します。
  - タイマーがゼロに向けてカウント ダウンするときにウォッチドッグ タイマーがイベントを発行します。タイマーそれ自体が自動的に初期値にリセットされ、カウント ダウンが再開されます。
  - イベントが発行されるタイミングが定義された UNIX 標準 CRON 仕様によって、CRON タイマーがイベントを発行します。CRON タイマーがイベントを発行するのは 1 分ごとに 1 回だけです。
- ウォッチドッグ イベント ディテクタ（IOSWDSysMon）：次のイベントのいずれかが発生するときにイベントを発行します。
  - Cisco IOS 処理の CPU 使用率がしきい値を超える。
  - Cisco IOS 処理のメモリ使用率がしきい値を超える。

  2 つのイベントを同時に監視できます。イベント発行基準は、1 つまたは両方のイベントが指定したしきい値を超えることです。

Embedded Event Manager のアクション

イベントに応じて、次のアクションが発生します。

- 名前付きカウンタの変更
- アプリケーション特有のイベントの発行
- SNMP トラップの生成
- プライオリティ付けされたシスログ メッセージの生成
- Cisco IOS ソフトウェアのリロード

Embedded Event Manager ポリシー

EEM によって、イベントを監視して情報を取得したり、監視対象のイベントが発生した、またはしきい値に達した場合に、適切な対策をとったりすることができます。EEM ポリシーは、イベントを定義し、また、そのイベントが発生したときに実行するアクションを定義するエンティティです。

EEM ポリシーには、アプレットとスクリプトの 2 種類があります。アプレットは、CLI 設定の中で定義される簡単なポリシーです。イベント スクリーニング基準、およびそのイベントが発生するときに実行するアクションを定義するための簡潔な手段です。スクリプトは、ASCII エディタを使用して、ネットワーキング デバイス上で定義します。その後、スクリプト（バイトコード（.tbc）およびテキスト（.tcl）スクリプトにすることが可能）をネットワーキング デバイスにコピーして、EEM で登録します 1 つの .tcl ファイル内に複数のイベントを登録することも可能です。

シスコによるキーワード拡張による TCL の拡張によって、EEM ポリシーの作成が容易になっています。これらのキーワードによって、検出対象イベント、後続のアクション、ユーティリティ情報、カウンタ値、およびシステム情報が識別されます。

EEM ポリシーおよびスクリプトの設定の詳細については、『*Cisco IOS Network Management Configuration Guide*』*Release 12.4T* を参照してください。

Embedded Event Manager の環境変数

EEM では、EEM ポリシー内で環境変数が使用されます。次の変数は、CLI コマンドおよび **event manager environment** コマンドを実行することによって、EEM ポリシー Tool Command Language（TCL）スクリプト内で定義します。

ユーザ定義変数

ユーザ定義ポリシー用に、ユーザが定義します。

- シスコ定義変数

  特定のサンプル ポリシー用に、シスコが定義したものです。

- シスコ組み込み変数（EEM アプレット内で使用可能）

  シスコによって定義され、読み込み専用と、読み取り / 書き込みがあります。読み取り専用変数は、アプレットが実行を開始する前に、システムによって設定されます。単一の読み取り / 書き込み変数（_exit_status）によって、同期イベントからトリガーされるポリシーの終了ステータスを設定できます。

シスコ定義環境変数およびシスコ システム定義環境変数は、ある特定のイベント ディテクタに適用することも、すべてのイベント ディテクタに適用することも可能です。ユーザ定義の、またはサンプル ポリシー内のシスコが定義した環境変数は、**event manager environment** グローバル コンフィギュレーション コマンドを使用して設定します。ポリシーを登録する前に、EEM ポリシー内で変数を定義する必要があります。

EEM でサポートされている環境変数については、『*Cisco IOS Network Management Configuration Guide*』*Release 12.4T* を参照してください。

EEM 3.2

EEM 3.2 は、Cisco IOS リリース 12.2(52)SE 以降でサポートされており、次のイベント ディテクタが導入されています。

- 近接ディスカバリ：近接ディスカバリ イベント ディテクタでは、次の場合に、自動近接検出に応答するためのポリシーを発行する機能が提供されます。
  - Cisco Discovery Protocol（CDP; シスコ検出プロトコル）キャッシュ エントリが追加、削除、または更新される。
  - Link Layer Discovery Protocol（LLDP; リンク レイヤ検出プロトコル）キャッシュ エントリが追加、削除、または更新される。
  - インターフェイス リンク ステータスが変更される。
  - インターフェイス ライン ステータスが変更される。
- ID：AAA 許可および認証が成功するとき、障害が発生するとき、または、ポート上の通常のユーザ トラフィックがフローを許可された後に、ID イベント ディテクタによって、イベントが生成されます
- MAC アドレス テーブル：MAC アドレスが MAC アドレス テーブル内で学習されるときに、MAC アドレス テーブル イベント ディテクタによってイベントが生成されます。

（注）　MAC アドレス テーブル イベント ディテクタがサポートされるのは、スイッチ プラットフォーム上だけであり、MAC アドレスが学習されるレイヤ 2 インターフェイス上でだけ使用できます。レイヤ 3 インターフェイスでは、アドレスは学習されません。また、通常の場合、ルータでは、学習された MAC アドレスを EEM に通知するために必要な MAC アドレス テーブル インフラストラクチャはサポートされません。

EEM 3.2 には、新しいイベント ディテクタで動作するアプレットをサポートするための CLI コマンドも導入されています。

EEM 3.2 機能の詳細については、Embedded Event Manager 3.2 のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_3.2.html

Embedded Event Manager の設定

- 「Embedded Event Manager アプレットの登録および定義」（P.31-6）
- 「Embedded Event Manager TCL スクリプトの登録および定義」（P.31-7）

Embedded Event Manager の設定の詳細については、『*Cisco IOS Network Management Configuration Guide*』*Release 12.4T* を参照してください。

Embedded Event Manager アプレットの登録および定義

EEM でアプレットを登録する、および、**event applet** と **action applet** コンフィギュレーション コマンドを使用して EEM アプレットを定義するには、特権 EXEC モードで、次のタスクを実行します。

（注）　1 つの EEM アプレット内で許可される event applet コマンドは 1 つだけです。action applet コマンドは複数でも許可されます。**no event** および **no action** コマンドを指定しない場合、アプレットは、コンフィギュレーション モードを終了すると削除されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**event manager applet** *applet-name*	EEM でアプレットを登録し、アプレット コンフィギュレーション モードを開始します。
ステップ 3	**event snmp oid** *oid-value* **get-type** {**exact** | **next**} **entry-op** {**gt** | **ge** | **eq** | **ne** | **lt** | **le**} **entry-val** *entry-val* [**exit-comb** {**or** |**and**}] [**exit-op** {**gt** | **ge** | **eq** | **ne** | **lt** | **le**}] [**exit-val exit-val**] [**exit-time** *exit-time-val*] **poll-interval** *poll-int-val*	EEM アプレットの実行の契機となるイベント基準を指定します。 （任意）終了基準。終了基準を指定しない場合、イベントのモニタリングがただちに再イネーブル化されます。

	コマンド	目的
ステップ 4	**action label syslog** [**priority** *priority-level*] **msg** *msg-text*	EEM アプレットがトリガーされるときのアクションを指定します。他の CLI コマンドをアプレットに追加する場合、このアクションを繰り返します。 • （任意）キーワード priority によって、Syslog メッセージのプライオリティ レベルを指定します。選択する場合、引数 priority-level を指定する必要があります。 • *msg-text* には、引数に文字テキスト、環境変数、またはその 2 つの組み合せを指定できます。
ステップ 5	**end**	アプレット コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次に、SNMP オブジェクト ID によって指定されたフィールドの 1 つが定義済みのしきい値を超えるときの EEM の出力例を示します。

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
```

次に、EEM イベントに応じて実行されるアクションの例を示します。

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current
available memory is $_snmp_oid_val bytes"

Switch (config-applet)# action 2.0 force-switchover
```

Embedded Event Manager TCL スクリプトの登録および定義

TCL スクリプトを EEM で登録し、その TCL スクリプトとポリシー コマンドを定義するには、特権 EXEC モードで次のタスクを実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 1	**show event manager environment** [**all** | *variable-name*]	（任意）**show event manager environment** コマンドを実行すると、EEM 環境変数の名前と値が表示されます。 • （任意）キーワード **all** を指定すると、EEM 環境変数が表示されます。 • （任意）引数 *variable-name* を指定すると、指定した環境変数に関する情報が表示されます。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**event manager environment variable-name string**	指定した EEM 環境変数の値を指定します。必要なすべての環境変数に関して、このステップを繰り返します。
ステップ 4	**event manager policy policy-file-name** [**type system**] [**trap**]	ポリシー内で定義されている、指定したイベントが発生するときに実行される EEM ポリシーを登録します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次に、show event manager environment コマンドのサンプル出力例を示します。

```
Switch# show event manager environment all
No.  Name                           Value
```

```
1    _cron_entry                  0-59/2 0-23/1 * * 0-6
2    _show_cmd                    show ver
3    _syslog_pattern              .*UPDOWN.*Ethernet1/0.*
4    _config_cmd1                 interface Ethernet1/0
5    _config_cmd2                 no shut
```

次に、ソフトウェアによって割り当てられた CRON タイマー 環境変数の例を示します。毎日、毎時間、2 分ごとという設定が行われています。

```
Switch (config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

```
This example shows the sample EEM policy named tm_cli_cmd.tcl registered as a system
policy. The system policies are part of the Cisco IOS image. User-defined TCL scripts must
first be copied to flash memory.
```

```
Switch (config)# event manager policy tm_cli_cmd.tcl type system
```

Embedded Event Manager 情報の表示

EEM 登録済みポリシーや EEM 履歴データなど、EEM に関する情報の表示については、『*Cisco IOS Network Management Command Reference*』を参照してください。

CHAPTER 32

ACL によるネットワーク セキュリティの設定

この章では、Access Control List（ACL; アクセス コントロール リスト）を使用して、Cisco ME 3400E イーサネット アクセス スイッチにネットワーク セキュリティを設定する方法について説明します。ACL は、コマンドやテーブルではアクセス リストとも呼びます。

（注） IP ACL に関するこの章の情報は、IP バージョン 4（IPv4）に限定されています。IPv6 ACL の設定の詳細については、第 39 章「IPv6 ACL の設定」を参照してください。

この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Addressing and Services」の章にある「Configuring IP Services」、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』*Release 12.2* を参照してください。

この章で説明する内容は、次のとおりです。

- 「ACL の概要」（P.32-1）
- 「IPv4 ACL の設定」（P.32-6）
- 「名前付き MAC 拡張 ACL の作成」（P.32-27）
- 「VLAN マップの設定」（P.32-30）
- 「ルータ ACL を VLAN マップと組み合せて使用する方法」（P.32-37）
- 「IPv4 ACL の設定の表示」（P.32-40）

ACL の概要

パケット フィルタリングを使用すると、ネットワーク トラフィックを制限したり、特定のユーザやデバイスによるネットワークの使用を制限したりできます。ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN（仮想 LAN）でパケットを許可、または拒否します。ACL は、パケットに適用される許可および拒否条件を順番に並べたものです。インターフェイスにパケットが着信すると、スイッチはパケットのフィールドを該当する ACL と比較し、ACL で指定されている条件に基づいて、パケットに対して転送が許可されているかどうかを検証します。パケットは、アクセス リスト内の条件に対して 1 つずつテストされます。最初に見つかった一致条件によって、パケットが許可されるか、または拒否されるかが決まります。スイッチは、最初の一致が見つかるとテストを終了するので、アクセス リスト内の条件の順序が重要となります。一致する条件がない場合、パケットは拒否されます。制約がない場合、スイッチはパケットを転送し、制約がある場合はパケットを廃棄します。スイッチは、転送するすべてのパケット上で ACL を使用できます。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセス リストを設定します。ACL を設定しないと、スイッチを通過するすべてのパケットが、ネットワーク内のすべての場所に転送されることがあります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、E メール トラフィックの転送を許可して、Telnet トラフィックの転送を禁止することが可能です。また、ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定できます。

ACL には Access Control Entry（ACE; アクセス コントロール エントリ）が順番に記述されています。各 ACE は、許可（*permit*）または拒否（*deny*）、および ACE と一致するためにパケットが満たす必要がある条件を指定します。*許可*または*拒否*の意味は、ACL の使用状況に応じて変わります。

スイッチは IPv4 ACL およびイーサネット（MAC [メディア アクセス制御]）ACL をサポートします。

- IP ACL は、TCP、UDP、Internet Group Management Protocol（IGMP）、Internet Control Message Protocol（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は、非 IP トラフィックをフィルタリングします。

このスイッチは、QoS（Quality of Service）分類 ACL もサポートしています。詳細については、「QoS の概要」（P.34-1）を参照してください。

ここでは、次の概要について説明します。

- 「サポートされる ACL」（P.32-2）
- 「分割されたトラフィックおよび分割されていないトラフィックの処理」（P.32-5）

サポートされる ACL

トラフィックをフィルタリングするため、次に示す 3 種類の ACL のアプリケーションがサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス制御します。発信方向のポート ACL はサポートされません。1 つのレイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックをアクセス制御し、特定の方向（着信または発信）のレイヤ 3 インターフェイスに適用されます。ルータ ACL をサポートするには、スイッチでメトロ IP アクセス イメージが稼動している必要があります。
- VLAN ACL または VLAN マップは、すべてのパケット（フォワーデッド パケットおよびルーテッド パケット）をアクセス制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップは、IPv4 のレイヤ 3 アドレスに基づいてアクセス制御するように設定されています。サポートされていないプロトコルはイーサネット ACE を使用し、MAC アドレスを通じてアクセス制御されます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケットが VLAN マップと照合されます。パケットはスイッチ ポートを経由して、ルーティングされたパケットの場合はルーテッド ポートを経由して、VLAN に入ります。

同じスイッチ上で入力ポート ACL、ルータ ACL、VLAN マップを併用できます。ただし、ポートの ACL はルータの ACL、または VLAN マップより優先されます。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。

- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド IPv4 パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信ルーテッド IPv4 パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってだけフィルタリングされます。その他のポートに着信したルーテッド IPv4 パケットは、VLAN マップおよびルータ ACL の両方によってフィルタリングされます。他のパケットには、VLAN マップのフィルタのみ適用されます。
- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってだけフィルタリングされます。発信されるルーテッド IPv4 パケットは、VLAN マップおよびルータ ACL の両方によってフィルタリングされます。他のパケットには、VLAN マップのフィルタのみ適用されます。

インターフェイスで IEEE 802.1Q トンネリングを設定している場合、トンネル ポートで受信した IEEE 802.1Q カプセル化 IPv4 パケットは、MAC ACL によってフィルタリングされますが、IPv4 ACL ではフィルタリングされません。これは、スイッチが IEEE 802.1Q ヘッダー内部のプロトコルを認識しないためです。ルータ ACL、ポート ACL、および VLAN マップに、この制限が適用されます。IEEE 802.1Q トンネリングの詳細については、第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

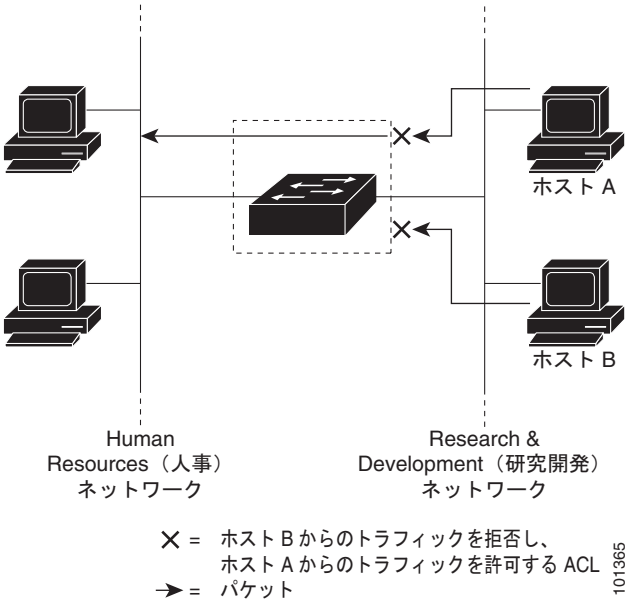
ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL は物理インターフェイスでだけサポートされ、EtherChannel インターフェイスではサポートされません。また、着信方向のインターフェイスにだけ適用されます。次のアクセス リストは、レイヤ 2 インターフェイスでサポートされます。

- 送信元アドレスを使用する標準 IP アクセス リスト
- 送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用する拡張 IP アクセス リスト
- 送信元 MAC アドレス、宛先 MAC アドレス、およびオプションのプロトコル タイプ情報を使用する MAC 拡張アクセス リスト

スイッチはインターフェイスに設定されている着信機能に関連付けられている ACL すべてをテストし、パケットが ACL 内のエントリと一致するかどうかによって、パケットの転送を許可または拒否します。このようにして、ACL はネットワーク全体、または一部のネットワークへのアクセスを制御するために使用されます。図 32-1 に、すべてのワークステーションが同じ VLAN 内にある場合に、ポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 への入力に適用されている ACL により、ホスト A は人事部ネットワークへのアクセスが許可されますが、ホスト B は拒否されます。レイヤ 2 インターフェイスで、ポート ACL を適用できるのは、着信方向に対してだけです。

図 32-1　　ACL によるネットワークへのトラフィックの制御



ポート ACL をトランク ポートに適用すると、そのトランク ポートにあるすべての VLAN で ACL によるトラフィックのフィルタリングが実行されます。

ポート ACL を使用すると、IP アクセス リストを使用して IP トラフィックをフィルタリングし、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイスに IP アクセス リストと MAC アクセス リストを両方適用すると、そのレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックをフィルタリングできます。

（注）　1 つのレイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが 1 つ設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換えられます。

ルータ ACL

スイッチでメトロ IP アクセス イメージが稼動している場合は、VLAN へのレイヤ 3 インターフェイスである SVI、物理レイヤ 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

1 つの ACL をある特定のインターフェイスの複数の機能に使用できます。また、1 つの機能に複数の ACL を使用することも可能です。1 つのルータ ACL を複数の機能で使用する場合、そのルータ ACL は複数回、照合されます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストは、送信元アドレスを使用して一致処理を行います。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチは特定のインターフェイスに設定されている機能に関連付けられている ACL をテストします。ただし、ルータ ACL は双方向でサポートされています。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてから次のホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス制御が可能です。図 32-1 では、ルータへの入力に適用されている ACL により、ホスト A は人事部ネットワークへのアクセスが許可されますが、ホスト B は拒否されます。

VLAN マップ

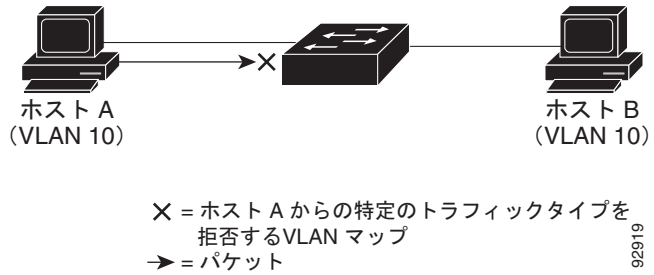
VLAN ACL または VLAN マップを使用して、すべてのトラフィックをアクセス制御できます。VLAN との間でルーティングされる、またはスイッチの VLAN 内で転送されるすべてのパケットに、VLAN マップを適用できます。VLAN マップは、セキュリティ パケットのフィルタリングに使用され、方向（入力または出力）によっては定義されません。

VLAN マップを設定すると、IPv4 トラフィックのレイヤ 3 アドレスと照合できます。

すべての非 IP プロトコルは、MAC VLAN マップを使用して MAC アドレスおよび EtherType によってアクセス制御されます（IP トラフィックには、MAC VLAN マップによるアクセス制御が*行われません*）。VLAN マップはスイッチを通過するパケットだけに適用できます。ハブのホスト間、またはこのスイッチに接続された別のスイッチのホスト間を通過するトラフィックには、VLAN マップを適用できません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。図 32-2 に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。1 つの VLAN に適用できる VLAN マップは、1 つだけです。

図 32-2　VLAN マップによるトラフィックの制御



分割されたトラフィックおよび分割されていないトラフィックの処理

ネットワークを通過する IPv4 パケットは分割できます。IPv4 パケットを分割すると、パケットの先頭を含むフラグメントにだけ、TCP、UDP ポート番号、ICMP タイプおよびコードなどのレイヤ 4 情報が格納されます。その他のすべてのフラグメントには、この情報が格納されません。

一部の ACE ではレイヤ 4 情報が確認されないため、このような ACE はすべてのパケット フラグメントに適用されます。通常の方法では、レイヤ 4 情報をテストする ACE を、分割された IPv4 パケットのほとんどのフラグメントに適用できません。レイヤ 4 情報が格納されていないフラグメントに対してレイヤ 4 情報がテストされる場合、一致規則は次のように変更されます。

- フラグメントのレイヤ 3 情報（TCP や UDP のようなプロトコル タイプなど）を確認する許可 ACE の場合は、格納されていないレイヤ 4 情報に関係なく、フラグメントが一致すると見なされます。
- レイヤ 4 情報を確認する拒否 ACE の場合は、フラグメントが一致しないと見なされます。ただし、フラグメントにレイヤ 4 情報が格納されている場合は、一致すると見なされます。

次のコマンドで設定し、3 つの分割パケットに適用される access-list 102 の例を以下に示します。

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

（注）　この例の最初および 2 番目の ACE では、宛先アドレスのあとにキーワード *eq* が指定されています。これは、TCP 宛先ポートのうち、Simple Mail Transfer Protocol（SMTP）および Telnet それぞれに対応する well-known 番号についてテストすることを示します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットが分割パケットの場合、最初のフラグメントにはすべてのレイヤ 4 情報が格納されているため、完全なパケットと同様に見なされ、最初の ACE（許可）に一致します。SMTP ポート情報が入っていなくても、残りのフラグメントも最初の ACE に一致します。最初の ACE はフラグメントに適用されたとき、レイヤ 3 情報だけを確認するためです。この例での情報は、パケットが TCP で、宛先が 10.1.1.1 です。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットが分割パケットの場合、最初のフラグメントにはレイヤ 3 情報およびレイヤ 4 情報がすべて格納されているため、2 番目の ACE（拒否）に一致します。このパケットの残りのフラグメントにはレイヤ 4 情報が格納されていないため、2 番目の ACE には一致しません。残りのフラグメントは 3 番目の ACE（許可）に一致します。

  最初のフラグメントが拒否されているため、ホスト 10.1.1.2 は完全なパケットを再構築できません。したがって、実際にはパケット B は拒否されます。ただし、ホスト 10.1.1.2 がパケットを再構築しようとするとき、許可されたフラグメントによってネットワーク帯域幅とこのホストのリソースが消費されます。
- 分割パケット C はホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットが分割パケットの場合、最初のフラグメントは 4 番目の ACE（拒否）に一致します。その他のすべてのフラグメントも 4 番目の ACE に一致します。これは、すべてのフラグメントについてレイヤ 4 情報が確認されず、レイヤ 3 情報によってすべてのフラグメントがホスト 10.1.1.3 に送信中であることが認識されたため、およびこの宛先ホストがこれ以前の許可 ACE の確認対象から外れていたためです。

IPv4 ACL の設定

スイッチに IPv4 ACL を設定する手順は、シスコ製スイッチおよびルータに IPv4 ACL を設定する場合と同じです。その手順を簡単に説明します。ACL の設定に関する詳細情報については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』*Release 12.2* を参照してください。

スイッチは、次の Cisco IOS ルータ ACL 関連機能をサポートしません。

- 非 IP プロトコルの ACL（表 32-1（P.32-8）を参照）またはブリッジグループ ACL
- IP アカウンティング
- 着信速度および発信速度の制限（QoS ACL による制限を除く）
- 再帰 ACL またはダイナミック ACL
- ポート ACL および VLAN マップに関する ACL ロギング

スイッチ上で IP ACL を使用する手順は、次のとおりです。

ステップ 1　アクセス リスト番号または名前、およびアクセス条件を指定して ACL を作成します。

ステップ 2　ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することも可能です。

ここでは、次の設定情報について説明します。

- 「標準および拡張 IPv4 ACL の作成」（P.32-7）
- 「端末回線への IPv4 ACL の適用」（P.32-18）
- 「インターフェイスへの IPv4 ACL の適用」（P.32-19）
- 「IP ACL のハードウェアおよびソフトウェア処理」（P.32-20）
- 「ACL のトラブルシューティング」（P.32-21）
- 「IPv4 ACL の設定例」（P.32-22）

標準および拡張 IPv4 ACL の作成

ここでは、IP ACL について説明します。ACL は許可および拒否条件を順に並べたものです。パケットは、ACL 内の条件に対して 1 つずつ照合されます。最初に見つかった一致条件によって、パケットが許可されるか、または拒否されるかが決まります。最初の一致が見つかると条件のテストを終了するので、条件の順序が重要となります。一致する条件がない場合、パケットは拒否されます。

ソフトウェアは次に示す ACL タイプ、または IPv4 のアクセス リストをサポートします。

- 標準 IP アクセス リストは、送信元アドレスを使用して一致処理を行います。
- 拡張 IP アクセス リストは、送信元アドレスおよび宛先アドレスを使用して一致処理を行います。より細部にわたる制御を行う場合は、オプションのプロトコルタイプを使用します。

ここでは、アクセス リストの概要および作成方法について説明します。

- 「IPv4 アクセス リスト番号」（P.32-8）
- 「ACL のロギング」（P.32-8）
- 「番号付き標準 ACL の作成」（P.32-9）
- 「番号付き拡張 ACL の作成」（P.32-10）
- 「ACL 内の ACE の並べ替え」（P.32-14）
- 「名前付きの標準および拡張 ACL の作成」（P.32-14）
- 「ACL での時間範囲の使用法」（P.32-16）
- 「ACL へのコメントの挿入」（P.32-18）

IPv4 アクセス リスト番号

IPv4 ACL を表す番号は、作成しているアクセス リストのタイプを示します。表 32-1 に、アクセス リスト番号および対応するアクセスリスト タイプ、スイッチでのアクセス リストに対するサポートの有無を示します。スイッチでは、IPv4 標準および IPv4 拡張アクセス リストがサポートされています（番号は 1 ～ 199、1300 ～ 2699）。

表 32-1　　アクセス リスト番号

アクセス リスト番号	タイプ	サポートの有無
1 ～ 99	IP 標準アクセス リスト	あり
100 ～ 199	IP 拡張アクセス リスト	あり
200 ～ 299	プロトコル タイプコード アクセス リスト	なし
300 ～ 399	DECnet アクセス リスト	なし
400 ～ 499	XNS 標準アクセス リスト	なし
500 ～ 599	XNS 拡張アクセス リスト	なし
600 ～ 699	AppleTalk アクセス リスト	なし
700 ～ 799	48 ビット MAC アドレス アクセス リスト	なし
800 ～ 899	IPX 標準アクセス リスト	なし
900 ～ 999	IPX 拡張アクセス リスト	なし
1000 ～ 1099	IPX SAP アクセス リスト	なし
1100 ～ 1199	拡張 48 ビット MAC アドレス アクセス リスト	なし
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	なし
1300 ～ 1999	IP 標準アクセス リスト（拡張範囲）	あり
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	あり

（注） 番号付きの標準 IPv4 ACL および拡張 IPv4 ACL 以外に、サポートされている番号を使用して名前付きの標準 IPv4 ACL および拡張 IPv4 ACL を作成することも可能です。つまり、標準 IP ACL の名前には 1 ～ 99 を、拡張 IP ACL の名前には 100 ～ 199 を使用できます。番号付き ACL ではなく名前付き ACL を使用することで、名前付きリストから個別にエントリを削除することが可能となります。

ACL のロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、Syslog メッセージを制御するロギング コンソール コマンドで制御されます。

（注） ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、キーワード *log* を含む*許可（permit）*または**拒否（deny）**ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	送信元アドレスおよびワイルドカードを使用し、標準 IPv4 アクセス リストを定義します。 *access-list-number* は 1 ～ 99 または 1300 ～ 1999 の 10 進数です。 条件が一致する場合にアクセスを拒否するか、許可するかを指定するため、**deny** または **permit** を入力します。 *source* はパケットの送信元であるネットワークまたはホストのアドレスです。次のいずれかで指定します。 • ドット付き 10 進表記による 32 ビットの数値 • **source** と *source-wildcard* の値 0.0.0.0 255.255.255.255 の短縮形であるキーワード *any*。送信元ワイルドカードを入力する必要はありません。 • 送信元と送信元ワイルドカードの値 **source** 0.0.0.0 の短縮形である *host* （任意）*source-wildcard* を指定すると、送信元にワイルドカード ビットが適用されます。 （任意）**log** を指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** [*number* | *name*]	アクセス リストの設定を表示します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストからは、ACE を個別に削除できません。

（注）　ACL を作成するときは、ACL の末尾に暗黙の 拒否文がデフォルトで存在し、それ以前の文で一致が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、対応する IP ホスト アドレスの ACL を指定するときにマスクを省略すると、0.0.0.0 がマスクとして使用されます。

次に、IP ホスト 171.69.198.102 へのアクセスを拒否してそれ以外のアドレスへのアクセスを許可し、その結果を表示する標準 ACL の作成例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
```

```
10 deny   171.69.198.102
20 permit any
```

host 一致条件が指定されたエントリ、および 0.0.0.0 の無視（*don't care*）マスクが指定されたエントリが、リストの先頭（ゼロ以外の無視 [*don't care*] マスクが指定されたすべてのエントリの上）に来るように、標準アクセス リストの順序が常に書き換えられます。したがって、**show** コマンドの出力およびコンフィギュレーション ファイルで、ACE は必ずしも入力した順番に表示されるとは限りません。

作成した番号付き標準 IPv4 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.32-18）を参照）、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.32-19）を参照）、または VLAN（「VLAN マップの設定」（P.32-30）を参照）に適用できます。

番号付き拡張 ACL の作成

標準 ACL の場合、一致基準には送信元アドレスだけが使用されますが、拡張 ACL の場合は、一致処理に送信元アドレスおよび宛先アドレスを使用したり、オプションのプロトコル タイプ情報を使用してより細部にわたる制御を行ったりできます。番号付き拡張 ACL を作成したあとに ACE を新たに作成するときは、リストの末尾に新しい ACE が配置されることに注意してください。リストを再び並べ替えたり、番号が指定された ACL の特定の位置で ACE を追加または削除したりはできません。

プロトコルには、専用のパラメータおよびキーワードを使用できるものもあります。

次の IP プロトコルがサポートされます（プロトコル キーワードはカッコ内の太字）。

Authentication Header Protocol（**ahp**）、Enhanced Interior Gateway Routing Protocol（**eigrp**）、Encapsulation Security Payload（**esp**）、Generic Routing Encapsulation（**gre**）、Internet Control Message Protocol（**icmp**）、Internet Group Management Protocol（**igmp**）、任意の Interior Protocol（**ip**）、IP in IP トンネリング（**ipinip**）、KA9Q NOS 互換 IP over IP トンネリング（**nos**）、Open Shortest Path First ルーティング（**ospf**）、Payload Compression Protocol（**pcp**）、Protocol Independent Multicast（**pim**）、TCP（**tcp**）、UDP（**udp**）。

（注） ICMP エコー応答はフィルタリングできません。他のすべての ICMP コードまたはタイプはフィルタリング可能です。

各プロトコルの特定のキーワードに関する詳細は、次のコマンド リファレンスを参照してください。

- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』*Release 12.2*
- 『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2*
- 『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』*Release 12.2*

（注） ダイナミック アクセス リストや再帰アクセス リストはサポートされません。また、最小コストの Type of Service（ToS; サービス タイプ）ビットに基づくフィルタリングもサポートされません。

サポートされているパラメータは、TCP、UDP、ICMP、IGMP、または他の IP の、いずれかのカテゴリにグループ分けできます。

拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2a	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *DSCP*] **（注）** **dscp** 値を入力した場合、**tos** または **precedence** は入力できません。**dscp** を入力しない場合は、tos と **precedence** を両方とも入力できます。	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* は 100 ～ 199 または 2000 ～ 2699 の 10 進数です。 **deny** または **permit** を入力して、条件が一致する場合にパケットを拒否するか許可するかを指定します。 *protocol* には、IP プロトコルの名前または番号を入力します。**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、**udp**）、または IP プロトコル番号を表す 0 ～ 255 の整数を使用できます。すべてのインターネット プロトコル（ICMP、TCP、UDP など）と一致させる場合は、キーワード **ip** を使用します。 **（注）** このステップには、ほとんどの IP プロトコルに使用可能なオプションが含まれます。TCP、UDP、ICMP、IGMP の具体的なパラメータについては、ステップ 2b ～ 2e を参照してください。 *source* はパケットの送信元であるネットワークまたはホストの番号です。 *source-wildcard* を指定すると、送信元にワイルドカード ビットが適用されます。 *destination* はパケットの宛先となるネットワークまたはホストの番号です。 *destination-wildcard* を指定すると、宛先にワイルドカード ビットが適用されます。 source、source-wildcard、destination、destination-wildcard は、次の方法で指定できます。 • ドット付き 10 進表記による 32 ビットの数値 • 0.0.0.0 255.255.255.255 を表すキーワード **any**（任意のホスト） • 単一のホスト 0.0.0.0 を表すキーワード **host** その他のキーワードは任意で、意味は次のとおりです。 • **precedence**：0 ～ 7 の番号または名前で指定された優先順位を使用し、パケットを比較します。使用できる名前および番号は、**routine**（**0**）、***priority***（**1**）、**immediate**（**2**）、**flash**（**3**）、**flash-override**（**4**）、**critical**（**5**）、**internet**（6）、**network**（**7**）です。 • **fragments**：先頭以外のフラグメントを確認します。 • **tos**：0 ～ 15 の番号または名前で指定された ToS レベルを使用して比較します。使用できる名前および番号は、**normal**（**0**）、**max-reliability**（**2**）、**max-throughput**（**4**）、**min-delay**（**8**）です。 • **log**：エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。**log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。 • **time-range**：このキーワードの説明については、「ACL での時間範囲の使用法」（P.32-16）を参照してください。 • **dscp**：0 ～ 63 の番号で指定された DSCP 値を使用してパケットを照合します。疑問符（?）を使用すると、使用可能な値のリストが表示されます。

	コマンド	目的
または	**access-list** *access-list-number* {**deny** | permit} *protocol* any any [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	アクセス リスト コンフィギュレーション モードで、送信元と送信元ワイルドカードの値 0.0.0.0 255.255.255.255 の短縮形を使用するか、または宛先と宛先ワイルドカードの値 0.0.0.0 255.255.255.255 の短縮形を使用し、拡張 IP アクセス リストを定義します。 送信元/宛先アドレスとワイルドカードの代わりに、キーワード **any** を使用できます。
または	**access-list** *access-list-number* {**deny** | **permit**} *protocol* **host** *source* **host** *destination* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [log] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	送信元と送信元ワイルドカードの値 *source* 0.0.0.0 の短縮形を使用するか、または宛先と宛先ワイルドカードの値 *destination* 0.0.0.0 の短縮形を使用し、拡張 IP アクセス リストを定義します。 送信元と宛先のワイルドカードまたはマスクの代わりに、**host** キーワードを使用できます。
ステップ 2b	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*]	（任意）拡張 TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。 次に示す例外を除き、ステップ 2a で説明するパラメータと同じパラメータを使用します。 （任意）*operator* および *port* を入力すると、送信元ポート（*source source-wildcard* のあとに入力した場合）または宛先ポート（*destination destination-wildcard* のあとに入力した場合）が比較されます。使用可能な演算子は **eq**（等しい）、**gt**（より大きい）、**lt**（より小さい）、**neq**（等しくない）、**range**（包含範囲）などです。演算子にはポート番号を指定する必要があります（**range** の場合は 2 つのポート番号をスペースで区切って指定します）。 *port* にポート番号を 10 進数（0 ～ 65,535）として入力するか、または TCP ポート名を入力します。TCP ポート名を確認するには、「?」を使用するか、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。TCP をフィルタリングするときは、TCP ポートの番号または名前だけを使用します。 その他のオプションのキーワードの意味は次のとおりです。 • **established**：確立された接続と比較します。このキーワードは、**ack** または **rst** フラグを指定した場合の一致検索機能と同じです。 • *flag*：指定された TCP ヘッダー ビットを基準にして比較します。入力できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）、**urg**（緊急）です。
ステップ 2c	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP の場合は、**udp** を入力します。 UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[*operator port*] のポート番号またはポート名は、UDP ポートの番号または名前とします。UDP の場合、**flag** および **established** の各パラメータは無効です。

	コマンド	目的
ステップ 2d	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP の場合は、**icmp** を入力します。 ICMP パラメータはステップ 2a の IP プロトコルで説明されているパラメータと同じですが、ICMP メッセージ タイプとコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプを使用してフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-code*：ICMP メッセージ コード タイプを使用してフィルタリングされた ICMP パケットをフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-message*：ICMP メッセージ タイプ名または ICMP メッセージのタイプおよびコード名を使用して、ICMP パケットをフィルタリングします。ICMP メッセージ タイプ名およびコード名を確認するには、「?」を使用するか、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「Configuring IP Services」の章を参照してください。
ステップ 2e	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。 IGMP の場合は、**igmp** を入力します。 IGMP パラメータはステップ 2a の IP プロトコルで説明されているパラメータと同じですが、次に示すパラメータが追加されています。 *igmp-type*：IGMP メッセージ タイプと比較するには、0 ～ 15 の番号またはメッセージ名（**host-query**、**host-report**、**pim**、または **trace**）を入力します。 **（注）** **dvmrp** は、コマンドライン ヘルプでは表示されますが、サポートされません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** [*number* | *name*]	アクセス リストの設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リスト全体を削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストからは、ACE を個別に削除できません。

次に、ネットワーク 171.69.198.0 内の任意のホストからネットワーク 172.20.52.0 内の任意のホストへの Telnet アクセスを拒否し、それ以外のアクセスを許可する拡張アクセス リストを作成、表示する例を示します （キーワード **eq** を宛先アドレスのあとに指定すると、Telnet に対応する TCP 宛先ポート番号がテストされます）。

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq
telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
    10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
    20 permit tcp any any
```

ACL が作成されたあとに追加された ACE（端末から入力された ACE など）は、リストの末尾に配置されます。番号が指定されたアクセス リストの特定の位置での ACE の追加または削除はできません。

（注）　ACL を作成するときは、アクセス リストの末尾に暗黙の 拒否文がデフォルトで存在し、それ以前の文で一致が見つからなかったすべてのパケットに適用されることに注意してください。

作成した番号付き拡張 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.32-18）を参照）、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.32-19）を参照）、または VLAN（「VLAN マップの設定」（P.32-30）を参照）に適用できます。

ACL 内の ACE の並べ替え

新しい ACL が作成されると、アクセス リスト内のエントリのシーケンス番号が自動的に生成されます。**ip access-list resequence** グローバル コンフィギュレーション コマンドを使用すると、ACL 内のシーケンス番号を編集したり、ACE が適用される順番を変更したりできます。たとえば、新しい ACE を ACL に追加する場合、リストの最後に配置されます。シーケンス番号を変更すると、その ACE を ACL 内の別の場所に移動できます。

ip access-list resequence コマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsaclseq.htm

名前付きの標準および拡張 ACL の作成

IPv4 ACL は、番号でなく英数字（名前）で指定することも可能です。名前付き ACL を使用すると、番号付きアクセス リストの場合より多くの IPv4 アクセス リストをルータに設定できます。アクセス リストを番号でなく名前で指定する場合は、モードおよびコマンド構文が若干異なります。ただし、IP アクセス リストを使用するすべてのコマンドで、名前付きアクセス リストを使用できるわけではありません。

（注）　標準または拡張 ACL に指定する名前には、サポートされているアクセス リスト番号範囲内の番号を指定することも可能です。つまり、標準 IP ACL の名前には 1 ～ 99 を、拡張 IP ACL の名前には 100 ～ 199 を使用できます。番号付き ACL ではなく名前付き ACL を使用することで、名前付きリストから個別にエントリを削除することが可能となります。

名前付き ACL を設定する前に、次に示す注意事項および制限事項を考慮してください。

- 番号付き ACL を指定できるすべてのコマンドで、名前付き ACL を指定できるとは限りません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL には名前を使用できます。VLAN マップには名前を使用できます。
- 標準 ACL および拡張 ACL には、同じ名前を設定できません。
- 番号付き ACL も使用できます（「標準および拡張 IPv4 ACL の作成」（P.32-7）を参照）。
- VLAN マップには、標準 ACL および拡張 ACL（名前付きまたは番号付き）を使用できます。

名前付き標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list standard** *name*	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 **（注）**　名前は 1 ～ 99 の番号にできます。
ステップ 3	**deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**] または **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]	アクセス リスト コンフィギュレーション モードで、1 つまたは複数の条件を拒否または許可に指定し、パケットの転送または廃棄を決定します。 • **host** *source*：送信元と送信元ワイルドカードの値 *source* 0.0.0.0 • **any**：送信元と送信元ワイルドカードの値 0.0.0.0 255.255.255.255
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

名前付き標準 ACL を削除するには、**no ip access-list standard** *name* グローバル コンフィギュレーション コマンドを使用します。

名前を使用して拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list extended** *name*	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 **（注）**　名前は 100 ～ 199 の番号にできます。
ステップ 3	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**] [**time-range** *time-range-name*]	アクセスリスト コンフィギュレーション モードで、許可または拒否の条件を指定します。キーワード **log** を使用すると、違反を含むアクセス リストのログ メッセージを取得できます。 プロトコルおよびその他のキーワードの定義については、「番号付き拡張 ACL の作成」（P.32-10）を参照してください。 • **host** *source*：送信元と送信元ワイルドカードの値 *source* 0.0.0.0 • ***host destination***：宛先と宛先ワイルドカードの値 *destination* 0.0.0.0 • **any**：送信元と送信元ワイルドカードの値、または宛先と宛先ワイルドカードの値である 0.0.0.0 255.255.255.255
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

名前付き拡張 ACL を削除するには、**no ip access-list extended** *name* グローバル コンフィギュレーション コマンドを使用します。

標準または拡張 ACL を作成するときは、ACL の末尾に暗黙の 拒否文がデフォルトで存在し、それ以前の文で一致が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、対応する IP ホスト アドレスのアクセス リストを指定するときにマスクを省略すると、0.0.0.0 がマスクとして使用されます。

ACL を作成したあとに追加された ACE は、リストの末尾に配置されます。特定の ACL に対して、個別に ACE エントリを追加できません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。

次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

番号付き ACL ではなく、名前付き ACL を使用することで、名前付き ACL から行を個別に削除することが可能となります。

作成した名前付き ACL はインターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.32-19）を参照）または VLAN（「VLAN マップの設定」（P.32-30）を参照）に適用できます。

ACL での時間範囲の使用法

曜日および時刻に基づいて拡張 ACL を選択的に適用するには、**time-range** グローバル コンフィギュレーション コマンドを使用します。最初に時間範囲の名前を定義し、時間範囲の時刻、日付、または曜日を設定します。次に、ACL を適用するときに時間範囲名を入力し、アクセス リストに制限を適用します。時間範囲を使用することで、ACL の許可文または拒否文が有効な時間（指定期間内、指定曜日など）を定義できます。**time-range** キーワードおよび引数については、前述の「標準および拡張 IPv4 ACL の作成」（P.32-7）および「名前付きの標準および拡張 ACL の作成」（P.32-14）に記載されている、名前付きおよび番号付き拡張 ACL のタスク表を参照してください。

時間範囲を使用する利点の一部を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザ アクセスをより厳密に許可または拒否できます。
- ログ メッセージを制御できます。ACL エントリを使用して特定の時刻に関してだけトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新規設定を他の機能や、Ternary CAM（TCAM）にロードされた結合済みの設定と統合する必要があるためです。このため、複数のアクセス リストが短期間に連続して（互いに数分以内に）有効となるような設定を行わないように、注意する必要があります。

（注） 時間範囲には、スイッチのシステム クロックが使用されるため、信頼できるクロック ソースが必要です。スイッチ クロックを同期するには、Network Time Protocol（NTP）を使用することを推奨します。詳細については、「システム日時の管理」（P.5-1）を参照してください。

ACL の time-range パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**time-range** *time-range-name*	作成する時間範囲には意味のある名前（*workhours* など）を割り当て、時間範囲コンフィギュレーション モードを開始します。名前の先頭には文字を指定し、途中にスペースまたは引用符を含めないようにします。

	コマンド	目的
ステップ 3	**absolute** [**start** *time date*] [**end** *time date*] または **periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm* または **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*	時間範囲を適用する機能が作動する時間を指定します。 • 時間範囲内では、**absolute** 文を 1 回に限り使用できます。複数の absolute 文を設定した場合は、最後に設定された文だけが実行されます。 • 複数の **periodic** 文を入力できます。たとえば、平日と週末で異なる時間を設定できます。 設定例を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show time-range**	設定した時間範囲を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

複数の項目を異なる時刻に有効としたい場合、このステップを繰り返します。設定された時間範囲の制限を削除するには、**no time-range** *time-range-name* グローバル コンフィギュレーション コマンドを使用します。

次に、営業時間（*workhours*）の時間範囲を設定し、会社の休業日を 2006 年 1 月 1 日に設定して、その設定を確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に、時間範囲名を入力します。次に、定義された休日中に任意の送信元から任意の宛先に送信される TCP トラフィックを拒否し、営業時間中にすべての TCP トラフィックを許可する拡張アクセス リスト 188 を作成、確認する例を示します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して、同じトラフィックを許可および拒否する例を示します。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

ACL へのコメントの挿入

キーワード **remark** を使用すると、エントリに関するコメント（備考）を任意の IP 標準および拡張 ACL に追加できます。コメントを追加すると、ACL の把握および走査がより簡単になります。各コメント行には、100 文字まで入力できます。

コメントは許可文または拒否文の前後に指定できます。コメントに対応する許可文または拒否文が明確になるように、コメントの記述位置を統一する必要があります。混乱を避けるため、たとえば、許可文または拒否文の前に記述されているコメントと、文のあとに記述されているコメントが混在しないようにします。

番号付きの IP 標準または拡張 ACL にコメントを挿入するには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、上記のコマンドの **no** 形式を使用します。

次の例では、Jones が所有するワークステーションのアクセスは許可されていますが、Smith が所有するワークステーションのアクセスは禁止されています。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL にエントリする場合は、**remark** アクセス リスト コンフィギュレーション コマンドを使用します。コメントを削除するには、上記のコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットは発信 Telnet の使用が禁止されています。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

端末回線への IPv4 ACL の適用

番号付き ACL を使用すると、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべての仮想端末回線に同一の制限を設定する必要があります。

インターフェイスに ACL を適用する手順については、「インターフェイスへの IPv4 ACL の適用」（P.32-19）を参照してください。VLAN に ACL を適用する手順については、「VLAN マップの設定」（P.32-30）を参照してください。

ACL 内のアドレスと仮想端末回線との間の着信接続および発信接続を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number*	設定する特定の回線を指定し、インライン コンフィギュレーション モードを開始します。 • **console**：コンソール端末回線を指定します。コンソール ポートは DCE です。 • **vty**：リモート コンソール アクセス用の仮想端末を指定します。 *line-number* は、連続した一連の番号の最初の回線番号で、回線タイプを指定するときに設定する必要があります。指定できる範囲は 0 ～ 16 です。

	コマンド	目的
ステップ 3	**access-class** *access-list-number* {**in** | **out**}	特定の仮想端末回線（デバイス側）とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

端末回線から ACL を削除するには、**no access-class** *access-list-number* {**in** | **out**} ライン コンフィギュレーション コマンドを使用します。

インターフェイスへの IPv4 ACL の適用

ここでは、ネットワーク インターフェイスに IPv4 ACL を適用する手順について説明します。レイヤ 3 インターフェイスの場合は、ACL を着信または発信の*いずれか*の方向に適用できます。レイヤ 2 インターフェイスでは、着信トラフィックにだけ ACL を適用できます。次の注意事項を考慮してください。

- インターフェイスへのアクセスを制御する場合は、名前付きまたは番号付き ACL を使用できます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。レイヤ 2 ポートに着信したパケットは、常にポート ACL でフィルタリングされます。
- レイヤ 3 インターフェイスに ACL が適用され、スイッチ上でルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。
- プライベート VLAN が設定されている場合、プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。

（注） パケットがアクセス グループによって拒否された場合、デフォルトでは、ルータは ICMP（Internet Control Message Protoco）到達不能メッセージを送信します。アクセスグループによって拒否されたこれらのパケットはハードウェアで廃棄されず、スイッチの CPU にブリッジングされて、ICMP 到達不能メッセージを生成します。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ 3 インターフェイス（ルータ ACL）を指定できます。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**ip access-group** {*access-list-number* | *name*} {**in** | **out**}	指定したインターフェイスへのアクセスを制御します。 キーワード **out** はレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	アクセス リストの設定を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

指定されたアクセス グループを削除するには、**no ip access-group** {*access-list-number* | *name*} {**in** | **out**} インターフェイス コンフィギュレーション コマンドを使用します。

次に、アクセス リスト 2 をポートに適用して、ポートに入るパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet0/1
Router(config-if)# ip access-group 2 in
```

（注）　**ip access-group** インターフェイス コンフィギュレーション コマンドをレイヤ 3 インターフェイス（SVI、レイヤ 3 EtherChannel、またはルーテッド ポート）に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ 3 アクセス グループは、CPU のレイヤ 3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。

着信 ACL の場合、パケットの受信後、スイッチはパケットを ACL と照合します。ACL によってパケットが許可された場合は、パケットの処理が続行されます。拒否された場合、パケットは廃棄されます。

発信 ACL の場合、パケットを受信し制御対象インターフェイスにルーティングしたあと、スイッチはパケットを ACL と照合します。ACL によってパケットが許可された場合、パケットは送信されます。拒否された場合、パケットは廃棄されます。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断して処理を行い、すべてのパケットが許可されます。ネットワーク セキュリティのため、未定義の ACL を使用する場合は注意してください。

IP ACL のハードウェアおよびソフトウェア処理

ACL は主にハードウェアで処理されますが、一部のトラフィックは CPU に転送してソフトウェアで処理する必要があります。ハードウェアの容量が一杯になり、ACL 設定を保管できなくなると、パケットは CPU に送信されて転送されます。ソフトウェアで転送されるトラフィックの転送速度は、ハードウェアで転送されるトラフィックに比べて大幅に低下します。

（注）　スイッチのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受ける（ソフトウェアで転送される）のは、スイッチに着信した該当 VLAN 内のトラフィックだけです。パケットのソフトウェア転送が発生すると、消費される CPU サイクル数に応じて、スイッチのパフォーマンスが低下することがあります。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードの使用
- ICMP 到達不能メッセージの生成

トラフィック フローのロギングと転送の両方を行う場合、転送はハードウェアで処理されますが、ロギングはソフトウェアで処理する必要があります。ハードウェアとソフトウェアではパケット処理能力が異なるため、ロギング中であるすべてのフロー（許可フローと拒否フロー）の合計帯域幅が非常に大きい場合は、転送されたパケットの一部をロギングできません。

ルータ ACL の設定をハードウェアに適用できない場合、VLAN に着信したルーティング対象パケットはソフトウェアでルーティングされます。ACL によって多数のパケットが CPU に転送されると、スイッチのパフォーマンスが低下することがあります。

show ip access-lists 特権 EXEC コマンドを入力したときに表示される一致の個数に、ハードウェアでアクセス制御されるパケットは含まれません。スイッチド パケットおよびルーテッド パケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、**show access-lists hardware counters** 特権 EXEC コマンドを使用します。

ルータ ACL の機能は次のとおりです。

- 標準 ACL および拡張 ACL（入力および出力）の許可アクションや拒否アクションをハードウェアで制御し、アクセス制御のセキュリティを強化します。
- **ip unreachables** がディセーブルの場合、*log* を指定しないと、セキュリティ ACL の*拒否*文と一致するフローがハードウェアによって廃棄されます。*許可*文と一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。ACE が*許可*文の場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

ACL のトラブルシューティング

次の ACL マネージャのメッセージが表示され、[chars] がアクセス リスト名である場合、

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

スイッチには、ACL のハードウェア表現を作成するためのリソースが不足しています。そのリソースには、ハードウェア メモリおよびラベル スペースは含まれますが、CPU メモリは含まれません。この問題は、使用可能な論理演算ユニットまたは専用のハードウェア リソースの不足が原因です。論理演算ユニットは、TCP フラグの一致、または TCP、UDP、SCTP ポート番号での **eq** 以外（**ne**、**gt**、**lt**、**range**）のテストで必要です。

次の対応策のいずれかを実行します。

- ACL 設定を変更して使用するリソースを減らします。
- その ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します。

専用のハードウェア リソースを確認するには、**show platform layer4 acl map** 特権 EXEC コマンドを入力します。スイッチに使用可能なリソースがない場合、インデックス 0 ～ 15 が使用不能であることが出力に表示されます。

リソースが不足している ACL の設定の詳細については、Bug Toolkit の CSCsq63926 を参照してください。

たとえば、次の ACL をインターフェイスに適用し、

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
```

```
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

次のメッセージが表示される場合、

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

フラグ関連の演算子が存在しません。この問題を回避するには、次の手順を実行します。

- **ip access-list resequence** グローバル コンフィギュレーション コマンドを使用して、1 番目の ACE の前に 4 番目の ACE を移動します。

  ```
  permit tcp source source-wildcard destination destination-wildcard
  permit tcp source source-wildcard destination destination-wildcard range 5 60
  permit tcp source source-wildcard destination destination-wildcard range 15 160
  permit tcp source source-wildcard destination destination-wildcard range 115 1660
  ```

  または

- 他の ACL よりも英数字順で先に表示される名前または番号に ACL の名前を変更します（たとえば、ACL *79* を ACL *1* に変更します）。

これで、ACL 内の 1 番目の ACE をインターフェイスに適用できます。スイッチによって、ACE が、Opselect インデックス内の使用可能なマッピング ビットに割り当てられ、次に、TCAM 内の同じビットを使用するために、フラグ関連の演算子が割り当てられます。

IPv4 ACL の設定例

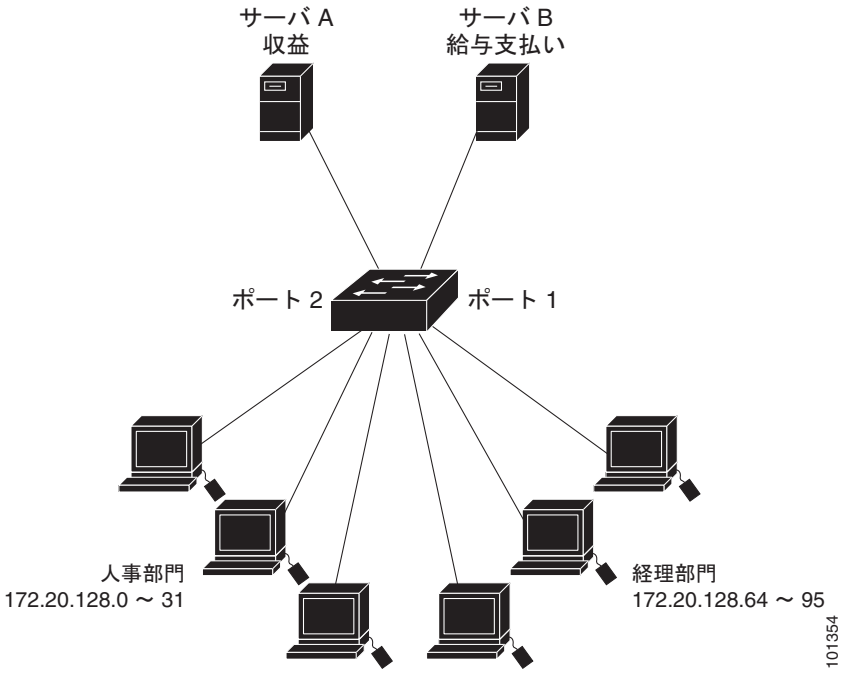
ここでは、IPv4 ACL の設定例および適用例を示します。ACL のコンパイルの詳細については、『*Cisco IOS Security Configuration Guide*』*Release 12.2*、および『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。

図 32-3 に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。

ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングします。

図 32-3　ルータ ACL によるトラフィックの制御



次に、標準 ACL を使用してポートからサーバ B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 6 out
```

次に、拡張 ACL を使用してサーバ B からポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。この ACL は、ルーテッド ポート 1 に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前にプロトコル（IP）を入力する必要があります。

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 106 in
```

番号付き ACL

次の例のネットワーク 36.0.0.0 は、2 番目のオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク アドレス 36.0.0.0 の 3 番目および 4 番目のオクテットは、特定のホストを指定します。アクセス リスト 2 を使用して、サブネット 48

のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。ACL は、ポートに入るパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番目の行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。3 番目の行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in
```

拡張 ACL を使用する別の例として、インターネットに接続されたネットワークがあり、ネットワーク上の任意のホストが、インターネット上の任意のホストと TCP 接続を確立できるようにする場合を考えます。ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにするとします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。発信パケットのポート番号は予約されています。安全なネットワーク システムでは常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できます。ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。キーワード **established** は、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。ギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in
```

名前付き ACL

次に、*internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスと宛先ワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。また、ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスに送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

IP ACL に適用される時間範囲

次に、月曜から金曜の午前 8 時 ～ 午後 6 時（18:00）の間、IP の HTTP トラフィックを拒否する例を示します。また、土曜および日曜の正午 ～ 午後 8 時の間だけ、UDP トラフィックを許可します。(20:00).

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group strict in
```

コメント付きの IP ACL エントリ

次に示す番号付き ACL の例では、Jones が所有するワークステーションのアクセスは許可されていますが、Smith が所有するワークステーションのアクセスは禁止されています。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションは Web 閲覧が禁止されます。

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットはアクセスが禁止されます。

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットは発信 Telnet の使用が禁止されます。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

ACL のロギング

ルータ ACL では、2 種類のロギングがサポートされています。キーワード **log** を指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。キーワード **log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。キーワード **log** も指定されています。

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
```

```
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8
packets
```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOG で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、キーワード **log-input** を指定した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1
0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet
```

キーワード **log** を指定した場合、同様のパケットに関するログ メッセージには入力インターフェイス情報が追加されません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1
packet
```

名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングする場合は、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。手順については、他の名前付き拡張 ACL の場合と同様です。

（注） レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

mac access-list extended コマンドでサポートされている非 IP プロトコルの詳細については、このリリースのコマンド リファレンスを参照してください。

（注） **appletalk** はコマンドラインのヘルプに表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされません。

名前付き MAC 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name*	名前を使用して MAC 拡張アクセス リストを定義します。

	コマンド	目的
ステップ 3	{**deny** | **permit**} {**any** | **host** *source MAC address* | *source MAC address mask*} {**any** | **host** *destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap** *lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp** | *0-65535*] [**cos** *cos*]	拡張 MAC アクセスリスト コンフィギュレーション モードでは、あらゆる（**any**）送信元 MAC アドレス、マスク付きの送信元 MAC アドレス、または特定の（**host**）送信元 MAC アドレス、およびあらゆる（**any**）宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、**permit** または **deny** を指定します。 （任意）次のオプションを入力することも可能です。 • *type mask*：Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、または 8 進数で表記できます。EtherType に適用される *don’t care* ビットの任意のマスクが付加され、一致検査が行われます。 • **lsap** *lsap mask*：IEEE802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。*don’t care* ビットの任意のマスクが付加されます。 • **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp** - 非 IP プロトコル • **cos** *cos*：プライオリティを設定するために使用される、0 ～ 7 の IEEE 802.1Q Cost of Service（CoS）番号
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除するには、**no mac access-list extended** *name* グローバル コンフィギュレーション コマンドを使用します。名前付き MAC 拡張 ACL から ACE を個別に削除することも可能です。

次に、DECnet Phase IV という EtherType のトラフィックだけを拒否し、その他のすべてのタイプのトラフィックを許可する、*mac1* という名前のアクセス リストを作成、表示する例を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    10 deny   any any decnet-iv
    20 permit any any
```

レイヤ 2 インターフェイスへの MAC ACL の適用

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用する場合は、次の注意事項を考慮してください。

- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。レイヤ 2 ポートに着信したパケットは、常にポート ACL でフィルタリングされます。

- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アクセス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC ACL を適用すると、以前に設定した ACL が新しい ACL に置き換わります。

レイヤ 2 インターフェイスへのアクセスを制御するため MAC アクセスリストを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイス（ポート ACL）でなければなりません。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**mac access-group** {*name*} {**in**}	MAC アクセスリストを使用し、指定されたインターフェイスへのアクセスを制御します。 **（注）**　ポート ACL は、着信方向に関してだけサポートされます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show mac access-group** [**interface** *interface-i*d]	そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

指定されたアクセス グループを削除するには、**no mac access-group** {*name*} インターフェイス コンフィギュレーション コマンドを使用します。

次に、アクセス リスト *mac1* をポートに適用して、ポートに入るパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet0/2
Router(config-if)# mac access-group mac1 in
```

（注）　**mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用された場合に限り、有効です。EtherChannel ポート チャネルで、このコマンドは使用できません。

スイッチは受信したパケットを入力 ACL と照合します。ACL によってパケットが許可された場合は、パケットの処理が続行されます。拒否された場合、パケットは廃棄されます。未定義の ACL をインターフェイスに適用すると、スイッチは ACL が適用されていないと判断して処理を行い、すべてのパケットが許可されます。ネットワーク セキュリティのため、未定義の ACL を使用する場合は注意してください。

VLAN マップの設定

ここでは、VLAN マップを設定する方法について説明します。この方法は、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当タイプのパケット（IP または MAC）に対する match 文が存在する場合、デフォルトではマップ内のどのエントリにも一致しないパケットが廃棄されます。該当タイプのパケットに対する match 文が存在しない場合、デフォルトではパケットが転送されます。

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

VLAN マップを作成して 1 つまたは複数の VLAN に適用するには、次の手順を実行します。

ステップ 1　VLAN に適用する標準 IPv4 ACL または拡張 IPv4 ACL、または名前付き MAC 拡張 ACL を作成します。「標準および拡張 IPv4 ACL の作成」（P.32-7）および「VLAN マップの作成」（P.32-32）を参照してください。

ステップ 2　VLAN ACL マップ エントリを作成するには、**vlan access-map** グローバル コンフィギュレーション コマンドを入力します。

ステップ 3　アクセス マップ コンフィギュレーション モードでは、**action** として、**forward**（デフォルト）または **drop** を任意で入力できます。また、**match** コマンドを入力し、既知の MAC アドレスだけが格納された IP パケットまたは非 IP パケットを指定したり、1 つまたは複数の ACL（標準または拡張）とパケットを照合したりできます。

（注）　VLAN マップに、該当タイプ（IP または MAC）のパケットに対する match 文が存在する場合に、マップ アクションが廃棄されると、そのタイプに一致するすべてのパケットが廃棄されます。VLAN マップに match 文が存在しない場合に、設定されたアクションが廃棄されると、すべての IP パケットおよびレイヤ 2 パケットが廃棄されます。

ステップ 4　**vlan filter** グローバル コンフィギュレーション コマンドは、VLAN マップを 1 つまたは複数の VLAN に適用します。

ここでは、次の設定情報について説明します。

- 「VLAN マップ設定時の注意事項」（P.32-30）
- 「VLAN マップの作成」（P.32-32）
- 「VLAN への VLAN マップの適用」（P.32-34）
- 「ネットワークでの VLAN マップの使用法」（P.32-35）

VLAN マップ設定時の注意事項

- トラフィックを拒否するように設定された ACL がインターフェイスに存在せず、VLAN マップが設定されていない場合は、すべてのトラフィックが許可されます。

- 各 VLAN マップは一連のエントリで構成されます。VLAN マップではエントリの順序が重要です。スイッチに着信したパケットは、VLAN マップの最初のエントリに対して比較検査されます。一致した場合は、VLAN マップで指定されたアクションが行われます。一致しなかった場合、パケットはマップ内の次のエントリに対して比較検査されます。
- 該当タイプのパケット（IP または MAC）に対する match 文が VLAN マップに 1 つまたは複数存在する場合でも、パケットがそれらの match 文に一致しない場合は、デフォルトでパケットが廃棄されます。該当タイプのパケットに対する match 文が VLAN マップ内に存在しない場合、デフォルトではパケットが転送されます。
- 多数の ACL が設定されている場合は、システムの起動に時間がかかることがあります。
- VLAN マップのロギングはサポートされません。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットをソフトウェアでルーティングする必要があります。
- スイッチのレイヤ 2 インターフェイスに IP アクセス リストまたは MAC アクセス リストが適用されていて、ポートが属する VLAN に VLAN マップを適用した場合、このポートの ACL は VLAN マップよりも優先されます。
- プライマリおよびセカンダリ VLAN で VLAN マップを設定できます。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。
  - ホスト ポートからプロミスキャス ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN に設定されている VLAN マップが適用されます。
  - プロミスキャス ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN に設定されている VLAN マップが適用されます。

  プライベート VLAN の特定の IP トラフィックをフィルタリングするには、VLAN マップをプライマリおよびセカンダリ VLAN の両方に適用します。プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。
- 設定例については、「ネットワークでの VLAN マップの使用法」（P.32-35）を参照してください。
- ルータ ACL および VLAN マップを組み合せて使用する方法については、「VLAN マップとルータ ACL の設定時の注意事項」（P.32-37）を参照してください。

VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップ エントリを作成、追加、削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan access-map** *name* [*number*]	VLAN マップを作成し、名前および番号（任意）を付けます。番号は、マップ内のエントリの順序を表す数字です。 同じ名前の VLAN マップを作成すると、10 ずつ増分する番号が順に割り当てられます。マップを変更または削除するときは、目的のマップ エントリの番号を入力できます。 このコマンドを入力すると、アクセスマップ コンフィギュレーション モードに変わります。
ステップ 3	**action** {**drop** | **forward**}	（任意）マップ エントリに対するアクションを設定します。デフォルトは forward です。
ステップ 4	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]	1 つまたは複数の標準または拡張アクセス リストに対してパケットを比較します（IP または MAC アドレスを使用）。パケットの比較は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して比較されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ比較されます。
ステップ 5	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**show running-config**	アクセス リストの設定を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

マップを削除するには、**no vlan access-map** *name* グローバル コンフィギュレーション コマンドを使用します。

マップ内の単一のシーケンス エントリを削除するには、**no vlan access-map** *name number* グローバル コンフィギュレーション コマンドを使用します。

デフォルトのアクションである転送を行うには、**no action** アクセスマップ コンフィギュレーション コマンドを使用します。

VLAN マップでは、特定の permit または deny キーワードは使用されません。VLAN マップを使用してパケットを拒否するには、パケットと比較する ACL を作成し、アクションを廃棄に設定します。ACL にキーワード permit を指定した場合は一致と見なされます。ACL にキーワード deny を指定した場合は一致しないと見なされます。

ACL および VLAN マップの例

次に、特定の目的で ACL および VLAN マップを作成する例を示します。

例 1

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、*ip1* ACL（TCP パケット）に一致するすべてのパケットが廃棄されます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1*ACL を作成します。VLAN マップには IP パケットに対する match 文が存在するため、デフォルトではどの match 文とも一致しないすべての IP パケットが廃棄されます。

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可します。*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL とも一致しなかったすべての IP パケット（TCP でも UDP でもないパケット）が廃棄されます。

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

例 2

次の例の VLAN マップには、IP パケットの廃棄および MAC パケットの転送というデフォルト アクションがあります。標準の ACL 101 と名前付き拡張アクセス リスト **igmp-match** および **tcp-match** をこのマップと組み合せて使用すると、次のようになります。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットが廃棄されます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットが廃棄されます。
- すべての非 IP パケットが転送されます。

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

例 3

次の例の VLAN マップには、MAC パケットの廃棄および IP パケットの転送というデフォルト アクションがあります。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** とこのマップを組み合せて使用すると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-ip または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットが廃棄されます。

- すべての IP パケットが転送されます。

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any decnet-ip
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

例 4

次の例の VLAN マップには、すべてのパケット（IP および非 IP）が廃棄されるデフォルト アクションがあります。例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合せて使用すると、次のようになります。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットが廃棄されます。
- その他のすべての MAC パケットが廃棄されます。

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan filter** *mapname* **vlan-list** *list*	VLAN マップを 1 つまたは複数の VLAN ID に適用します。 list には単一の VLAN ID（22）、連続した範囲（10-22）、または VLAN ID からなるストリング（12,22,30）を指定できます。カンマやハイフンの前後にスペースを挿入することも可能です。
ステップ 3	**show running-config**	アクセス リストの設定を表示します。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN マップを削除するには、**no vlan filter** *mapname* **vlan-list** *list* グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN マップ 1 を VLAN 20 ～ 22 に適用する例を示します。

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

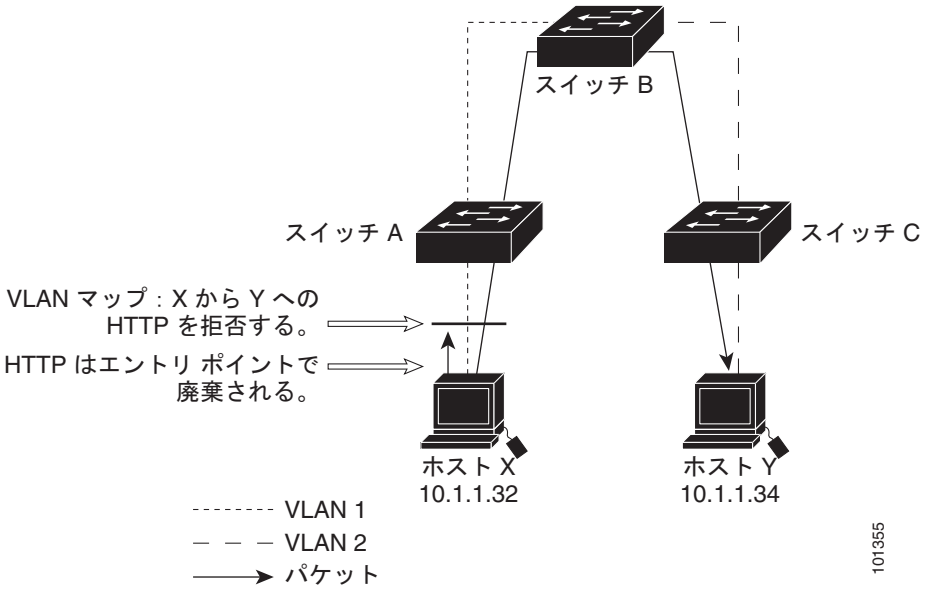
ネットワークでの VLAN マップの使用法

- 「ワイヤリング クローゼットの構成」（P.32-35）
- 「別の VLAN にあるサーバへのアクセス拒否」（P.32-36）

ワイヤリング クローゼットの構成

ワイヤリング クローゼット構成におけるスイッチでは、ルーティングがイネーブルでない可能性があります。ただし、この構成でも VLAN マップおよび QoS 分類 ACL はサポートされています。図 32-4 では、ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリング クローゼット スイッチ A およびスイッチ C に接続されていると想定しています。ホスト X からホスト Y へのトラフィックは、ルーティングがイネーブルに設定されたレイヤ 3 スイッチであるスイッチ B によって最終的にルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス制御できます。

図 32-4　　ワイヤリング クローゼットの構成



HTTP トラフィックをホスト X からホスト Y にスイッチングしない場合は、ホスト X（IP アドレス 10.1.1.32）からホスト Y（IP アドレス 10.1.1.34）への HTTP トラフィックがすべてスイッチ A で廃棄されてスイッチ B に転送されないようにスイッチ A の VLAN マップを設定します。

まず、HTTP ポートですべての TCP トラフィックを許可（一致）する IP アクセス リスト *http* を定義します。

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

次に、*http* アクセス リストと一致するトラフィックが廃棄され、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

次に、VLAN アクセスマップ *map2* を VLAN 1 に適用します。

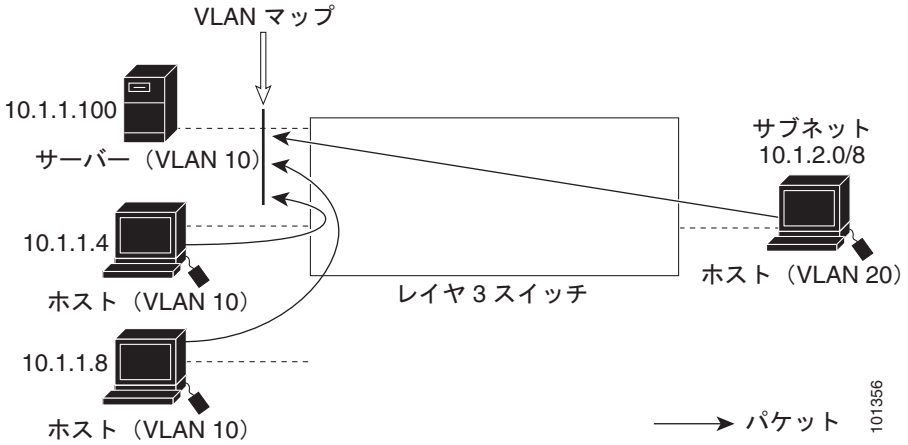
```
Switch(config)# vlan filter map2 vlan 1
```

別の VLAN にあるサーバへのアクセス拒否

別の VLAN にあるサーバへのアクセスを制限できます。たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります（図 32-5 を参照）。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。

図 32-5　別の VLAN にあるサーバへのアクセス拒否



次に、サブネット 10.1.2.0/8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 へのアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ SERVER1 を作成して、別の VLAN 内のサーバへのアクセスを拒否する例を示します。最後に、VLAN マップ SERVER1 を VLAN 10 に適用します。

ステップ 1　対応するパケットと比較する IP ACL を定義します。

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl))# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl))# exit
```

ステップ 2　SERVER1_ACL と一致する IP パケットを廃棄し、一致しない IP パケットを転送するこの ACL を使用して、VLAN マップを定義します。

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

ステップ 3　VLAN 10 に VLAN マップを適用します。

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

ルータ ACL を VLAN マップと組み合せて使用する方法

ルーティングされたトラフィックに対してアクセス制御を行うには、VLAN マップを単独で使用するか、またはルータ ACL と VLAN マップを組み合せて使用します。ルータ ACL は、入力および出力の両方向のルーテッド VLAN インターフェイスで定義できます。パケット フローが ACL 内 VLAN マップの deny 文と一致した場合、ルータ ACL の設定に関係なく、パケット フローは拒否されます。

（注）　ルータ ACL を VLAN マップと組み合せて使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

パケット タイプ（IP または MAC）に対する match 文が VLAN マップに存在し、パケットがそのタイプに一致しない場合は、デフォルトでパケットが廃棄されます。VLAN マップ内に match 文がなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。

ここでは、ルータ ACL を VLAN マップと組み合せて使用する方法について説明します。

- 「VLAN マップとルータ ACL の設定時の注意事項」（P.32-37）
- 「VLAN に適用されるルータ ACL と VLAN マップの例」（P.32-38）

VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL *および*VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

スイッチ ハードウェアは、方向（入力および出力）ごとにセキュリティ ACL を 1 回検索します。したがって、ルータ ACL および VLAN マップを同じ VLAN に設定する場合は、これらを統合する必要があります。ルータ ACL と VLAN マップを統合すると、ACE の数が膨大になる場合があります。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつのみ設定できます。

- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルト アクションだけが反対のタイプとなるように ACL を記述します。次のいずれかの形式を使用して、ACL を記述します。

  permit...
  permit...
  permit...
  deny ip any any

  または

  deny...
  deny...
  deny...
  permit ip any any

- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。レイヤ 4 情報を追加すると、統合プロセスが複雑になります。ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。可能な限り、IP アドレスには *don’t care* ビットを使用してください。

  IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

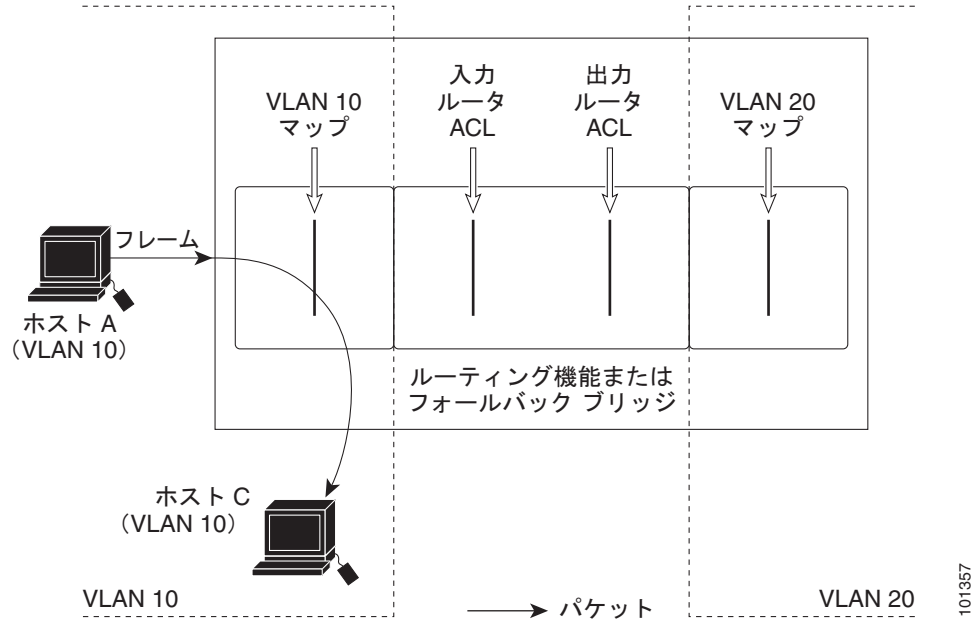
VLAN に適用されるルータ ACL と VLAN マップの例

ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す線と交差するポイントで、パケットを転送せずに廃棄する可能性もあります。

ACL およびスイッチド パケット

図 32-6 に、VLAN 内でスイッチングされるパケットに ACL を適用する方法を示します。ルーティングまたは転送されず、VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップだけが適用されます。

図 32-6　スイッチド パケットへの ACL の適用

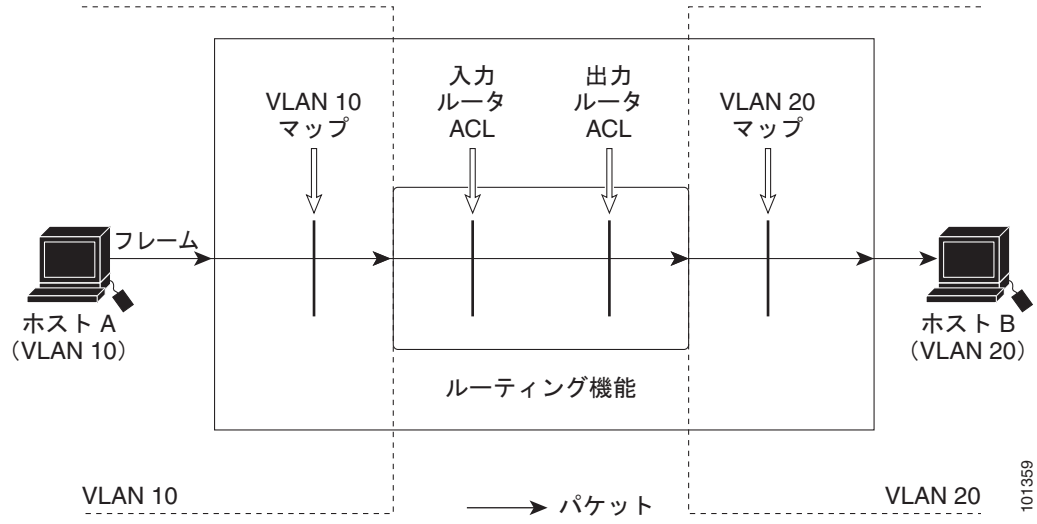


ACL およびルーテッド パケット

図 32-7 に、ルーテッド パケットに ACL を適用する方法を示します。ルーテッド パケットの場合、ACL は次の順番で適用されます。

1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ

図 32-7　ルーテッド パケットへの ACL の適用

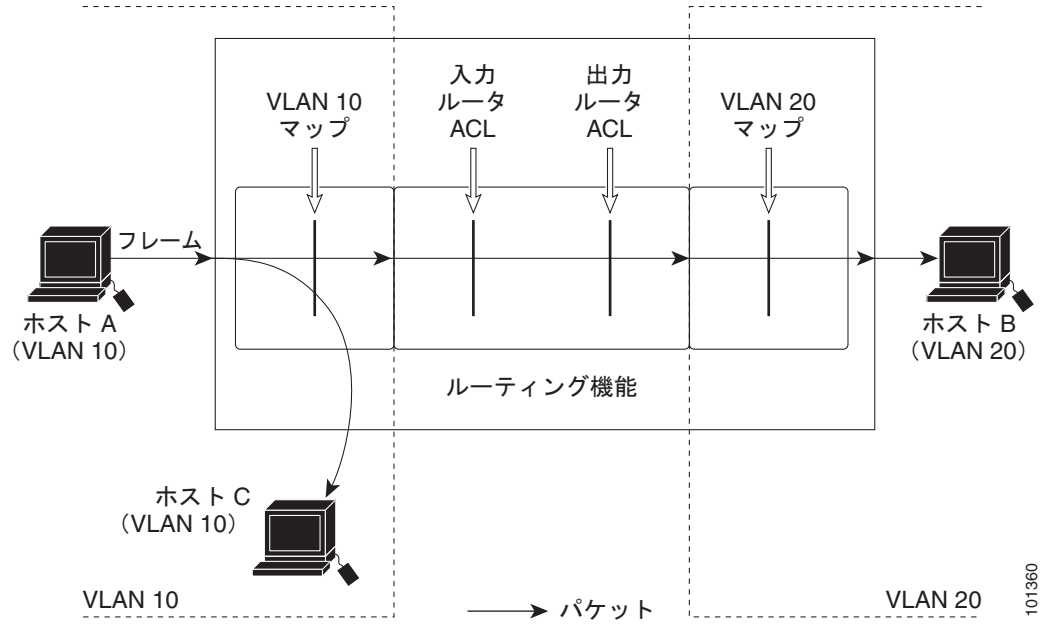


ACL およびマルチキャスト パケット

図 32-8 に、IP マルチキャスト用に複製されたパケットに ACL を適用する方法を示します。ルーティングされるマルチキャスト パケットには、2 つの異なるフィルタが適用されます。1 つは、宛先が入力 VLAN 内の他のポートである場合に使用され、もう 1 つは、宛先がパケットのルーティング先である別の VLAN 内にある場合に使用されます。パケットは複数の出力 VLAN にルーティングされる場合がありますが、この場合は宛先 VLAN ごとに異なるルータ出力 ACL および VLAN マップが適用されます。

最終的に、パケットは一部の出力 VLAN 内で許可され、それ以外の VLAN で拒否されます。パケットのコピーが、許可された宛先に転送されます。ただし、入力 VLAN マップ（図 32-8 の VLAN 10 マップ）によってパケットが廃棄される場合、パケットのコピーは宛先に送信されません。

図 32-8　　マルチキャスト パケットへの ACL の適用



IPv4 ACL の設定の表示

スイッチ上に設定されている ACL、およびインターフェイスや VLAN に適用された ACL を表示できます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。レイヤ 2 インターフェイスに適用された MAC ACL を表示することも可能です。この情報を表示するには、特権 EXEC コマンドを使用します（表 32-2 を参照）。

表 32-2　アクセス リストおよびアクセス グループを表示するためのコマンド

コマンド	目的
show access-lists [*number* | *name*]	最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	最新の IP アクセス リスト全体、または特定の IP アクセス リスト（番号付きまたは名前付き）を表示します。
show ip interface *interface-id*	インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
show running-config [**interface** *interface-id*]	スイッチまたは特定のインターフェイスに関するコンフィギュレーション ファイルの内容（設定されたすべての MAC および IP アクセス リスト、インターフェイスに適用されているアクセス グループなど）を表示します。
show mac access-group [**interface** *interface-i*d]	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。

VLAN アクセスマップまたは VLAN フィルタに関する情報も表示できます。VLAN マップ情報を表示するには、表 32-3 に記載された特権 EXEC コマンドを使用します。

表 32-3　VLAN マップ情報を表示するためのコマンド

コマンド	目的
show vlan access-map [*mapname*]	すべての VLAN アクセスマップまたは指定されたアクセスマップに関する情報を表示します。
show vlan filter [**access-map** *name* | **vlan** *vlan-id*]	すべての VLAN フィルタに関する情報、または指定された VLAN や VLAN アクセスマップに関する情報を表示します。

CHAPTER 33

コントロール プレーンのセキュリティ設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにコントロール プレーンのセキュリティ機能の設定方法について説明します。いずれのネットワークでも、レイヤ 2 スイッチおよびレイヤ 3 スイッチは、ネットワーク内の他のスイッチと制御パケットを交換します。Cisco ME スイッチは、カスタマー ネットワークとサービスプロバイダー ネットワーク間の変換として機能し、コントロール プレーン セキュリティを使用して 2 つのネットワーク間のトポロジ情報が分離されていることを確認します。このメカニズムにより、起こりうる他のカスタマー ネットワークによる DoS 攻撃から保護します。

- 「コントロール プレーンのセキュリティの概要」（P.33-1）
- 「コントロール プレーンのセキュリティ設定」（P.33-6）
- 「コントロール プレーンのセキュリティのモニタリング」（P.33-8）

コントロール プレーンのセキュリティの概要

Cisco ME スイッチでは、Network Node Interface（NNI; ネットワーク ノード インターフェイス）として設定されたポートがサービス プロバイダー ネットワークに接続されます。このスイッチは、これらのポートを介してネットワークのその他のスイッチと通信し、通常のトラフィックに加えてプロトコル制御パケットを交換します。Cisco ME スイッチ上のその他のポートは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）であり、カスタマー側のポートとして使用されます。ポートはそれぞれ単一のカスタマーに接続され、通常、スイッチとカスタマー間のネットワーク プロトコル制御パケット交換は必要ありません。レイヤ 2 プロトコルのほとんどは、UNI ではサポートされていません。偶発的または意図的な CPU 過負荷から保護するために、Cisco ME スイッチでは UNI の事前定義された一組のレイヤ 2 制御パケットおよび一部のレイヤ 3 制御パケットを廃棄またはレート制限することにより、自動的にコントロール プレーン セキュリティを実現します。

3 番目のポート タイプである、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）も設定できます。ENI は、UNI と同様、カスタマー側のインターフェイスです。ENI 上では、デフォルトで、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）、Link Layer Discovery Protocol（LLDP; リンク レイヤ検出プロトコル）などのレイヤ 2 制御プロトコルがディセーブルになっています。ENI 上では、UNI とは異なり、これらのプロトコルをイネーブルにできます。ポート チャネルで ENI を設定する際に、Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）、および Port Aggregation Protocol（PAgP; ポート集約プロトコル）もイネーブルにできます。プロトコルがインターフェイス上でイネーブルになっているかディセーブルになっているかによって、ENI は、プロトコル パケットを破棄するか、またはレート制限します。ENI 上の他のすべての制御プロトコルに関して、スイッチは、UNI の場合と同じ方法でパケットを破棄するかレート制限します。

CPU 保護（デフォルトでイネーブルになっています）では、ポートごとに 19 のポリサーが使用されます。CPU 保護がイネーブルになっている場合、ポートごとに最大 45 のポリサーを設定できます。ポートごとのポリサーをより多く設定する必要がある場合、**no policer cpu uni all** グローバル コンフィギュレーション コマンドを入力してスイッチをリロードすることによって、CPU 保護をディセーブルにできます。CPU 保護をディセーブルにすると、ユーザ定義クラスに対してポートごとに最大 63 のポリサー（すべての 4 番目のポート上に 62）を、class-default に対して 1 つのポリサーを設定できます。

（注） CPU をオフにするとプロトコル パケットが CPU に到達可能となり、これが、CPU 処理の過負荷や、ソフトウェアによるストーム制御の原因となる可能性があります。

コントロール プレーンのセキュリティは、ポートがルーティング モードまたは非ルーティング モードであるかにかかわらず、ルータの MAC アドレスを含むレイヤ 2 制御パケットおよび非 IP パケットに対して、ポート上でサポートされます（ポートがルーティング モードとなるのは、グローバル IP ルーティングがイネーブルで、ポートが **no switchport** インターフェイス コンフィギュレーション コマンドにより設定されているか、または Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）がアクティブな VLAN に関連付けられている場合です）。これらのパケットは、レイヤ 2 プロトコル設定に応じて、廃棄されるかまたはレート制限されます。レイヤ 3 制御パケットの場合、ルーティング モードのポート上では（レイヤ 3 サービス ポリシーが付加されているかどうかにかかわらず）、コントロール プレーンのセキュリティにより、Internet Group Management Protocol（IGMP）制御パケットのレート制限だけがサポートされます。レイヤ 3 パケットの場合、非ルーティング モードのポート上では（レイヤ 2 サービス ポリシーが付加されているかどうかにかかわらず）、ルータ MAC アドレスが設定された IP パケットだけが廃棄されます。

次の制御パケット タイプが、廃棄またはレート制限されます。

- レイヤ 2 プロトコル制御パケット
  - UNI および ENI 上で常に廃棄される制御パケット（Dynamic Trunking Protocol [DTP; ダイナミック トランキング プロトコル] パケットおよび一部の Bridge Protocol Data Unit [BPDU; ブリッジ プロトコル データ ユニット] など）
  - デフォルトでは廃棄されるが、イネーブルまたはトンネリングできる制御パケット（CDP、STP、LLDP、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）、UniDirectional Link Detection（UDLD; 単一方向リンク検出）プロトコル、LACP および PAgP パケットなど）。これらのプロトコル パケットがイネーブルである場合は、スイッチによりレート制限およびトンネリングされます。
  - スイッチで必要とされる制御パケットまたは管理パケット（キープアライブ パケットなど）。これらの制御パケットは CPU により処理されますが、CPU が過負荷にならないよう標準または安全限界にレート制限されます。
- ルータ MAC アドレスが設定された非 IP パケット
- ルータ MAC アドレスが設定された IP パケット
- デフォルトでイネーブルに設定されていて、レート制限される必要がある IGMP 制御パケット。ただし、IGMP スヌーピングおよび IP マルチキャスト ルーティングがディセーブルである場合、これらのパケットはデータ パケットのように処理され、ポリサーは割り当てされません。

スイッチではポリシングを使用して、レイヤ 2 制御プロトコルを廃棄またはレート制限することにより、コントロール プレーンのセキュリティを実行します。レイヤ 2 プロトコルが UNI または ENI ポートでイネーブルであり、スイッチ上でトンネリングされる場合に、これらのプロトコル パケットはレート制限されます。レート制限されない場合は、制御パケットが廃棄されます。

プロトコル トラフィックには、デフォルトで CPU により廃棄されるものと、レート制限されるものがあります。表 33-1 に、この機能がイネーブルである場合またはレイヤ 2 プロトコル トンネリングがプロトコルに対してイネーブルである場合のデフォルト アクションおよびレイヤ 2 プロトコル パケットに対するアクションを示します。これらの機能には、UNI 上でイネーブルにできないものがあり、す

べてのプロトコルをトンネリングできるわけではない（ダッシュで示される）ことに注意してください。レイヤ 2 プロトコル トンネリングが*任意の*サポート対象プロトコル（CDP、STP、VTP、LLDP、LACP、PAgP、または UDLD）に対してイネーブルである場合、スイッチのレイヤ 2 プロトコル トンネリング プロトコルはすべてのポート上でレート制限ポリサーを使用します。UDLD がポート上でイネーブルであるか、UDLD トンネリングがイネーブルである場合、UDLD パケットはレート制限されます。

表 33-1　UNI または ENI で受信されるレイヤ 2 プロトコル パケットのコントロール プレーンのセキュリティ アクション

プロトコル	デフォルト	機能がイネーブルである場合	レイヤ 2 プロトコル トンネリングがイネーブルである場合 [1]
STP	廃棄	レート制限 **（注）** STP をイネーブルにできるのは、ENI 上でだけです。	レート制限
RSCD_STP（予約された IEEE 802.1D アドレス）	廃棄	Ethernet Link Management Interface（ELMI）がイネーブルである場合、グローバルまたはポート単位のいずれか最後に設定された方法で、スロットル ポリサーがポートに割り当てられる。ELMI がディセーブルである場合、（グローバルまたはポート単位のいずれか最後に設定された方法で）廃棄ポリサーがポートに割り当てられる。	
PVST+	廃棄	–	レート制限
LACP	廃棄	レート制限 **（注）** LACP をイネーブルにできるのは、ENI 上でだけです。	レート制限
PAgP	廃棄	レート制限 **（注）** PAgP をイネーブルにできるのは、ENI 上でだけです。	レート制限
IEEE 802.1x	廃棄	レート制限	–
CDP	廃棄	レート制限 **（注）** CDP をイネーブルにできるのは、ENI 上でだけです。	レート制限
LLDP	廃棄	レート制限 **（注）** LLDP をイネーブルにできるのは、ENI 上でだけです。	レート制限
DTP	廃棄	–	–
UDLD	廃棄	レート制限	レート制限
VTP	廃棄	–	レート制限
CISCO_L2（MAC アドレス 01:00:0c:cc:cc:cc が設定されたその他のシスコ レイヤ 2 プロトコル）	廃棄	–	CDP、DTP、UDLD、PAgP、または VTP がレイヤ 2 トンネリングされる場合にレート制限される。

表 33-1　UNI または ENI で受信されるレイヤ 2 プロトコル パケットのコントロール プレーンのセキュリティ アクション（続き）

プロトコル	デフォルト	機能がイネーブルである場合	レイヤ 2 プロトコル トンネリングがイネーブルである場合 [1]
KEEPALIVE（MAC アドレス、SNAP カプセル化、LLC、Org ID、または HDLC パケット）	レート制限	–	–
イーサネット Connectivity Fault Management（CFM）	ポリサーは割り当てられない	CFM がグローバルにイネーブルである場合、スロットル ポリサーがすべてのポートに割り当てられる。CFM がグローバルにディセーブルである場合、ヌル ポリサーがすべてのポートに割り当てられる。	–

1. レイヤ 2 プロトコル トンネリングが任意のポートの任意のプロトコルに対してイネーブルである場合に、レイヤ 2 プロトコル トラフィックがレート制限されます。

スイッチは、CPU 保護のため、自動的に 27 のコントロール プレーンのセキュリティ ポリサーを割り当てます。システムの起動時に、0 ～ 26 に番号付けされたポートごとに 1 つのポリサーを割り当てます。ポートに割り当てられたポリサーは、ポートに着信したプロトコル パケットがレート制限されるか廃棄されるかを決定します。ME 3400E-24TS スイッチ上では、ポリサー 26 は、廃棄ポリサーを意味するグローバル ポリサーです。いずれのポートでも、26 として示されるすべてのトラフィック タイプは廃棄されます。ポリサー 0 ～ 25 はレート制限ポリサーで、プロトコルのポートに割り当てられます。ポリサー 0 ～ 23 はファスト イーサネット ポート 1 ～ 24 の論理 ID で、ポリサー 24 および 25 はそれぞれ、ギガビット イーサネット ポート 1 および 2 を意味します。ポリサー 255 は、ポリサーがプロトコルに割り当てられないことを意味します。

ME 3400EG-12CS および ME 34000EG-2CS スイッチの場合、ポリサー 4 は、廃棄ポリサーを意味します。ポート上で 4 として示されるトラフィック タイプは破棄されます。ポリサー 0 ～ 3 はレート制限ポリサーで、プロトコルのポートに割り当てられます。

インターフェイス上のプロトコルに割り当てられるポリサー アクションを確認するには、**show platform policer cpu interface** *interface-id* 特権 EXEC コマンドを入力します。

（注）　特に指示の無い場合、例は ME 3400E-24TS スイッチのものです。

次に、UNI でのデフォルト ポリサー設定を示します。ポートがファスト イーサネット 1 であるため、レート制限されるプロトコルの ID は 0 で、ファスト イーサネット ポート 5 には、ID 4 が表示されます。*Policer Index* は、特定のプロトコルを意味します。ASIC 番号は、ポリサーが異なる ASIC 上にある場合を表します。

UNI では、STP、CDP、LLDP、LACP、および PAgP がサポートされていないので、これらのパケットは破棄されます（物理ポリサー 26）。ENI でもこれらのプロトコルはデフォルトでディセーブルになっていますが、イネーブルにすることが可能です。ENI 上でイネーブルにすると、制御パケットがレート制限され、レート制限ポリサーが、これらのプロトコルに割り当てられます（物理ポリサー 22）。

```
Switch# show platform policer cpu interface fastethernet 0/3
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/1
STP                                  1            26            0
LACP                                 2            26            0
```

```
8021X                              3            26            0
RSVD_STP                           4            26            0
PVST_PLUS                          5            26            0
CDP                                6            26            0
LLDP                               7            26            0
DTP                                8            26            0
UDLD                               9            26            0
PAGP                              10            26            0
VTP                               11            26            0
CISCO_L2                          12            26            0
KEEPALIVE                         13             0            0
CFM                               14           255            0
SWITCH_MAC                        15            26            0
SWITCH_ROUTER_MAC                 16            26            0
SWITCH_IGMP                       17             0            0
SWITCH_L2PT                       18            26            0
```

次に、制御プロトコルがインターフェイス上でイネーブルになったときに ENI に割り当てられるポリサーの例を示します。値 22 は、プロトコル パケットが、そのプロトコルに関してレート制限されていることを示しています。プロトコルがイネーブルになっていない場合、デフォルトは UNI の場合と同じです。

```
Switch# show platform policer cpu interface fastethernet0/23
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/23
STP                                1            26            0
LACP                               2            22            0
8021X                              3            26            0
RSVD_STP                           4            26            0
PVST_PLUS                          5            26            0
CDP                                6            22            0
LLDP                               7            26            0
DTP                                8            26            0
UDLD                               9            26            0
PAGP                              10            26            0
VTP                               11            26            0
CISCO_L2                          12            22            0
KEEPALIVE                         13            22            0
CFM                               14           255            0
SWITCH_MAC                        15            26            0
SWITCH_ROUTER_MAC                 16            26            0
SWITCH_IGMP                       17            22            0
SWITCH_L2PT                       18            22            0
```

次に、ME 3400EG-12CS または ME 34000EG-2CS スイッチ上でのレート制限の例を示します。値 1 は、プロトコル パケットが、そのプロトコルに関してレート制限されていることを示しています。

```
Switch #show platform policer cpu interface gigabitethernet 0/2
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Gi0/2
STP                                1             4            0
LACP                               2             4            0
8021X                              3             4            0
RSVD_STP                           4             1            0
PVST_PLUS                          5             4            0
```

```
CDP                                 6             4             0
LLDP                                7             4             0
DTP                                 8             4             0
UDLD                                9             4             0
PAGP                               10             4             0
VTP                                11             4             0
CISCO_L2                           12             4             0
KEEPALIVE                          13             1             0
CFM                                14           255             0
SWITCH_MAC                         15             4             0
SWITCH_ROUTER_MAC                  16             4             0
SWITCH_IGMP                        17             1             0
SWITCH_L2PT                        18             4             0
```

次に、NNI に割り当てられるデフォルト ポリサーを示します。ほとんどのプロトコルでは、NNI にポリサーが割り当てられません。値 255 は、プロトコルのポートにポリサーが割り当てられないことを意味します。

```
Switch #show platform policer cpu interface gigabitethernet 0/1
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Gi0/1
STP                                 1            255             0
LACP                                2            255             0
8021X                               3            255             0
RSVD_STP                            4            255             0
PVST_PLUS                           5            255             0
CDP                                 6            255             0
LLDP                                7            255             0
DTP                                 8            255             0
UDLD                                9            255             0
PAGP                               10            255             0
VTP                                11            255             0
CISCO_L2                           12            255             0
KEEPALIVE                          13            255             0
CFM                                14            255             0
SWITCH_MAC                         15            255             0
SWITCH_ROUTER_MAC                  16            255             0
SWITCH_IGMP                        17            255             0
SWITCH_L2PT                        18            255             0
```

コントロール プレーンのセキュリティ設定

CPU 保護は、デフォルトでイネーブルになっており、CPU ポリサーは事前に割り当てられています。CPU 保護をディセーブルにするには、**no policer cpu uni all** グローバル コンフィギュレーション コマンドを入力し、再度イネーブルにするには、**policer cpu uni all** グローバル コンフィギュレーション コマンドを入力します。CPU 保護をディセーブルまたはイネーブルにする場合、設定が反映される前に **reload** 特権 EXEC コマンドを入力することによって、スイッチをリロードする必要があります。

CPU 保護がイネーブルになっている場合、ポートごとに設定できるポリサーは 45 だけです。CPU 保護をディセーブルにすると、ポートごとに最大 64 のポリサーを設定できます。CPU 保護をディセーブルにする際はこれらの制限事項について注意してください。

- CPU 保護をディセーブルにすると、ユーザ定義クラスに対してポートごとに最大 63 のポリサー（すべての 4 番目のポート上に 62）を、class-default に対して 1 つのポリサーを設定できます。

- Cisco ME 3400EG-12CS スイッチ上では、ハードウェア制限のため、64 のポート単位 VLAN 単位ポリサーを割り当てられるポート数は最大 6 です。6 を超えるポート単位 VLAN 64 ポリサー ポリシー マップを付加しようとすると、*VLAN labels exceeded* エラー メッセージが出力されて、その付加は失敗します。
- CPU 保護をディセーブルにして、45 を超えるポリサーを持つポリシー マップを付加してから、CPU 保護を再度イネーブルにして、リロードした場合、CPU 保護には、ポートごとに 19 のポリサーが再度必要となります。リロード中、ポリサー 46 以降は、*policer resources exceeded* のエラー条件を満たすことになるので、これらのクラスに付加されるポリサーはありません。

設定できるのは、レート制限しきい値だけです。設定されたしきい値は、すべての UNI および ENI 上のすべてのサポート対象制御プロトコルに適用されます。また、プロトコルが ENI 上でイネーブルになっている場合、STP、CDP、LLDP、LACP、および PAgP にも適用されます。

（注） 通常のレイヤ 2 動作時には、UNI または ENI からスイッチに対して ping を実行できません。この制限事項は、NNI には適用されません。テスト状況で ping をイネーブルにする方法については、「ping の使用」（P.46-10）を参照してください。

CPU 保護用にしきい値レートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policer cpu uni** *rate*	CPU 保護のポリシングしきい値レートを設定します。指定できる範囲は 8000 ～ 409500 b/s です。設定されない場合は、デフォルトの 160000 b/s となります。 **（注）** 設定されたレートは、すべての UNI および ENI 上のすべてのサポート対象およびイネーブルにされた制御プロトコルに適用されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show policer cpu uni-eni rate**	設定された CPU ポリサー レートを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのしきい値レートに戻るには、**no policer cpu uni** グローバル コンフィギュレーション コマンドを使用します。CPU 保護をディセーブルにするには、**no policer cpu uni all** グローバル コンフィギュレーション コマンドを入力して、スイッチをリロードします。

次に、CPU 保護しきい値を 10000 b/s に設定し、その設定を確認する例を示します。

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# policer cpu uni 10000
Switch(config)# end
Switch# show policer cpu uni-eni rate
CPU UNI/ENI port police rate = 10000 bps
```

次に、CPU 保護がディセーブルになっているときの show コマンドの出力例を示します。

```
Switch# show policer cpu uni-eni rate
CPU Protection feature is not enabled
```

コントロール プレーンのセキュリティのモニタリング

スイッチまたはインターフェイス上のコントロール プレーンのセキュリティ設定および統計情報は、モニタリングできます。また、これらの統計情報は、表 33-2 に示す特権 EXEC コマンドを使用することによって、いつでも消去できます。このコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

表 33-2　コントロール プレーンのセキュリティをモニタリングするためのコマンド

コマンド	目的
clear policer cpu uni-eni counters {**classification** | **drop**}	機能ごとにコントロール プレーンのすべての統計情報を消去するか（**classification**）、またはコントロール プレーン ポリサーで維持されるすべての統計情報を消去します（**drop**）。
debug platform policer cpu uni-eni	コントロール プレーン ポリサーのデバッグをイネーブルにします。このコマンドにより、CPU 保護に対して何らかの変更があった場合に、情報メッセージが表示されます。
show platform policer cpu {**classification** | **interface** *interface-id*}	コントロール プレーンのポリサー情報を表示します。 • **classification**：分類の統計情報を示します。 • **interface** *interface-id*：指定されたインターフェイスのポリサー インデックスを示します。

show policer cpu uni-eni {**drop** [**interface** *interface-id*] | **rate**}	スイッチの CPU ポリサー情報を表示します。
	• **drop** [**interface** *interface-id*] ：すべてのインターフェイスまたは指定したインターフェイスの廃棄フレーム数を示します。
	• **rate**：CPU ポリサーに設定されたしきい値レートを示します。
	CPU 保護がディセーブルになっている場合、次のメッセージが出力内に表示されます。
	`Switch# show policer cpu uni drop`
	`CPU Protection feature is not enabled`

CHAPTER 34

QoS の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチ上で、Modular Quality of Service CLI（MQC; モジュラ QoS コマンドライン インターフェイス）コマンドを使用して QoS を設定する方法について説明します。QoS を使用すると、特定のタイプのトラフィックを他のトラフィックよりも優先的に処理できます。QoS が設定されていない場合、パケットの内容やサイズに関係なく、各パケットにベストエフォート型サービスが提供されます。信頼性、遅延限度、スループットが保証されずに、パケットが送信されます。MQC では、特定のトラフィック ストリームの優先順位付けまたは制限を行うための総合的な階層型設定のフレームワークを提供します。

（注） IPv6 QoS はサポートされません。

Cisco IOS の MQC コマンドの詳細については、次のサイトにある「Cisco IOS Quality of Service Solutions Command Reference」を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087f48.html

この章で使用するプラットフォーム特有のコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

イーサネット ターミナル ループバックを使用したインターフェイスでの完全パス QoS の詳細については、「イーサネット ループバックのイネーブル化」（P.43-42）を参照してください。

- 「QoS の概要」（P.34-1）
- 「Performance-Monitoring プロトコルの QoS 処理」（P.34-23）
- 「QoS の設定」（P.34-37）
- 「QoS 情報の表示」（P.34-83）
- 「ポリシー マップの設定例」（P.34-84）

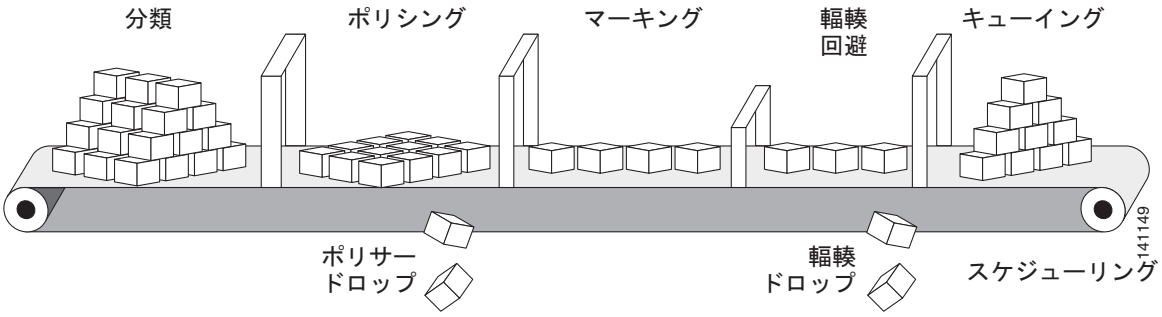
QoS の概要

ネットワークは通常、ベストエフォート型の配信方式で動作します。この場合、すべてのトラフィックに同じプライオリティが与えられ、送信されるタイミングも同じです。輻輳が発生した場合に廃棄される可能性も、すべてのトラフィックで同等です。

QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてプライオリティを指定し、トラフィック管理技術を使用して、優先処理を行うことができます。ネットワークに QoS を実装すると、ネットワークのパフォーマンスが予想しやすくなり、帯域利用率がより効果的になります。

図 34-1 に、MQC のモデルを示します。

図 34-1　MQC のモデル



基本的な QoS には、次のアクションが含まれます。

- パケット分類：トラフィックが特定の基準に一致するかどうかに基づいて、トラフィックを組織化します。スイッチはパケットを受信すると、すべての主要なパケット フィールド（Class of Service [CoS; サービス クラス]、Differentiated Service Code Point [DSCP]、または IP precedence）を識別します。スイッチは、この内容または Access Control List（ACL; アクセス コントロール リスト）検索に基づいて、パケットを分類します。詳細については、「分類」（P.34-6）を参照してください。
- パケット ポリシングは 着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを決定します。Committed Information Rate（CIR; 認定情報レート）および Peak Information Rate（PIR; 最大情報レート）を設定し、CIR および PIR に適合するパケット（conform-action）、PIR には適合するが CIR には適合しないパケット（exceed-action）、および PIR 値を超えるパケット（violate-action）で実行するアクションを設定できます。詳細については、「ポリシング」（P.34-16）を参照してください。
- パケットの優先順位付けまたはマーキングは、分類およびポリサー情報を評価して、実行するアクションを決定します。分類に属するすべてのパケットを、マーキングできます。ポリサーを設定した場合、許可された帯域幅要件（bps）に一致するまたは超過するパケットを条件付きで通過、廃棄、または再分類できます。詳細については、「マーキング」（P.34-22）を参照してください。
- 輻輳管理は、キューイングおよびスケジューリング アルゴリズムを使用して、ポートから発信されるトラフィックをキューイングおよびソートします。スイッチは、スケジューリングおよびトラフィック制限機能（Class-Based Weighted Fair Queuing [CBWFQ; クラスベース均等化キューイング]、クラスベース トラフィック シェーピング、ポート シェーピング、およびクラスベース プライオリティ キューイング）をサポートします。他のトラフィック キューの処理中でも、特定のトラフィック クラスに保証された帯域幅を割り当てることができます。詳細については、「輻輳管理およびスケジューリング」（P.34-27）を参照してください。
- スイッチ上でのキューイングは輻輳回避メカニズムである Weighted Tail-Drop（WTD）アルゴリズムによって拡張されます。WTD では、分類に基づいてトラフィック クラスを区別し、キュー サイズ（パケット数）を調整します。詳細については、「輻輳回避およびキューイング」（P.34-34）を参照してください。

ここでは、次の内容について説明します。

- 「MQC」（P.34-3）
- 「入力ポリシーおよび出力ポリシー」（P.34-4）
- 「分類」（P.34-6）
- 「テーブル マップ」（P.34-15）
- 「ポリシング」（P.34-16）

- 「マーキング」（P.34-22）
- 「輻輳管理およびスケジューリング」（P.34-27）
- 「輻輳回避およびキューイング」（P.34-34）

MQC

MQC により、ユーザはトラフィック ポリシーを作成し、それらをインターフェイスに適用できます。トラフィック ポリシーには、トラフィック クラスおよび 1 つまたは複数の QoS 機能が含まれます。トラフィックの分類には、トラフィック クラスを使用します。また、トラフィック ポリシーの QoS 機能により、分類されたトラフィックの処理方法を決定します。

MQC を設定する手順は、次のとおりです。

ステップ 1　トラフィック クラスを定義します。

class-map [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用して、トラフィック クラスを定義し、クラスマップ コンフィギュレーション モードを開始します。トラフィック クラスは、名前、設定済み **match** コマンドの評価方法の指示（クラス マップで複数の match コマンドが設定されている場合）、および一連の **match** コマンドの 3 つの要素で構成されます。

- **class-map** コマンド ラインで、トラフィック クラスの名前を指定し、クラスマップ コンフィギュレーション モードを開始します。
- **class-map match-any** または **class-map match-all** を入力することにより、次の match コマンドを評価するためのキーワードを任意で指定できます。**match-any** を指定した場合、評価されるトラフィックは指定の基準のいずれか *1* つに一致する必要があります。**match-all** を指定した場合、評価されるトラフィックは指定の基準の *すべて* に一致する必要があります。**match-all** クラス マップには、1 つの match 文しか含めることができませんが、**match-any** クラス マップには複数の match 文を含めることができます。

（注）　**match-all** または **match-any** を入力しない場合、デフォルトは match-all になります。

- パケット分類のための基準を指定するには、**match** クラス マップ コンフィギュレーション コマンドを使用します。パケットが指定の基準に一致する場合、このパケットはクラスのメンバーと見なされて、トラフィック ポリシーで設定された QoS 仕様に従って転送されます。いずれの基準にも一致しないパケットは、デフォルト トラフィック クラスのメンバーとして分類されます。

ステップ 2　トラフィック ポリシーを作成し、1 つまたは複数の QoS 機能にトラフィック クラスを関連付けます。

policy-map *policy-map-name* グローバル コンフィギュレーション コマンドを使用して、トラフィック ポリシーを作成し、ポリシーマップ コンフィギュレーション モードを開始します。トラフィック ポリシーでは、QoS 機能を定義して、指定されたトラフィック クラスに関連付けます。トラフィック ポリシーは、名前、トラフィック クラス（**class** ポリシーマップ コンフィギュレーション コマンドにより指定される）、およびそのクラスで設定された QoS ポリシーの 3 つの要素で構成されます。

- **policy-map** コマンド ラインで、トラフィック ポリシーの名前を指定し、ポリシーマップ コンフィギュレーション モードを開始します。
- ポリシーマップ コンフィギュレーション モードで、指定のポリシーに対するトラフィックの分類で使用されるトラフィック クラス名を入力して、ポリシーマップ クラス コンフィギュレーション モードを開始します。

- ポリシーマップ クラス コンフィギュレーション モードで、QoS 機能を開始すると、分類されたトラフィックに適用できます。たとえば、入力ポリシー マップに、**set**、**police**、または **police aggregate** コマンドを使用したり、出力ポリシー マップに、**bandwidth**、**priority**、**queue-limit**、または **shape average** コマンドを使用できます。

（注）　1 つのパケットは、トラフィック ポリシー内の 1 つのトラフィック クラスにだけ一致できます。パケットがトラフィック ポリシー内の複数のトラフィック クラスに一致する場合、ポリシーで定義された最初のトラフィック クラスが使用されます。パケットに複数の一致基準を設定するには、単一のトラフィック ポリシーに複数のトラフィック クラスを関連付けます。

ステップ 3　インターフェイスにトラフィック ポリシーを付加します。

service-policy インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスで送受信されるパケット用にポリシー マップをインターフェイスに付加できます。トラフィック ポリシーの特性を着信または発信パケットに適用するかどうかを指定する必要があります。たとえば、**service-policy output class1** インターフェイス コンフィギュレーション コマンドを入力すると、*class1* という名前のトラフィック ポリシーのすべての特性が、指定されたインターフェイスに付加されます。指定されたインターフェイスから発信されるすべてのパケットは、*class1* という名前のトラフィック ポリシーで指定された基準に従って評価されます。

（注）　**no** policy-map コンフィギュレーション コマンドまたは **no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシー マップを削除する場合、ポリシー マップが消去されているインターフェイスの一覧を示する警告メッセージが表示されます。ポリシー マップは消去および削除されます。たとえば、次のようなメッセージが表示されます。

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

入力ポリシーおよび出力ポリシー

ポリシー マップは、入力ポリシー マップまたは出力ポリシー マップのいずれかになり、スイッチでパケットが送受信される際に、インターフェイスに適用されたサービス ポリシーによって付加されます。入力ポリシー マップは、受信されたトラフィック上でポリシングおよびマーキングを実行します。ポリシングされたパケットが最大許容レートを超過している場合、廃棄されるか、またはプライオリティが低くなります（マーク ダウン）。出力ポリシー マップは、スイッチから発信されるトラフィック上でスケジューリングおよびキューイングを実行します。

入力ポリシーと出力ポリシーは、基本構造は同じですが規制する特性が異なります。図 34-2 に、入力ポリシーと出力ポリシーの関係を示します。

最大 256 のポリシー マップを定義できます。

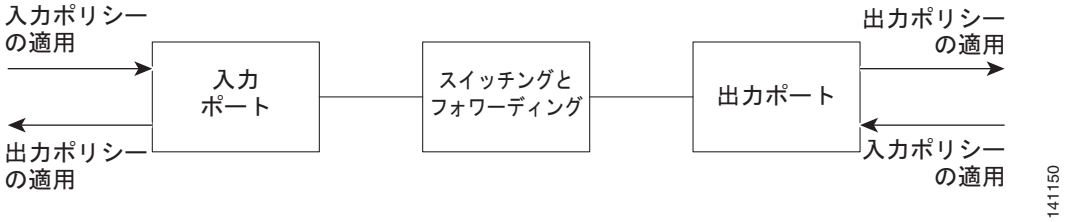
ME-3400 上に設定できるポリサー プロファイルの数は 254 です。ME-3400E でサポートされているポリサー インスタンスの数は 1024 - 1 で、スイッチ上のインターフェイス数より多い数です。24 ポート スイッチでは、使用できるポリサー インスタンスの数は 999 です。ポリサー プロファイルは複数のインスタンスで使用できます。

1 つのインターフェイスには、入力ポリシー マップと出力ポリシー マップを 1 つずつ適用できます。

CPU 保護がイネーブルになっている場合（デフォルト）、ポート当たり 45 の入力ポリサーを設定できます。**no policer cpu uni all** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードして CPU 保護をディセーブルにすると、ユーザ定義クラスにはポート当たり最大 63 のポリ

サー（すべての 4 番目のポート上で 62）および class-default に 1 つのポリサーを設定できます。**show policer cpu uni-eni** {**drop** | **rate**} 特権 EXEC コマンドを入力し、CPU 保護がイネーブルになっているかどうか確認できます。

図 34-2　　入力ポリシーおよび出力ポリシーの関係



入力ポリシー マップ

入力ポリシー マップの分類基準には、CoS、DSCP、または IP precedence 値のマッチング、または Access Control List（ACL; アクセス コントロール リスト）か VLAN ID（ポート単位、VLAN QoS 単位）のマッチングが含まれます。入力ポリシー マップでは、次のいずれかのアクションを実行できます。

- CoS、DSCP、IP precedence、または QoS グループ値の設定、もしくはマーキング
- 個別のポリシング
- 集約ポリシング

アクセス グループまたは VLAN ID の照合は入力ポリシーだけで実行され、QoS グループの照合は出力ポリシーでだけ実行されます。入力ポリシーに割り当てられた QoS グループ番号を、出力ポリシーで照合できます。クラスの **class-default** は、ポリシー マップで他のいずれのクラスとも明示的に一致しない任意のトラフィックに対して、ポリシー マップで使用されます。入力ポリシー マップでは、**bandwidth**、**queue-limit**、**priority**、および **shape average** などのキューイングおよびスケジューリング キーワードはサポートされていません。

入力ポリシー マップの最大クラス数は 64 + **class-default** です。入力ポリシーには、最大 64 のクラスを設定できます。

出力ポリシー マップ

出力ポリシー マップの分類基準には、CoS、DSCP、IP Precedence、または QoS グループ値のマッチングが含まれます。出力ポリシー マップでは、次のいずれかのアクションを実行できます。

- キューイング（**queue-limit**）
- スケジューリング（**bandwidth**、**priority**、**shape average**）

出力ポリシー マップでは、アクセス グループのマッチングをサポートしません。その代わり、入力ポリシー マップの該当するアクセス グループを照合し、QoS グループを設定することにより、QoS グループを使用できます。出力ポリシー マップでは、QoS グループを照合できます。詳細については、「QoS グループ に基づく分類」（P.34-12）を参照してください。

出力ポリシーは、マーキングまたはポリシングをサポートしません（ポリシングのあるプライオリティの場合は除く）。スイッチ上では、出力パケットのマーキングは実行されません（出力ポリシーには **set** コマンドが含まれません）。

クラスの **class-default** は、ポリシー マップで他のいずれのクラスとも明示的に一致しない任意のトラフィックに対して、ポリシー マップで使用されます。出力ポートには最大 4 つのキューがあるため、出力ポリシー マップには最大 4 つのクラスを設定できます（class-defalt を含む）。

出力ポートに付加される出力ポリシー マップは、パケットの入力ポートに付加された入力ポリシー マップですでに一致しているパケットだけを照合できます。スイッチ上の任意のポートまたはすべてのポートに、出力ポリシー マップを付加できます。スイッチは各ポートに固有の出力ポリシー マップの設定および付加をサポートしています。ただし、これらの出力ポリシー マップには、それぞれ固有のキュー制限を 3 つしか設定できません。これら 3 つの固有のキュー制限設定は、スイッチ上にあるポート数に応じた数の出力ポリシー マップに含まれます。帯域幅、プライオリティ、またはシェーピングの設定には制限はありません。

cpu traffic qos [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] グローバル コンフィギュレーション コマンドを使用して、CPU が生成したトラフィックの出力ポリシー分類基準を設定できます。

分類

分類では、パケット ヘッダーのフィールドを検査して、トラフィックの種類を区別します。スイッチはパケットを受信すると、ヘッダーを検査して、すべての主要なパケット フィールドを識別します。パケットは、パケットの ACL、DSCP 値、CoS 値、IP precedence 値、または VLAN ID に基づいて分類されます。図 34-3 に、分類情報を伝達するのに、非推奨 IP Type of Service（ToS; サービス タイプ）フィールドから 6 ビットを使用する、レイヤ 2 またはレイヤ 3 IP パケット ヘッダーで伝達される分類情報の例を示します。

- レイヤ 2 の IEEE 802.1Q トランクとして設定されたポートでは、ネイティブ VLAN（仮想 LAN）のトラフィックを除き、すべてのトラフィックが 802.1Q フレームに収められます。レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット（ユーザ プライオリティ ビット）で CoS 値を、下位 12 ビットで VLAN ID 値を伝達します。その他のフレーム タイプでは、レイヤ 2 の CoS 値を伝達できません。

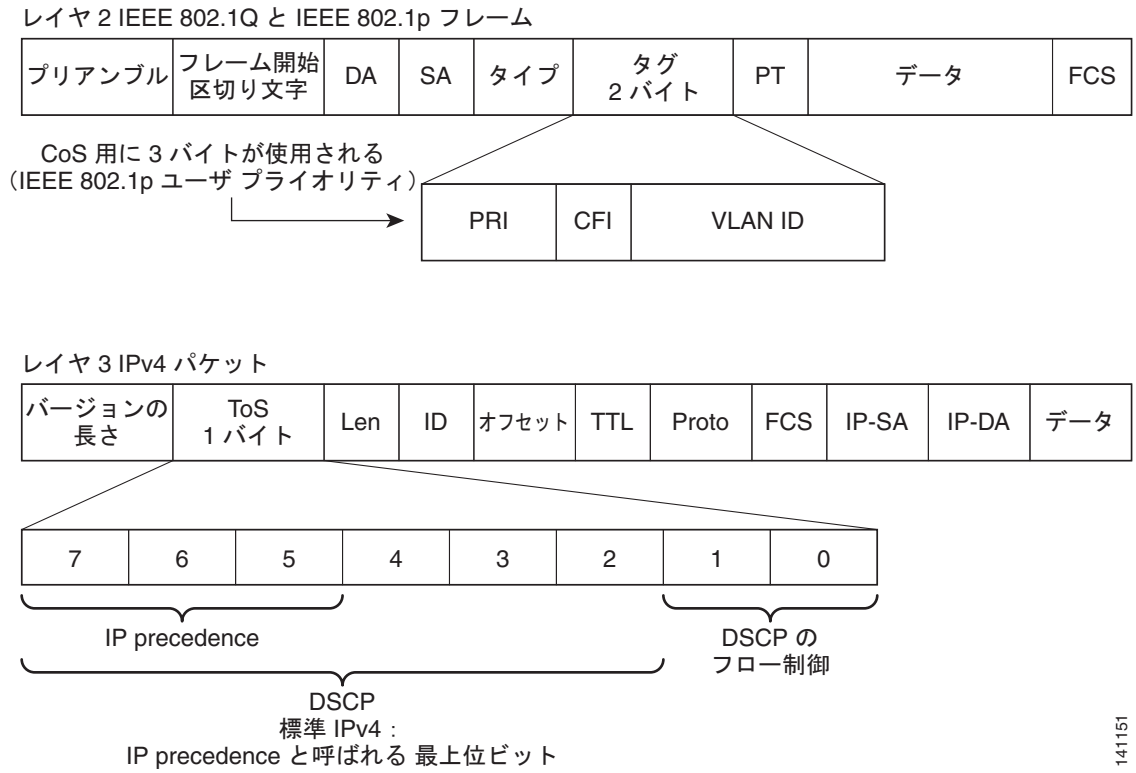
  レイヤ 2 CoS 値の範囲は 0 ～ 7 です。

- レイヤ 3 IP パケットは、IP precedence 値または DSCP 値のいずれかを伝達します。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

  IP precedence 値の範囲は、0 ～ 7 です。DSCP 値の範囲は、0 ～ 63 です。

- 出力は、レイヤ 2 またはレイヤ 3 のマーキング タイプ、マーキング値、およびパケット タイプに基づいて再マーキングされます。

図 34-3　フレームおよびパケットの QoS 分類レイヤ



ここでは、分類に関するその他の情報について説明します。

- 「クラス マップ」（P.34-7）
- 「match コマンド」（P.34-8）
- 「レイヤ 2 CoS に基づく分類」（P.34-8）
- 「IP precedence に基づく分類」（P.34-9）
- 「IP DSCP に基づく分類」（P.34-9）
- 「分類の比較」（P.34-11）
- 「QoS ACL に基づく分類」（P.34-11）
- 「QoS グループ に基づく分類」（P.34-12）
- 「VLAN ID に基づく分類」（P.34-13）

クラス マップ

前述のとおり、MQC クラス マップを使用して、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別します。クラス マップでは、特定のトラフィック フローとの比較を行い、さらにそれを分類するために使用する基準を定義します。複数のタイプのトラフィックを分類する場合は、別のクラス マップを作成し、異なる名前を付けることができます。クラスマップ名を指定して **class-map** コマンドを入力すると、クラスマップ コンフィギュレーション モードが開始されます。このモードでは **match** クラス マップ コンフィギュレーション コマンドを使用し、トラフィックの一致基準を定義します。パケットはクラスマップ基準に照合されてから、ポリシー マップで指定された関連アクションが実行されます。

分類では、複数の基準に照合できます。また、**class map match-all** *class-map name* グローバル コンフィギュレーション コマンドを使用して、クラス マップ コンフィギュレーション モードを開始することにより、パケット ヘッダー内にクラス マップのすべての一致基準が存在する必要があるクラス マップを作成できます。

（注）　**match-all** クラス マップで設定できる match エントリは 1 つだけです。

class map match-any *class-map name* グローバル コンフィギュレーション コマンドを使用すると、リストされた基準のいずれかを使用する分類を定義できます。

（注）　**match-all** または **match-any** を入力しない場合、デフォルトは match-all になります。match-all クラス マップでは、複数の分類基準（match 文）を設定できません。一致条件を含まないクラス マップは、デフォルトで **match-all** となります。

match コマンド

パケットの分類に使用される内容の種類を設定するには、**match** クラス マップ コンフィギュレーション コマンドを使用して、分類基準を指定します。設定された基準に一致するパケットは、特定のクラスに属し、指定されたポリシーに従って転送されます。たとえば、CoS 値、IP DSCP 値、および IP precedence 値で **match** クラス マップ コマンドを使用できます。これらの値は、パケット上でマーキングと呼ばれます。また、アクセス グループ、QoS グループ、または VLAN ID、またはポート単位、VLAN QoS 単位の ID 範囲と照合できます。

- 入力ポリシー マップでは、同じポリシー マップまたはクラス マップ内に IP 分類（**match ip dscp**、**match ip precedence**、**match ip acl**）と非 IP 分類（**match cos** または **match mac acl**）を設定できません。
- レイヤ 2 だけ分類が設定された入力ポリシーマップが、ルーテッド ポートまたはルーテッド Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を含むスイッチ ポートに付加されている場合、サービス ポリシーはルーティング適格トラフィック上ではなく、スイッチング適格トラフィック上でだけ機能します。
- 802.1Q トンネル ポート上でトラフィックを分類するには、MAC ACL に基づくレイヤ 2 分類を含む入力ポリシー マップだけが使用できます。レイヤ 3 分類、match レイヤ 2 CoS 分類、またはポート単位、VLAN 単位のポリシーが設定された入力ポリシー マップは、トンネル ポート上でサポートされません。
- 出力ポリシー マップでは、異なるクラス マップで同じ分類基準（つまり、同じ match 修飾子および match 値）を使用できません。

次に、クラス マップ *example* を作成して、リストされた基準のいずれかに一致するクラスを定義する例を示します。この例では、DSCP 値 が 32 または 40 のパケットが受信された場合、このパケットはクラス マップにより識別（分類）されます。

```
Switch(config)# class-map match-any example
Switch(config-cmap)# match ip dscp 32
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# exit
```

レイヤ 2 CoS に基づく分類

match コマンドを使用することにより、CoS 値（0 ～ 7 の範囲）に基づいてレイヤ 2 トラフィックを分類できます。

（注）　**match cos** コマンドは、レイヤ 2 802.1Q トランク ポートでだけサポートされます。

次に、CoS 値 5 に一致するクラス マップを作成する例を示します。

```
Switch(config)# class-map premium
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

IP precedence に基づく分類

IPv4 トラフィックは、パケットの IP precedence 値（0 ～ 7 の範囲）に基づいて分類できます。

次に、IP precedence 値 4 に一致するクラス マップを作成する例を示します。

```
Switch(config)# class-map sample
Switch(config-cmap)# match ip precedence 4
Switch(config-cmap)# exit
```

IP DSCP に基づく分類

IP DSCP 値に基づいて IPv4 トラフィックを分類し、**match ip dscp** クラス マップ コンフィギュレーション コマンドを入力する場合、次のいくつかの分類オプションがあります。

- 特定の DSCP 値（0 ～ 63）の入力
- IP precedence 値および DSCP 値 0 に対応するデフォルト サービスの使用。デフォルトの Per Hop Behavior（PHB）は通常、ベストエフォート サービスです。
- DSCP 値をバイナリ形式で入力する、Assured Forwarding（AF; 保証型転送）の使用。AF では、輻輳が発生し、トラフィックが最大許容レートを超過していない場合に、パケットの特定のクラスが転送される相対的な確率を設定します。AF *per-hop behavior* により、IP パケットが異なる 4 つの AF クラス（AF11 ～ 13 [最高]、AF21 ～ 23、AF31 ～ 33、および AF41 ～ 43 [最低]）で配信されます。各 AF クラスには、特定のバッファ スペース容量および廃棄確立が割り当てられ、DSCP 番号がバイナリ形式で指定されます。輻輳が発生すると、パケットの廃棄優先順位により、クラス内のパケットの相対的な重要性が決定されます。AF41 では、パケットがネットワークの端から端へ転送される確立が最も高くなります。
- 1 ～ 7 の範囲の Class Selector（CS ; クラス セレクタ）サービス値の入力（パケットの ToS フィールドの IP precedence ビットに対応）
- Expedited Forwarding（EF; 急送型転送）の使用による低遅延パスの指定。これは、DSCP 値 46 に対応します。EF サービスでは、プライオリティ キューイングを使用して、プライオリティの低いトラフィック クラスをプリエンプトします。

次に、使用可能な分類オプションを表示します。

```
Switch(config-cmap)# match ip dscp ?
  <0-63>   Differentiated services codepoint value
  af11     Match packets with AF11 dscp (001010)
  af12     Match packets with AF12 dscp (001100)
  af13     Match packets with AF13 dscp (001110)
  af21     Match packets with AF21 dscp (010010)
  af22     Match packets with AF22 dscp (010100)
  af23     Match packets with AF23 dscp (010110)
  af31     Match packets with AF31 dscp (011010)
  af32     Match packets with AF32 dscp (011100)
  af33     Match packets with AF33 dscp (011110)
  af41     Match packets with AF41 dscp (100010)
  af42     Match packets with AF42 dscp (100100)
```

```
af43     Match packets with AF43 dscp (100110)
cs1      Match packets with CS1(precedence 1) dscp (001000)
cs2      Match packets with CS2(precedence 2) dscp (010000)
cs3      Match packets with CS3(precedence 3) dscp (011000)
cs4      Match packets with CS4(precedence 4) dscp (100000)
cs5      Match packets with CS5(precedence 5) dscp (101000)
cs6      Match packets with CS6(precedence 6) dscp (110000)
cs7      Match packets with CS7(precedence 7) dscp (111000)
default  Match packets with default dscp (000000)
ef       Match packets with EF dscp (101110)
```

DSCP のプライオリティ設定の詳細については、RFC-2597（AF PHB）、RFC-2598（EF）、または RFC-2475（DSCP）を参照してください。

802.1Q トンネリング CoS マッピング

ME-3400E では、Customer VLAN-ID（C-VLAN; カスタマー VLAN）から Service-Provider VLAN-ID（S-VLAN; サービス プロバイダー VLAN）への VLAN マッピングがサポートされています。「VLAN マッピングの概要」（P.14-8）を参照してください。QoS の場合、スイッチは Customer CoS（C-CoS; カスタマー CoS）または Customer DSCP（C-DSCP: カスタマー DSCP）値から Service-Provider CoS（S-CoS; サービス プロバイダー CoS）を設定でき、従来の 802.1Q トンネリング（QinQ）または選択した QinQ VLAN マッピングにより任意のトラフィックについて内部 CoS を外部 CoS にマッピングできます。このデフォルトにより、カスタマー CoS がサービス プロバイダー ネットワークにコピーされます。

ME-3400E では、トランク ポートで従来の QinQ および選択した QinQ について C-CoS から S-CoS への伝播がサポートされています。これはデフォルト動作であり、設定は必要ありません。1 対 2 VLAN マッピングを使用し、レイヤ 2 トランク ポートで従来の QinQ または選択した QinQ を設定する場合、またスイッチで C-DSCP から S-CoS を設定できます。

VLAN マッピングに設定された 802.1Q トンネル ポートまたはトランク ポート上のスイッチを開始するトラフィックについては、スイッチは、カスタマー パケット ヘッダーを検査し、カスタマー CoS 値またはカスタマー DSCP 値からサービス プロバイダー CoS 値（S-CoS）を設定する機能を備えています。

802.1Q マップ ポートでの CoS マッチングは、次のように設定されます。

- （トンネル ポートまたはトランク ポート上の）802.1Q トンネリングまたは（トランク ポート上の）選択した 802.1Q に設定されたインターフェイスで、インターフェイス（C-CoS）上で受信した VLAN タグ（内部 VLAN または C-VLAN）の CoS 値は、デフォルトでトンネル VLAN タグ（外部 VLAN または S-VLAN）に自動的に反映されます。
- **set cos** ポリシー マップ クラス コンフィギュレーション コマンドは常に、処理が完了した後、最も外側の VLAN タグである S-VLAN-ID に適用されます。たとえば、802.1Q トンネルでは、**set cos** コマンドを入力すると、カプセル化されたパケットの外部タグの CoS 値だけ変更されます。
- **match dscp** クラス マップ コンフィギュレーション コマンドを入力してポリシーを設定し、QinQ および選択した QinQ マッピング インターフェイスの **set cos** ポリシー マップ クラス コンフィギュレーション コマンドを入力すると、DSCP の一致によりカプセル化値の外部 CoS が設定されます。
- 外部 VLAN が一致した場合に DSCP を設定できます。
- 従来の QinQ マッピングまたは選択した QinQ マッピングに設定したインターフェイスで **match cos** コマンドを入力すると、外部 CoS、つまり反映された内部 Cos（C-CoS）に対して一致します。

分類の比較

表 34-1 に、一般的なトラフィックタイプに推奨される IP DSCP 値、IP precedence 値、および CoS 値を示します。

表 34-1　一般的なトラフィック分類

トラフィック タイプ	ホップ単位の DSCP	DSCP（10 進数）	IP precedence	CoS
音声ベアラ：プライオリティ キュー、または最高のサービス ウェイトおよび最低の廃棄プライオリティを持つキューのトラフィック	EF	46	5	5
音声制御：音声ゲートウェイまたは音声アプリケーション サーバからの、コール セットアップに関連したシグナリング トラフィック	AF31	26	3	3
ビデオ会議：ほとんどのネットワークで、IP 上でのビデオ会議には、損失、遅延、および遅延の種類に関して Voice over IP（VoIP）トラフィックと同様な要件があります。	AF41	34	4	4
ストリーミング ビデオ：損失、遅延、および遅延の種類に関して高い耐性を持つ、比較的高い帯域幅のアプリケーション。通常、E メールおよび Web 参照のような日常的なバックグラウンド アプリケーションよりも重要と見なされます。	AF13	14	1	1
ミッション クリティカル データ（ゴールド データ）：企業の業務上重要な、遅延に影響されやすいアプリケーション				
レベル 1	AF21	18	2	2
レベル 2	AF22	20	2	2
レベル 3	AF23	22	2	2
重要度が低いデータ（シルバー データ）：クリティカルではないが、比較的重要なデータ				
レベル 1	AF11	10	1	1
レベル 2	AF12	12	1	1
レベル 3	AF13	14	1	1
ベストエフォート データ（ブロンズ データ）：重要度に関係なく、すべての非対話型トラフィックを含むその他のトラフィック	デフォルト	0	0	0
ベストエフォート データよりも重要でないデータ：クリティカルでなく、優先度が低い、帯域幅を消費するデータ トラフィック。これは、最初に廃棄されるトラフィック タイプです。				
レベル 1		2	0	0
レベル 2		4	0	0
レベル 3		6	0	0

QoS ACL に基づく分類

パケットは、入力ポリシー マップで ACL 検索に基づいても分類されます。ACL 分類は、入力ポリシー マップの QoS グループまたは QoS 番号を割り当てることにより、出力ポリシーに伝達されます。ACL 検索に基づいて分類する場合は、まず IP ACL または MAC ACL を作成します。クラス マップを設定し、**match access-group** {*acl-number* | *acl name*} クラス マップ コンフィギュレーション コマンドを使用して、ポリシー マップにクラス マップを付加します。

（注）　出力ポリシー マップには、**match access-group** を設定できません。

IP 標準、IP 拡張、またはレイヤ 2 MAC ACL を使用すると、同じ特性（クラス）を持つパケットのグループを定義できます。レイヤ 3 およびレイヤ 4 パラメータに基づいて IP トラフィックを分類する IP ACL を設定するには、**access-list** グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 パラメータに基づいて IP および 非 IP トラフィックを分類するレイヤ 2 MAC ACL を設定するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

（注）　IP フラグメントを設定済みの IP 拡張 ACL に照合して、QoS を実行できません。IP フラグメントはベストエフォート型として送信されます。IP フラグメントは IP ヘッダー内のフィールドで指定されます。

match access-group コマンドでは、許可アクションが含まれる ACL だけを使用できます。拒否アクションが含まれる ACL は、QoS ポリシーで照合されません。

（注）　入力ポリシー マップのクラスごとに 1 つのアクセス グループだけがサポートされます。

QoS グループ に基づく分類

QoS グループは、スイッチがパケットを特定のクラスのメンバーとして識別するのに使用する内部ラベルです。このラベルはパケット ヘッダーには含まれず、ラベルを設定するスイッチに制限されています。QoS グループにより、明示的にパケットをマーキング（変更）しない後続の QoS アクションにパケットのタグ付け方法が提供されます。次に、入力ポリシー マップから出力ポリシー マップに ACL 一致を伝達できます。

QoS グループは、入力側で識別されて出力側で使用されます。また、入力ポリシーに割り当てられて、出力ポリシーのパケットを識別します。図 34-3 を参照してください。QoS グループにより、出力ポリシーの特定のアクションに対して、入力トラフィックの異なるクラスが集約されます。

図 34-4　　QoS グループ

QoS グループを使用すると、出力ポート上での同じ QoS 処理に対する入力クラス間およびポリシー マップ間の複数の入力ストリームを集約できます。同じ出力処理が必要なすべてのストリームに、入力ポリシー マップ内の同一の QoS グループ番号を割り当てて、出力ポリシー マップの QoS グループ番号に照合して、必要なキューイングおよびスケジューリング アクションを指定します。

また、QoS グループを使用すると、トラフィックが入力インターフェイスに基づいて出力側で異なる方法で処理される必要がある場合に、特定のインターフェイスに着信するトラフィックを識別できます。

QoS グループを使用すると、VLAN 上のブリッジド トラフィックに対して、出力インターフェイス上でポート単位、VLAN 単位の QoS 出力ポリシーを設定できます。ポート単位、VLAN 単位の入力ポリシーを設定することにより、入力インターフェイス上の VLAN に QoS グループ番号を割り当てます。次に、出力側での分類に同一の QoS グループ番号を使用します。ブリッジド トラフィックの VLAN は、スイッチを介して転送される間は変更されないため、入力 VLAN に割り当てられる QoS グループ番号は、出力インターフェイスで同じ VLAN を識別するのに使用できます。

cpu traffic qos [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] グローバル コンフィギュレーション コマンドを使用して、CPU が生成したトラフィックの QoS グループ番号を設定できます。

QoS グループ番号は、入力側でインターフェイス、VLAN、トラフィック フロー、および集約トラフィックの任意の組み合せに個別に割り当てできます。QoS グループ番号を割り当てるには、入力ポリシー マップの QoS グループ マーキングと同時に、入力ポリシー マップ内の同一サービス クラスに必要なその他のマーキングまたはポリシング アクションを設定します。出力分類では QoS グループだけを使用する必要があるため、これにより、入力マーキングおよび入力ポリシング機能を出力分類機能（必要な場合）から切り離すことができます。

ACL 分類を出力ポリシーに伝達するには、入力側でパケットを指定する QoS 番号を割り当てます。次の例では、出力ポリシーであとで処理できるように、特定のパケットを QoS グループ 1 の一部として識別します。

```
Switch(config)# policy-map in-gold-policy
Switch(config-pmap)# class in-class1
Switch(config-pmap-c)# set qos-group 1
Switch(config-cmap-c)# exit
Switch(config-cmap)# exit
```

set qos-group コマンドは、入力ポリシーでだけ使用します。割り当てられた QoS グループ識別子は、パケットにマーキングまたは変更を行わずに出力ポリシーであとで使用されます。**match qos-group** は、出力ポリシーで使用します。

（注）　入力ポリシー マップには、**match qos-group** を設定できません。

次に、出力ポリシーを作成して、入力ポリシー マップ *in-gold-policy* で作成された QoS グループを照合する例を示します。*qos-group 1* として内部的にタグ付けされたトラフィックは、出力ポリシーで識別され、処理されます。

```
Switch(config)# class-map out-class1
Switch(config-cmap)# match qos-group 1
Switch(config-cmap)# exit
```

スイッチは、最大 100 の QoS グループをサポートします。

VLAN ID に基づく分類

VLAN ID に基づく分類により、所定のインターフェイスにユーザが指定した VLAN 上で送信されるフレームに QoS ポリシーを適用できます。トランク ポートでの VLAN 単位の分類に階層型ポリシー マップを使用できます。アクセス ポートでは単一 VLAN のトラフィックを伝送するため、VLAN 単位の分類は必要ありません。トランク ポートではないポートに、ポート単位、VLAN 単位の階層型ポリシーを付加しようとすると、設定は拒否されます。

スイッチでは、*parent* レベルおよび *child* レベルの 2 つのポリシー レベルがサポートされています。QoS の親子構造により、親ポリシー内の子ポリシーを参照して、特定のトラフィック タイプをさらに細かく制御できるようになります。ポート単位、VLAN 単位の QoS の場合、親レベルのクラス マップは VLAN 一致基準だけを指定し、子レベルのクラス マップは親レベルのクラス マップに一致するフレームをより詳細に分類します。親レベルで複数のサービス クラスを設定して、各種 VLAN の組み合せを照合し、任意の子ポリシー マップを使用して、親のサービス クラスごとに個別の QoS ポリシーを適用できます。

（注） ポート単位、VLAN 単位の親レベルのクラス マップでは、子ポリシー アソシエーションだけをサポートします。いずれのアクションも設定できません。さらに、親レベルのクラス マップでは、クラスの **class-default** のアクションまたは子ポリシー アソシエーションを設定できません。

ポート単位、VLAN 単位 QoS には、次の制限事項があります。

- ポート単位、VLAN 単位の階層型ポリシー マップは、トランク ポートにだけ適用できます。
- VLAN ID に基づく分類は、ポート単位、VLAN 単位の階層型ポリシー マップの親レベルでだけ設定できます。
- VLAN または VLAN のセットに付加されている子ポリシー マップに、レイヤ 3 分類（**match ip dscp**、**match ip precedence**、**match IP ACL**）だけが含まれる場合、これらの VLAN は、必ずポート単位、VLAN 単位ポリシーが付加されているポート上でだけ実行されることに注意する必要があります。この制限事項に従わない場合は、これらの VLAN 上のスイッチに着信するトラフィックの QoS 動作が不適切になる場合があります。
- また、ポート単位 VLAN 単位が適用されるトランク ポート上で、**switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用して、VLAN メンバーシップを制限することも推奨します。レイヤ 3 分類が設定されたポート単位、VLAN 単位のポリシーが含まれるトランク ポート間で VLAN メンバーシップが重複した場合も、予期せぬ QoS 動作が発生する可能性があります。

次の例では、子レベルのポリシー マップのクラス マップが音声、データ、およびビデオ トラフィックの一致基準を指定して、子ポリシー マップが各トラフィック タイプの入力ポリシングに対するアクションを設定します。親レベルのポリシー マップは、指定されたポート上の子ポリシー マップが適用される VLAN を指定します。

```
Switch(config)# class-map match-any dscp-1 data
Switch(config-cmap)# match ip dscp 1
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```

（注） また、一致基準を **match vlan 100 200 300** と入力した場合でも、同じ結果になります。

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
```

```
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-1 data
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# set ip precedence 4
Switch(config-pmap-c)# exit

Switch(config)# policy-map parent-customer-1
Switch(config-pmap)# class customer-1-vlan
Switch(config-pmap-c)# service-policy ingress-policy-1
Switch(config-pmap-c)# exit

Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy input customer-1-ingress
Switch(config-pmap-c)# exit
```

（注）　各ポート単位、VLAN 単位の親ポリシー クラス（**class-default** を除く）には、子ポリシー アソシエーションを設定できます。

設定上の注意事項および制限事項を含む設定情報については、「階層型入力ポリシー マップを含むポート単位、VLAN 単位 QoS の設定」（P.34-60）を参照してください。

テーブル マップ

テーブル マップを使用すると、単一のコマンドで多数のトラフィック フローを管理できます。**set** コマンドで指定したテーブル マップを、ポリシーのマークダウン マッピングとして使用できます。また、テーブル マップを使用すると、多数の明示的な match および set を設定せずに、着信 QoS マーキングを代わりのマーキングにマッピングできます。テーブル マップは、入力ポリシー マップでだけ使用されます。

テーブル マップは、次の用途に使用されます。

- 特定の CoS、DSCP、または IP precedence 値と特定の CoS、DSCP、または IP precedence 値を相互に関連付ける
- CoS、DSCP、または IP precedence 値をマーク ダウンする
- マッピングされていない値に、デフォルトを割り当てる

テーブル マップには、次のデフォルト アクションのいずれかが含まれます。

- **default** *default-value*：すべてのマッピングされていない値に特定のデフォルト値（0 ～ 63）を適用します。
- **default copy**：すべてのマッピングされていない値を別の修飾子の同等な値にマッピングします。
- **default ignore**：マッピングされていない値を変更しません。

次に、特定の CoS 値を DSCP 値にマッピングするテーブルを作成する例を示します。**default** コマンドにより、すべてのマッピングされていない CoS 値が DSCP 値 63 にマッピングされます。

```
Switch(config)# table-map cos-dscp-tablemap
Switch(config-tablemap)# map from 5 to 46
Switch(config-tablemap)# map from 6 to 56
Switch(config-tablemap)# map from 7 to 57
Switch(config-tablemap)# default 63
Switch(config-tablemap)# exit
```

スイッチでは、最大 256 の一意のテーブル マップをサポートしています。テーブル マップでは、最大 64 の異なる **map from–to** エントリを入力できます。スイッチでは、次のテーブル マップがサポートされます。

- DSCP/CoS
- DSCP/precedence
- DSCP/DSCP
- CoS/DSCP
- CoS/precedence
- CoS/CoS
- Precedence/CoS
- precedence/DSCP
- precedence/precedence

テーブル マップは、1 つのパラメータ（CoS、IP precedence、または DSCP のいずれか設定されているもの）だけを変更し、ポリシー マップで **set** コマンドにより設定されている場合、またはポリシング機能で設定されている場合にだけ有効です。個々のポリサーはまた、**violate-action** コマンドをサポートしていますが、集約ポリサーは violate-action によるテーブル マップはサポートしていません。

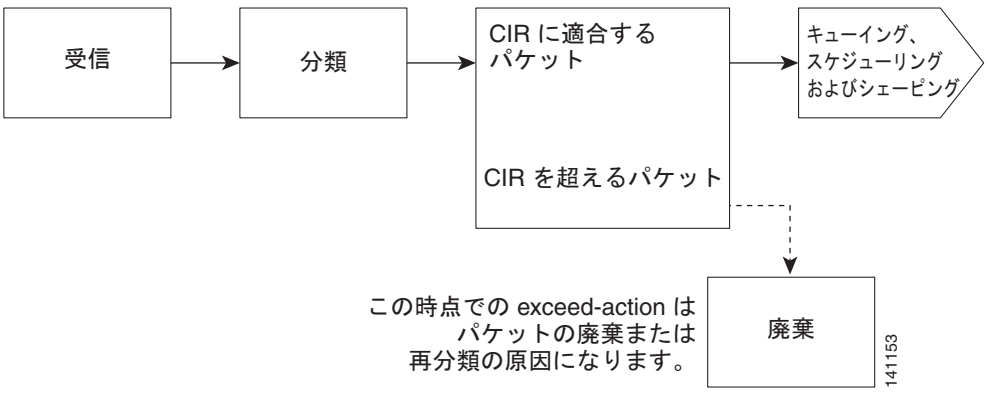
テーブル マップは、出力ポリシー マップでサポートされません。詳細については、「テーブル マップの設定」（P.34-45）を設定してください。

ポリシング

パケットが分類されたあと、図 34-5 に示されるポリシングを使用して、トラフィック クラスを規制できます。ポリシング機能では、特定のトラフィック フローで使用可能な帯域幅量を制限するか、または任意のトラフィック タイプが過剰な帯域幅およびシステム リソースを使用しないようにします。ポリサーは、ポリサーおよびトラフィック クラスの設定プロファイルと着信トラフィックのレートを比較することにより、パケットを適合または不適合として識別します。許容平均レートまたはバースト レートを超過するパケットは、*不適合*または*非適合*となります。これらのパケットは、ポリサーの設定に応じて、廃棄されるかまたは変更（追加処理用にマーキング）されます。

ポリシングは、主に受信インターフェイス上で使用されます。ポリサーを含むポリシー マップは、入力サービス ポリシーに限り付加できます。出力ポリシー マップでは、プライオリティ クラスのポリシングだけが許可されます。「無条件のプライオリティ ポリシング」（P.34-21）を参照してください。

図 34-5　　分類されたパケットのポリシング



ここでは、スイッチでサポートされるポリシング タイプについて説明します。

- 「個別のポリシング」（P.34-17）
- 「集約ポリシング」（P.34-19）
- 「無条件のプライオリティ ポリシング」（P.34-21）

個別のポリシング

個別のポリシングは、入力ポリシー マップにだけ適用されます。ポリシーマップ コンフィギュレーション モードで、**class** コマンドのあとにクラスマップ名を入力して、ポリシーマップ クラス コンフィギュレーション モードを開始します。

ME-3400E スイッチは、個別ポリシングまたは集約ポリシングについて 1-rate、2-color 入力ポリシングおよび 2-rate、3-color のポリシングをサポートします。

1-rate、2-color ポリシングについては、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリサー、トラフィックの認定速度制限、トラフィックの認定バースト サイズ制限、または制限未満（**conform-action**）および制限を越える（**exceed-action**）トラフィックに対して実行するアクションを定義します。バースト サイズ（bc）を指定しない場合は、システムにより適切なバースト サイズ値が算出されます。算出された値は、ほとんどのアプリケーションに適しています。詳細については、「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）を参照してください。

最初のトークン バケットを更新するため、Committed Information Rate（CIR; 認定情報レート）の設定を含む、2-rate ポリサーを設定する場合、2 番目のトークン バケットが更新される Peak Information Rate（PIR; 最大情報レート）も設定します。PIR を設定しない場合、ポリサーは標準 1-rate、2-color ポリサーです。

2-rate、3-color ポリシングについては、指定の CIR および PIR に適合するパケット（conform-action）、PIR には適合するが CIR には適合しないパケット（exceed-action）、および PIR 値を超えるパケット（violate-action）で実行するアクションを任意に設定できます。

- PIR に等しい CIR 値を設定している場合、CIR 以下のトラフィック レート速度は適合範囲内です。CIR を超えるトラフィックは違反範囲に入ります。
- CIR より大きな PIR を設定している場合、CIR 未満のトラフィック レートは適合範囲内です。CIR を超えるが、PIR 以下のトラフィック レートは超過範囲に入ります。PIR を超えるトラフィック レートは違反範囲内です。
- PIR を設定しない場合、ポリサーは 1-rate、2-color ポリサーとして設定されます。

バースト サイズの設定が低すぎると、バースト トラフィックがある状況でスループットが低下する場合があります。バースト サイズの設定が高すぎると、トラフィック レートが高くなりすぎる場合があります。

（注）　ME-3400E では、**show policy-map interface** 特権 EXEC コマンド出力で conform、exceed、および violate の各クラスのバイトレベル統計情報がバイト カウンタでサポートされています。

ポリシー マップを有効にするには、**service-policy input** インターフェイス コンフィギュレーション コマンドを使用し、ポリシー マップを物理ポートに付加します。ポリシングは、受信トラフィックでだけ行われるため、ポリサーは入力サービス ポリシーにだけ付加できます。

次に、CoS 値が 4 のすべての受信トラフィックに対する基本的なポリシングの例を示します。**police** コマンドのあとに続く最初の値は、平均トラフィック レートを 10,000,000 bps に制限し、次の値は追加のバースト サイズ（10 キロバイト）を表します。ポリシーは、ファスト イーサネット ポート 1 に割り当てられます。

```
Switch(config)# class-map video-class
```

```
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police 10000000 10000
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input video-policy
Switch(config-if)# exit
```

conform-action、**exceed-action**、および **violate-action** ポリシー マップ クラス コンフィギュレーション コマンド、または **conform-action**、**exceed-action**、および **violate-action** ポリシー マップ クラス ポリシング コンフィギュレーション コマンドを使用すると、パケットが指定のトラフィック レートに適合するまたは超過する場合に実行するアクションを指定できます。適合アクション、超過アクション、および違反アクションは、パケットを廃棄する、パケットを変更しないで送信する、新しい CoS 値、DSCP 値、IP precedence 値を設定する、または出力側での分類用に QoS グループ値を設定することです。

明示的な値、テーブル マップ、またはその両方を組み合せて、各マーキング アクションを設定できます。テーブル マップでは、特定のトラフィック アトリビュートを示し、それらを他のアトリビュートにマッピング（変換）します。

各サービス クラスで複数の適合アクション、超過アクション、および違反アクションを同時に設定できます。**violate-action** を設定しない場合、デフォルトで違反クラスが **exceed-action** と同じアクションに割り当てられます。

テーブル マップの作成後、ポリシーマップ ポリサーを設定して、テーブル マップを使用します。

（注） 入力ポリシー マップでテーブル マップを使用する場合、テーブル マップの **from** - アクションのプロトコル タイプは、対応する分類のプロトコル タイプと同じである必要があります。たとえば、クラス マップが IP 分類を表す場合、テーブル マップの **from** - タイプ アクションは、**dscp** または **precedence** である必要があります。クラス マップが非 IP 分類を表す場合、テーブル マップの **from** - タイプ アクションは、**cos** である必要があります。

クラスで複数の動作を設定する場合、ポリシーマップ クラス ポリシング コンフィギュレーション モードで複数の適合、超過、または違反の各アクションのエントリを入力する必要があります（次の例を参照）。

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 100000 500000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 4
Switch(config-pmap-c-police)# conform-action set-dscp-transmit dscp table
conform-dscp-to-dscp-mutation
Switch(config-pmap-c-police)# conform-action set-qos-transmit 10
Switch(config-pmap-c-police)# exceed-action set-cos-transmit 2
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table
exceed-dscp-to-dscp-mutation
Switch(config-pmap-c-police)# exceed-action set-qos-transmit 20
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

集約ポリシング

集約ポリシングは、入力ポリシー マップにだけ適用されます。集約ポリサーは、個別のポリサーとは異なり、ポリシー マップ内の複数のトラフィック クラスで共有されます。ME-3400E スイッチは、集約ポリシングについて 1-rate、2-color 入力ポリシングおよび 2-rate、3-color のポリシングをサポートします。

policer aggregate グローバル コンフィギュレーション コマンドを使用して、物理インターフェイスで送受信されるすべてのトラフィックのポリサーを設定できます。集約ポリサーを設定すると、特定のバースト サイズおよび適合アクションと超過アクションを設定できます。バースト サイズ（**bc**）を指定しない場合は、システムにより適切なバースト サイズ値が算出されます。算出された値は、ほとんどのアプリケーションに適しています。

最初のトークン バケットを更新するため、Committed Information Rate（CIR; 認定情報レート）の設定を含む、2-rate ポリサーを設定する場合、2 番目のトークン バケットが更新される Peak Information Rate（PIR; 最大情報レート）も設定します。PIR を設定しない場合、ポリサーは標準 1-rate、2-color ポリサーです。

2-rate、3-color ポリシングについては、指定の CIR および PIR に適合するパケット（conform-action）、PIR には適合するが CIR には適合しないパケット（exceed-action）、および PIR 値を超えるパケット（violate-action）で実行するアクションを任意に設定できます。

（注）　適合アクションが drop に設定されている場合、超過アクションおよび違反アクションは自動的に drop に設定されます。超過アクションが drop に設定されている場合、違反アクションは自動的に drop に設定されます。

- PIR に等しい CIR 値を設定している場合、CIR 以下のトラフィック レート速度は適合範囲内です。CIR を超えるトラフィックは違反範囲に入ります。
- CIR より大きな PIR を設定している場合、CIR 未満のトラフィック レートは適合範囲内です。CIR を超えるが、PIR 以下のトラフィック レートは超過範囲に入ります。PIR を超えるトラフィック レートは違反範囲内です。
- PIR を設定しない場合、ポリサーは 1-rate、2-color ポリサーとして設定されます。

バースト サイズの設定が低すぎると、予想よりトラフィックが少なくなる場合があります。バースト サイズの設定が高すぎると、予想よりトラフィックが多くなる場合があります。

各サービス クラスで複数の適合アクション、超過アクション、および違反アクションを同時に設定できます。**conform-action**、**exceed-action**、および **violate-action** ポリシー マップ クラス コンフィギュレーション コマンド、または **conform-action**、**exceed-action**、および **violate-action** ポリシー マップ クラス ポリシング コンフィギュレーション コマンドを使用すると、パケットが指定のトラフィックレートに適合するまたは超過する場合に実行するアクションを指定できます。適合アクション、超過アクション、および違反アクションは、パケットを廃棄する、パケットを変更しないで送信する、新しい CoS 値、DSCP 値、IP precedence 値を設定する、または出力側での分類用に QoS グループ値を設定することです。

（注）　適合アクションが drop に設定されている場合、超過アクションおよび違反アクションは自動的に drop に設定されます。超過アクションが drop に設定されている場合、違反アクションは自動的に drop に設定されます。

明示的な値、テーブル マップ、またはその両方を組み合せて、マーキングの適合アクション、超過アクション、または違反アクションをそれぞれ設定できます。**violate-action** を設定しない場合、デフォルトで違反クラスが **exceed-action** と同じアクションに割り当てられます。

テーブル マップでは、特定のトラフィック アトリビュートを示し、それらを他のアトリビュートにマッピング（変換）します。超過アクションのテーブル マップを設定し、違反アクションのアクションが明示的に設定されていない限り、集約ポリシングの **violate-action** に対するテーブル マップはサポートされません。

テーブル マップの作成後、ポリシーマップ ポリサーを設定して、テーブル マップを使用します。

（注）　入力ポリシー マップでテーブル マップを使用する場合、テーブル マップの **from** - アクションのプロトコル タイプは、対応する分類のプロトコル タイプと同じである必要があります。たとえば、クラス マップが IP 分類を表す場合、テーブル マップの **from** - タイプ アクションは、**dscp** または **precedence** である必要があります。クラス マップが非 IP 分類を表す場合、テーブル マップの **from** - タイプ アクションは、**cos** である必要があります。

複数の適合、超過、違反アクションを集約ポリサーに **policer aggregate** グローバル コンフィギュレーション コマンドのパラメータとして同時に設定できますが、次の順序でアクションを入力する必要があります。「集約ポリシングを含む入力ポリシー マップの設定」（P.34-54）にある設定時の注意事項を参照してください。

集約ポリサーを設定したあとで、ポリシー マップおよび対応するクラス マップを作成し、集約ポリサーにポリシー マップを関連付けて、サービス ポリシーをポートに適用します。

（注）　1 つのポリシー マップだけが、任意の特定の集約ポリサーを使用できます。集約ポリシングは、複数のインターフェイス上のトラフィック ストリームの集約には使用できません。集約ポリシングは、インターフェイスに付加されるポリシー マップの複数のクラスにまたがるトラフィック ストリームの集約、およびポート単位、VLAN 単位ポリシー マップのポート上の複数の VLAN にまたがるストリームの集約にだけ使用できます。

ポリシー マップおよびポリシング アクションを設定したあとで、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、入力ポートにポリシーを付加します。

次の例のクラス マップとは、アクセス リストを意味します。

```
Switch(config)# policer aggregate agg1 cir 23000 bc 10000 conform-action set-dscp-transmit
46 exceed-action drop
Switch(config)# class-map testclass
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map videoclass
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate agg1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police aggregate agg1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

設定の詳細については、「集約ポリシングを含む入力ポリシー マップの設定」（P.34-54）を参照してください。

集約ポリシングを使用して、複数の VLAN にまたがるトラフィック ストリームの規制もできます（次の例を参照）。

```
Switch(config)# policer aggregate agg1 cir 23000 bc 10000 conform-action set-dscp-transmit
af31 set-cos-transmit 3 exceed-action set-dscp-transmit af11 set-cos-transmit 1
Switch(config)# class-map video-provider-1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map video-provider-2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer1-provider-100
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer1-provider-200
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# exit
Switch(config)# policy-map child-policy-1
Switch(config-pmap)# class video-provider-1
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police aggregate agg1
Switch(config-pmap-c)# exit
Switch(config)# policy-map child-policy-2
Switch(config-pmap)# class video-provider-2
Switch(config-pmap-c)# set dscp cs4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police aggregate agg1
Switch(config-pmap-c)# exit
Switch(config)# policy-map customer-1-ingress
Switch(config-pmap)# class customer1-provider-100
Switch(config-pmap-c)# service-policy child-policy-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class customer1-provider-200
Switch(config-pmap-c)# service-policy child-policy-2
Switch(config-pmap-c)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy input customer-1-ingress
Switch(config-pmap-c)# exit
```

無条件のプライオリティ ポリシング

プライオリティ ポリシングは、出力ポリシー マップにだけ適用されます。出力ポリシー マップで **priority** ポリシー マップ クラス コンフィギュレーション コマンドを使用すると、特定のトラフィック クラスに対して低遅延パスまたはクラスベース プライオリティ キューイングを指定できます。完全プライオリティ キューイングを使用すると、プライオリティ キューのパケットは、キューが空になるまで他のキューよりも優先的にスケジューリングされ、送信されます。高いプライオリティ キューイングを過剰に使用すると、下位のプライオリティ トラフィックで輻輳が発生する場合があります。

このような輻輳を排除するには、ポリシング機能があるプライオリティ（プライオリティ ポリシング）を使用すると、プライオリティ キューで使用される帯域幅を削減し、他のキューにトラフィック レートを割り当てることができます。ポリシング機能があるプライオリティは、出力ポリシー マップでサポートされるポリシング形式だけになります。

（注） プライオリティで出力ポリシー マップの 1-rate、2-color ポリサーを設定できます。出力ポリシーの 2-rate、3-color ポリサーは設定できません。

「クラスベース プライオリティ キューイングを含む出力ポリシー マップの設定」（P.34-71）も参照してください。

（注）　無条件のプライオリティ ポリサー用にバースト サイズが認定されたポリサーは、設定できません。設定されたバースト サイズは、いずれも無視されます。

次に、**priority** コマンドと **police** コマンドを併用して、*out-class1* をプライオリティ キューとして設定し、キューに着信するトラフィックを 20,000,000 bps に制限して、プライオリティ キューがそれを超えるレートを使用しないようにする例を示します。このレートを超えるトラフィックは、廃棄されます。これにより、他のトラフィック キューはポート帯域幅の一部を受け取ります。この場合、最小帯域幅保証は、500,000 および 200,000 kbps です。クラスの **class-default** キューは、残りのポート帯域幅を受け取ります。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth 500000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth 200000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

マーキング

入力ポリシー マップでパケット マーキングを使用すると、特定のクラスに属するトラフィックのアトリビュートを設定または変更できます。ネットワーク トラフィックがクラス内に組み込まれたあとで、マーキングを使用して、特定のトラフィック タイプを識別して固有の処理を行います。たとえば、クラスの CoS 値を変更したり、特定のトラフィック タイプの IP DSCP 値または IP precedence 値を設定できます。その後、これらの新しく設定された値を使用して、トラフィックの処理方法を決定します。また、マーキングを使用すると、スイッチ内の QoS グループにトラフィックを割り当てることもできます。

トラフィック マーキングは通常、入力ポートの特定のトラフィック タイプで実行されます。マーキング アクションにより、CoS、DSCP、または precedence ビットは、設定に応じて書き換えられるか、またはそのまま変更されません。これにより、QoS ドメインで使用されるポリシーに従って、パケットのプライオリティが高くなるかまたは低くなります。そのため、他の QoS 機能ではマーキング情報を使用して、パケットの相対的および絶対的な重要性を判断できます。マーキング機能では、ポリシング機能から取得した情報または分類機能から直接取得した情報を使用できます。

ポリシー マップで、すべてのサポート対象の QoS マーキング（CoS、IP DSCP、IP precedence、および QoS グループ）に対して **set** コマンドを使用することにより、トラフィックを指定およびマーキングできます。**set** コマンドにより、特定クラスに一致するパケットは無条件にマーキングされます。その後、インターフェイスにポリシー マップを入力ポリシー マップとして付加します。

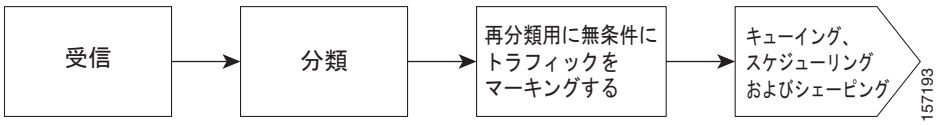
また、テーブル マップと **set** コマンドを併用しても、トラフィックをマーキングできます。テーブル マップでは、特定トラフィックのアトリビュートを表示し、他のアトリビュートにそれらをマッピング（変換）します。テーブル マップでは、アトリビュートの to-from 関係を確立し、行われた変更を定義します。

QoS グループ マーキング アクションと同一サービスのパケットの DSCP、precedence、および CoS マーキングを変更するアクションを同時に設定できます。出力分類に関してマーキング アクションで定義された QoS グループ番号を使用できます。

（注）　入力ポリシー マップでテーブル マップを使用する場合、テーブル マップの **from** - アクションのプロトコル タイプは、対応する分類のプロトコル タイプと同じである必要があります。たとえば、クラス マップが IP 分類を表す場合、テーブル マップの **from** - タイプ アクションは、**dscp** または **precedence** である必要があります。クラス マップが非 IP 分類を表す場合、テーブル マップの **from** - タイプ アクションは、**cos** である必要があります。

テーブル マップの作成後、ポリシーマップを設定して、テーブル マップを使用します。「輻輳管理およびスケジューリング」（P.34-27）を参照してください。図 34-6 に、トラフィックのマーキングの手順を示します。

図 34-6　　分類されたトラフィックのマーキング



次に、ポリシー マップを使用してパケットをマーキングする例を示します。最初のマーキング（**set** コマンド）は、クラス *AF31* ～ *AF33* によって一致しなかったすべてのトラフィックを照合する QoS デフォルト クラス マップに適用され、すべてのトラフィックの IP DSCP 値を 1 に設定します。2 番目のマーキングは、クラス AF31 ～ AF33 のトラフィックの IP DSCP を 3 に設定します。

```
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

Performance-Monitoring プロトコルの QoS 処理

- 「Cisco IP-SLAs」（P.34-24）
- 「双方向アクティブ測定プロトコル」（P.34-24）
- 「IP-SLA および TWAMP プローブの QoS 処理」（P.34-24）
- 「CPU 生成トラフィックの QoS マーキング」（P.34-24）
- 「CPU 生成トラフィックの QoS キューイング」（P.34-25）
- 「設定時の注意事項」（P.34-26）

Cisco IP-SLAs

Cisco IP Service Level Agreement（SLAs; サービス レベル契約）の詳細については、「Cisco IOS IP SLA の概要」（P.41-2）を参照してください。

双方向アクティブ測定プロトコル

Two-Way Active Measurement Protocol（TWAMP; 双方向アクティブ測定プロトコル）の詳細については、「TWAMP の概要」（P.41-14）および「TWAMP の設定」（P.41-15）を参照してください。

IP-SLA および TWAMP プローブの QoS 処理

IP-SLA および TWAMP プローブの QoS 処理では、デバイス間を行き交う通常のデータ トラフィックに発生する影響が正確に反映されていなければなりません。

生成元のデバイスでは、プローブ マーキングを変更してはいけません。通常トラフィックに設定したキューイング ポリシーに基づいて、これらのプローブをキューイングする必要があります。

マーキング

デフォルトでは、（CFM プローブを使用した IP SLAs を含む）CFM トラフィックの Class of Service（CoS; サービス クラス）マーキングは変更されません。この機能では、この動作は変更できません。

デフォルトでは、（IP SLA および TWAMP プローブを含む）IP トラフィック マーキングは変更されません。この機能では、この動作は変更できます。

キューイング

（CFM プローブを使用した IP SLAs を含む）CFM トラフィックは、通常のトラフィック同様、その CoS 値および出力ポートで設定された出力ポリシー マップにしたがってキューイングされます。この機能では、この動作は変更できません。

（IP SLA および TWAMP プローブを含む）IP トラフィックは、**cpu traffic qos** グローバル コンフィギュレーション コマンドおよび出力ポートの出力ポリシー マップで指定されたマーキングにしたがってキューイングされます。このコマンドが設定されていない場合、すべての IP トラフィックは、出力ポートのキューにスタティックにマッピングされます。

CPU 生成トラフィックの QoS マーキング

QoS マーキングを使用して、CPU からのトラフィックのアトリビュートを設定または変更できます。QoS マーキング アクションにより、パケット内の CoS、DSCP、または IP precedence ビットは書き換えられるか、またはそのまま変更されません QoS はパケット マーキングを使用して、あるトラフィック タイプおよびローカル スイッチおよびネットワーク上でのそれらのタイプの処理方法を識別します。

また、マーキングを使用すると、スイッチ内の QoS グループにトラフィックを割り当てることもできます。この QoS グループは、パケットを変更しない内部ラベルですが、ネットワーク ポートで出力キューイングを設定する場合のトラフィック タイプの識別に使用できます。

次のグローバル コンフィギュレーション コマンドを使用して、CPU 生成トラフィックを指定し、マーキングできます。

cpu traffic qos cos {*cos_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-ma**p *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

cpu traffic qos dscp {*dscp_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

cpu traffic qos precedence {*precedence_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

cpu traffic qos qos-group *value*

明示的な値を設定する、またはキーワード **table-map** を使用して、CoS、IP-DSCP、IP precedence、および QoS グループをマークできます。テーブル マップでは、特定のトラフィック アトリビュートを示し、それらを別のアトリビュートにマッピング（変換）します。テーブル マップでは、アトリビュートの to-from 関係を確立し、行われた変更を定義します。

- IP CPU パケットの CoS、または IP-DSCP、または IP precedence を使用した CoS のマーキング
- 非 IP CPU パケットの CoS を使用した CoS のマーキング
- CPU パケットの CoS、または IP-DSCP、または IP precedence を使用した IP DSCP のマーキング
- CPU パケットの CoS、または IP-DSCP、または IP precedence を使用した IP precedence のマーキング

IP-DSCP または IP precedence いずれかのマーキングを設定できます。

また同時に、CoS、IP-DSCP または IP precedence、および QoS グループを修正するマーキング アクションを設定できます。

cpu traffic qos コマンドは、適用先となるトラフィックを指定します。それらは、すべての CPU トラフィック、CPU IP トラフィックだけ、または CPU 非 IP トラフィックだけです。その他のすべてのトラフィックは、その QoS マーキングを保持しています。この機能は CFM トラフィック（CFM を使用したレイヤ 2 IP SLA プローブを含む）には影響を与えません。

（注） Cisco IOS リリース 12.2(52)SE には、テーブル マップを使用して CPU が生成したトラフィックの CoS、IP-DSCP および IP precedence をマーキングする機能が搭載されています。

CPU 生成トラフィックの QoS キューイング

cpu traffic qos グローバル コンフィギュレーション コマンドにより、出力ポリシー マップのクラス マップでパケット ID として CPU 生成トラフィックに確立された QoS マーキングを使用して、CPU トラフィックを出力ポートの出力ポリシー マップのクラス キューにマッピングできます。出力ポートの出力ポリシー マップを使用して、そのポートのスイッチから発信されるトラフィックのキューイングおよびスケジューリングを設定できます。

CoS、IP DSCP、または IP-precedence パケット マーキングを変更せずに、*すべての* CPU 生成トラフィックを出力ポリシー マップの 1 つのクラスにマッピングする場合、CPU 生成グループのマーキングに QoS グループを使用できます。

IP DSCP または IP-precedence に基づき、それらのパケット マーキングを変更せずに、*すべての* CPU 生成 IP トラフィックを出力ポリシー マップの複数クラスにマッピングする場合、テーブル マップを使用できます。

- テーブル マップを*指定せず*、**DSCP** または **precedence** を **map from** 値として使用することで、IP-DSCP または IP precedence マーキングを設定します。

- **default** および **copy** の各キーワードだけを使用したテーブル マップを*指定し*、**DSCP** または **precedence** を **map from** 値として使用することで、IP-DSCP または IP precedence マーキングを設定します。

CoS に基づき、CoS パケット マーキングを変更せずに、*すべての* CPU 生成トラフィックを出力ポリシー マップの複数クラスにマッピングする場合、テーブル マップを使用できます。

- テーブル マップを*指定せず*、**CoS** を **map from** 値として使用することで、CoS マーキングを設定します。
- **default** および **copy** の各キーワードだけを使用したテーブル マップを*指定し*、**CoS** を **map from** 値として使用することで、CoS マーキングを設定します。

テーブル マップの詳細については、「テーブル マップ」（P.34-15）を参照してください。

テーブル マッピングで **cpu traffic qos** グローバル コンフィギュレーション コマンドを使用すると、複数のマーキング ポリシーおよびキューイング ポリシーがともに動作、または個別に動作するよう設定できます。**cpu traffic qos** グローバル コンフィギュレーション コマンドを使用して設定された CoS マーキングに基づき、ネイティブ VLAN トラフィックをキューイングできます。

cpu traffic qos コマンドは、適用先となるトラフィックを指定します。それらは、すべての CPU トラフィック、CPU IP トラフィックだけ、または CPU 非 IP トラフィックだけです。その他のトラフィックは、出力ポートの CPU デフォルト キューにスタティックにマッピングされます。すべての CFM トラフィック（CFM を使用したレイヤ 2 IP SLA プローブを含む）は、出力ポリシー マップのクラスにマッピングされ、その CoS 値に基づいてキューイングされます。

（注）　Cisco IOS リリース 12.2(52)SE には、テーブル マップを使用して CPU が生成したトラフィックの CoS、IP-DSCP および IP precedence に基づいてキューイングする機能が搭載されています。

設定時の注意事項

- この機能は、スイッチにグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。
- 別々のラインに各 **cpu traffic qos** マーキング アクションを入力します。
- **cpu traffic qos cos** グローバル コンフィギュレーション コマンドは、特定の CoS 値またはテーブル マップの両方ではなく、いずれかを使用して、CPU 生成トラフィックの CoS マーキングを設定します。新しい設定により、既存の設定が上書きされます。
- **cpu traffic qos dscp** グローバル コンフィギュレーション コマンドは、特定の DSCP 値またはテーブル マップの両方ではなく、いずれかを使用して、CPU 生成 IP トラフィックの IP-DSCP マーキングを設定します。新しい設定により、既存の設定が上書きされます。
- **cpu traffic qos precedence** グローバル コンフィギュレーション コマンドは、特定の precedence 値またはテーブル マップの両方ではなく、いずれかを使用して、CPU 生成 IP トラフィックの IP-precedence マーキングを設定します。新しい設定により、既存の設定が上書きされます。
- **cpu traffic qos dscp** と **cpu traffic qos precedence** の各グローバル コンフィギュレーション コマンドは相互に排他的です。新しい設定により、既存の設定が上書きされます。
- **cpu traffic qos dscp** グローバル コンフィギュレーション コマンドがテーブル マップで設定されている場合、一度に 1 つの **map from** 値（DSCP、precedence、または CoS）しか設定できません。新しい設定により、既存の設定が上書きされます。このコマンドでマーキングされたパケットは、マーキングされた DSCP 値または precedence 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

- **cpu traffic qos precedence** グローバル コンフィギュレーション コマンドがテーブル マップで設定されている場合、一度に 1 つの **map from** 値（DSCP、precedence、または CoS）しか設定できません。新しい設定により、既存の設定が上書きされます。このコマンドでマーキングされたパケットは、マーキングされた precedence 値または DSCP 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- DSCP および precedence 両方の **map from** 値は設定できません。新しい設定により、既存の設定が上書きされます。
- **cpu traffic qos cos** グローバル コンフィギュレーション コマンドがテーブル マップで設定されている場合、一度に 2 つの **map from** 値（CoS と DSCP または precedence のいずれか）を設定できます。
- **cpu traffic qos cos** グローバル コンフィギュレーション コマンドが DSCP または precedence の **map from** 値だけで設定されている場合、次のようになります。
  - IP パケットの CoS 値は、パケットの DSCP（または precedence）値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
  - 非 IP パケットの CoS 値は変わりません。
- **cpu traffic qos cos** グローバル コンフィギュレーション コマンドが CoS の **map from** 値で設定されている場合、次のようになります。
  - IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
  - 非 IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- **cpu traffic qos cos** グローバル コンフィギュレーション コマンドが DSCP または precedence および CoS の **map from** 値で設定されている場合、次のようになります。
  - IP パケットの CoS 値は、パケットの DSCP または precedence 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
  - 非 IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- **cpu traffic qos qos-group** グローバル コンフィギュレーション コマンドを使用して、特定の QoS グループの CPU 生成トラフィックだけの QoS グループ マーキングを設定できます。**table-map** オプションは使用できません。

輻輳管理およびスケジューリング

Cisco Modular QoS CLI（MQC）は、発信トラフィック フローを制御する関連メカニズムをいくつか備えています。これらのメカニズムは、出力ポリシー マップに実装され、出力トラフィック キューを制御します。スケジューリング ステージでは、該当する時間までパケットを保有してから、4 つのトラフィック キューのいずれかに送信します。キューイングは、パケット クラスに基づいて特定のキューにパケットを割り当てて、輻輳を回避するため、WTD アルゴリズムにより拡張されます。異なるスケジューリング メカニズムを使用すると、他のトラフィックを均等に処理しながら、特定のトラフィック クラスに保証された帯域幅を割り当てることができます。特定のトラフィック クラスで消費される最大帯域幅を制限して、低遅延キューの遅延の影響を受けやすいトラフィックが他のキューよりも先に送信されるように保証できます。

スイッチでは、次のスケジューリング メカニズムをサポートします。

- トラフィック シェーピング

  shape average ポリシー マップ クラス コンフィギュレーション コマンドを使用すると、特定のトラフィック クラスで最大許容平均レートを使用するように指定できます。最大レートは bps で指定します。

- CBWFQ

  bandwidth ポリシー マップ クラス コンフィギュレーション コマンドを使用すると、特定のクラスに割り当てられる帯域幅を制御できます。最小帯域幅は、ビット レート、または総帯域幅もしくは残りの帯域幅との割合で指定できます。

- プライオリティ キューイングまたはクラスベース プライオリティ キューイング

  priority ポリシー マップ クラス コンフィギュレーション コマンドを使用して、他のトラフィック タイプよりも優先されるトラフィック タイプを指定します。プライオリティの高いトラフィックには、完全プライオリティを指定して、その他のトラフィック キューには余剰の帯域幅を割り当てたり、またはプライオリティの高いトラフィックの無条件のポリシングを含むプライオリティを指定して、その他のトラフィック キュー間に既知の残りの帯域幅を割り当てることが出来ます。

  - 完全プライオリティを設定するには、**priority** ポリシー マップ クラス コンフィギュレーション コマンドだけを使用して、プライオリティ キューを設定します。その他のトラフィック クラスには、**bandwidth remaining percent** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、必要な比率で余剰の帯域幅を割り当てます。
  - 無条件のポリシングを含むプライオリティを設定するには、**priority** ポリシー マップ クラス コンフィギュレーション コマンドおよび **police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、プライオリティ キューを無条件にレート制限します。この場合、他のトラフィック クラスは、要件に応じて **bandwidth** または **shape average** により設定できます。

ここでは、スケジューリングに関するその他の情報について説明します。

- 「トラフィック シェーピング」（P.34-28）
- 「CBWFQ」（P.34-30）
- 「プライオリティ キューイング」（P.34-32）

トラフィック シェーピング

トラフィック シェーピングは、トラフィック ポリシングと同様のトラフィック制御メカニズムです。入力ポリシー マップでトラフィック ポリシングが使用されている場合、トラフィック シェーピングはインターフェイスからトラフィックを発信するときに実行されます。スイッチは、インターフェイスから発信されるトラフィックのクラスにはクラスベース シェーピングを、およびインターフェイスから発信されるすべてのトラフィックにはポート シェーピングを適用できます。トラフィック シェーピングのキュー設定により、キューの最大帯域幅および Peak Information Rate（PIR）が設定されます。

（注）　出力ポリシー マップ内の同一のクラスに、トラフィック シェーピング（**shape average**）と CBWFQ（**bandwidth**）、またはプライオリティ キューイング（**priority**）を設定できません。出力ポリシー マップ内の別のクラスに、完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合、特定のトラフィック クラスにトラフィック シェーピングを設定できません。

クラスベース シェーピング

クラスベース シェーピングは、**shape average** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、データ伝送速度（bps）を制限し、トラフィック クラスの Committed Information Rate（CIR; 認定情報速度）に使用します。スイッチは、3 つのトラフィック クラスごとに別々のキューをサポートします。4 番めのキューは常に、クラス **class-default**、未分類トラフィック用のデフォルト キューです。

（注）　Cisco ME スイッチでは、トラフィック シェーピングの設定により、キューの最小帯域幅保証または CIR を PIR と同じ値に自動的に設定します。

次に、ファスト イーサネット ポート上で発信トラフィックのトラフィック シェーピングを設定し、*outclass1*、*outclass2*、および *outclass3* がそれぞれ使用可能なポート帯域幅のうち最大 50 Mbps、20 Mbps、10 Mbps を取得する例を示します。クラス **class-default** は、最低限として、残りのポート帯域幅を受け取ります。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

ポート シェーピング

ポート シェーピング（送信ポート シェーパ）を設定するには、デフォルト クラスだけを含むポリシー マップを作成して、**shape average** コマンドを使用してポートの最大帯域幅を指定します。

次に、前の例で設定された *out-policy* ポリシー マップに応じて割り当てられた、ポートを 90 Mbps にシェーピングするポリシー マップを設定する例を示します。**service-policy** ポリシー マップ クラス コマンドは、親ポリシーに子ポリシーを作成する場合に使用されます。

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output out-policy-parent
Switch(config-if)# exit
```

親子階層

トラフィック シェーピングでは、*parent* ポリシー レベルおよび *child* ポリシー レベルもサポートされます。QoS の親子構造は、特定のトラフィック タイプをさらに詳細に制御するために、子ポリシーが親ポリシー内で参照されるという特定の目的に使用されます。

最初のポリシー レベルは親レベルで、ポート シェーピングに使用されます。また、ポリシー内にクラス タイプの **class-default** を 1 つだけ特定できます。次に、親レベルのポリシー マップの例を示します。

```
Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
```

2 番めのポリシー レベルは子レベルで、特定のトラフィック ストリームまたはトラフィック クラスを制御するのに使用されます（次の例を参照）。

```
Switch(config)# policy-map child
Switch(config-pmap)# class class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
```

（注） 子ポリシーの各キューにおける最小帯域幅保証の合計（CIR）は、ポート シェーピング レートの合計を上回ることはできません。

次に、親子設定の例を示します。

```
Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# service-policy child
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output parent
Switch(config-if)# exit
```

CBWFQ

CBWFQ を設定することにより、ポートで使用可能な総帯域幅の一部を割り当てて、キューの相対的優先順位を設定できます。**bandwidth** ポリシー マップ クラス コンフィギュレーション コマンドを使用すると、トラフィック クラスの出力帯域幅をレート（kbps）、総帯域幅に対するパーセンテージ、または残りの帯域幅に対するパーセンテージで設定できます。

（注） ポリシー マップで帯域幅を設定する場合は、すべてのレートを同じ形式（設定されたレートまたはパーセンテージ）で設定する必要があります。ポリシーの各キューにおける最小帯域幅保証の合計（CIR）は、親の合計速度を上回ることはできません。

- **bandwidth** ポリシーマップ クラス コンフィギュレーション コマンドを使用して、トラフィック クラスを絶対レート（kbps）または総帯域幅に対するパーセンテージで設定する場合、これはそのトラフィック クラスの最小帯域幅保証（CIR）を表します。つまり、トラフィック クラスは最低でもコマンドにより指定された帯域幅を取得しますが、その帯域幅に制限されるわけではありません。ポート上の余剰の帯域幅はすべて、CIR レートの設定と同じ比率で各クラスに割り当てられます。

  （注） 出力ポリシーの別のクラスに完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合には、帯域幅を絶対レートまたは総帯域幅に対するパーセンテージでは設定できません。

- **bandwidth** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、トラフィック クラスを*残り*の帯域幅に対するパーセンテージで設定する場合、これはクラスに割り当てられるポートの余剰帯域幅の一部を表しています。つまり、ポート上に余剰の帯域幅がある場合、およびこのトラフィック クラスに最小帯域幅保証がない場合にだけ、クラスに帯域幅が割り当てられます。

（注）　出力ポリシー マップの別のクラスに完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合にだけ、帯域幅を残りの帯域幅に対するパーセンテージで設定できます。

詳細については、「CBWFQ を含む出力ポリシー マップの設定」（P.34-67）を参照してください。

（注）　出力ポリシー マップ内の同一のクラスには、帯域幅とトラフィック シェーピング（**shape average**）またはプライオリティ キューイング（**priority**）を設定できません。

次に、帯域幅（kbps）を設定することにより、出力キューの優先順位を設定する例を示します。クラス *outclass1*、*outclass2*、*outclass3*、および **class-default** は、それぞれ 40000、20000、10000、および 10000 kbps の最小帯域幅を取得します。余剰の帯域幅はすべて、CIR レートと同じ比率でクラス間に分配されます。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 40000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

（注）　クラスの CIR 帯域幅を絶対レートまたは総帯域幅に対するパーセンテージで設定する場合、ポリシー マップ内のすべてのクラスの CIR の処理後に残った余剰な帯域幅すべては、CIR レートと同じ比率でクラス間に分配されます。クラスの CIR レートが 0 に設定されている場合、このクラスはどの余剰帯域幅に対しても不適格となるため、帯域幅を取得できません。

次に、トラフィック クラスの帯域幅を残りの帯域幅に対するパーセンテージで設定することにより、キュー間に余剰の帯域幅を割り当てる例を示します。*outclass1* クラスには、プライオリティ キュー処理が行われます。他のクラスは、プライオリティ キューの処理後に余剰の帯域幅が残っている場合に、その帯域幅に対するパーセンテージを取得するよう設定されます。*outclass2* は、50% を取得するように、*outclass3* は 20% を取得するように、またクラス **class-default** は残りの 30% を取得するように設定されます。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
```

```
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

プライオリティ キューイング

priority ポリシー マップ クラス コンフィギュレーション コマンドを使用すると、特定のトラフィック クラスで優先処理が行われるよう保証できます。完全プライオリティ キューイングを使用すると、プライオリティ キューは常に処理されます。キュー内のすべてのパケットは、キューが空になるまでスケジューリングされ、送信されます。プライオリティ キューイングにより、関連付けられたクラスのトラフィックは、他のキューのパケットよりも先に送信されます。

（注）　**priority** コマンドを使用する際は注意してください。完全プライオリティ キューイングを過剰に使用すると、他のキューで輻輳が発生する場合があります。

スイッチでは、完全プライオリティ キューイングまたは **police** ポリシー マップ コマンドと併用されるプライオリティをサポートしています。

- *完全プライオリティ キューイング*（ポリシングなしのプライオリティ）では、トラフィック クラスを低遅延キューに割り当てて、このクラスのパケットの遅延確率が最小になるよう保証します。完全プライオリティ キューイングが設定されている場合、プライオリティ キューは空になるまで継続的に処理され、他のキューのパケットは処理されない場合もあります。

  （注）　同一出力ポリシー マップ内の別のクラスで、トラフィック シェーピングまたは CBWFQ が設定されている場合は、トラフィック クラスに対するポリシングなしのプライオリティを設定できません。

- **police** ポリシー マップ コマンドとプライオリティを併用するか、または*無条件のプライオリティ ポリシング*を使用することにより、プライオリティ キューで使用される帯域幅を削減できます。これは、出力ポリシー マップでサポートされる唯一のポリシング形式です。このようにコマンドを組み合せて、プライオリティ キューの最大レートを設定します。また、他のクラスに **bandwidth** および **shape average** の各ポリシー マップ コマンドを使用すると、他のキューのトラフィック レートを割り当てることができます。

  （注）　出力ポリシー マップに **police** コマンドを*使用せずに*プライオリティが設定されている場合に他のキューを設定するには、**bandwidth remaining percent** ポリシー マップ コマンドを使用して余剰の帯域幅を割り当てることによって共有するしかありません。

プライオリティ キューイングには、次の制限事項があります。

- **priority** コマンドは、スイッチ上で付加されたすべての出力ポリシーの単一の一意のクラスに関連付けできます。
- 同一クラスでは、プライオリティとその他のスケジューリング アクション（**shape average** または **bandwidth**）を設定できません。
- 出力ポリシー マップの **class-default** にはプライオリティ キューイングを設定できません。

詳細については、「クラスベース プライオリティ キューイングを含む出力ポリシー マップの設定」（P.34-71）を参照してください。

次に、クラス *out-class1* を完全プライオリティ キューとして設定し、このクラスのすべてのパケットが他のトラフィック クラスより先に送信される例を示します。他のトラフィック キューでは、*out-class2* は残りの帯域幅の 50%、*out-class3* は残りの帯域幅の 20% を取得するように設定されます。クラス **class-default** は、保証なしで、残りの 30% を取得します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

次に、**priority** コマンドと **police** コマンドを併用して、*out-class1* をプライオリティ キューとして設定し、キューに着信するトラフィックを 20000000 bps に制限して、プライオリティ キューがそれを超えるレートを使用しないようにする例を示します。このレートを超えるトラフィックは、廃棄されます。他のトラフィック キューは、残りの帯域幅の 50% および 20% を使用するように設定されます（上記の例を参照）。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

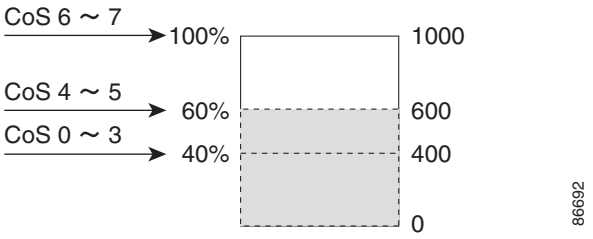
輻輳回避およびキューイング

輻輳回避では、テール ドロップなどのアルゴリズムを使用して、キューイングおよびスケジューリング ステージを開始するパケット数を制御して、輻輳およびネットワークのボトルネックを回避します。スイッチは、Weighted Tail-Drop（WTD）を使用して、キュー サイズを管理し、トラフィック分類の廃棄優先順位を指定します。キュー サイズの制限は、キューのパケット マーキングに応じて設定されます。スイッチを通過するパケットごとに、特定のキューおよびしきい値が割り当てられます。たとえば、特定の DSCP 値または CoS 値は特定の出力キューおよびしきい値にマッピングされます。

WTD はキュー サイズを管理したり、トラフィック分類ごとに廃棄優先順位を設定するためにトラフィック キューに実装されます。WTD ではパケット分類を使用して、特定のキューに着信したフレームにそれぞれ異なるしきい値を適用します。宛先キューの合計サイズが、再分類された任意のトラフィックのしきい値を上回る場合、そのトラフィックの次のフレームは廃棄されます。

図 34-7 に 1000 フレームのキューにおける WTD の動作例を示します。40%（400 フレーム）、60%（600 フレーム）、および 100%（1000 フレーム）の 3 つの廃棄の割合が設定されています。これらのパーセンテージは、40% のしきい値に再分類されたトラフィックは、キュー深度が 400 フレームを超過すると廃棄され、60% のしきい値に再分類されたトラフィックは、キュー深度が 600 フレームを超過すると廃棄されるということを意味します。また、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

図 34-7　　WTD およびキューの動作



この例では、CoS 値 6 および 7 は、他の CoS 値よりも重要度が高く、100% 廃棄しきい値に割り当てられます（キューフル ステート）。CoS 値 4 および 5 は 60% しきい値に、CoS 値 0 ～ 3 は 40% しきい値に割り当てられます。

すでにキューが 600 フレームで満たされている場合に、4 および 5 の CoS 値を含む新しいフレームが着信すると、このフレームは 60% しきい値の対象となります。このフレームがキューに追加されると、しきい値を超過するため、フレームは廃棄されます。

WTD は、**queue-limit** ポリシー マップ クラス コマンドにより設定されます。このコマンドにより、特定のトラフィック クラスに関連するキュー サイズ（バッファ サイズ）が調整されます。しきい値をパケット数で指定する場合、各パケットは 256 バイトの固定単位となります。同一キュー内のトラフィック クラス（CoS、DSCP、precedence、または QoS グループ）ごとに、異なるキュー サイズを指定できます。キュー制限を設定することにより、対応するトラフィックの輻輳発生時の廃棄しきい値が確立されます。

（注） **queue-limit** ポリシー マップ クラス コマンドを使用してキュー サイズを設定する場合は、まずスケジューリング アクション（**bandwidth**、**shape average** または **priority**）を設定する必要があります。唯一の例外は、出力ポリシー マップの **class-default** のキュー制限を設定する場合です。

スイッチは、すべての出力ポリシー マップにおいてそれぞれ固有のキュー制限設定を最大 3 つまでサポートしています。出力ポリシー マップ内で許容されるキュー（クラス）は 4 つだけです（クラス デフォルトを含む）。各キューには 3 つのしきい値が定義されています。スイッチ上では、固有のしきい値を 3 つまで設定できます。ただし、複数のポリシー マップで同じキュー制限を共有できます。2 つのポリシー マップがキュー制限の設定を共有する場合、両方のポリシー マップのすべてのクラスで、すべてのしきい値が同じでなければなりません。

詳細については、「CBWFQ を含む出力ポリシー マップの設定」（P.34-67）を参照してください。

次に、*class A* が DSCP 値およびポリシー マップ、*PM1* に一致するよう設定する例を示します。30 および 50 の DSCP は、一意のしきい値（それぞれ 32 および 64）にマッピングされます。40 および 60 の DSCP 値は、112 パケットの最大しきい値にマッピングされます。

```
Switch(config)# class-map match-any classA
Switch(config-cmap)# match ip dscp 30 40 50 60
Switch(config-cmap)# exit
Switch(config)# policy-map PM1
Switch(config-pmap)# class classA
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 112
Switch(config-pmap-c)# queue-limit dscp 30 32
Switch(config-pmap-c)# queue-limit dscp 50 64
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output PM1
Switch(config-if)# exit
```

スイッチ上の複数の出力ポリシー マップで同じキュー制限値を使用できます。ただし、クラスのキュー制限値の 1 つを変更すると、新たな固有のキュー制限設定が作成されます。インターフェイスに付加できる出力ポリシー マップの固有のキュー制限設定は、どの時点でも 3 つだけです。4 つめのキュー制限が設定された出力ポリシー マップを付加しようとすると、次のエラー メッセージが表示されます。

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

（注） 出力ポリシー マップで特定のクラスにキュー制限を設定する場合、他のすべての出力ポリシー マップでは、同一の修飾子タイプおよび修飾値の形式を使用する必要があります。キュー制限のしきい値に限り、異なる値を設定できます。たとえば、ポリシー マップ *PM1* の **dscp 30** および **dscp 50** に、*class A* のキュー制限のしきい値が設定されていて、ポリシー マップ *PM2* で *class A* のキュー制限を設定する場合、**dscp 30** および **dscp 50** を修飾子として使用する必要があります。**dscp 20** および **dscp 40** は、使用できません。別のしきい値を設定できますが、これにより、新たなキュー制限設定が作成されます。

デフォルトでは、バッファ スペースの総容量は、すべてのポートおよび各ポートのすべてのキューで均等に分配されます。これは、多くのアプリケーションに適合します。遅延の影響を受けやすいトラフィックのキュー サイズを削減したり、またはバースト性のあるトラフィックのキュー サイズを増加させたりできます。

（注） **queue-limit** コマンドを使用して、クラスのキューしきい値を設定する場合、WTD しきい値は、キューの最大しきい値以下にする必要があります。修飾子なしで設定されたキュー サイズは、修飾子を使用して設定されたいずれのキュー サイズよりも大きくする必要があります。

キュー制限を設定する場合、指定できるパケット数の範囲は 16 の倍数で、16 ～ 544 です。この場合、各パケットは 256 バイトの単位となります。

（注）　最適なパフォーマンスを実現するため、キュー制限を 272 以下に設定することを推奨します。

キューの帯域幅とキュー サイズ（キュー制限）は、別々に設定されます。相互依存はしません。帯域幅およびキュー制限を設定する場合、送信されるトラフィック タイプを考慮する必要があります。

- 大きなバッファ（キュー制限）により、パケットを損失しないでバースト性のあるトラフィックに対応できますが、遅延は増えます。
- 小さなバッファは遅延を減らしますが、バースト性のあるトラフィックより安定したトラフィック フローに適しています。
- 非常に小さなバッファは通常、プライオリティ キューイングを最適化するのに使用されます。プライオリティ キューイングされるトラフィックの場合、通常少しのパケットに対応するだけのバッファ サイズが必要です。通常、大きなバッファ サイズは遅延を増加させるため、必要ではありません。高いプライオリティの遅延の影響を受けやすいパケットには、相対的に大きな帯域幅および相対的に小さなキュー サイズを設定します。

（注）　これらの制限事項は、WTD 修飾子に適用されます。

- **queue-limit** コマンドを使用した場合、WTD 修飾子（**cos**、**dscp**、**precedence**、**qos-group**）に 3 つ以上のしきい値を設定できません。ただし、これらのしきい値にマッピングできる修飾子の数に制限はありません。修飾子を指定しないで **queue-limit** コマンドを使用することにより、最大キューを設定する 3 番めのしきい値を設定できます。
- **queue-limit** コマンドの WTD 修飾子は、関連するクラス マップの少なくとも 1 つの **match** 修飾子と同じである必要があります。

次に、*out-class1*、*out-class2*、*out-class3*、および **class-default** がそれぞれ最低 40、20、10、および 10% のトラフィック帯域幅を取得するように、帯域幅およびキュー制限を設定する例を示します。対応するキューサイズは、48、32、16、および 272（256 バイト）パケットに設定されます。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# queue-limit 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 272
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

スイッチポート数に応じた数の出力ポリシー マップを設定および付加できますが、一意のキュー制限は 3 つしか設定できません。他の出力ポリシー マップが同じキュー制限およびクラス設定を使用する場合、帯域幅パーセンテージが異なる場合でも、キュー制限設定は同じであると見なされます。

QoS の設定

QoS を設定する前に、次の内容を理解しておいてください。

- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン
- トラフィックの特性およびネットワークのニーズ。トラフィックのバースト性の有無。音声およびビデオ ストリーム用に帯域幅を確保する必要性
- 帯域要件およびネットワーク速度
- ネットワークで輻輳が発生する場所

次に、着信トラフィックの分類、ポリシングおよびマーキング方法と発信トラフィックのスケジューリングおよびキューイング方法について説明します。ネットワーク設定に応じて、次の作業を 1 つまたは複数実行する必要があります。

- 「デフォルトの QoS 設定」（P.34-37）
- 「QoS 設定時の注意事項」（P.34-37）
- 「ACL を使用したトラフィックの分類」（P.34-39）
- 「クラス マップを使用したトラフィック クラスの定義」（P.34-43）
- 「テーブル マップの設定」（P.34-45）
- 「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）
- 「入力ポリシー マップの設定」（P.34-47）
- 「出力ポリシー マップの設定」（P.34-65）
- 「CPU 生成トラフィックの QoS マーキングおよびキューイングの設定」（P.34-78）

デフォルトの QoS 設定

ポリシー マップ、クラス マップ、テーブル マップ、またはポリサーは設定されていません。出力ポートでは、すべてのトラフィックは動作可能なポートの全帯域幅を割り当てられる単一のデフォルト キューを介して発信されます。デフォルト キューのデフォルト サイズは、160（256 バイト）パケットです。

パケットは変更されません（パケット内の CoS、DSCP、および IP precedence 値は変更されません）。トラフィックはパススルー モードでスイッチングされ、書き換えられずにポリシングを伴わないベストエフォート型として分類されます。

QoS 設定時の注意事項

- QoS は、物理ポート上でだけ設定できます。
- QoS が設定されたポートでは、そのポートを通じて受信されるすべてのトラフィックは、ポートに付加された入力ポリシー マップに従って分類、ポリシング、およびマーキングが行われます。QoS が設定されたトランク ポートでは、そのポートを通じて受信されるすべての VLAN 内トラフィックは、ポートに付加されたポリシー マップに従って分類、ポリシング、およびマーキングが行われます。ポート単位、VLAN 単位ポリシー マップが付加された場合、トランク ポート上のトラフィックは、親レベルのポリシーで指定された VLAN に対して、各 VLAN に関連付けられた子ポリシー マップに従って分類、ポリシング、およびマーキングされます。

- スイッチに EtherChannel ポートが設定されている場合は、EtherChannel を構成する各物理ポートで QoS の分類、ポリシング、マッピング、およびキューイングを設定する必要があります。EtherChannel のすべてのポートで、QoS 設定を統一するかどうかを決定します。
- スイッチで受信された制御トラフィック（スパニング ツリー Bridge Protocol Data Unit [BPDU; ブリッジ プロトコル データ ユニット]やルーティング アップデート パケットなど）には、すべての入力 QoS 処理が行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。
- 新しいポリシーをインターフェイスに付加しようとし、これによりポリサー *インスタンス*の数が 1024 -（スイッチ上のインターフェイス数 + 1）より多い数になる場合、エラー メッセージを受信し、設定は失敗します。
- 新しいポリシーをインターフェイスに付加しようとし、これによりポリサー *プロファイル*の数が 254 より多い数になる場合、エラー メッセージを受信し、設定は失敗します。プロファイルは、認定速度、最大速度、認定バースト、および最大バーストの組み合せです。1 つのプロファイルを複数のインスタンスに付加できますが、これらの特性のいずれかが異なっている場合、ポリサーに新しいプロファイルがあると見なされます。
- すべての ME 3400E スイッチで、スイッチのすべてのポートに、256 のポート単位、VLAN 単位ポリシー マップ内の*固有の* VLAN 分類基準を指定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*VLAN label resources exceeded* というエラー メッセージが返されます。
- すべての ME 3400E スイッチで、QoS ACE 分類リソース制限に達するまで、ポート単位およびポート単位、VLAN 単位のポリシー マップをスイッチのすべてのポートに付加できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*TCAM resources exceeded* というエラー メッセージが返されます。
- CPU 保護がイネーブルになっている場合、ポートごとに設定できるポリサーは 45 だけです。CPU 保護をディセーブルにすると、ポートごとに最大 64 のポリサーを設定できます。**show policer cpu uni-eni** {**drop** | **rate**} 特権 EXEC コマンドを入力し、CPU 保護がイネーブルになっているかどうか確認できます。
- CPU 保護をディセーブルにする際はこれらの制限事項について注意してください。
  - CPU 保護をディセーブルにすると、ユーザ定義クラスに対してポートごとに最大 63 のポリサー（すべての 4 番目のポート上で 62）を、すべての ME 3400E スイッチの class-default に対して 1 つのポリサーを設定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*policer resources exceeded* というエラー メッセージが返されます。
  - CPU 保護をディセーブルにすると、ME3400E-24TS プラットフォームについてスイッチに最大 255 のポリサーを設定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*policer resources exceeded* というエラー メッセージが返されます。
  - CPU 保護をディセーブルにして、45 を超えるポリサーを持つポリシー マップを付加してから、CPU 保護を再度イネーブルにして、リロードした場合、CPU 保護には、ポートごとに 19 のポリサーが再度必要となります。リロード中、ポリサー 46 以降は、*policer resources exceeded* のエラー条件を満たすことになるので、これらのクラスに付加されるポリサーはありません。
- 内部 QoS ラベル数が 254 を超えると、エラー メッセージを受信します。
- 超過アクションのテーブル マップを設定し、違反アクションのアクションが明示的に設定されていない限り、集約ポリシングの **violate-action** に対するテーブル マップはサポートされません。個々のポリサーおよび集約ポリサー両方について、**violate-action** を設定しない場合、デフォルトで違反クラスが **exceed-action** と同じアクションに割り当てられます。

- トランクまたは 802.1Q トンネル インターフェイスで 2 重タグ パケットを受信すると、これらのパケットは他のパラメータとともに DSCP および IP precedence で分類されますが、発信パケットで DSCP または IP precedence は設定できません。発信パケットで CoS を設定できます。

各機能に関連する設定上の注意事項の詳細については、特定の QoS 機能の設定の説明を参照してください。

ACL を使用したトラフィックの分類

IP 標準または IP 拡張 ACL を使用すると、IP トラフィックを分類できます。レイヤ 2 MAC ACL を使用すると、IP および非 IP トラフィックを分類できます。ACL の設定の詳細については、第 32 章「ACL によるネットワーク セキュリティの設定」を参照してください。

QoS ACL を設定する場合は、次の注意事項に従ってください。

- IP フラグメントを設定済みの IP 拡張 ACL に照合して、QoS を実行できません。IP フラグメントはベストエフォート型として送信されます。IP フラグメントは IP ヘッダー内のフィールドで指定されます。
- スイッチは、入力ポリシー マップのクラスごとにアクセス グループを 1 つだけサポートします。
- 出力ポリシー マップには、**match-access** グループを設定できません。

ここでは、QoS ACL の作成方法について説明します。

- 「IP 標準 ACL の作成」（P.34-39）
- 「IP 拡張 ACL の作成」（P.34-41）
- 「レイヤ 2 MAC ACL の作成」（P.34-42）

IP 標準 ACL の作成

IP トラフィック用の IP 標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	IP 標準 ACL を作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。指定できる範囲は 1 ～ 99 および 1300 ～ 1999 です。 • QoS ポリシーの一致基準として使用される ACL には、必ずキーワード **permit** を使用します。QoS ポリシーは、キーワード **deny** を使用する ACL には一致しません。 • *source* には、パケットの送信元であるネットワークまたはホストを入力します。キーワード **any** は 0.0.0.0 255.255.255.255 の短縮形として使用できます。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。
または	**ip access-list standard** *name*	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。名前は 1 ～ 99 の番号にできます。 アクセスリスト コンフィギュレーション モードで、**permit** *source* [*source-wildcard*] を入力します。

	コマンド	目的
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。

次に、指定された 3 つのネットワーク上のホストにだけアクセスを許可する例を示します。ワイルド カード ビットはネットワーク アドレスのホスト部分に適用されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
```

IP 拡張 ACL の作成

IP トラフィック用の IP 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **permit** *protocol* {*source source-wildcard destination destination-wildcard*} [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] （注）　**dscp** 値を入力した場合、**tos** または **precedence** は入力できません。**dscp** を入力しない場合は、tos と **precedence** を両方とも入力できます。	IP 拡張 ACL を作成します。必要な回数だけ、この手順を繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。指定できる範囲は 100 ～ 199、および 2000 ～ 2699 です。 • QoS ポリシーの一致基準として使用される ACL には、必ずキーワード **permit** を使用します。QoS ポリシーは、**deny** ACL に一致しません。 • *protocol* には、IP プロトコルの名前または番号を入力します。使用可能なプロトコル キーワードのリストを表示するには、疑問符（?）を使用します。すべてのインターネット プロトコル（ICMP、TCP、UDP を含む）と一致させる場合は、**ip** を入力します。 • *source* はパケットの送信元であるネットワークまたはホストの番号です。 • *source-wildcard* を指定すると、送信元にワイルドカード ビットが適用されます。 • *destination* はパケットの宛先となるネットワークまたはホストの番号です。 • *destination-wildcard* を指定すると、宛先にワイルドカード ビットが適用されます。 source、destination、wildcards は、次のように指定できます。 • ドット付き 10 進表記による 32 ビットの数値 • 0.0.0.0 255.255.255.255 を表すキーワード **any**（任意のホスト） • 単一のホスト 0.0.0.0 を表すキーワード **host** その他のキーワードは任意で、意味は次のとおりです。 • **precedence**：0 ～ 7 の番号または名前で指定された優先順位を使用し、パケットを比較します。使用できる名前および番号は、**routine**（**0**）、**priority**（**1**）、**immediate**（**2**）、**flash**（**3**）、**flash-override**（**4**）、**critical**（**5**）、**internet**（6）、**network**（**7**）です。 • **tos**：0 ～ 15 の番号または名前で指定された ToS レベルを使用して比較します。使用できる名前および番号は、**normal**（**0**）、**max-reliability**（**2**）、**max-throughput**（**4**）、**min-delay**（**8**）です。 • **dscp**：0 ～ 63 の番号で指定された DSCP 値を使用してパケットを照合します。疑問符（?）を使用すると、使用可能な値のリストが表示されます。

	コマンド	目的
または	**ip access-list extended** *name*	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。*name* は 100 ～ 199 の番号にできます。 アクセスリスト コンフィギュレーション モードで、ステップ 2 で定義した **permit** *protocol* {*source source-wildcard destination destination-wildcard*} [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。

次に、任意の送信元から任意の宛先への IP トラフィック（DSCP 値は 32）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IP トラフィック（precedence 値は 5）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

レイヤ 2 MAC ACL の作成

非 IP トラフィック用のレイヤ 2 MAC ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name*	リストの名前を指定して、レイヤ 2 MAC ACL を作成し、拡張 MAC ACL コンフィギュレーション モードを開始します。
ステップ 3	**permit** {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	QoS ポリシーの一致基準として使用される ACL には、必ずキーワード **permit** を使用します。 • *src-MAC-addr* には、パケットの送信元であるホストの MAC アドレスを入力します。MAC アドレスは、16 進表記（H.H.H）で、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff にキーワード **any** を使用したり、*source* 0.0.0 にキーワード **host** を使用して指定できます。 • *mask* には、無視するビット位置に 1 を指定してワイルドカード ビットを入力します。 • *dst-MAC-addr* には、パケットの送信先となるホストの MAC アドレスを入力します。MAC アドレスは、16 進表記（H.H.H）で、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff にキーワード **any** を使用したり、*source* 0.0.0 にキーワード **host** を使用して指定できます。 • （任意）*type mask* には、Ethernet II または SNAP でカプセル化されたパケットの EtherType 番号を指定し、パケットのプロトコルを指定します。*type* の範囲は 0 ～ 65535 です。通常は 16 進数で指定します。*mask* には、一致を調べる前に EtherType に適用される *don't care* ビットを入力します。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*access-list-number* | *access-list-name*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no mac access-list extended** *access-list-name* グローバル コンフィギュレーション コマンドを使用します。

次に、2 つの **permit** 文を含むレイヤ 2 の MAC ACL を作成する例を示します。最初の文では、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番めの文では、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、EtherType が XNS-IDP のトラフィックだけが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-macl)# exit
```

クラス マップを使用したトラフィック クラスの定義

特定のトラフィック フロー（またはクラス）を他のすべてのトラフィックと区別して名前を付けるには、**class-map** グローバル コンフィギュレーション コマンドを使用します。クラス マップが、特定のトラフィック フローとの照合を行い、さらにそれを分類するために使用する基準を定義します。match 文には、ACL、CoS 値、DSCP 値、IP precedence 値、QoS グループ値、または VLAN ID などの基準が含まれます。一致基準は、クラスマップ コンフィギュレーション モードで入力される 1 つまたは複数の **match** 文で定義されます。

クラス マップの設定を行うときは、次の注意事項に従ってください。

- **match-all** クラス マップには、1 つの分類基準（match 文）しか指定できませんが、**match-any** クラス マップには複数の match 文を指定できます。
- **match cos** コマンドおよび **match vlan** コマンドは、レイヤ 2 802.1Q トランク ポート上でだけサポートされます。
- **match vlan** コマンドを含むクラス マップは、トランク ポート上のポート単位、VLAN 単位 QoS に関する入力階層型ポリシー マップの親ポリシーで使用します。子ポリシー マップに関連付けられた 1 つまたは複数のクラスがあるポリシーは、親ポリシー マップと見なされます。親ポリシー マップ内の各クラスは、親クラスと呼ばれます。親クラスでは、**match vlan** コマンドだけを設定できます。子ポリシー マップ内のクラスでは、**match vlan** コマンドを設定できません。
- 入力ポリシー マップでは、同じポリシー マップまたはクラス マップ内に IP 分類（**match ip dscp**、**match ip precedence**、**match ip acl**）と非 IP 分類（**match cos** または **match mac acl**）を設定できません。ポート単位、VLAN 単位階層型ポリシー マップでは、これを子ポリシー マップに適用します。
- 入力ポリシー マップには、**match qos-group** を設定できません。
- 出力ポリシー マップでは、異なるクラス マップで同じ分類基準（つまり、同じ match 修飾子および match 値）を使用できません。
- スイッチ上のクラス マップの最大数は 1024 です。

クラス マップを作成し、トラフィックを分類するための一致基準を定義するには、特権 EXEC モードで次の作業を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。デフォルトでは、クラス マップは定義されていません。 • （任意）このクラス マップのすべての一致文に対して論理 AND を実行するには、キーワード **match-all** を使用します。この場合は、クラス マップ内のすべての一致基準と一致する必要があります。 • （任意）このクラス マップのすべての一致文に対して論理 OR を実行するには、キーワード **match-any** を使用します。この場合は、1 つまたは複数の一致基準と一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 一致文が指定されない場合、デフォルトは **match-all** になります。 **（注）**　**match-all** クラス マップでは、複数の分類基準（match 文）を設定できません。
ステップ 3	**match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **qos-group** *value* | **vlan** *vlan-list*}	トラフィックを分類する一致基準を定義します。デフォルトで、一致基準は定義されていません。 各クラス マップでサポートされる一致タイプおよび ACL は、それぞれ 1 つだけです。 • **access-group** *acl-index-or-name* を指定する場合は、ACL の番号または名前を指定します。アクセス グループの照合は、入力ポリシー マップでだけサポートされます。 • **cos** *cos-list* を指定する場合は、1 行に最大 4 つの CoS 値のリストを入力して、着信パケットと照合します。各値はスペースで区切ります。5 つ以上の CoS 値を照合する場合は、複数の *cos-list* 行を入力できます。指定できる範囲は 0 ～ 7 です。 • **ip dscp** *dscp-list* を指定する場合は、着信パケットと照合する最大 8 つの IPv4 DSCP 値を入力します。各値はスペースで区切ります。9 つ以上の DSCP 値を照合する場合は、複数の *dscp-list* 行を入力できます。指定できる数値範囲は 0 ～ 63 です。DSCP 値は、他の形式でも設定できます。「IP DSCP に基づく分類」（P.34-9）を参照してください。 • **ip precedence** *ip-precedence-list* を指定する場合は、着信パケットと照合する最大 4 つの IPv4 precedence 値のリストを入力します。各値はスペースで区切ります。5 つ以上の precedence 値を照合する場合は、複数の *ip-precedence-list* 行を入力できます。指定できる範囲は 0 ～ 7 です。 • **vlan** *vlan-list* を指定する場合、トランク ポート上のポート単位、VLAN 単位の QoS に関して親ポリシー マップで使用される VLAN ID または VLAN 範囲を指定します。VLAN ID の範囲は 1 ～ 4094 です。 • **qos-group** *value* を指定する場合、QoS グループ番号を指定します。指定できる範囲は、0 ～ 99 です。QoS グループの照合は、出力ポリシー マップでだけサポートされます。
ステップ 4	**end**	特権 EXEC モードに戻ります。

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

既存のクラス マップまたは一致基準を削除するには、該当するコマンドの **no** 形式を使用します。

次に、アクセス リスト 103 を作成し、*class1* という名前のクラス マップを設定する例を示します。*class1* にはアクセス リスト 103 という一致基準が 1 つ設定されています。このクラス マップによって、DSCP 値 10 と一致する任意のホストから任意の宛先へのトラフィックが許可されます。

```
Switch(config)# access-list 103 permit any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

次に、DSCP 値 10、11、12 で着信トラフィックと照合する、*class2* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map match-any class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

次に、IP precedence 値 5、6、7 で着信トラフィックと照合する、*class3* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map match-any class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

次に、30 ～ 40 の範囲の VLAN ID で着信トラフィックと照合する、*parent-class* という名前の親クラスマップを作成する例を示します。

```
Switch(config)# class-map match-any parent-class
Switch(config-cmap)# match vlan 30-40
Switch(config-cmap)# exit
```

テーブル マップの設定

テーブル マップを設定すると、単一のコマンドで多数のトラフィック フローを管理できます。テーブル マップを使用して、特定の DSCP 値、IP precedence 値、および CoS 値を相互に関連付けて、DSCP 値、IP precedence 値、または CoS 値をマークダウンするか、それらにデフォルト値を割り当てます。**set** コマンドで指定したテーブル マップを、ポリシーのマークダウン マッピングとして使用できます。

スイッチでは、次のテーブル マップがサポートされます。

- DSCP/CoS、precedence、または DSCP
- CoS/DSCP、precedence、または CoS
- precedence/CoS、DSCP、または precedence

テーブル マップの設定を行うときは、次の注意事項に従ってください。

- スイッチでは、最大 256 の一意のテーブル マップをサポートしています。
- テーブル マップ内の map 文の最大数は 64 です。
- テーブル マップは、出力ポリシー マップで使用できません。
- 超過アクションのテーブル マップを設定し、違反アクションのアクションが明示的に設定されていない限り、集約ポリシングの **violate-action** に対するテーブル マップはサポートされません。

テーブル マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**table-map** *table-map-name*	テーブル マップ名を入力してテーブル マップを作成し、テーブルマップ コンフィギュレーション モードを開始します。
ステップ 3	**map from** *from-value* **to** *to-value*	テーブルに含めるマッピング値を入力します。たとえば、テーブル マップが DSCP/CoS のテーブル マップである場合、*from-value* は DSCP 値で、*to-value* は CoS 値となります。指定できる範囲は、いずれも 0 ～ 63 です。 このコマンドを複数回入力して、マッピングするすべての値を含めるようにします。
ステップ 4	**default** {*default-value* | **copy** | **ignore**}	テーブル マップで検出されない値のデフォルト動作を設定します。 • *default-value* を入力して、特定の値を指定します。たとえば、DSCP/CoS テーブル マップでは、すべてのマッピングされていない DSCP 値に適用する特定の CoS 値となります。指定できる範囲は 0 ～ 63 です。 • **copy** を入力して、マッピングされていない値を同等な値にマッピングします。DSCP/CoS テーブル マップでは、このコマンドによりすべてのマッピングされていない DSCP 値が同等の CoS 値にマッピングされます。 • **ignore** を入力すると、マッピングされていない値は変更されません。DSCP/CoS テーブル マップでは、マッピングされていない DSCP 値の CoS 値は変更されません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show table-map** [*table-map-name*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

テーブル マップを削除するには、**no table-map** *table-map-name* グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP/CoS テーブル マップを作成する例を示します。完全なテーブルには通常、大きな DSCP 値用の追加の map 文が含まれます。このテーブルのデフォルト 4 は、マッピングされていない DSCP が CoS 値 4 に割り当てられるということを意味します。

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 1 to 1
Switch(config-tablemap)# map from 2 to 1
Switch(config-tablemap)# map from 3 to 1
Switch(config-tablemap)# map from 4 to 2
Switch(config-tablemap)# map from 5 to 2
Switch(config-tablemap)# map from 6 to 3
Switch(config-tablemap)# default 4
Switch(config-tablemap)# end
Switch# show table-map dscp-to-cos
```

インターフェイスへのトラフィック ポリシーの付加

service-policy インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスにトラフィック ポリシーを付加し、ポリシーが適用される方向（着信トラフィックの入力ポリシー マップ、または発信トラフィックの出力ポリシー マップ）を指定します。入力ポリシー マップおよび出力ポリシー マップは、別々の QoS 機能をサポートします。入力ポリシー マップおよび出力ポリシー マップの制限事項に関しては、「入力ポリシー マップの設定」（P.34-47）および「出力ポリシー マップの設定」（P.34-65）を参照してください。

サービス ポリシーは、物理ポートにだけ付加できます。ポートごとに、入力ポリシー マップおよび出力ポリシー マップをそれぞれ 1 つだけ付加できます。

（注）　**no** policy-map コンフィギュレーション コマンドまたは **no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシー マップを削除する場合、ポリシー マップが消去されているインターフェイスの一覧を示す警告メッセージが表示されます。ポリシー マップは消去および削除されます。たとえば、次のようなメッセージが表示されます。

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

ポートに ポリシー マップを付加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	ポリシー マップに付加するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスは物理ポートです。
ステップ 3	**service-policy** {**input** | **output**} *policy-map-name*	ポリシー マップの名前、およびそれが入力ポリシー マップか出力ポリシー マップのいずれかを指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show policy-map interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポリシー マップとポートの関連付けを解除するには、**no service-policy** {**input** | **output**} *policy-map-name* インターフェイス コンフィギュレーション コマンドを使用します。

入力ポリシー マップの設定

ポリシー マップでは、動作の実行対象トラフィック クラスおよびそのアクションを指定します。トラフィック クラスの一致基準に一致しないすべてのトラフィックは、デフォルト クラスに属します。スイッチに着信するトラフィックは、入力ポリシー マップにより規制されます。入力ポリシー マップでは、CoS、DSCP、IP precedence、ACL、または VLAN ID を照合して、個別のポリシング、集約ポリシング、または CoS 値、IP precedence 値、QoS グループ値へのマーキングを設定できます。

入力ポリシー マップの設定を行うときは、次の注意事項に従ってください。

- 1 つのポートに付加できる入力ポリシー マップは 1 つに限られます。
- スイッチ上に設定されるポリシー マップの最大数は 256 です。

- ME-3400 上に設定できるポリサー プロファイルの合計数は 254 です。ME-3400E でサポートされているポリサー インスタンスの合計数は 1024 - 1 で、スイッチ上のインターフェイス数より多い数です。24 ポート スイッチでは、使用できるポリサー インスタンスの数は 999 です。ポリサー プロファイルは複数のインスタンスで使用できます。
- 各入力ポリシー マップの最大クラス数は、64 + **class-default** です。
- スイッチに付加できる入力ポリシー マップ数は、ハードウェア リソースのアベイラビリティにより制限されます。いずれかのハードウェア リソースの制限を超過する原因となる入力ポリシー マップを付加しようとすると、設定エラーになります。
- **service-policy input** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスに単一レベルのポリシー マップを付加すると、インターフェイスからポリシーを消去せずに、ポリシーを変更できます。分類基準、クラス、またはアクションの追加または削除、もしくは設定されたアクション（ポリサー、レート、マッピング、マーキングなど）のパラメータの変更を行えます。また、ポート単位、VLAN 単位の階層型ポリシー マップのように、階層型ポリシー マップの子ポリシーの基準の変更にも適用されます。

  階層型ポリシー マップの親ポリシーの場合、ポリシー マップがインターフェイスに付加されていると、親レベルのクラスを追加または削除できません。インターフェイスからポリシーを消去して、ポリシーを変更してから、このポリシーを再度インターフェイスに付加する必要があります。
- 最大 2 レベルの階層型ポリシー マップを、親レベルの VLAN ベース分類だけ含み、子レベルの VLAN ベース分類を含まない入力ポリシー マップとして設定できます。
- レイヤ 2 分類だけを含む入力ポリシー マップが、ルーテッド SVI を含むルーテッド ポートまたはスイッチ ポートに付加されている場合、サービス ポリシーはルーティング適格トラフィック上ではなく、スイッチング適格トラフィック上でだけ作用します。
- 802.1Q トンネル ポート上でトラフィックを分類するには、MAC ACL に基づくレイヤ 2 分類を含む入力ポリシー マップだけが使用できます。CoS または VLAN ID に基づくレイヤ 3 分類またはレイヤ 2 分類を含む入力ポリシー マップは、トンネル ポート上でサポートされません。
- 入力ポリシー マップは、スケジューリングまたはキューイングではなく、ポリシングおよびマーキングをサポートします。入力ポリシー マップでは、**bandwidth**、**priority**、**queue-limit**、または **shape average** を設定できません。

次に、異なるタイプの入力ポリシー マップの設定方法を説明します。

- 「個別のポリシングを含む入力ポリシー マップの設定」（P.34-48）
- 「集約ポリシングを含む入力ポリシー マップの設定」（P.34-54）
- 「マーキングを含む入力ポリシー マップの設定」（P.34-58）
- 「階層型入力ポリシー マップを含むポート単位、VLAN 単位 QoS の設定」（P.34-60）

個別のポリシングを含む入力ポリシー マップの設定

トラフィックの認定速度制限、認定バースト サイズ制限、およびトラフィック クラスの動作を定義するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、個別のポリサーを設定します。

個別のポリサーを設定する場合は、次の注意事項に従ってください。

- ポリシングは、入力ポリシー マップ上でだけサポートされます。
- スイッチ上では、最大 229 のポリサーがサポートされます （228 のユーザ設定可能なポリサーと、1 つの内部使用に予約されたポリサー）。

- CPU 保護がイネーブルになっている場合（デフォルト）、ポート当たり 45 の入力ポリサーを設定できます。**no policer cpu uni all** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードして CPU 保護をディセーブルにすると、ユーザ定義クラスにはポート当たり最大 63 のポリサー（すべての 4 番目のポート上で 62）および class-default に 1 つのポリサーを設定できます。**show policer cpu uni-eni** {**drop** | **rate**} 特権 EXEC コマンドを入力し、CPU 保護がイネーブルになっているかどうか確認できます。
- 入力ポリシー マップのポリシング超過アクションにテーブル マップを使用する場合、*map from* アクションタイプのプロトコル タイプは、対応する分類のプロトコル タイプと同じである必要があります。たとえば、対応するクラス マップが IP 分類を表す場合、テーブル マップを参照する **map from** アクション タイプは、**dscp** または **precedence** である必要があります。対応するクラス マップが非 IP 分類を表す場合、テーブル マップを参照する **map from** アクションタイプは、**cos** である必要があります。
- 2-rate、3-color ポリシングは、入力ポリシー マップでだけサポートされており、1-rate、2-color ポリシングは入力および出力ポリシー マップ両方でサポートされています。
- スイッチ上のポリサー インスタンスの数は 1024 -（インターフェイス数 + 1）です。スイッチは、最大 254 のポリサー プロファイルをサポートします。
- violate-action を設定しない場合、デフォルトで違反クラスが exceed-action と同じアクションに割り当てられます。

no policy-map コンフィギュレーション コマンドまたは **no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシー マップを削除する場合、ポリシー マップが消去されているインターフェイスの一覧を示する警告メッセージが表示されます。ポリシー マップは消去および削除されます。たとえば、次のようなメッセージが表示されます。

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

個別の 2-rate、3-color ポリシングを含む入力ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。デフォルトでは、クラス マップは定義されていません。
ステップ 3	**class** {*class-map-name* | **class-default**}	クラスマップ名またはすべての未分類のパケットを照合する **class-default** を入力して、ポリシー マップ クラス コンフィギュレーション モードを開始します。 クラスマップ名を入力する場合には、**class-map** グローバル コンフィギュレーション コマンドにより、クラス マップを作成しておく必要があります。

	コマンド	目的
ステップ 4	**police** {*rate-bps* | **cir** {*cir-bps*} [*burst-bytes*] [**bc** [*conform-burst*] [**pir** *pir-bps* [**be** *peak-burst*]]	トラフィックのクラスの 1 つまたは 2 つのレート、Committed Information Rate（CIR; 認定情報レート）および Peak Information Rate（PIR; 最大情報レート）を使用してポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。 • *rate-bps* には、平均トラフィック レートを bps 単位で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • **cir** *cir-bps* には、bc トークン バケットが更新される CIR を bps で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • *burst-bytes*（任意）には、標準バースト サイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）**bc** *conform-burst* には、ポリシングの bc トークン バケットで使用される認定バーストを指定します。指定できる範囲は、8000 ～ 1000000 バイトです。 • （任意）**pir** *pir-bps* には、ポリシングの be トークン バケットが更新される最大情報レートを指定します。指定できる範囲は、8000 ～ 1000000000 b/s です。**pir** *pir-bps* を入力しない場合、ポリサーは 1-rate、2-color ポリサーとして設定されます。 • **be** *peak-burst* には、be トークン バケットで使用するピーク バースト サイズを指定します。指定できる範囲は 8000 ～ 1000000 バイトです。デフォルト値は、ユーザ設定に基づき内部で計算されます。

	コマンド	目的
ステップ 5	**conform-action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**] | **exceed-action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**] | **violate- action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**]	（任意）パケットが CIR に適合するか、PIR に適合するかにより、パケットで実行するアクションを入力します。 • （任意）**conform-action** については、CIR および PIR に適合するパケットで実行するアクションを指定します。デフォルトは **transmit** です。 • （任意）**exceed-action** については、PIR に適合するが、CIR には適合しないパケットで実行するアクションを指定します。デフォルトは **drop** です。 • （任意）**violate-action** については、PIR を超過するパケットで実行するアクションを指定します。デフォルトは **drop** です。 • （任意）*action* については、パケットで実行する次のいずれかのアクションを指定します。 – **drop**：パケットを廃棄します。 **（注）** 適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。 – **set-cos-transmit** *cos-value*：パケットに割り当てる新しい CoS 値を入力し、パケットを送信します。指定できる範囲は 0 ～ 7 です。 – **set-dscp-transmit** *dscp-value*：パケットに割り当てる新しい IP DSCP 値を入力し、パケットを送信します。指定できる範囲は 0 ～ 63 です。また、よく使用される値にはニーモニック名を入力できます。 – **set-prec-transmit** *cos-value*：パケットに割り当てる新しい IP precedence 値を入力し、パケットを送信します。指定できる範囲は 0 ～ 7 です。 – **set-qos-transmit** *qos-group-value*：出力側で使用される QoS グループを識別して、特定のパケットを指定します。指定できる範囲は 0 ～ 99 です。 – **transmit**：パケットを変更せず送信します。 **（注）** police コマンドのあとに、単一の適合アクションをコマンドストリングの一部として入力できます。また、**police** コマンドのあとに Enter キーを押して、ポリシー マップ クラス ポリシング コンフィギュレーション モードを開始でき、ここで複数のアクションを入力できるようになります。ポリシー マップ クラス ポリシング コンフィギュレーション モードでは、実行するアクションを入力する必要があります。
ステップ 6	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**service-policy input** *policy-map-name*	入力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。

	コマンド	目的
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show policy-map** [*policy-map-name*| **interface**]	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

作成した入力ポリシー マップを、入力方向のインターフェイスに付加します。「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）を参照してください。

既存のポリシー マップ、クラス マップ、またはポリサーを削除するには、該当するコマンドの **no** 形式を使用します。

次に、ポリシーマップ コンフィギュレーション モードを使用して 2-rate、3-color ポリシングを設定する例を示します。

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000 conform-action transmit
exceed-action set-dscp-transmit 24 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

次に、ポリシーマップ クラス ポリシング コンフィギュレーション モードで同じ設定を作成する例を示します。

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

次に、CoS 値が 4 のトラフィック分類を作成して、ポリシー マップを作成し、入力ポートに付加する例を示します。平均トラフィック レートは、10000000 b/s に制限され、バースト サイズは 10000 バイトです。

```
Switch(config)# class-map video-class
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police 10000000 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input video-policy
Switch(config-if)# exit
```

次に、**set dscp** の適合アクションおよびデフォルトの超過アクションを含むポリシー マップを作成する例を示します。

```
Switch(config)# class-map in-class-1
Switch(config-cmap)# match dscp 14
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class in-class-1
Switch(config-pmap-c)# police 230000 8000 conform-action set-dscp-transmit 33
exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

次に、ポリシーマップ クラス ポリシング コンフィギュレーション モードを使用して、複数の適合アクションおよび 1 つの超過アクションを設定する例を示します。このポリシー マップでは、CIR を 23000 bps に、適合バースト サイズを 10000 バイトに設定します。このポリシー マップには、複数の適合アクション（DSCP 用およびレイヤ 2 CoS 用）および超過アクションが含まれます。

```
Switch(config)# class-map cos-set-1
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input map1
Switch(config-if)# exit
```

次に、ポリシーマップ クラス ポリシング コンフィギュレーション モードで、テーブル マップを使用して超過アクションのマークダウンを設定する例を示します。このポリシー マップでは、CIR を 23000 bps に、適合バースト サイズを 10000 バイトに設定します。このポリシー マップには、デフォルトの適合アクション（**transmit**）およびテーブル マップに基づいてレイヤ 2 CoS 値をマークダウンし、af41 の IP DSCP をマーキングする超過アクションが含まれます。

```
Switch(config)# policy-map in-policy
Switch(config-pmap)# class in-class-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# exceed-action set-cos-transmit cos table
police-cos-markdn-tablemap
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit af41
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

集約ポリシングを含む入力ポリシー マップの設定

集約ポリサーを設定するには、**policer aggregate** グローバル コンフィギュレーション コマンドを使用します。集約ポリサーは、同一ポリシー マップ内の複数のトラフィック クラスで共有されます。集約ポリサーを定義し、ポリシー マップを作成し、ポリシー マップにクラス マップを関連付け、集約ポリサーにポリシー マップを関連付け、ポートにサービス ポリシーを適用します。

集約ポリサーを設定する場合は、次の注意事項に従ってください。

- 集約ポリシングは、入力ポリシー マップ上でだけサポートされます。
- スイッチ上では、ポートに関連付けられた最大 229 のポリサーがサポートされます（228 のユーザ設定可能なポリサーと、1 つの内部使用に予約されたポリサー）。ポート上では、最大 45 のポリサーを設定できます。
- CPU 保護がイネーブルになっている場合（デフォルト）、ポート当たり 45 の入力ポリサーを設定できます。**no policer cpu uni all** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードして CPU 保護をディセーブルにすると、ユーザ定義クラスにはポート当たり最大 63 のポリサー（すべての 4 番目のポート上で 62）および class-default に 1 つのポリサーを設定できます。**show policer cpu uni-eni** {**drop** | **rate**} 特権 EXEC コマンドを入力し、CPU 保護がイネーブルになっているかどうか確認できます。
- 設定される集約ポリサーの最大数は 256 です。
- スイッチ上のポリサー インスタンスの数は 1024 -（スイッチ上の合計インターフェイス数 + 1）です。スイッチは、最大 254 のポリサー プロファイルをサポートします。
- violate-action を設定しない場合、デフォルトで違反クラスが exceed-action と同じアクションに割り当てられます。
- 1 つのポリシー マップだけが、任意の特定の集約ポリサーを使用できます。集約ポリシングは、複数のインターフェイス上のストリームの集約には使用できません。集約ポリシングは、インターフェイスに付加されるポリシー マップの複数のクラスにまたがるストリームの集約、およびポート単位、VLAN 単位ポリシー マップのポート上の VLAN にまたがるトラフィック ストリームの集約にだけ使用できます。
- 入力ポリシー マップのポリシング超過アクションにテーブル マップを使用する場合、map from アクションタイプのプロトコル タイプは、対応する分類のプロトコル タイプと同じである必要があります。たとえば、対応するクラス マップが IP 分類を表す場合、テーブル マップを参照する **map from** のアクション タイプは、**dscp** または **precedence** のいずれかである必要があります。対応するクラス マップが非 IP 分類を表す場合、テーブル マップを参照する **map from** アクションタイプは、**cos** である必要があります。
- **exceed-action** のテーブル マップを設定し、違反アクションのアクションが明示的に設定されていない限り、集約ポリシングの **violate-action** に対するテーブル マップはサポートされません。

複数の適合、超過、違反アクションを集約ポリサーに **policer aggregate** グローバル コンフィギュレーション コマンドのパラメータとして同時に設定できますが、次の順序でアクションを入力する必要があります。

- **drop**、または **transmit** あるいは **set** アクションは、**conform-action** のあとに次の順序で入力する必要があります。

  set-qos-transmit

  set-dscp-transmit または **set-prec-transmit**

  set-cos-transmit

- **drop**、**transmit** または **set** アクションは、**exceed-action** のあとに次の順序で入力する必要があります。

  set-qos-transmit

set-dscp-transmit または **set-prec-transmit**

set-cos-transmit

- **drop**、**transmit** または **set** アクションは、**violate-action** のあとに次の順序で入力する必要があります。

  set-qos-transmit

  set-dscp-transmit または **set-prec-transmit**

  set-cos-transmit

（注）　ポリシー マップ クラス ポリシング コンフィギュレーション モードでは、集約ポリサーの適合アクション、超過アクション、および違反アクションは設定しません。すべてのアクションはストリングで入力する必要があります。その結果、複数の適合、超過、および違反の各アクションを入力すると、コマンドが著しく長くなり、切り捨てられたり読みにくくなる場合があります。

2-rate、3-color 集約ポリサーを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policer aggregate** *aggregate-policer-name* {*rate-bps* | **cir** *cir-bps*} [*burst-bytes*] [**bc** [*conform-burst*] [**pir** *pir-bps* [**be** *peak-burst*]] [**conform-action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**] [**exceed-action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**]] [**violate- action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**]} | **set-qos-transmit** *qos-group_value* | **transmit**]]	同じポリシー マップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。 • *aggregate-policer-name* には、集約ポリサーの名前を指定します。 • *rate-bps* には、平均トラフィック レートを b/s 単位で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • **cir** *cir-bps* には、最初のトークン バケットが更新される CIR を b/s 単位で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • *burst-bytes*（任意）には、標準バースト サイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）**bc** *conform-burst* には、ポリシングの最初のトークン バケットで使用される認定バーストを指定します。指定できる範囲は、8000 ～ 1000000 バイトです。 • （任意）**pir** *pir-bps* には、ポリシングの 2 番目のトークン バケットが更新される最大情報レートを指定します。指定できる範囲は 8000 ～ 1000000000 bps です。**pir** *pir-bps* を入力しない場合、ポリサーは 1-rate、2-color ポリサーとして設定されます。 • **be** *peak-burst* には、2 番目のトークン バケットで使用するピーク バースト サイズを指定します。指定できる範囲は 8000 ～ 1000000 バイトです。デフォルト値は、ユーザ設定に基づき内部で計算されます。 • （任意）**conform-action** については、CIR に適合するパケットで実行するアクションを指定します。デフォルトでは、パケットを送信します。 **（注）** 適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。 • （任意）**exceed-action** については、CIR に適合するパケットで実行するアクションを指定します。デフォルトでは、パケットを廃棄します。 • （任意）**violate-action** については、CIR に適合するパケットで実行するアクションを指定します。デフォルトでは、パケットを廃棄します。 アクション キーワードの定義については、このリリースのコマンド リファレンス、または「個別のポリシングを含む入力ポリシー マップの設定」（P.34-48）を参照してください。 **（注）** **exceed-action** のテーブル マップを設定し、違反アクションのアクションが明示的に設定されていない限り、集約ポリシングの **violate-action** に対するテーブル マップは設定できません。
ステップ 3	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**class** {*class-map-name* | **class-default**}	クラスマップ名またはすべての未分類のパケットを照合する **class-default** を入力して、ポリシー マップ クラス コンフィギュレーション モードを開始します。 クラスマップ名を入力する場合には、**class-map** グローバル コンフィギュレーション コマンドにより、クラス マップを作成しておく必要があります。
ステップ 5	**police aggregate** *aggregate-policer-name*	同じポリシー マップの複数のクラスに集約ポリサーを適用します。*aggregate-policer-name* には、ステップ 2 で指定した名前を入力します。
ステップ 6	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**service-policy input** *policy-map-name*	入力インターフェイスにポリシー マップ（ステップ 3 で作成）を付加します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show policer aggregate** [*aggregate-policer-name*]	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

集約ポリサーを作成してから、それを入力ポートに付加します。「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）を参照してください。

指定した集約ポリサーをポリシー マップから削除するには、**no police aggregate** *aggregate-policer-name* ポリシー マップ コンフィギュレーション モードを使用します。集約ポリサーおよびそのパラメータを削除するには、**no policer aggregate** *aggregate-policer-name* グローバル コンフィギュレーション コマンドを使用します。

次に、集約ポリサーを作成し、ポリシー マップ内の複数のクラスに付加する例を示します。ポリシー マップは入力ポートに付加されます。

```
Switch(config)# policer aggregate example 10900000 80000 conform-action transmit
exceed-action drop
Switch(config)# class-map testclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map testclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# class testclass2
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

次に、2-rate、3-color 集約ポリサーを作成し、ポリシー マップ内の複数のクラスに付加する例を示します。ポリシー マップは入力ポートに付加されます。

```
Switch(config)# policer aggregate example cir 10900000 pir 80000000 conform-action
transmit exceed-action drop violate-action drop
Switch(config)# class-map testclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map testclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# class testclass2
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

マーキングを含む入力ポリシー マップの設定

特定のクラスに属するトラフィックのアトリビュートを設定または変更するには、**set** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。ポリシー マップでマーキングの設定を行うときは、次の注意事項に従ってください。

- スイッチ上には、最大 100 の QoS グループを設定できます。
- 入力ポリシー マップのマーキングにテーブル マップを使用する場合、map from アクション タイプのプロトコル タイプは、対応する分類のプロトコル タイプと同じである必要があります。たとえば、対応するクラス マップが IP 分類を表す場合、テーブル マップを参照する **map from** のアクション タイプは、**dscp** または **precedence** のいずれかである必要があります。対応するクラス マップが非 IP 分類を表す場合、テーブル マップを参照する **map from** アクションタイプは、**cos** である必要があります。

トラフィックをマーキングする入力ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 3	**class** {*class-map-name* | **class-default**}	クラスマップ名または **class-default** を入力して、すべての未分類のパケットを照合し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 クラスマップ名を入力する場合には、**class-map** グローバル コンフィギュレーション コマンドにより、クラス マップを作成しておく必要があります。

	コマンド	目的
ステップ 4	**set qos-group** *value* および **set cos** {*cos_value* | **cos** [**table** *table-map-name*] | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]} および **set** [**ip**] **dscp** {*dscp_value* | **cos** [**table** *table-map-name*] | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]} および **set** [**ip**] **precedence** {*precedence_value* | **cos** [**table** *table-map-name*] | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]}	パケットに新しい値を設定するか、テーブル マップを指定するか、または QoS グループを指定することにより、トラフィックをマーキングします。 • **qos-group *value*** には、出力側で使用される QoS グループを識別して、特定のパケットを識別します。指定できる範囲は 0 ～ 99 です。 • **cos** *cos_value* には、分類されたトラフィックに割り当てる新しい CoS 値を入力します。指定できる範囲は 0 ～ 7 です。 • [**ip**] **dscp** *new-dscp* には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。 • [**ip**] **precedence** *new-precedence* には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ～ 7 です。 • または、CoS、DSCP、もしくは IP precedence テーブルを設定して、任意でテーブル名を入力します。**table** *table-map name* を入力しない場合、テーブル マップは、デフォルトの動作 **copy** になります。「テーブル マップの設定」（P.34-45）を参照してください。
ステップ 5	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**service-policy input** *policy-map-name*	入力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポリシー マップまたはテーブル マップを削除する場合、または割り当てられた CoS 値、DSCP 値、precedence 値、または QoS グループ値を削除する場合は、該当するコマンドの **no** 形式を使用します。

次に、ポリシー マップを使用してパケットをマーキングする例を示します。最初のマーキング（**set** コマンド）は、クラス *AF31* ～ *AF33* によって一致しなかったすべてのトラフィックを照合する QoS デフォルト クラス マップに適用され、すべてのトラフィックの IP DSCP 値を 1 に設定します。2 番目のマーキングは、クラス AF31 ～ AF33 のトラフィックの IP DSCP を 3 に設定します。

```
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

階層型入力ポリシー マップを含むポート単位、VLAN 単位 QoS の設定

ポート単位、VLAN 単位 QoS により、所定のインターフェイスおよび VLAN 上で受信されるフレームへの QoS の適用に関して、VLAN ID に基づく分類が可能になります。これは、親ポリシーおよび子ポリシーを含む階層型ポリシー マップの使用により実現されます。

ポート単位、VLAN 単位 QoS を設定する場合は、次の注意事項および制限事項に留意してください。

- この機能は、2 レベルの階層型入力ポリシー マップを使用する場合に限り、サポートされます。このポリシー マップは、親レベルで VLAN ベースの分類を定義し、子レベルで 1 つまたは複数の該当する VLAN に適用される QoS ポリシーを定義します。
- 親レベルで複数のサービス クラスを設定することにより、各種 VLAN の組み合せを照合できます。また、子ポリシー マップを使用することにより、親サービス クラスごとに個別の QoS ポリシーを適用できます。
- 子ポリシー マップに関連付けられた 1 つまたは複数のクラスがあるポリシーは、親ポリシー マップと見なされます。親ポリシー マップ内の各クラスは、親クラスと呼ばれます。親クラスでは、**match vlan** クラス マップ コンフィギュレーション コマンドだけを設定できます。子ポリシー マップ内のクラスでは、**match vlan** コマンドを設定できません。
- ポート単位 VLAN 単位の親レベルのクラス マップでは、子ポリシー アソシエーションだけをサポートします。いずれのアクションも設定できません。親レベルのクラス マップでは、クラスの **class-default** のアクションまたは子ポリシー アソシエーションを設定できません。
- 子ポリシー マップ内では、レイヤ 2 とレイヤ 3 が混在するクラス マップを設定できません。このような子ポリシー マップを親ポリシーに関連付けようとすると、設定は拒否されます。ただし、レイヤ 2 とレイヤ 3 の子ポリシーを異なる親レベルのクラス マップに関連付けることはできます。
- ポート単位、VLAN 単位 QoS は、802.1Q トランク ポート上でだけサポートされます。
- VLAN または一連の VLAN に付加されている子ポリシー マップに、レイヤ 3 分類（**match ip dscp**、**match ip precedence**、**match IP ACL**）だけが含まれる場合は、これらの VLAN が、必ずポート単位 VLAN 単位ポリシーが付加されているポート上でだけ伝送されることに注意する必要があります。このルールに従わない場合は、これらの VLAN 上のスイッチに着信するトラフィックの QoS 動作が不適切になる場合があります。
- また、ポート単位 VLAN 単位が適用されるトランク ポート上で、**switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用して、VLAN メンバーシップを制限することも推奨します。レイヤ 3 分類が設定されたポート単位、VLAN 単位のポリシーが含まれるトランク ポート間で VLAN メンバーシップが重複した場合も、予期せぬ QoS 動作が発生する可能性があります。

ポート単位、VLAN 単位 QoS の設定手順は、次のとおりです。

- 「子ポリシーのクラス マップの作成」（P.34-61）
- 「親ポリシーのクラス マップの作成」（P.34-62）
- 「子ポリシー マップの作成」（P.34-63）
- 「親ポリシー マップの作成」（P.34-63）
- 「インターフェイスへの親ポリシー マップの付加」（P.34-64）

子ポリシーのクラス マップの作成

1 つまたは複数の子ポリシーのクラス マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *child-class-map-name*	クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。デフォルトでは、クラス マップは定義されていません。 • （任意）このクラス マップのすべての一致文に対して論理 AND を実行するには、キーワード **match-all** を使用します。この場合は、クラス マップ内のすべての一致基準と一致する必要があります。 • （任意）このクラス マップのすべての一致文に対して論理 OR を実行するには、キーワード **match-any** を使用します。この場合は、1 つまたは複数の一致基準と一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 一致文が指定されない場合、デフォルトは **match-all** になります。 **（注）** **match-all** クラス マップでは、複数の分類基準（match 文）を設定できません。

	コマンド	目的
ステップ 3	**match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **qos-group** *value* | **vlan** *vlan-list*}	トラフィックを分類する一致基準を定義します。デフォルトで、一致基準は定義されていません。 各クラス マップでサポートされる一致タイプおよび ACL は、それぞれ 1 つだけです。 • **access-group** *acl-index-or-name* を指定する場合は、ACL の番号または名前を指定します。アクセス グループの照合は、入力ポリシー マップでだけサポートされます。 • **cos** *cos-list* を指定する場合は、1 行に最大 4 つの CoS 値のリストを入力して、着信パケットと照合します。各値はスペースで区切ります。5 つ以上の CoS 値を照合する場合は、複数の *cos-list* 行を入力できます。指定できる範囲は 0 ～ 7 です。 • **ip dscp** *dscp-list* を指定する場合は、着信パケットと照合する最大 8 つの IPv4 DSCP 値を入力します。各値はスペースで区切ります。9 つ以上の DSCP 値を照合する場合は、複数の *dscp-list* 行を入力できます。指定できる数値範囲は 0 ～ 63 です。DSCP 値は、他の形式でも設定できます。「IP DSCP に基づく分類」（P.34-9）を参照してください。 • **ip precedence** *ip-precedence-list* を指定する場合は、着信パケットと照合する最大 4 つの IPv4 precedence 値のリストを入力します。各値はスペースで区切ります。5 つ以上の precedence 値を照合する場合は、複数の *ip-precedence-list* 行を入力できます。指定できる範囲は 0 ～ 7 です。 • **qos-group** *value* を指定する場合、QoS グループ番号を指定します。指定できる範囲は 0 ～ 99 です。QoS グループの照合は、出力ポリシー マップでだけサポートされます。 • **vlan** *vlan-list* を指定する場合、トランク ポート上のポート単位、VLAN 単位の QoS に関して親ポリシー マップで使用される VLAN ID または VLAN 範囲を指定します。VLAN ID の範囲は 1 ～ 4094 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show class-map**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

親ポリシーのクラス マップの作成

1 つまたは複数の親ポリシーのクラス マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map match-any** *parent-class-map-name*	親ポリシーに **match-any** クラス マップを作成して、クラスマップ コンフィギュレーション モードを開始します。 **（注）** 1 つの VLAN ID だけを照合する場合は、**match-all** を入力するか、または **match-any** もしくは **match-all** のいずれも入力しません（デフォルトの **match-all** になります）。

	コマンド	目的
ステップ 3	**match vlan** *vlan-id*	トラフィックを分類する 1 つまたは複数の VLAN を定義します。 *vlan-id* には、トランク ポート上のポート単位、VLAN 単位 QoS の親ポリシー マップで使用される、VLAN ID、スペースで区切られた一連の VLAN ID、またはハイフンで区切られた VLAN 範囲を指定します。VLAN ID の範囲は 1 ～ 4094 です。 また、**match vlan** コマンドを複数回入力すると、複数の VLAN を照合できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show class-map**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

子ポリシー マップの作成

1 つまたは複数の子ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *child-policy-map-name*	ポリシー マップ名を入力して子ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 3	**class** {*child-class-map-name* | **class-default**}	子クラスマップ名またはすべての未分類のパケットを照合する **class-default** を入力して、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 4	**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、トラフィック クラスのポリサーおよびアクションを設定するか、または **set** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、クラスに属するトラフィックをマーキングします。	
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show policy-map** [*child-policy-map-name* [**class** *class-map-name*]]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

親ポリシー マップの作成

親ポリシー マップを作成し、それをインターフェイスに付加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *parent-policy-map-name*	ポリシー マップ名を入力して親ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 3	**class** *parent-class-map-name*	親クラスマップ名を入力し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 4	**service policy** *child-policy-map-name*	親ポリシー マップに子ポリシー マップを関連付けます。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show policy-map** [*parent-policy-map-name* [**class** *class-map-name*]]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスへの親ポリシー マップの付加

作成した親ポリシー マップをインターフェイスに付加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 4	**switchport trunk allowed vlan** *vlan-list*	（推奨）ポート単位、VLAN 単位ポリシーにレイヤ 3 分類が含まれる場合は、トランク ポートの VLAN メンバーシップを制限して、VLAN メンバーシップが重複しないようにします。
ステップ 5	**service-policy input** *parent-policy-map-name*	入力インターフェイスに親ポリシー マップ（前述の手順で作成）を付加します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show policy-map interface** [*interface-id*]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、複数の親クラスを使用して、カスタマー VLAN 上の音声およびビデオの一致基準を分類する例を示します。

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match ip dscp af41
Switch(config-cmap)# exit
Switch(config)# class-map match-any voice
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# exit

Switch(config)# class-map match-any customer1-vlan
Switch(config-cmap)# match vlan 100-105
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer2-vlan
Switch(config-cmap)# match vlan 110-120
Switch(config-cmap)# exit

Switch(config)# policy-map child-policy-1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit

Switch(config)# policy-map child-policy-2
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police cir 5000000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# police cir 40000000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 4
Switch(config-pmap-c-police)# exceed-action set-cos-transmit 1
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit

Switch(config)# policy-map uni-parent
Switch(config-pmap)# class customer1-vlan
Switch(config-pmap-c)# service-policy child-policy-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class customer2-vlan
Switch(config-pmap-c)# service-policy child-policy-2
Switch(config-pmap-c)# exit

Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100-105, 110-120
Switch(config-if)# service-policy input uni-parent
Switch(config-pmap-c)# exit
```

出力ポリシー マップの設定

出力ポリシー マップは、スイッチから発信されるパケットの輻輳回避、キューイング、およびスケジューリングを管理するのに使用されます。スイッチには、4 つの出力キューがあり、そのキュー トラフィックを制御するには、出力ポリシー マップを使用します。これらのキューでは、シェーピング、キュー制限、および帯域幅を設定します。高いプライオリティ（クラスベース プライオリティ キューイング）を使用できます。クラスベース プライオリティ キューイングにポリシング付きプライオリティが設定されている場合以外は、ポリシングは出力ポリシー マップでサポートされません。出力ポリシー マップの分類基準には、CoS 値、DSCP 値、IP Precedence 値、または QoS グループ値の照合が含まれます。

物理ポートに出力ポリシー マップを設定する際は、次の注意事項に従ってください。

- スイッチ上のポート数に応じた数の出力ポリシー マップを設定および付加できます。複数の出力ポリシー マップで同じキュー制限設定を使用できます。ただし、これらのポリシー マップには、固有のキュー制限を 3 つしか設定できません。
- 出力ポリシー マップには、最大 4 つのクラス（クラス **class-default** を含む）を含めることができます。
- すべての出力ポリシー マップでは、同じ数（1、2、または 3 のいずれか）のクラス マップが定義されている必要があります。
- 出力ポリシー マップごとに各クラスで異なるアクションを設定できますが、すべての出力ポリシー マップで同じクラス設定を使用する必要があります。

- 子ポリシー マップでは、**class-default** が、**priority** および **police** 以外のすべての出力ポリシー マップ アクションをサポートします。**class-default** のキュー制限の設定で、スケジューリング動作を設定する必要がないこと以外は、**class-default** の動作制限はその他のクラスと同じです。
- 出力側の基準に基づいて分類する場合、その基準を入力側で確立する必要があります。マーキングはなくポリシングだけが設定されている場合に限り、分類を使用して、または任意のマーキング（**conform** または **exceed** マーキングを含むポリシングか、無条件の **set** マーキング）が設定されている場合は、明示的なマーキングを使用して、入力側で基準を確立できます。
- 出力ポリシー マップのクラス **class-default** にはクラスベース プライオリティ キューイングを設定できません。
- 出力ポリシー マップでは、プライオリティ キューイングが設定されていない限り、クラスのデフォルトには、ポート上の未設定の帯域幅に等しい最小帯域幅保証を受信します。
- 設定済みアクションのパラメータ（レート、パーセンテージなど）だけを変更したり、またはインターフェイスにポリシー マップが付加されている場合にクラス マップの分類基準を追加、削除する場合は、まず **service-policy** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスに出力ポリシー マップを付加します。クラスまたはアクションを追加、削除するには、すべてのインターフェイスからポリシー マップを消去して、変更し、再度インターフェイスに付加する必要があります。

（注） ポリシー マップで 3 つのクラスが必要となる予定がある場合は、その時点では 3 つすべてを使用しないときでも、ポリシー マップの作成時に 3 つのクラスを定義する必要があります。インターフェイスにポリシー マップを付加したあとで、ポリシー マップにクラスを追加できません。

- アクティブ ポートに少なくとも 1 つの出力ポリシー マップが付加されている場合、出力ポリシー マップが付加されていないアクティブ ポートでは、付加された出力ポリシー マップと同じクラスを使用しているトラフィックを適切にスケジューリングしたり、順序付けできない場合があります。使用中のすべてのポートに、出力ポリシー マップを付加することを推奨します。また、未使用のポートは、**shutdown** インターフェイス コンフィギュレーション コマンドを使用してシャットダウン ステートにすることも推奨します。たとえば、DSCP 23 トラフィックをシェーピングする出力ポリシー マップをポートに付加する場合に、同一ポートから他のトラフィックが送出されると、ポリシー マップが付加されていない他のポートから送信される DSCP トラフィックは適切にスケジューリングまたは順序付けされない場合があります。
- 出力ポリシー マップをポートに付加して、ポートが出力ポリシー マップを無効にするレートに自動ネゴシエーションされないようにする場合は、ポート速度の自動ネゴシエーションをディセーブルにするよう強く推奨します。**speed** インターフェイス コンフィギュレーション コマンドを使用すると、スタティックなポート速度を設定できます。自動ネゴシエーションするように設定されているポートで出力ポリシー マップが設定されていて、その速度がポリシーを無効にする値に自動ネゴシエーションされた場合、ポートは error-disabled ステートになります。
- 1 つのポートに付加できる出力ポリシー マップは、1 つに限られます。
- スイッチ上に設定されるポリシー マップの最大数は 256 です。

ここでは、異なるタイプの出力ポリシー マップの設定について説明します。

- 「CBWFQ を含む出力ポリシー マップの設定」（P.34-67）
- 「クラスベース シェーピングを含む出力ポリシー マップの設定」（P.34-68）
- 「ポート シェーピングを含む出力ポリシー マップの設定」（P.34-70）
- 「クラスベース プライオリティ キューイングを含む出力ポリシー マップの設定」（P.34-71）
- 「WTD を含む出力ポリシー マップの設定」（P.34-75）

CBWFQ を含む出力ポリシー マップの設定

CBWFQ を設定するには、**bandwidth** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。CBWFQ では、ポートで使用可能な総帯域幅の一部を割り当てることにより、キューの相対的な優先順位を設定します。

CBWFQ の設定時は、次の注意事項に従ってください。

- ポリシー マップで帯域幅を設定する場合は、すべてのレート設定を同じ形式（設定されたレートまたはパーセンテージ）にする必要があります。
- ポリシーの各キューにおける最小帯域幅保証の合計速度は、インターフェイスの合計速度を上回ることはできません。
- 出力ポリシー マップ内の同一のクラスに、CBWFQ（**bandwidth**）とトラフィック（**shape average**）またはプライオリティ キューイング（**priority**）を設定できません。
- 別のクラス マップで完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合には、帯域幅を絶対レートまたは総帯域幅に対するパーセンテージとして設定できません。
- 出力ポリシー マップの別のクラスで完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合にだけ、帯域幅を残りの帯域幅に対するパーセンテージで設定できます。
- クラスの CIR 帯域幅を絶対レートまたは総帯域幅に対するパーセンテージで設定する場合、ポリシー マップ内のすべてのクラスの CIR の処理後に残った余剰な帯域幅は、いずれも CIR レートと同じ比率でクラス間に分配されます。クラスの CIR レートを 0 に設定した場合、このクラスはいずれの余剰帯域幅に対しても不適格となり、帯域幅を取得できません。

最小帯域幅をビット レートまたはパーセンテージで指定することにより、CBWFQ を使用してトラフィック クラスに割り当てられる帯域幅を制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 3	**class** {*class-map-name* | **class-default**}	*子クラスマップ名*またはすべての未分類のパケットを照合する **class-default** を入力して、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 4	**bandwidth** {*rate* | **percent** *value* | **remaining percent** *value*}	ポリシー マップ クラスに出力帯域幅制限を設定します。 • 帯域幅を kps で設定するには、*rate* を入力します。指定できる範囲は 64 ～ 1000000 です。 • 総帯域幅のパーセンテージとして帯域幅を設定するには、**percent** *value* を入力します。指定できる範囲は 1 ～ 100% です。 • 残りの帯域幅のパーセンテージとして帯域幅を設定するには、**remaining percent** *value* を入力します。指定できる範囲は 1 ～ 100% です。このキーワードは、出力ポリシー マップ内の他のクラスに完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合に限り有効です。 出力ポリシー内の各帯域幅設定では、同一の単位（絶対レートまたはパーセンテージ）を指定する必要があります。合計保証帯域幅は、使用可能な合計レートを超過できません。
ステップ 5	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 7	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**service-policy output** *policy-map-name*	出力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

作成された出力ポリシー マップを、出力ポートに付加します。「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）を参照してください。

既存のポリシー マップ、クラス マップ、または帯域幅設定を削除するには、該当するコマンドの **no** 形式を使用します。

（注）　**no** policy-map コンフィギュレーション コマンドまたは **no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシー マップを削除する場合、ポリシー マップが消去されているインターフェイスの一覧を示す警告メッセージが表示されます。ポリシー マップは消去および削除されます。たとえば、次のようなメッセージが表示されます。

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

次に、クラス マップで定義されたトラフィック クラスに、使用可能な合計帯域幅の 25% を割り当てて、キューの優先順位を設定する例を示します。

```
Switch(config)# policy-map gold_policy
Switch(config-pmap)# class out_class-1
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output gold_policy
Switch(config-if)# exit
```

クラスベース シェーピングを含む出力ポリシー マップの設定

トラフィック シェーピングを設定するには、**shape average** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。クラスベース シェーピングは、インターフェイスから発信されるトラフィック クラスに適用される制御メカニズムで、クラスの CIR で使用されるデータ伝送速度を制限するには、shape average コマンドを使用します。

クラスベース シェーピングの設定を行うときは、次の注意事項に従ってください。

- トラフィック シェーピングのキュー設定により、キューの最大帯域幅および Peak Information Rate（PIR）が設定されます。Cisco ME スイッチでは、トラフィック シェーピングの自動設定により、キューの最小帯域幅保証または CIR も PIR と同じ値に設定されます。
- 出力ポリシー マップ内の同一のクラスに、CBWFQ（**bandwidth**）またはプライオリティ キューイング（**priority**）およびトラフィック（**shape average**）を設定できません。
- 出力ポリシー マップ内の別のクラスに、完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合、特定のトラフィック クラスにトラフィック シェーピングを設定できません。

クラスベース シェーピングを使用して、トラフィック クラスの最大許容平均速度を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 3	**class** {*class-map-name* | **class-default**}	*child class-map name* またはすべての未分類のパケットを照合する **class-default** を入力して、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 4	**shape average** *target bps*	平均クラスベース シェーピング速度を指定します。 *target bps* には、平均ビット レートを bps で指定します。指定できる範囲は 64000 ～ 1000000000 です。
ステップ 5	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**service-policy output** *policy-map-name*	出力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

作成された出力ポリシー マップを、出力ポートに付加します。「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）を参照してください。

既存のポリシー マップ、クラス マップ、またはクラスベース シェーピングの設定を削除するには、該当するコマンドの **no** 形式を使用します。

次に、ファスト イーサネット ポート上で発信トラフィックのトラフィック シェーピングを設定し、*outclass1*、*outclass2*、および *outclass3* が使用可能なポート帯域幅のうち最大 50 Mb/s、20 Mb/s、10 Mb/s を取得する例を示します。クラスの **class-default** は、残りのポート帯域幅を取得します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

ポート シェーピングを含む出力ポリシー マップの設定

ポート シェーピングは、インターフェイスから発信されるすべてのトラフィックに適用されます。**shape average** コマンドによりポートの最大帯域幅が指定されている場合は、クラスのデフォルトだけを使用するポリシー マップを使用します。子ポリシーが、階層型ポリシー マップ形式でクラスのデフォルトに付加されると、シェーピング ポート上のキューのクラスベース アクションを指定できます。

子ポリシーの各キューにおける最小帯域幅保証の合計（CIR）は、ポート シェーピングの合計速度を上回ることはできません。

ポート シェーピングを使用して、トラフィック クラスの最大許容平均速度を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *policy-map-name*	階層型ポリシー マップ名を入力して階層型ポリシー マップを作成し、親ポリシーのポリシーマップ コンフィギュレーション モードを開始します。
ステップ 3	**class class-default**	デフォルト クラスのポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 4	**shape average** *target bps*	平均クラスベース シェーピング速度を指定します。 *target bps* には、平均ビット レートを bps で指定します。指定できる範囲は 4000000 ～ 1000000000 です。
ステップ 5	**service-policy** *policy-map-name*	必要に応じて、階層型ポリシー マップで使用される子ポリシー マップを指定します。
ステップ 6	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**service-policy output** *policy-map-name*	出力インターフェイスに親ポリシー マップ（ステップ 2 で作成）を付加します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

作成された階層型出力ポリシー マップを、出力ポートに付加します。「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）を参照してください。

既存の階層型ポリシー マップ、ポート シェーピングの設定を削除したり、または階層型ポリシー マップからポリシー マップを削除するには、該当するコマンドの **no** 形式を使用します。

次に、前述の例で設定された *out-policy* ポリシー マップに基づいて割り当てられ、ポートを 90 Mbps にシェーピングする階層型ポリシー マップを設定して、ポート シェーピングを設定する例を示します。

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
```

```
Switch(config-if)# service-policy output out-policy-parent
Switch(config-if)# exit
```

クラスベース プライオリティ キューイングを含む出力ポリシー マップの設定

priority ポリシー マップ クラス コンフィギュレーション コマンドを使用すると、特定のトラフィック クラスで優先処理が行われるよう保証できます。完全プライオリティ キューイングの場合、プライオリティ キューは常に処理されます。キュー内のすべてのパケットは、キューが空になるまでスケジューリングされ、送信されます。プライオリティ キューを過剰に使用すると、他のキューのパケットが遅延して、不必要な輻輳が発生する可能性があります。

完全プライオリティ キューイング（ポリシングなしのプライオリティ）または無条件のプライオリティ ポリサー（ポリシングありのプライオリティ）を設定できます。プライオリティ キューイングの設定時は、次の注意事項に従ってください。

- **priority** コマンドは、スイッチ上で付加されたすべての出力ポリシーの単一の一意のクラスに関連付けられます。
- トラフィック クラスをプライオリティ キューとして設定する場合、同一クラスのその他のキューイング アクションとして設定できるのは、**police** および **queue-limit** だけです。同一クラスのプライオリティ キューを使用して、**bandwidth** または **shape average** を設定できません。
- **priority** コマンドは、出力ポリシー マップの **class-default** に関連付けられません。

ポリシングなしのプライオリティの設定

完全プライオリティ キューイング（ポリシングなしのプライオリティ）の設定を行う場合は、次の注意事項に従ってください。

- クラスベース シェーピング（**shape average**）または CBWFQ（**bandwidth**）が出力ポリシー マップ内の他のクラスに設定されている場合は、トラフィック クラスにポリシングなしのプライオリティ キューイングを設定できません。
- トラフィック クラスにポリシングなしのプライオリティ キューイングを設定する場合、余剰の帯域幅を割り当てるには、**bandwidth remaining percent** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、他のキューで共有を設定するしかありません。このコマンドは、割り当てられた帯域幅を保証しませんが、分散レートは保証されます。

完全プライオリティ キューを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** *class-map-name*	3 つの出力キューのクラスを作成します。各クラスの一致条件での分類を開始します。
ステップ 3	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class** *class-map-name*	プライオリティ クラスの名前（**class-map** グローバル コンフィギュレーション コマンドを使用して作成）を入力して、プライオリティ クラスでポリシーマップ クラス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 5	**priority**	このクラスに完全スケジューリング プライオリティを設定します。 （注）　**priority** コマンドに関連付けられるのは、スイッチ上の 1 つの一意のクラス マップだけです。その他のキューイング アクション（**bandwidth** または **shape average**）と、プライオリティを同時に設定できません。
ステップ 6	**exit**	プライオリティ クラスのポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 7	**class** *class-map-name*	非プライオリティ クラスの名前を入力して、そのクラスのポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**bandwidth remaining percent** *value*	ポリシー マップ クラスの出力帯域幅制限を、残りの帯域幅のパーセンテージとして設定します。指定できる範囲は 1 ～ 100% です。
ステップ 9	**exit**	クラスのポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**service-policy output** *policy-map-name*	出力インターフェイスにポリシー マップ（ステップ 3 で作成）を付加します。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show policy-map**	設定を確認します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

作成された出力ポリシー マップを、出力ポートに付加します。「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）を参照してください。

既存のポリシー マップまたはクラス マップの削除、プライオリティ クラスの完全プライオリティ キューイングまたは他のクラスへの帯域幅設定の解除を行うには、該当するコマンドの **no** 形式を使用します。

次に、クラス *out-class1* を完全プライオリティ キューとして設定し、このクラスのすべてのパケットが他のトラフィック クラスより先に送信される例を示します。他のトラフィック キューでは、*out-class2* は残りの帯域幅の 50%、*out-class3* は残りの帯域幅の 20% を取得するように設定されます。クラス **class-default** は、保証なしで、残りの 30% を取得します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

ポリシングを含むプライオリティの設定

ポリシング機能のあるプライオリティを使用して無条件のプライオリティ ポリサーを設定すると、プライオリティ キューで使用される帯域幅の制限、帯域幅の割り当て、または他のキューのシェーピングが可能になります。ポリシングを含むプライオリティの設定時は、次の注意事項に従ってください。

- CLI ヘルプでキーワードが表示される場合でも、無条件のプライオリティ ポリサーに対して認定バースト サイズを設定できません。出力サービス ポリシーを付加しようとすると、設定済みのバースト サイズはすべて無視されます。
- CLI ヘルプに表示される範囲が 8000 ～ 1000000000 bps である場合でも、許容ポリシング レートの範囲は 64000 ～ 1000000000 bps です。範囲外のレートでは、出力サービス ポリシーを付加できません。
- 同じ出力ポリシー マップ内の別のクラスで **bandwidth remaining percent** が設定されている場合は、トラフィック クラスにポリシングのあるプライオリティを設定できません。
- プライオリティで出力ポリシーの 1-rate、2-color ポリサーを設定できます。出力ポリシーの 2-rate、3-color ポリサーは設定できません。

ポリシングのあるプライオリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** *class-map-name*	3 つの出力キューのクラスを作成します。各クラスの一致条件での分類を開始します。
ステップ 3	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class** *class-map-name*	プライオリティ クラスの名前（**class-map** グローバル コンフィギュレーション コマンドを使用して作成）を入力して、プライオリティ クラスでポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**priority**	このクラスをプライオリティ クラスとして設定します。 （注）　**priority** コマンドに関連付けられるのは、スイッチ上の 1 つの一意のクラス マップだけです。
ステップ 6	**police** {*rate-bps* | **cir** *cir-bps*}	トラフィックのプライオリティ クラスのポリサーを定義します。 • *rate-bps* には、平均トラフィック レートを bps 単位で指定します。指定できる範囲は 64000 ～ 1000000000 です。 （注）　出力ポリシーで **police** コマンドと **priority** コマンドを併用する場合に、CLI ヘルプで表示される範囲が 8000 ～ 1000000000 bps であっても、ポリシング レートおよび CIR の範囲は 64000 ～ 1000000000 bps です。範囲外のレートでは、出力サービス ポリシーを付加できません。 • **cir** *cir-bps* には、CIR を bps で指定します。指定できる範囲は 64000 ～ 1000000000 です。 （注）　バースト サイズ オプションは、コマンド ライン ヘルプ ストリングで表示される場合でも、出力ポリシー マップでサポートされません。バースト サイズが設定された出力サービス ポリシー マップは付加できません。

	コマンド	目的
ステップ 7	**conform-action** [**transmit**]	（任意）CIR に適合するパケットで実行するアクションを入力します。アクションが入力されない場合は、デフォルトのパケット送信のアクションになります。 **（注）** **police** コマンドのあとに、単一の適合アクションをコマンド ストリングの一部として入力できます。また、**police** コマンドのあとに CR（復帰）を入力すると、ポリシーマップ クラス ポリシング コンフィギュレーション モードが開始され、適合アクションを入力できます。*police* コマンドが、出力ポリシー マップのプライオリティにより設定されている場合は、デフォルトの適合アクションである **transmit** だけがサポートされます。その他のポリシング適合アクションは、コマンド ライン ヘルプ ストリングで表示される場合でも、出力ポリシー マップでサポートされません。
ステップ 8	**exceed-action** [**drop**]	（任意）CIR に適合しないパケットに実行するアクションを入力します。アクションが入力されない場合は、デフォルトのパケット廃棄のアクションになります。 **（注）** **police** コマンドのあとに、単一の超過アクションをコマンド ストリングの一部として入力できます。また、**police** コマンドのあとに CR（復帰）を入力すると、ポリシーマップ クラス ポリス コンフィギュレーション モードが開始され、超過アクションを入力できます。*police* コマンドが、出力ポリシー マップのプライオリティにより設定されている場合は、デフォルトの超過アクションである **drop** だけがサポートされます。その他のポリシング超過アクションは、コマンド ライン ヘルプ ストリングで表示される場合でも、出力ポリシー マップでサポートされません。
ステップ 9	**exit**	プライオリティ クラスのポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 10	**class** *class-map-name*	最初に非プライオリティ クラスの名前を入力して、そのクラスのポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**bandwidth** {**rate** | **percent** *value*} または **shape average** *target bps*	ポリシー マップ クラスの出力帯域幅制限を kbps で設定するか（範囲は 64 ～ 1000000）、または総帯域幅に対するパーセンテージ（範囲は 1 ～100%）を設定します。または平均クラスベース シェーピング レートを bps で指定します（範囲は 64000 ～ 1000000000）。
ステップ 12	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 13	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**service-policy output** *policy-map-name*	出力インターフェイスにポリシー マップ（ステップ 3 で作成）を付加します。
ステップ 16	**end**	特権 EXEC モードに戻ります。
ステップ 17	**show policy-map**	設定を確認します。
ステップ 18	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

作成された出力ポリシー マップを、出力ポートに付加します。「インターフェイスへのトラフィック ポリシーの付加」（P.34-47）を参照してください。

既存のポリシー マップまたはクラス マップの削除、プライオリティ クラスのプライオリティ キューイング、ポリシング、または他のクラスへの帯域幅設定の解除を行うには、該当するコマンドの **no** 形式を使用します。

次に、**priority** コマンドと **police** コマンドを併用して、*out-class1* をプライオリティ キューとして設定し、キューに着信するトラフィックを 20000000 bps に制限して、プライオリティ キューがそれを超えるレートを使用しないようにする例を示します。このレートを超えるトラフィックは、廃棄されます。その他のトラフィック キューは、前述の例のとおり設定されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

WTD を含む出力ポリシー マップの設定

WTD では、トラフィック クラスに関連付けられたキュー サイズ（バッファ サイズ）を調整します。WTD は、**queue-limit** ポリシー マップ クラス コンフィギュレーション コマンドにより設定されます。

WTD を設定する場合は、次の注意事項に従ってください。

- **queue-limit** コマンドによる WTD の設定は、最初にスケジュール アクション（**bandwidth**、**shape average**、または **priority** など）を設定する場合にだけサポートされます。**class-default** で **queue-limit** を設定する場合は、例外です。
- ポート数に応じた数の出力ポリシー マップを設定および付加できます。複数の出力ポリシー マップで同じキュー制限設定を使用できます。ただし、これらのポリシー マップには、固有のキュー制限を 3 つしか設定できません。
- **queue-limit** コマンドを使用して CPU が生成したトラフィックのキュー制限を設定できます。
- **queue-limit** コマンドを使用して、クラスのキューしきい値を設定する場合、WTD しきい値は、キューの最大しきい値以下にする必要があります。修飾子なしで設定されたキュー サイズは、修飾子を使用して設定されたいずれのキュー サイズよりも大きくする必要があります。
- **queue-limit** コマンドで、WTD 修飾子（**cos**、**dscp**、**precedence**、**qos-group**）に 3 つ以上の一意のしきい値を設定できません。ただし、これらのしきい値にマッピングできる修飾子の数に制限はありません。修飾子なしの **queue-limit** コマンドを使用することにより、3 番めの一意のしきい値を設定して、最大キューを設定できます。
- **queue-limit** コマンドの WTD 修飾子は、関連するクラス マップの少なくとも 1 つの **match** 修飾子と同じである必要があります。
- 出力ポリシー マップで一意のクラスにキュー制限を設定した場合、他のすべての出力ポリシー マップでは、修飾子タイプおよび修飾値に同じ形式を使用する必要があります。キュー制限しきい値だけ、異なる値を設定できます。たとえば、**ポリシー マップ 1** の **dscp 30** および *dscp 50* に、クラス A のキュー制限のしきい値を設定して、ポリシー マップ 2 でクラス A のキュー制限を設定す

る場合、**dscp 30** および **dscp 50** を修飾子として使用する必要があります。**dscp 20** および **dscp 40** は、使用できません。別のしきい値を設定できますが、これにより、新しいキュー制限設定が作成されます。

WTD を使用してトラフィック クラスのキュー サイズを調整するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 3	**class** {*class-map-name* | **class-default**}	子クラスマップ名またはすべての未分類のパケットを照合する **class-default** を入力して、ポリシーマップ クラス コンフィギュレーション モードを開始します。 • クラスマップ名を入力する場合、ステップ 5 でキュー制限を設定する前に、ステップ 4 を実行して、スケジューリング アクション（**bandwidth**、**shape average**、または **priority**）を設定する必要があります。 • class-default を入力する場合は、ステップ 4 を省略できます。
ステップ 4	**bandwidth** {*rate* | **percent** *value* | **remaining percent** *value*} or **shape average** *target bps* or **priority**	トラフィック クラスのスケジューリング アクションを設定します。詳細については、「CBWFQ を含む出力ポリシー マップの設定」（P.34-67）、「クラスベース シェーピングを含む出力ポリシー マップの設定」（P.34-68）、「ポート シェーピングを含む出力ポリシー マップの設定」（P.34-70）、または「クラスベース プライオリティ キューイングを含む出力ポリシー マップの設定」（P.34-71）を参照してください。
ステップ 5	**queue-limit** [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] *number-of-packets* [**packets**]}	トラフィック クラスのキュー サイズを指定します。 • （任意）**cos** *value* には、CoS 値を指定します。指定できる範囲は 0 ～ 7 です。 • （任意）**dscp** *value* には、DSCP 値を指定します。指定できる範囲は 0 ～ 63 です。 • （任意）**precedence** *value* には、IP precedence 値を指定します。指定できる範囲は 0 ～ 7 です。 • （任意）**qos-group** *value* には、QoS グループ値を入力します。指定できる範囲は 0 ～ 99 です。 • *number-of-packets* には、WTD の最小しきい値を設定します。指定できる範囲は、16 の倍数で 16 ～ 544 です。この場合、各パケットは 256 バイトの固定単位になります。 **（注）** 最適なパフォーマンスを実現するため、キュー制限を 272 以下に設定することを推奨します。 値は、デフォルトでパケットに指定されますが、キーワード **packets** は任意です。 **（注）** 複数の出力ポリシー マップで同じキュー制限設定を使用できます。ただし、これらのポリシー マップには、固有のキュー制限を 3 つしか設定できません。
ステップ 6	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ポリシーを付加するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**service-policy output** *policy-map-name*	出力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。 **（注）** 4 つめのキュー制限設定を含む出力ポリシー マップを付加しようとすると、エラー メッセージが表示され、付加は許可されません。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

作成された出力ポリシー マップを、出力ポートに付加します。「出力ポリシー マップの設定」（P.34-65）を参照してください。

既存のポリシー マップ、クラス マップ、または WTD 設定を削除するには、該当するコマンドの **no** 形式を使用します。

次に、指定された帯域幅およびキュー サイズが設定されたポリシー マップの例を示します。DSCP 30 または 10 ではないトラフィックには、112 パケットのキュー制限が割り当てられます。DSCP 値が 30 のトラフィックには、48 パケットのキュー制限が、また、DSCP 値が 10 のトラフィックには、32 パケットのキュー制限が割り当てられます。クラス トラフィックに属していないすべてのトラフィックは、class-default に分類され、使用可能な合計帯域幅の 10% が、256 パケットのラージ キュー サイズで設定されます。

```
Switch(config)# policy-map gold-policy
Switch(config-pmap)# class traffic
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 112
Switch(config-pmap-c)# queue-limit dscp 30 48
Switch(config-pmap-c)# queue-limit dscp 10 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 256
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output gold-policy
Switch(config-if)# exit
```

CPU 生成トラフィックの QoS マーキングおよびキューイングの設定

CPU 生成トラフィックのマーキングおよびキューイングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	グローバル テーブル マップを設定します。	「テーブル マップの設定」（P.34-45）を参照してください。
ステップ 3	**cpu traffic qos cos** {***cos-value*** | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **prec** [**table-map** *table-map-name*]}	新しい CoS 値を設定するか、テーブル マップを指定することにより、トラフィックをマーキングします。 • *cos-value* には、新しい CoS 値を入力します。指定できる範囲は 0 ～ 7 です。 • また、CoS、DSCP、または IP-precedence 値に基づき CoS をマーキングできます。任意にテーブル マップを使用して、CoS を設定できます。**table-map** *table-map-name* を入力しない場合、テーブル マップは、デフォルトの動作 **copy** になります。「テーブル マップ」（P.34-15）を参照してください。 このステップを完了したら、ステップ 7 に進みます。
ステップ 4	**cpu traffic qos dscp** {***dscp_value*** | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **prec** [**table-map** *table-map-name*]}	新しい DsCP 値を設定するか、テーブル マップを指定することにより、トラフィックをマーキングします。 • **dscp** *new-dscp* には、分類されたトラフィックに新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。 • また、テーブル マップを設定して、CoS、DSCP、または IP-precedence 値に基づいて DSCP をマーキングできます。任意でテーブル名を入力できます。**table-map** *table-map-name* を入力しない場合、テーブル マップは、デフォルトの動作 **copy** になります。「テーブル マップ」（P.34-15）を参照してください。 • DSCP 分類オプションの詳細については、「IP DSCP に基づく分類」（P.34-9）を参照してください。 このステップを完了したら、ステップ 7 に進みます。
ステップ 5	**cpu traffic qos precedence** {***precedence_value*** | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **prec** [**table-map** *table-map-name*]}	新しい precedence 値を設定するか、テーブル マップを指定することにより、トラフィックをマーキングします。 • **precedence** *new-precedence* には、0 ～ 7 の番号または名前で新しい IP-precedence 値を入力します。使用できる名前および番号は、**routine (0)**、**priority (1)**、**immediate (2)**、**flash (3)**、**flash-override (4)**、**critical (5)**、**internet (6)**、**network (7)** です。 • また、テーブル マップを設定して、CoS、DSCP、または IP-precedence 値に基づいて precedence をマーキングできます。任意でテーブル名を入力できます。**table-map** *table-map-name* を入力しない場合、テーブル マップは、デフォルトの動作 **copy** になります。「テーブル マップ」（P.34-15）を参照してください。 このステップを完了したら、ステップ 7 に進みます。

	コマンド	目的
ステップ 6	**cpu traffic qos qos-group** *qos-group-value*	QoS グループを使用してトラフィックをマーキングします。 *qos-group-value* には、出力側で使用される QoS グループを識別します。指定できる範囲は 0 ～ 99 です。 このステップを完了したら、ステップ 7 に進みます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	COS、IP DSCP、IP precedence および QoS グループなどの QoS マーキングをクラス キューにマッピングするために出力ポリシー マップを設定し、キューイングおよびスケジューリングを設定します。	「出力ポリシー マップの設定」（P.34-65）を参照してください。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 10	**show running-config**	設定済みのクラス マップ、ポリシー マップ、ポリシー マップ、テーブル マップ、および CPU トラフィック QoS 設定を表示します。
ステップ 11	**show cpu traffic qos**	CPU 生成トラフィックの QoS マーキング値を表示します。
ステップ 12	**show table-map** [*table-map-name*]	すべてのテーブル マップまたは指定されたテーブル マップの情報を表示します。
ステップ 13	**show policy-map** [*policy-map-name* | **interface** [*interface-id*] [**output**] [**class** *class-name*]]	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシー マップ クラスの QoS ポリシー マップ情報を表示します。

コマンドをディセーブルにするには、そのコマンドの **no** 形式を使用します。

例 1

次に、CPU 生成 IP パケットの DSCP 値に基づいて出力キューイングを設定する例を示します。

- IP DSCP 値および設定済み出力ポリシー マップ *output-policy* に基づく、出力ポート上のすべての CPU 生成 IP トラフィック キュー。
- 音声トラフィックをシミュレートする DSCP 値が *ef* のすべての IP SLA または TWAMP プローブが *voice* クラスに割り当てられている。
- 音声トラフィックをシミュレートする DSCP 値が *af41*、*af42* および *af43* のすべての IP SLA または TWAMP が *video* クラスに割り当てられている。
- DSCP 値が 48 および 56 のすべての IP 制御プロトコル トラフィックが *network-internetwork-control* クラスに割り当てられている。
- 残りの IP トラフィックがデフォルト クラスに割り当てられている。
- すべての CPU 生成非 IP トラフィックが、スタティックに出力ポートの固定キューにマッピングされている。
- CoS に基づくクラスが存在しないため、すべての CFM トラフィックがデフォルト クラスにキューイングされている。

```
Switch(config)# cpu traffic qos dscp dscp
```

Class:

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match ip dscp af41 af42 af43
```

```
Switch(config-cmap)# exit

Switch(config)# class-map match-any voice
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# exit

Switch(config)# class-map match-any network-internetwork-control
Switch(config-cmap)# match ip dscp 48 56
Switch(config-cmap)# exit
```

Policy:

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class network-internetwork-control
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

Interface

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

例 2

次に、パケットの DSCP 値に基づいて CPU 生成 IP トラフィック（IP-SLA および TWAMP を含む）の CoS をマーキングし、CoS 値に基づいて出力キューイングを設定する例を示します。

- IP DSCP 値および *output-policy* という設定済み出力ポリシー マップに基づく、出力ポート上のすべての CPU 生成 IP トラフィック キュー。
- 音声トラフィックをシミュレートする DSCP 値が *ef* のすべての IP SLA または TWAMP プローブが *voice* クラスに割り当てられている。
- 音声トラフィックをシミュレートする DSCP 値が *af41*、*af42* および *af43* のすべての IP SLA または TWAMP が *video* クラスに割り当てられている。
- DSCP 値が 48 および 56 のすべての IP 制御プロトコル トラフィックが *network-internetwork-control* クラスに割り当てられている。
- 残りの IP トラフィックがデフォルト クラスに割り当てられている。
- CoS 5 のすべての CPU 生成非 IP トラフィックが *voice* クラスに割り当てられている。
- CoS 3 のすべての CPU 生成非 IP トラフィックが *video* クラスに割り当てられている。
- CoS 6 および 7 のすべての CPU 生成非 IP トラフィックが *network-internetwork-control* クラスに割り当てられている。
- CoS 5 のすべての CFM トラフィックが *voice* クラスに割り当てられている。
- CoS 3 のすべての CFM トラフィックが *video* クラスに割り当てられている。

- CoS 6 および 7 のすべての CFM トラフィックが *network-internetwork-control* クラスに割り当てられている。

Table Map:

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# map from af41 to 3
Switch(config-tablemap)# map from af42 to 3
Switch(config-tablemap)# map from af43 to 3
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

CPU QoS:

```
Switch(config)# cpu traffic qos cos dscp table-map dscp-to-cos
Switch(config)# cpu traffic qos cos cos
```

Class:

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit

Switch(config)# class-map match-any voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit

Switch(config)# class-map match-any network-internetwork-control
Switch(config-cmap)# match cos 6 7
Switch(config-cmap)# exit
```

Policy:

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class network-internetwork-control
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

Interface

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

例 3

次の例を示します。

- パケットの DSCP 値に基づいて CPU 生成 IP トラフィック（IP-SLA および TWAMP を含む）の DSCP 値をマーキングする。
- パケットの DSCP 値に基づいて CPU 生成 IP トラフィック（IP-SLA および TWAMP を含む）の CoS をマーキングする。
- パケットの CoS 値に基づいて CPU 生成非 IP トラフィックの CoS をマーキングする。
- QoS グループが付いたすべての CPU 生成トラフィックをマーキングする。
- QoS グループに基づいて出力キューイングを設定する。

次のような結果になります。

- DSCP 値が 46、48、および 56 のすべての CPU 生成 IP トラフィックでは、既存のマーキングが維持される。
- その他のすべての CPU 生成 IP パケットについては、DSCP 値はゼロにリセットされる。
- DSCP 値が 46、48、および 56 のすべての CPU 生成 IP トラフィックは、それぞれ対応する CoS 値 5、6、および 7 にマッピングされる。
- その他のすべての CPU 生成 IP パケットについては、CoS 値はゼロにリセットされる。
- CoS 値が 5、6、および 7 のすべての CPU 生成非 IP トラフィックでは、既存のマーキングが維持される。
- その他のすべての CPU 生成非 IP パケットについては、CoS 値はゼロにリセットされる。
- すべての CPU 生成トラフィックは、*cpu-traffic* という 1 つのクラスを通過する。*user-voice* クラスである *user-voice* および *user-video* は、ユーザ トラフィック用に確保されています。その結果、CPU トラフィックおよびユーザ トラフィック は出力ポートのさまざまなキューに分割されています。

Table Map

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end

Switch(config)# table-map dscp-to-dscp
Switch(config-tablemap)# map from 46 to 46
Switch(config-tablemap)# map from 48 to 48
Switch(config-tablemap)# map from 56 to 56
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end

Switch(config)# table-map cos-to-cos
Switch(config-tablemap)# map from 5 to 5
Switch(config-tablemap)# map from 6 to 6
Switch(config-tablemap)# map from 7 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

CPU QoS:

```
Switch(config)# cpu traffic qos dscp dscp table-map dscp-to-dscp
Switch(config)# cpu traffic qos cos dscp table dscp-to-cos
```

```
Switch(config)# cpu traffic qos cos cos table cos-to-cos
Switch(config)# cpu traffic qos qos-group 50
```

Class:

```
Switch(config)# class-map match-any cpu-traffic
Switch(config-cmap)# match qos-group 50
Switch(config-cmap)# exit

Switch(config)# class-map match-any user-video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit

Switch(config)# class-map match-any user-voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

Policy:

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class user-voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class user-video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cpu-traffic
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

Interface:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

QoS 情報の表示

QoS 情報を表示するには、表 34-2 に示す特権 EXEC コマンドを 1 つまたは複数組み合せて使用します。使用できるキーワードについては、このリリースのコマンド リファレンスを参照してください。

表 34-2　標準 QoS 情報を表示するためのコマンド

コマンド	目的
show class-map [*class-map-name*]	すべてのクラス マップまたは指定されたクラス マップの QoS クラスマップ情報を表示します。
show policer aggregate [*aggregate-policer-name*]	すべての集約ポリサーまたは指定された集約ポリサーの情報を表示します。
show policy-map [*policy-map-name* | **interface** [*interface-id*] [**input** | **output**] [**class** *class-name*]]	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシー マップ クラスの QoS ポリシー マップ情報を表示します。
show cpu traffic qos	CPU 生成トラフィックの QoS マーキング値を表示します。

表 34-2　標準 QoS 情報を表示するためのコマンド （続き）

コマンド	目的
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。
show table-map [*table-map-name*]	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報を表示します。

インターフェイス上の両方向で完全パス QoS をテストするには、**ethernet loopback facility** インターフェイス コンフィギュレーション コマンドを入力してイーサネット ターミナル ループバックを設定できます。ターミナル ループバック モードでは、ポートは、リンクがアップに見える状態になりますが、実際はリンクはダウンになっており、パケットは送信されません。ポートの設定変更は、ループバックされているトラフィックに即座に影響を与えます。イーサネット ターミナル ループバックの詳細については、「イーサネット ループバックのイネーブル化」（P.43-42）を参照してください。

QoS 統計情報

QoS 入力および出力ポリシー マップの統計情報を表示する方法は、いくつかあります。

入力ポリシー マップの場合、**show policy-map interface** [*interface-id*] 特権 EXEC コマンドを使用してクラス単位、ポリサー単位の適合および超過統計情報を表示できます。ポリサーの適合統計情報は設定済みポリサー プロファイルに適合するパケット数で、ポリサーの超過統計情報は設定済みポリサー プロファイルを超過したパケット数です。スイッチでは、クラス単位の分類統計情報をサポートしませんが、クラスの回線速度でポリシングを設定することによりこれらの統計情報を決定できます。この場合、設定済みポリサー プロファイルを超過するパケットはありません。また、ポリサーの適合統計情報はクラスの分類統計情報に等しくなります。

またこの出力には、conform、exceed、および violate の各クラスのバイト レベルの統計情報が含まれています。

入力 QoS 統計情報を表示する別の方法として、**show platform qos statistics interface** [*interface-id*] 特権 EXEC コマンドの出力があります。ポート単位のフレームの統計情報は、ポート上の着信フレームの DSCP 値および CoS 値でソートされています。これらの統計情報には、インターフェイス上で設定される MQC 入力ポリシー マップについての情報は含まれません。

出力ポリシー マップの場合、**show policy-map interface** [*interface-id*] コマンドを使用して、指定されたクラスに一致する合計パケット数を示すクラス単位の分類統計情報を表示できます。このカウントには、指定のクラスで送信および廃棄された合計パケット数も含まれます。クラス単位のテール ドロップ統計情報を表示する場合も、同じコマンドが使用できます。

ポリシー マップの設定例

ここでは、設定に関する注意事項および制限事項を含む Cisco ME スイッチ上での QoS ポリシーの設定例を示します。ここでは、カスタマーが実行する設定動作ごとにわかれています。各項では、設定または変更を正常に行うために必要な手順を正確な順序で説明します。

- 「カスタマー A の QoS 設定」（P.34-85）
- 「カスタマー B の QoS 設定」（P.34-87）
- 「出力ポリシーの変更および分類基準の追加と削除」（P.34-87）
- 「出力ポリシーの変更およびキューイングまたはスケジューリング パラメータの変更」（P.34-88）
- 「出力ポリシーの変更および設定済み動作の追加または削除」（P.34-89）
- 「出力ポリシーの変更およびクラスの追加または削除」（P.34-90）

カスタマー A の QoS 設定

ここでは、カスタマー スイッチの初期設定および QoS ポリシーのアクティブ化の例を示します。入力および出力 QoS サービス ポリシーは、要件に基づいて設定され、関連ポートに付加されます。

カスタマー A の初期設定では、ファスト イーサネット ポート 1 ～ 24 は User Network Interface（UNI; ユーザ ネットワーク インターフェイス）で、デフォルトではディセーブルです。ギガビット イーサネット ポート 1 ～ 2 は、Network Node Interface（NNI; ネットワーク ノード インターフェイス）で、デフォルトではイネーブルです。

次に、初期設定の全体的な流れを示します。

- クラスおよびポリシーを設定します。
- すべてのアクティブ ポートをシャットダウンします。
- アクティブ化されるようにポートにポリシーを付加します。
- ポートのシャットダウン ステートを終了する。
- 未使用のポートはシャットダウンのままにします。

出力ポリシーを設定する際の制限事項は、次のとおりです。

- 出力ポリシー マップでは、最大 3 つのクラスを定義できます。
- 定義されたクラスは、他の出力ポリシー マップと同一でなければなりません。
- 各出力ポリシーマップで定義されるクラス数は、同じである必要があります。
- クラスごとに動作を割り当てる必要があります。つまり、空のクラスはありません。
- 各クラス設定は、入力ポリシー マップで実行された分類/マーキングに基づいている必要があります。

次に、入力サービス ポリシーのクラスを設定し、3 つの サービス クラス（gold、silver、bronze）を定義する例を示します。**match-all** 分類（デフォルト）には単一の分類基準しかないため、**match-any** 分類を使用して将来的に分類基準を追加できるようにします。

```
Switch# config terminal
Switch(config)# class-map match-any gold-in
Switch(config-cmap)# match ip dscp af11
Switch(config-cmap)# exit
Switch(config)# class-map match-any silver-in
Switch(config-cmap)# match ip dscp af21
Switch(config-cmap)# exit
Switch(config)# class-map match-any bronze-in
Switch(config-cmap)# match ip dscp af31
Switch(config-cmap)# exit
```

次に、gold クラスをマーキングして、silver クラスを 50 Mb/s に、bronze クラスを 20 Mb/s にポリシングする入力ポリシー マップを設定する例を示します。

```
Switch(config)# policy-map input-all
Switch(config-pmap)# class gold-in
Switch(config-pmap-c)# set ip dscp af43
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-in
Switch(config-pmap-c)# police 50000000
Switch(config-pmap)# class bronze-in
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
```

次に、3 つの サービス クラス（gold、silver、bronze）を備えた出力サービス ポリシーのクラスを設定する例を示します。gold クラスは、入力サービス ポリシーでマーキングされた値を照合するように設定されます。**match-all** 分類（デフォルト）には単一の分類基準しかないため、**match-any** 分類を使用して将来的に分類基準を追加できるようにします。

```
Switch# config terminal
Switch(config)# class-map match-any gold-out
Switch(config-cmap)# match ip dscp af43
Switch(config-cmap)# exit
Switch(config)# class-map match-any silver-out
Switch(config-cmap)# match ip dscp af21
Switch(config-cmap)# exit
Switch(config)# class-map match-any bronze-out
Switch(config-cmap)# match ip dscp af31
Switch(config-cmap)# exit
```

次に、両方のギガビット イーサネット NNI に適用され、gold クラスへのレート制限があるプライオリティ、silver クラスへのクラスベース シェーピング、および bronze クラスへの 10% の最小帯域幅保証を割り当てる例を示します。

```
Switch(config)# policy-map output-g1-2
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# shape average 200000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
```

次に、ファスト イーサネット UNI 1 ～ 8 に適用される 2 番めの出力サービス ポリシーを設定し、gold クラスには完全プライオリティを割り当てて、残りのクラス間で所定の比率で残りの帯域幅を分配する例を示します。

```
Switch(config)# policy-map output1-8
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
```

次に、ギガビット イーサネット ポートに入力および出力サービス ポリシーを付加して、アクティブ化する例を示します。

```
Switch(config)# interface range gigabitethernet0/1-2
Switch(config-if-range)# service-policy input input-all
Switch(config-if-range)# service-policy output output-g1-2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

次に、ファスト イーサネット ポート 1 ～ 8 に入力および出力サービス ポリシーを付加して、アクティブ化する例を示します。

```
Switch(config)# interface range fastethernet0/1 - 8
Switch(config-if-range)# service-policy input input-all
Switch(config-if-range)# service-policy output output1-8
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

カスタマー B の QoS 設定

このセクションでは、現在のカスタマーに影響を与えずに一連の新しいカスタマーにスイッチ上で QoS ポリシーを設定してアクティブ化する例を示します。入力および出力 QoS サービス ポリシーは、要件に基づいて設定され、関連ポートに付加されます。この例では、既存の入力ポリシー マップを使用し、新しいカスタマーには新しい出力ポリシー マップを設定します。

カスタマー B に対する初期設定では、ファスト イーサネット ポート 1 ～ 8 が UNI で、アクティブです。ファスト イーサネット ポート 9 ～ 24 は、UNI で、シャットダウンしています。ギガビット イーサネット ポート 1 および 2 は、NNI で、デフォルトでイネーブルに設定されています。

次に、初期設定の全体的な流れを示します。

- 新しく必要になったすべての出力ポリシーを定義します。
- アクティブ化されたポートに入力および出力ポリシーを付加する。
- ポートのシャットダウン ステートを終了する。

出力ポリシーを設定する際の制限事項は、次のとおりです。

- 出力ポリシー マップでは、最大 3 つのクラスを定義できます。
- 定義されたクラスは、他の出力ポリシー マップと同一でなければなりません。
- 各出力ポリシーマップで定義されるクラス数は、同じである必要があります。
- クラスごとに動作を割り当てる必要があります。つまり、空のクラスはありません。
- 各クラス設定は、入力ポリシー マップで実行された分類/マーキングに基づいている必要があります。

次に、ファスト イーサネット UNI 9 ～ 12 に付加される 3 番めの出力サービス ポリシーを設定して、最小保証帯域幅を、gold クラスには 50 Mb/s、silver クラスには 20 Mb/s、bronze クラスには 10 Mb/s を割り当てる例を示します。

```
Switch(config)# policy-map output9-12
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# bandwidth 50000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
```

次に、ファスト イーサネット ポート 9 ～ 12 に出力ポリシーを付加して、ポートをアクティブ化する例を示します。

```
Switch# config terminal
Switch(config)# interface range fastethernet0/9-12
Switch(config-if-range)# service-policy input input-all
Switch(config-if-range)# service-policy output output9-12
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

出力ポリシーの変更および分類基準の追加と削除

ここでは、既存の一連の出力ポリシー マップを更新して、分類基準を追加または削除する例を示します。サービス プロビジョニング要件または入力サービス ポリシー マップでの変更により、修正が必要となる場合があります。いずれのポートもシャットダウンすることなく、変更できます。

初期設定では、ファスト イーサネット ポート 1 ～ 12 が UNI で、アクティブです。ファスト イーサネット ポート 13 ～ 24 は、UNI で、シャットダウンしています。ギガビット イーサネット ポート 1 および 2 は、NNI で、デフォルトでイネーブルに設定されています。

次に、初期設定の全体的な流れを示します。

- 入力サービス ポリシーの設定済みクラス マップを変更します。
- 出力サービス ポリシーの設定済みクラス マップを変更します。

次に、silver-in クラスに分類基準を追加して、入力サービス ポリシーのクラスを変更し、dscp cs5 も照合する例を示します。これは、dscp cs5 を照合する出力ポリシー マップで必要となります。

```
Switch(config)# class-map match-any silver-in
Switch(config-cmap)# match ip dscp af21
Switch(config-cmap)# match ip dscp cs5
Switch(config-cmap)# exit
```

次に、silver-out クラスに分類基準を追加して、出力サービス ポリシーのクラスを変更し、dscp cs5 も照合する例を示します。これにより、すべての設定済みおよび付加済み出力サービス ポリシーで dscp cs5 が silver-out クラスに追加されます。これで dscp cs5 フローが、silver-out クラスと同じキューイングおよびスケジューリング処理を受信します。

```
Switch# config terminal
Switch(config)# class-map match-any silver-out
Switch(config-cmap)# match ip dscp af21
Switch(config-cmap)# match ip dscp cs5
Switch(config-cmap)# exit
```

設定されたクラスに関連付けられた match 文を削除する場合は、同じ手順を使用する必要があります。

出力ポリシーの変更およびキューイングまたはスケジューリング パラメータの変更

ここでは、既存の一連の出力ポリシー マップを更新して、設定済みのキューイングおよびスケジューリング アクションのパラメータを変更する例を示します。サービス プロビジョニング要件での変更により、出力ポリシー マップでの修正が必要となる場合があります。いずれのポートもシャットダウンすることなく、変更できます。

初期設定では、ファスト イーサネット ポート 1 ～ 12 が UNI で、アクティブです。ファスト イーサネット ポート 13 ～ 24 は、UNI で、シャットダウンしています。ギガビット イーサネット ポート 1 および 2 は、NNI で、デフォルトでイネーブルに設定されています。

要件は、アクション パラメータを変更することです。

出力ポリシーを設定する際の制限事項は、次のとおりです。

- 出力ポリシー マップでは、最大 3 つのクラスを定義できます。
- 定義されたクラスは、他の出力ポリシー マップと同一でなければなりません。
- 各出力ポリシーマップで定義されるクラス数は、同じである必要があります。
- クラスごとに動作を割り当てる必要があります。つまり、空のクラスはありません。
- 各クラス設定は、入力ポリシー マップで実行された分類またはマーキングに基づいている必要があります。

次に、最小保証帯域幅を gold クラスには 40 Mb/s（50 Mb/s から変更）、silver クラスには 30 Mb/s（20 Mb/s から変更）、および bronze クラスには 20 Mb/s（10 Mb/s から変更）を割り当て、ファスト イーサネット UNI 8 ～ 12 を処理する 3 番目の出力サービス ポリシーを変更する例を示します。

```
Switch(config)# policy-map output9-12
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# bandwidth 40000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth 30000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
```

出力ポリシーの変更および設定済み動作の追加または削除

ここでは、既存の一連の出力ポリシー マップを更新して、キューイングおよびスケジューリング動作を追加または削除する例を示します。サービス プロビジョニング要件での変更により、出力ポリシー マップでの修正が必要となる場合があります。変更される出力ポリシー マップが設定されていないポートをシャットダウンしないで、変更できます。ただし、出力ポリシー マップが設定されているポートは、シャットダウンする必要があります。この出力ポリシー マップを使用しないカスタマーは、影響を受けません。

初期設定では、ファスト イーサネット ポート 1 ～ 12 が UNI で、アクティブです。ファスト イーサネット ポート 13 ～ 24 は、UNI で、シャットダウンしています。ギガビット イーサネット ポート 1 および 2 は、NNI で、デフォルトでイネーブルに設定されています。

次に、設定の全体的な流れを示します。

- 変更されるポリシーを伝搬するすべてのアクティブ ポートをシャットダウンします。
- 出力ポリシーが付加されているすべてのポートから、ポリシーを消去します。
- 出力ポリシーを変更します。
- 該当するポートに、出力ポリシーを再度付加します。
- ポートのシャットダウン ステートを終了します。

出力ポリシーを設定する際の制限事項は、次のとおりです。

- 出力ポリシー マップでは、最大 3 つのクラスを定義できます。
- 定義されたクラスは、他の出力ポリシー マップと同一でなければなりません。
- 各出力ポリシーマップで定義されるクラス数は、同じである必要があります。
- クラスごとに動作を割り当てる必要があります。つまり、空のクラスはありません。
- 各クラス設定は、入力ポリシー マップで実行された分類/マーキングに基づいている必要があります。

次の手順では、出力ポリシーを伝搬するポートすべて（この場合は、ギガビット イーサネット ポートだけ）がシャットダウンされます。

```
Switch(config)# interface range gigabitEthernet0/1-2
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
```

次の手順では、変更される出力ポリシー（この場合は、ギガビット イーサネット ポートに設定されたポリシー）が削除されます。

```
Switch(config)# interface range gigabitEthernet0/1-2
Switch(config-if-range)# no service-policy output output-g1-2
Switch(config-if-range)# exit
```

次の手順では、ギガビット イーサネット NNI を処理する出力サービス ポリシーが変更されます。ポリシーは、bronze クラスに最小帯域幅保証の 10% を割り当てる代わりに、クラスベース シェーピングに 100000 bps を割り当てるように変更されます。

```
Switch(config)# policy-map output-g1-2
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# no bandwidth percent 10
Switch(config-pmap-c)# shape average 100000
Switch(config-pmap-c)# exit
```

次の手順では、出力ポリシーがギガビット イーサネットポートに再度付加されます。

```
Switch(config)# interface range gigabitethernet0/1-2
Switch(config-if-range)# service-policy output output9-12
Switch(config-if-range)# exit
```

次の手順では、すべてのギガビット イーサネット ポートがアクティブ化されます。

```
Switch(config)# interface range gigabitethernet0/1-2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

出力ポリシーの変更およびクラスの追加または削除

ここでは、既存の一連の出力ポリシー マップを更新して、すべてのクラスを追加または削除する例を示します。サービス プロビジョニング要件または入力サービス ポリシーでの変更により、出力ポリシー マップでの修正が必要となる場合があります。この変更を行うには、スイッチ上のすべてのアクティブ ポートをシャットダウンする必要があります。任意の出力ポリシー マップに対するこの種の更新は、すべてのカスタマーに影響を及ぼす場合があります。これを回避するため、出力サービス ポリシーでクラスを設定する場合は将来的に可能性のある更新について考慮することを推奨します。

初期設定では、ファスト イーサネット ポート 1 ～ 12 が UNI で、アクティブです。ファスト イーサネット ポート 13 ～ 24 は、UNI で、シャットダウンしています。ギガビット イーサネット ポート 1 および 2 は、NNI で、デフォルトでイネーブルに設定されています。

次に、設定の全体的な流れを示します。

- すべてのアクティブ ポートをシャットダウンします。
- すべてのファスト イーサネットおよびギガビット イーサネット ポートから出力ポリシーを消去します。
- クラスを削除します。
- ファスト イーサネットおよびギガビット イーサネット ポートに出力ポリシーを再度付加します。
- ファスト イーサネットおよびギガビット イーサネット ポートのシャットダウン ステートを終了します。

次の手順では、すべてのアクティブで適用可能なファスト イーサネットおよびギガビット イーサネット ポートをシャットダウンします。

```
Switch(config)# interface range gigabitethernet0/1-2, fastethernet0/1-12
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
```

次の手順では、影響を受けるファスト イーサネットおよびギガビット イーサネット ポートからすべての出力ポリシーを消去します。

```
Switch(config)# interface range fastethernet0/1-8
Switch(config-if-range)# no service-policy output output1-8
Switch(config-if-range)# exit
```

```
Switch(config)# interface range fastethernet0/9-12
Switch(config-if-range)# no service-policy output output9-12
Switch(config-if-range)# exit


Switch(config)# interface range gigabitethernet0/1-2
Switch(config-if-range)# no service-policy output output-g1-2
Switch(config-if-range)# exit
```

次の手順では、すべての出力ポリシー マップおよび入力ポリシー マップからクラスを削除します。入力ポリシーは付加したままでも、消去してもかまいません。

```
Switch(config)# policy-map output1-8
Switch(config-pmap)# no class bronze-out
Switch(config-pmap-c)# exit
Switch(config)# policy-map output9-12
Switch(config-pmap)# no class bronze-out
Switch(config-pmap-c)# exit
Switch(config)# policy-map output-g1-2
Switch(config-pmap)# no class bronze-out
Switch(config-pmap-c)# exit
Switch(config)# policy-map input-all
Switch(config-pmap)# no class bronze-in
Switch(config-pmap-c)# exit
```

ファスト イーサネットおよびギガビット イーサネット ポートにすべてのポリシーを再度付加します。

```
Switch(config)# interface range fastethernet0/1-8
Switch(config-if-range)# service-policy output output1-8
Switch(config-if-range)# exit

Switch(config)# interface range fastethernet0/9-12
Switch(config-if-range)# service-policy output output9-12
Switch(config-if-range)# exit

Switch(config)# interface range gigabitethernet0/1-2
Switch(config-if-range)# service-policy output output9-12
Switch(config-if-range)# exit
```

次の手順では、すべての適用可能なファスト イーサネットおよびギガビット イーサネット ポートをアクティブ化します。

```
Switch(config)# interface range gigabitethernet0/1-2, fastethernet0/1-12
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

付加された出力サービス ポリシーにクラスを追加する場合は、同じ手順を使用する必要があります。

（注）　前述の順序に従わない場合は、問題が発生する可能性があります。

インターフェイスにポリシー マップを付加する場合、ポリシー マップ内の設定済みのクラス マップに明示的に一致しないすべてのトラフィックは、デフォルト キュー（クラス **class-default**）を通過します。ただし、場合によっては、出力ポリシー マップに明示的に一致しないトラフィックが複数のキューを通過する場合があります。このようなキューイング問題は、前述の手順に従わない場合、およびすべてのアクティブ ポートに出力ポリシーが付加されていない場合に発生する可能性があります。

たとえば、2 つのポートにだけ出力ポリシーが設定されていて、出力ポリシー内のクラスを削除する場合を検討します。

2 つのポートをシャットダウンします。

```
Switch(config)# interface range fastethernet0/1-2
```

```
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
```

両方のポートから出力ポリシーを消去します。

```
Switch(config)# interface range fastEthernet0/1-2
Switch(config-if)# no service-policy output output1-2
Switch(config-if)# exit
```

出力ポリシー内のクラスを削除します。

```
Switch(config)# policy-map output1-2
Switch(config-pmap)# no class bronze-out
Switch(config-pmap-c)# exit
```

1 つのポートにだけ出力ポリシーを付加して、もう 1 つには付加しません。

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# service-policy output output1-2
Switch(config-if)# exit
```

両方のポートをイネーブルにします。

```
Switch(config)# interface range fastethernet0/1-2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

この時点では、トラフィックが単一のデフォルトキューを通過せずに、ファスト イーサネット ポート 2 から発信される場合、ファスト イーサネット ポート 1 に付加された出力ポリシーマップに定義されたクラスがある場合と同じ数のキューを通過します。この場合は 3 つです。フローが複数のキューに分割された場合は、場合によっては、ファスト イーサネット ポート 2 から発信されるフローのパケットが再度順番付けされる可能性があります。出力ポリシーを付加するまでポートをシャットダウン ステートのままにすることにより、この問題を回避できます。

CHAPTER 35

EtherChannel およびリンクステート トラッキングの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチのレイヤ 2 およびレイヤ 3 ポートに EtherChannel を設定する方法について説明します。EtherChannel は、スイッチ、ルータ、サーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用して配線クローゼットとデータ センタ間の帯域幅を拡張したり、ボトルネックが発生しやすいネットワーク内の任意の場所に EtherChannel を配備したりできます。EtherChannel には、残りのリンク間で負荷を再分配し、リンク切断から自動的に回復する機能があります。リンクに障害が発生した場合、EtherChannel は仲介なしに、障害のあるリンクからチャネル内の残りのリンクにトラフィックをリダイレクトします。またこの章では、リンクステート トラッキングの設定方法についても説明します。

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

- 「EtherChannel の概要」（P.35-1）
- 「EtherChannel の設定」（P.35-9）
- 「EtherChannel、PAgP、および LACP ステータスの表示」（P.35-22）
- 「リンクステート追跡の概要」（P.35-22）
- 「リンクステート追跡の設定」（P.35-24）
- 「リンクステート追跡ステータスの表示」（P.35-25）

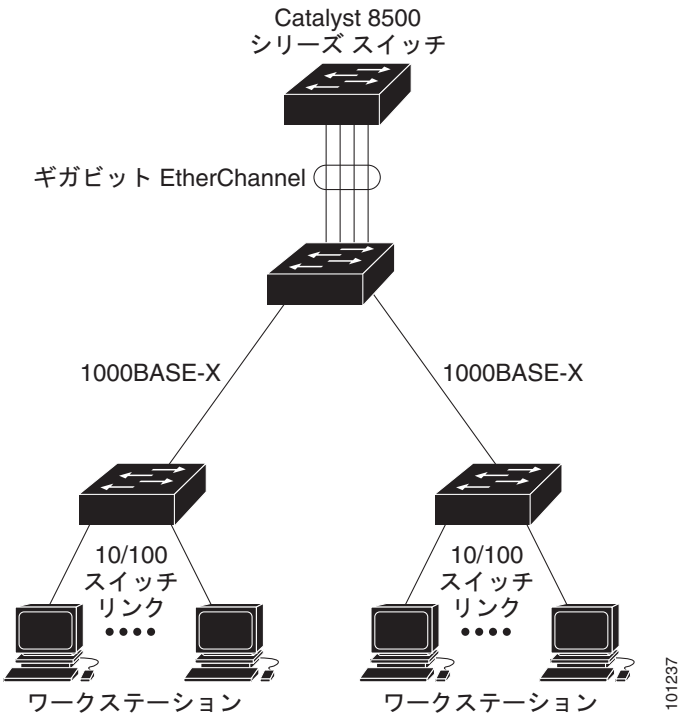
EtherChannel の概要

- 「EtherChannel の概要」（P.35-2）
- 「ポート チャネル インターフェイス」（P.35-3）
- 「ポート集約プロトコル」（P.35-4）
- 「Link Aggregation Control Protocol」（P.35-6）
- 「EherChannel の on モード」（P.35-7）
- 「ロード バランシングおよび転送方式」（P.35-7）

EtherChannel の概要

EtherChannel は、単一の論理リンクにバンドルされた個々のファスト イーサネットまたはギガビット イーサネット リンクで構成されます（図 35-1 を参照）。

図 35-1　　EtherChannel の一般的な構成



EtherChannel は、24 のファスト イーサネット ポートを持つスイッチ上の Fast EtherChannel の場合、スイッチ間、またはスイッチとホスト間に最大 800 Mbps の全二重帯域幅を提供します。Gigabit EtherChannel の場合は、サポートされるギガビット イーサネット インターフェイス数に応じて、最大 8 Gbps（1 Gbps が 8 ポート）まで設定できます。

（注）　Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）や Port Aggregation Protocol（PAgP; ポート集約プロトコル）をサポートしているのは、Network Node Interfaces（NNI; ネットワーク ノード インターフェイス）および Enhanced Network Interfaces（ENI; 拡張ネットワーク インターフェイス）だけです。**port-type** {**eni** | **nni**} インターフェイス コンフィギュレーション コマンドを使用して、ENI または NNI としてポートを設定します。スイッチで 5 つ以上のポートを NNI として設定する場合は、メトロ IP アクセス イメージが稼動している必要があります。

各 EtherChannel には、最大 8 つの（設定に互換性のある）イーサネット ポートを含めることができます。各 EtherChannel 内のすべてのポートは、レイヤ 2 またはレイヤ 3 ポートのいずれかとして設定する必要があります。EtherChannel の数は 48 に制限されています。詳細については、「EtherChannel 設定時の注意事項」（P.35-10）を参照してください。EtherChannel レイヤ 3 ポートは、ルーテッド ポートで構成されます。ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。詳細については、第 10 章「インターフェイスの設定」を参照してください。

EtherChannel には、Port Aggregation Protocol（PAgP; ポート集約プロトコル）、Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）、または on のいずれかのモードを設定できます。PAgP および LACP は、NNI および ENI 上でだけ使用できます。EtherChannel の両端は同じモードで設定します。

- EtherChannel の一端を PAgP または LACP モードのいずれかで設定すると、システムはチャネルのもう一端とネゴシエートして、アクティブになるポートを決定します。互換性のないポートは停止します。
- **on** モードで EtherChannel を設定した場合、ネゴシエーションは実行されません。スイッチは EtherChannel の互換性のあるポートすべてを強制的にアクティブにします。チャネルのもう一端（他のスイッチ上の）も **on** モードで設定する必要があります。そうしないと、パケット損失が発生します。

  ローカル ポートは独立ステートとなり、他の単一リンクと同様にデータ トラフィックを継続して伝送します。ポート設定は変更されませんが、EtherChannel には参加しません。

EtherChannel 内のリンクで障害が発生すると、障害リンク上でそれまで伝送されていたトラフィックがその EtherChannel 内の残りのリンクに切り替えられます。障害の場合はトラップが送信され、スイッチ、EtherChannel、および障害リンクを識別します。EtherChannel の 1 つのリンクに着信したブロードキャストおよびマルチキャスト パケットが、EtherChannel の別のリンクに戻されることはありません。

ポート チャネル インターフェイス

EtherChannel を作成すると、ポート チャネル論理インターフェイスも作成されます。

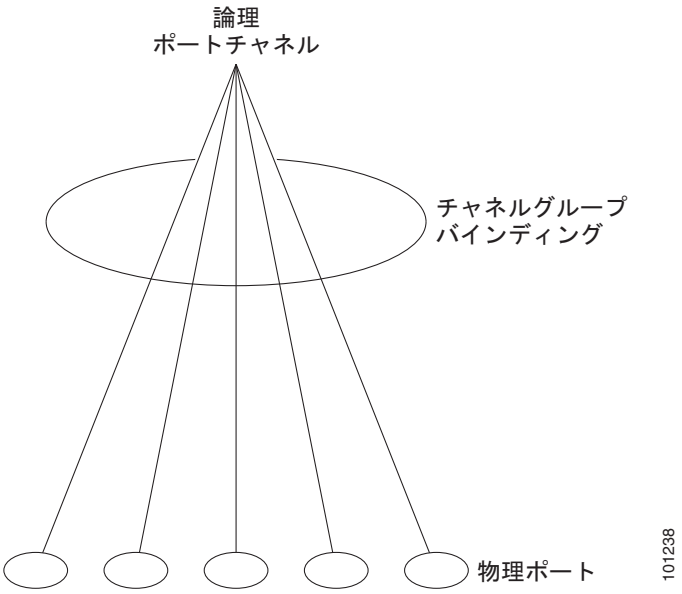
- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポート チャネル論理インターフェイスを動的に作成します。

  また、**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用して、ポート チャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。*channel-group-number* は *port-channel-number* と同じ値に設定したり、新しい番号を使用したりできます。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。
- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。そのあと、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

レイヤ 2 およびレイヤ 3 ポートのいずれの場合も、**channel-group** コマンドを実行すると、物理ポートと論理インターフェイスがバインドされます（図 35-2 を参照）。

各 EtherChannel には、1 ～ 48 まで番号付けされたポート チャネルの論理インターフェイスがあります。このポート チャネル インターフェイスの番号は、**channel-group** インターフェイス コンフィギュレーション コマンドにより指定された番号に対応します。

図 35-2　物理ポート、論理ポート チャネル、およびチャネル グループの関係



EtherChannel を設定したあとに、ポート チャネル インターフェイスの設定を変更すると、そのポート チャネル インターフェイスに割り当てられたすべての物理ポートの設定も変更されます。物理ポートの設定を変更した場合は、設定を適用したポートだけが影響を受けます。EtherChannel のすべてのポートのパラメータを変更するには、ポート チャネル インターフェイスにコンフィギュレーション コマンドを適用します。

ポート集約プロトコル

PAgP はシスコ独自のプロトコルで、シスコ製スイッチと、PAgP に対応するためにライセンスを得たベンダーのスイッチだけで動作します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。

（注）　PAgP を使用できるのは、NNI および ENI 上だけです。

スイッチは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化するときの基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、速度、デュプレックス モード、ネイティブ VLAN（仮想 LAN）、VLAN 範囲、トランキング ステータスおよびタイプが同じであるポートが PAgP によってグループ化されます。リンクが EtherChannel にグループ化されたあと、グループは PAgP によって単一のスイッチ ポートとしてスパニング ツリーに追加されます。

PAgP モード

表 35-1 に、**channel-group** インターフェイス コンフィギュレーション コマンドで NNI または ENI 上にユーザが設定できる EtherChannel PAgP モードを示します。

表 35-1　EtherChannel PAgP モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。このステートの場合、ポートは受信した PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始しません。この設定では、PAgP パケットの伝送が最小化されます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。このステートの場合、ポートは PAgP パケットを送信し、他のポートとのネゴシエーションを開始します。

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定されたパートナー ポートだけと PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードの場合、ポートはパートナー ポートとネゴシエーションを行い、一定の基準に従って EtherChannel を形成します。その基準とは、ポート速度、およびレイヤ 2 EtherChannel の場合、トランキング ステートと VLAN 番号などです。

ポート間で PAgP モードが異なっていても、モードに互換性があれば EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** または **auto** モードの別のポートと EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートと EtherChannel を形成できます。

auto モードのポートは、**auto** モードの別のポートとは EtherChannel を形成することができません。どちらのポートも、PAgP ネゴシエーションを開始しないためです。

PAgP 機能を持つパートナーにスイッチが接続されている場合は、キーワード **non-silent** を使用して、非サイレント動作を行うようにスイッチ ポートを設定できます。**auto** モードまたは **desirable** モードの場合は、**non-silent** を指定しないとサイレント モードになります。

PAgP 機能を備えていない、または備えていてもパケット送信量がわずかしかないデバイスにスイッチが接続されている場合は、サイレント モードを使用します。サイレント パートナーの例としては、トラフィックを生成しないファイル サーバやパケット アナライザがあります。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼動させると、このスイッチ ポートが動作しなくなります。ただし、サイレント設定を使用すると、PAgP が動作したり、チャネル グループにポートを接続したり、ポートを伝送に使用したりできます。

PAgP と他の機能との相互作用

Cisco Discovery Protocol（CDP; シスコ検出プロトコル）は、EtherChannel の物理ポートを経由してパケットを送受信します。

（注） PAgP および CDP を使用できるのは、NNI および ENI 上だけです。User Network Interface（UNI; ユーザ ネットワーク インターフェイス）では、PAgP または CDP をサポートしていません。

トランク ポートは、番号が最小の VLAN 上で PAgP Protocol Data Unit（PDU; プロトコル データ ユニット）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを渡します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを渡します。

PAgP は、auto または desirable モードに設定され、PAgP がイネーブルである稼動状態のポートからだけ PAgP PDU を送受信します。

Link Aggregation Control Protocol

LACP は IEEE 802.3ad 標準で定義されていて、シスコ製スイッチは、この標準に準拠するスイッチ間のイーサネット チャネルを管理できます。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

（注）　LACP を使用できるのは、NNI および ENI 上だけです。

スイッチは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化するときの基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータスおよびタイプが同じであるポートが LACP によってグループ化されます。リンクが EtherChannel にグループ化されたあと、グループは LACP によって単一のスイッチ ポートとしてスパニング ツリーに追加されます。

LACP モード

表 35-2 に、**channel-group** インターフェイス コンフィギュレーション コマンドで NNI または ENI 上にユーザが設定できる EtherChannel LACP モードを示します。

表 35-2　EtherChannel LACP モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。このステートの場合、ポートは LACP パケットを送信し、他のポートとのネゴシエーションを開始します。
passive	ポートをパッシブ ネゴシエーション ステートにします。このステートの場合、ポートは受信した LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始しません。この設定では、LACP パケットの伝送が最小化されます。

active モードおよび **passive LACP** モードの場合、ポートはパートナー ポートとネゴシエーションを行い、一定の基準に従って EtherChannel を形成します。その基準とは、ポート速度、レイヤ 2 EtherChannel の場合、トランキング ステートと VLAN 番号などです。

ポート間で LACP モードが異なっていても、モードに互換性があれば EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートと EtherChannel を形成できます。
- **passive** モードのポートは、**passive** モードの別のポートとは EtherChannel を形成することができません。どちらのポートも、LACP ネゴシエーションを開始しないためです。

LACP と他の機能との相互作用

CDP は、EtherChannel の物理ポートを経由してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを渡します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを渡します。

LACP は、active または passive モードに設定され、LACP がイネーブルである稼動状態のポートだけから LACP PDU を送受信します。

EherChannel の on モード

EherChannel の **on** モードを使用すると、手動で EherChannel を設定できます。**on** モードにすると、ポートはネゴシエーションせずに強制的に EtherChannel に加入されます。リモート デバイスで PAgP または LACP がサポートされていない場合に、on モードは便利な機能です。**on** モードでは、リンクの両端のスイッチが **on** モードで設定されている場合にだけ、EtherChannel を使用できます。

（注） UNI の場合、使用可能なモードは **on** だけです。

on モードで設定された同一チャンネル グループ内のポートは、速度およびデュプレックスなどのポート特性に互換性がある必要があります。**on** モードで設定されていても、互換性のないポートは停止します。

注意 **on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端にあるポートで同じ設定になっている必要があります。グループの設定を誤ると、パケット損失またはスパニングツリーのループが発生することがあります。

ロード バランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンを部分的に縮小し、チャネル内の 1 つのリンクを選択する数値にすることによって、チャネル内のリンク間でトラフィックの負荷を分散させます。EtherChannel のロード バランシングには、MAC アドレスや IP アドレス、送信元アドレスや宛先アドレス、または送信元と宛先の両方のアドレスを使用できます。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。ロード バランシングおよび転送方法を設定するには、**port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、ロード バランシングを行うために、異なるホストからのパケットにはチャネル内の別のポート、同じホストからのパケットにはチャネル内の同じポートが使用されます。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットに指定されている宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、同じ宛先へのパケットは同じポートを経由して転送され、異なる宛先へのパケットはチャネル内の別のポートを経由して送信されます。

ME-3400E スイッチ上では、宛先ホスト MAC アドレスに基づいた負荷分散がサポートしているポートは、EtherChannel ごとに 4 つだけです。EtherChannel 宛先 MAC アドレス ロード バランシングを設定する場合、チャンネル グループ内の 4 つのポート間だけでトラフィックが均等化されます。宛先 MAC アドレス負荷分散を使用して EtherChannel 内で 4 つを超えるポートを設定すると、4 つのポートだけによって、分散されたトラフィックが受信されます。この制限は、他の負荷分散方式には適用されません。

送信元/宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。この転送方式は、送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式の負荷分散を組み合せたものです。特定のスイッチに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のいずれが適切であるかが不明な場合に使用できます。送信元/宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

送信元 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、異なる IP アドレスからのパケットにはチャネル内の別のポート、同じ IP アドレスからのパケットにはチャネル内の同じポートが使用されます。

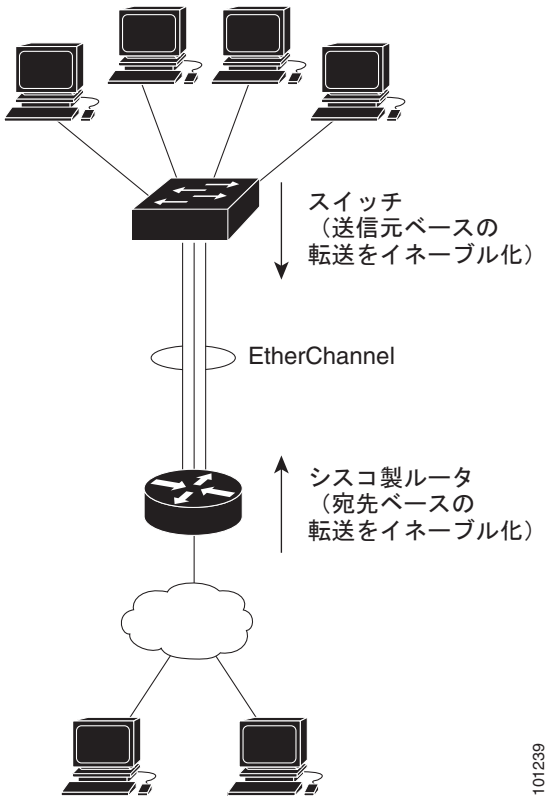
宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは異なるチャネル ポートに送信される場合があります。ただし、異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常に同じチャネル ポートに送信されます。

送信元/宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合せたものです。特定のスイッチに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のいずれが適切であるかが不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

ロード バランシング方式ごとに利点が異なります。ロード バランシング方式は、ネットワーク内のスイッチの位置、および負荷分散が必要なトラフィックの種類に基づいて選択する必要があります。図 35-3 では、4 台のワークステーションで構成された EtherChannel がルータと通信しています。ルータは単一の MAC アドレスを持つデバイスであるため、スイッチ EtherChannel で送信元ベース転送を行うことにより、ルータが使用できる全帯域をスイッチが使用するようになります。ルータは、宛先ベース転送を行うように設定されます。このように設定すると、多数のワークステーションで、ルータ EtherChannel からのトラフィックが均等に分散されることが保証されるためです。

設定には最も柔軟なオプションを使用してください。たとえば、チャネル上のトラフィックが単一 MAC アドレスを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンクが常に選択されます。送信元アドレスまたは IP アドレスを使用した方が、ロード バランシングの効率がよくなることがあります。

図 35-3　負荷分散および転送方法



EtherChannel の設定

- 「EtherChannel のデフォルト設定」（P.35-10）
- 「EtherChannel 設定時の注意事項」（P.35-10）
- 「レイヤ 2 EtherChannel の設定」（P.35-12）（必須）
- 「レイヤ 3 EtherChannel の設定」（P.35-14）（必須）
- 「EtherChannel ロード バランシングの設定」（P.35-17）（任意）
- 「PAgP 学習方式およびプライオリティの設定」（P.35-18）（任意）
- 「LACP ホットスタンバイ ポートの設定」（P.35-19）（任意）

（注）　ポートが正しく設定されていることを確認してください。詳細については、「EtherChannel 設定時の注意事項」（P.35-10）を参照してください。

（注）　EtherChannel を設定したあとに、ポート チャネル インターフェイスの設定を変更すると、そのポート チャネル インターフェイスに割り当てられたすべての物理ポートの設定も変更されます。物理ポートの設定変更では、そのポートだけが変更されます。

EtherChannel のデフォルト設定

表 35-3 に、EtherChannel のデフォルト設定を示します。

表 35-3　EtherChannel のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポート チャネル論理インターフェイス	定義なし。
PAgP モード	デフォルトなし。
PAgP の学習方式	すべての NNI および ENI で集約ポート学習
PAgP プライオリティ	すべての NNI および ENI で 128
LACP モード	デフォルトなし。
LACP の学習方式	すべての NNI および ENI で集約ポート学習
LACP ポート プライオリティ	すべての NNI および ENI で 32768
LACP システム プライオリティ	32768.
LACP システム ID	LACP システム プライオリティおよびスイッチの MAC アドレス
ロード バランシング	スイッチの負荷分散は、着信パケットの送信元 MAC アドレスに基づいて行われます。

EtherChannel 設定時の注意事項

EtherChannel が正しく設定されていない場合、ネットワーク ループなどの問題を回避するために、一部の EtherChannel ポートが自動的にディセーブルになることがあります。設定上の問題を回避するために、次の注意事項に従ってください。

- 48 より多くの EtherChannel をスイッチで設定しようとしないでください。
- NNI だけ、または ENI だけを含む PAgP EtherChannel を設定してください。
- NNI だけ、または ENI だけを含む LACP EtherChannel を設定してください。
- EtherChannel 内のすべてのポートが、同じ速度および同じデュプレックス モードで動作するように設定してください。
- EtherChannel のすべてのポートは、同じタイプ（UNI、NNI、ENI のいずれか）になるようにする必要があります。1 つの EtherChannel 内で各種ポート タイプを混在できません。
- UNI では、EtherChannel モードが常に **on** に設定されている必要があります。
- EtherChannel のすべてのポートをイネーブルにしてください。**shutdown** インターフェイス コンフィギュレーション コマンドを使用してディセーブル化された EtherChannel のポートは、リンク障害として処理され、トラフィックは EtherChannel の残りのポートのいずれかに転送されます。UNI と ENI は、デフォルトでディセーブルに設定されています。NNI はデフォルトでイネーブルです。
- グループを初めて作成したときは、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次に示すパラメータのいずれかの設定を変更する場合は、グループ内のすべてのポートに関する設定も変更してください。
  - 許可 VLAN リスト
  - 各 VLAN のスパニング ツリー パス コスト

  - 各 VLAN のスパニング ツリー ポート プライオリティ
  - スパニング ツリーの PortFast 設定

（注）　スパニング ツリー プロトコルがサポートされているのは、そのプロトコルが特にイネーブルにされている NNI または ENI 上だけです。

- ポートが複数の EtherChannel グループのメンバーにならないように設定してください。
- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP と LACP が稼動している EtherChannel グループは同じスイッチ上に共存できます。個々の EtherChannel グループは PAgP または LACP のどちらかを実行できますが、相互運用することはできません。

（注）　PAgP および LACP を使用できるのは、NNI および ENI 上だけです。

- スイッチでメトロ アクセス イメージが稼動している場合、スイッチで同時に設定できる NNI は 4 つだけです。つまり、LACP および PAgP を同時にサポートできる EtherChannel 内のポートは 4 つだけになります。スイッチでメトロ IP アクセス イメージが稼動している場合、スイッチに設定できる NNI 数に制限はありません。
- EtherChannel の一部として Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポートを設定しないでください。
- EtherChannel の一部としてセキュア ポートを設定したり、その逆の設定を行ったりしないでください。
- プライベート VLAN ポートを EtherChannel の一部として設定しないでください。
- EtherChannel のアクティブ メンバーであるポートまたはまだアクティブ メンバーでないポートを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。
- EtherChannel がスイッチ インターフェイスに設定されている場合、スイッチで 802.1x をグローバルにイネーブルにする前に、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して EtherChannel 設定を削除します。
- レイヤ 2 EtherChannel の場合
  - EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されているポートは、EtherChannel を形成することができません。
  - トランク ポートから EtherChannel を設定する場合は、すべてのトランクでトランキング モードが同じであることを確認してください。EtherChannel ポートでトランク モードが統一されていない場合は、予想外の結果を招くことがあります。
  - EtherChannel がサポートする VLAN の許容範囲は、トランキング レイヤ 2 EtherChannel 内のポートすべてで同じです。VLAN の許容範囲が同じでない場合は、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
  - NNI または ENI のスパニング ツリー パス コストが異なっていても、他の設定条件に矛盾がなければ、EtherChannel を形成できます。異なるスパニング ツリー パス コストを設定しても、それ自体は、EtherChannel の形成でポートに矛盾をもたらしません。
- レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャネル内の物理ポートでなく、ポート チャネル論理インターフェイスに割り当ててください。

レイヤ 2 EtherChannel の設定

レイヤ 2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネル グループにポートを割り当てます。このコマンドにより、ポート チャネル論理インターフェイスが自動的に作成されます。

レイヤ 2 EtherChannel にレイヤ 2 イーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。 PAgP EtherChannel の場合、同一タイプ、同一速度のポートを 8 つまで同一グループに設定できます。 LACP EtherChannel の場合は、同一タイプのイーサネット ポートを 16 まで設定できます。最大 8 個のポートをアクティブにして、最大 8 個のポートをスタンバイ モードにすることができます。 **（注）** インターフェイスが UNI の場合は、PAgP または LACP を設定する前に、**port-type** {**eni** | **nni**} インターフェイス コンフィギュレーション コマンドを入力する必要があります。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport mode** {**access** | **trunk**} **switchport access vlan** *vlan-id*	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN にだけ割り当ててください。指定できる範囲は 1 ～ 4094 です。

	コマンド	目的
ステップ 5	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}	ポートをチャネル グループに割り当て、PAgP または LACP モードを指定します。 *channel-group-number* の範囲は 1 ～ 48 です。 **（注）**　UNI の場合、使用可能なモードは **on** だけです。 **mode** には、次のキーワードのいずれかを選択します。 • **auto**：PAgP デバイスが検出された場合にだけ、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。このステートの場合、ポートは受信した PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始しません。 • **desirable**：PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。このステートの場合、ポートは PAgP パケットを送信し、他のポートとのネゴシエーションを開始します。 • **on**：PAgP や LACP を使用せずに、ポートを強制的にチャネル化します。**on** モードでは、**on** モードのポート グループが **on** モードの別のポート グループに接続されている場合にだけ、EtherChannel を使用することが可能となります。 • **non-silent**：（任意）PAgP 対応のパートナーに接続されたスイッチのポートが **auto** モードまたは **desirable** モードの場合に、非サイレント動作を行うようにこのポートを設定します。**non-silent** を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザに接続する場合に使用します。この設定を使用すると、PAgP が動作したり、チャネル グループにポートを接続したり、ポートを伝送に使用したりできます。 • **active**：LACP デバイスが検出された場合にだけ、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。このステートの場合、ポートは LACP パケットを送信し、他のポートとのネゴシエーションを開始します。 • **passive**：ポートで LACP をイネーブルにしてパッシブ ネゴシエーション ステートにします。このステートの場合、ポートは受信した LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始しません。 スイッチとパートナー間で互換性のあるモードの詳細については、「PAgP モード」（P.35-5）および「LACP モード」（P.35-6）を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EtherChannel グループからポートを削除するには、**no channel-group** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、EtherChannel を設定する方法を示します。2 つのポートは VLAN 10 のスタティックアクセス ポートとして、PAgP モードが **desirable** であるチャネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 -2
Switch(config-if-range)# port-type nni
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

次の例では、EtherChannel を設定する方法を示します。2 つのポートは VLAN 10 のスタティックアクセス ポートとして、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

レイヤ 3 EtherChannel の設定

レイヤ 3 EtherChannel を設定するには、ポート チャネル論理インターフェイスを作成し、そのポート チャネルにイーサネット ポートを組み込みます。次に設定方法を説明します。

ポート チャネル論理インターフェイスの作成

レイヤ 3 EtherChannel を設定する場合、まず **interface port-channel** グローバル コンフィギュレーション コマンドを使用し、ポート チャネル論理インターフェイスを手動で作成しなければなりません。次に、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して論理インターフェイスをチャネル グループに配置します。

（注） 物理ポートから EtherChannel に IP アドレスを移動するには、物理ポートから IP アドレスを削除してから、その IP アドレスをポート チャネル インターフェイス上で設定する必要があります。

レイヤ 3 EtherChannel 用のポート チャネル インターフェイスを作成するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *port-channel-number*	ポート チャネル論理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 *port-channel-number* の 範囲は 1 ～ 48 です。
ステップ 3	**no switchport**	ポート チャネル インターフェイスをレイヤ 3 モードにします。
ステップ 4	**ip address** *ip-address mask*	EtherChannel に IP アドレスおよびサブネット マスクを割り当てます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show etherchannel** *channel-group-number* **detail**	設定を確認します。

	コマンド	目的
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 8		レイヤ 3 EtherChannel にイーサネット ポートを割り当てます。詳細については、「物理インターフェイスの設定」（P.35-15）を参照してください。

ポート チャネルを削除するには、**no interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用します。

次に、論理ポート チャネル 5 を作成し、IP アドレスとして 172.10.20.10 を割り当てる例を示します。

```
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

物理インターフェイスの設定

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。 PAgP EtherChannel の場合、同一タイプ、同一速度のポートを 8 つまで同一グループに設定できます。 LACP EtherChannel の場合は、同一タイプのイーサネット ポートを 16 まで設定できます。最大 8 個のポートをアクティブにして、最大 8 個のポートをスタンバイ モードにすることができます。 **（注）** インターフェイスが UNI の場合は、PAgP または LACP を設定する前に、**port-type {eni | nni}** インターフェイス コンフィギュレーション コマンドを入力する必要があります。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**no ip address**	この物理ポートに割り当てられている IP アドレスをすべて削除します。
ステップ 5	**no switchport**	ポートをレイヤ 3 モードにします。

	コマンド	目的
ステップ 6	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}	ポートをチャネル グループに割り当て、PAgP または LACP モードを指定します。 *channel-group-number* の範囲は 1 ～ 48 です。この番号は、「ポート チャネル論理インターフェイスの作成」（P.35-14）で設定された *port-channel-number*（論理ポート）と同じである必要があります。 **（注）**　UNI の場合、使用可能なモードは **on** だけです。 **mode** には、次のキーワードのいずれかを選択します。 • **auto**：PAgP デバイスが検出された場合にだけ、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。このステートの場合、ポートは受信した PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始しません。 • **desirable**：PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。このステートの場合、ポートは PAgP パケットを送信し、他のポートとのネゴシエーションを開始します。 • **on**：PAgP や LACP を使用せずに、ポートを強制的にチャネル化します。**on** モードでは、**on** モードのポート グループが **on** モードの別のポート グループに接続されている場合にだけ、EtherChannel を使用することが可能となります。 • **non-silent**：（任意）PAgP 対応のパートナーに接続されたスイッチのポートが **auto** モードまたは **desirable** モードの場合に、非サイレント動作を行うようにこのポートを設定します。**non-silent** を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザに接続する場合に使用します。この設定を使用すると、PAgP が動作したり、チャネル グループにポートを接続したり、ポートを伝送に使用したりできます。 • **active**：LACP デバイスが検出された場合にだけ、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。このステートの場合、ポートは LACP パケットを送信し、他のポートとのネゴシエーションを開始します。 • **passive**：ポートで LACP をイネーブルにしてパッシブ ネゴシエーション ステートにします。このステートの場合、ポートは受信した LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始しません。 スイッチとパートナー間で互換性のあるモードの詳細については、「PAgP モード」（P.35-5）および「LACP モード」（P.35-6）を参照してください。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、EtherChannel を設定する方法を示します。2 つのポートは、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

EtherChannel ロード バランシングの設定

ここでは、送信元ベースまたは宛先ベースの転送方法を使用し、EtherChannel のロード バランシングを設定する方法について説明します。詳細については、「ロード バランシングおよび転送方式」（P.35-7）を参照してください。

EtherChannel のロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}	EtherChannel のロード バランシング方法を設定します。 デフォルトは **src-mac** です。 次の負荷分散方式のいずれかを選択します。 • **dst-ip**：宛先ホスト IP アドレスに基づいて負荷分散を行います。 • **dst-mac**：着信パケットの宛先ホスト MAC アドレスに基づいて負荷分散を行います。 （注）　**dst-mac** キーワードを入力すると、チャンネル グループ内の 4 つのポート間だけで、トラフィックが均等化されます。宛先 MAC アドレス負荷分散を使用して EtherChannel 内で 4 つを超えるポートを設定すると、4 つのポートだけによって、分散されたトラフィックが受信されます。この制限は、他の負荷分散方式には適用されません。 • **src-dst-ip**：送信元/宛先ホスト IP アドレスに基づいて負荷分散を行います。 • **src-dst-mac**：送信元/宛先ホスト MAC アドレスに基づいて負荷分散を行います。 • **src-ip**：送信元ホスト IP アドレスに基づいて負荷分散を行います。 • **src-mac**：着信パケットの送信元 MAC アドレスに基づいて負荷分散を行います。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show etherchannel load-balance**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EtherChannel のロード バランシングをデフォルト設定に戻すには、**no port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

PAgP 学習方式およびプライオリティの設定

ネットワーク デバイスは PAgP の物理ラーナーまたは集約ポート ラーナーとして分類されます。物理ポートでアドレスを学習し、その知識に基づいて伝送を指示するデバイスが物理ラーナーです。集約（論理）ポートでアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

（注）　PAgP を使用できるのは、NNI および ENI 上だけです。

デバイスとそのパートナーが両方とも集約ポート ラーナーである場合、これらは論理ポート チャネルのアドレスを学習します。このデバイスは EtherChannel のポートのいずれかを使用し、送信元にパケットを送信します。集約ポート学習の場合、どの物理ポートにパケットが着信するかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーになる時期、および論理デバイスが集約ポート ラーナーになる時期を自動的には検出しません。したがって、物理ポートを使用してアドレスを学習する場合は、ローカル デバイスに手動で学習方式を設定する必要があります。負荷分散方式を送信元ベースに設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内にグループ内の未使用のポートに切り替えて動作させることができます。あるポートが常にパケット伝送に選択されるように設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注）　キーワード **physical-port** が CLI（コマンドライン インターフェイス）に指定されている場合でも、スイッチは集約ポートでだけアドレス学習を実行できます。**pagp learn-method** コマンドおよび **pagp port-priority** コマンドは、スイッチのハードウェアには影響しませんが、PAgP が物理ポートによるアドレス ラーニングだけをサポートするデバイスと相互運用するのに必要となります。

スイッチのリンク パートナーが物理ラーナーである場合は、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して、Cisco ME スイッチを物理ポート ラーナーとして設定することを推奨します。送信元 MAC アドレスに基づいて負荷分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。この設定により、送信元アドレスの学習元である EtherChannel 内の同じポートを使用して、パケットが物理ラーナー スイッチに送信されます。**pagp learn-method** コマンドは、この場合にだけ使用してください。

スイッチを PAgP 物理ポート ラーナーとして設定し、バンドル内の同じポートがパケット送信用として選択されるようにプライオリティを調整するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 （注）　インターフェイスが UNI の場合は、LACP を設定する前に、**port-type** {**eni** | **nni**} インターフェイス コンフィギュレーション コマンドを入力する必要があります。
ステップ 3	**pagp learn-method** physical-port	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port** 学習が選択されています。これにより、EtherChannel 内のいずれかのポートを使用して、パケットが送信元に送信されます。集約ポート学習の場合、どの物理ポートにパケットが着信するかは重要ではありません。 物理ラーナーである別のスイッチに接続するには、**physical-port** を選択します。**port-channel load-balance** グローバル コンフィギュレーション コマンドは、必ず **src-mac** に設定してください（「EtherChannel ロード バランシングの設定」（P.35-17）を参照）。 学習方式はリンクの両端で同一に設定する必要があります。 （注）　インターフェイスが UNI の場合は、PAgP を設定する前に、**port-type** {**eni** | **nni**} インターフェイス コンフィギュレーション コマンドを入力する必要があります。
ステップ 4	**pagp port-priority** *priority*	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* の範囲は 0 ～ 255 です。デフォルト値は 128 です。プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高まります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** または **show pagp** *channel-group-number* **internal**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

プライオリティをデフォルト設定に戻すには、**no pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。学習方式をデフォルト設定に戻すには、**no pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

LACP ホットスタンバイ ポートの設定

LACP がイネーブルの場合、チャネル内に最大数の LACP 対応ポートを設定しようとします（最大 16 ポート）。同時にアクティブにできる LACP リンクは 8 つだけです。これ以上のリンクはソフトウェアによってホットスタンバイ モードになります。アクティブ リンクの 1 つが非アクティブになると、代わりにホットスタンバイ モードになっているリンクがアクティブになります。

（注）　LACP を使用できるのは、NNI および ENI 上だけです。

EtherChannel グループに 8 リンクより多く設定されている場合、LACP プライオリティに基づいて、アクティブにするホットスタンバイ ポートがソフトウェアによって自動的に決定されます。ソフトウェアは LACP が動作するシステム間のリンクごとに、次の要素（プライオリティ順）からなる一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID（LACP システム プライオリティとスイッチの MAC アドレスの組み合せ）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。ハードウェアの制限により互換性のあるポートの一部を集約できない場合は、プライオリティによって、スタンバイ モードにする必要があるポートが決定されます。

ポートは、集約でプライオリティが最高のリンクに付加されたポートからリンクプライオリティの順番でアクティブに使用されるよう考慮されます。各ポートは、以前の高いプライオリティ選択が維持される場合にも、アクティブに使用されるよう選択されます。維持されない場合、ポートはスタンバイ モードとして選択されます。

LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更して、ソフトウェアによるアクティブおよびスタンバイ リンクの選択方法を変更できます。詳細については、「LACP システム プライオリティの設定」（P.35-20）および「LACP ポート プライオリティの設定」（P.35-21）を参照してください。

LACP システム プライオリティの設定

lacp system-priority グローバル コンフィギュレーション コマンドを使用して、LACP で使用可能なすべての EtherChannel にシステム プライオリティを設定できます。各 LACP 設定チャネルにはシステム プライオリティを設定できません。この値をデフォルトから変更すると、アクティブおよびスタンバイ リンクの選択方法を変更できます。

ホットスタンバイ モードのポートを確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します（ホットスタンバイ モードのポートには H ポートステート フラグが付加されます）。

LACP システム プライオリティを設定するには、特権 EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**lacp system-priority** *priority*	LACP システム プライオリティを設定します。 *priority* の範囲は 1 ～ 65535 です。デフォルト値は 32768 です。 値が小さいほど、システム プライオリティは高くなります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** または **show lacp sys-id**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

LACP システム プライオリティをデフォルト値に戻すには、**no lacp system-priority** グローバル コンフィギュレーション コマンドを使用します。

LACP ポート プライオリティの設定

すべてのポートは、デフォルトで同じポート プライオリティに設定されています。ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。ポート番号が小さなホットスタンバイ ポートほど、先にチャネル内でアクティブになります。ホットスタンバイ モードのポートを確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します（ホットスタンバイ モードのポートには H ポートステート フラグが付加されます）。

（注） LACP が互換性のあるすべてのポートを集約できない場合（たとえば、リモート システムのハードウェア上の制限など）、EtherChannel にアクティブに含められないすべてのポートはホット スタンバイ ステートとなり、チャネル ポートのいずれかが故障した場合にだけ使用されます。

LACP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 **（注）** インターフェイスが UNI の場合は、LACP を設定する前に、**port-type** {**eni** | **nni**} インターフェイス コンフィギュレーション コマンドを入力する必要があります。
ステップ 3	**lacp port-priority** *priority*	LACP ポート プライオリティを設定します。 *priority* の範囲は 1 ～ 65535 です。デフォルト値は 32768 です。プライオリティが低いほど、ポートが LACP 伝送に使用される可能性が高まります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show lacp** [*channel-group-number*] **internal**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

LACP ポート プライオリティをデフォルト値に戻すには、**no lacp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel、PAgP、および LACP ステータスの表示

EtherChannel、PAgP、および LACP ステータス情報を表示するには、表 35-4 に記載された特権 EXEC コマンドを使用します。

表 35-4　EtherChannel、PAgP、および LACP ステータスを表示するためのコマンド

コマンド	説明
show etherchannel [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}	EtherChannel 情報を簡潔、詳細に、1 行のサマリー形式で表示します。さらに、ロード バランシングまたはフレーム分散方式、ポート、ポート チャネル、およびプロトコル情報も表示します。
show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 PAgP 設定、近接情報などの PAgP 情報を表示します。
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 LACP 設定、近接情報などの LACP 情報を表示します。

PAgP チャネルグループ情報およびトラフィック カウンタをクリアするには、**clear pagp** {*channel-group-number* **counters** | **counters**} 特権 EXEC コマンドを使用します。

LACP チャネルグループ情報およびトラフィック カウンタをクリアするには、**clear lacp** {*channel-group-number* **counters** | **counters**} 特権 EXEC コマンドを使用します。

出力内の各フィールドについては、このリリースのコマンド リファレンス を参照してください。

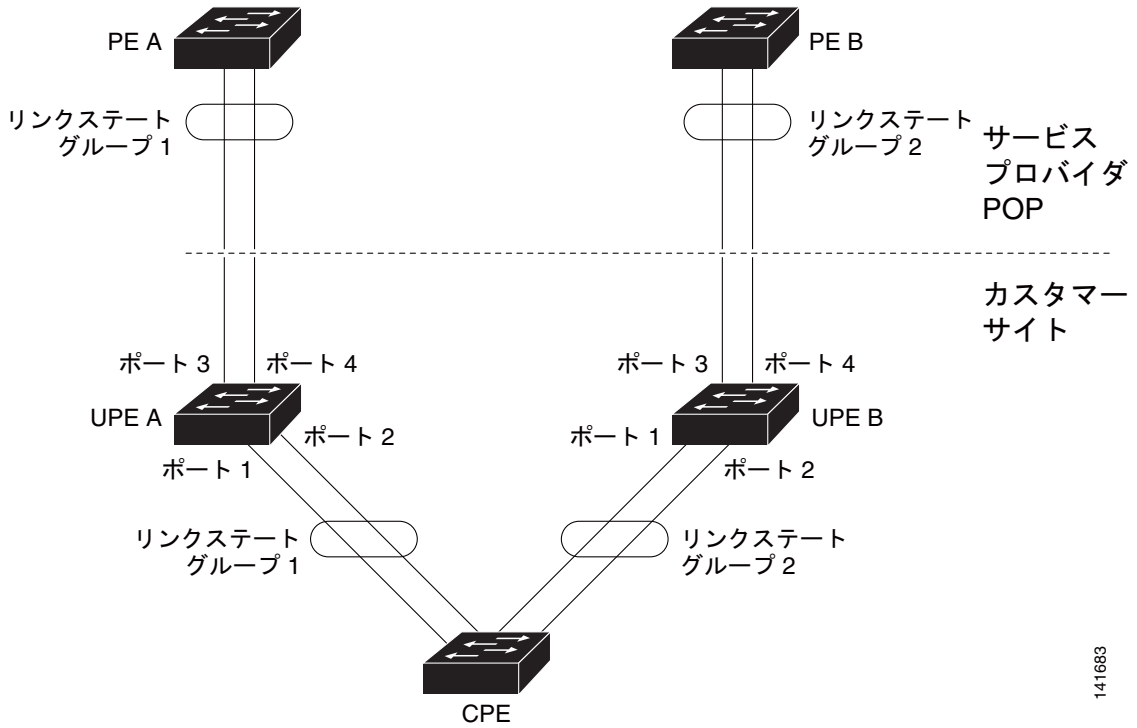
リンクステート追跡の概要

リンクステート追跡（トランク フェールオーバーとも呼ばれる）は、複数のインターフェイスのリンク ステートをバインドする機能です。たとえば、リンクステート追跡を Flex Link と一緒に使用すると、ネットワークの冗長性が実現されます。プライマリ インターフェイスでリンクが損失した場合、接続はセカンダリ インターフェイスに透過的に切り替えられます。

図 35-4 に示すように、Cisco ME 3400E スイッチの可能性あるスイッチは、Customer Premises Equipment（CPE; 顧客宅内機器）スイッチに接続されたプロバイダー ネットワークのエッジで、カスタマー側の User-facing Provider Edge（UPE）スイッチとして使用されます。UPE スイッチは、Service Provider（SP）ネットワークの Provider Edge（PE）スイッチに接続されます。クライアントなどの CPE スイッチに接続されているカスタマー デバイスは、SP ネットワークとの複数の回線を維持できます。この設定により、カスタマー側から SP へのトラフィック フロー（その逆も同様）が均等化されます。CPE に接続されるポートは、ダウンストリーム ポートと呼ばれ、PE スイッチに接続されるポートは、アップストリーム ポートと呼ばれます。

- UPE スイッチ A は、リンクステート グループ 1 を介して CPE へのリンクを提供します。ポート 1 および 2 は、CPE に接続されています。ポート 3 およびポート 4 は、リンクステート グループ 1 を介して PE スイッチ A に接続されています。
- UPE スイッチ B は、リンクステート グループ 2 を介する CPE へのリンクを提供します。ポート 1 および 2 は、CPE に接続されています。ポート 3 およびポート 4 は、リンクステート グループ 2 を介して PE スイッチ A に接続されます。

図 35-4　一般的なリンクステート追跡の設定



スイッチ上でリンクステート追跡をイネーブルにすると、ダウンストリーム ポートのリンク ステートは、1 つまたは複数のアップストリーム ポートのリンク ステートにバインドされます。一連のダウンストリーム ポートを一連のアップストリーム ポートに関連付けたあとで、すべてのアップストリーム ポートが使用不可になった場合、リンクステート追跡により関連付けられたダウンストリーム ポートが自動的に errdisable ステートになります。これにより、CPE プライマリ インターフェイスはセカンダリ インターフェイスにフェールオーバーします。

PE スイッチで障害が発生したり、ケーブルが切断されたり、またはリンクが損失したりした場合、アップストリーム インターフェイスの接続が切断される可能性があります。リンクステート追跡がイネーブルでない場合に、アップストリーム インターフェイスで接続が切断されても、ダウンストリーム インターフェイスのリンク ステートは変更されません。CPE は、アップストリームの接続が切断されたことを認識しないため、セカンダリ インターフェイスにフェールオーバーしません。

インターフェイスはポートの集約（EtherChannel）、アクセス モードまたはトランク モードでの単一の物理ポート、またはルーテッド ポートにできます。これらのインターフェイスはまとめてバンドルでき、各ダウンストリーム インターフェイスは複数のアップストリーム インターフェイスで構成される単一のグループ（リンクステート グループと呼ばれる）に関連付けることができます。

リンクステート グループでは、ダウンストリーム インターフェイスのリンク ステートはアップストリーム インターフェイスのリンク ステートによって異なります。リンクステート グループ内のすべてのアップストリーム インターフェイスがリンクダウン ステートである場合、関連付けられたダウンストリーム インターフェイスは強制的にリンクダウン ステートになります。リンクステート グループ内の任意のアップストリーム インターフェイスがリンクアップ ステートである場合、関連付けられたダウンストリーム インターフェイスはリンクアップ ステートに変更されるか、リンクアップ ステートのままにできます。

たとえば図 35-4 では、UPE スイッチ A 上のダウンストリーム インターフェイス 1 および 2 は、アップストリーム インターフェイス 3 および 4 を含むリンクステート グループ 1 に定義されます。同様に、UPE スイッチ B 上のダウンストリーム インターフェイス 1 および 2 は、アップストリーム インターフェイス 3 および 4 を含むリンクステート グループ 2 に定義されます。

アップストリーム インターフェイス 3 でリンクが損失した場合、ダウンストリーム インターフェイス 1 および 2 のリンク ステートは変更されません。アップストリーム インターフェイス 4 でもリンクが損失した場合は、ダウンストリーム インターフェイス 1 および 2 はリンクダウン ステートに変更されます。CPE スイッチは、PE スイッチ A へのトラフィック転送を停止して、PE スイッチ B へのトラフィック転送を開始します。

リンクステート グループから障害のあるダウンストリーム ポートを削除することにより、ダウンストリーム インターフェイスのリンクダウン状態から回復できます。複数のダウンストリーム インターフェイスを回復するには、リンクステート グループをディセーブルにします。

リンクステート追跡の設定

- 「リンクステート追跡のデフォルト設定」（P.35-24）
- 「リンクステート追跡の設定上の注意事項」（P.35-24）
- 「リンクステート追跡の設定」（P.35-24）

リンクステート追跡のデフォルト設定

リンクステート グループは定義されていません。また、リンクステート追跡はどのグループに対してもイネーブルではありません。

リンクステート追跡の設定上の注意事項

- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。
- インターフェイスは、複数のリンクステート グループのメンバーにはなれません。
- スイッチごとに設定できるのは、2 個のリンクステート グループのみです。

リンクステート追跡の設定

リンクステート グループを設定し、そのグループにインターフェイスを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**link state track** *number*	リンクステート グループを作成して、リンクステート追跡をイネーブルにします。指定できるグループ番号は 1 ～ 2 で、デフォルトは 1 です。

	コマンド	目的
ステップ 3	**interface** *interface-id*	設定する物理インターフェイスまたはインターフェイスの範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、アクセス モードまたはトランク モード（IEEE 802.1Q）のスイッチポート、ルーテッド ポート、または EtherChannel インターフェイス（スタティックまたは LACP）にバンドルされている複数のポート（トランク モード）が含まれます。
ステップ 4	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5	**link state group** [*number*] {**upstream** | **downstream**}	リンクステート グループを指定して、グループ内の**アップストリーム**または**ダウンストリーム**インターフェイスとしてインターフェイスを設定します。指定できる番号は 1 ～ 2 で、デフォルトは 1 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、リンクステート グループを作成して、インターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range fastethernet/0/9 -10
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface fastethernet0/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

リンクステート グループをディセーブルにするには、**no link state track** *number* グローバル コンフィギュレーション コマンドを使用します。

リンクステート追跡ステータスの表示

リンクステート グループの情報を表示するには、**show link state group** コマンドを使用します。キーワードを指定しないでこのコマンドを使用すると、すべてのリンクステート グループの情報が表示されます。特定のグループの情報を表示するには、グループ番号を入力します。グループの詳細情報を表示するには、detail キーワードを使用します。

次の例では、**show link state group 1** コマンドの出力を示します。

```
Switch> show link state group 1

Link State Group: 1      Status: Enabled, Down
```

次の例では、**show link state group detail** コマンドの出力を示します。

```
Switch> show link state group detail
```

```
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Fa0/15(Dwn) Fa0/16(Dwn)
Downstream Interfaces : Fa0/11(Dis) Fa0/12(Dis) Fa0/13(Dis) Fa0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Fa0/15(Dwn) Fa0/16(Dwn) Fa0/17(Dwn)
Downstream Interfaces : Fa0/11(Dis) Fa0/12(Dis) Fa0/13(Dis) Fa0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

CHAPTER 36

IP ユニキャスト ルーティングの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチ上で IP バージョン 4（IPv4）ユニキャスト ルーティングを設定する方法について説明します。IPv6 ルーティングの詳細については、第 37 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

（注） ルーティングは、メトロ IP アクセス イメージが稼動しているスイッチ上でだけサポートされています。

IPv4 ユニキャスト設定の詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* を参照してください。この章で使用するコマンドの構文および使用方法については、次のコマンド リファレンスを参照してください。

- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』*Release 12.2*
- 『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2*
- 『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』*Release 12.2*

この章で説明する内容は、次のとおりです。

- 「IP ルーティングの概要」（P.36-2）
- 「ルーティングを設定する手順」（P.36-3）
- 「IP アドレス指定の設定」（P.36-4）
- 「IPv4 ユニキャスト ルーティングのイネーブル化」（P.36-19）
- 「RIP の設定」（P.36-20）
- 「OSPF の設定」（P.36-25）
- 「EIGRP の設定」（P.36-38）
- 「BGP の設定」（P.36-45）
- 「ISO CLNS ルーティングの設定」（P.36-67）
- 「BFD の設定」（P.36-78）
- 「マルチ VRF CE の設定」（P.36-88）
- 「プロトコルに依存しない機能の設定」（P.36-101）
- 「IP ネットワークのモニタリングおよびメンテナンス」（P.36-117）

（注） スイッチにルーティング パラメータを設定する場合、使用できるユニキャスト ルート数が最大となるようにシステム リソースを割り当てるには、**sdm prefer default** グローバル コンフィギュレーション コマンドを使用して、バランス リソースに Switch Database Management（SDM; スイッチ データベース管理）機能を設定する必要があります。レイヤ 2 テンプレートでは、ルーティングはサポートされて

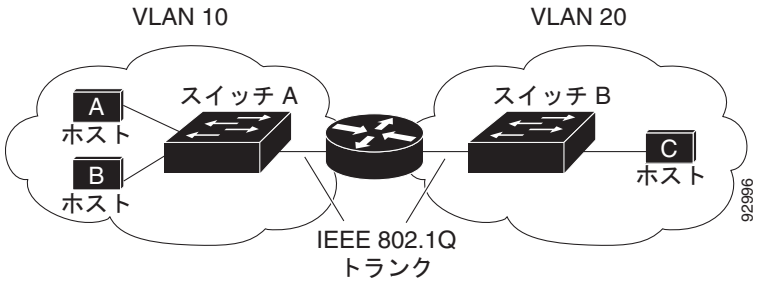
いません。そのため、ルーティングはすべてソフトウェアを介して実行されます。この場合、CPU に負荷がかかり、ルーティングのパフォーマンスが大幅に低下します。SDM テンプレートの詳細については、第 7 章「SDM テンプレートの設定」、またはこのリリースのコマンド リファレンスの **sdm prefer** コマンドの項を参照してください。

IP ルーティングの概要

IP ネットワークでは、各サブネットワークは 1 つの VLAN に対応しています。ただし、別々の VLAN に属するネットワーク デバイスが相互に通信するには、VLAN 間でトラフィックをルーティング（VLAN 間ルーティング）するレイヤ 3 デバイス（ルータ）が必要です。VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

図 36-1 は、基本的なルーティング トポロジを示したものです。スイッチ A は VLAN 10 に、スイッチ B は VLAN 20 にそれぞれ属しています。ルータには、各 VLAN のインターフェイスがあります。

図 36-1　　ルーティング トポロジの例



VLAN 10 内のホスト A が VLAN 10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。スイッチ A はパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでそのトラフィックを受信します。ルータは、ルーティング テーブルをチェックして、適切な発信インターフェイスを特定し、VLAN 20 インターフェイスからパケットをスイッチ B へ転送します。スイッチ B はパケットを受け取り、それをホスト C へ転送します。

ルーティングのタイプ

ルータおよびレイヤ 3 スイッチは、次の 3 つの方法でパケットをルーティングできます。

- デフォルト ルーティングを使用する（ルータにとって宛先が不明なトラフィックをデフォルトの出口または宛先に送信する）
- トラフィックに対して事前にプログラミングされたスタティック ルートを使用する

  スタティック ユニキャスト ルーティングの場合、パケットは事前に設定されたポートから単一のパスを経由して、ネットワークの内部または外部に転送されます。スタティック ルーティングでは、ネットワーク内の構成の変更に自動的には対応できないため、パケットが宛先に到達しない場合があります。
- ルーティング プロトコルを使用してルートをダイナミックに計算する

ダイナミック ルーティング プロトコルに基づいて、トラフィックを転送する最適ルートがルータによりダイナミックに計算されます。スイッチでは、ルーティング プロトコルとして、Routing Information Protocol（RIP）、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）、Open Shortest Path First（OSPF）プロトコル、Enhanced IGRP（EIGRP）、Intermediate System-to-Intermediate System（IS-IS）、および Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）がサポートされています。

ルーティングを設定する手順

デフォルトでは、IPv4 ルーティングはスイッチ上でディセーブルとなっています。ルーティングを行う前に、IPv4 ルーティングをイネーブルにする必要があります。IP ルーティング コンフィギュレーションの詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* を参照してください。

以下で説明する手順では、次に示すレイヤ 3 インターフェイスのうちいずれか 1 つを指定する必要があります。

- ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドによりレイヤ 3 ポートとして設定された物理ポート。
- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）：**interface vlan** *vlan_id* グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
- レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイス。詳細については、「レイヤ 3 EtherChannel の設定」（P.35-14）を参照してください。

（注）　スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。

ルーティングが発生するすべてのレイヤ 3 インターフェイスに、IP アドレスを割り当てる必要があります。「ネットワーク インターフェイスへの IP アドレスの割り当て」（P.36-5）を参照してください。

（注）　レイヤ 3 スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。ソフトウェアには、設定できるルーテッド ポートおよび SVI の個数制限はありません。ただし、ハードウェアには限界があるため、この個数と実装されている他の機能の数との組み合せによっては、CPU のパフォーマンスに影響する場合もあります。IPv4 ルーティングをサポートするには、**sdm prefer default** グローバル コンフィギュレーション コマンドを使用します。

IPv4g ルーティングを設定するための主な手順は次のとおりです。

- VLAN インターフェイスをサポートするために、スイッチ上で VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てます。詳細については、第 12 章「VLAN の設定」を参照してください。
- レイヤ 3 インターフェイスを設定します。
- スイッチ上で IPv4 ルーティングをイネーブルにします。
- レイヤ 3 インターフェイスに IPv4 アドレスを割り当てます。
- 選択したルーティング プロトコルをスイッチ上でイネーブルにします。
- ルーティング プロトコル パラメータを設定します（任意）。

IP アドレス指定の設定

IP ルーティングでは、レイヤ 3 ネットワーク インターフェイスに IP アドレスを割り当てて、そのインターフェイスをイネーブルにし、IP を使用するインターフェイスを介してホストと通信できるようにする必要があります。ここでは、さまざまな IP アドレス指定機能の設定方法について説明します。IP アドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

- 「アドレス指定のデフォルト設定」（P.36-4）
- 「ネットワーク インターフェイスへの IP アドレスの割り当て」（P.36-5）
- 「アドレス解決方法の設定」（P.36-8）
- 「IP ルーティングがディセーブルの場合のルーティング支援機能」（P.36-11）
- 「ブロードキャスト パケットの処理方法の設定」（P.36-13）
- 「IP アドレス指定のモニタリングおよびメンテナンス」（P.36-18）

アドレス指定のデフォルト設定

表 36-1　アドレス指定のデフォルト設定

機能	デフォルト設定
IP アドレス	定義なし。
ARP	Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュに永続的なエントリはありません。 カプセル化：標準イーサネット形式の ARP。 タイムアウト：14400 秒（4 時間）。
IP ブロードキャスト アドレス	255.255.255.255（すべて 1）。
IP クラスレス ルーティング	イネーブル。
IP デフォルト ゲートウェイ	ディセーブル。
IP ダイレクト ブロードキャスト	ディセーブル（すべての IP ダイレクト ブロードキャストが廃棄されます）。
IP ドメイン	ドメイン リスト：ドメイン名は定義されていません。 ドメイン検索：イネーブル。 ドメイン名：イネーブル。
IP 転送プロトコル	ヘルパー アドレスが定義されているか、または UDP フラッディングが設定されている場合、デフォルト ポートでは UDP 転送がイネーブルとなります。 ローカル ブロードキャスト：ディセーブル。 ターボ フラッディング：ディセーブル。
IP ヘルパー アドレス	ディセーブル。
IP ホスト	ディセーブル。

表 36-1　アドレス指定のデフォルト設定 （続き）

機能	デフォルト設定
ICMP Router Discovery Protocol（IRDP）	ディセーブル。 イネーブルの場合のデフォルト： • ブロードキャスト IRDP アドバタイズメント • アドバタイズメント間の最大インターバル：600 秒。 • アドバタイズメント間の最小インターバル：最大インターバルの 0.75 倍。 • プリファレンス：0。
IP プロキシ ARP	イネーブル。
IP ルーティング	ディセーブル。
IP サブネットゼロ	ディセーブル。

ネットワーク インターフェイスへの IP アドレスの割り当て

IP パケットの送信先は、IP アドレスで表されます。インターフェイスには、1 つのプライマリ IP アドレスを設定できます。マスクは、IP アドレスのネットワーク番号を表すビット列を特定するためのものです。マスクを使用してネットワークをサブネット化する場合、そのマスクをサブネット マスクと呼びます。割り当てられているネットワーク番号については、インターネット サービス プロバイダーにお問い合せください。

IP アドレスおよびネットワーク マスクをレイヤ 3 インターフェイスに割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）および Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブル、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルです。
ステップ 4	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 5	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **show ip interface** [*interface-id*] **show running-config interface** [*interface-id*]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

サブネット ゼロの使用

サブネット アドレスがゼロのサブネットは絶対に作成しないでください。同じアドレスを持つネットワークおよびサブネットがある場合に問題が発生するおそれがあります。たとえば、ネットワーク 131.108.0.0 のサブネットが 255.255.255.0 の場合、サブネット ゼロは 131.108.0.0 と記述され、ネットワーク アドレスと同じとなってしまいます。

オール 1 サブネット（131.108.255.0）は使用可能です。また、IP アドレス用にサブネット スペース全体が必要な場合は、サブネット ゼロの使用をイネーブルにできます（ただし推奨できません）。

サブネット ゼロをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip subnet-zero**	インターフェイス アドレスおよびルーティングの更新時におけるサブネット ゼロの使用をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトに戻して サブネット ゼロの使用をディセーブルにするには、**no ip subnet-zero** グローバル コンフィギュレーション コマンドを使用します。

クラスレス ルーティング

ルーティングを行うように設定されたスイッチ上では、クラスレス ルーティング動作がデフォルトでイネーブルになっています。クラスレス ルーティングがイネーブルの場合、デフォルト ルートがないネットワークのサブネット宛パケットを受信したルータは、最適なスーパーネット ルートにパケットを転送します。*スーパーネット*は、連続する複数のクラス C アドレス レンジを 1 つにまとめたブロックにより構成され、それぞれのブロックにより比較的規模の大きな 1 つのアドレス レンジが疑似的に形成されます。スーパーネットは、クラス B アドレス レンジの急速な枯渇を回避するために設計されたものです。

図 36-2 では、クラスレス ルーティングがイネーブルとなっています。ホストから 128.20.4.1 へパケットが送信されると、ルータはそのパケットを廃棄せずに、最適なスーパーネット ルートに転送します。クラスレス ルーティングがディセーブルの場合、デフォルト ルートがないネットワークのサブネット宛パケットを受信したルータは、パケットを廃棄します。

図 36-2　IP クラスレス ルーティングがイネーブルの場合

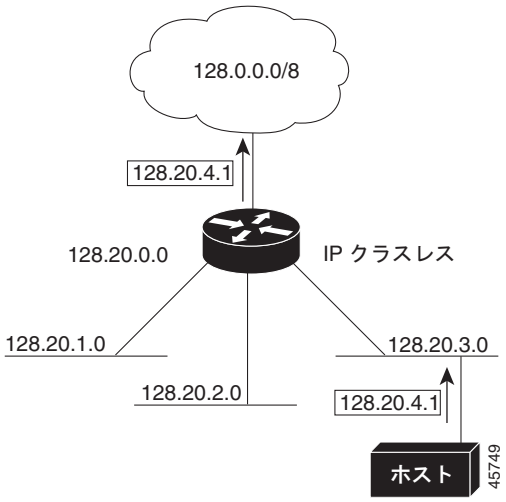
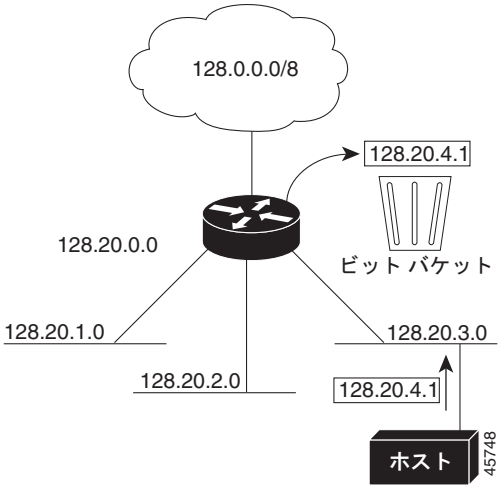


図 36-3 では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、および 128.20.3.0 に接続されています。ホストから 128.20.4.1 へパケットが送信された場合、ネットワークにはデフォルト ルートが存在しないため、ルータはそのパケットを廃棄します。

図 36-3　IP クラスレス ルーティングがディセーブルの場合



認識されないサブネット宛のパケットが最適なスーパーネット ルートに転送されないようにするには、クラスレス ルーティング動作をディセーブルにします。

クラスレス ルーティングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ip classless**	クラスレス ルーティング動作をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトに戻して、デフォルト ルートがないネットワークのサブネット宛パケットが最適なスーパーネット ルートに転送されるようにするには、**ip classless** グローバル コンフィギュレーション コマンドを使用します。

アドレス解決方法の設定

インターフェイス固有の IP 処理方法を制御するには、アドレス解決を行います。IP を使用するデバイスには、ローカル セグメントまたは LAN 上のデバイスを一意に定義するローカル アドレス（MAC アドレス）と、そのデバイスが属しているネットワークを表すネットワーク アドレスが割り当てられます。ソフトウェアがイーサネット上のデバイスと通信するには、デバイスの MAC アドレスを学習する必要があります。IP アドレスから MAC アドレスを学習するプロセスを、「*アドレス解決*」と呼びます。MAC アドレスから IP アドレスを学習するプロセスを、「*逆アドレス解決*」と呼びます。

スイッチでは、次の形式のアドレス解決を行えます。

- ARP：IP アドレスを基に対応する MAC アドレスを取得する場合に使用します。ARP は、入力として IP アドレスを受け取ると、それに対応する MAC アドレスを学習します。また、以降の取得を高速化できるように、IP アドレスと MAC アドレスの対応が ARP キャッシュに格納されます。そのあと、IP データグラムはリンクレイヤ フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化、および ARP 要求や応答については、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）で規定されています。
- プロキシ ARP：ルーティング テーブルを持たないホストで、他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにします。スイッチ（ルータ）が送信元と異なるインターフェイス上のホストに宛てた ARP 要求を受信した場合、他のインターフェイスを経由してそのホストに至るすべてのルートがそのルータに格納されていれば、ルータは自身のローカル データ リンク アドレスを示すプロキシ ARP パケットを生成します。ARP 要求を送信したホストはルータにパケットを送信し、ルータはそれらのパケットを目的のホストに転送します。

スイッチでは、ARP と同様の機能（ローカル MAC アドレスでなく IP アドレスを要求する点を除く）を持つ Reverse Address Resolution Protocol（RARP; 逆アドレス解決プロトコル）を使用することもできます。RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメント上に RARP サーバを設置する必要があります。サーバを特定する必要がある場合は、**ip rarp-server** *address* インターフェイス コンフィギュレーション コマンドを使用します。

RARP の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』*Release 12.2* を参照してください。

アドレス解決を設定するために必要な作業は次のとおりです。

- 「スタティック ARP キャッシュの定義」（P.36-8）
- 「ARP カプセル化の設定」（P.36-10）
- 「プロキシ ARP のイネーブル化」（P.36-10）

スタティック ARP キャッシュの定義

ARP などのアドレス解決プロトコルを使用すると、IP アドレスと MAC アドレスをダイナミックにマッピングできます。ほとんどのホストではダイナミックなアドレス解決がサポートされているため、通常は、スタティック ARP キャッシュ エントリを指定する必要はありません。スタティック ARP キャッシュ エントリを定義する必要がある場合は、グローバルに定義できます。グローバルに定義すると、IP アドレスを MAC アドレスに変換するために使用される永続的なエントリを ARP キャッシュに設定できます。また、指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定することもできます。ARP エントリを永続的なエントリにしない場合は、その ARP エントリに対してタイムアウト期間を指定できます。

IP アドレスと MAC アドレスの間でスタティック マッピングを行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**arp** *ip-address hardware-address type*	ARP キャッシュ内で IP アドレスを MAC（ハードウェア）アドレスにグローバルに関連付け、次に示すカプセル化タイプのいずれかを指定します。 • **arpa**：ARP カプセル化（イーサネット インターフェイス用） • **snap**：SNAP カプセル化（トークンリングおよび FDDI のインターフェイス用） • **sap**：HP の ARP タイプ
ステップ 3	**arp** *ip-address hardware-address type* [*alias*]	（任意）指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定します。
ステップ 4	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 5	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 6	**arp timeout** *seconds*	（任意）ARP キャッシュ エントリがキャッシュに保持される期間を設定します。デフォルトは 14400 秒（4 時間）です。指定できる範囲は 0 ～ 2147483 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*]	すべてのインターフェイスまたは特定のインターフェイスで使用される ARP のタイプおよびタイムアウト値を確認します。
ステップ 9	**show arp** または **show ip arp**	ARP キャッシュの内容を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ARP キャッシュからエントリを削除するには、**no arp** *ip-address hardware-address type* グローバル コンフィギュレーション コマンドを使用します。ARP キャッシュから非スタティック エントリをすべて削除するには、**clear arp-cache** 特権 EXEC コマンドを使用します。

ARP カプセル化の設定

IP インターフェイスでは、イーサネット ARP 形式の ARP カプセル化（キーワード **arpa** で表される）がデフォルトでイネーブルに設定されています。ネットワークの必要性に応じて、カプセル化方法を SNAP に変更できます。

ARP カプセル化タイプを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**arp** {**arpa** | **snap**}	ARP カプセル化方法を指定します。 • **arpa**：ARP • **snap**：SNAP
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスの ARP カプセル化設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

カプセル化タイプをディセーブルにするには、**no arp arpa** インターフェイス コンフィギュレーション コマンドまたは **no arp snap** インターフェイス コンフィギュレーション コマンドを使用します。

プロキシ ARP のイネーブル化

デフォルトの場合、スイッチでは、ホストが他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにするためのプロトコルとして、プロキシ ARP が使用されます。

ディセーブルになっているプロキシ ARP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip proxy-arp**	インターフェイスでプロキシ ARP をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show ip interface** [*interface-id*]	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスでプロキシ ARP をディセーブルにするには、**no ip proxy-arp** インターフェイス コンフィギュレーション コマンドを使用します。

IP ルーティングがディセーブルの場合のルーティング支援機能

IP ルーティングがイネーブルでないスイッチでは、次のメカニズムを使用することで、別のネットワークへのルートを学習できます。

- 「プロキシ ARP」（P.36-11）
- 「デフォルト ゲートウェイ」（P.36-11）
- 「IRDP」（P.36-12）

プロキシ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネット ホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。ルーティング情報を持たないホストは、すべてのホストが同じローカル イーサネット上にあり、かつそれらが ARP を使用して MAC アドレスを学習するという仮定の下で動作します。送信元と異なるネットワーク上のホストに宛てた ARP 要求を受信したスイッチは、そのホストへの最適なルートがあるかどうかを調べます。最適ルートがある場合、スイッチはスイッチ自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信します。要求の送信元ホストはパケットをスイッチに送信し、スイッチはそのパケットを目的のホストに転送します。プロキシ ARP では、すべてのネットワークがローカルにある場合と同様に処理され、IP アドレスごとに ARP 要求が実行されます。

デフォルトでは、プロキシ ARP はイネーブルに設定されています。ディセーブル化されたプロキシ ARP をイネーブルにする方法については、「プロキシ ARP のイネーブル化」（P.36-10）を参照してください。プロキシ ARP は、他のルータでサポートされていれば有効です。

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法として、デフォルト ルータ（デフォルト ゲートウェイ）を定義するという方法があります。ローカルでないすべてのパケットはこのルータに送信されます。このルータは、適切にルーティングを行うか、または IP Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）リダイレクト メッセージを返信することでホストが使用するローカル ルータを指定します。スイッチはリダイレクト メッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送します。この方法には、デフォルト ルータがダウンした場合や使用できなくなった場合に、そのことを検出できないという短所があります。

IP ルーティングがディセーブルの場合にデフォルト ゲートウェイ（ルータ）を定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip default-gateway** *ip-address*	デフォルト ゲートウェイ（ルータ）を設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip redirects**	設定を確認するため、デフォルト ゲートウェイ ルータのアドレスを表示します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、**no ip default-gateway** グローバル コンフィギュレーション コマンドを使用します。

IRDP

スイッチでは、ルータ ディスカバリを使用することにより、IRDP を介して他のネットワークへのルートをダイナミックに学習できます。ホストは、IRDP を使用してルータを特定します。クライアントとして動作しているスイッチは、ルータ ディスカバリ パケットを生成します。ホストとして動作しているスイッチは、ルータ ディスカバリ パケットを受信します。スイッチは RIP ルーティングの更新を受信し、この情報からルータの場所を推測することもできます。ただし、実際のところ、スイッチには、ルーティング デバイスによって送信されたルーティング テーブルが格納されるわけではなく、どのシステムがデータを送信しているのかが記録されるだけです。IRDP には、プライオリティと、パケットが受信されなくなってからデバイスがダウンしていると見なされるまでの期間を、ルータごとに指定できるという利点があります。

検出された各デバイスは、デフォルト ルータの候補となります。プライオリティがより高いルータが検出された場合、現在のデフォルト ルータがダウンしたと宣言された場合、または再転送が多すぎるために TCP 接続がタイムアウトに近づいている場合には、最も高いプライオリティを持つルータが新たに選択されます。

インターフェイスで IRDP ルーティングを行うには、そのインターフェイスで IRDP 処理をイネーブルにしてください。IRDP 処理をイネーブルにすると、デフォルトのパラメータが適用されます。これらのパラメータは、必要に応じて変更することもできます。

インターフェイス上で IRDP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip irdp**	インターフェイス上で IRDP 処理をイネーブルにします。

	コマンド	目的
ステップ 5	**ip irdp multicast**	（任意）IP ブロードキャストの代わりとして、マルチキャスト アドレス（224.0.0.1）に IRDP アドバタイズメントを送信します。 **（注）** このコマンドを使用すると、IRDP パケットをマルチキャストとして送信するサン マイクロシステムズ社の Solaris との互換性を維持できます。実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。
ステップ 6	**ip irdp holdtime** *seconds*	（任意）アドバタイズメントが有効である IRDP 期間を設定します。デフォルトは **maxadvertinterval** 値の 3 倍です。**maxadvertinterval** 値よりも大きな値（9000 秒以下）を指定する必要があります。**maxadvertinterval** 値を変更すると、この値も変更されます。
ステップ 7	**ip irdp maxadvertinterval** *seconds*	（任意）アドバタイズメント間の IRDP の最大インターバルを設定します。デフォルトは 600 秒です。
ステップ 8	**ip irdp minadvertinterval** *seconds*	（任意）アドバタイズメント間の IRDP の最小インターバルを設定します。デフォルトは **maxadvertinterval** 値の 0.75 倍です。**maxadvertinterval** を変更すると、この値も新しいデフォルト値（**maxadvertinterval** の 0.75 倍）に変更されます。
ステップ 9	**ip irdp preference** *number*	（任意）デバイスの IRDP プリファレンス レベルを設定します。指定できる範囲は -2^{31} ～ 2^{31} です。デフォルト値は 0 です。この値を大きくするにつれて、ルータのプリファレンス レベルは高くなります。
ステップ 10	**ip irdp address** *address* [*number*]	（任意）プロキシアドバタイズを行うために必要な IRDP アドレスおよびプリファレンスを指定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip irdp**	IRDP 値を表示し、設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

maxadvertinterval 値を変更すると、**holdtime** 値および **minadvertinterval** 値も変更されます。そのため、**holdtime** 値または **minadvertinterval** 値のいずれかを手動で変更するには、最初に **maxadvertinterval** 値を変更しておくことが重要です。

IRDP ルーティングをディセーブルにするには、**no ip irdp** インターフェイス コンフィギュレーション コマンドを使用します。

ブロードキャスト パケットの処理方法の設定

IP インターフェイス アドレスを設定すると、ルーティングをイネーブルにしたり、1 つまたは複数のルーティング プロトコルを設定したり、ネットワーク ブロードキャストへのスイッチの応答方法を設定したりできます。ブロードキャストは、物理ネットワーク上のすべてのホスト宛のデータ パケットです。スイッチでは、2 種類のブロードキャストがサポートされています。

- ダイレクト ブロードキャスト パケット：特定のネットワークまたは一連のネットワークに送信されます。ダイレクト ブロードキャスト アドレスには、ネットワーク フィールドまたはサブネット フィールドが含まれます。
- フラッディング ブロードキャスト パケット：すべてのネットワークに送信されます。

（注）　**storm-control** インターフェイス コンフィギュレーション コマンドを使用してトラフィック抑制レベルを設定することによっても、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、マルチキャストの各トラフィックを制限できます。詳細については、第 23 章「ポートベースのトラフィック制御の設定」を参照してください。

ルータでは、ブロードキャスト ストームを防ぐため、ローカル ケーブル長が制限されています。ブリッジ（インテリジェント ブリッジを含む）はレイヤ 2 デバイスであるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームが伝播します。ブロードキャスト ストーム問題を解決するには、ネットワーク上で単一のブロードキャスト アドレス方式を使用するのが最善の方法です。最新の IP 実装機能ではほとんどの場合、アドレスをブロードキャスト アドレスとして使用するように設定できます。スイッチでは、ブロードキャスト メッセージの転送用として複数のアドレス指定スキームがサポートされています。

- 「指定ブロードキャストから物理ブロードキャストへの変換のイネーブル化」（P.36-14）
- 「UDP ブロードキャスト パケットおよびプロトコルの転送」（P.36-15）
- 「IP ブロードキャスト アドレスの確立」（P.36-16）
- 「IP ブロードキャストのフラッディング」（P.36-17）

指定ブロードキャストから物理ブロードキャストへの変換のイネーブル化

サービス拒絶攻撃からルータを極力保護するため、デフォルトでは、IP ダイレクト ブロードキャストは転送されず廃棄されます。ブロードキャストが物理（MAC レイヤ）ブロードキャストになるインターフェイスでは、IP ダイレクト ブロードキャストの転送をイネーブルにできます。転送できるのは、**ip forward-protocol** グローバル コンフィギュレーション コマンドを使用して設定したプロトコルだけです。

アクセス リストを指定すると、転送するブロードキャストを制御できます。アクセス リストで許可されている IP パケットに限り、指定ブロードキャストから物理ブロードキャストに変換できるようになります。アクセス リストの詳細については、第 32 章「ACL によるネットワーク セキュリティの設定」を参照してください。

インターフェイス上で IP 指定ブロードキャストの転送をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip directed-broadcast** [*access-list-number*]	インターフェイス上で、指定ブロードキャストから物理ブロードキャストへの変換をイネーブルにします。アクセス リストを指定すると、転送するブロードキャストを制御できます。アクセス リストを指定した場合、そのアクセス リストで許可されている IP パケットだけが変換可能となります。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	ブロードキャスト パケットを転送する際に、ルータによって転送されるプロトコルおよびポートを指定します。 • **udp**：UDP データグラムを転送します。 *port*：（任意）転送される UDP サービスを制御する宛先ポートを指定します。 • **nd**：ND データグラムを転送します。 • **sdns**：SDNS データグラムを転送します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** [*interface-id*] または **show running-config**	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

指定ブロードキャストから物理ブロードキャストへの変換をディセーブルにするには、**no ip directed-broadcast** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

UDP ブロードキャスト パケットおよびプロトコルの転送

User Datagram Protocol（UDP; ユーザ データグラム プロトコル）は、2 つのエンド システム間でオーバーヘッドの少ないコネクションレス型セッションを実現する IP ホストツーホスト レイヤ プロトコルです。UDP では、受信したデータグラムの確認応答は行われません。ネットワーク ホストでは、UDP ブロードキャストを使用して、アドレス、設定、名前などの情報の検索が行われる場合もあります。このようなホストが、サーバの存在しないネットワーク セグメントに属する場合は、通常 UDP ブロードキャストは転送されません。ルータ上では、特定のクラスのブロードキャストがヘルパー アドレスへ転送されるように、インターフェイスを設定できます。それぞれのインターフェイスに対して、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定すると、転送される UDP サービスを制御できます。UDP プロトコルは複数指定することもできます。また、旧式のディスクレス Sun ワークステーションおよびネットワーク セキュリティ プロトコル SDNS で使用される Network Disk（ND; ネットワーク ディスク）プロトコルも指定できます。

ヘルパー アドレスがインターフェイスに定義されている場合、デフォルトでは UDP と ND の両方の転送がイネーブルになっています。UDP ポートを指定しない場合にデフォルトで転送されるポートについては、『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』*Release 12.2* の **ip forward-protocol** インターフェイス コンフィギュレーション コマンドに関する説明箇所に記載されているリストを参照してください。

UDP ブロードキャストの転送を設定するときに UDP ポートを指定しないと、ルータは BOOTP 転送エージェントとして動作するように設定されます。BOOTP パケットは Dynamic Host Configuration Protocol（DHCP）情報を搬送します。

インターフェイス上で UDP ブロードキャスト パケットの転送をイネーブルにし、宛先アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip helper-address** *address*	転送をイネーブルにし、BOOTP などの UDP ブロードキャスト パケットを転送するための宛先アドレスを指定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルを指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** [*interface-id*] または **show running-config**	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定アドレスへのブロードキャスト パケットの転送をディセーブルにするには、**no ip helper-address** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

IP ブロードキャスト アドレスの確立

最も一般的な（デフォルトの）IP ブロードキャスト アドレスは、すべて 1 で構成されたアドレスです（255.255.255.255）。ただし、任意の形式の IP ブロードキャスト アドレスを生成するようにスイッチを設定することもできます。

インターフェイス上で IP ブロードキャスト アドレスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip broadcast-address** *ip-address*	デフォルト値と異なるブロードキャスト アドレス（128.1.255.255 など）を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show ip interface** [*interface-id*]	指定されたインターフェイスまたはすべてのインターフェイスのブロードキャスト アドレスを確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ブロードキャスト アドレスをデフォルトに戻すには、**no ip broadcast-address** インターフェイス コンフィギュレーション コマンドを使用します。

IP ブロードキャストのフラッディング

IP ブロードキャストをインターネットワーク全体に、制御可能な方法でフラッディングできるようにするには、ブリッジング STP で作成されたデータベースを使用します。この機能を使用すると、ループを回避することもできます。この機能を使用できるようにするには、フラッディングに関与するインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイスでは、ブロードキャストを受信できますが、受信したブロードキャストは転送できません。また同じルータのある別のインターフェイス上で受信されたブロードキャストが、そのインターフェイスを介して送信されることもありません。

IP ヘルパー アドレスのメカニズムを使用して単一のネットワーク アドレスに転送されるパケットはフラッディング可能です。各ネットワーク セグメントには、パケットのコピーが 1 つだけ送信されます。

フラッディングを行う場合、パケットは次の条件を満たす必要があります （これらの条件は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです）。

- MAC レベルのブロードキャストであること。
- IP レベルのブロードキャストであること。
- Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、Domain Name System（DNS; ドメイン ネーム システム）、Time、NetBIOS、ND、または BOOTP パケット、または **ip forward-protocol udp** グローバル コンフィギュレーション コマンドで指定された UDP であること。
- Time To Live（TTL）値が 2 以上であること。

フラッディングされた UDP データグラムには、出力インターフェイス上で **ip broadcast-address** インターフェイス コンフィギュレーション コマンドにより指定された宛先アドレスを設定します。宛先アドレスは、任意のアドレスに設定できるため、データグラムがネットワーク上を伝播していくのに伴って変更されることもあります。送信元アドレスは変更されません。TTL 値は 1 ずつ減少します。

フラッディングされた UDP データグラムがインターフェイスから送信されると（場合によっては宛先アドレスが変更される）、そのデータグラムは通常の IP 出力ルーチンに渡されます。そのため、出力インターフェイスにアクセス リストがある場合、データグラムはその影響を受けます。

ブリッジング スパニング ツリー データベースを使用して UDP データグラムをフラッディングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip forward-protocol spanning-tree**	ブリッジング スパニング ツリー データベースを使用し、UDP データグラムをフラッディングします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ブロードキャストのフラッディングをディセーブルにするには、**no ip forward-protocol spanning-tree** グローバル コンフィギュレーション コマンドを使用します。

スイッチでは、パケットの大部分がハードウェアで転送され、スイッチの CPU を経由しません。CPU に送信されるパケットの場合は、ターボ フラッディングを使用して、スパニング ツリー ベースの UDP フラッディングを約 4 ～ 5 倍高速化できます。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされています。

スパニング ツリー ベースのフラッディングを高速化させるには、特権 EXEC モードで次の手順を実行します

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip forward-protocol turbo-flood**	スパニング ツリー データベースを使用し、UDP データグラムのフラッディングを高速化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、**no ip forward-protocol turbo-flood** グローバル コンフィギュレーション コマンドを使用します。

IP アドレス指定のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になる、またはその可能性がある場合は、**clear** 特権 EXEC コマンドを使用して、すべての内容を消去できます。

表 36-2　キャッシュ、テーブル、およびデータベースを消去するためのコマンド

コマンド	目的
clear arp-cache	IP ARP キャッシュおよび高速スイッチング キャッシュを消去します。
clear host {*name* | *}}	ホスト名およびアドレス キャッシュから 1 つまたはすべてのエントリを削除します。
clear ip route {*network* [*mask*] |*}	IP ルーティング テーブルから 1 つまたは複数のルートを削除します。

IP ルーティング テーブル、キャッシュ、およびデータベースの内容（ノードへの到達可能性、ネットワーク内のパケットのルーティング経路など）のような特定の統計情報を表示できます。

表 36-3　キャッシュ、テーブル、およびデータベースを表示するためのコマンド

コマンド	目的
show arp	ARP テーブルのエントリを表示します。
show hosts	デフォルトのドメイン名、検索サービスの方式、サーバ ホスト名、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。
show ip aliases	TCP ポートにマッピングされた IP アドレスを表示します（エイリアス）。
show ip arp	IP ARP キャッシュを表示します。
show ip interface [*interface-id*]	インターフェイスの IP ステータスを表示します。

表 36-3　キャッシュ、テーブル、およびデータベースを表示するためのコマンド （続き）

コマンド	目的
show ip irdp	IRDP 値を表示します。
show ip masks *address*	ネットワーク アドレスに対して使用されるマスク、および各マスクを使用するサブネットの数を表示します。
show ip redirects	デフォルト ゲートウェイのアドレスを表示します。
show ip route [*address* [*mask*]]	[*protocol*]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	ルーティング テーブルの現在の状態をサマリー形式で表示します。

IPv4 ユニキャスト ルーティングのイネーブル化

デフォルトでは、スイッチはレイヤ 2 スイッチング モード、IP ルーティングはディセーブルになっています。スイッチのレイヤ 3 機能を使用するには、IP ルーティングをイネーブルにする必要があります。

IP ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします
ステップ 3	**router** *ip_routing_protocol*	IP ルーティング プロトコルを指定します。このステップでは、他のコマンドを実行することもできます。たとえば、**network**（RIP）ルータ コンフィギュレーション コマンドを使用して、ルーティングするネットワークを指定できます。具体的なプロトコルの詳細については、この章の後半および『*Cisco IOS IP Configuration Guide*』*Release 12.2* を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。

次に、ルーティング プロトコルとして RIP を使用した IP ルーティングをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end
```

この時点で、選択したルーティング プロトコルのパラメータを設定できます。手順については次の各セクションで説明します。

- 「RIP の設定」（P.36-20）
- 「OSPF の設定」（P.36-25）
- 「EIGRP の設定」（P.36-38）

- 「BGP の設定」（P.36-45）
- 「ISO CLNS ルーティングの設定」（P.36-67）
- 「OSFP に対する BFD の設定」（P.36-82）
- 「プロトコルに依存しない機能の設定」（P.36-101）（任意）

RIP の設定

RIP は、小規模な同種ネットワーク間で使用される Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）です。RIP は、ブロードキャスト UDP データ パケットを使用してルーティング情報を交換するディスタンスベクトル ルーティング プロトコルです。RIP の詳細については、『*IP Routing Fundamentals*』（Cisco Press 刊）を参照してください。

RIP を使用している場合、スイッチからはルーティング情報アップデート（アドバタイズメント）が 30 秒間隔で送信します。180 秒以上を経過しても別のルータからアップデートがルータに届かない場合、該当するルータから送られたルートは使用不能としてマークされます。240 秒が経過してもアップデートが届かない場合、アップデートを行わないルータに関するルーティング テーブル エントリはすべて削除されます。

RIP では、各ルートの値を評価するためにホップ カウントが使用されます。ホップ カウントは、ルート内で経由するルータ数です。直接接続されているネットワークのホップ カウントは 0 です。また、ホップ カウントが 16 のネットワークには到達できません。このように到達可能範囲（0 ～ 15）が狭いため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP では、ルータを疑似ネットワーク 0.0.0.0 にリンクするルートがアドバタイズされます。0.0.0.0 は、実在するネットワークではありませんが、RIP では、デフォルトのルーティング機能を実行するためのネットワークとして扱われます。デフォルト ネットワークが RIP によって学習された場合、またはルータが最終ゲートウェイで、RIP にデフォルト メトリックが設定されている場合、スイッチはデフォルト ネットワークをアドバタイズします。RIP では、指定されたネットワーク内のインターフェイスにアップデートが送信されます。インターフェイスのネットワークは、指定されていなければ、RIP アップデート中にアドバタイズされません。

ここでは、次の設定情報について説明します。

- 「RIP のデフォルト設定」（P.36-20）
- 「基本的な RIP パラメータの設定」（P.36-21）
- 「RIP 認証の設定」（P.36-23）
- 「スプリット ホライズンの設定」（P.36-23）

RIP のデフォルト設定

表 36-4　RIP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。
デフォルト情報の送信	ディセーブル。
デフォルト メトリック	自動メトリック変換（組み込み）。

表 36-4　RIP のデフォルト設定 （続き）

機能	デフォルト設定
IP RIP 認証キーチェーン	認証なし。 認証モード：クリア テキスト。
IP RIP 受信バージョン	**version** ルータ コンフィギュレーション コマンドに準拠。
IP RIP 送信バージョン	**version** ルータ コンフィギュレーション コマンドに準拠。
IP RIP のトリガー	**version** ルータ コンフィギュレーション コマンドに準拠。
IP スプリット ホライズン	メディアにより異なる。
Neighbor	定義なし。
ネットワーク	指定なし。
オフセット リスト	ディセーブル。
出力遅延	0 ミリ秒。
タイマー基準	• アップデート：30 秒。 • 無効：180 秒。 • ホールドダウン：180 秒。 • フラッシュ：240 秒。
アップデート送信元の検証	イネーブル。
バージョン	RIP バージョン 1 パケットおよびバージョン 2 パケットを受信し、バージョン 1 パケットを送信。

基本的な RIP パラメータの設定

RIP を設定する場合は、ネットワークに対して RIP ルーティングをイネーブルにします。他のパラメータを設定することもできます。Cisco ME 3400E スイッチに対して RIP コンフィギュレーション コマンドを有効にするには、ネットワーク番号を設定する必要があります。

RIP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします（IP ルーティングがディセーブルになっている場合に限り必須です）。
ステップ 3	**router rip**	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**network** *network number*	ネットワークを RIP ルーティング プロセスに関連付けます。複数の **network** コマンドを指定できます。RIP ルーティング アップデートの送受信を行うためには、これらのネットワークのインターフェイスを経由することが必要です。 **（注）** RIP コマンドを有効にするには、ネットワーク番号を設定する必要があります。
ステップ 5	**neighbor** *ip-address*	（任意）ルーティング情報を交換する隣接ルータを定義します。これにより、RIP（通常はブロードキャスト プロトコル）からのルーティング アップデートが非ブロードキャスト ネットワークに到達するようになります。

	コマンド	目的
ステップ 6	**offset list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*]	（任意）オフセット リストをルーティング メトリックに適用し、RIP を通じて学習したルートへの着信メトリックおよび発信メトリックを増やします。オフセット リストは、アクセス リストまたはインターフェイスを使用して制限できます。
ステップ 7	**timers basic** *update invalid holddown flush*	（任意）ルーティング プロトコル タイマーを調整します。すべてのタイマーの有効範囲は 0 ～ 4294967295 秒です。 • *update*：ルーティング アップデートの送信間隔を指定します。デフォルトは 30 秒です。 • *invalid*：ルートが無効と宣言されるまでの制限時間を指定します。デフォルトは 180 秒です。 • *holddown*：ルートがルーティング テーブルから削除されるまでの時間を指定します。デフォルトは 180 秒です。 • *flush*：ルーティング アップデートが延期される時間を指定します。デフォルトは 240 秒です。
ステップ 8	**version** {**1** | **2**}	（任意）RIP バージョン 1 または RIP バージョン 2 のパケットだけが送受信されるようにスイッチを設定します。デフォルトの場合、スイッチはバージョン 1 およびバージョン 2 を受信し、バージョン 1 だけを送信します。 インターフェイス上での送受信に使用されるバージョンを制御するには、インターフェイス コマンド **ip rip** {**send** | **receive**} **version 1** | **2** | **1 2**} を使用することもできます。
ステップ 9	**no auto summary**	（任意）自動サマライズをディセーブルにします。デフォルトでは、クラスフル ネットワーク境界を通過するときにサブプレフィクスがサマライズされます。サマライズをディセーブルにし（RIP バージョン 2 に限る）、クラスフル ネットワーク境界にサブネットおよびホストのルーティング情報をアドバタイズします。
ステップ 10	**no validate-update-source**	（任意）着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。デフォルトの場合、スイッチでは着信 RIP ルーティング アップデートの送信元 IP アドレスの検証が行われます。送信元アドレスが無効な場合、アップデートは廃棄されます。通常の環境で使用するときは、この機能をディセーブルにしないでください。ただし、ネットワークに接続されていないルータがあり、そのルータのアップデートを受信する場合は、このコマンドを使用できます。
ステップ 11	**output-delay** *delay*	（任意）送信する RIP アップデートのパケット間遅延を追加します。 デフォルトでは、複数のパケットからなる RIP アップデートにパケット間遅延は追加されません。パケットを低速なデバイスに送信する場合は、8 ～ 50 ミリ秒のパケット間遅延を追加できます。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip protocols**	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RIP ルーティング プロセスをオフにするには、**no router rip** グローバル コンフィギュレーション コマンドを使用します。

アクティブなルーティング プロトコル プロセスのパラメータと現在の状態を表示するには、**show ip protocols** 特権 EXEC コマンドを使用します。RIP データベースのサマリー アドレス エントリを表示するには、**show ip rip database** 特権 EXEC コマンドを使用します。

RIP 認証の設定

RIP バージョン 1 では、認証はサポートされていません。RIP バージョン 2 のパケットを送受信するには、インターフェイスで RIP 認証をイネーブルにできます。インターフェイスで使用できる一連の鍵は、キー チェーンによって決まります。キー チェーンが設定されていないと、デフォルトの場合でも認証は実行されません。そのため、「認証鍵の管理」（P.36-116）に記載されている作業も実行する必要があります。

スイッチでは、RIP 認証がイネーブルであるインターフェイスに対して、プレーン テキストと MD5 の 2 種類のモードでの認証がサポートされています。デフォルトはプレーン テキストです。

インターフェイスに RIP 認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip rip authentication key-chain** *name-of-chain*	RIP 認証をイネーブルにします。
ステップ 5	**ip rip authentication mode** [**text** | **md5**}	プレーン テキスト認証（デフォルト）または MD5 ダイジェスト認証を使用するようにインターフェイスを設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface** [*interface-id*]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

クリア テキスト認証に戻すには、**no ip rip authentication mode** インターフェイス コンフィギュレーション コマンドを使用します。認証を実行しない場合は、**no ip rip authentication key-chain** インターフェイス コンフィギュレーション コマンドを使用します。

スプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは通常、ルーティング ループの発生を回避するために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンを適用した場合、ルータでは、ルートに関する情報がその送信元インターフェイスからアドバタイズされなくなります。この機能を使用すると、リンクが壊れている場合に複数のルータ間通信が最適化されます。

（注） ルートが適切にアドバタイズされるようアプリケーションでスプリット ホライズンをディセーブルにすることが必要である場合を除いて、通常はこの機能をディセーブルにしないでください。

インターフェイスでスプリット ホライズンをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**no ip split-horizon**	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スプリット ホライズン メカニズムをイネーブルにするには、**ip split-horizon** インターフェイス コンフィギュレーション コマンドを使用します。

サマリー アドレスの設定

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカルな IP アドレス プールがアドバタイズされるように、RIP が実行されているインターフェイスを設定するには、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドを使用します。

（注）　スプリット ホライズンがイネーブルの場合、自動サマリー アドレスとインターフェイス IP サマリー アドレスはともにアドバタイズされません。

サマライズされたローカル IP アドレスをアドバタイズし、インターフェイスのスプリット ホライズンをディセーブルにするようにインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**ip summary-address rip** *ip address ip-network mask*	サマライズする IP アドレス、および IP ネットワーク マスクを設定します。
ステップ 6	**no ip split horizon**	インターフェイスでスプリット ホライズンをディセーブルにします。

	コマンド	目的
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** *interface-id*	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP サマライズをディセーブルにするには、**no ip summary-address rip** ルータ コンフィギュレーション コマンドを使用します。

次の例では、主要ネットは 10.0.0.0 です。自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイス ギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。インターフェイスがレイヤ 2 モード（デフォルト）の場合は、**no switchport** インターフェイス コンフィギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

（注）　スプリット ホライズンがイネーブルである場合、（**ip summary-address rip** ルータ コンフィギュレーション コマンドによって設定される）自動サマリー アドレスとインターフェイス サマリー アドレスはともにアドバタイズされません。

```
Switch(config)# router rip
Switch(config-router)# interface gi0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

OSPF の設定

OSPF は IP ネットワーク専用の IGP で、IP サブネット化、および外部から取得したルーティング情報のタグ付けをサポートしています。OSPF では、パケット認証も可能であり、パケットを送受信するときには IP マルチキャストが使用されます。

ここでは、OSPF の設定方法の概要を説明します。OSPF コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* の「OSPF Commands」を参照してください。

（注）　OSPF では、各メディアがブロードキャスト ネットワーク、Nonbroadcast Multiaccess（NBMA; 非ブロードキャスト マルチアクセス）ネットワーク、またはポイントツーポイント ネットワークに分類されます。ブロードキャスト ネットワークおよび非ブロードキャスト ネットワークは、ポイントツーマルチポイント ネットワークとしても設定できます。スイッチでは、これらすべてのネットワーク タイプがサポートされています。

シスコの実装機能は、OSPF バージョン 2 仕様に準拠しています。主な特徴は次のとおりです。

- スタブ エリアの定義がサポートされています。
- 任意の IP ルーティング プロトコルによって学習したルートは、別の IP ルーティング プロトコルに再配布できます。つまり OSPF では、ドメイン内レベルで、EIGRP および RIP によって学習したルートを取り込むことができます。OSPF ルートを RIP にエクスポートすることもできます。
- エリア内の隣接ルータ間におけるプレーン テキスト認証および MD5 認証がサポートされています。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータの dead インターバルおよび hello インターバル、認証鍵などがあります。
- 仮想リンクがサポートされています。
- RFC 1587 に基づく Not-So-Stubby-Area（NSSA）がサポートされています。

通常、OSPF を使用するためには、多くの内部ルータ、複数のエリアに接続された *Area Border Router*（ABR; エリア境界ルータ）、および *Autonomous System Boundary Router*（ASBR; 自律システム境界ルータ）の間で調整を行う必要があります。最低限の設定では、すべてのデフォルト パラメータ値、エリアに割り当てられたインターフェイスが使用され、認証は行われません。環境をカスタマイズする場合は、すべてのルータの設定を調整する必要があります。

ここでは、次の設定情報について説明します。

- 「OSPF のデフォルト設定」（P.36-27）
- 「NSF 認識」（P.36-28）
- 「OSPF インターフェイスの設定」（P.36-29）
- 「OSPF のネットワーク タイプの設定」（P.36-30）
- 「OSPF エリア パラメータの設定」（P.36-33）
- 「その他の OSPF パラメータの設定」（P.36-34）
- 「LSA グループ ペーシングの変更」（P.36-36）
- 「ループバック インターフェイスの設定」（P.36-36）
- 「OSPF のモニタリング」（P.36-37）

OSPF のデフォルト設定

表 36-5　　OSPF のデフォルト設定

機能	デフォルト設定
インターフェイス パラメータ	コスト：デフォルト コストは未定義。 再送信インターバル：5 秒。 送信遅延：1 秒。 プライオリティ：1。 hello インターバル：10 秒。 dead インターバル：hello インターバルの 4 倍。 認証なし。 パスワードの指定なし。 MD5 認証はディセーブル。
エリア	認証タイプ：0（認証なし）。 デフォルト コスト：1。 範囲：ディセーブル。 スタブ：スタブ エリアの定義なし。 NSSA：NSSA の定義なし。
自動コスト	100 Mbps。
デフォルト情報の送信	ディセーブル。イネーブルの場合、デフォルトのメトリック設定は 10 、デフォルトの外部ルート タイプはタイプ 2。
デフォルト メトリック	各ルーティング プロトコルに適した組み込みの自動メトリック変換。
距離 OSPF	dist1（エリア内部のすべてのルート）：110。 dist2（エリア間のすべてのルート）：110。 dist3（他のルーティング ドメインからのルート）：110。
OSPF データベース フィルタ	ディセーブル。すべての発信 LSA がインターフェイスにフラッディング。
IP OSPF 名検索	ディセーブル。
隣接関係変更ログ	イネーブル。
Neighbor	指定なし。
近接データベース フィルタ	ディセーブル。発信 LSA はすべてネイバーにフラッディング。
ネットワーク エリア	ディセーブル。
NSF[1] 認識	イネーブル[2]。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中、隣接する NSF 対応ルータからのパケットを転送し続けることが可能。
ルータ ID	OSPF ルーティング プロセスは未定義。
サマリー アドレス	ディセーブル。
タイマー LSA グループ ペーシング	240 秒。
タイマー Shortest Path First（SPF）	SPF 遅延：5 秒。 SPF ホールドタイム：10 秒。

表 36-5　OSPF のデフォルト設定 （続き）

機能	デフォルト設定
仮想リンク	エリア ID またはルータ ID は未定義 hello インターバル：10 秒。 再送信インターバル：5 秒。 送信遅延：1 秒。 dead インターバル：40 秒。 認証鍵：鍵は未定義。 メッセージダイジェスト鍵（MD5）：鍵は未定義。

1. NSF = Nonstop Forwarding（ノンストップ フォワーディング）
2. OSPF NSF 認識は、メトロ IP アクセス イメージを実行しているスイッチ上の IPv4 に対してイネーブルになっています。

NSF 認識

メトロ IP アクセス イメージの IPv4 に対しては、OSPF NSF 認識機能がサポートされています。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータ内で障害が発生したプライマリ Route Processor（RP; ルート プロセッサ）がバックアップ RP によって引き継がれる間、または処理を中断することなくソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからのパケットが転送され続けます。

この機能は、ディセーブルにできません。この機能の詳細については、次の URL にある『*OSPF Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

http://cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a0080153edd.shtml

基本的な OSPF パラメータの設定

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成して、そのルーティング プロセスに関連付ける IP アドレスの範囲を指定し、この範囲に関連付けるエリア ID を割り当てる必要があります。

OSPF をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID は、内部で使用するためにローカルに割り当てられる識別パラメータです。プロセス ID には、任意の正の整数を指定できます。各 OSPF ルーティング プロセスには一意の値が割り当てられます。
ステップ 3	**network** *address wildcard-mask* **area** *area-id*	OSPF が動作するインターフェイス、およびそのインターフェイスのエリア ID を定義します。wildcard-mask を指定すると、1 つのコマンドを使用するだけで、特定の OSPF エリアに関連付けるインターフェイスを 1 つまたは複数定義できます。エリア ID には 10 進数または IP アドレスを指定できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。

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

OSPF ルーティング プロセスを終了するには、**no router ospf** *process-id* グローバル コンフィギュレーション コマンドを使用します。

次に、OSPF ルーティング プロセスを設定し、それにプロセス番号 109 を割り当てる例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

OSPF インターフェイスの設定

ip ospf インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイス固有の OSPF パラメータを変更できます。これらのパラメータは変更する必要はありませんが、一部のインターフェイス パラメータ（hello インターバル、dead インターバル、認証鍵など）については、接続されたネットワーク内のすべてのルータで値を統一する必要があります。これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。

（注）　**ip ospf** インターフェイス コンフィギュレーション コマンドはすべて任意です。

OSPF インターフェイス パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip ospf** *cost*	（任意）インターフェイスでパケットを送信するコストを明示的に指定します。
ステップ 5	**ip ospf retransmit-interval** *seconds*	（任意）Link State Advertisement（LSA; リンク ステート アドバタイズメント）の送信間隔を秒単位で指定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 5 秒です。
ステップ 6	**ip ospf transmit-delay** *seconds*	（任意）リンク ステート アップデート パケットを送信するまでの予測待機時間を秒単位で設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 1 秒です。
ステップ 7	**ip ospf priority** *number*	（任意）ネットワークに対して、OSPF で指定されたルータを検索する際の手掛かりとなるプライオリティを設定します。指定できる範囲は 0 ～ 255 です。デフォルトは 1 です。
ステップ 8	**ip ospf hello-interval** *seconds*	（任意）OSPF インターフェイスにおける hello パケットの送信間隔を秒単位で設定します。この値は、ネットワークのすべてのノードで同じであることが必要です。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。

	コマンド	目的
ステップ 9	**ip ospf dead-interval** *seconds*	（任意）最後のデバイスの hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間を秒単位で設定します。この値は、ネットワークのすべてのノードで同じであることが必要です。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は hello インターバルの 4 倍です。
ステップ 10	**ip ospf authentication-key** *key*	（任意）隣接 OSPF ルータで使用されるパスワードを割り当てます。パスワードには、キーボードから入力した任意の文字列（最大 8 バイト長）を指定できます。同じネットワーク上のすべての隣接ルータには、OSPF 情報を交換できるように、同じパスワードを設定する必要があります。
ステップ 11	**ip ospf message digest-key** *keyid* **md5** *key*	（任意）MDS 認証をイネーブルにします。 • *keyid* : ID を 1 ～ 255 の範囲で指定します。 • *key* : 英数字パスワードを指定します（最大 16 バイト）。
ステップ 12	**ip ospf database-filter all out**	（任意）インターフェイスへの OSPF LSA パケットのフラッディングを阻止します。デフォルトの場合、OSPF では、LSA が到達するインターフェイスを除く、同じエリア内のすべてのインターフェイスに新しい LSA がフラッディングされます。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show ip ospf interface** [*interface-name*]	OSPF に関連するインターフェイス情報を表示します。
ステップ 15	**show ip ospf neighbor detail**	近接スイッチの NSF 認識ステータスを表示します。出力は、次のいずれかに一致します。 • *Options is 0x52* *LLS Options is 0x1 (LR)* この 2 つの行が表示されれば、近接スイッチは NSF 認識です。 • *Options is 0x42* : 近接スイッチが NSF 認識でないことを表します。
ステップ 16	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定されたパラメータ値を削除する場合、またはデフォルト値に戻すには、上記コマンドの **no** 形式を使用します。

OSPF のネットワーク タイプの設定

OSPF では、デフォルトで各メディアが次の 3 タイプのネットワークに分類されます。

- ブロードキャスト ネットワーク（イーサネット、トークン リング、および FDDI）
- NBMA ネットワーク（Switched Multimegabit Data Service [SMDS; スイッチド マルチメガビット データ サービス]、フレーム リレー、および X.25）
- ポイントツーポイント ネットワーク（High-Level Data Link Control [HDLC; ハイレベル データリンク制御]、PPP [ポイントツーポイント プロトコル]）

また、ネットワーク インターフェイスは、デフォルトのメディア タイプに関係なく、ブロードキャスト ネットワークまたは NBMA ネットワークのいずれかに設定できるほか、ポイントツーポイントまたはポイントツーマルチポイントのいずれかに設定することもできます。

非ブロードキャスト ネットワークに対する OSPF の設定

OSPF ネットワークには多数のルータが付加される可能性があるため、ネットワークに対して代表ルータを選択します。ネットワーク内でブロードキャスト機能が設定されていない場合に、代表ルータを選択するには、特別なコンフィギュレーション パラメータが必要となります。これらのパラメータを設定する必要があるのは、代表ルータまたはバックアップの代表ルータになることが許可されている（つまりルータ プライオリティ値が 0 でない）デバイスに対してだけです。

非ブロードキャスト ネットワークと相互接続するルータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	必要に応じて、ネイバー パラメータにより OSPF ネイバーを指定します。 • *ip-address*：OSPF ネイバーのインターフェイス IP アドレスを入力します。 • （任意）**priority** *number*：IP アドレスに関連付けられた非ブロードキャスト ネイバーのルータ プライオリティ値を指定します。指定できる範囲は 0 ～ 255 で、デフォルト値は 0 です。 • （任意）**poll-interval** *seconds*：ポーリング インターバル（秒単位）を表す数値を指定します。ただし、hello インターバルに比べて十分大きな値を指定することを推奨します。指定できる範囲は 0 ～ 4294967295 で、デフォルトは 120 秒（2 分）です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip ospf** [*process-id*]	OSPF に関連する情報を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポイントツーマルチポイントの非ブロードキャスト ネットワークでは、さらに **neighbor** ルータ コンフィギュレーション コマンドを使用してネイバーを指定します。ネイバーにコストを割り当てるかどうかは任意です。

OSPF インターフェイスに対するネットワーク タイプの設定

ネットワーク インターフェイスは、デフォルトのメディア タイプに関係なく、ブロードキャストまたは NBMA のいずれかに設定できるほか、ポイントツーポイントまたはポイントツーマルチポイントのいずれかに設定することもできます。

OSPF ポイントツーマルチポイント インターフェイスは、1 つまたは複数のネイバーを持つ番号付けされたポイントツーポイント インターフェイスとして定義されます。ポイントツーマルチポイント ブロードキャスト ネットワークでは、ネイバーを指定するかどうかは任意です。メディアがブロードキャストをサポートしていない場合にインターフェイスをポイントツーマルチポイントとして設定するには、**neighbor** コマンドを使用してネイバーを指定する必要があります。

インターフェイスに OSPF ネットワーク タイプを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip ospf network** {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}	指定されたインターフェイスに対する OSPF ネットワーク タイプを設定します。次のいずれかのネットワーク タイプを選択します。 • **broadcast**：OSPF ブロードキャスト マルチアクセス ネットワークを指定します。 • **non-broadcast**：OSPF NBMA ネットワークを指定します。 • **point-to-multipoint**：OSPF ポイントツーマルチポイント ネットワークを指定します。別のキーワードを入力しない場合、インターフェイスはブロードキャスト メディアでポイントツーマルチポイントとなります。 • **point-to-multipoint non-broadcast**：OSPF 非ブロードキャスト ポイントツーマルチポイント ネットワークを指定します。 • **point-to-point**：OSPF ポイントツーポイント ネットワークを指定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**router ospf** *process-id*	（ポイントツーマルチポイントの場合は任意、ポイントツーマルチポイント非ブロードキャストの場合は必須）OSPF ルーティング プロセスを設定して、ルータ コンフィギュレーション モードを開始します。
ステップ 7	**neighbor** *ip-address* **cost** *number*	（ポイントツーマルチポイントの場合は任意、ポイントツーマルチポイント非ブロードキャストの場合は必須）設定済みの OSPF ネイバーを指定し、そのネイバーにコストを割り当てます。 • *ip-address*：OSPF ネイバーのインターフェイス IP アドレスを入力します。 • **cost** *number*：ネイバーのコストを 1 ～ 65535 の整数で指定します。 **（注）** ポイントツーマルチポイント ブロードキャスト ネットワークでは、ネイバーを指定するかどうかは任意ですが、ネイバーを指定する場合は、必ずネイバーにコストを指定する必要があります。 ポイントツーマルチポイント非ブロードキャスト ネットワークでは、ネイバーを指定する必要がありますが、ネイバーにコストを割り当てるかどうかは任意です。割り当てない場合は、**ip ospf cost** インターフェイス コンフィギュレーション コマンドに基づいてインターフェイスのコストがネイバーのコストと見なされます。
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**show ip ospf interface** [*interface-id*]	OSPF に関連するインターフェイス情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

メディアのネットワーク タイプをデフォルトに戻すには、**ip ospf network** コマンドの **no** 形式を使用します。

OSPF エリア パラメータの設定

OSPF エリア パラメータは、必要に応じて複数設定することもできます。設定できるパラメータには、エリア、スタブ エリア、および NSSA への不正アクセスをパスワードによって阻止する認証用パラメータも含まれます。*スタブ エリア*は、外部ルートに関する情報が送信されないエリアです。ただし、Autonomous System（AS; 自律システム）外の宛先に対しては、エリア境界ルータ（ABR）によってスタブ エリアへのデフォルトの外部ルートが生成されます。NSSA では、コアからそのエリアへ向かう LSA がすべてフラッディングされるわけではありませんが、再配布すればエリア内の AS 外部ルートをインポートできます。

経路集約とは、アドバタイズされたアドレスを、他のエリアでアドバタイズされる単一のサマリー ルートに統合することです。ネットワーク番号が連続する場合は、**area range** ルータ コンフィギュレーション コマンドを使用して、範囲内のすべてのネットワークを対象とするサマリー ルートをアドバタイズするように ABR を設定できます。

（注）　OSPF の **area** ルータ コンフィギュレーション コマンドはすべて任意です。

エリア パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**area** *area-id* **authentication**	（任意）指定したエリアに対して、パスワードによる不正アクセスの防止機能を有効にします。ID には 10 進数または IP アドレスのいずれかを指定できます。
ステップ 4	**area** *area-id* **authentication message-digest**	（任意）エリアに対して MD5 認証をイネーブルにします。
ステップ 5	**area** *area-id* **stub** [**no-summary**]	（任意）エリアをスタブ エリアとして定義します。**no-summary** キーワードを指定すると、ABR はサマリー リンク アドバタイズメントをスタブ エリアに送信できなくなります。

	コマンド	目的
ステップ 6	**area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**]	（任意）エリアを NSSA として定義します。同じエリア内の各ルータは、エリアが NSSA であることを認識する必要があります。次のキーワードのいずれかを選択します。 • **no-redistribution**：ルータが NSSA ABR であり、かつ **redistribute** コマンドを使用してルートを（NSSA ではなく）通常のエリアへインポートする場合に選択します。 • **default-information-originate**：NSSA にタイプ 7 LSA をインポートできるようにする場合に ABR で選択します。 • **no-redistribution**：サマリー LSA を NSSA に送信しない場合に選択します。
ステップ 7	**area** *area-id* **range** *address mask*	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip ospf** [*process-id*]	設定を確認するため、一般的な OSPF ルーティング プロセスまたは特定のプロセス ID に関する情報を表示します。
	show ip ospf [*process-id* [*area-id*]] **database**	特定のルータの OSPF データベースに関連する情報のリストを表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定されたパラメータ値を削除する場合、またはデフォルト値に戻すには、上記コマンドの **no** 形式を使用します。

その他の OSPF パラメータの設定

ルータ コンフィギュレーション モードで、その他の OSPF パラメータを設定することもできます。

- 経路集約：他のプロトコルからのルートを再配布すると（「ルート マップによるルーティング情報の再配布」（P.36-105）を参照）、各ルートは外部 LSA 内で個別にアドバタイズされます。OSPF リンク ステート データベースのサイズを小さくするには、**summary-address** ルータ コンフィギュレーション コマンドを使用して、指定されたネットワーク アドレスおよびマスクに含まれる、再配布されたすべてのルートを単一のルータにアドバタイズします。
- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続である場合に仮想リンクを確立するには、2 つの ABR を仮想リンクのエンドポイントとして設定します。設定情報には、他の仮想エンドポイント（他の ABR）の ID や、2 つのルータに共通する非バックボーン リンク（通過エリア）などが含まれます。仮想リンクは、スタブ エリアを介しては設定できません。
- デフォルト ルート：OSPF ルーティング ドメイン内へのルート再配布を設定すると、ルータは自動的に ASBR になります。ASBR は、OSPF ルーティング ドメインへのデフォルト ルートが強制的に生成されるよう設定できます。
- すべての OSPF **show** 特権 EXEC コマンドで使用される Domain Name Server（DNS; ドメイン ネーム サーバ）名を使用すると、ルータ ID やネイバー ID を指定して表示する場合に比べ、ルータを簡単に特定できます。

- デフォルト メトリック：OSPF では、インターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックが計算されます。メトリックは、帯域幅で分割された *ref-bw* として計算されます。ただし、*ref* のデフォルト値は 10 、帯域幅（*bw*）は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。大きな帯域幅を持つ複数のリンクの場合は、大きな数値を指定すると、これらのリンクのコストを区別できます。
- 管理ディスタンスは、ルーティング情報送信元の信頼性を表す数値です。0 ～ 255 の整数を指定でき、値が大きいほど信頼性は低下します。管理ディスタンスが 255 の場合は、ルーティング情報送信元をまったく信頼できないため、その値は無視してください。OSPF では、エリア内のルート（エリア内）、別のエリアへのルート（エリア間）、および再配布によって学習した別のルーティング ドメインからのルート（外部）という 3 種類の管理ディスタンスが使用されます。これらいずれの管理ディスタンスも値を変更できます。
- 受動インターフェイス：イーサネット上の 2 つのデバイス間に位置するインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信側インターフェイスに hello パケットを送信しないようにするには、送信側デバイスを受動インターフェイスに設定する必要があります。この 2 つのデバイスは、受信側インターフェイス宛の hello パケットを介して、相互を認識します。
- ルート計算タイマー：OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールド タイムを設定できます。
- 隣接関係変更ログ：OSPF 近接状態が変更されたときに Syslog メッセージを送信するようにルータを設定し、ルータの変更を詳細に表示できます。

これらの OSPF パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**summary-address** *address mask*	（任意）1 つのサマリー ルートだけがアドバタイズされるように、再配布されたルートのアドレスおよび IP サブネット マスクを指定します。
ステップ 4	**area** *area-id* **virtual-link** router-id [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**trans**] [[**authentication-key** *key*] | **message-digest-key** *keyid* **md5** *key*]]	（任意）仮想リンクを確立し、そのパラメータを設定します。パラメータ定義については「OSPF インターフェイスの設定」（P.36-29）、仮想リンクのデフォルト設定については表 36-5（P.36-27）を参照してください。
ステップ 5	**default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]	（任意）OSPF ルーティング ドメインへのデフォルト ルートが強制的に生成されるよう ASBR を設定します。パラメータはすべて任意です。
ステップ 6	ip ospf name-lookup	（任意）DNS 名検索を設定します。デフォルトはディセーブルです。
ステップ 7	**ip auto-cost reference-bandwidth** *ref-bw*	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	**distance ospf** {[**inter-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}	（任意）OSPF 距離の値を変更します。各ルート タイプに対するデフォルトの距離は 110 です。指定できる範囲は 1 ～ 255 です。
ステップ 9	**passive-interface** *type number*	（任意）指定されたインターフェイスからの hello パケットの送信を抑制します。

	コマンド	目的
ステップ 10	**timers throttle spf** *spf-delay spf-holdtime spf-wait*	（任意）ルート計算タイマーを設定します。 • *spf-delay*：SPF 計算の変更を受信する間の遅延を指定します。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-holdtime*：最初と 2 番めの SPF 計算の間の遅延を指定します。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-wait*：SPF 計算の最大待機時間をミリ秒単位で指定します。指定できる範囲は 1 ～ 600000 ミリ秒です。
ステップ 11	**ospf log-adj-changes**	（任意）近接状態の変更時に Syslog メッセージを送信します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip ospf** [*process-id* [*area-id*]] **database**	特定のルータの OSPF データベースに関連する情報のリストを表示します。キーワード オプションの一部については、「OSPF のモニタリング」（P.36-37）を参照してください。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

LSA グループ ペーシングの変更

OSPF LSA グループ ペーシング機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、エージング機能の同期を取って、ルータをより効率的に使用することが可能となります。デフォルトでこの機能はイネーブルとなっています。デフォルトのペーシング インターバルは 4 分間です。通常、このパラメータを変更する必要はありません。最適なグループ ペーシング インターバルは、ルータがリフレッシュ、チェックサム、およびエージングを行う LSA 数に反比例します。たとえば、データベース内に約 10000 個の LSA が格納されている場合は、ペーシング インターバルを短くすると便利です。小さなデータベース（40 ～ 100 LSA）を使用する場合は、ペーシング インターバルを 10 ～ 20 分と長めに設定してください。

OSPF LSA ペーシングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id*	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**timers lsa-group-pacing** *seconds*	LSA のグループ ペーシングを変更します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト値に戻すには、**no timers lsa-group-pacing** ルータ コンフィギュレーション コマンドを使用します。

ループバック インターフェイスの設定

OSPF では、インターフェイス上に設定されている中で最大の IP アドレスが、ルータ ID として使用されます。このインターフェイスがダウンした場合または削除された場合は、OSPF プロセスによって新しいルータ ID が再計算され、そのインターフェイスからすべてのルーティング情報が再送信されま

す。ループバック インターフェイスに IP アドレスが設定されている場合、他のインターフェイスにより大きな IP アドレスがある場合でも、OSPF ではこの IP アドレスがルータ ID として使用されます。ループバック インターフェイスには障害が発生しないため、ループバック インターフェイスを使用することで安定性は増大します。OSPF では、ループバック インターフェイスが他のインターフェイスよりも自動的に優先され、すべてのループバック インターフェイスの中で最大の IP アドレスが選択されます。

ループバック インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface loopback 0**	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** *address mask*	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ループバック インターフェイスをディセーブルにするには、**no interface loopback 0** グローバル コンフィギュレーション コマンドを使用します。

OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

表 36-6 は、統計情報を表示するために使用する特権 EXEC コマンドの一部を示したものです。**show ip ospf database** 特権 EXEC コマンドのオプションおよび表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* を参照してください。

表 36-6　IP OSPF 統計情報の表示コマンド

コマンド	目的
show ip ospf [*process-id*]	OSPF ルーティング プロセスに関する一般的な情報を表示します。
show ip ospf [*process-id*] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id*] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id*] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**database-summary**]	OSPF データベースに関連する情報を表示します。
show ip ospf border-routes	内部 OSPF ルーティングの ABR テーブル エントリおよび ASBR テーブル エントリを表示します。
show ip ospf interface [*interface-name*]	OSPF に関連するインターフェイス情報を表示します。

表 36-6　IP OSPF 統計情報の表示コマンド

コマンド	目的
show ip ospf neighbor [*interface-name*] [*neighbor-id*] **detail**	OSPF インターフェイスのネイバー情報を表示します。
show ip ospf virtual-links	OSPF に関連する仮想リンク情報を表示します。

EIGRP の設定

EIGRP は IGRP のシスコ独自の拡張バージョンです。EIGRP は、使用されるディスタンス ベクトル アルゴリズムおよび距離情報は IGRP と同じですが、コンバージェンス特性および動作効率が大幅に改善されています。

コンバージェンス技術には、Diffusing Update Algorithm（DUAL; Diffusing アップデート アルゴリズム）と呼ばれるアルゴリズムが採用されています。DUAL を使用すると、ルート計算の各段階でループが発生しなくなり、トポロジの変更に関連するすべてのデバイスを同時に同期できます。トポロジ変更の影響を受けないルータは、再計算から除外されます。

IP EIGRP を導入すると、ネットワークの幅が広がります。RIP の場合、ネットワークの最大幅は 15 ホップです。EIGRP メトリックは数千ホップをサポートするほど大きいため、ネットワークを拡張するときに問題となるのは、トランスポート レイヤのホップ カウンタだけです。EIGRP において転送制御フィールドの値が増加するのは、IP パケットが 15 台のルータを経由し、宛先方向のネクストホップが EIGRP によって学習されている場合に限ります。

EIGRP には次に示す 4 つの基本コンポーネントがあります。

- *近隣探索および回復*：直接接続されたネットワーク上の他のルータに関する情報をダイナミックに学習するために、ルータで使用されるプロセスです。ネイバーが到達不能になる場合、または動作不能になった場合、ルータもこの情報を検出する必要があります。近隣探索および回復は、サイズの小さな hello パケットを定期的に送信することにより実現されます。ネイバーは、hello パケットを受信している限り、動作していると判断されます。動作していると判断されると、隣接ルータはルーティング情報を交換します。
- *信頼できるトランスポート プロトコル*：EIGRP パケットがすべてのネイバーに順序どおり、確実に配信されます。マルチキャスト パケットおよびユニキャスト パケットが混在する送信もサポートされます。EIGRP パケットには確実に送信する必要があるものと、そうでないものがあります。効率を高めるために、必要な場合だけ信頼性が確保されます。たとえば、マルチキャスト機能があるマルチアクセス ネットワークでは、すべてのネイバーそれぞれに対して hello パケットを確実に送信する必要はありません。そのため EIGRP では、マルチキャスト hello を送信する際には、確認応答が不要であることを受信者に知らせるための情報がそのパケット内に格納されます。他のタイプのパケット（アップデートなど）の場合は、確認応答（ACK パケット）が要求されます。コンバージェンス時間を短縮するため、確認応答のない保留中パケットがある場合には、信頼性の高い転送によってマルチキャスト パケットが迅速に送信されます。
- *DUAL 有限状態マシン*：すべてのルート計算に関する決定プロセスが処理されます。DUAL 有限状態マシンでは、すべてのネイバーによりアドバタイズされた全ルートが追跡され、距離情報（メトリック）に基づいて、ループのない効率的なパスが選択されます。さらに DUAL は適切な後継ルータに基づいて、ルーティング テーブルに挿入するルートを選択します。後継ルータは、宛先への最小コスト パスを持った（ルーティング ループに含まれないことが保証されている）、パケット転送用の隣接ルータです。

  適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は、再計算を行って新たな後継ルータを決定する必要があります。ルートの再計算に要する時間によって、コンバージェンス時間は変わります。トポロジが変更された場合、DUAL では、不要な再計算を省略するために、適切な後継ルータが存在するかどうかのテストが行われます。

- *プロトコル依存モジュール*：ネットワーク レイヤ プロトコル固有の作業を行います。たとえば、IP でカプセル化された EIGRP パケットの送受信を行う IP EIGRP モジュールは、プロトコル依存モジュールの 1 つです。このモジュールは、EIGRP パケットを解析し、受信した新しい情報を DUAL に通知する作業を行います。ルーティングの決定結果は IP ルーティング テーブルに格納されます。また EIGRP では、他の IP ルーティング プロトコルにより学習されたルートが再配布されます。

ここでは、次の設定情報について説明します。

- 「EIGRP のデフォルト設定」（P.36-39）
- 「基本的な EIGRP パラメータの設定」（P.36-40）
- 「EIGRP インターフェイスの設定」（P.36-41）
- 「EIGRP ルート認証の設定」（P.36-42）
- 「EIGRP スタブ ルーティングの設定」（P.36-43）
- 「EIGRP のモニタリングおよびメンテナンス」（P.36-45）

EIGRP のデフォルト設定

表 36-7、パート 1 EIGRP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。クラスフル ネットワーク境界を通過するとき、この境界にサブプレフィクスが集約される。
デフォルト情報	再配布中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報の受け渡しが行われる。
デフォルト メトリック	デフォルト メトリックなしで再配布できるのは、接続されたルートおよびインターフェイスのスタティック ルートに限る。デフォルト メトリックは次のとおり。 • 帯域幅：0 kbps 以上。 • 遅延（10 マイクロ秒単位）：0 または 39.1 ナノ秒の倍数である任意の正数。 • 信頼性：0 ～ 255 の任意の数値（255 の場合は信頼性が 100%）。 • 負荷：0 ～ 255 の数値で表される有効帯域幅（255 の場合は 100% の負荷）。 • MTU：バイトで表されたルートの MTU サイズ （0 または任意の正の整数）。
距離	内部距離：90。 外部距離：170。
EIGRP の隣接関係変更ログ	ディセーブル。隣接関係変更はロギングされない。
IP 認証キーチェーン	認証なし。
IP 認証モード	認証なし。
IP 帯域幅比率	50%。
IP hello インターバル	低速 NBMA ネットワーク：60 秒。それ以外のネットワーク：5 秒。
IP ホールド タイム	低速 NBMA ネットワーク：180 秒。それ以外のネットワーク：15 秒。
IP スプリット ホライズン	イネーブル。
IP サマリー アドレス	サマリー集約アドレスは未定義。
メトリックの重み	tos：0、k1 および k3：1、k2、k4、および k5：0。

表 36-7、パート 1 EIGRP のデフォルト設定 （続き）

機能	デフォルト設定
ネットワーク	指定なし。
NSF[1] 認識	イネーブル[2]。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中、隣接する NSF 対応ルータからのパケットを転送し続けることが可能。
オフセットリスト	ディセーブル。
ルータ EIGRP	ディセーブル。
メトリック設定	ルート マップにはメトリック設定なし。
トラフィック共有	メトリックの比率に応じて配分。
分散	1（等価コスト ロード バランシング）。

1. NSF = Nonstop Forwarding（ノンストップ フォワーディング）
2. EIGRP NSF 認識は、メトロ IP アクセス イメージを実行しているスイッチ上の IPv4 に対してイネーブルになっています。

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにし、ネットワークを関連付ける必要があります。EIGRP では、指定されたネットワーク内のインターフェイスにアップデートが送信されます。インターフェイス ネットワークを指定しない場合は、どの EIGRP アップデートでもアドバタイズされません。

NSF 認識

メトロ IP アクセス イメージの IPv4 に対しては、EIGRP NSF 認識機能がサポートされています。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータ内で障害が発生したプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断することなくソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからのパケットが転送され続けます。

この機能は、ディセーブルにできません。この機能に関する詳細については、次の URL にある『*EIGRP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080160010.html

基本的な EIGRP パラメータの設定

EIGRP を設定するには、特権 EXEC モードで次の手順を実行します。ルーティング プロセスの設定は必須ですが、それ以外のステップは任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *autonomous-system*	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号は、他の EIGRP ルータへのルートを識別するためのもので、ルーティング情報のタグ付けに使用されます。
ステップ 3	**network** *network-number*	ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP では、指定されたネットワーク内のインターフェイスにアップデートが送信されます。

	コマンド	目的
ステップ 4	**eigrp log-neighbor-changes**	（任意）EIGRP 隣接関係変更のロギングをイネーブルにし、ルーティング システムの安定性をモニタします。
ステップ 5	**metric weights** *tos k1 k2 k3 k4 k5*	（任意）EIGRP メトリックを調整します。デフォルト値は、多くのネットワークが適切に動作するよう配慮して設定されていますが、必要であれば調整することも可能です。 **注意**　メトリックの設定は複雑な作業です。メトリックの設定は熟練したネットワーク設計者の指導のもとで行ってください。
ステップ 6	**offset list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*]	（任意）オフセット リストをルーティング メトリックに適用し、EIGRP によって学習したルートへの着信メトリックおよび発信メトリックの値を増やします。オフセット リストは、アクセス リストまたはインターフェイスを使用して制限できます。
ステップ 7	**no auto-summary**	（任意）ネットワーク レベル ルートへのサブネット ルートの自動サマライズをディセーブルにします。
ステップ 8	**ip summary-address eigrp** *autonomous-system-number address mask*	（任意）サマリー集約を設定します。
ステップ 9	**end**	特権 EXEC モードに戻ります。

ステップ 10	**show ip protocols**	設定を確認します。
		NSF 認識の場合、出力には次のように表示されます。
		`*** IP Routing is NSF aware ***`
		`EIGRP NSF enabled`

ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、または設定をデフォルト値に戻すには、上記コマンドの **no** 形式を使用します。

EIGRP インターフェイスの設定

他の任意の EIGRP パラメータは、インターフェイスごとに設定できます。

EIGRP インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip bandwidth-percent eigrp** *percent*	（任意）インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。デフォルト値は 50% です。

	コマンド	目的
ステップ 5	**ip summary-address eigrp** *autonomous-system-number address mask*	（任意）指定されたインターフェイスのサマリー集約アドレスを設定します（auto-summary がイネーブルの場合は、通常設定する必要はありません）。
ステップ 6	**ip hello-interval eigrp** *autonomous-system-number seconds*	（任意）EIGRP ルーティング プロセスの hello タイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは、低速 NBMA ネットワークでは 60 秒、その他すべてのネットワークでは 5 秒です。
ステップ 7	**ip hold-time eigrp** *autonomous-system-number seconds*	（任意）EIGRP ルーティング プロセスのホールド タイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは、低速 NBMA ネットワークでは 180 秒、その他すべてのネットワークでは 15 秒です。 **注意** ホールド タイムを調整する場合は、事前にシスコのテクニカル サポートにお問い合せください。
ステップ 8	**no ip split-horizon eigrp** *autonomous-system-number*	（任意）スプリット ホライズンをディセーブルにし、ルート情報がその送信元インターフェイスからルータによってアドバタイズされるようにします。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show ip eigrp interface**	EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、または設定をデフォルト値に戻すには、上記コマンドの **no** 形式を使用します。

EIGRP ルート認証の設定

EIGRP ルート認証を設定すると、EIGRP ルーティング プロトコルからのルーティング アップデートに対して MD5 認証が実行されます。これにより、承認されていない送信元からの不正なルーティング メッセージや問題のあるルーティング メッセージの受信を回避できます。

認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**ip authentication mode eigrp** *autonomous-system* **md5**	IP EIGRP パケットの MD5 認証をイネーブルにします。
ステップ 5	**ip authentication key-chain eigrp** *autonomous-system key-chain*	IP EIGRP パケットの認証をイネーブルにします。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**key chain** *name-of-chain*	キーチェーンを指定し、キーチェーン コンフィギュレーション モードを開始します。ステップ 4 で設定したものと同じ名前を指定します。
ステップ 8	**key** *number*	キーチェーン コンフィギュレーション モードで、鍵番号を指定します。
ステップ 9	**key-string** *text*	キーチェーン コンフィギュレーション モードで、キーストリングを指定します。
ステップ 10	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）鍵を受信できる期間を指定します。 *start-time* および *end-time* の構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無期限です。指定できる最初の日付は 1993 年 1 月 1 日です。*end-time* および **duration** のデフォルトは **infinite** です。
ステップ 11	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）鍵を送信できる期間を指定します。 *start-time* および *end-time* の構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無期限です。指定できる最初の日付は 1993 年 1 月 1 日です。*end-time* および **duration** のデフォルトは **infinite** です。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show key chain**	認証鍵情報を表示します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにする場合、または設定をデフォルト値に戻すには、上記コマンドの **no** 形式を使用します。

EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティング機能を使用すると、ルーテッド トラフィックをエンド ユーザの近くへ移動することで、リソースの使用量を軽減できます。EIGRP スタブ ルーティングを使用するネットワークでは、ユーザへの IP トラフィックに対して許可されたルートだけが、EIGRP スタブ ルーティングが設定されたスイッチを通過できます。スイッチでは、ユーザのインターフェイスとして設定された、または他のデバイスに接続されたインターフェイスへ、ルーテッド トラフィックが送信されます。

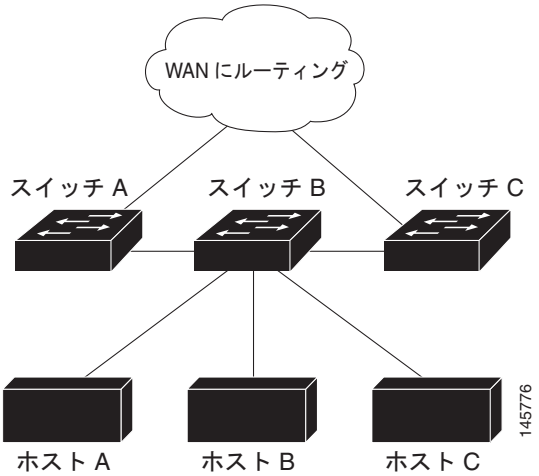
EIGRP スタブ ルーティングを使用する場合は、EIGRP が使用されるように配信ルータおよびリモート ルータを設定し、スイッチだけをスタブとして設定する必要があります。スイッチからは、指定したルートだけが伝播されます。スイッチは、サマリー、接続されたルート、およびルーティング アップデートに関するすべてのクエリーに応答します。

（注）　EIGRP タブ ルーティングでは、接続されたルートまたはサマリー ルートに限り、ルーティング テーブルからネットワーク内の別のスイッチへアドバタイズされます。スイッチでは、アクセス レイヤでの EIGRP スタブ ルーティングにより、その他のタイプのルーティング アドバタイズメントが不要になります。マルチ VRF-CE と EIGRP スタブ ルーティングは、同時には設定できません。

スタブ ステータスを知らせるパケットを受信したネイバーは、スタブ ルータに対してルートに関するクエリーを送信しません。また、スタブ ピアを持つルータが、そのピアに対してクエリーを送信することもありません。スタブ ルータからすべてのピアへ適切なアップデートが送信される場合、その処理は配信ルータが行います。

図 36-4 では、スイッチ B が EIGRP スタブ ルータとして設定されています。スイッチ A およびスイッチ C は、外部の WAN に接続されています。スイッチ B からは、接続されたスタティック ルート、再配布ルート、およびサマリー ルートがスイッチ A およびスイッチ C へアドバタイズされます。スイッチ B では、スイッチ A から学習したルートはアドバタイズされません（同様にスイッチ A でも、スイッチ B から学習されたルートはアドバタイズされません）。

図 36-4　　EIGRP スタブ ルータの設定



EIGRP スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols*』*Release 12.2*（Cisco.com ページから [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] を選択）の「Configuring EIGRP Stub Routing」を参照してください。

EIGRP スタブ ルーティング用のリモート ルータまたはスポーク ルータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp 1**	EIGRP プロセスが実行されるようにリモート ルータまたは配信ルータを設定し、ルータ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**network** *network-number*	ネットワークを EIGRP ルーティング プロセスに関連付けます。
ステップ 4	**eigrp stub** [**receive-only** | **connected** | **static** | **summary**]	リモート ルータを EIGRP スタブ ルータとして設定します。キーワードの意味は次のとおりです。 • **receive-only**：ルータを受信専用ネイバーとして設定する場合に入力します。 • **connected**：接続されたルートをアドバタイズする場合に入力します。 • **static**：スタティック ルートをアドバタイズする場合に入力します。 • **summary**：サマリー ルートをアドバタイズする場合に入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip eigrp neighbor detail**	リモート ルータが EIGRP スタブ ルータとして設定されたことを確認します。出力の最後の行には、リモート ルータまたはスポーク ルータのスタブ ステータスが表示されます。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定を確認するには、配信ルータから **show ip eigrp neighbor detail** 特権 EXEC コマンドを入力します。

EIGRP のモニタリングおよびメンテナンス

ネイバー テーブルからネイバーを削除できます。また、EIGRP ルーティングに関するさまざまな統計情報を表示できます。表 36-8 は、ネイバーの削除および統計情報の表示に使用できる特権 EXEC コマンドをまとめたものです。表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* を参照してください。

表 36-8　IP EIGRP の clear コマンドおよび show コマンド

コマンド	目的
clear ip eigrp neighbors [*if-address* | *interface*]	ネイバー テーブルからネイバーを削除します。
show ip eigrp interface [*interface*] [*as number*]	EIGRP 用に設定されたインターフェイスの情報を表示します。
show ip eigrp neighbors [*type-number*]	EIGRP によって検出されたネイバーを表示します。
show ip eigrp topology [*autonomous-system-number*] | [[*ip-address*] *mask*]]	指定されたプロセスの EIGRP トポロジ テーブルを表示します。
show ip eigrp traffic [*autonomous-system-number*]	すべてまたは特定の EIGRP プロセスの送受信パケット数を表示します。

BGP の設定

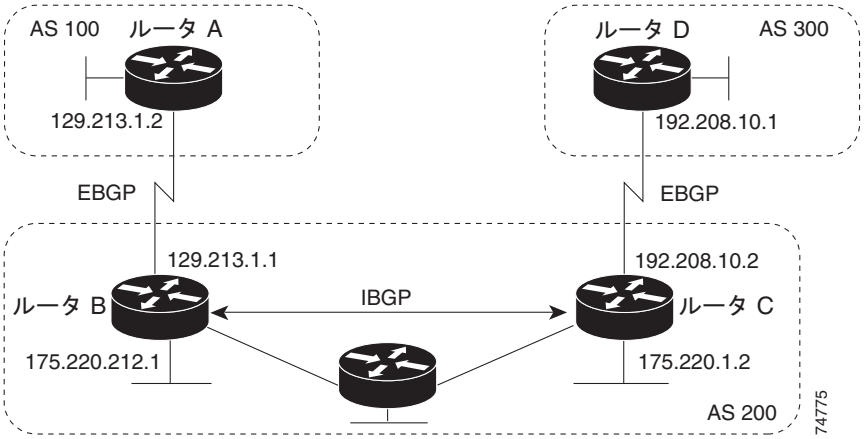
BGP は、Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）です。AS 間で、ループの発生しないルーティング情報交換を行うためのドメイン間ルーティング システムを設定する際に使用されます。AS は、共通の管理の下で動作する複数のルータにより構成されます。EGP を介して相互に接続されたこれらのルータによって、RIP や OSPF などの IGP が境界内で実行されます。BGP バージョン 4 は、インターネット内でドメイン間ルーティングを行うための標準 EGP です。

BGP に関する詳細については、『*Internet Routing Architectures*』（Cisco Press 刊）、および『*Cisco IOS IP and IP Routing Configuration Guide*』の「Configuring BGP」を参照してください。

BGP のコマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* の「IP Routing Protocols」を参照してください。表示されるにもかかわらずスイッチでサポートされていない BGP コマンドについては、付録 C「Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド」を参照してください。

BGP アップデートを交換する場合、同じ AS に属するルータは *Internal BGP*（IBGP; 内部 BGP）を実行し、異なる AS に属するルータは *External BGP*（EBGP; 外部 BGP）を実行します。コンフィギュレーション コマンドの機能は、EBGP を設定する場合と IBGP を設定する場合ではほぼ同じです。異なるのは、ルーティング アップデートが AS 間で交換されるか（EBGP）、AS 内で交換されるか（IBGP）という点です。図 36-5 は、EBGP と IBGP がともに稼動しているネットワークを示したものです。

図 36-5　EBGP、IBGP、および複数の AS



外部 AS と情報を交換する前に、BGP では、AS 内のネットワークに必ず到達できるように、AS 内のルータ間で内部 BGP ピアリングが定義され、IGRP や OSPF など AS 内で稼動する IGP に BGP ルーティング情報が再配布されます。

BGP ルーティング プロセスを実行するルータは通常、BGP *スピーカー*と呼ばれます。BGP では、トランスポート プロトコルとして TCP（特にポート 179）が使用されます。ルーティング情報を交換するため相互に TCP 接続された 2 つの BGP スピーカーを、*ピア*または*ネイバー*と呼びます。図 36-5 では、ルータ A とルータ B、ルータ B と ルータ C、ルータ C とルータ D がそれぞれ BGP ピアを構成しています。ルーティング情報は、宛先ネットワークへのフル パスを示す一連の AS 番号です。BGP では、この情報を基にしてループのない AS マップが作成されます。

このネットワークの特徴は次のとおりです。

- ルータ A およびルータ B では EBGP が、ルータ B およびルータ C では IBGP が稼動しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。IGP が稼動し、2 つのネイバーが相互に到達できるのであれば、IBGP ピアを直接接続する必要はありません。
- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。つまり AS 内の BGP スピーカーは、論理的には完全メッシュ型に接続する必要があります。BGP4 により実現される*連合*および*ルート リフレクタ*という 2 つの技術を使用すると、論理的な完全メッシュ型を構成するための要件を緩和できます。
- AS 200 は AS 100 および AS 300 の *中継 AS* です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティング テーブルを最初に交換し、差分更新だけを送信します。また BGP ピアは、キープアライブ メッセージ（接続が有効であることを確認）、および通知メッセージ（エラーまたは特殊条件に応答）も交換します。

BGP の場合、各ルートは、ネットワーク番号、情報が通過した AS のリスト（*AS パス*）、および他の *パス アトリビュート* リストで構成されます。BGP システムの主な機能は、AS パスのリストに関する情報など、ネットワークの到達可能性情報を他の BGP システムと交換することにあります。この情報は、AS が接続されているかどうかを判別したり、ルーティング ループをプルーニングしたり、AS レベル ポリシー判断を行ったりするために使用できます。

Cisco IOS が稼動しているルータまたはスイッチが IBGP ルートを選択または使用するのは、ネクストホップ ルータで使用可能なルートがあり、かつ IGP から同期信号を受信している（IGP 同期がディセーブルの場合は除く）場合です。複数のルートが使用可能な場合、BGP では *アトリビュート*値に基づいてパスが選択されます。BGP アトリビュートの詳細については、「BGP 判断アトリビュートの設定」（P.36-54）を参照してください。

BGP バージョン 4 では Classless Interdomain Routing（CIDR; クラスレス ドメイン間ルーティング）がサポートされているため、集約ルートを作成して *スーパーネット*を構築し、ルーティング テーブルのサイズを削減できます。CIDR により、BGP 内部のネットワーク クラスという概念は不要になり、IP プレフィクスのアドバタイズがサポートされます。

ここでは、次の設定情報について説明します。

- 「BGP のデフォルト設定」（P.36-48）
- 「BGP ルーティングのイネーブル化」（P.36-50）
- 「ルーティング ポリシー変更の管理」（P.36-52）
- 「BGP 判断アトリビュートの設定」（P.36-54）
- 「ルート マップによる BGP フィルタリングの設定」（P.36-56）
- 「ネイバー単位での BGP フィルタリングの設定」（P.36-57）
- 「BGP フィルタリング用のプレフィクス リストの設定」（P.36-58）
- 「BGP コミュニティ フィルタリングの設定」（P.36-59）
- 「BGP ネイバーおよびピア グループの設定」（P.36-61）
- 「集約アドレスの設定」（P.36-63）
- 「ルーティング ドメイン連合の設定」（P.36-63）
- 「BGP ルート リフレクタの設定」（P.36-64）
- 「ルート ダンプニングの設定」（P.36-65）
- 「BGP のモニタリングおよびメンテナンス」（P.36-66）

BGP 設定の詳細については、『Cisco IOS IP Configuration Guide』Release 12.2 の「IP Routing Protocols」にある「Configuring BGP」を参照してください。特定のコマンドに関する詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* を参照してください。また、表示されるにもかかわらずスイッチでサポートされていない BGP コマンドについては、付録 C「Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド」を参照してください。

BGP のデフォルト設定

表 36-9　BGP のデフォルト設定

機能	デフォルト設定
集約アドレス	ディセーブル：定義なし。
AS パス アクセス リスト	定義なし。
自動サマリー	イネーブル。
最適パス	• ルータはルートを選択する場合に *AS パス*を考慮するが、外部 BGP ピアからの類似ルートは比較されない。 • ルータ ID の比較：ディセーブル。
BGP コミュニティ リスト	• 番号：定義なし。コミュニティ番号を示す特定の値を許可すると、許可されていないその他すべてのコミュニティ番号は、暗黙的に拒否されるようデフォルト設定される。 • フォーマット：シスコ デフォルト フォーマット（32 ビット番号）
BGP 連合 ID/ ピア	• ID：設定なし。 • ピア：指定なし。
BGP 高速外部フォールオーバー	イネーブル。
BGP ローカル プリファレンス	100. 指定できる範囲は 0 ～ 4294967295（大きな値を推奨）。
BGP ネットワーク	指定なし。バックドア ルートのアドバタイズなし。
BGP ルート ダンプニング	デフォルトでディセーブル。イネーブルの場合は、次のとおり。 • 半減期は 15 分。 • 再使用は 750（10 秒増分）。 • 抑制は 2000（10 秒増分）。 • 最大抑制時間は半減期の 4 倍（60 分）。
BGP ルータ ID	ループバック インターフェイスに IP アドレス（設定されている場合）、またはルータの物理インターフェイスに対して設定された最大の IP アドレス。
デフォルト情報の送信（プロトコルまたはネットワーク再配布）	ディセーブル。
デフォルト メトリック	自動メトリック変換（組み込み）。
距離	• 外部ルートの管理ディスタンス：20（指定できる範囲は 1 ～ 255） • 内部ルートの管理ディスタンス：200（指定できる範囲は 1 ～ 255） • ローカル ルートの管理ディスタンス：200（指定できる範囲は 1 ～ 255）
配布リスト	• 入力（アップデート中に受信されたネットワークをフィルタリング）：ディセーブル。 • 出力（アップデート中のネットワークのアドバタイズを抑制）：ディセーブル。
内部ルート再配布	ディセーブル。
IP プレフィクス リスト	定義なし。

表 36-9　BGP のデフォルト設定 （続き）

機能	デフォルト設定
Multi Exit Discriminator（MED）	• 常に比較：ディセーブル。異なる AS 内のネイバーからのパスについては MED を比較しない。 • 最適パスの比較：ディセーブル。 • 最悪パスである MED の除外：ディセーブル。 • 決定的な MED 比較：ディセーブル。
Neighbor	• アドバタイズメント インターバル：外部ピアの場合は 30 秒、内部ピアの場合は 5 秒。 • 変更ロギング：イネーブル。 • 条件付きアドバタイズメント：ディセーブル。 • デフォルトの送信：ネイバーにデフォルト ルートは送信されない。 • 説明：なし。 • 配布リスト：定義なし。 • 外部 BGP マルチホップ：直接接続されたネイバーに限り許可。 • フィルタ リスト：使用しない。 • 受信されるプレフィクスの最大数：制限なし。
Neighbor	• ネクストホップ（BGP ネイバーのネクストホップとなるルータ）：ディセーブル。 • パスワード：ディセーブル。 • ピア グループ：定義なし。割り当てられたメンバーなし。 • プレフィクス リスト：指定なし。 • リモート AS（ネイバーの BGP テーブルにエントリを追加）：定義されたピアなし。 • プライベート AS 番号の削除：ディセーブル。 • ルート マップ：ピアへの適用なし。 • コミュニティ アトリビュートの送信：ネイバーへの送信なし。 • シャットダウンまたはソフト再設定：イネーブルでない。 • タイマー：キープアライブは 60 秒、ホールドタイムは 180 秒。 • アップデート送信元：最適ローカル アドレス。 • バージョン：BGP バージョン 4。 • 重み：BGP ピアを介して学習したルートの場合は 0、ローカル ルータからのルートの場合は 32768。
NSF[1] 認識	ディセーブル[2]。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中、隣接する NSF 対応ルータからのパケットを転送し続けることが可能。
ルート リフレクタ	設定なし。
同期化（BGP および IGP）	イネーブル。
テーブル マップ アップデート	ディセーブル。
タイマー	キープアライブ：60 秒、ホールドタイム：180 秒。

1. NSF = Nonstop Forwarding（ノンストップ フォワーディング）
2. メトロ IP アクセス イメージが実行されているスイッチ上の IPv4 に対しては、グレースフル リスタートをイネーブルにすることにより、BGP NSF 認識をイネーブルにできます。

NSF 認識

メトロ IP アクセス イメージの IPv4 に対しては、BGP NSF 認識機能がサポートされています。BGP ルーティングでこの機能をイネーブルにするには、グレースフル リスタートをイネーブルにする必要があります。隣接ルータが NSF 対応である場合、この機能をイネーブルにすると、レイヤ 3 スイッチでは、ルータ内で障害が発生したプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断することなくソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからのパケットが転送され続けます。

詳細については、次の URL にある『*BGP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008015fede.html

BGP ルーティングのイネーブル化

BGP ルーティングをイネーブルにするためには、BGP ルーティング プロセスを確立し、ローカル ネットワークを定義する必要があります。BGP はネイバーとの関係を完全に認識する必要があるため、BGP ネイバーについても指定する必要があります。

BGP では、内部ネイバーおよび外部ネイバーという 2 種類のネイバーがサポートされています。*内部ネイバー*は同じ AS 内にあるネイバー、*外部ネイバー*は異なる AS 内にあるネイバーのことです。通常、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダーによって割り当てられ、ルートが外部ネイバーにアドバタイズされないシステムに設定されます。プライベート AS 番号は、64512 ～ 65535 の範囲で指定できます。**neighbor remove-private-as** ルータ コンフィギュレーション コマンドを使用すると、AS パスからプライベート AS 番号が削除されるように外部ネイバーを設定できます。これにより、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号が削除されます。

AS が別の AS から受け取ったトラフィックをさらに別の AS に渡す場合は、アドバタイズ対象のルートに矛盾がないことが重要です。BGP によりルートがアドバタイズされてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかったトラフィックを受信することがあります。このような事態を避けるため、IGP により AS に情報が伝播され BGP が IGP と*同期化*されるまで、BGP は待機する必要があります。同期化は、デフォルトでイネーブルに設定されています。AS が別の AS から受け取ったトラフィックをその他の AS へ渡さない場合、または AS 内のすべてのルータで BGP が稼動している場合は、同期化をディセーブルにして、IGP 内で伝送されるルート数を少なくし、BGP のコンバージェンス時間を短縮します。

BGP ルーティングをイネーブルにし、BGP ルーティング プロセスを確立して、ネイバーを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします（IP ルーティングがディセーブルになっている場合に限り必須）。
ステップ 3	**router bgp** *autonomous-system*	BGP ルーティング プロセスをイネーブルにして、それに AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。指定できる AS 番号は 1 ～ 65535 です。64512 ～ 65535 は、プライベート AS 番号専用です。

	コマンド	目的
ステップ 4	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]	この AS に対してローカルとなるようにネットワークを設定し、そのネットワークを BGP テーブルに格納します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	BGP ネイバー テーブルにエントリを追加し、IP アドレスで指定したネイバーが、指定された AS に属するようにします。 EBGP では、通常ネイバーは直接接続されており、IP アドレスは接続の他端に位置するインターフェイスのアドレスです。 IBGP では、IP アドレスにはルータ インターフェイス内の任意のアドレスを指定できます。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remove-private-as**	（任意）発信ルーティング アップデート内の AS パスからプライベート AS 番号を削除します。
ステップ 7	**no synchronization**	（任意）BGP と IGP の同期化をディセーブルにします。
ステップ 8	**no auto-summary**	（任意）自動ネットワーク サマライズをディセーブルにします。デフォルトでは、IGP から BGP にサブネットが再配布された場合、ネットワーク ルートだけが BGP テーブルに追加されます。
ステップ 9	**bgp fast-external-fallover**	（任意）外部ネイバー間のリンクが切断された場合、BGP セッションが自動的にリセットされるようにします。デフォルトの場合、セッションは即座にはリセットされません。
ステップ 10	**bgp graceful-restart**	（任意）スイッチ上の NSF 認識をイネーブルにします。NSF 認識はデフォルトではディセーブルです。
ステップ 11	**end**	特権 EXEC モードに戻ります。

ステップ 12	**show ip bgp network** *network-number*
	or
	show ip bgp neighbor
		設定を確認します。
		NSF 認識（グレースフル リスタート）がネイバーでイネーブルであることを確認します。
		スイッチおよびネイバーで NSF 認識がイネーブルである場合は、次のメッセージが表示されます。
		`Graceful Restart Capability: advertised and received`
		NSF 認識がスイッチではイネーブル、ネイバーではディセーブルの場合は、次のメッセージが表示されます。
		`Graceful Restart Capability: advertised`

ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP AS を削除するには、**no router bgp** *autonomous-system* グローバル コンフィギュレーション コマンドを使用します。BGP テーブルからネットワークを削除するには、**no network** *network-number* ルータ コンフィギュレーション コマンドを使用します。ネイバーを削除するには、**no neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number* ルータ コンフィギュレーション コマンドを使用します。ネイバーにアップデート内のプライベート AS 番号を追加するには、**no neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** ルータ コンフィギュレーション コマンドを使用します。同期化を再度イネーブルにするには、**synchronization** ルータ コンフィギュレーション コマンドを使用します。

次に、図 36-5 の各ルータ上で BGP を設定する例を示します。

ルータ A：

```
Switch(config)# router bgp 100
Switch(config-router)# neighbor 129.213.1.1 remote-as 200
```

ルータ B：

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 129.213.1.2 remote-as 100
Switch(config-router)# neighbor 175.220.1.2 remote-as 200
```

ルータ C：

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 175.220.212.1 remote-as 200
Switch(config-router)# neighbor 192.208.10.1 remote-as 300
```

ルータ D：

```
Switch(config)# router bgp 300
Switch(config-router)# neighbor 192.208.10.2 remote-as 200
```

BGP ピアが稼動していることを確認するには、**show ip bgp neighbors** 特権 EXEC コマンドを使用します。次に、ルータ A にこのコマンドを実行した場合の出力例を示します。

```
Switch# show ip bgp neighbors

BGP neighbor is 129.213.1.1, remote AS 200, external link
 BGP version 4, remote router ID 175.220.212.1
 BGP state = established, table version = 3, up for 0:10:59
 Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
 Minimum time between advertisement runs is 30 seconds
 Received 2828 messages, 0 notifications, 0 in queue
 Sent 2826 messages, 0 notifications, 0 in queue
 Connections established 11; dropped 10
```

state = established 以外の情報が出力された場合、ピアは稼動していません。リモート ルータ ID は、ルータ上の最大の IP アドレス（または最大のループバック インターフェイス）です。テーブルは、新規情報によりアップデートされるたびに、そのバージョン番号が増加します。継続的にテーブル バージョン番号が増加している場合は、ルートがフラッピングし、ルーティング アップデートが絶えず発生していると判断できます。

外部プロトコルの場合、**network** ルータ コンフィギュレーション コマンドから IP ネットワークへの参照によって制御されるのは、アドバタイズされるネットワークだけです。これは、**network** コマンドを使用してアップデートの送信先を指定する IGP（EIGRP など）とは対照的です。

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Routing Protocols」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* を参照してください。表示されるにもかかわらずスイッチでサポートされていない BGP コマンドについては、付録 C「Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド」を参照してください。

ルーティング ポリシー変更の管理

ピアのルーティング ポリシーには、着信ルーティング テーブルまたは発信ルーティング テーブルのアップデートに影響する可能性のある設定がすべて含まれています。BGP ネイバーとして定義された 2 台のルータは、BGP 接続を形成し、ルーティング情報を交換します。そのあとで BGP フィルタ、重み、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行うには、BGP セッションをリセットし、設定の変更内容を有効にする必要があります。

リセットには、ハード リセットとソフト リセットの 2 つのタイプがあります。両方の BGP ピアでソフト ルート リフレッシュ機能がサポートされている場合、スイッチでは事前に設定を行うことなくソフト リセットを使用できます。ソフト ルート リフレッシュ機能は、ピアによって TCP セッションが確

立されたときに送信される OPEN メッセージによりアドバタイズされます。ソフト リセットを使用すると、BGP ルータ間でルート リフレッシュ要求およびルーティング情報をダイナミックに交換したり、それぞれの発信ルーティング テーブルをあとで再アドバタイズしたりできます。

- ソフト リセットによってネイバーから着信アップデートが生成される場合、このリセットを*ダイナミック着信ソフト リセット*といいます。
- ソフト リセットによってネイバーに一連のアップデートが送信される場合、このリセットを*発信ソフト リセット*といいます。

ソフト着信リセットを実行すると、新規着信ポリシーが有効になります。ソフト発信リセットを実行すると、BGP セッションがリセットされることなく、新規ローカル発信ポリシーが有効になります。発信ポリシーのリセット中に一連のアップデートが新たに送信されると、新しい着信ポリシーが有効になる場合があります。

表 36-10　ハード リセットとソフト リセットの長所および短所

リセット タイプ	長所	短所
ハード リセット	メモリ オーバーヘッドが発生しません。	ネイバーから取得した BGP テーブル、IP テーブル、および Forwarding Information Base（FIB; 転送情報ベース）テーブル内のプレフィクスが失われます。推奨されません。
発信ソフト リセット	ルーティング テーブル アップデートが設定、保存されません。	着信ルーティング テーブル アップデートがリセットされません。
ダイナミック着信ソフト リセット	BGP セッションおよびキャッシュが消去されません。 ルーティング テーブル アップデートを保存する必要がなく、メモリ オーバーヘッドが発生しません。	両方の BGP ルータで、ルート リフレッシュ機能がサポートされている必要があります。

BGP ピアがルート リフレッシュ機能をサポートしているかどうかを確認し、BGP セッションをリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**show ip bgp neighbors**	ネイバーがルート リフレッシュ機能をサポートしているかどうかを表示します。サポートされている場合は、ルータに関する次のメッセージが表示されます。 *Received route refresh capability from peer*
ステップ 2	**clear ip bgp** {***** | *address* | *peer-group-name*}	指定された接続上でルーティング テーブルをリセットします。 • すべての接続をリセットするには、アスタリスク（*）を入力します。 • 特定の接続をリセットするには、IP *アドレス*を入力します。 • ピア グループをリセットするには、そのピア グループ名を入力します。

	コマンド	目的
ステップ 3	**clear ip bgp** {***** | *address* | *peer-group-name*} **soft out**	（任意）発信ソフト リセットを実行して、指定された接続上で着信ルーティング テーブルをリセットします。このコマンドは、ルート リフレッシュがサポートされている場合に使用してください。 • すべての接続をリセットするには、アスタリスク（*****）を入力します。 • 特定の接続をリセットするには、IP *アドレス*を入力します。 • ピア グループをリセットするには、そのピア グループ名を入力します。
ステップ 4	**show ip bgp** **show ip bgp neighbors**	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断アトリビュートの設定

BGP スピーカーが複数の AS から受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達する最適パスを 1 つ選択する必要があります。この判断は、アップデートに格納されているアトリビュート値、および BGP で設定可能なその他の基準に基づいて行われます。選択されたパスは BGP ルーティング テーブルに格納され、ネイバーに伝播されます。

BGP ピアは、プレフィクスに対する 2 つの EBGP パスをネイバー AS から学習する際、最適パスを選択し、それを IP ルーティング テーブルに挿入します。BGP マルチパス サポートがイネーブルの場合、同じネイバー AS から複数の EBGP パスを学習すると、IP ルーティング テーブルには複数のパスが格納されます。さらに、パケット スイッチング中に、複数のパス間でパケット単位または宛先単位でのロード バランシングが実行されます。**maximum-paths** ルータ コンフィギュレーション コマンドを使用すると、許可されるパス数を制御できます。

これらの要因により、BGP が最適パスを選択するためにアトリビュートを評価する際の基準と評価する順序が決定されます。

1. パスで指定されているネクストホップが到達不能な場合、このアップデートは廃棄されます。BGP のネクストホップ アトリビュート（ソフトウェアによって自動判別される）は、宛先へ到達するために使用されるネクストホップの IP アドレスです。EBGP の場合、通常このアドレスは **neighbor remote-as** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクストホップの処理をディセーブルにするには、ルート マップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。
2. 重み（シスコ独自のパラメータ）が最大であるパスを優先します。重みアトリビュートはルータに対してローカルであるため、ルーティング アップデートでは伝播されません。デフォルトでは、ルータ送信元のパスに関する重みアトリビュートは 32768 で、それ以外のパスの重みアトリビュートは 0 です。重みを設定するには、アクセス リスト、ルート マップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。
3. ローカル プリファレンスが最大であるルートを優先します。ローカル プリファレンスはルーティング アップデートに含まれ、同じ AS 内のルータ間で交換されます。ローカル プリファレンス アトリビュートのデフォルト値は 100 です。ローカル プリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルート マップを使用します。
4. ローカル ルータ上で稼動する BGP から送信されたルートを優先します。
5. AS パスが最短のルートを優先します。
6. 送信元タイプが最小のルートを優先します。内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP によって学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。

7. 想定されるすべてのルートについてネイバー AS が同じである場合は、MED メトリック アトリビュートが最小のルートを優先します。MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。
8. 内部（IBGP）パスより、外部（EBGP）パスを優先します。
9. 最も近い IGP ネイバー（最小の IGP メトリック）を通って到達できるルートを優先します。この場合、ルータは、AS 内の最短の内部パス（BGP のネクストホップへの最短パス）を使用して宛先に到達します。
10. 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入します。
    - 最適ルートと目的のルートがともに外部ルートである
    - 最適ルートと目的のルートの両方が、同じネイバー AS からのルートである
    - maximum-paths がイネーブルである
11. マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレスが最小であるルートを優先します。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック（仮想）アドレスですが、場合によっては実装に依存します。

判断アトリビュートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルーティング プロセスをイネーブルにして、それに AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp best-path as-path ignore**	（任意）ルート選択中に AS パス長を無視するようにルータを設定します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	（任意）ネクストホップ アドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクストホップの処理をディセーブルにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **weight** *weight*	（任意）ネイバー接続に重みを割り当てます。指定できる値は 0 ～ 65535 です。重み最大のルートが優先されるルートです。別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカル ルータから送信されたルートのデフォルトの重みは 32768 です。
ステップ 6	**default-metric** *number*	（任意）優先されるパスが外部ネイバーに設定されるように MED メトリックを設定します。MED を持たないルータもすべて、この値に設定されます。指定できる範囲は 1 ～ 4294967295 です。この値が最小であるパスが最優先されます。
ステップ 7	**bgp bestpath med missing-as-worst**	（任意）MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。
ステップ 8	**bgp always-compare med**	（任意）異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。デフォルトでは、MED は同じ AS 内のパス間に限って比較されます。

	コマンド	目的
ステップ 9	**bgp bestpath med confed**	（任意）連合内の異なるサブ AS によってアドバタイズされたパスの中から特定のパスを選択する場合に、MED を考慮するようスイッチを設定します。
ステップ 10	**bgp deterministic med**	（任意）同じ AS 内の異なるピアによってアドバタイズされたルートの中から選択する場合に、MED 変数を考慮するようスイッチを設定します。
ステップ 11	**bgp default local-preference** *value*	（任意）デフォルトのローカル プリファレンス値を変更します。指定できる範囲は 0 ～ 4294967295 で、デフォルト値は 100 です。最大のローカル プリファレンス値を持つパスが優先されます。
ステップ 12	**maximum-paths** *number*	（任意）IP ルーティング テーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティング テーブルに追加されます。指定できる範囲は 1 ～ 8 です。複数のパスが追加されると、パス間のロード バランシングが可能になります。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show ip bgp** **show ip bgp neighbors**	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト状態に戻すには、各コマンドの **no** 形式を使用します。

ルート マップによる BGP フィルタリングの設定

BGP 内でルート マップを使用すると、ルーティング情報を制御、変更したり、ルーティング ドメイン間でルートを再配布する条件を定義したりできます。ルート マップの詳細については、「ルート マップによるルーティング情報の再配布」（P.36-105）を参照してください。各ルート マップには、ルート マップを識別する名前（マップ タグ）およびオプションのシーケンス番号が付いています。

ルート マップを使用してネクストホップ処理をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [[**permit** | **deny**] | *sequence-number*]]	ルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。
ステップ 3	**set ip next-hop** *ip-address* [*...ip-address*] [**peer-address**]	（任意）ネクストホップ処理をディセーブルにするようにルート マップを設定します。 • 着信ルート マップの場合は、一致するルートのネクストホップをネイバー ピア アドレスに設定し、サードパーティのネクストホップを上書きします。 • BGP ピアの発信ルート マップの場合は、ネクストホップをローカル ルータのピア アドレスに設定して、ネクストホップ計算をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show route-map** [*map-name*]	設定を確認するため、設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート マップを削除するには、**no route-map** *map-tag* コマンドを使用します。ネクストホップ処理を再びイネーブルにするには、**no set ip next-hop** *ip-address* コマンドを使用します。

ネイバー単位での BGP フィルタリングの設定

BGP アドバタイズメントをフィルタリングするには、**as-path access-list** グローバル コンフィギュレーション コマンドや **neighbor filter-list** ルータ コンフィギュレーション コマンドなどの AS パス フィルタを使用します。**neighbor distribute-list** ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。distribute-list フィルタはネットワーク番号に適用されます。**distribute-list** コマンドの詳細については、「ルーティング アップデートのアドバタイズおよび処理の制御」（P.36-114）を参照してください。

ネイバー単位でルート マップを使用すると、アップデートをフィルタリングしたり、各アトリビュートを変更したりできます。ルート マップは、着信アップデートまたは発信アップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデートで送信または許可されます。着信および発信の両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づく照合がサポートされています。AS パスの照合には **match as-path access-list** ルート マップ コマンド、コミュニティに基づく照合には **match community-list** ルート マップ コマンド、ネットワークに基づく照合には **ip access-list** グローバル コンフィギュレーション コマンドがそれぞれ必要です。

ネイバー単位のルート マップを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルーティング プロセスをイネーブルにして、それに AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** {*ip-address* | *peer-group name*} **distribute-list** {*access-list-number* | *name*} {**in** | **out**}	（任意）アクセス リストの指定に従って、ネイバーとの間で送受信される BGP ルーティング アップデートをフィルタリングします。 **（注）** **neighbor prefix-list** ルータ コンフィギュレーション コマンドを使用して、アップデートをフィルタリングすることもできますが、両方のコマンドを使用しても同じ BGP ピアを設定できません。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **route-map** *map-tag* {**in** | **out**}	（任意）ルート マップを適用し、着信ルートまたは発信ルートをフィルタリングします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ネイバーからアクセス リストを削除するには、**no neighbor distribute-list** コマンドを使用します。ネイバーからルート マップを削除するには、**no neighbor route-map** *map-tag* ルータ コンフィギュレーション コマンドを使用します。

BGP AS パスに基づいて着信および発信の両方のアップデートにアクセス リスト フィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現に基づくアクセス リストです（正規表現の作成方法については、『*Cisco IOS Dial Technologies Command Reference*』*Release 12.2* の付録「Regular Expressions」を参照してください）。この方法を使用するには、AS パスのアクセス リストを定義し、特定のネイバーに対して送受信されるアップデートに適用する必要があります。

BGP パス フィルタリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip as-path access-list** *access-list-number* {**permit** | **deny**} *as-regular-expressions*	BGP 関連アクセス リストを定義します。
ステップ 3	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **filter-list** {*access-list-number* | *name*} {**in** | **out** | **weight** *weight*}	アクセス リストに基づいて、BGP フィルタを作成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** [**paths** regular-expression]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP フィルタリング用のプレフィクス リストの設定

neighbor distribute-list ルータ コンフィギュレーション コマンドなどの多数の BGP ルート フィルタリング コマンドでは、アクセス リストの代わりにプレフィクス リストを使用できます。プレフィクス リストによるフィルタリングでは、アクセス リストの照合の場合と同様に、プレフィクス リストに記載されたプレフィクスとルートのプレフィクスが照合されます。一致するルートが存在する場合は、そのルートが使用されます。プレフィクスが許可されるか、または拒否されるかは、次に示す規則に基づいて決定されます。

- プレフィクス リストが空の場合は、すべてのプレフィクスが許可されます。
- 指定されたプレフィクスがプレフィクス リスト内のどのエントリとも一致しない場合は、暗黙的に拒否されたと見なされます。
- 指定されたプレフィクスと一致するエントリがプレフィクス リスト内に複数存在する場合は、シーケンス番号が最小であるプレフィクス リスト エントリが特定されます。

デフォルトでは、シーケンス番号は自動生成され、5 ずつ増分します。シーケンス番号の自動生成をディセーブルにした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号を指定する場合の増分値に制限はありません。増分値が 1 の場合、そのリストには追加エントリを挿入できません。また、増分値として大きな値を選択すると、値が不足する可能性があります。

コンフィギュレーション エントリを削除するときは、シーケンス番号を指定する必要はありません。**show** コマンドの出力にも、シーケンス番号が表示されます。

コマンド内でプレフィクス リストを使用する場合は、あらかじめプレフィクス リストを設定しておく必要があります。プレフィクス リストを作成する、またはプレフィクス リストにエントリを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip prefix-list** *list-name* [**seq** *seq-value*] **deny** | **permit** *network*/*len* [**ge** *ge-value*] [**le** *le-value*]	照合する条件に合せて、アクセスを拒否（**deny**）または許可（**permit**）するプレフィクス リストを作成します。シーケンス番号を指定することもできます。**permit** 句または **deny** 句を少なくとも 1 つ入力する必要があります。 • *network*/*len* には、ネットワーク番号およびネットワーク マスクの長さ（ビット単位）を指定します。 • （任意）**ge** および **le** の値は、照合するプレフィクス長の範囲を表します。*ge-value* および *le-value* に指定する値は、*len* < *ge-value* < *le-value* < 32 という条件を満たしていることが必要です。
ステップ 3	**ip prefix-list** *list-name* **seq** *seq-value* **deny** | **permit** *network*/*len* [**ge** *ge-value*] [**le** *le-value*]	（任意）プレフィクス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip prefix list** [**detail** | **summary**] *name* [*network*/*len*] [**seq** *seq-num*] [**longer**] [**first-match**]	プレフィクス リストまたはプレフィクス リスト エントリに関する情報を表示して、設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

プレフィクス リストまたはそのエントリをすべて削除するには、**no ip prefix-list** *list-name* グローバル コンフィギュレーション コマンドを使用します。プレフィクス リストから特定のエントリを削除するには、**no ip prefix-list seq** *seq-value* グローバル コンフィギュレーション コマンドを使用します。シーケンス番号の自動生成をディセーブルにするには **no ip prefix-list sequence number** コマンドを、自動生成を再びイネーブルにする場合は **ip prefix-list sequence number** コマンドを使用します。プレフィクス リスト エントリのヒット数テーブルを消去するには、**clear ip prefix-list** 特権 EXEC コマンドを使用します。

BGP コミュニティ フィルタリングの設定

BGP コミュニティ フィルタリングは、COMMUNITIES アトリビュートの値を基に BGP でルーティング情報の配布を制御する方法の 1 つです。コミュニティは、共通するいくつかのアトリビュートを共有する宛先のグループです。各宛先は複数のコミュニティに属することもあります。AS 管理者は、宛先が属するコミュニティを定義できます。デフォルトでは、すべての宛先が一般的なインターネット コミュニティに属します。コミュニティは、推移的でグローバルな、オプションの COMMUNITIES アトリビュート（1 ～4294967200）によって識別されます。事前に定義された既知のコミュニティの一部を、次に示します。

- **internet**：インターネット コミュニティにこのルートをアドバタイズします。このコミュニティには、すべてのルータが所属します。
- **no-export**：EBGP ピアにこのルートをアドバタイズしません。
- **no-advertise**：どのピア（内部または外部）にもこのルートをアドバタイズしません。
- **local-as**：ローカルな AS 外部のピアにこのルートをアドバタイズしません。

コミュニティに基づき、他のネイバーに対して許可、推奨、または配布されるルーティング情報を制御できます。BGP スピーカーは、ルートを学習、アドバタイズ、または再配布するときに、ルートのコミュニティを設定、追加、または変更します。ルートを集約すると、作成された集約内の COMMUNITIES アトリビュートに、すべての初期ルートの全コミュニティが含まれます。

コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。さらに、アクセス リストの場合と同様、一連のコミュニティ リストを作成することもできます。文のチェックは、一致が検出されるまで続けられ、いずれか 1 つの文に一致した時点で、テストは終了します。

コミュニティに基づいて COMMUNITIES アトリビュートおよび match 句を設定するには、「ルートマップによるルーティング情報の再配布」（P.36-105）に記載されている **match community-list** ルートマップ コンフィギュレーション コマンドおよび **set community** ルートマップ コンフィギュレーション コマンドを参照してください。

デフォルトでは、ネイバーに COMMUNITIES アトリビュートは送信されません。COMMUNITIES アトリビュートが特定の IP アドレスのネイバーに送信されるように指定するには、**neighbor send-community** ルータ コンフィギュレーション コマンドを使用します。

コミュニティ リストを作成、適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip community-list** *community-list-number* {**permit** | **deny**} *community-number*	コミュニティ リストを作成し、それに番号を割り当てます。 • *community-list-number* には 1 ～ 99 の整数を指定します。この値により、1 つまたは複数のコミュニティの許可グループまたは拒否グループが識別されます。 • *community-number* には、**set community** ルートマップ コンフィギュレーション コマンドで設定される番号を指定します。
ステップ 3	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **send-community**	この IP アドレスのネイバーに送信する COMMUNITIES アトリビュートを指定します。
ステップ 5	**set comm-list** *list-num* **delete**	（任意）ルート マップで指定された標準または拡張のコミュニティ リストと一致する着信アップデートまたは発信アップデートのコミュニティ アトリビュートから、コミュニティを削除します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip bgp-community new-format**	（任意）AA:NN のフォーマットで BGP コミュニティを表示し、解析を行います。 BGP コミュニティは、2 つの部分からなる 2 バイト長フォーマットで表示されます。シスコのデフォルトのコミュニティ フォーマットは NNAA です。BGP に関する最新の RFC では、コミュニティは AA:NN のフォーマットをとります。最初の部分は AS 番号で、その次の部分は 2 バイトの数値です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp community**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ネイバーおよびピア グループの設定

通常は、多数の BGP ネイバーに同一のアップデート ポリシー（同じ発信ルート マップ、配布リスト、フィルタ リスト、アップデート送信元など）が設定されます。アップデート ポリシーが同じであるネイバーをピア グループにまとめると設定が簡単になり、アップデートの効率が高まります。多数のピアを設定した場合は、この方法を推奨します。

BGP ピア グループを設定するには、ピア グループを作成し、そこにオプションを割り当てて、ピア グループ メンバーとしてネイバーを追加する必要があります。ピア グループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。デフォルトでは、ピア グループ メンバーは remote-as（設定されている場合）、version、update-source、out-route-map、out-filter-list、out-dist-list、minimum-advertisement-interval、next-hop-self など、ピア グループの設定オプションをすべて継承します。また、すべてのピア グループ メンバーが、ピア グループに対する変更を継承します。さらには、発信アップデートに影響しないオプションを無効にするように、メンバーを設定することもできます。

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用して、次に示すルータ コンフィギュレーション コマンドのいずれかを指定します。ピア グループにオプションを割り当てるには、ピア グループ名を使用して、いずれかのコマンドを指定します。**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用すると、いずれの設定情報も削除することなく、BGP ピアまたはピア グループをディセーブルにできます。

BGP ピアを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** *peer-group-name* **peer-group**	BGP ピア グループを作成します。
ステップ 4	**neighbor** *ip-address* **peer-group** *peer-group-name*	BGP ネイバーをピア グループのメンバーにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	BGP ネイバーを指定します。**remote-as** *number* を使用してピア グループが設定されていない場合は、このコマンドを使用して、EBGP ネイバーを含むピア グループを作成します。指定できる範囲は 1 ～ 65535 です。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **description** *text*	（任意）ネイバーに説明を関連付けます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]	（任意）BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに送信する COMMUNITIES アトリビュートを指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface*	（任意）IBGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop**	（任意）ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを使用可能にします。マルチホップ ピア アドレスへの唯一のルートがデフォルト ルート（0.0.0.0）の場合、マルチホップ セッションは確立されません。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **local-as** *number*	（任意）ローカル AS として使用する AS 番号を指定します。指定できる範囲は 1 ～ 65535 です。

	コマンド	目的
ステップ 12	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*	（任意）BGP ルーティング アップデートを送信する最小インターバルを設定します。
ステップ 13	**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*]	（任意）ネイバーから受信できるプレフィクス数を制御します。指定できる範囲は 1 ～ 4294967295 です。*threshold*（任意）は、警告メッセージが生成される基準となる最大値（パーセント）です。デフォルト値は 75% です。
ステップ 14	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	（任意）ネイバー宛の BGP アップデートに関するネクストホップ処理をディセーブルにします。
ステップ 15	**neighbor** {*ip-address* | *peer-group-name*} **password** *string*	（任意）TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。
ステップ 16	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}	（任意）着信ルートまたは発信ルートにルート マップを適用します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに送信する COMMUNITIES アトリビュートを指定します。
ステップ 18	**neighbor** {*ip-address* | *peer-group-name*} **timers** *keepalive holdtime*	（任意）ネイバーまたはピア グループ用のタイマーを設定します。 • *keepalive* には、キープアライブ メッセージがピアに送信される時間間隔を指定します。指定できる範囲は 1 ～ 4294967295 秒で、デフォルトは 60 秒です。 • *holdtime* には、キープアライブ メッセージを受信しなかった場合にピアが非アクティブと宣言されるまでの時間間隔を指定します。指定できる範囲は 1 ～ 4294967295 秒で、デフォルトは 180 秒です。
ステップ 19	**neighbor** {*ip-address* | *peer-group-name*} **weight** *weight*	（任意）ネイバーからのすべてのルートに対して重みを指定します。
ステップ 20	**neighbor** {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *name*} {**in** | **out**}	（任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。
ステップ 21	**neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out** | **weight** *weight*}	（任意）BGP フィルタを作成します。
ステップ 22	**neighbor** {*ip-address* | *peer-group-name*} **version** *value*	（任意）ネイバーと通信するときに使用する BGP バージョンを指定します。
ステップ 23	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**	（任意）受信したアップデートの保存を開始するようにソフトウェアを設定します。
ステップ 24	**end**	特権 EXEC モードに戻ります。
ステップ 25	**show ip bgp neighbors**	設定を確認します。
ステップ 26	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

既存の BGP ネイバーまたはネイバー ピア グループをディセーブルにするには、**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。ディセーブル化されている既存のネイバーまたはネイバー ピア グループをイネーブルにするには、**no neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。

集約アドレスの設定

CIDR を使用すると、集約ルート（または*スーパーネット*）を作成して、ルーティング テーブルのサイズを最小化できます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配布するか、または BGP ルーティング テーブル内に集約エントリを作成します。BGP テーブル内に特定のエントリが 1 つ以上存在する場合は、BGP テーブルに集約アドレスが追加されます。

ルーティング テーブル内に集約アドレスを作成するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**aggregate-address** *address mask*	BGP ルーティング テーブル内に集約エントリを作成します。集約ルートは AS からのルートとしてアドバタイズされます。情報が失われた可能性があることを示すため、アトミック集約アトリビュートが設定されます。
ステップ 4	**aggregate-address** *address mask* **as-set**	（任意）AS 設定パス情報を生成します。このコマンドを使用すると、その直前にあるコマンドと同じ規則に従う集約エントリを作成できます。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。多数のパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、更新されます。
ステップ 5	**aggregate-address** *address-mask* **summary-only**	（任意）サマリー アドレスだけをアドバタイズします。
ステップ 6	**aggregate-address** *address mask* **suppress-map** *map-name*	（任意）選択された、より具体的なルートを抑制します。
ステップ 7	**aggregate-address** *address mask* **advertise-map** *map-name*	（任意）ルート マップによって指定された条件に基づいて集約を生成します。
ステップ 8	**aggregate-address** *address mask* **attribute-map** *map-name*	（任意）ルート マップで指定されたアトリビュートを持つ集約を生成します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp neighbors** [**advertised-routes**]	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

集約エントリを削除するには、**no aggregate-address** *address mask* ルータ コンフィギュレーション コマンドを使用します。オプションをデフォルト値に戻すには、このコマンドにキーワードを指定して実行します。

ルーティング ドメイン連合の設定

IBGP メッシュの単純化は、AS を複数のサブ AS に分割し、単独の AS としてされる 1 つの連合にグループ化することによっても実現できます。各 AS はその内部構造が完全メッシュ型になっており、同じ連合内の他の AS との間には数本の接続があります。異なる AS 内にあるピアでは EBGP セッションが使用されますが、ルーティング情報は IBGP ピアと同様の方法で交換されます。特に、ネクストホップ、MED、およびローカル プリファレンス情報が維持されるため、すべての AS に対して共通の IGP を使用できます。

BGP 連合を設定するには、AS グループの AS 番号として機能する連合 ID を指定する必要があります。BGP 連合を設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp confederation identifier** *autonomous-system*	BGP 連合 ID を設定します。
ステップ 4	**bgp confederation peers** *autonomous-system* [*autonomous-system ...*]	連合に属する AS、および特殊な EBGP ピアとして処理する AS を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbor** **show ip bgp network**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ルート リフレクタの設定

BGP では、すべての IBGP スピーカーを完全メッシュ型に接続する必要があります。外部ネイバーからルートを受信したルータは、そのルートをすべての内部ネイバーにアドバタイズする必要があります。ルーティング情報のループを防ぐには、すべての IBGP スピーカーを接続する必要があります。内部ネイバーは、学習したルートを他の内部ネイバーには送信しません。

ルート リフレクタを使用すると、学習されたルートをネイバーへ渡す際に他の方法が使用されるため、すべての IBGP スピーカーを完全メッシュ型に接続する必要はありません。IBGP ピアを*ルート リフレクタ*として設定すると、その IBGP ピアでは IBGP によって学習されたルートが一連の IBGP ネイバーに送信されるようになります。ルート リフレクタの内部ピアは、*クライアント ピア*および*非クライアント ピア*（AS システム内に存在するその他すべてのルータ）という 2 つのグループに分類されます。ルート リフレクタは、これらの 2 つのグループ間でルートを反映させます。ルート リフレクタおよびそのクライアント ピアは、*クラスタ*を形成します。非クライアント ピアは完全メッシュ型に相互接続する必要がありますが、クライアント ピアはその必要はありません。クラスタ内のクライアントは、そのクラスタ外部の IBGP スピーカーとは通信しません。

アドバタイズされたルートを受信したルート リフレクタは、ネイバーに応じて、次のいずれかのアクションを実行します。

- EBGP スピーカーからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。
- 非クライアント ピアからのルートをすべてのクライアントにアドバタイズします。
- クライアントからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。したがって、クライアントは完全メッシュ型に接続にする必要はありません。

通常、クライアントのクラスタにはルート リフレクタが 1 つあり、各クラスタはルート リフレクタのルート ID によって識別されます。冗長性を高め、シングル ポイント障害を回避するには、クラスタに複数のルート リフレクタを設定する必要があります。このように設定した場合は、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるように、クラスタ内のすべてのルート リフレクタに同じクラスタ ID（4 バイト）を設定する必要があります。1 つのクラスタ内にあるルート リフレクタ全体は、完全メッシュ型に接続したうえで、一連のクライアント ピアおよび非クライアント ピアを共有する必要があります。

ルート リフレクタおよびクライアントを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** *ip-address* | *peer-group-name* **route-reflector-client**	ローカル ルータを BGP ルート リフレクタとして設定し、指定されたネイバーをクライアントとして設定します。
ステップ 4	**bgp cluster-id** *cluster-id*	（任意）クラスタに複数のルート リフレクタが存在する場合にクラスタ ID を設定します。
ステップ 5	**no bgp client-to-client reflection**	（任意）クライアント間のルート反映をディセーブルにします。デフォルトでは、ルート リフレクタ クライアントからのルートは、他のクライアントに反映されます。ただし、それらのクライアントが完全メッシュ型に接続されている場合、ルート リフレクタはルートをクライアントに反映させる必要はありません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp**	設定を確認します。送信元の ID およびクラスタリスト アトリビュートを表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート ダンプニングの設定

ルート フラップ ダンプニングを使用すると、インターネットワーク全体におけるフラッピング ルートの伝播を最小限に抑制できます。ルートがフラッピングと見なされるのは、そのルートの状態が、使用可能状態と使用不可能状態との間で繰り返し変化する場合です。ルート ダンプニングがイネーブルの場合は、フラッピングしているルートに *ペナルティ* 値が割り当てられます。ルートの累積ペナルティが、設定された制限値に達すると、ルートが稼動している場合であっても、BGP によりルートのアドバタイズが抑制されます。*再使用限度*は、ペナルティと比較される設定可能な値です。ペナルティが再使用限度より小さくなると、アップ状態のまま抑制されているルートのアドバタイズが再開されます。

IBGP によって学習されたルートには、ダンプニングが適用されません。このポリシーにより、IBGP ピアのペナルティが AS 外部のルートよりも大きくなることはありません。

BGP ルート ダンプニングを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp dampening**	BGP ルート ダンプニングをイネーブルにします。
ステップ 4	**bgp dampening** *half-life reuse suppress max-suppress* [**route-map** *map*]	（任意）ルート ダンプニング係数のデフォルト値を変更します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp flap-statistics** [{**regexp** *regexp*} | {**filter-list** *list*} | {*address mask* [**longer-prefix**]}]	（任意）フラッピングしているすべてのパスのフラップをモニタします。ルートの抑制が終了し、安定状態になると、統計情報は削除されます。
ステップ 7	**show ip bgp dampened-paths**	（任意）抑制されるまでの時間を含めて、ダンプニングされたルートを表示します。

	コマンド	目的
ステップ 8	**clear ip bgp flap-statistics** [{**regexp** *regexp*} | {**filter-list** *list*} | {*address mask* [**longer-prefix**]}	（任意）BGP フラップ統計情報を消去して、ルートがダンプニングされる可能性を小さくします。
ステップ 9	**clear ip bgp dampening**	（任意）ルート ダンプニング情報を消去して、ルートの抑制を解除します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

フラップ ダンプニングをディセーブルにするには、**no bgp dampening** ルータ コンフィギュレーション コマンドをキーワードなしで使用します。ダンプニング係数をデフォルト値に戻すには、**no bgp dampening** ルータ コンフィギュレーション コマンドに値を指定して実行します。

BGP のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。この作業は、特定の構造を持つ内容が無効になる場合、または無効である疑いがある場合に必要となります。

BGP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示することもできます。また、リソースの利用率を取得したり、ネットワークの問題点を解消するための情報を使用したりすることも可能です。さらには、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティング パスを検出することもできます。

表 36-8 は、BGP を消去および表示するために使用する特権 EXEC コマンドをまとめたものです。表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* を参照してください。

表 36-11　IP BGP の clear コマンドおよび show コマンド

コマンド	目的
clear ip bgp *address*	特定の BGP 接続をリセットします。
clear ip bgp *	すべての BGP 接続をリセットします。
clear ip bgp peer-group *tag*	BGP ピア グループのすべてのメンバーを削除します。
show ip bgp *prefix*	プレフィクスがアドバタイズされたピア グループ、またはピア グループに含まれないピアを表示します。ネクストホップやローカル プレフィクスなどのプレフィクス アトリビュートも表示されます。
show ip bgp cidr-only	サブネット マスクおよびスーパーネット ネットワーク マスクを含むすべての BGP ルートを表示します。
show ip bgp community [*community-number*] [**exact**]	指定されたコミュニティに属するルートを表示します。
show ip bgp community-list *community-list-number* [**exact-match**]	コミュニティ リストで許可されたルートを表示します。
show ip bgp filter-list *access-list-number*	指定された AS パス アクセス リストで一致したルートを表示します。
show ip bgp inconsistent-as	送信元の AS と整合しないルートを表示します。
show ip bgp regexp *regular-expression*	コマンドラインに入力された特定の正規表現と一致する AS パスを持ったルートを表示します。
show ip bgp	BGP ルーティング テーブルの内容を表示します。
show ip bgp neighbors [*address*]	各ネイバーとの BGP 接続および TCP 接続に関する詳細情報を表示します。

表 36-11　IP BGP の clear コマンドおよび show コマンド （続き）

コマンド	目的
show ip bgp neighbors [*address*] [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** *regular-expression* | **received-routes** | **routes**]	特定の BGP ネイバーから学習されたルートを表示します。
show ip bgp paths	データベース内のすべての BGP パスを表示します。
show ip bgp peer-group [*tag*] [**summary**]	BGP ピア グループに関する情報を表示します。
show ip bgp summary	すべての BGP 接続のステータスを表示します。

bgp log-neighbor changes ルータ コンフィギュレーション コマンドを使用して、BGP ネイバーをリセット、起動、またはダウンさせるときに生成されるメッセージのロギングをイネーブルにすることもできます。

ISO CLNS ルーティングの設定

International Organization for Standardization（ISO; 国際標準化機構）Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）プロトコルは、Open Systems Interconnection（OSI; 開放型システム間相互接続）モデルにおけるネットワーク レイヤの標準です。ISO ネットワーク アーキテクチャのアドレスは、Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレスおよび Network Entity Title（NET）と呼ばれます。OSI ネットワークの各ノードには、1 つまたは複数の NET が設定されています。さらに、各ノードには NSAP アドレスが多数存在します。

clns routing グローバル コンフィギュレーション コマンドを使用してコネクションレス型ルーティングをスイッチ上でイネーブルにすると、そのスイッチは転送の判断だけを行い、ルーティング関連の機能は使用しません。ダイナミック ルーティングの場合は、ルーティング プロトコルもイネーブルにする必要があります。スイッチは、ISO CLNS ネットワークの IS-IS ダイナミック ルーティング プロトコルをサポートしています。このルーティング プロトコルでは、*エリア*という概念が使用されます。エリア内では、すべてのルータがすべてのシステム ID の到達方法を認識しています。エリア間でも、いくつかのルータが適切なエリアに到達する方法を認識しています。IS-IS では、*ステーション ルーティング*（エリア内部）および*エリア ルーティング*（エリア間）という 2 つのレベルのルーティングがサポートされています。

ISO IGRP と IS-IS NSAP のアドレス指定方式の重要な違いは、エリア アドレスの定義にあります。どちらも、レベル 1 ルーティング（エリア内ルーティング）のシステム ID を使用しますが、アドレスをエリア ルーティング用に指定する方式が異なります。ISO IGRP NSAP アドレスには、*ドメイン*、*エリア*、*システム ID* という、互いに独立した 3 つのルーティング用フィールドが含まれています。一方、IS-IS アドレスには、*エリア*、*システム ID* という 2 つのフィールドが含まれていますが、このうちエリア フィールドは、ドメイン フィールドとエリア フィールドを連結して 1 つにしたフィールドです。

（注）　ISO CLNS の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide*』*Release 12.2* を参照してください。このセクションで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference*』*Release 12.2* を参照するか、IOS コマンド リファレンス マスター インデックスやオンライン検索を使用して情報を取得してください。

IS-IS ダイナミック ルーティングの設定

IS-IS は、ISO のダイナミック ルーティング プロトコルです。IS-IS をイネーブルにするには、IS-IS ルーティング プロセスを作成したうえで、それをネットワークではなく、特定のインターフェイスに割り当てる必要があります。マルチエリア IS-IS コンフィギュレーション構文を使用することにより、レイヤ 3 スイッチまたはルータごとに複数の IS-IS ルーティング プロセスを指定できます。次に、IS-IS ルーティング プロセスの各インスタンスにパラメータを設定します。

小規模な IS-IS ネットワークは、すべてのルータがネットワーク内に含まれる単独のエリアとして確立されます。IS-IS ネットワークは通常、規模が拡大するにつれて、すべてのエリアから接続された（次にローカル エリアに接続される）複数のレベル 2 ルータで構成されるバックボーン エリアに再構成されます。ローカル エリア内では、ルータはすべてのシステム ID への到達方法を認識しています。エリア間では、ルータはバックボーンへの到達方法を、バックボーン ルータはその他のエリアへの到達方法をそれぞれ認識しています。

ルータは、ローカル エリア内のルーティング（ステーション ルーティング）を実行するのに、レベル 1 の隣接関係を確立します。ルータは、レベル 1 エリア間のルーティング（エリア ルーティング）を実行するのに、レベル 2 の隣接関係を確立します。

各シスコ ルータは、最大 29 エリアのルーティングに参加でき、バックボーンでレベル 2 ルーティングを実行できます。通常、各ルーティング プロセスは 1 つのエリアに対応付けられます。デフォルトでは、設定済みのルーティング プロセスの最初のインスタンスはレベル 1 およびレベル 2 の両方のルーティングを実行します。これ以外にもルータ インスタンスを設定できますが、このインスタンスは自動的にレベル 1 エリアとして処理されます。IS-IS ルーティング プロセスの各インスタンスには、個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングの場合、各シスコ ユニットには最大 29 のレベル 1 エリアを定義できますが、レベル 2 ルーティングを実行するよう設定できるのは 1 つのプロセスに限られます。いずれかのプロセスに対してレベル 2 ルーティングを設定した場合、追加されたプロセスはすべて自動的にレベル 1 として設定されます。このプロセスは、同時にレベル 1 ルーティングを実行するように設定できます。レベル 2 ルーティングがルータ インスタンスとして望ましくない場合は、**is-type** グローバル コンフィギュレーション コマンドを使用して、レベル 2 機能を削除します。また、レベル 2 ルータとして異なるルータ インスタンスを設定する場合にも、**is-type** コマンドを使用します。

（注） IS-IS の詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「IP Routing Protocols」を参照してください。このセクションで説明するコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference*』*Release 12.2* を参照してください。

ここでは、IS-IS ルーティングの設定方法の概要を説明します。内容は次のとおりです。

- 「IS-IS のデフォルト設定」（P.36-69）
- 「NSF 認識」（P.36-69）
- 「IS-IS グローバル パラメータの設定」（P.36-72）
- 「IS-IS インターフェイス パラメータの設定」（P.36-74）

IS-IS のデフォルト設定

表 36-12　IS-IS のデフォルト設定

機能	デフォルト設定
Link-State PDU（LSP）エラーを無視	イネーブル。
IS-IS タイプ	従来型 IS-IS：ルータはレベル 1（ステーション）とレベル 2（エリア）の両方のルータとして動作。 マルチエリア IS-IS：IS-IS ルーティング プロセスの最初のインスタンスは、レベル 1 とレベル 2 の両方のルータとして動作。その他のインスタンスは、レベル 1 ルータ。
デフォルト情報の送信	ディセーブル。
IS-IS 隣接状態変更のログ	ディセーブル。
LSP 生成スロットリング タイマー	2 つの連続する LSP 生成間の最大インターバル：5 秒。 最初の LSP 生成遅延：50 ミリ秒。 最初と 2 番めの LSP 生成間のホールド タイム：5000 ミリ秒。
LSP 最大ライフタイム（リフレッシュなし）	LSP パケットが削除されるまで 1200 秒（20 分）。
LSP リフレッシュ インターバル	LSP リフレッシュを 900 秒（15 分）ごとに送信。
最大 LSP パケット サイズ	1497 バイト。
NSF[1] 認識	イネーブル[2]。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中、隣接する NSF 対応ルータからのパケットを転送し続けることが可能。
Partial Route Computation（PRC）スロットリング タイマー	最大 PRC 待機インターバル：5 秒。 トポロジ変更後の最初の PRC 計算遅延：2000 ミリ秒。 最初と 2 番めの RPC 計算間のホールド タイム：5000 ミリ秒。
パーティション回避	ディセーブル。
パスワード	エリア パスワードまたはドメイン パスワードの定義なし。認証はディセーブル。
set-overload-bit	ディセーブル。イネーブルの場合に引数が入力されなければ、過負荷ビットが即座に設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになる。
Shortest Path First（SPF）スロットリング タイマー	連続する SFP 間の最大インターバル：10 秒。 トポロジ変更後の最初の SFP 計算遅延：5500 ミリ秒。 最初と 2 番めの SFP 計算間のホールド タイム：5500 ミリ秒。
サマリー アドレス	ディセーブル。

1. NSF = Nonstop Forwarding（ノンストップ フォワーディング）
2. IS-IS NSF 認識は、メトロ IP アクセス イメージを実行しているスイッチ上の IPv4 に対してイネーブルになっています。

NSF 認識

メトロ IP アクセス イメージの IPv4 に対しては、統合型 IS-IS NSF 認識機能がサポートされています。この機能により、NSF 認識 Customer-Premises Equipment（CPE; 顧客宅内機器）ルータが、NSF 対応のルータにパケットの NSF を実行させることができます。ローカル ルータは NSF を必ずしも実行す

る必要はありませんが、その NSF 認識により、スイッチオーバー プロセスの間、隣接する NSF 対応ルータ上のルーティング データベースおよびリンクステート データベースの整合性と信頼性を維持できます。

この機能は自動的にイネーブルになるため、設定は必要ありません。この機能に関する詳細については、次の URL にある『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a00801541c7.shtml

IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにする際は、まず各ルーティング プロセスの名前および NET を指定します。次に、インターフェイス上で IS-IS ルーティングをイネーブルにして、ルーティング プロセスの各インスタンスにエリアを指定します。

IS-IS をイネーブルにして、IS-IS ルーティング プロセスの各インスタンスにエリアを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clns routing**	スイッチ上で ISO コネクションレス型ルーティングをイネーブルにします。
ステップ 3	**router isis** [*area tag*]	指定されたルーティング プロセスに対し IS-IS ルーティングをイネーブルにして、IS-IS ルーティング コンフィギュレーション モードを開始します。 （任意）引数 *area tag* を使用して、IS-IS ルータが割り当てられるエリアを指定します。複数の IS-IS エリアを設定するときは、値を入力する必要があります。 設定された最初の IS-IS インスタンスは、デフォルトでレベル 1 とレベル 2 です。それ以降のインスタンスは、自動的にレベル 1 となります。**is-type** グローバル コンフィギュレーション コマンドを使用すると、ルーティングのレベルを変更できます。
ステップ 4	**net** *network-entity-title*	ルーティング プロセスの NET を設定します。マルチエリア IS-IS を設定する場合は、ルーティング プロセスごとに NET を指定します。NET およびアドレスの名前を指定できます。
ステップ 5	**is-type** {**level-1** | **level-1-2** | **level-2-only**}	（任意）レベル 1（ステーション）ルータ、マルチエリア ルーティング用のレベル 2（エリア）ルータ、またはその両方（デフォルト）として機能するように、ルータを設定できます。 • **level-1**：ステーション ルータとしてだけ機能します。 • **level-1-2**：ステーション ルータおよびエリア ルータの両方として機能します。 • **level-2**：エリア ルータとしてだけ機能します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *interface-id*	IS-IS をルーティングするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力して、インターフェイスをレイヤ 3 モードにします。
ステップ 8	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 9	**ip router isis** [*area tag*]	インターフェイスの ISO CLNS に IS-IS ルーティング プロセスを設定し、そのルーティング プロセスにエリア指定子を関連付けます。
ステップ 10	**clns router isis** [*area tag*]	インターフェイスの ISO CLNS をイネーブルにします。
ステップ 11	**ip address** *ip-address-mask*	インターフェイスの IP アドレスを定義します。いずれか 1 つのインターフェイスが IS-IS ルーティング用に設定されている場合、IS-IS 対応エリアのすべてのインターフェイスに IP アドレスが必要となります。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show isis** [*area tag*] **database detail**	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IS-IS ルーティングをディセーブルにするには、**no router isis** *area-tag* ルータ コンフィギュレーション コマンドを使用します。

次に、IP ルーティング プロトコルとして従来型 IS-IS を実行するように、3 つのルータを設定する例を示します。従来型 IS-IS では、すべてのルータがレベル 1 およびレベル 2 のルータとして機能します（デフォルト）。

ルータ A

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000a.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ B

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000b.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ C

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000c.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

IS-IS グローバル パラメータの設定

次に、任意で設定可能な一部の IS-IS グローバル パラメータについて説明します。

- ルート マップにより制御されるデフォルト ルートを設定することで、IS-IS ルーティング ドメイン内にデフォルト ルートを強制的に 設定できます。また、ルート マップで設定可能なその他のフィルタリング オプションも指定できます。
- ルータに対しては、内部チェックサム エラーとともに受信した IS-IS LSP を無視するよう設定できるほか、破損した LSP を消去するよう設定することもできます。消去された LSP は、その発信側で再生成されます。
- エリアおよびドメインには、パスワードを割り当てることができます。
- サマリー アドレス（経路集約）によりルーティング テーブルで表示される集約アドレスを作成できます。他のルーティング プロトコルから学習されたルートも集約できます。サマリーのアドバタイズには、対象となる全ルートのメトリックの中で最小のメトリックが使用さます。
- 過負荷ビットを設定できます。
- LSP リフレッシュ インターバル、およびリフレッシュなしで LSP がルータ データベース内に存続できる最大時間を設定できます。
- LSP 生成、SPF 計算、および PRC 計算のスロットリング タイマーを設定できます。
- IS-IS 隣接状態が変更（アップまたはダウン）した場合に、ログ メッセージが生成されるようスイッチを設定できます。
- ネットワーク内のリンクの MTU サイズが 1500 バイト未満である場合は、ルーティングが引き続き実行されるように LSP MTU を小さくできます。
- partition avoidance ルータ コンフィギュレーション コマンドを使用すると、レベル 1/ レベル 2 境界ルータ、隣接するレベル 1 ルータ、またはエンド ホストの間ですべての回線が切断された場合にエリアが分割されないようにできます。

IS-IS パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clns routing**	スイッチ上で ISO コネクションレス型ルーティングをイネーブルにします。
ステップ 3	**router isis**	IS-IS ルーティング プロトコルを指定して、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**default-information originate** [**route-map** *map-name*]	（任意）IS-IS ルーティング ドメイン内にデフォルト ルートを強制的に設定します。**route-map** *map-name* を入力した場合に、ルート マップが満たされていると、ルーティング プロセスではデフォルト ルートが生成されます。
ステップ 5	**ignore-lsp-errors**	（任意）内部チェックサム エラーを含む LSP を、消去せず無視するようルータを設定します。このコマンドはデフォルトでイネーブルです（破損した LSP は廃棄されます）。破損した LSP を消去するには、**no ignore-lsp-errors** ルータ コンフィギュレーション コマンドを入力します。
ステップ 6	**area-password** *password*	（任意）レベル 1（ステーション ルータ レベル）の LSP に挿入されるエリア認証パスワードを設定します。
ステップ 7	**domain-password** *password*	（任意）レベル 2（エリア ルータ レベル）の LSP に挿入されるルーティング ドメイン認証パスワードを設定します。

	コマンド	目的
ステップ 8	**summary-address** *address mask* [**level-1** | **level-1-2** | **level-2**]	（任意）所定レベルのアドレスのサマリーを作成します。
ステップ 9	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}]	（任意）ルータに問題がある場合、他のルータが SFP 計算の際にこのルータを無視するように、過負荷ビット（hippity ビット）を設定します。 • （任意）**on-startup**：起動時にだけ、過負荷ビットを設定します。**on-startup** が指定されない場合、過負荷ビットが即座に設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになります。**on-startup** が指定された場合は、秒数または **wait-for-bgp** を入力する必要があります。 • *seconds*：キーワード **on-startup** が設定されている場合、システム起動時に過負荷ビットが設定され、この秒数の間設定されたままになります。指定できる範囲は 5 ～ 86400 秒です。 • **wait-for-bgp**：キーワード **on-startup** が設定されている場合、システム起動時に過負荷ビットが設定され、BGP がコンバージするまで設定されたままになります。BGP がコンバージしたことが IS-IS に通知されない場合、過負荷ビットは 10 分後に無効となります。
ステップ 10	**lsp-refresh-interval** *seconds*	（任意）LSP リフレッシュ インターバルを秒単位で設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルトでは、LSP リフレッシュは 900 秒（15 分）ごとに送信されます。
ステップ 11	**max-lsp-lifetime** *seconds*	（任意）LSP パケットがリフレッシュされないままルータ データベース内に存続する最大時間を設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 1200 秒（20 分）です。指定された時間が経過すると、LSP パケットは削除されます。
ステップ 12	**lsp-gen-interval** [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*]	（任意）IS-IS LSP 生成スロットリング タイマーを設定します。 • *lsp-max-wait* : LSP が生成されてから次の LSP が生成されるまでの最大時間間隔（秒）を指定します。指定できる範囲は 1 ～ 120 で、デフォルトは 5 です。 • *lsp-initial-wait*：最初の LSP 生成遅延（ミリ秒）を指定します。指定できる範囲は 1 ～ 10000 で、デフォルト値は 50 です。 • *lsp-second-wait* ：LSP が最初に生成されてからその次に生成されるまでのホールド タイム（ミリ秒）を指定します。指定できる範囲は 1 ～ 10000 で、デフォルト値は 5000 です。
ステップ 13	**spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]	（任意）IS-IS SPF スロットリング タイマーを設定します。 • *spf-max-wait*：連続する SFP 間（秒）の最大時間間隔を指定します。指定できる範囲は 1 ～ 120 で、デフォルトは 10 です。 • *spf-initial-wait*：トポロジが変更されてから最初の SFP 計算が行われるまでの時間（ミリ秒）を指定します。指定できる範囲は 1 ～ 10000 で、デフォルト値は 5500 です。 • *spf-second-wait* ：SFP 計算が最初に行われてからその次に行われるまでのホールド タイム（ミリ秒）を指定します。指定できる範囲は 1 ～ 10000 で、デフォルト値は 5500 です。

	コマンド	目的
ステップ 14	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*]	（任意）IS-IS PRC スロットリング タイマーを設定します。 • *prc-max-wait*：PRC 計算が行われてから次の PRC 計算が行われるまでの最大時間間隔（秒）を指定します。指定できる範囲は 1 ～ 120 で、デフォルトは 5 です。 • *prc-initial-wait*：トポロジが変更されてから最初の SFP 計算が行われるまでの時間（ミリ秒）を指定します。指定できる範囲は 1 ～ 10000 で、デフォルトは 2000 です。 • *prc-second-wait*：PRC 計算が最初に行われてからその次に行われるまでのホールド タイム（ミリ秒）を指定します。指定できる範囲は 1 ～ 10000 で、デフォルトは 5000 です。
ステップ 15	**log-adjacency-changes** [**all**]	（任意）IS-IS 隣接状態変更をログに記録するようルータを設定します。End System-to-Intermediate System PDU および Link State Packet（LSP）など、IS-IS Hello に関連しないイベントにより生成されたすべての変更をログに記録するには、**all** を入力します。
ステップ 16	**lsp-mtu** *size*	（任意）最大 LSP パケット サイズをバイト単位で指定します。指定できる範囲は 128 ～ 4352 バイトで、デフォルトは 1497 バイトです。 **（注）** ネットワーク内の任意のリンクで MTU サイズが縮小された場合は、ネットワーク内のすべてのルータで LSP MTU サイズを変更する必要があります。
ステップ 17	**partition avoidance**	（任意）境界ルータ、すべての隣接レベル 1 ルータ、およびエンド ホストの間で、フル接続が切断された場合、IS-IS レベル 1/ レベル 2 境界ルータがレベル 1 エリア プレフィクスをレベル 2 バックボーンにアドバタイズしないようにします。
ステップ 18	**end**	特権 EXEC モードに戻ります。
ステップ 19	**show clns**	設定を確認します。
ステップ 20	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト ルートの生成をディセーブルにするには、**no default-information originate** ルータ コンフィギュレーション コマンドを使用します。パスワードをディセーブルにするには、**no area-password** ルータ コンフィギュレーション コマンドまたは **no domain-password** ルータ コンフィギュレーション コマンドを使用します。LSP MTU 設定をディセーブルにする場合はは、**no lsp mtu** ルータ コンフィギュレーション コマンドを使用します。サマリー アドレス割り当て、LSP リフレッシュ インターバル、LSP ライフタイム、LSP タイマー、SFP タイマー、および PRC タイマーをデフォルト状態に戻すには、これらのコマンドの **no** 形式を使用します。出力形式をディセーブルにするには、**no partition avoidance** ルータ コンフィギュレーション コマンドを使用します。

IS-IS インターフェイス パラメータの設定

必要に応じて、特定のインターフェイス固有の IS-IS パラメータを、付加されている他のルータとは別に設定できます。ただし、一部の値（乗数および時間間隔など）をデフォルトから変更するには、複数のルータおよびインターフェイス上でもこれらの値を変更する必要があります。ほとんどのインターフェイス パラメータは、レベル 1、レベル 2、またはその両方で設定できます。

次に、設定可能なインターフェイス レベル パラメータの一部を示します。

- インターフェイスのデフォルト メトリック。IS-IS メトリックの値として使用され、QoS ルーティングが実行されない場合に割り当てられます。

- hello インターバル（インターフェイスから送信される hello パケットの間隔）またはデフォルトの hello パケット乗数。インターフェイスにおいて、IS-IS hello パケットにより送信されるホールド タイムを決定する際に使用されます。このホールド タイムにより、ネイバーがダウンしていると宣言するまでに、別の hello パケットを待機する時間が決まります。これにより、障害があるリンクまたはネイバーの検出速度も決定されるため、ルートを再計算できるようになります。hello パケットの消失や、IS-IS 隣接関係の障害が頻発する場合は、hello 乗数を変更します。hello 乗数を大きくし、それに対応して hello インターバルを小さくすると、リンク障害の検出に要する時間を増やすことなく、hello プロトコルの信頼性を高めることができます。
- その他の時間間隔。
  - Complete Sequence Number PDU（CSNP）インターバル：CSNP は、データベースの同期を維持するため、指定ルータにより送信されます。
  - 再送信インターバル：ポイントツーポイント リンクの IS-IS LSP の再送信間隔です。
  - IS-IS LSP 再送信スロットル インターバル：IS-IS LSP がポイントツーポイント リンクで再送信される最大レート（パケット間のミリ秒数）です。このインターバルは、連続して*同じ* LSP が再送信される場合の送信間隔を表す再送信インターバルとは異なります。
- 代表ルータの選択プライオリティ。マルチアクセス ネットワークで必要な隣接数を減らし、ひいてはルーティング プロトコル トラフィックの量およびトポロジ データベースのサイズを軽減できます。
- インターフェイス回線タイプ。指定されたインターフェイス上のネイバーに必要な隣接関係のタイプです。
- インターフェイスのパスワード認証。

IS-IS インターフェイス パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力して、インターフェイスをレイヤ 3 モードにします。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**isis metric** *default-metric* [**level-1** | **level-2**]	（任意）指定されたインターフェイスのメトリック（またはコスト）を設定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 10 です。レベルが入力されない場合は、レベル 1 ルータおよびレベル 2 ルータの両方にデフォルト値が適用されます。
ステップ 5	**isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**]	（任意）スイッチが hello パケットを送信する時間間隔を指定します。デフォルトでは、hello インターバル *seconds* の 3 倍の値が、送信される hello パケットの *holdtime* としてアドバタイズされます。hello インターバルが短くなると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。 • **minimal**：ホールド タイムが 1 秒になるように、システムが hello 乗数に基づいて hello インターバルを計算するようにします。 • *seconds*：指定できる範囲は 1 ～ 65535 です。デフォルトは 10 秒です。

	コマンド	目的
ステップ 6	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**]	（任意）ルータが隣接装置のダウンを宣言するためにネイバーで消失すべき IS-IS hello パケット数を指定します。指定できる範囲は 3 ～ 1000 です。デフォルト値は 3 です。使用する hello 乗数が比較的小さいと、コンバージェンス時間は短縮されますが、ルーティングがより不安定になる可能性があります。
ステップ 7	**isis csnp-interval** *seconds* [**level-1** | **level-2**]	（任意）インターフェイスに IS-IS CSNP インターバルを設定します。指定できる範囲は 0 ～ 65535 です。デフォルト値は 10 秒です。
ステップ 8	**isis retransmit-interval** *seconds*	（任意）ポイントツーポイント リンクの IS-IS LSP の再送信間隔を秒単位で設定します。指定する値は、ネットワーク上にある任意の 2 つのルータ間における予測ラウンドトリップ遅延よりも大きい整数であることが必要です。指定できる範囲は 0 ～ 65535 です。デフォルト値は 5 秒です。
ステップ 9	**isis retransmit-throttle-interval** *milliseconds*	（任意）IS-IS LSP 再送信スロットル インターバルを設定します。これは、IS-IS LSP がポイントツーポイント リンク上で再送信される最大レート（パケット間のミリ秒数）です。指定できる範囲は 0 ～ 65535 です。デフォルト値は、**isis lsp-interval** コマンドにより指定されます。
ステップ 10	**isis priority** *value* [**level-1** | **level-2**]	（任意）代表ルータの選択に使用するプライオリティを設定します。指定できる範囲は 0 ～ 127 です。デフォルト値は 64 です。
ステップ 11	**isis circuit-type** {**level-1** | **level-1-2** | **level-2-only**}	（任意）指定されたインターフェイス上のネイバーで必要な隣接関係のタイプを設定します（インターフェイスの回線タイプを指定します）。 • **level-1**：このノードとネイバーに共通のエリア アドレスが少なくとも 1 つある場合、レベル 1 隣接関係が確立されます。 • **level-1-2**：ネイバーがレベル 1 およびレベル 2 の両方として設定されており、かつ共通のエリアが少なくとも 1 つ存在する場合、レベル 1 およびレベル 2 の隣接関係が確立されます。共通のエリアがない場合は、レベル 2 隣接関係が確立されます。これはデフォルト設定です。 • **level 2**：レベル 2 隣接関係が確立されます。ネイバー ルータがレベル 1 ルータである場合、隣接関係は確立されません。
ステップ 12	**isis password** *password* [**level-1** | **level-2**]	（任意）インターフェイスの認証パスワードを設定します。デフォルトでは、認証はディセーブルに設定されています。レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 ルーティング用またはレベル 2 ルーティング用のパスワードだけがイネーブルになります。レベルを指定しない場合のデフォルトはレベル 1 およびレベル 2 です。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show clns interface** *interface-id*	設定を確認します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

IS-IS のモニタリングおよびメンテナンス

CLNS キャッシュのすべての内容または特定のネイバーまたはルートの情報を削除できます。ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の CLNS または IS-IS の統計情報を表示することもできます。また、特定のインターフェイス、フィルタ、またはネイバーに関する情報も表示できます。

表 36-13 は、ISO CLNS および IS-IS ルーティングを消去および表示するための特権 EXEC コマンドをまとめたものです。出力フィールドの詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference*』*Release 12.2* を参照するか、IOS コマンド リファレンス マスター インデックスやオンライン検索を使用して情報を取得してください。

表 36-13　ISO CLNS および IS-IS の clear コマンドおよび show コマンド

コマンド	目的
clear clns cache	CLNS ルーティング キャッシュを消去して、再初期化します。
clear clns es-neighbors	隣接データベースから End System（ES; エンド システム）ネイバー情報を削除します。
clear clns is-neighbors	隣接データベースから Intermediate System（IS; 中継システム）ネイバー情報を削除します。
clear clns neighbors	隣接データベースから CLNS ネイバー情報を削除します。
clear clns route	ダイナミックに取得された CLNS ルーティング情報を削除します。
show clns	CLNS ネットワークについての情報を表示します。
show clns cache	CLNS ルーティング キャッシュのエントリを表示します。
show clns es-neighbors	関連するエリアを含む、ES ネイバー エントリを表示します。
show clns filter-expr	フィルタ式を表示します。
show clns filter-set	フィルタ セットを表示します。
show clns interface [*interface-id*]	各インターフェイスの CLNS 固有の情報または ES-IS 情報を表示します。
show clns neighbor	IS-IS ネイバーについての情報を表示します。
show clns protocol	このルータの IS-IS ルーティング プロセスまたは ISO IGRP ルーティング プロセスごとにプロトコル固有の情報を表示します。
show clns route	このルータがルーティング方法を認識している CLNS パケットの宛先をすべて表示します。
show clns traffic	このルータが認識している CLNS パケットの情報を表示します。
show ip route isis	IS-IS IP ルーティング テーブルの現在の状態を表示します。
show isis database	IS-IS リンクステート データベースを表示します。
show isis routes	IS-IS レベル 1 ルーティング テーブルを表示します。
show isis spf-log	IS-IS の SPF 計算履歴を表示します。
show isis topology	すべてのエリア内の接続されたルータすべてのリストを表示します。
show route-map	設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。
trace clns *destination*	ネットワークのパケットが、指定された宛先へ到達するまでに経由するパスを検出します。
which-route {*nsap-address* | *clns-name*}	指定された CLNS 宛先が検出されたルーティング テーブルを表示します。

BFD の設定

BFD プロトコルを使用すると、さまざまなメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルに合せて、フォワーディング パスの障害を瞬時に検出できます。BFD プロトコルは、2 つのシステム間で転送されるすべてのデータ プロトコルの上位においてユニキャスト（ポイントツーポイント）モードで動作し、直接接続されたネイバー間の IPv4 接続を追跡する役割を持ちます。BFD パケットは、宛先のポート番号 3784 または 3785 とともに UDP パケットでカプセル化されます。

EIGRP、IS-IS、および OSPF の導入下では、BFD の次善手段として、改良された障害検出メカニズムを使用できます。この場合、EIGRP タイマー、IS-IS タイマー、および OSPF タイマーの値を小さくすることで 1 ～ 2 秒間隔での障害検出が可能ですが、BFD を使用すれば障害検出の間隔は 1 秒未満です。BFD は、これらのタイマーの値を小さくした場合に比べて CPU への負荷が小さいほか、特定のルーティング プロトコルとは連動していないため、さまざまなルーティング プロトコルに対応できる汎用的で一貫性のある障害検出メカニズムとして使用できます。

BFD セッションを作成するには、ピアとなる両方のシステム（BFD ピア）上に BFD を設定する必要があります。BFD ピア上において、インターフェイス レベルおよびルーティング プロトコル レベルで BFD をイネーブルにすると、BFD セッションを作成できます。BFD タイマーがネゴシエートされると、BFD ピアでは、そのネゴシエートされた間隔で制御パケットが相互に送信されます。ネイバーが直接接続されていないと、BFD ネイバー登録は拒否されます。

図 36-6 は、OSPF および BFD が稼動する 2 つのルータで構成された単純なネットワークを表したものです。OSPF によりネイバーが検出されると（1）、ODFP 隣接ルータとの BFD ネイバー セッションが開始されるよう BFD プロセスに要求が送信され（2）、BFD ネイバー セッションが確立されます（3）。

図 36-6　BFD セッションの確立

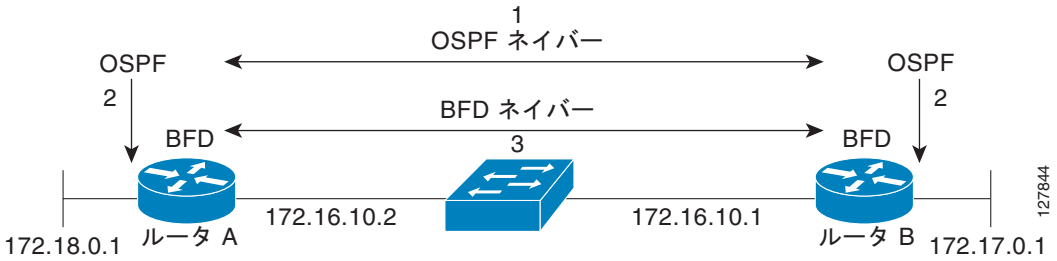
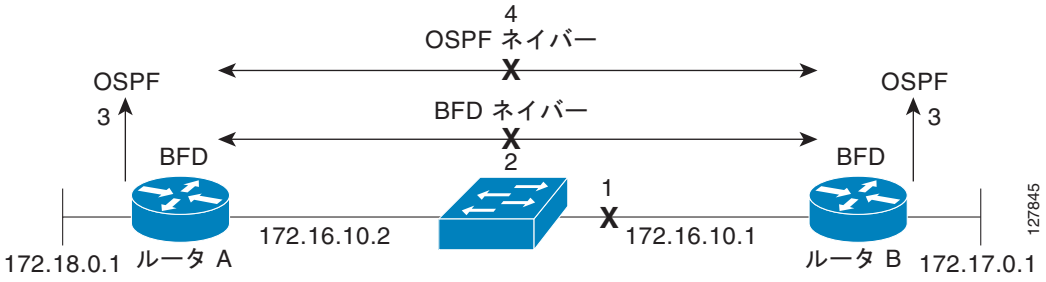


図 36-7 は、ネットワーク内で障害が発生した場合（1）の動作を示したものです。この場合、OSPF ネイバーとの BFD ネイバー セッションは終了します（2）。BFD から OSPF プロセスへは、その BFD ネイバーが到達不能になったことが通知され、OSFP プロセスによって OSPF ネイバー関係が解消されます（4）。代替パスが使用できる場合は、ルータによりそのパス上でコンバージェンスが開始されます。

図 36-7　OSPF ネイバー関係の解消



BFD クライアントでは、ネイバーを BFD に登録するためのルーティング プロトコルが実行されます。スイッチでは、ISIS、OSPF v1 および v2、BGP、EIGRP、および HSRP の各クライアントがサポートされており、複数のクライアント プロトコルに対して、1 つの BFD セッションを共用できます。たとえば、同一ピアへの同一リンク上で OSPF と EIGRP が稼動しているネットワークでは、BFD セッションを 1 つだけ作成すれば、情報は 2 つのルーティング プロトコルで共有されます。

スイッチでは、BFD バージョン 0 およびバージョン 1 がサポートされています。BFD ネイバーではバージョンのネゴシエーションが自動的に行われ、プロトコルは常に新しい方のバージョンで実行されます。デフォルトのバージョンはバージョン 1 です。

デフォルトの場合、BFD ネイバーは、制御パケットとエコー パケットの両方を交換することで、フォワーディングの障害検出を行います。スイッチでは、設定された BFD インターバル（50 ～ 999 ミリ秒）でエコー パケットが送信されます。また制御パケットは、BFD のスロータイマー レート（1000 ～ 3000 ミリ秒）で送信されます。

障害発生率の検出は、BFD エコー モードを使用することでより高速化できます。BFD エコー モードは、BFD セッションを設定すればデフォルトでイネーブルになります。このモードの場合、スイッチは BFD ソフトウェア レイヤからエコー パケットを送信し、BFD ネイバーは、高速スイッチング レイヤを介してそのエコー パケットに応答します。エコー パケットは、BFD ネイバーのソフトウェア レイヤには到達せず、障害検出を行うフォワーディング パスを介して戻されます。**bfd interval** インターフェイス コンフィギュレーション コマンドを使用すると、BFD インターフェイスから BFD エコー パケットが送信される頻度を設定できます。

帯域幅の使用量を抑える場合は、**no bfd echo** インターフェイス コンフィギュレーション コマンドを使用して、エコー パケットの送信をディセーブルにします。エコー モードがディセーブルの場合、フォワーディングの障害検出には制御パケットが使用されます。制御パケットは、設定されたスロータイマー レートで交換されます。そのため、障害検出に要する時間が長くなる場合があります。スロータイマー レートの設定は、**bfd slow-timer** グローバル コンフィギュレーション コマンドで行います。設定できる範囲は 1000 ～ 3000 ミリ秒で、デフォルトは 1000 ミリ秒です。

エコー処理は、BFD ネイバーの設定とは独立したスイッチ インターフェイスで、イネーブルとディセーブルを切り替えられます。エコー モードをディセーブルにしても、インターフェイスからのエコー パケット送信がディセーブルになるだけです。エコー パケットを受信する高速スイッチング レイヤでは常に、エコー パケットが送信者へ返送されます。

スイッチ上で BFD を稼動させるためには、BFD インターフェイス上で基本的な BFD インターバル パラメータを設定し、スイッチ上でルーティングをイネーブルにしたあと、BFD のルーティング プロトコル クライアントを少なくとも 1 つイネーブルにする必要があります。また、参加するスイッチ上で Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）がイネーブル（デフォルト）になっていることを確認する必要もあります。

設定の詳細については、次の URL にある『Bidirectional Forwarding Detection』フィーチャ モジュールを参照してください。

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

コマンドの詳細については、次の URL にある『Master Index to the Cisco IOS Command List for Release 12.4』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

ここでは、BFD の設定について説明します。

- 「BFD のデフォルト設定」（P.36-80）
- 「BFD のデフォルト設定に関する注意事項」（P.36-80）
- 「インターフェイスに対する BFD セッション パラメータの設定」（P.36-80）
- 「BFD ルーティング プロトコル クライアントのイネーブル化」（P.36-82）

BFD のデフォルト設定

BFD セッションは設定されていません。BFD はすべてのインターフェイス上でディセーブルです。

BFD が設定されている場合、デフォルトはバージョン 1 です。ただし、バージョンはスイッチによりネゴシエートされます。バージョン 0 もサポートされています。

スタンバイ BFD（HSRP 用）はデフォルトでイネーブルに設定されています。

BFD セッションの設定時には非同期 BFD エコー モードがイネーブルになります。

BFD のデフォルト設定に関する注意事項

スイッチで同時に使用できる BFD セッションの数は 最大で 28 です。

スイッチ上で BFD を実行する手順は次のとおりです。

- BFD セッションを実行する各インターフェイス上で、基本的な BFD インターバル パラメータを設定します。
- スイッチ上でルーティングをイネーブルにします。BFD を設定する際は必ずしもルーティングをイネーブルにする必要はありませんが、BFD セッションをアクティブにするには、スイッチおよび BFD インターフェイスにおいてルーティングがイネーブルになっている必要があります。
- BFD のルーティング プロトコル クライアントを少なくとも 1 つイネーブルにします。使用するルーティング プロトコルに対しては、高速コンバージェンスを実装することを推奨します。高速コンバージェンスの詳細については、この章または『*Cisco IOS IP Configuration Guide*』*Release 12.2* の IP ルーティングに関する項を参照してください。

（注）　ルーティング プロトコル コマンドを設定する前に、インターフェイス上で BFD インターバル パラメータを設定することを推奨します（特に EIGRP を使用する場合）。

参加するスイッチ上で、IP ルーティングのほかに CEF もイネーブル（デフォルト）になっていることを確認します。

BFD は、ルーティング インターフェイスとして設定された物理インターフェイス上でサポートされます。レイヤ 2 インターフェイス、疑似回線、スタティック ルート、SVI インターフェイス、およびポート チャネルではサポートされていません。

レイヤ 2 ポート上に BFD インターフェイス コマンドを設定できますが、そのインターフェイス上で BFD セッションが動作するためには、それをレイヤ 3 インターフェイスとして設定し（no switchport）、さらに IP アドレスを割り当てる必要があります。

HSRP BFD ではデフォルトで、スタンバイ BFD がすべてのインターフェイス上でグローバルにイネーブル化されています。いずれかのインターフェイス上でスタンバイ BFD をディセーブルにした場合、BFD セッションをアクティブにするには、スタンバイ BFD をいったんグローバルにディセーブル化したあと、再度グローバルにイネーブル化する必要があります。

BFD エコー モード（デフォルト）を使用するには、BFD インターフェイス上で **no ip redirects** インターフェイス コンフィギュレーション コマンドを入力し、ICMP リダイレクト メッセージの送信をディセーブルにすることを推奨します。

インターフェイスに対する BFD セッション パラメータの設定

インターフェイス上で BFD セッションを開始するには、事前にそのインターフェイスをレイヤ 3 モードにしたうえで、ベースライン BFD パラメータを設定する必要があります。

（注）　レイヤ 2 インターフェイス上で BFD を設定できますが、BFD セッションを開始するためには、双方のインターフェイスをレイヤ 3 モードにし、スイッチ上でルーティングをイネーブルにする必要があります。

BFD セッションに参加するインターフェイス上で BFD を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	BFD セッションに使用するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。BFD がサポートされるのは物理インターフェイスだけです。
ステップ 3	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）および Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブル、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルです。
ステップ 4	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します。
ステップ 5	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 6	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *value*	インターフェイス上でエコー パケットごとに BFD パラメータを設定します。 • **interval**：BFD エコー パケットを BFD ピアに送信する時間間隔を指定します。指定できる範囲は 50 ～ 999 ミリ秒（ms）です。 • **min_rx**：BFD ピアから返送された BFD エコー パケットを受信する時間間隔を指定します。指定できる範囲は 50 ～ 999 ミリ秒です。 • **multiplier**：BFD ピアが使用不能になったことを宣言し、障害の発生を他の BFD に通知するための基準として、その BFD ピアにおける BFD エコー パケットの連続消失数を指定します。指定できる範囲は 3 ～ 50 です。 **（注）**　ベースライン BFD パラメータにはデフォルト値はありません。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**show bfd neighbor detail**	（任意）ネイバーによるセッション作成時に、最終的に設定された値またはネゴシエートされた値を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BFD パラメータの設定を削除するには、**no bfd interval** インターフェイス コンフィギュレーション コマンドを使用します。

BFD ルーティング プロトコル クライアントのイネーブル化

インターフェイス上で BFD パラメータの設定が完了すると、1 つまたは複数のルーティング プロトコルに対して BFD セッションを開始できます。最初にスイッチ上で **ip routing** グローバル コンフィギュレーション コマンドを入力して、ルーティングをイネーブルにする必要があります。ただし、インターフェイス上で BFD セッションを開始する方法は複数あり、どの方法を使用するかはルーティング プロトコルによって異なります。

- 「OSFP に対する BFD の設定」（P.36-82）
- 「IS-IS に対する BFD の設定」（P.36-83）
- 「BGP に対する BFD の設定」（P.36-85）
- 「EIGRP に対する BFD の設定」（P.36-86）
- 「HSRP に対する BFD の設定」（P.36-86）

OSFP に対する BFD の設定

OSPF 用の BFD セッションを開始するには、参加するすべてのデバイス上で OSPF が稼動している必要があります。BFD の OSPF サポートをイネーブルにする場合は、それをすべての OSPF インターフェイス上、またはいずれか 1 つ以上の OSPF インターフェイス上でイネーブルにします。

OSFP BFD のグローバルな設定

OSFP BFD をグローバルに設定し、必要に応じてそれを特定のインターフェイス上でディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process- id*	OSPF プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bfd all-interfaces**	OSPF ルーティング プロセスに対応付けられているすべてのインターフェイス上で BFD をグローバルにイネーブル化します。
ステップ 4	**exit**	（任意）1 つまたは複数の OSPF インターフェイス上で BFD をディセーブルにする場合は、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	（任意）インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip ospf bfd disable**	（任意）指定した OSPF インターフェイス上で BFD をディセーブルにします。BFD セッションを実行しないすべての OSPF インターフェイスに対して、ステップ 5 および 6 を繰り返し実行します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show bfd neighbors** [**detail**]	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

すべてのインターフェイス上で OSPF BFD をディセーブルにするには、**no bfd all-interfaces** ルータ コンフィギュレーション コマンドを使用します。いずれかのインターフェイス上で OSPF BFD をディセーブルにする場合は、そのインターフェイス上で **no ip osfp bfd** インターフェイス コンフィギュレーション コマンドまたは **ip ospf bfd disable** インターフェイス コンフィギュレーション コマンドを実行します。

一部のインターフェイス上でだけ OSPF BFD を稼動させる場合は、OSPF BFD をグローバルにイネーブル化する代わりに、それらのインターフェイス上で **ip ospf bfd** インターフェイス コンフィギュレーション コマンドを実行することもできます。詳細については、次に説明する手順を参照してください。

（注）　レイヤ 2 インターフェイス上で OSPF BFD を設定しても、その設定は認識されません。

次に、すべての OSPF インターフェイス上で OSPF BFD を設定する例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# bfd all-interfaces
Switch(config-router)# exit
```

インターフェイス上での OSPF BFD 設定

個々のインターフェイス上で OSPF BFD を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process- id*	OSPF プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip ospf bfd**	指定された OSPF インターフェイス上で BFD をイネーブルにします。BFD セッションを実行するすべての OSPF インターフェイスに対して、ステップ 3 および 4 を繰り返し実行します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show bfd neighbors** [**detail**]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

いずれかのインターフェイス上で OSPF BFD をディセーブルにするには、そのインターフェイス上で **no ip osfp bfd** インターフェイス コンフィギュレーション コマンドまたは **ip ospf bfd disable** インターフェイス コンフィギュレーション コマンドを実行します。

次に、単独のインターフェイス上で OSPF BFD を設定する例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip ospf bfd
```

IS-IS に対する BFD の設定

IS-IS 用の BFD セッションを開始する場合は、BFD に参加するすべてのデバイス上で、IS-IS が稼動している必要があります。BFD の IS-IS サポートをグローバルにイネーブルにする場合は、それをすべての IS-IS インターフェイス上、またはいずれか 1 つ以上の IS-IS インターフェイス上でイネーブルにします。

IS-IS BFD のグローバルな設定

IS-IS BFD をグローバルに設定し、必要に応じてそれを特定のインターフェイス上でディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router is-is** *area-tag*	IS-IS プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bfd all-interfaces**	OSPF ルーティング プロセスに対応付けられているすべてのインターフェイス上で IS-IS をグローバルにイネーブル化します。
ステップ 4	**exit**	（任意）1 つまたは複数の IS-IS インターフェイス上で BFD をディセーブルにする場合は、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	（任意）インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip router isis**	（任意）インターフェイス上で IPv4 IS-IS ルーティングをイネーブルにします。
ステップ 7	**isis bfd disable**	（任意）IS-IS インターフェイス上で BDF をディセーブルにします。BFD セッションを実行しないすべての IS-IS インターフェイスに対して、ステップ 5 ～ 7 を繰り返し実行します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show bfd neighbors** [**detail**]	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

すべてのインターフェイス上で IS-IS BFD をディセーブルにするには、**no bfd all-interfaces** ルータ コンフィギュレーション コマンドを使用します。指定されたインターフェイス上で IS-IS BFD をディセーブルにするには、そのインターフェイス上で **no isis bfd** インターフェイス コンフィギュレーション コマンドまたは **isis bfd disable** インターフェイス コンフィギュレーション コマンドを実行します。

一部のインターフェイス上でだけ IS-IS BFD を稼動させる場合は、IS-IS BFD をグローバルにイネーブル化する代わりに、それらのインターフェイス上で **isis bfd** インターフェイス コンフィギュレーション コマンドを実行することもできます。詳細については、次に説明する手順を参照してください。

（注） IS-IS BFD が稼動するのはレイヤ 3 インターフェイス上だけですが、IS-IS BFD はレイヤ 2 モードのインターフェイス上でもレイヤ 3 モードのインターフェイス上でも設定できます。IS-IS BFD をイネーブルにすると、次のようなメッセージが表示されます。

```
%ISIS BFD is reverting to router mode configuration, and remains disabled.
```

次に、高速コンバージェンスを設定したうえで、すべての IS-IS インターフェイス上に IS-IS BFD を設定する例を示します。

```
Switch(config)# router is-is tag1
Switch(config-router)# bfd all-interfaces
Switch(config-router)# exit
```

インターフェイス上での IS-IS BFD の設定

個々のインターフェイス上で IS-IS BFD を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router is-is** *area-tag*	IS-IS プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**isis bfd**	指定された IS-IS インターフェイス上で BFD をイネーブルにします。 BFD セッションを実行するすべての IS-IS インターフェイスに対して、ステップ 3 および 4 を繰り返し実行します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show bfd neighbors** [**detail**]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

いずれかのインターフェイス上で IS-IS BFD をディセーブルにするには、そのインターフェイス上で **no isis bfd** インターフェイス コンフィギュレーション コマンドまたは **isis bfd disable** インターフェイス コンフィギュレーション コマンドを実行します。

次に、単独のインターフェイス上で IS-IS BFD を設定する例を示します。

```
Switch(config)# router is-is tag1
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# isis bfd
```

BGP に対する BFD の設定

BGP 用の BFD セッションを開始するときは、参加するすべてのデバイス上で BGP が稼動している必要があります。BGP BFD をイネーブルにするには、BFD ネイバーの IP アドレスを入力します。

BGP BFD をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-tag*	BGP AS を指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** *ip-address* **fall-over bfd**	BFD ネイバー上で、BFD のフォールオーバー サポートをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show bfd neighbors** [**detail**] > **show ip bgp neighbor**	設定を確認します。 ネイバーへの BGP 接続に関する情報を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP BFD をディセーブルにするには、**no neighbor** *ip-address* **fall-over bfd** ルータ コンフィギュレーション コマンドを使用します。

EIGRP に対する BFD の設定

EIGRP 用の BFD セッションを開始する場合は、参加するすべてのデバイス上で EIGRP が稼動している必要があります。BFD の EIGRP サポートをグローバルにイネーブルにする場合は、それをすべての EIGRP インターフェイス上、またはいずれか 1 つ以上の EIGRP インターフェイス上でイネーブルにします。

EIGRP BFD を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *as-number*	EIGRP AS 番号を指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**log-adjacency changes** [**detail**]	EIGRP ネイバーがアップまたはダウンした際、システム ロギング メッセージが送信されるようにスイッチを設定します。
ステップ 4	**bfd** {**all-interfaces** | **interface** *interface-id*}	EIGRP BFD をイネーブルにします。 • EIGRP ルーティング プロセスに対応付けられたすべてのインターフェイス上で、BFD をグローバルにイネーブル化する場合は **all-interfaces** を入力します。 • EIGRP ルーティング プロセスに対応付けられた 1 つまたは複数のインターフェイスに対して BFD を個別にイネーブル化するには、**interface** *interface-id* を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show bfd neighbors** [**detail**]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

すべてのインターフェイス上で EIGRP BFD をディセーブルにするには、**no bfd all-interfaces** ルータ コンフィギュレーション コマンドを使用します。いずれかのインターフェイス上で OSPF BFD をディセーブルにするには、そのインターフェイス上で **no bfd interface** *interface-id* ルータ コンフィギュレーション コマンドを実行します。

HSRP に対する BFD の設定

HSRP ではデフォルトで BFD がサポートされています。BFD はすべてのインターフェイス上でグローバルにイネーブル化されています。HSRP サポートが手動でディセーブル化されている場合は、インターフェイス コンフィギュレーション モードまたはグローバル コンフィギュレーション モードで再度イネーブル化できます。参加するすべてのデバイスで、HSRP および CEF がイネーブルになっている必要があります（CEF はデフォルトでイネーブル）。

HSRP BFD を再度イネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	BFD セッションに使用するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。BFD がサポートされるのは物理インターフェイスだけです。
ステップ 3	**ip address** *ip-address subnet-mask*	インターフェイスの IP アドレスおよび IP サブネット マスクを設定します。

	コマンド	目的
ステップ 4	**standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]	HSRP をアクティブにします。
ステップ 5	**standby bfd**	（任意）インターフェイス上で BFD の HSRP サポートをイネーブルにします。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**standby bfd all-interfaces**	（任意）すべてのインターフェイス上で BFD の HSRP サポートをイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show standby neighbors**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

すべてのインターフェイス上で BFD の HSRP サポートをディセーブルにするには、**no standby bfd all-interfaces** グローバル コンフィギュレーション コマンドを使用します。いずれかのインターフェイス上で BFD の HSRP サポートをディセーブルにするには、**no standby bfd** インターフェイス コンフィギュレーション コマンドを使用します。

（注）　**no standby bfd** インターフェイス コンフィギュレーション コマンドを入力してインターフェイス上のスタンバイ BFD をディセーブルにした場合、その他のインターフェイス上で BFD セッションをアクティブにするためには、**no standby bfd all-interfaces** グローバル コンフィギュレーション コマンドと **standby bfd all-interfaces** グローバル コンフィギュレーション コマンドをこの順に入力して、スタンバイ BFD をいったんグローバルにディセーブル化したあと、再度グローバルにイネーブル化する必要があります。

BFD エコー モードのディセーブル化

BFD セッションを設定すると、BFD インターフェイスでは BFD エコー モードがデフォルトでイネーブルになります。インターフェイス上でエコー モードをディセーブルにすると、そのインターフェイスでは、エコー パケットは送信されず、ネイバーから受信したエコー パケットに限り返送されます。エコー モードがディセーブルの場合、フォワーディングの障害検出には制御パケットが使用されます。BFD 制御パケットの送信頻度を低くする場合は、スロー タイマーを設定します。

BFD デバイス上でエコー モードをディセーブルにし、スロータイマー レートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	BFD インターフェイスを入力し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no bfd echo**	インターフェイス上で BFD エコー モードをディセーブルにします。BFD エコー モードは、デフォルトでイネーブルに設定されていますが、BFD ネイバー上では個別にディセーブル化できます。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**bfd slow-timer** [*milliseconds*]	（任意）BFD のスロータイマーの値を設定します。指定できる範囲は 1000 ～ 30000 ミリ秒です。デフォルト値は 1000 ミリ秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show bfd neighbors detail**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ上でエコー モードをディセーブルにしたあと、再度イネーブルにするには、**bfd echo** グローバル コンフィギュレーション モードを使用します。

マルチ VRF CE の設定

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を使用すると、ISP バックボーン ネットワーク上で帯域幅をセキュアな方法で共有できます。VPN は、共通ルーティング テーブルを共有するサイトの集合です。カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーでは、VPN Routing/Forwarding（VRF; VPN ルーティングおよび転送）テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスが関連付けられます。

スイッチは、Customer Edge（CE; カスタマー エッジ）デバイスの複数の VRF（マルチ VRF）インスタンスをサポートしています（マルチ VRF CE）。サービス プロバイダーは、マルチ VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。

（注）　スイッチでは、VPN のサポートに、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）は使用されません。MPLS VRF の詳細については、『*Cisco IOS Switching Services Configuration Guide*』*Release 12.2* を参照してください。

- 「マルチ VRF CE の概要」（P.36-88）
- 「マルチ VRF CE のデフォルト設定」（P.36-90）
- 「マルチ VRF CE の設定時の注意事項」（P.36-91）
- 「VRF の設定」（P.36-91）
- 「VRF 認識サービスの設定」（P.36-92）
- 「VPN ルーティング セッションの設定」（P.36-95）
- 「BGP PE/CE ルーティング セッションの設定」（P.36-96）
- 「マルチ VRF CE の設定例」（P.36-97）
- 「マルチ VRF CE ステータスの表示」（P.36-101）

マルチ VRF CE の概要

マルチ VRF CE は、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複して使用できるようにする機能です。マルチ VRF CE は入力インターフェイスを使用して、さまざまな VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスと各 VRF を関連付けて仮想パケット転送テーブルを形成します。VRF 内のインターフェイスは、イーサネット ポートのように物理的なもの、または VLAN SVI のように論理的なものにもできますが、複数の VRF には所属させられません。

（注）　マルチ VRF CE インターフェイスは、レイヤ 3 インターフェイスであることが必要です。

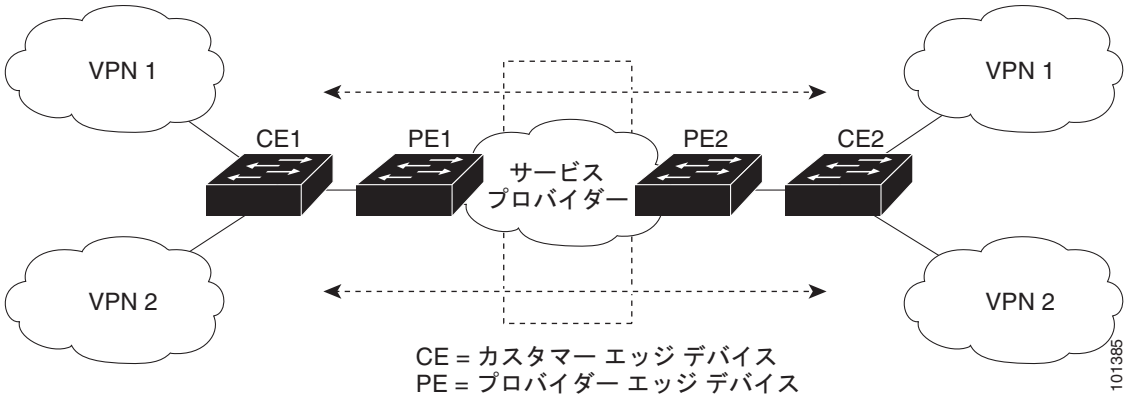
マルチ VRF CE には、次のようなデバイスがあります。

- Customer edge（CE; カスタマー エッジ）：カスタマーは、CE デバイスにより、1 つまたは複数の Provider Edge（PE; プロバイダー エッジ）ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカル ルートをルータにアドバタイズし、そこからリモート VPN ルートを学習します。Cisco ME 3400 スイッチは、CE として使用できます。
- Provider edge（PE; プロバイダー エッジ）：PE ルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE デバイスとルーティング情報を交換します。PE では、直接接続している VPN の VPN ルートだけを維持すればよく、すべてのサービス プロバイダー VPN ルートを維持する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に参加する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- CE デバイスに接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

マルチ VRF CE では、複数のカスタマーが 1 つの CE を共有でき、CE と PE の間ではただ 1 つの物理リンクが使用されます。共有 CE は、カスタマーごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、カスタマーごとにパケットをスイッチングまたはルーティングします。マルチ VRF CE は、制限付きの PE 機能を CE デバイスに拡張して、別々の VRF テーブルを維持し、VPN のプライバシおよびセキュリティを支店に拡張します。

図 36-8 は、Cisco ME スイッチを使用した複数の仮想 CE による構成を示したものです。このシナリオは、中小企業など、VPN サービスの帯域幅要件が低いカスタマーに適しています。このような場合、Cisco ME スイッチではマルチ VRF CE のサポートが必要です。マルチ VRF CE はレイヤ 3 機能であるため、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスであることが必要です。

図 36-8　　複数の仮想 CE として機能するスイッチ



CE スイッチは、レイヤ 3 インターフェイスを VRF に追加するコマンドを受信すると、マルチ VRF CE 関連のデータ構造で VLAN ID と Policy Label（PL; ポリシー ラベル）の間に適切なマッピングを設定し、VLAN ID と PL を VLAN データベースに追加します。

マルチ VRF CE を設定すると、レイヤ 3 転送テーブルは、概念的に次の 2 つのセクションに分割されます。

- マルチ VRF CE ルーティング セクション：さまざまな VPN からのルートが含まれます。
- グローバル ルーティング セクション：インターネットなど、VPN 以外のネットワークへのルートが含まれます。

各 VRF の VLAN ID は別々のポリシー ラベルにマッピングされます。処理を行う際はこれを使用して VRF が区別されます。レイヤ 3 転送テーブルのマルチ VRF CE セクションでルートが検出されない場合は、グローバル ルーティング セクションを使用してフォワーディング パスを決定します。レイヤ 3 設定機能では、学習された新しい VPN ルートごとに、入力ポートの VLAN ID を使用してポリシー ラベルが取得され、マルチ VRF CE ルーティング セクションにポリシー ラベルおよび新しいルートが挿入されます。ルーテッド ポートからパケットを受信した場合は、ポートの内部 VLAN ID 番号が使用されます。SVI からパケットを受信した場合は、VLAN 番号が使用されます。

マルチ VRF CE 対応ネットワークのパケット転送処理は次のとおりです。

- スイッチは、VPN からパケットを受信すると、入力ポリシー ラベル番号に基づいてルーティング テーブルを検索します。ルートが見つかると、スイッチはパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかると、ルータは対応する MPLS ラベルをパケットに追加し、それを MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去し、そのラベルに基づいて正しい VPN ルーティング テーブルを特定します。次に、通常のルート検索を実行します。ルートが見つかると、パケットを正しい隣接装置に転送します。
- CE は、出力 PE からパケットを受信すると、入力ポリシー ラベルを使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかると、パケットを VPN 内で転送します。

VRF を設定する場合は、VRF テーブルを作成し、VRF に関連するレイヤ 3 インターフェイスを指定します。次に、VPN 内のルーティング プロトコル、および CE と PE の間のルーティング プロトコルを設定します。プロバイダーのバックボーンで VPN ルーティング情報を配布する場合は、BGP が望ましいルーティング プロトコルです。マルチ VRF CE ネットワークには、次の 3 つの主要コンポーネントがあります。

- VPN ルート ターゲット コミュニティ：VPN コミュニティのその他すべてのメンバーを表示します。VPN コミュニティ メンバーごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング：VPN コミュニティのすべてのメンバーに VRF 到達可能性情報を伝播します。VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービスプロバイダー ネットワークを介し、全 VPN コミュニティ メンバー間で、全トラフィックを伝送します。

マルチ VRF CE のデフォルト設定

表 36-14 は、VRF のデフォルト設定をまとめたものです。

表 36-14　VRF のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル。VRF は定義されていない。
マップ	インポート マップ、エクスポート マップ、およびルート マップは定義されていない。
VRF 最大ルート数	5000
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブル。

マルチ VRF CE の設定時の注意事項

ネットワークに VRF を設定する場合は、次の事項に注意してください。

- マルチ VRF CE を含むスイッチは複数のカスタマーで共有しますが、一方で各カスタマーには独自のルーティング テーブルがあります。
- カスタマーは、別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN であれば IP アドレスの重複が許可されます。
- マルチ VRF CE では、複数のカスタマーが、PE と CE の間で同じ物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、カスタマー間でパケットが区別されます。それぞれのカスタマーには独自の VLAN があります。
- マルチ VRF CE には、サポートしていない MPLS-VRF 機能があります。ラベル交換、LDP 隣接関係、ラベル付きパケットはサポートされません。
- PE ルータの場合、マルチ VRF CE の使用と複数の CE の使用に違いはありません。図 36-8 では、複数の仮想レイヤ 3 インターフェイスがマルチ VRF CE デバイスに接続されています。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合せを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートを介して接続できます。
- カスタマーは、別のカスタマーと重複しないかぎり、複数の VLAN を使用できます。カスタマーの VLAN は、スイッチに保存されている適切なルーティング テーブルを識別するために使用される特定のルーティング テーブル ID にマッピングされます。
- スイッチは、1 つのグローバル ネットワークおよび最大 26 の VRF をサポートしています。
- CE と PE の間では、ほとんどのルーティング プロトコル（BGP、OSPF、RIP、EIGRP およびスタティック ルーティング）を使用できます。ただし、次の理由から （EBGP; 外部 BGP）を使用することを推奨します。
  - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
  - BGP は、さまざまな管理者により運用されるシステム間でルーティング情報を受け渡しできるように設計されています。
  - BGP では、ルートのアトリビュートを CE へ簡単に渡すことができます。
- マルチ VRF CE は、パケットのスイッチング レートに影響しません。
- VRF を設定しない場合は、最大 105 のポリシーを設定できます。
- VRF を 1 つでも設定した場合、設定できるポリシーの数は 41 となります。
- 設定されているポリシーの数が 41 を超えている場合は、VRF を設定できません。
- VRF とプライベート VLAN は相互に排他的です。プライベート VLAN では VRF をイネーブルにできません。同様に、VLAN インターフェイスで VRF が設定されている VLAN では、プライベート VLAN をイネーブルにはできません。
- VRF と Policy-Based Routing（PBR; ポリシーベース ルーティング）は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっている場合、VRF をイネーブルにはできません。VRF がインターフェイスでイネーブルになっている場合、PBR をイネーブルにはできません。

VRF の設定

1 つまたは複数の VRF を設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference*』*Release 12.2* を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします
ステップ 3	**ip vrf** *vrf-name*	VRF に名前を付けて VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher*	ルート識別子を指定し、VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community*	指定した VRF のインポート コミュニティ、エクスポート コミュニティ、またはインポートとエクスポートのルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同じであることが必要です。
ステップ 6	**import map** *route-map*	（任意）ルート マップを VRF に関連付けます。
ステップ 7	**interface** *interface-id*	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには、ルーテッド ポートまたは SVI を指定できます。
ステップ 8	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 9	**ip vrf forwarding** *vrf-name*	VRF をレイヤ 3 インターフェイスに関連付けます。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VRF と、そのインターフェイスすべてを削除するには、**no ip vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。VRF からいずれかのインターフェイスを削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

VRF 認識サービスの設定

IP サービスは、グローバル インターフェイス上で設定できます。これらのサービスは、グローバル ルーティング インスタンス内で実行されます。IP サービスは、複数のルーティング インスタンスで実行されるように拡張されています。これが VRF 認識です。システム内に設定された VRF は、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームから独立したモジュールに実装されています。VRF とは、Cisco IOS における複数のルーティング インスタンスのことです。各プラットフォームでは、サポートされる VRF 数に独自の制限があります

VRF 認識サービスには次のような特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに対して PING を実行できます。
- ARP エントリは、それぞれの VRF 内で個別に学習されます。ユーザは、特定の VRF に関する ARP エントリを表示できます。

次のサービスはすべて VRF 認識です。

- ARP
- PING
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
- Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）
- syslog
- traceroute
- FTP および TFTP

（注）　Unicast Reverse Path Forwarding（uRPF; ユニキャスト RPF）に対しては、VRF 認識サービスはサポートされていません。

ARP のユーザ インターフェイス

ARP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference*』*Release 12.2* を参照してください。

コマンド	目的
show ip arp vrf *vrf-name*	指定した VRF の ARP テーブルを表示します。

PING のユーザ インターフェイス

PING の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference*』*Release 12.2* を参照してください。

コマンド	目的
ping vrf *vrf-name* **ip-host**	指定した VRF の ARP テーブルを表示します。

SNMP のユーザ インターフェイス

SNMP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference*』*Release 12.2* を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server trap authentication vrf**	VRF 上のパケットに対して SNMP トラップをイネーブルにします。
ステップ 3	**snmp-server engineID remote** <*host*> **vrf** <*vpn instance*> <*engine-id string*>	スイッチ上のリモート SNMP エンジンに名前を設定します。
ステップ 4	**snmp-server host** <*host*> **vrf** <*vpn instance*> **traps** <*community*>	SNMP トラップ動作の受信側を指定し、SNMP トラップの送信に使用する VRF テーブルを指定します。

	コマンド	目的
ステップ 5	**snmp-server host <*host*> vrf** <*vpn instance*> **informs** <*community*>	SNMP インフォーム動作の受信側を指定し、SNMP インフォームの送信に使用する VRF テーブルを指定します。
ステップ 6	**snmp-server user** <*user*> <*group*> **remote** <*host*> **vrf** <*vpn instance*> <*security model*>	SNMP アクセス用に、VRF 上にあるリモート ホストの SNMP グループにユーザを追加します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

HSRP のユーザ インターフェイス

VRF の HSRP サポートにより、HSRP 仮想 IP アドレスが正しい IP ルーティング テーブルへ追加されることが保証されます。

HSRP に対して VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference*』*Release 12.2* を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	**ip vrf forwarding** <*vrf-name*>	インターフェイス上で VRF を設定します。
ステップ 5	**ip address** *ip address*	インターフェイスの IP アドレスを入力します。
ステップ 6	**standby 1 ip** *ip address*	HSRP をイネーブルにし、仮想 IP アドレスを設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

syslog のユーザ インターフェイス

syslog の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference*』*Release 12.2* を参照してください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging on**	ストレージ ルータ イベント メッセージのロギングをイネーブル、または一時的にディセーブルにします。
ステップ 3	**logging host *ip address* vrf *vrf name***	ロギング メッセージが送信される syslog サーバのホスト アドレスを指定します。
ステップ 4	**logging buffered** *logging buffered size* **debugging**	メッセージを内部バッファにログとして記録します。
ステップ 5	**logging trap debugging**	syslog サーバに送信するロギング メッセージを制限します。
ステップ 6	**logging facility** *facility*	システム ロギング メッセージをロギング ファシリティに送信します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

traceroute のユーザ インターフェイス

traceroute の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference*』*Release 12.2* を参照してください。

コマンド	目的
traceroute vrf *vrf-name ipaddress*	宛先アドレスを検索する VPN VRF の名前を指定します。

FTP および TFTP のユーザ インターフェイス

FTP および TFTP が VRF 認識であるためには、いくつかの FTP/TFTP CLI を設定する必要があります。たとえば、インターフェイス E1/0 に付随する VRF テーブルを使用する場合であれば、特定のルーティング テーブルを使用することが FTP/TFTP に通知されるよう CLI **ip [t]ftp source-interface E1/0** を設定する必要があります。この例では、宛先 IP アドレスの検索に VRF テーブルが使用されます。これらの変更は、下位互換性があるため、既存の動作には影響しません。つまり、source-interface CLI を使用すれば、VRF が設定されていないインターフェイスに対してもパケットを送信できます。

FTP 接続の送信元 IP アドレスを指定するには、**ip ftp source-interface** 表示モード コマンドを使用します。接続が行われるインターフェイスのアドレスを使用するには、このコマンドの **no** 形式を使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip ftp source-interface** *interface-type interface-number*	FTP 接続の送信元 IP アドレスを指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

インターフェイスの IP アドレスを TFTP 接続の送信元アドレスとして指定するには、**ip tftp source-interface** 表示モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip tftp source-interface** *interface-type interface-number*	TFTP 接続の送信元 IP アドレスを指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされている任意のルーティング プロトコル（RIP、OSPF、EIGRP、BGP）、またはスタティック ルーティングで設定できます。ここでは OSPF の設定について説明しますが、その他のプロトコルでも手順は同じです。

（注）　EIGRP ルーティング プロセスが VRF インスタンス内部で実行されるよう設定するには、**autonomous-system** a*utonomous-system-number* address-family コンフィギュレーション モード コマンドを使用して、AS 番号を設定する必要があります。

VPN 内で OSPF を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id* **vrf** *vrf-name*	OSPF ルーティングをイネーブルにし、VPN 転送テーブルを指定して、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**log-adjacency-changes**	（任意）隣接状態の変更をログに記録します。これがデフォルトの状態になります。
ステップ 4	**redistribute bgp** *autonomous-system-number* subnets	BGP ネットワークから OSPF ネットワークに情報を再配布するようにスイッチを設定します。
ステップ 5	**network** *network-number* **area** *area-id*	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip ospf** *process-id*	OSPF ネットワークの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VPN 転送テーブルと OSPF ルーティング プロセスの関連付けを解除するには、**no router ospf** *process-id* **vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。

BGP PE/CE ルーティング セッションの設定

BGP PE/CE ルーティング セッションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number*	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**network** *network-number* **mask** *network-mask*	ネットワークとマスクを指定し、BGP の使用を通知します。
ステップ 4	**redistribute ospf** *process-id* **match internal**	OSPF 内部ルートを再配布するようにスイッチを設定します。
ステップ 5	**network** *network-number* **area** *area-id*	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**address-family ipv4 vrf** *vrf-name*	PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレスファミリー モードを開始します。
ステップ 7	**neighbor** *address* **remote-as** *as-number*	PE ルータと CE ルータの間の BGP セッションを定義します。
ステップ 8	**neighbor** *address* **activate**	IPv4 アドレス ファミリーのアドバタイズメントをアクティブにします。
ステップ 9	**end**	特権 EXEC モードに戻ります。

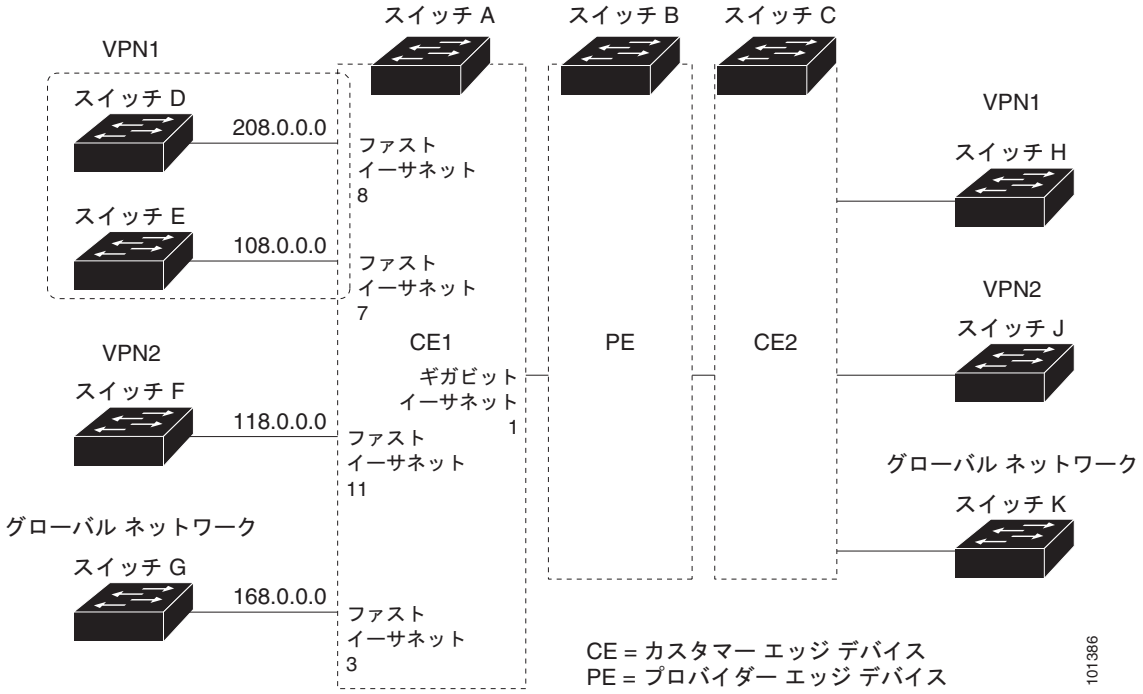
	コマンド	目的
ステップ 10	**show ip bgp [ipv4] [neighbors]**	BGP 設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ルーティング プロセスを削除するには、**no router bgp** *autonomous-system-number* グローバル コンフィギュレーション コマンドを使用します。ルーティング特性を削除するには、このコマンドにキーワードを指定して使用します。

マルチ VRF CE の設定例

図 36-9 は、図 36-8 と同様のネットワークにおける物理的な接続を単純化した例です。VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。この図のあとに記載されている例は、Cisco ME 3400 スイッチを CE Switch A として設定する方法、および カスタマー スイッチ D および F の VRF 設定です。CE スイッチ C やその他のカスタマー スイッチを設定するためのコマンドは記載されていませんが、この例で使用されているコマンドとほぼ同じです。この例には、PE ルータとして動作する Catalyst 6000 スイッチまたは Catalyst 6500 スイッチのスイッチ A へのトラフィックを設定するコマンドも含まれています。

図 36-9　　マルチ VRF CE の設定例



スイッチ A の設定

スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
```

```
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ A 上でループバックおよび物理インターフェイスを設定します。ギガビット イーサネット ポート 1 は、PE へのトランク接続です。ファスト イーサネット ポート 8 と 11 は VPN に接続されます。

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface gigabitethernet0/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet0/8
Switch(config-if)# no shutdown
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet0/11
Switch(config-if)# no shutdown
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

スイッチ A 上で使用する VLAN を設定します。VLAN 10 は、CE と PE の間の VRF 11 によって使用されます。VLAN 20 は、CE と PE の間の VRF 12 によって使用されます。VLAN 118 と VLAN 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

```
Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
```

```
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
```

VPN1 と VPN2 で OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf vl1
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf vl2
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE/PE ルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit

Switch(config-router)# address-family ipv4 vrf vl1
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

スイッチ D の設定

Switch D は VPN 1 に属します。次のコマンドを使用してスイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet0/2
Switch(config-if)# no shutdown
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

スイッチ F の設定

Switch F は VPN 2 に属します。次のコマンドを使用してスイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
```

```
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

PE スイッチ B の設定

スイッチ B（PE ルータ）では、次のコマンドを使用することにより、CE デバイス、スイッチ A への接続だけが設定されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitthernet0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

マルチ VRF CE ステータスの表示

マルチ VRF CE の設定とステータスに関する情報を表示するには、表 36-15 の特権 EXEC コマンドを使用します。

表 36-15　マルチ VRF CE 情報を表示するコマンド

コマンド	目的
show ip protocols vrf *vrf-name*	VRF に関するルーティング プロトコル情報を表示します。
show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRF に関する IP ルーティング テーブル情報を表示します。
show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義した VRF インスタンスに関する情報を表示します。

表示される情報の詳細については、『*Cisco IOS Switching Services Command Reference*』*Release 12.2* を参照してください。

プロトコルに依存しない機能の設定

ここでは、IP ルーティング プロトコルに依存しない機能の設定方法について説明します。この章で説明する IP ルーティング プロトコルに依存しないコマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* の「IP Routing Protocol-Independent Commands」を参照してください。

ここでは、次の設定情報について説明します。

- 「CEF の設定」（P.36-101）
- 「等価コスト ルーティング パスの個数の設定」（P.36-103）
- 「スタティック ユニキャスト ルートの設定」（P.36-103）
- 「デフォルトのルートおよびネットワークの指定」（P.36-105）
- 「ルート マップによるルーティング情報の再配布」（P.36-105）
- 「PBR の設定」（P.36-109）
- 「ルーティング情報のフィルタリング」（P.36-113）
- 「認証鍵の管理」（P.36-116）

CEF の設定

CEF は、ネットワーク パフォーマンスを最適化するために使用されるレイヤ 3 IP スイッチング技術です。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。CEF は、高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、より多くの CPU 処理能力をパケット転送に割り振ることができます。ダイナミックなネットワークでは、ルーティングの変更によって、高速スイッチング キャッシュ エントリが頻繁に無効となります。高速スイッチング キャッシュ エントリが無効になると、トラフィックがルート キャッシュによって高速スイッチングされずに、ルーティング テーブルによってプロセス スイッチングされることがあります。CEF は FIB 検索テーブルを使用して、宛先ベースの IP パケット スイッチングを実行します。

CEF の 2 つの主要な構成要素は、分散 FIB と分散隣接関係テーブルです。

- FIB はルーティング テーブルや情報ベースと同様、IP ルーティング テーブルに転送情報のミラー イメージが保持されます。ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルがアップデートされ、これらの変更が FIB に反映されます。FIB には、IP ルーティング テーブル内の情報に基づいて、ネクストホップのアドレス情報が保持されます。FIB にはルーティング テーブル内の既知のルートがすべて格納されているため、CEF はルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。
- リンク レイヤ上でネットワーク内のノードが 1 ホップで相互に到達可能な場合、これらのノードは隣接関係にあるといいます。CEF は、隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報を付加します。隣接関係テーブルには、すべての FIB エントリに対する、レイヤ 2 のネクストホップのアドレスが保持されます。

スイッチは、（ASIC; 特定用途向け IC）を使用してギガビット回線レートの IP トラフィックを実現しているため、CEF 転送はソフトウェア フォワーディング パス、つまり CPU が転送するトラフィックにだけ適用されます。

デフォルトでは、CEF はグローバルにイネーブル化されています。何らかの理由で CEF がディセーブルになった場合は、**ip cef** グローバル コンフィギュレーション コマンドを使用して、再度イネーブルに設定できます。

デフォルト設定では、CEF はすべてのレイヤ 3 インターフェイス上でイネーブルです。**no ip route-cache cef** インターフェイス コンフィギュレーション コマンドを入力すると、ソフトウェアにより転送されるトラフィックに対して CEF がディセーブルになります。このコマンドは、ハードウェア フォワーディング パスには影響しません。CEF をディセーブルにして **debug ip packet detail** 特権 EXEC コマンドを使用すると、ソフトウェア転送トラフィックをデバッグするのに便利です。ソフトウェア フォワーディング パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。

注意　CLI には、インターフェイス上で CEF をディセーブルにする **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、インターフェイス上の CEF をデバッグ目的以外でディセーブルにすることは避けてください。

CEF をグローバルにイネーブル化したり、ソフトウェア転送トラフィック用のインターフェイス上でディセーブルになった場合にそのインターフェイス上で CEF をイネーブルにしたりするには、特権 EXEC モードで、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip cef**	CEF の動作をイネーブルにします。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5	**ip route-cache cef**	ソフトウェア転送トラフィック用のインターフェイスで CEF をイネーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip cef**	すべてのインターフェイスの CEF ステータスを表示します。

	コマンド	目的
ステップ 8	**show cef linecard** [**detail**]	CEF に関連するインターフェイス情報を表示します。
ステップ 9	**show cef interface** [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスの詳細な CEF 情報を表示します。
ステップ 10	**show adjacency**	CEF の隣接関係テーブル情報を表示します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

等価コスト ルーティング パスの個数の設定

同じネットワークへ向かう同じメトリックのルートが複数ルータに格納されている場合、これらのルートは等価コストを保有していると見なされます。ルーティング テーブルに複数の等価コスト ルートが含まれる場合は、これらを*パラレル パス*と呼ぶこともあります。ネットワークへの等価コスト パスがルータに複数格納されている場合、ルータはこれらを同時に使用できます。パラレル パスを使用すると、回線に障害が発生した場合に備えて冗長性を確保できます。また、使用可能なパスにパケットの負荷を分散し、使用可能な帯域幅を有効利用することもできます。

等価コスト ルートはルータによって自動的に学習、設定されますが、ルーティング テーブルの IP ルーティング プロトコルでサポートされるパラレル パスの最大数は制御可能です。

ルーティング テーブルに格納されるパラレル パスのデフォルトの最大数を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**maximum-paths** *maximum*	プロトコル ルーティング テーブルのパラレル パスの最大数を設定します。指定できる範囲は 1 ～ 8 です。ほとんどの IP ルーティング プロトコルではデフォルトは 4 ですが、BGP に限りデフォルトは 1 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols**	*Maximum path* フィールドの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト値に戻すには、**no maximum-paths** ルータ コンフィギュレーション コマンドを使用します。

スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートは、特定のパスを経由して送信元と宛先の間でパケットを転送するユーザ定義のルートです。スタティック ルートは、ルータが特定の宛先へのルートを構築できない場合に重要性を持つことがあり、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip route** *prefix mask* {*address* | *interface*} [*distance*]	スタティック ルートを確立します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip route**	設定を確認するため、ルーティング テーブルの現在の状態を表示します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック ルートを削除するには、**no ip route** *prefix mask* {*address* | *interface*} グローバル コンフィギュレーション コマンドを使用します。

スタティック ルートは、ユーザによって削除されるまでスイッチに保持されます。ただし、管理ディスタンスの値を割り当てることで、スタティック ルートをダイナミック ルーティング情報で上書きできます。各ダイナミック ルーティング プロトコルには、デフォルトの管理ディスタンスが設定されています（表 36-16 を参照）。ダイナミック ルーティング プロトコルの情報でスタティック ルートを上書きする場合は、スタティック ルートの管理ディスタンスがダイナミック プロトコルの管理ディスタンスよりも大きな値になるように設定します。

表 36-16　ダイナミック ルーティング プロトコルのデフォルトの管理ディスタンス

ルート送信元	デフォルト距離
接続されたインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
EBGP	20
内部 EIGRP	90
IGRP	100
OSPF	110
IBGP	200
不明	225

インターフェイスを指し示すスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルを通してアドバタイズされます。**redistribute** スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、ルーティング テーブルでは、インターフェイスを指し示すスタティック ルートが接続され、その結果スタティックな性質を失ったと見なされるためです。ただし、network コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに **redistribute** スタティック コマンドを指定しないかぎり、ルートはアドバタイズされません。

インターフェイスがダウンすると、そのインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。転送ルータのアドレスとして指定されたアドレスに対して有効なネクストホップが見つからないスタティック ルートも IP ルーティング テーブルから削除されます。

デフォルトのルートおよびネットワークの指定

ルータは、他のネットワークすべてへのルートを学習できるわけではありません。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートをスマート ルータ宛に指定します （スマート ルータには、インターネットワーク全体のルーティング テーブル情報が格納されます)。これらのデフォルト ルートはダイナミックに学習されるか、ルータごとに設定されます。ダイナミックな内部ルーティング プロトコルはそのほとんどが、スマート ルータを使用してデフォルト情報をダイナミックに生成し、それを他のルータに転送するメカニズムを備えています。

指定されたデフォルト ネットワークに直接接続されたインターフェイスがルータに存在する場合は、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

ネットワークのデフォルト ルートを生成しているルータには、そのルータ自身のデフォルト ルートも指定する必要があります。ルータのデフォルト ルートをそのルータ自身で生成できるようにする方法はいくつかありますが、適切なデバイスを経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定するという方法もその 1 つです。

ネットワークへのスタティック ルートをスタティック デフォルト ルートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip default-network** *network number*	デフォルト ネットワークを指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip route**	選択されたデフォルト ルートを最終ゲートウェイのディスプレイに表示します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルートを削除するには、**no ip default-network** *network number* グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ルーティング プロトコルによってデフォルト情報を送信する場合は、これ以上の設定は必要ありません。システムにより、ルーティング テーブルが定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。IGRP ネットワークでは、システムのデフォルト ネットワークの候補が複数存在する場合もあります。シスコのルータでは、デフォルト ルートまたは最終ゲートウェイを設定するため、管理ディスタンスおよびメトリック情報が使用されます。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用して、デフォルト ルートの候補を指定します。このネットワークが任意の送信元のルーティング テーブルに格納されている場合は、デフォルト ルートの候補としてフラグ付けされます。ルータにデフォルト ネットワークのインターフェイスが存在しない場合でも、そこへのパスが格納されていれば、そのネットワークは 1 つの候補と見なされ、最適なデフォルト パスへのゲートウェイが最終ゲートウェイになります。

ルート マップによるルーティング情報の再配布

スイッチでは、複数のルーティング プロトコルを同時に実行して、ルーティング プロトコル間で情報を再配布できます。ルーティング プロトコル間での情報の再配布は、サポートされているすべての IP ベース ルーティング プロトコルで行われます。

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配布を条件付きで制御することもできます。**match** ルートマップ コンフィギュレーション コマンドおよび **set** ルートマップ コンフィギュレーション コマンドを使用すると、ルート マップの条件部を定義できます。**match** コマンドは条件が一致しなければならないことを示します。**set** コマンドを使用すると、match コマンドで定義された条件をルーティング アップデートが満たす場合に実行されるアクションを指定できます。再配布はプロトコルに依存しない機能ですが、**match** ルート マップ コンフィギュレーション コマンドおよび **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコルに固有のものです。

route-map コマンドのあとに、**match** コマンドおよび **set** コマンドをそれぞれ 1 つまたは複数指定します。**match** コマンドを指定しない場合は、すべて一致すると見なされます。**set** コマンドを指定しない場合、一致以外の処理は一切実行されません。このため、**match** コマンドまたは **set** コマンドを少なくとも 1 つは指定する必要があります。

（注）　**set** ルートマップ コンフィギュレーション コマンドが指定されていないルート マップは CPU に送信されるため、CPU の使用量が増大する原因となります。

route-map 文は、**permit** が指定されているか **deny** が指定されているかによって、その意味が異なります。この文に deny が指定されている場合、一致基準を満たすパケットは通常の転送チャネルを通じて返送されます（宛先ベース ルーティング）。この文に permit が指定されている場合は、一致基準を満たすパケットに set 句が適用されます。一致基準を満たさないパケットは、通常のルーティング チャネルを介して転送されます。

match 句および set 句による入力の実行が完了したら、BGP ルート マップの **continue** 句を使用して、ルート マップに対する追加の入力を実行できます。**continue** 句を使用して、より多くのモジュラ ポリシー定義を設定して組織化すれば、特定のポリシー設定を同じルート マップ内で繰り返す必要がなくなります。スイッチでは、発信ポリシーに対して **continue** 句がサポートされています。ルート マップの **continue** 句の使用に関する詳細については、次の URL にある『BGP Route-Map Continue Support for an Outbound Policy feature guide for Cisco IOS Release 12.4(4)T』を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_feature_guides_list.html

（注）　次に示すステップ 3 ～ 14 はいずれも任意ですが、**match** ルート マップ コンフィギュレーション コマンドおよび **set** ルート マップ コンフィギュレーション コマンドはそれぞれ、少なくとも 1 つ入力する必要があります。

再配布用のルート マップを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [**permit** | **deny**] [*sequence number*]	再配布を制御するために使用するルート マップを定義し、ルートマップ コンフィギュレーション モードを開始します。 *map-tag*：ルート マップ用のわかりやすい名前を指定します。**redistribute** ルータ コンフィギュレーション コマンドでは、この名前を使用してルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。 （任意）**permit** が指定され、このルート マップの一致基準が満たされている場合は、set アクションの制御に従ってルートが再配布されます。**deny** が指定されている場合、ルートは再配布されません。 *sequence number*（任意）：すでに同じ名前が設定されているルート マップのリスト内で、新しいルート マップの位置を表す番号を指定します。
ステップ 3	**match as-path** *path-list-number*	BGP AS パス アクセス リストを一致基準にします。
ステップ 4	**match community-list** *community-list-number* [**exact**]	BGP コミュニティ リストを一致基準にします。
ステップ 5	**match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	名前または番号を指定し、標準アクセス リストを一致基準にします。1 ～ 199 の整数を指定できます。
ステップ 6	**match metric** *metric-value*	指定されたルート メトリックを一致基準にします。*metric-value* には、0 ～ 4294967295 の範囲で値が指定された EIGRP のメトリックを指定できます。
ステップ 7	**match ip next-hop** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	指定されたアクセス リスト（番号 1 ～ 199）のいずれかで送信されるネクスト ホップのルータ アドレスを一致基準にします。
ステップ 8	**match tag** *tag value* [*...tag-value*]	1 つまたは複数のルート タグ値の中から指定されたタグ値を一致基準にします。0 ～ 4294967295 の整数を指定できます。
ステップ 9	**match interface** *type number* [*...type number*]	指定されたインターフェイスの 1 つから指定されたネクスト ホップへのルートを一致基準にします。
ステップ 10	**match ip route-source** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	指定されたアドバタイズ済みアクセス リストによって指定されるアドレスを一致基準にします。
ステップ 11	**match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**]}	指定された **route-type** の値を一致基準にします。 • **local**：ローカルに生成された BGP ルート • **internal**：OSPF エリア内ルートおよびエリア間ルート、または EIGRP 内部ルート • **external**：OSPF 外部ルート（タイプ 1 またはタイプ 2）または EIGRP 外部ルート

	コマンド	目的
ステップ 12	**set dampening** *halflife reuse suppress max-suppress-time*	BGP ルート ダンプニング係数を設定します。
ステップ 13	**set local-preference** *value*	ローカル BGP パスに値を割り当てます。
ステップ 14	**set origin** {**igp** | **egp** *as* | **incomplete**}	BGP の送信元コードを設定します。
ステップ 15	**set as-path** {**tag** | **prepend** *as-path-string*}	BGP AS パスを変更します。
ステップ 16	**set level** {**level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone**}	ルーティング ドメインの指定エリアにアドバタイズされるルートのレベルを設定します。**stub-area** および **backbone** は、OSPF の NSSA エリアおよびバックボーン エリアです。
ステップ 17	**set metric** *metric value*	再配布されるルートに指定するメトリック値を設定します（EIGRP 専用）。*metric value* には 294967295 ～ 294967295 の整数を指定します。
ステップ 18	**set metric** *bandwidth delay reliability loading mtu*	再配布されるルートに指定するメトリック値を設定します（EIGRP 専用）。 • *bandwidth* : ルートのメトリック値または IGRP 帯域幅（キロビット/秒単位）を 0 ～ 4294967295 の範囲で指定します。 • *delay* : ルート遅延を 0 ～ 4294967295 の範囲で指定します（10 マイクロ秒単位）。 • *reliability* : パケット伝送の成功可能性を 0 ～ 255 の数値で指定します。255 は信頼性が 100% であること、0 は信頼性がないことを意味します。 • *loading* : ルートの有効帯域幅を 0 ～ 255 の数値で指定します（255 は 100% の負荷）。 • *mtu* : ルートの MTU の最小サイズをバイト単位で指定します。指定できる範囲は 0 ～ 4294967295 です。
ステップ 19	**set metric-type** {**type-1** | **type-2**}	再配布されるルートに OSPF 外部メトリック タイプを設定します。
ステップ 20	**set metric-type internal**	ネクストホップの IGP メトリックと一致するように、EBGP ネイバーにアドバタイズされるプレフィクスの MED 値を設定します。
ステップ 21	**set weight**	ルーティング テーブルの BGP の重みを設定します。指定できる値は 1 ～ 65535 です。
ステップ 22	**end**	特権 EXEC モードに戻ります。
ステップ 23	**show route-map**	設定を確認するため、設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。
ステップ 24	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

エントリを削除するには、**no route-map** *map tag* グローバル コンフィギュレーション コマンド、**no match** ルート マップ コンフィギュレーション コマンド、または **no set** ルート マップ コンフィギュレーション コマンドを使用します。

ルーティング ドメイン間でルートを配布したり、ルート再配布を制御したりできます。

ルート再配布を制御するには、特権 EXEC モードで次の手順を実行します。キーワードは前述の手順で定義されたキーワードと同じです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type** *type-value*] [**match internal** | **external** *type-value*] [**tag** *tag-value*] [**route-map** *map-tag*] [**weight** *weight*] [**subnets**]	ルーティング プロトコル間でルートを再配布します。route-map を指定しないと、すべてのルートが再配布されます。キーワード **route-map** に *map-tag* を指定しないと、ルートは配布されません。
ステップ 4	**default-metric** *number*	現在のルーティング プロトコルが、再配布されたすべてのルートに対して同じメトリック値を使用するように設定します（BGP、RIP、OSPF）。
ステップ 5	**default-metric** *bandwidth delay reliability loading mtu*	EIGRP ルーティング プロトコルが、EIGRP 以外で再配布されたすべてのルートに対して同じメトリック値を使用するように設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show route-map**	設定を確認するため、設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

再配布をディセーブルにするには、そのコマンドの **no** 形式を使用します。

異なるルーティング プロトコル間では、必ずしもメトリックは変換されません。このような場合、再配布されたルートには疑似的なメトリックが割り当てられます。さまざまなルーティング プロトコル間でルーティング情報を無制御に交換するとルーティング ループが発生し、ネットワーク動作が著しく低下することがあります。

メトリック変換の代わりに使用されるデフォルトの再配布メトリックが定義されていない場合は、ルーティング プロトコル間でメトリックが自動的に変換されることもあります。

- RIP では、スタティック ルートの自動的な再配布が可能です。スタティック ルートにはメトリック 1（直接接続）が割り当てられます。
- デフォルト モードでは、いずれのプロトコルでも、他のルーティング プロトコルの再配布が可能です。

PBR の設定

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。PBR を使用すると、ルーティング プロトコルから取得したルートの信頼度を下げることで、ルーティングをより細かく制御できます。PBR では、次の基準に基づいてパスを許可または拒否するルーティング ポリシーを設定できます。

- 特定のエンド システムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、双方向対バッチ トラフィックに基づくルーティング、専用リンクに基づくルーティングを実現できます。たとえば、在庫記録を本社に送信する場合は広帯域で高コストのリンクを短時間使用し、E メールなど日常的に使用するアプリケーション データは狭帯域で低コストのリンクで送信できます。

PBR がイネーブルの場合は、Access Control List（ACL; アクセス コントロール リスト）を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。PBR は着信パケットに適用されます。PBR がイネーブルのインターフェイスで受信されたパケットはすべて、ルート マップを通過します。ルート マップで定義された基準に基づいて、パケットは適切なネクスト ホップに転送（ルーティング）されます。

- パケットがどの route-map 文とも一致しない場合は、すべての set 句が適用されます。
- いずれかの文に permit が指定されている場合、どの route-map 文とも一致しないパケットは、通常の転送チャネルを通じて送信され、宛先ベースのルーティングが実行されます。
- PBR では、deny を指定できる route-map 文はサポートされていません。

ルート マップの設定に関する詳細については、「ルート マップによるルーティング情報の再配布」（P.36-105）を参照してください。

送信元アドレスの一致基準を指定する場合は標準 IP ACL を使用し、アプリケーション、プロトコル タイプ、またはエンド ステーションを基にした一致基準を指定する場合は拡張 IP ACL 使用します。ルート マップでは、一致が検出されるまでこのプロセスが行われます。一致が検出されない場合は、通常の宛先ベース ルーティングが行われます。match 文のリストの末尾には、暗黙的に拒否されるエントリがあります。

match 句に一致した場合は、set 句を使用して、パス内のネクストホップ ルータを識別する IP アドレスを指定できます。

PBR のコマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』*Release 12.2* を参照してください。表示されるにもかかわらずスイッチでサポートされていない PBR コマンドについては、付録 C「Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド」を参照してください。

PBR 設定時の注意事項

PBR の設定を開始する前に、次の点に注意してください。

- マルチキャスト トラフィックについては、ポリシーによるルーティングが行われません。PBR が適用されるはユニキャスト トラフィックだけです。
- PBR は、ルーテッド ポートまたは SVI 上でイネーブルにできます。
- スイッチでは、PBR に対して **route-map deny** 文を使用できません。
- ポリシー ルート マップは、レイヤ 3 モードの EtherChannel ポート チャネルには適用できますが、EtherChannel のメンバーである物理インターフェイスには適用できません。適用しようとすると、コマンドが拒否されます。ポリシー ルート マップが適用されている物理インターフェイスは、EtherChannel のメンバーにはなれません。
- スイッチには最大 246 の IP ポリシー ルート マップを定義できます。
- スイッチには、PBR 用として最大 512 の Access Control Entry（ACE; アクセス コントロール エントリ）を定義できます。
- ルート マップに一致基準を設定する場合は、次の点に注意してください。
  - ローカル アドレス宛のパケットを許可する ACL は、一致基準にはしないでください。PBR がこれらのパケットを転送すると、ping や Telnet の障害、またはルート プロトコル フラッピングの原因となります。

  - 拒否 ACE を含む ACL は、一致基準にはしないでください。拒否 ACE に一致するパケットは CPU に送信されるため、場合によっては CPU の利用率が高くなる原因となります。

- PBR を使用するには、**sdm prefer default** グローバル コンフィギュレーション コマンドを使用して、デフォルト テンプレートをイネーブルにしておく必要があります。PBR では、レイヤ 2 テンプレートは使用できません。SDM テンプレートの詳細については、第 7 章「SDM テンプレートの設定」を参照してください。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっている場合、VRF をイネーブルにはできません。VRF がインターフェイスでイネーブルになっている場合、PBR をイネーブルにはできません。
- PBR で使用される Ternary CAM（TCAM）エントリの数は、ルート マップそのもの、使用される ACL、および ACL とルート マップ エントリの順序によって異なります。
- パケット長、IP precedence および Type of Service（ToS; サービス タイプ）、set interface、set default next hop、または set default interface に基づく PBR はサポートされていません。有効な set アクションがないか、または set アクションが *Don't Fragment* に設定されているポリシー マップは、サポートされていません。

PBR のイネーブル化

デフォルトでは、PBR はスイッチ上でディセーブルです。PBR をイネーブルにするには、一致基準およびすべての match 句と一致した場合の動作を指定したルート マップを作成する必要があります。さらに、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにする必要があります。指定したインターフェイスに着信したパケットのうち、match 句と一致したものはすべて PBR の対象になります。

PBR の高速スイッチングや実装は、スイッチの速度低下を引き起こさない速度範囲で行われます。高速スイッチングされた PBR では、ほとんどの match コマンドおよび set コマンドを使用できます。PBR の高速スイッチングをイネーブルにするには、事前に PBR をイネーブルにする必要があります。PBR の高速スイッチングは、デフォルトでディセーブルです。

スイッチで生成されたパケット（ローカル パケット）は通常、ポリシー ルーティングされません。スイッチ上でローカル PBR をグローバルにイネーブル化すると、そのスイッチから送信されるすべてのパケットがローカル PBR の対象となります。ローカル PBR は、デフォルトでディセーブルに設定されています。

PBR を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [**permit**] [*sequence number*]	パケットの出力場所を制御するために使用するルート マップを定義し、ルートマップ コンフィギュレーション モードを開始します。 • *map-tag*：ルート マップ用のわかりやすい名前を指定します。**ip policy route-map** インターフェイス コンフィギュレーション コマンドでは、この名前を使用してルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。 • （任意）**permit** が指定され、このルート マップの一致基準が満たされている場合は、set アクションの制御に従ってルートがポリシールーティングされます。 **（注）** インターフェイスに適用される PBR ルート マップでは、**route-map deny** 文はサポートされていません。 • *sequence number*（任意）：すでに同じ名前が設定されているルート マップのリスト内で、新しいルート マップの位置を表す番号を指定します。
ステップ 3	**match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	1 つまたは複数の標準アクセス リストまたは拡張アクセス リストで許可されている送信元 IP アドレスおよび宛先 IP アドレスを一致基準にします。 **（注）** 拒否 ACE を含む ACL や、ローカル アドレス宛のパケットを許可する ACL は入力しないでください。 **match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。
ステップ 4	**set ip next-hop** *ip-address* [*...ip-address*]	基準と一致するパケットの動作を指定します。パケットのルーティング先となるネクスト ホップを設定します（ネクスト ホップは隣接していなければなりません）。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 7	**no shutdown**	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 8	**ip policy route-map** *map-tag*	レイヤ 3 インターフェイス上で PBR をイネーブルにし、使用するルート マップを指定します。1 つのインターフェイスに設定できるルート マップは 1 つだけです。ただし、シーケンス番号が異なる複数のルート マップ エントリを設定できます。これらのエントリは、最初の一致が検出されるまで、シーケンス番号順に評価されます。一致が検出されない場合、パケットは通常どおりにルーティングされます。 **（注）** IP ポリシー ルート マップに **deny** 文が含まれている場合、設定は失敗します。

	コマンド	目的
ステップ 9	**ip route-cache policy**	（任意）PBR の高速スイッチングをイネーブルにします。PBR の高速スイッチングをイネーブルにするには、まず PBR をイネーブルにする必要があります。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**ip local policy route-map** *map-tag*	（任意）ローカル PBR をイネーブルにして、スイッチから送信されるパケットに対して PBR を実行します。ローカル PBR は、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show route-map** [*map-name*]	（任意）設定を確認するため、設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。
ステップ 14	**show ip policy**	（任意）インターフェイスに適用されたポリシー ルート マップを表示します。
ステップ 15	**show ip local policy**	（任意）ローカル PBR がイネーブルであるかどうかを表示します。またイネーブルの場合は、使用されているルート マップも表示します。
ステップ 16	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

エントリを削除するには、**no route-map** *map-tag* グローバル コンフィギュレーション コマンド、**no match** ルート マップ コンフィギュレーション コマンド、または **no set** ルート マップ コンフィギュレーション コマンドを使用します。インターフェイス上で PBR をディセーブルにするには、**no ip policy route-map** *map-tag* インターフェイス コンフィギュレーション コマンドを使用します。PBR の高速スイッチングをディセーブルにするには、**no ip route-cache policy** インターフェイス コンフィギュレーション コマンドを使用します。スイッチから送信されるパケットに対して PBR をディセーブルにするには、**ip local policy route-map** *map-tag* グローバル コンフィギュレーション コマンドを使用します。

ルーティング情報のフィルタリング

ここでは、ルーティング プロトコル情報をフィルタリングする手順について説明します。

（注）　OSPF プロセス間でルートが再配布される場合、OSPF メトリックは保持されません。

受動インターフェイスの設定

ローカル ネットワーク上の他のルータがルートをダイナミックに学習しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用して、ルーティング アップデート メッセージがルータ インターフェイスを経由して送信されないようにします。OSPF プロトコルでこのコマンドを使用すると、受動として指定したインターフェイス アドレスが OSPF ドメインのスタブ ネットワークとして表示されます。OSPF ルーティング情報は、指定されたルータ インターフェイスを経由しては送受信されません。

多数のインターフェイスが存在するネットワークで、手動による受動インターフェイスの設定を省くには、**passive-interface default** ルータ コンフィギュレーション コマンドを使用して、すべてのインターフェイスをデフォルトで受動インターフェイスになるように設定します。そのうえで、隣接関係が必要なインターフェイスを手動で設定します。

受動インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**passive-interface** *interface-id*	指定されたレイヤ 3 インターフェイス経由のルーティング アップデートの送信を抑制します。
ステップ 4	**passive-interface default**	（任意）すべてのインターフェイスを、デフォルトで受動インターフェイスとなるように設定します。
ステップ 5	**no passive-interface** *interface type*	（任意）隣接関係を送信する必要があるインターフェイスだけをアクティブにします。
ステップ 6	**network** *network-address*	（任意）ルーティング プロセス用のネットワーク リストを指定します。*network-address* には IP アドレスを指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

受動インターフェイスとしてイネーブルにしたインターフェイスを確認するには、**show ip ospf interface** などのネットワーク モニタリング特権 EXEC コマンドを使用します。アクティブとしてイネーブルにしたインターフェイスを確認する場合は、**show ip interface** 特権 EXEC コマンドを使用します。

ルーティング アップデートの送信を再度イネーブルにするには、**no passive-interface** *interface-id* ルータ コンフィギュレーション コマンドを使用します。キーワード **default** を指定すると、すべてのインターフェイスがデフォルトで受動インターフェイスに設定されます。このとき、**no passive-interface** ルータ コンフィギュレーション コマンドを使用することで、隣接関係を必要とする各インターフェイスを個別に設定できます。**default** キーワードは、ほとんどの配信ルータに 200 を超えるインターフェイスが備わっているインターネット サービス プロバイダーや大規模な企業ネットワークで使用するのが有効です。

ルーティング アップデートのアドバタイズおよび処理の制御

ACL と **distribute-list** ルータ コンフィギュレーショ ンコマンドを組み合せて使用すると、ルーティング アップデート中にルートのアドバタイズを抑制し、他のルータが 1 つまたは複数のルートを学習しないようにできます。この機能は、OSPF で使用した場合、外部ルートにだけ適用されるため、インターフェイス名は指定できません。

distribute-list ルータ コンフィギュレーション コマンドを使用して、着信したアップデートのリストのうち特定のルートを処理しないようにすることもできます （この機能は OSPF には適用されません）。

ルーティング アップデートのアドバタイズまたは処理を制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distribute-list** {*access-list-number* | *access-list-name*} **out** [*interface-name* | *routing process* | *autonomous-system-number*]	アクセス リスト内のアクションに応じて、ルーティング アップデート内のルートのアドバタイズを許可または拒否します。

	コマンド	目的
ステップ 4	**distribute-list** {*access-list-number* | *access-list-name*} **in** [*type-number*]	アップデートにリストされたルートの処理を抑制します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

フィルタを変更または取り消すには、**no distribute-list in** ルータ コンフィギュレーション コマンドを使用します。アップデート中のネットワーク アドバタイズメントの抑制を取り消すには、**no distribute-list out** ルータ コンフィギュレーション コマンドを使用します。

ルーティング情報の送信元のフィルタリング

ルーティング情報には、それぞれの正確性に差があることもあります。そこで、さまざまな送信元から送られる情報には、フィルタリングを使用することによりプライオリティを設定できるようになっています。「*管理ディスタンス*」は、ルータやルータ グループといったルーティング情報の送信元に対する信頼度を表した数値です。大規模ネットワークでは、各ルーティング プロトコルの信頼度に違いがある場合があります。管理ディスタンスの値を指定すると、ルーティング情報の送信元がルータによって自動的に区別されるようになります。ルータでは常に、ルーティング プロトコルの管理ディスタンスが最短（値が最小）であるルートが選択されます。表 36-16（P.36-104）は、ルーティング情報のさまざまな送信元に対するデフォルトの管理ディスタンスをまとめたものです。

各ネットワークには独自の要件があるため、管理ディスタンスを割り当てる一般的な注意事項はありません。

ルーティング情報の送信元をフィルタリングするには、特権 EXEC モードで、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distance** *weight* {*ip-address* {*ip-address mask*}} [*ip access list*]	管理ディスタンスを定義します。 *weight*：管理ディスタンスを 10 ～ 255 の整数として指定します。*weight* を単独で使用すると、デフォルトの管理ディスタンスが指定されます。デフォルトの管理ディスタンスは、ルーティング情報の送信元に対して他の指定事項がない場合に使用されます。管理ディスタンスが 255 のルートはルーティング テーブルに格納されません。 （任意）*ip access list*：着信ルーティング アップデートに適用される IP 標準または IP 拡張アクセス リストです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols**	指定されたルーティング プロセス用のデフォルトの管理ディスタンスを表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

管理ディスタンスを削除するには、**no distance** ルータ コンフィギュレーション コマンドを使用します。

認証鍵の管理

鍵管理を使用すると、ルーティング プロトコルで使用される認証鍵を制御できます。一部のプロトコルでは、鍵管理を使用できません。認証鍵は EIGRP および RIP バージョン 2 で使用できます。

認証鍵の管理を行うには、あらかじめ認証をイネーブルにしておく必要があります。各プロトコルに対して認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。認証鍵の管理を行うには、キー チェーンを定義したあと、そのキー チェーンに属する鍵を指定し、それぞれの鍵の有効期間を指定します。それぞれの鍵には、ローカルに保存される独自の鍵 ID があります（**key** *number* キー チェーン コンフィギュレーション コマンドで指定）。鍵 ID、およびメッセージに関連付けられたインターフェイスの組み合せにより、使用中の認証アルゴリズムおよび Message Digest 5（MD5）認証鍵が一意に識別されます。

鍵は有効期間とともに複数設定できます。ただし、有効な鍵が複数存在する場合でも、送信される認証パケットは 1 つだけです。鍵番号は小さい方から大きい方へ順に調べられ、最初に見つかった有効な鍵が使用されます。鍵変更中は、有効期間が重なっても問題ありません。これらの有効期間は、ルータに通知する必要があります。

認証鍵を管理するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**key chain** *name-of-chain*	キー チェーンを指定し、キーチェーン コンフィギュレーション モードを開始します。
ステップ 3	**key** *number*	鍵番号を指定します。指定できる範囲は 0 ～ 2147483647 です。
ステップ 4	**key-string** *text*	キー ストリングを指定します。このストリングには 1 ～ 80 文字の大文字および小文字の英数字を指定できますが、先頭文字には数字を使用できません。
ステップ 5	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）鍵を受信できる期間を指定します。 *start-time* および *end-time* の構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無期限です。指定できる最初の日付は 1993 年 1 月 1 日です。*end-time* および **duration** のデフォルトは **infinite** です。
ステップ 6	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）鍵を送信できる期間を指定します。 *start-time* および *end-time* の構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無期限です。指定できる最初の日付は 1993 年 1 月 1 日です。*end-time* および **duration** のデフォルトは infinite です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show key chain**	認証鍵情報を表示します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

キー チェーンを削除するには、**no key chain** *name-of-chain* グローバル コンフィギュレーション コマンドを使用します。

IP ネットワークのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。ルートを消去したり、ステータスを表示したりするには、表 36-17 に示す特権 EXEC コマンドを使用します。

表 36-17　IP ルートの消去またはルート ステータスの表示に使用するコマンド

コマンド	目的
clear ip route {*network* [*mask* | ***]}	IP ルーティング テーブルから 1 つまたは複数のルートを消去します。
show ip protocols	アクティブなルーティング プロトコル プロセスのパラメータおよび状態を表示します。
show ip route [*address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	ルーティング テーブルの現在の状態をサマリー形式で表示します。
show ip route supernets-only	スーパーネットを表示します。
show ip cache	IP トラフィックのスイッチングに使用されるルーティング テーブルを表示します。
show route-map [*map-name*]	設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。

CHAPTER 37

IPv6 ユニキャスト ルーティングの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに IPv6 ユニキャスト ルーティングを設定する方法について説明します。

IPv4 ユニキャスト ルーティングの設定の詳細については、第 36 章「IP ユニキャスト ルーティングの設定」を参照してください。IPv6 Access Control List（ACL; アクセス コントロール リスト）の設定の詳細については、第 39 章「IPv6 ACL の設定」を参照してください。

この機能を使用するには、スイッチでメトロ IP アクセス イメージが稼動している必要があります。IPv6 ルーティングをイネーブルにするには、スイッチがデュアル IPv4 および IPv6 Switch Database Management（SDM; スイッチ データベース管理）テンプレートを使用するように設定する必要があります。「デュアル IPv4 および IPv6 プロトコル スタック」（P.37-5）を参照してください。

（注） この章で使用するコマンドの構文および使用方法の詳細については、手順に記載された Cisco IOS のマニュアルを参照してください。

- 「IPv6 の概要」（P.37-1）
- 「IPv6 の設定」（P.37-9）
- 「IPv6 の表示」（P.37-26）

IPv6 の概要

IPv4 ユーザが IPv6 に移行すると、エンドツーエンド セキュリティ、QoS（Quality Of Service）、およびグローバルに一意なアドレスなどのサービスを利用できます。IPv6 アドレス スペースにより、プライベート アドレス、およびネットワーク エッジの境界ルータでの Network Address Translation（NAT; ネットワーク アドレス変換）の必要性が減少します。

シスコシステムズの IPv6 実装方法の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能の詳細については、

- 次の URL から『*Cisco IOS IPv6 Configuration Guide*』にアクセスしてください。
  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.html
- Cisco.com の [Search] フィールドを使用し、Cisco IOS ソフトウェア マニュアルを特定します。たとえば、スタティック ルートについての情報が必要な場合は、[Search] フィールドに [*Implementing Static Routes for IPv6*] と入力すると、スタティック ルートに関する複数のマニュアルへのリンクが表示されます。

ここでは、スイッチへの IPv6 実装について説明します。内容は次のとおりです。

- 「IPv6 アドレス」（P.37-2）
- 「サポート対象の IPv6 ユニキャスト ルーティング機能」（P.37-2）
- 「サポートされていない IPv6 ユニキャスト ルーティング機能」（P.37-8）
- 「制限事項」（P.37-9）

IPv6 アドレス

スイッチがサポートするのは、IPv6 ユニキャスト アドレスだけです。サイトローカルなユニキャスト アドレス、エニーキャスト アドレス、またはマルチキャスト アドレスをサポートしていません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進数フィールド（n:n:n:n:n:n:n:n 形式）で表されます。次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）を使用して、ゼロが連続する 16 進数フィールドを表すことができます。ただし、この短縮形は、各アドレスで一回だけ使用できます。

2031:0:130F::09C0:080F:130B

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Information About Implementing Basic Connectivity for IPv6」の章の、次のセクションの内容がスイッチに適用できます。

- 「IPv6 Address Formats」
- 「IPv6 Address Type: Unicast」
- 「IPv6 Address Output Display」
- 「Simplified IPv6 Packet Header」

サポート対象の IPv6 ユニキャスト ルーティング機能

スイッチでは、拡張アドレス機能、ヘッダー形式の単純化、拡張子およびオプションのより高度なサポート、および拡張ヘッダーのハードウェア解析などがサポートされています。また、ホップバイホップの拡張ヘッダー パケットもサポートしており、これらをソフトウェアでルーティングまたはブリッジングします。

スイッチは、802.1Q トランク ポートによる IPv6 ルーティング（スタティック ルートの場合）機能、IPv6 対応の Routing Information Protocol（RIP）、および Open Shortest Path First（OSPF）バージョン 3 プロトコルを提供します。等価コスト ルートは 16 個までサポートされ、IPv4 および IPv6 フレームを回線レートで同時に転送できます。

- 「128 ビット幅のユニキャスト アドレス」（P.37-3）
- 「IPv6 の DNS」（P.37-4）
- 「IPv6 ユニキャストのパス MTU ディスカバリ」（P.37-4）

- 「ICMPv6」（P.37-4）
- 「近隣探索」（P.37-4）
- 「デフォルト ルータ プリファレンス（DRP）」（P.37-4）
- 「IPv6 のステートレス自動設定および重複アドレス検出」（P.37-5）
- 「IPv6 アプリケーション」（P.37-5）
- 「デュアル IPv4 および IPv6 プロトコル スタック」（P.37-5）
- 「IPv6 の DHCP アドレス割り当て」（P.37-6）
- 「IPv6 のスタティック ルート」（P.37-6）
- 「IPv6 の RIP」（P.37-6）
- 「IPv6 の OSPF」（P.37-7）
- 「EIGRP IPv6」（P.37-7）
- 「IPv6 のマルチプロトコル BGP」（P.37-7）
- 「IPv6 上の NMP および Syslog」（P.37-7）
- 「IPv6 上の HTTP」（P.37-8）

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクローカルなユニキャスト アドレスをサポートします。サイトローカルなユニキャスト アドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能なグローバル ユニキャスト プレフィクスの付いた IPv6 アドレスとなります。このアドレス構造を使用すると、ルーティング プレフィクスを厳格に集約でき、グローバル ルーティング テーブル内のルーティング テーブル エントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

  これらのアドレスはグローバル ルーティング プレフィクス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレスの割り当てには、バイナリ値 001（2000::/3）から開始するアドレス範囲が使用されます。プレフィクスが 2000::/3（001）から E000::/3（111）のアドレスには、Extended Unique Identifier（EUI）64 形式に 64 ビット インターフェイス ID を設定する必要があります。

- リンク ローカルなユニキャスト アドレスをすべてのインターフェイスに自動的に設定するには、修飾 EUI フォーマット内で、リンクローカルなプレフィクス FE80::/10（1111 1110 10）およびインターフェイス ID を使用します。Neighbor Discovery Protocol（NDP; 近隣探索プロトコル）およびステートレス自動設定プロセスでは、リンクローカルなアドレスを使用します。ローカル リンク上のノードは、リンクローカルなアドレスを使用します。通信においてグローバルに一意なアドレスは不要です。IPv6 ルータは、リンクローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある IPv6 ユニキャスト アドレスについてのセクションを参照してください。

IPv6 の DNS

IPv6 では、Domain Name System（DNS; ドメイン ネーム システム）の名前/アドレスおよびアドレス/名前の検索プロセスの DNS レコード タイプがサポートされています。DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートし、IPv4 A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチは Maximum Transmission Unit（MTU; システム最大伝送ユニット）の IPv6 ノードへのアドバタイズおよびパス MTU ディスカバリをサポートします。パス MTU ディスカバリを使用すると、ホストは指定されたデータ パスを通るすべてのリンクの MTU サイズの違いを動的に検出して、サイズに合せて調整できます。IPv6 では、パスを通るリンクの MTU サイズが小さくてパケット サイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。スイッチは、マルチキャスト パケットのパス MTU ディスカバリをサポートしません。

ICMPv6

IPv6 の Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）は ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、近隣探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

近隣探索

スイッチは、IPv6 の NDP（ICMPv6 の最上部で稼動するプロトコル）、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリーもサポートします。IPv6 近隣探索プロセスは ICMP メッセージおよび送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンクレイヤ アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 ビット未満のルートについて、ICMPv6 リダイレクトをサポートします。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトはサポートされません。

近隣探索スロットリングにより、IPv6 パケットをルーティングするためのネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不要な負荷がかかりません。スイッチがアクティブに解決を試行しているのと同じネイバーをネクストホップとした IPv6 パケットが追加されると、スイッチはそのパケットをドロップします。ドロップすることにより、CPU に余分な負荷がかかりません。

デフォルト ルータ プリファレンス（DRP）

スイッチは、ルータのアドバタイズメント メッセージの拡張である、IPv6 Default Router Preference（DRP; デフォルト ルータ プリファレンス）をサポートします。DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。その後、宛先用に選択されたルータは、宛先キャッシュに格納されます。IPv6 の NDP では、到達可能性が不明または信用できないルータより、到達可能または到達可能の可能性のあるルータが指定されます。NDP は、到達可能または到達可能の可能性のあるルータとして、常に同じルータを

選択するか、またはルータ リストから順番に選択できます。到達可能または到達可能の可能性がある 2 台のルータが存在する場合、DRP を使用することにより、IPv6 ホストがどちらか一方を優先するよう設定できます。

IPv6 の DRP の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチはステートレス自動設定を使用して、ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイト アドレス指定の変更を管理します。ホストは、リンクローカルな独自アドレスを自律設定します。起動元ノードはルータに送信要求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレスの検出の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

- Ping、traceroute、Telnet、TFTP、FTP
- IPv6 トランスポートによる Secure Shell（SSH; セキュア シェル）
- IPv6 トランスポートによる HTTP サーバ アクセス
- IPv4 トランスポートによる AAA の DNS リゾルバ
- IPv6 アドレスの Cisco Discovery Protocol（CDP; シスコ検出プロトコル）サポート

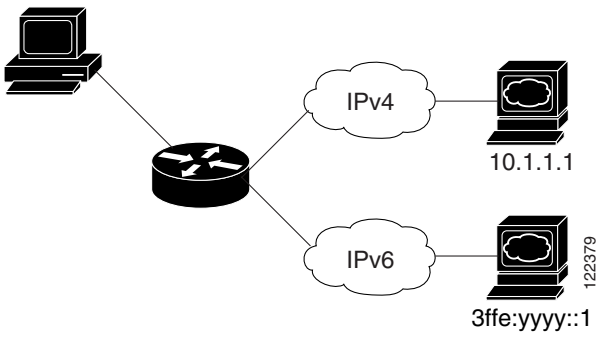
これらのアプリケーションを管理する機能については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4 および IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方でハードウェア メモリの使用を割り当てるには、デュアル IPv4 および IPv6 のテンプレートを使用する必要があります。

図 37-1 に、IP パケットおよび宛先アドレスに基づいて、同じインターフェイスを介して IPv4 および IPv6 トラフィックを転送するルータを示します。

図 37-1　インターフェイス上でのデュアル IPv4 および IPv6 のサポート



デュアル IPv4 および IPv6 スイッチ データベース管理（SDM）テンプレートを使用して、IPv6 のルーティング デュアル スタック環境（IPv4 および IPv6 の両方をサポートする）をイネーブルにします。デュアル IPv4 および IPv6 SDM テンプレートの詳細については、第 7 章「SDM テンプレートの設定」を参照してください。

- 最初にデュアル IPv4/IPv6 テンプレートを選択しないで IPv6 を設定しようとすると、警告メッセージが表示されます。
- IPv4 専用環境のスイッチは、IPv4 パケットをルーティングし、IPv4 の QoS および ACL をハードウェアで適用します。IPv6 パケットはサポートされません。
- デュアル IPv4 および IPv6 環境のスイッチは、IPv4 および IPv6 パケットを両方ルーティングし、IPv4 の QoS をハードウェアで適用します。
- IPv6 QoS はサポートされません。
- デュアル スタック テンプレートを使用すると、各リソースのハードウェア メモリ容量が少なくなるため、IPv6 を使用する予定がない場合はこのテンプレートを使用しないでください。

IPv4 および IPv6 のプロトコル スタックの詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 の DHCP アドレス割り当て

DHCPv6 により、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。アドレス割り当て機能は、ホストが接続されているネットワークに基づいて、適切なプレフィクスでの重複しないアドレス割り当てを管理します。アドレスは、1 つまたは複数のプレフィクス プールから割り当てられます。デフォルト ドメインおよび DNS ネーム サーバ アドレスなど、その他のオプションは、クライアントに戻すことができます。アドレス プールは、特定のインターフェイス、または複数のインターフェイス上で使用する場合に割り当てられます。また、サーバが自動的に適切なプールを検出できます。

このマニュアルでは、DHCPv6 のアドレスの割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、リレー エージェント機能の設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーク デバイス間のルートを明示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 の RIP

IPv6 の Routing Information Protocol（RIP）はルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル プロトコルです。IPv6 アドレスおよびプレフィクスのサポートや、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

IPv6 の RIP の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 の OSPF

スイッチは、IP のリンク ステート プロトコルとして IPv6 の Open Shortest Path First（OSPF）をサポートします。詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSFP for IPv6」の章を参照してください。

EIGRP IPv6

スイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP; Enhanced IGRP）をサポートします。IPv6 の EIGRP は稼動するインターフェイスで設定されるため、グローバルな IPv6 アドレスは不要です。

EIGRP IPv6 インスタンスでは、実行する前に暗黙的または明示的なルータ ID が必要です。暗黙的なルータ ID はローカルの IPv4 アドレスを基にして作成されるため、すべての IPv4 ノードには常に使用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードだけが含まれるネットワークで稼動している可能性もあるため、使用可能な IPv4 ルータ ID がない場合があります。

IPv6 の EIGRP の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 のマルチプロトコル BGP

マルチプロトコル Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）は、IPv6 でサポートされている外部ゲートウェイ プロトコルです。IPv6 用のマルチプロトコル BGP 拡張は、IPv4 BGP と同じ機能をサポートします。IPv6 のマルチプロトコル BGP への拡張には、IPv6 アドレス ファミリーへのサポート、Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着可能性情報）、および IPv6 アドレスを使用するネクストホップ（宛先へのパスの中の次のルータ）のアトリビュートが含まれます。

スイッチは、IPv6 または BGP IPv6 へのマルチキャスト BGP および Non-Stop Forwarding（NSF）をサポートしません。

IPv6 の BGP 設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Multiprotocol BGP for IPv6」の章を参照してください。

IPv6 上の NMP および Syslog

IPv4 および IPv6 の両方をサポートするには、IPv6 ネットワーク管理で IPv6 および IPv4 両方のトランスポートが必要です。IPv6 上の Syslog では、これらのトランスポートのアドレス データ タイプをサポートします。

IPv6 の SNMP および Syslog は、次の機能を提供します。

- IPv4 および IPv6 の両方に対するサポート
- SNMP 用の IPv6 トランスポート、および SNMP エージェントを変更し、IPv6 ホストのトラップをサポートするための IPv6 トランスポート
- IPv6 アドレッシングをサポートするための SNMP および Syslog 関連の MIB
- トラップ レシーバーとしての IPv6 ホストの設定

IPv6 上のサポートのため、SNMP は既存の IP トランスポート マッピングが IPv4 と IPv6 を同時にサポートするように変更します。IPv6 トランスポート管理をサポートする SNMP 動作は、次のとおりです。

- User Datagram Protocol（UDP; ユーザ データグラム プロトコル）の SNMP ソケットをデフォルト設定でオープンする

- 新しいトランスポート メカニズム（*SR_IPV6_TRANSPORT*）を提供する
- IPv6 トランスポート上で SNMP 通知を送信する
- IPv6 トランスポート用の SNMP の名前つきアクセス リストをサポートする
- IPv6 トランスポートを使用し SNMP プロキシ転送をサポートする
- SNMP マネージャ機能が IPv6 トランスポートと連動していることを確認する

IPv6 上の SNMP（設定手順を含む）の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Guide*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

IPv6 上の Syslog（設定手順を含む）の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 上の HTTP

HTTP クライアントは、IPv4 および IPv6 の両方の HTTP サーバに要求を送信し、HTTP サーバは IPv4 および IPv6 両方の HTTP クライアントからの要求に応答します。リテラルな IPv6 アドレスを持つ URL は、コロン区切りの 16 ビット値を使用した 16 進数表記で指定する必要があります。

受信ソケット コールは、IPv4 または IPv6 のアドレス ファミリーを選択します。受信ソケットは IPv4 ソケットまたは IPv6 ソケットのいずれかになります。リスニング ソケットは、接続を伝える IPv4 信号および IPv6 信号の両方の受信を待機します。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされます。

基本的な TCP/IP スタックはデュアルスタック環境をサポートしています。HTTP は、ネットワーク レイヤの相互作用の処理に、TCP/IP スタックおよびソケットを使用します。

HTTP 接続が確立される前に、クライアントとサーバ ホスト間に基本的なネットワーク接続（**ping**）が存在している必要があります。

詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

- IPv6 ポリシー ベース ルーティング
- IPv6 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の Routing And Forwarding（VRF; VPN ルーティングおよび転送）テーブルのサポート
- Intermediate System-to-Intermediate System（IS-IS）ルーティングのサポート
- サイトローカルなアドレス宛の IPv6 パケット
- IPv4/IPv6 または IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 ユニキャスト Reverse-Path Forwarding（RPF）
- IPv6 の一般的なプレフィクス
- IPv6 の HSRP

制限事項

スイッチでは IPv6 はハードウェアに実装されるため、ハードウェアメモリ内の IPv6 圧縮アドレスを使用することによる制限がいくつか発生します。これらのハードウェア制限により、機能の一部が失われたり制限されます。

- IPv6 関連機能で User-Network Interface（UNI; ユーザ ネットワーク インターフェイス）または Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）ポートを使用している場合、IPv6 ルーティングを使用していなくても、最初に **ip routing** および **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを入力し、スイッチでの IP ルーティングおよび IPv6 ルーティングをグローバルでイネーブルに設定する必要があります。
- IPv6 ホスト ルート（特定のホストに到達するために使用されるルート）またはマスク長が 64 ビットを越える IPv6 ルートでは、ICMPv6 リダイレクト機能がサポートされません。ホスト ルートまたはマスク長が 64 ビットを越えるルートを介して到達可能な特定の宛先の場合、スイッチは適性のより高い先頭ホップ ルータにホストをリダイレクトできません。
- IPv6 ホスト ルートまたはマスク長が 64 ビットを越える IPv6 ルートの場合、等価コストおよび不等価コスト ルートを使用するロード バランスはサポートされません。
- スイッチは、SNAP カプセル化 IPv6 パケットを正しく転送できません。

（注） SNAP カプセル化された IPv4 パケットでも同様の制限がありますが、パケットはスイッチで破棄されます。

- スイッチは、IPv6/IPv4 および IPv4/IPv6 パケットをハードウェアでルーティングしますが、スイッチを IPv6/IPv4 または IPv4/ IPv6 トンネル エンドポイントにはできません。
- ホップ単位の拡張ヘッダーを持つ、ブリッジングされた IPv6 パケットは、ソフトウェアで転送されます。IPv4 の場合、これらのパケットはソフトウェアでルーティングされ、ハードウェアでブリッジングされます。
- ソフトウェア コンフィギュレーション ガイドで定義された通常の SPAN および RSPAN 制限の他に、次のような IPv6 パケット固有の制限事項があります。
  - RSPAN IPv6 ルーテッド パケットを送信した場合、SPAN 出力パケット内の送信元 MAC アドレスが間違っている場合があります。
  - RSPAN IPv6 ルーテッド パケットを送信した場合、宛先 MAC アドレスが間違っている場合があります。標準トラフィックは影響を受けません。
- スイッチは、ソースルート IPv6 パケットに関する QoS 分類または Policy-Based Routing（PBR; ポリシーベース ルーティング）をハードウェアで適用できません。
- スイッチは、マルチキャスト パケットに対して ICMPv6 `Packet Too Big` メッセージを生成できません。

IPv6 の設定

- 「IPv6 のデフォルト設定」（P.37-10）
- 「IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化」（P.37-10）
- 「デフォルト ルータ プリファレンスの設定」（P.37-12）
- 「IPv4 および IPv6 プロトコル スタックの設定」（P.37-13）
- 「IPv6 の DHCP アドレス割り当ての設定」（P.37-15）

- 「IPv6 ICMP レート制限の設定」（P.37-18）
- 「IPv6 の CEF の設定」（P.37-19）
- 「IPv6 のスタティック ルーティングの設定」（P.37-19）
- 「IPv6 RIP の設定」（P.37-21）
- 「IPv6 OSPF の設定」（P.37-22）
- 「IPv6 の EIGRP の設定」（P.37-24）
- 「IPv6 の BGP の設定」（P.37-24）

IPv6 のデフォルト設定

表 37-1 に、IPv6 のデフォルト設定を示します。

表 37-1　IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルト
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル。
CEFv6	ディセーブル（IPv4 CEF はデフォルトでイネーブル）。 **（注）**　IPv6 ルーティングがイネーブルの場合、CEFv6 は自動的にイネーブル。
IPv6 アドレス	設定なし。

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化

スイッチ上で IPv6 を設定するときは、次の注意事項に従ってください。

- デュアル IPv4 および IPv6 SDM テンプレートを選択してください。
- スイッチでは、この章で説明したすべての機能がサポートされるわけではありません。「サポートされていない IPv6 ユニキャスト ルーティング機能」（P.37-8）を参照してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、*ipv6-address* および *ipv6-prefix* の各変数を、16 ビット値を使用したコロン区切りの 16 進数表記でアドレスを指定して入力する必要があります。変数 *prefix-length*（先頭にスラッシュ [/] を付加）は、プレフィクス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進数です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバルな IPv6 アドレスを設定する必要があります。インターフェイスに IPv6 アドレスを設定すると、リンクローカルなアドレスが自動的に設定され、そのインターフェイスで IPv6 が有効になります。設定されたインターフェイスは、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャスト アドレスの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスは近隣探索プロセスに使用される）
- すべてのノードを含む、リンクローカルなマルチキャスト グループ FF02::1
- すべてのルーター含む、リンクローカルなマルチキャスト グループ FF02::2

IPv6 ルーティングの設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

レイヤ 3 インターフェイスに IPv6 アドレスを割り当てて、IPv6 ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**}	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 • **default**：スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 • **routing**：スイッチをルーティング テンプレートに設定して、IPv4 ポリシーベース ルーティングなどの IPv4 および IPv6 ルーティングをサポートします。 • **vlan**：ハードウェアでのルーティングをサポートしないスイッチでの、VLAN コンフィギュレーションを最適化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**reload**	オペレーティング システムをリロードします。
ステップ 5	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。インターフェイスは、物理インターフェイス、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、またはレイヤ 3 EtherChannel に設定できます。
ステップ 7	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 8	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **ipv6 address** *ipv6-address* **link-local** または **ipv6 enable**	IPv6 アドレスの 下位 64 ビットの Extended Unique Identifier（EUI）を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィクスだけを指定します。最後の 64 ビットはスイッチの MAC アドレスから自動的に算出されます。これにより、インターフェイス上での IPv6 処理がイネーブルになります。 インターフェイスのリンクローカルなアドレスを指定します。このアドレスは、インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクローカルなアドレスの代わりに使用します。このコマンドにより、インターフェイス上での IPv6 処理がイネーブルになります。 インターフェイスで IPv6 のリンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクローカルなアドレスは、同じリンク上のノードと通信する場合にだけ使用されます。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ip routing**	スイッチ上で IP ルーティングをイネーブルにします。
ステップ 11	**ipv6 unicast-routing**	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 12	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 13	**show ipv6 interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **no ipv6 address** *ipv6-address* **link-local** の各インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスでの IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 プレフィクス 2001:0DB8:c18:1::/64 に基づく、リンクローカルなアドレスとグローバルアドレスを使用して、IPv6 をイネーブルにする例を示します。両方のアドレスの下位 64 ビットでは、EUI-64 インターフェイス ID が使用されます。**show ipv6 interface** EXEC コマンドからの出力は、インターフェイスのリンクローカルなプレフィクス FE80::/64 にインターフェイス ID（20B:46FF:FE2F:D940）を付加する方法を示すために追加されています。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet0/11
GigabitEthernet0/2 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

デフォルト ルータ プリファレンスの設定

ルータ アドバタイズメント メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定される Default Router Preference（DRP; デフォルト ルータ プリファレンス）とともに送信されます。DRP が設定されていない場合、ルータ アドバタイズメントは中小規模のプリファレンスとともに送信されます。

リンク上の 2 つのルータが、等価であってもルーティングが等価コストではない場合、およびポリシーによってホストがいずれかのルータを選択するよう指示されている場合は、DRP が有効です。

インターフェイス上のルータで DRP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、DRP を指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	**ipv6 nd router-preference** {**high** | **medium** | **low**}	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 DRP をディセーブルにするには、**no ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス上のルータに*高い* DRP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv6 の DRP の設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv4 および IPv6 プロトコル スタックの設定

IPv6 ルーティングを設定する前に、IPv4 および IPv6 をサポートする SDM テンプレートを選択する必要があります。まだ設定していない場合、**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} **global** コンフィギュレーション コマンドを使用して、IPv6 をサポートするテンプレートを設定します。新しいテンプレートを選択する場合は、**reload** 特権 EXEC コマンドを使用してスイッチをリロードし、テンプレートを有効にする必要があります。

IPv4 および IPv6 を両方サポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**}	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 • **default**：スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 • **routing**：スイッチをルーティング テンプレートに設定して、IPv4 ポリシーベース ルーティングなどの IPv4 および IPv6 ルーティングをサポートします。 • **vlan**：ハードウェアでのルーティングをサポートしないスイッチでの、VLAN コンフィギュレーションを最適化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**reload**	オペレーティング システムをリロードします。
ステップ 5	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 6	**ip routing**	スイッチ上で IPv4 ルーティングをイネーブルにします。
ステップ 7	**ipv6 unicast-routing**	スイッチ上での IPv6 データ パケットの転送をイネーブルに設定します。
ステップ 8	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 9	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 10	**ip address** *ip-address mask* [**secondary**]	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 11	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **ipv6 address** *ipv6-address* **link-local** または **ipv6 enable**	グローバル IPv6 アドレスを指定します。ネットワーク プレフィクスだけを指定します。最後の 64 ビットはスイッチの MAC アドレスから自動的に算出されます。 インターフェイスのリンクローカルなアドレスを指定します。このアドレスは、インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクローカルなアドレスの代わりに使用します。 インターフェイスで IPv6 のリンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクローカルなアドレスは、同じリンク上のノードと通信する場合にだけ使用されます。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show interface** *interface-id* **show ip interface** *interface-id* **show ipv6 interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv4 ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。IPv6 ルーティングをディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。インターフェイスの IPv4 アドレスを削除する場合は、**no ip address** *ip-address mask* インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **no ipv6 address** *ipv6-address* **link-local** の各インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスでの IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス上で IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

IPv6 の DHCP アドレス割り当ての設定

- 「DHCPv6 アドレス割り当てのデフォルト設定」（P.37-15）
- 「DHCPv6 アドレス割り当ての注意事項」（P.37-15）
- 「DHCPv6 サーバ機能のイネーブル化」（P.37-16）
- 「DHCPv6 クライアント機能のイネーブル化」（P.37-18）

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトでは、スイッチに Dynamic Host Configuration Protocol for IPv6（DHCPv6）機能は設定されていません。

DHCPv6 アドレス割り当ての注意事項

DHCPv6 アドレス割り当てを設定するときは、次の注意事項に従ってください。

- 以下の手順では、次のレイヤ 3 インターフェイスのうちいずれか 1 つを指定する必要があります。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイスでイネーブルに設定する必要があります。
  - SV：**interface vlan** *vlan_id* コマンドを使用して作成された VLAN インターフェイスです。
  - レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel port-channel-number** コマンドを使用して作成された ポートチャネル論理インターフェイスです。
- DHCPv6 を設定するときは、事前に IPv4 および IPv6 をサポートする SDM（スイッチ データベース管理）テンプレートを選択しておく必要があります。
- スイッチは、DHCPv6 クライアント、サーバ、リレー エージェントとして動作できます。DHCPv6 クライアント、サーバ、およびリレー機能は、1 つのインターフェイスでは同時に指定できません。

DHCPv6 サーバ機能のイネーブル化

インターフェイスで DHCPv6 サーバ機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 dhcp pool** *poolname*	DHCP プール コンフィギュレーション モードを開始し、IPv6 DHCP プールの名前を定義します。プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 3	**address prefix** *IPv6-prefix* **lifetime** {*t1 t1* | **infinite**}	（任意）アドレス割り当て用のアドレス プレフィクスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数にする必要があります。 **lifetime** *t1 t1*：IPv6 アドレス プレフィクスが有効ステータスを維持するタイム インターバル（秒）を指定します。指定できる範囲は 5 ～ 4294967295 秒です。時間間隔を指定しない場合は**無制限**になります。
ステップ 4	**link-address** *IPv6-prefix*	（任意）リンクアドレス IPv6 プレフィクスを指定します。 着信インターフェイスのアドレスまたはパケット内のリンクアドレスが指定の IPv6 プレフィクスと一致した場合、サーバは構成情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数にする必要があります。
ステップ 5	**vendor-specific** *vendor-id*	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有の ID 番号を入力します。この番号はベンダーの IANA 民間企業番号です。指定できる範囲は 1 ～ 4294967295 です。
ステップ 6	**suboption** *number* {**address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string*}	（任意）ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進数の文字列をサブオプション パラメータによって定義されたものとして入力します。
ステップ 7	**exit**	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンド	目的
ステップ 10	**ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]	インターフェイスで DHCPv6 サーバ機能をイネーブルにします。 • *poolname*：（任意）IPv6 DHCP プールのユーザ定義の名前です。プール名は、記号文字列（Engineering など）または整数（0 など）です。 • **automatic**：（任意）システムはクライアントにアドレスを割り当てる際に使用するプールを自動的に決定できます。 • **rapid-commit**：（任意）2 つのメッセージ交換方式を可能にします。 • **preference** *value*：（任意）サーバが送信するアドバタイズ メッセージの preference オプションで伝送される preference 値。指定できる範囲は 0 ～ 255 です。デフォルトの preference 値は 0 です。 • **allow-hint**：（任意）サーバが送信請求メッセージでクライアントの提案を考慮するかどうか指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ipv6 dhcp pool** または **show ipv6 dhcp interface**	DHCPv6 プール コンフィギュレーションを確認します。 DHCPv6 サーバ機能がインターフェイスでイネーブルに設定されていることを確認します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCPv6 プールを削除するには、**no ipv6 dhcp pool** *poolname* グローバル コンフィギュレーション コマンドを使用します。DHCPv6 プールの特性を変更するには、DHCP プール コンフィギュレーション モード コマンドの **no** 形式を使用します。インターフェイス上の DHCPv6 サーバ機能をディセーブルに設定するには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

次に、IPv6 アドレス プレフィクスを持つ *engineering* と呼ばれるプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)#address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 つのリンク アドレスと IPv6 アドレス プレフィクスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次の例では、ベンダー固有のオプションのある *350* というプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化

インターフェイスで DHCPv6 クライアント機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ipv6 address dhcp** [**rapid-commit**]	インターフェイスで、DHCPv6 サーバから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当ての 2 つのメッセージ交換方式を可能にします。
ステップ 4	**ipv6 dhcp client request** [**vendor-specific**]	（任意）インターフェイスが、ベンダー固有のオプションを要求するように設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 dhcp interface**	DHCPv6 クライアント機能がインターフェイスでイネーブルに設定されていることを確認します。

DHCPv6 クライアント機能をディセーブルにするには、**no ipv6 address dhcp** インターフェイス コンフィギュレーション コマンドを使用します。DHCPv6 クライアント要求を削除するには、**no ipv6 address dhcp client request** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、IPv6 アドレスを取得し、rapid-commit オプションをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

このマニュアルでは、DHCPv6 のアドレスの割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、リレー エージェント機能の設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 ICMP レート制限の設定

ICMP レート制限は、デフォルトでイネーブルに設定されています。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルトのバケット サイズ（バケットに格納される最大トークン数）は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 icmp error-interval** *interval* [*bucketsize*]	IPv6 ICMP エラー メッセージの間隔およびバケット サイズを設定します。 • *interval* : バケットに追加されるトークンの間隔（ミリ秒）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize* :（任意）バケットに格納される最大トークン数。指定できる範囲は 1 ～ 200 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 interface** [*interface-id*]	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ipv6 icmp error-interval** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Switch(config)#ipv6 icmp error-interval 50 20
```

IPv6 の CEF の設定

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）は、パケット転送により多くの CPU 処理能力を割り当てることが可能な、レイヤ 3 IP スイッチング テクノロジーです。デフォルトでは、IPv4 CEF はイネーブル化されています。IPv6 CEF はデフォルトではディセーブルに設定されていますが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ユニキャスト パケットをルーティングするには、最初に **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャスト パケットの転送をグローバルに設定します。また、**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用し、インターフェイスでの IPv6 アドレスおよび IPv6 処理を設定する必要があります。

IPv6 CEF をディセーブルに設定するには、**no ipv6 cef** グローバル コンフィギュレーション コマンドを使用します。IPv6 CEF をふたたびイネーブルに設定するには、**ipv6 cef** グローバル コンフィギュレーション コマンドを使用します。IPv6 ステートを確認するには、**show ipv6 cef** 特権 EXEC コマンドを入力します。

CEF の設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 のスタティック ルーティングの設定

スタティック IPv6 ルートの設定前には、次の処理を実行する必要があります。

- **ip routing** グローバル コンフィギュレーション コマンドを使用して、ルーティングをイネーブルに設定します。
- **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 パケットの転送をイネーブルに設定します。

- インターフェイスに IPv6 アドレスを設定して、少なくとも 1 つの IPv6 をレイヤ 3 インターフェイスでイネーブルに設定します。

IPv6 スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*]	スタティック IPv6 ルートを設定します。 • *ipv6-prefix* : スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートが設定されている場合は、ホスト名を設定することもできます。 • */prefix length* : IPv6 プレフィクスの長さ。プレフィクスの（アドレスのネットワーク部）の上位連続ビット数を示す 10 進値です。スラッシュ記号を 10 進値の前に付ける必要があります。 • *ipv6-address* : 指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。ネクスト ホップは直接接続する必要はありません。再帰処理が実行されて、直接接続されているネクスト ホップの IPv6 アドレスを検出します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 • *interface-id* : ポイントツーポイント インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。ポイントツーポイント インターフェイスの場合は、ネクスト ホップの IPv6 アドレスを指定する必要はありません。ブロードキャスト インターフェイスの場合は、ネクスト ホップの IPv6 アドレスを常に指定するか、または、リンクに対するローカル アドレスをネクスト ホップとして指定し、指定したプレフィックスがリンクに割り当てられるよう設定する必要があります。パケットが送信されるネクスト ホップの IPv6 アドレスを指定することもできます。 **（注）** リンクに対するローカル アドレスをネクスト ホップとして使用する場合は、*interface-id* を指定する必要があります。リンクに対するローカル ネクスト ホップは、隣接ルータに設定する必要があります。 • *administrative distance* :（任意）管理ディスタンス。指定できる範囲は 1 から 254 です。デフォルト値は 1 で、接続されたルートを除くすべてのルートよりもスタティック ルートが優先されます。フローティング スタティック ルートを設定するには、ダイナミック ルーティング プロトコルより大きい管理ディスタンスを使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**recursive**] [**detail**] または **show ipv6 route static** [*updated*]	IPv6 ルーティング テーブルを表示し、エントリを確認します。 • ***interface*** interface-id：（任意）出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートだけを表示します。 • **recursive**（任意）：再帰スタティック ルートだけを表示します。キーワード **recursive** は、キーワード **interface** と相互に排他的です。ただし、コマンド構文に IPv6 プレフィクスが指定されている場合も、指定されていない場合も使用できます。 • **detail**：（任意）次に示す追加情報を表示します。 – 有効な再帰ルートの場合、出力パス セットと最大分解深度。 – 無効なルートの場合、ルートが無効な理由。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定されたスタティック ルートを削除するには、**no ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] グローバル コンフィギュレーション コマンドを使用します。

次に、フローティング スタティック ルートをインターフェイスに設定する例を示します。このルートの管理ディスタンスは 130 です。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130
```

スタティックな IPv6 ルーティング設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 RIP の設定

IPv6 RIP を実行するようにスイッチを設定する前には、次の処理を実行する必要があります。

- **ip routing** グローバル コンフィギュレーション コマンドを使用して、ルーティングをイネーブルに設定します。
- **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 パケットの転送をイネーブルに設定します。
- IPv6 RIP をイネーブルに設定するレイヤ 3 インターフェイス上で IPv6 をイネーブルに設定する必要があります。

IPv6 RIP を設定するには、特権 EXEC モードで次の必須手順または任意の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router rip** *name*	IPv6 RIP ルーティング プロセスを設定し、このプロセスのルータ コンフィギュレーション モードを開始します。
ステップ 3	**maximum-paths** *number-paths*	（任意）IPv6 RIP がサポート可能な等価コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 64 です。デフォルトは 4 ルートです。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。

	コマンド	目的
ステップ 6	**ipv6 rip** *name* **enable**	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルに設定します。
ステップ 7	**ipv6 rip** *name* **default-information** {**only** | **originate**}	（任意）IPv6 デフォルト ルート（::/0）を、特定のインターフェイスから送信された RIP ルーティング プロセス アップデートに発信します。 **（注）** 任意のインターフェイスから IPv6 デフォルト ルート（::/0）を送信した後に、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。 • **only**：デフォルト ルートを送信し、このインターフェイスに送信されたアップデートの他のすべてのルートを抑制する場合に選択します。 • **originate**：このインターフェイスに送信された他のすべてのルートに加え、デフォルト ルートからも送信する場合に選択します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ipv6 rip** [*name*] [**interface** *interface-id*] [**database**] [**next-hops**] または **show ipv6 route rip** [*updated*]	現在の IPv6 RIP プロセスに関する情報を表示します。 IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RIP ルーティング プロセスをディセーブルに設定するには、**no ipv6 router rip** *name* グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して RIP ルーティング プロセスをディセーブルに設定するには、**no ipv6 rip** *name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、RIP プロセス *cisco* に最大 8 つの等価コスト ルートをイネーブルにし、インターフェイス上でこれをイネーブルに設定する例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# ipv6 rip cisco enable
```

IPv6 の RIP ルーティング設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 OSPF の設定

ネットワークでは、IPv6 OSPF をカスタマイズできます。ただし、デフォルト設定でほとんどのカスタマー要件と機能要件を満たします。

次の注意事項に従ってください。

- IPv6 コマンドのデフォルトを変更する場合は注意してください。変更することにより、IPv6 ネットワークの OSPF に悪影響を与える場合があります。

- インターフェイスで IPv6 OSPF をイネーブルにする前に、次の処理を実行する必要があります。
  - **ip routing** グローバル コンフィギュレーション コマンドを使用して、ルーティングをイネーブルに設定します。
  - **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 パケットの転送をイネーブルに設定します。
  - IPv6 OSPF をイネーブルに設定するレイヤ 3 インターフェイスで IPv6 をイネーブルに設定します。

IPv6 OSPF を設定するには、特権 EXEC モードで次の必須手順または任意の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router ospf** *process-id*	プロセスに対して OSPF ルータ コンフィギュレーション モードをイネーブルに設定します。プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルに設定したときに管理上割り当てられる番号です。この ID はローカルに割り当てられ、1 から 65535 までの正の整数を指定できます。
ステップ 3	**area** *area-id* **range** {*ipv6-prefix/prefix length*} [**advertise** | **not-advertise**] [**cost** *cost*]	（任意）エリア境界でルートを統合し、サマライズします。 • *area-id* : ルートをサマライズするエリアの ID。10 進数または IPv6 プレフィクスのいずれかで指定できます。 • *ipv6-prefix/prefix length :* IPv6 ネットワークの宛先、およびプレフィクス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進数。10 進値の前にスラッシュ記号（/）を付ける必要があります。 • **advertise**：（任意）Type 3 サマリー Link-State Advertisement（LSA; リンクステートアドバタイズメント）をアドバタイズ、生成するようにアドレス範囲ステータスを設定します。 • **not-advertise** : アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままとなります。 • **cost** *cost* :（任意）このサマリー ルートのメトリックまたはコスト。宛先への最短パスを決定する OSPF SPF 計算で使用します。指定できる値は 0 ～ 16777215 です。
ステップ 4	**maximum paths** *number-paths*	（任意）IPv6 OSPF がルーティング テーブルに入力する必要のある、同じ宛先への等価コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 64 です。デフォルトは 16 です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]	インターフェイスの IPv6 OSPF をイネーブルにします。 • **instance** *instance-id* :（任意）インスタンス ID。
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*] または **show ipv6 ospf** [*process-id*] [*area-id*]	OSPF インターフェイスについての情報を表示します。 OSPF ルーティング プロセスに関する一般的な情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF ルーティング プロセスをディセーブルに設定するには、no **ipv6 router ospf** *process-id* グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して OSPF ルーティング プロセスをディセーブルに設定するには、**no ipv6 ospf** *process-id* **area** *area-id* インターフェイス コンフィギュレーション コマンドを使用します。

IPv6 の OSPF ルーティング設定の詳細は、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

IPv6 の EIGRP の設定

デフォルトでは、IPv6 の EIGRP はディセーブルに設定されています。IPv6 の EIGRP は、インターフェイスで設定できます。ルータとインターフェイスを EIGRP 用に設定した後に、**no shutdown** 特権 EXEC コマンドを入力して EIGRP を開始します。

（注）　IPv6 の EIGRP がシャットダウン モードでない場合、EIGRP ルータモード コマンドを入力してルータおよびインターフェイスを設定する前に、EIGRP が稼動を開始する場合があります。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定されたルータ ID を参照してから、**router-id** コマンドを使用します。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv4 インターフェイスを指定し、そのサブセットを受動インターフェイスとして選択できます。**passive-interface default** コマンドを使用して、すべてのインターフェイスを受動インターフェイスに設定してから、選択したインターフェイスに対して **no passive-interface** コマンドを使用してアクティブに設定します。EIGRP IPv6 を受動インターフェイスとして設定する必要はありません。

設定手順の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 の BGP の設定

マルチプロトコル BGP の IPv6 拡張を設定する場合、BGP ルーティング プロセスの作成、ピアリング関係の設定、および特定のネットワーク向けの BGP のカスタマイズを行う必要があります。IPv6 において、BGP は IPv4 における場合と同様に動作します。IPv6 用に BGP を稼動させるようルータを設定する前に、**ipv6 unicast-routing** コマンドを使用し IPv6 ルーティングをグローバルでイネーブルに設定します。

IPv6 の BGP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number*	BGP ルーティング プロセスを設定し、自律システム番号を使用して BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**no bgp default ipv4-unicast**	前の手順で指定した BGP ルーティング プロセスに対する IPv4 ユニキャスト アドレス ファミリーをディセーブルに設定します。 IPv4 ユニキャスト アドレス ファミリーのルーティング情報は、デフォルトでは各 BGP ルーティング セッションに対してアドバタイズされていますが、**neighbor remote-as** コマンドを設定する前にこのコマンドを入力して、変更できます。
ステップ 4	**bgp router-id** *ip-address*	（任意）BGP が稼動しているローカル ルータの ID として固定 32 ビット ルータ ID を設定します。デフォルトでは、ルータ ID はルータ ループバック インターフェイスの IPv4 アドレスです。IPv6 だけに対してイネーブルに設定されているルータ（IPv4 アドレスはなし）では、BGP ルータ ID を手動で設定する必要があります。 **（注）** このコマンドを使用してルータ ID を設定すると、アクティブな BGP ピアリング セッションはすべてリセットされます。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*	指定された自律システムのネイバーの IPv6 アドレスを、ローカル ルータの IPv6 マルチプロトコル BGP ネイバー テーブルに追加します。 **（注）** *ipv6-address* は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
ステップ 6	**address-family ipv6**	IPv6 アドレス ファミリーを指定し、アドレス ファミリー コンフィギュレーション モードを開始します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**	ローカル ルータとの IPv6 アドレス ファミリーのプレフィクスの交換を、ネイバーでイネーブルに設定します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show bgp ipv6**	IPv6 BGP コンフィギュレーションの情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定手順の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Multiprotocol BGP for IPv6」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.html

スイッチは、マルチキャスト IPv6 BGP、IPv6 BGP の Nonstop Forwarding（NSF）、6PE マルチパス（EoMPLS）、および IPv6 VRF はサポートしません。

IPv6 の表示

これらのコマンドの構文および使用方法の詳細については、Cisco IOS コマンド リファレンスを参照してください。

表 37-2　IPv6 のモニタ用コマンド

コマンド	目的
show bgp ipv6	BGP IPv6 コンフィギュレーションおよびルーティング テーブルを表示します。
show ipv6 access-list	IPv6 のアクセス リストを表示します。
show ipv6 cef	IPv6 の Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）を表示します。
show ipv6 interface *interface-id*	IPv6 インターフェイスのステータスおよびコンフィギュレーションを表示します。
show ipv6 mtu	宛先キャッシュごとの IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 ospf	IPv6 の OSPF 情報を表示します。
show ipv6 prefix-list	IPv6 プレフィクス リストを表示します。
show ipv6 protocols	スイッチの IPv6 ルーティング プロトコルを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコルのステータスを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 37-3　EIGRP IPv6 情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [*as-number*] *interface*	EIGRP IPv6 用に設定されたインターフェイスの情報を表示します。
show ipv6 eigrp [*as-number*] *neighbor*	EIGRP IPv6 で検出されたネイバーを表示します。
show ipv6 eigrp [*as-number*] *traffic*	送受信された EIGRP IPv6 パケット数を表示します。
show ipv6 eigrp topology [*as-number* | *ipv6-address*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]	IPv6 トポロジ テーブルの EIGRP エントリを表示します。

表 37-4　IPv4 および IPv6 アドレス タイプを表示するためのコマンド

コマンド	目的
show ip http server history	HTTP サーバとの最新の 20 の接続を表示します。表示には、アクセスされた IP アドレスおよび接続がクローズされた時間が含まれます。
show ip http server connection	HTTP サーバとの現在の接続を表示します。表示には、アクセスされたローカル IP アドレスおよびリモート IP アドレスが含まれます。

表 37-4　IPv4 および IPv6 アドレス タイプを表示するためのコマンド （続き）

コマンド	目的
show ip http client connection	HTTP サーバとの HTTP クライアントの接続の設定値を表示します。
show ip http client history	HTTP クライアントからサーバへの最新の 20 の要求を表示します。

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

次に、**show ipv6 cef** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 cef
::/0
  nexthop 3FFE:C000:0:7::777 Vlan7
3FFE:C000:0:1::/64
  attached to Vlan1
3FFE:C000:0:1:20B:46FF:FE2F:D940/128
  receive
3FFE:C000:0:7::/64
  attached to Vlan7
3FFE:C000:0:7::777/128
  attached to Vlan7
3FFE:C000:0:7:20B:46FF:FE2F:D97F/128
  receive
3FFE:C000:111:1::/64
  attached to GigabitEthernet0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to GigabitEthernet0/43
3FFE:C000:168:1:20B:46FF:FE2F:D94B/128
  receive
3FFE:C000:16A:1::/64
  attached to Loopback10
3FFE:C000:16A:1:20B:46FF:FE2F:D900/128
  receive

<output truncated>
```

次に、**show ipv6 protocols** 特権 EXEC コマンドの出力の出力例を示します。

```
Switch# show ipv6 protocols
IPv6 Routing Protocol is "connected"
```

```
IPv6 Routing Protocol is “static”
IPv6 Routing Protocol is “rip fer”
  Interfaces:
    Vlan6
GigabitEthernet0/4
GigabitEthernet0/11
GigabitEthernet0/12
  Redistribution:
    None
```

次に、**show ipv6 rip** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 rip
RIP process "fer", port 521, multicast-group FF02::9, pid 190
     Administrative distance is 120. Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 9040, trigger updates 60
  Interfaces:
    Vlan6
GigabitEthernet0/4
GigabitEthernet0/11
GigabitEthernet0/12
Redistribution:
    None
```

次に、**show ipv6 neighbor** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
3FFE:C000:0:7::777                          - 0007.0007.0007  REACH Vl7
3FFE:C101:113:1::33                         - 0000.0000.0033  REACH Gi0/13
```

次に、**show ipv6 static** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via nexthop 3FFE:C000:0:7::777, distance 1
```

次に、**show ipv6 route** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 route
IPv6 Routing Table - 21 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 3FFE:C000:0:7::777
C   3FFE:C000:0:1::/64 [0/0]
     via ::, Vlan1
L   3FFE:C000:0:1:20B:46FF:FE2F:D940/128 [0/0]
     via ::, Vlan1
C   3FFE:C000:0:7::/64 [0/0]
     via ::, Vlan7
L   3FFE:C000:0:7:20B:46FF:FE2F:D97F/128 [0/0]
     via ::, Vlan7
C   3FFE:C000:111:1::/64 [0/0]
     via ::, GigabitEthernet0/11
L   3FFE:C000:111:1:20B:46FF:FE2F:D945/128 [0/0]
C   3FFE:C000:168:1::/64 [0/0]
```

```
     via ::, GigabitEthernet0/4
L   3FFE:C000:168:1:20B:46FF:FE2F:D94B/128 [0/0]
     via ::, GigabitEthernet0/4
C   3FFE:C000:16A:1::/64 [0/0]
     via ::, Loopback10
L   3FFE:C000:16A:1:20B:46FF:FE2F:D900/128 [0/0]
     via ::, Loopback10

<output truncated>
```

次に、**show ipv6 traffic** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  36861 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
         0 RPF drops, 0 RPF suppressed drops
  Mcast: 1 received, 36861 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 9944 router advert, 0 redirects
        84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

CHAPTER 38

IPv6 MLD スヌーピングの設定

Cisco ME 3400E イーサネット アクセス スイッチがメトロ IP アクセス イメージを実行している場合、Multicast Listener Discovery（MLD）スヌーピングを使用して、スイッチ ネットワーク内のクライアントおよびルータに IP バージョン 6（IPv6）マルチキャスト データを効率的に配信できます。

（注） IPv6 を使用するには、スイッチにデュアル IPv4 および IPv6 Switch Database Management（SDM; スイッチ データベース管理）テンプレートを設定しておく必要があります。テンプレートは、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力して選択します。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、第 7 章「SDM テンプレートの設定」を参照してください。
- スイッチの IPv6 の詳細については、第 37 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、または手順に記載された Cisco IOS のマニュアルを参照してください。

この章で説明する内容は、次のとおりです。

- 「MLD スヌーピングの概要」（P.38-1）
- 「IPv6 MLD スヌーピングの設定」（P.38-5）
- 「MLD スヌーピング情報の表示」（P.38-12）

MLD スヌーピングの概要

IP バージョン 4（IPv4）では、IP マルチキャスト デバイスに関連付けられたインターフェイスにだけマルチキャスト トラフィックが転送されるように、レイヤ 2 インターフェイスを動的に設定することで、レイヤ 2 スイッチは Internet Group Management Protocol（IGMP）スヌーピングを利用してマルチキャスト トラフィックのフラッディングを制限できます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングにより IPv6 マルチキャスト データは、VLAN 内のすべてのポートにフラッディングされることなく、データの受信先であるポートのリストに選択的に転送されます。このリストは IPv6 マルチキャスト制御パケットをスヌーピングすることにより作成されます。

MLD は、直接接続されているリンク上のマルチキャスト リスナー（IPv6 マルチキャスト パケットの受信先となるノード）の検出、および近接ノードに送る必要があるマルチキャスト パケットの検出のために、IPv6 マルチキャスト ルータによって使用されるプロトコルです。MLD は IGMP から派生したものです。MLD バージョン 1（MLDv1）は IGMPv2 と同等、MLD バージョン 2（MLDv2）は IGMPv3 と同等です。MLD は Internet Control Message Protocol バージョン 6（ICMPv6）のサブプロトコルであり、MLD メッセージは、先行する Next Header の値 58 によって IPv6 パケットとして識別される ICMPv6 メッセージのサブセットです。

このスイッチは次の 2 つのバージョンの MLD スヌーピングをサポートしています。

- MLDv1 スヌーピングは MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 basic snooping（MBSS; MLDv2 基本スヌーピング）は MLDv2 制御パケットを使用し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方をスヌーピングし、宛先 IPv6 マルチキャスト アドレスに基づいて IPv6 マルチキャスト データのブリッジングを実行します。

（注）　このスイッチは、IPv6 の送信元と宛先のマルチキャスト アドレスに基づいて転送を設定する、MLDv2 enhanced snooping（MESS; MLDv2 拡張スヌーピング）はサポートしていません。

MLD スヌーピングは VLAN ごとに、またはグローバルにイネーブルまたはディセーブルに設定できます。MLD スヌーピングがイネーブルに設定されると、VLAN 単位の IPv6 マルチキャスト MAC アドレス テーブルがソフトウェア内で作成され、また VLAN 単位の IPv6 マルチキャスト アドレス テーブルがソフトウェア内とハードウェア内で作成されます。次に、スイッチは、IPv6 マルチキャスト アドレスに基づくブリッジングをハードウェアで行います。

ここでは、IPv6 MLD スヌーピングのパラメータの一部について説明します。

- 「MLD メッセージ」（P.38-2）
- 「MLD クエリー」（P.38-3）
- 「マルチキャスト クライアント エージングのロバストネス」（P.38-3）
- 「マルチキャスト ルータ ディスカバリ」（P.38-3）
- 「MLD レポート」（P.38-4）
- 「MLD Done メッセージと即時脱退」（P.38-4）
- 「トポロジー変更通知の処理」（P.38-5）

MLD メッセージ

MLDv1 は次の 3 つのタイプのメッセージをサポートします。

- リスナー クエリーは IGMPv2 クエリーと同等であり、一般クエリーまたは Multicast-Address-Specific Query（MASQ）のいずれかとなります。
- マルチキャスト リスナー レポートは IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージは IGMPv2 Leave メッセージと同等です。

MLDv2 は、MLDv2 クエリーおよびレポートのほか、MLDv1 レポートおよび Done メッセージもサポートします。

メッセージ タイマーおよびメッセージの送受信の結果による状態の遷移は IGMPv2 メッセージと同一です。有効なリンクローカル IPv6 送信元アドレスのない MLD メッセージは MLD ルータと MLD スイッチでは無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築して、MLD グループ固有クエリーと、MLD グループおよび送信元固有クエリーを、MLD Done メッセージへの応答として生成します。このスイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタティック IPv6 マルチキャスト MAC アドレス設定もサポートします。

MLD スヌーピングがディセーブルに設定されると、すべての MLD クエリーは入力側 VLAN にフラッディングされます。

MLD スヌーピングがイネーブルにされると、受信した MLD クエリーが入力側 VLAN にフラッディングされ、クエリーのコピーが CPU に送られて処理されます。MLD スヌーピングは受信したクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャスト ルータ ポートを検出、タイマーを管理して、レポート応答時間を設定、VLAN のクエリア IP 送信元アドレスおよび VLAN 内のクエリア ポートを学習し、マルチキャスト アドレス エージングを管理します。

（注）　IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）が使用されている場合は、Catalyst 6500 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

MLD スヌーピング データベース内にグループが存在する場合、スイッチは MLDv1 レポートを送信してグループ固有クエリーに応答します。グループが不明の場合、グループ固有クエリーは入力側 VLAN にフラッディングされます。

ホストがマルチキャスト グループを脱退する時には、MLD Done メッセージ（IGMP Leave メッセージと同等）を送信します。スイッチが MLDv1 Done メッセージを受信したときに、即時脱退がイネーブルにされていない場合は、スイッチはメッセージの送信元になっているポートに MASQ を送信し、そのポートに接続されている他のデバイスがマルチキャスト グループに残るべきかどうかを判断します。

マルチキャスト クライアント エージングのロバストネス

アドレスからのポートのメンバーシップの削除を、クエリーの数に基づいて行うように設定できます。ポートは、設定された数のクエリーのレポートがポート上のアドレスに送られなかった場合にだけ、アドレスへのメンバーシップから削除されます。デフォルト値は 2 です。

マルチキャスト ルータ ディスカバリ

IGMP スヌーピングと同様に、MLD スヌーピングもマルチキャスト ルータ ディスカバリを実行します。MLD スヌーピングには次のような特徴があります。

- ユーザによって設定されたポートは期限切れにはならない。
- MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットによるダイナミックなポート学習。
- 同じレイヤ 2 インターフェイス上に複数のルータが存在する場合は、MLD スヌーピングはそのポート上の単一のマルチキャスト ルータ（一番最後にルータ制御パケットを送信したルータ）だけを追跡します。

- ダイナミック マルチキャスト ルータ ポート エージングのデフォルト タイマーは 5 分です。ポート上で 5 分間、制御パケットが受信されなかった場合、マルチキャスト ルータはルータ ポート リストから削除されます。
- IPv6 マルチキャスト ルータ ディスカバリは、スイッチで MLD スヌーピングがイネーブルにされている場合にだけ実行されます。
- 受信した IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルにされているかどうかに関係なく、常に入力側 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートを検出したら、不明な IPv6 マルチキャスト データは、検出されたルータ ポートにだけ転送されます（それ以前のものは、すべての IPv6 マルチキャスト データは入力側 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージの処理は、基本的に IGMPv2 と同じです。VLAN 内で IPv6 マルチキャスト ルータが検出されない場合は、レポートは処理されず、スイッチから転送もされません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートを受信した場合は、IPv6 マルチキャスト グループ アドレスおよび IPv6 マルチキャスト MAC アドレスが VLAN MLD データベースに登録されます。次に、VLAN 内のグループへ向かうすべての IPv6 マルチキャスト トラフィックは、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルに設定されると、レポートは入力側 VLAN にフラッディングされます。

MLD スヌーピングがイネーブルに設定されると、MLD レポート抑制（リスナー メッセージ抑制）が自動的にイネーブルに設定されます。スイッチはレポートを抑制して、グループで受信した最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。そのグループへの後続のレポートは、ルータには送られなくなります。MLD スヌーピングがディセーブルにされている場合、レポート抑制はディセーブルになり、MLDv1 レポートはすべて入力側 VLAN にフラッディングされます。

スイッチは MLDv1 プロキシ レポーティングもサポートしています。MLDv1 MASQ を受信すると、スイッチは、グループがスイッチ内の別のポートに存在する場合、およびクエリーを受信したポートがそのアドレスの最後のメンバー ポートではない場合は、クエリーを受信したアドレスに対して MLDv1 レポートで応答します。

MLD Done メッセージと即時脱退

即時脱退機能がイネーブルに設定された状態で、ホストが MLDv1 Done メッセージ（IGMP leave メッセージに相当）を送信した場合、Done メッセージを受信したポートは即座にグループから削除されます。VLAN 上で即時脱退（および IGMP スヌーピング）をイネーブルにする場合、ポートに単一のホストが接続されている VLAN でだけ、この機能を使用してください。ポートがグループの最後のメンバーの場合は、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN 内で即時脱退がイネーブルにされておらず（同一ポート上のグループに複数のクライアントが存在する場合が該当）、Done メッセージをポートで受信した場合、そのポートで MASQ が生成されます。ユーザは、既存アドレスからポートのメンバーシップをいつ削除するかを、MASQ の数によって制御できます。ポートは、設定された数のクエリーの MLDv1 レポートがポート上のアドレスに送られなかった場合に、アドレスへのメンバーシップから削除されます。

生成される MASQ の数は **ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルト値は 2 です。

MASQ は、Done メッセージを受信した IPv6 マルチキャスト アドレスに送られます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなかった場合、MASQ を受信したポートは IPv6 マルチキャスト データベースから削除されます。最大応答時間は **ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドを使用して設定します。削除されたポートがマルチキャスト アドレスの最後のメンバーである場合、マルチキャスト アドレスも削除され、スイッチはアドレス脱退情報をすべての検出済みマルチキャスト ルータに送信します。

トポロジー変更通知の処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して topology change notification（TCN; トポロジー変更通知）送信要求をイネーブルに設定した場合、MLDv1 スヌーピングは、選択したポートだけにマルチキャスト データの送信を開始する前に、設定した数の MLDv1 クエリーの送信により、すべての IPv6 マルチキャスト トラフィックをフラッディングするよう、VLAN を設定します。この値は **ipv6 mld snooping tcn flood query count** グローバル コンフィギュレーション コマンドで設定します。デフォルトでは 2 つのクエリーを送信します。スイッチは、VLAN 内で STP ルートになった場合、またはユーザによって設定された場合には、有効なリンクローカル IPv6 送信元アドレスを含む MLDv1 global Done メッセージも生成します。これは IGMP スヌーピングと同様です。

IPv6 MLD スヌーピングの設定

ここでは、IPv6 MLD スヌーピングの設定方法を説明します。

- 「MLD スヌーピングのデフォルト設定」（P.38-5）
- 「MLD スヌーピング設定時の注意事項」（P.38-6）
- 「MLD スヌーピングのイネーブル化またはディセーブル化」（P.38-6）
- 「スタティック マルチキャスト グループの設定」（P.38-8）
- 「マルチキャスト ルータ ポートの設定」（P.38-8）
- 「MLD 即時脱退のイネーブル化」（P.38-9）
- 「MLD スヌーピング クエリーの設定」（P.38-10）
- 「MLD リスナー メッセージ抑制のディセーブル化」（P.38-11）

MLD スヌーピングのデフォルト設定

表 38-1 は、MLD スヌーピングのデフォルト設定をまとめたものです。

表 38-1　MLD スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング（グローバル）	ディセーブル。
MLD スヌーピング（VLAN 単位）	イネーブル。VLAN MLD スヌーピングを使用するには、MLD スヌーピングがグローバルにイネーブルになっていることが必要です。
IPv6 マルチキャスト アドレス	設定なし。

表 38-1　MLD スヌーピングのデフォルト設定 （続き）

機能	デフォルト設定
IPv6 マルチキャスト ルータ ポート	設定なし。
MLD スヌーピング即時脱退	ディセーブル。
MLD スヌーピング ロバストネスの変数	グローバル：2。VLAN 単位：0。 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル カウントを使用します。
最終リスナー クエリー カウント	グローバル：2。VLAN 単位：0。 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル カウントを使用します。
最終リスナー クエリー インターバル	グローバル：1000（1 秒）。VLAN：0。 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル インターバルを使用します。
TCN クエリー送信請求	ディセーブル。
TCN クエリー カウント	2.
MLD リスナー抑制	イネーブル。

MLD スヌーピング設定時の注意事項

MLD スヌーピングを設定するときは、次の注意事項に従ってください。

- MLD スヌーピング特性はいつでも設定できますが、設定を有効にするには、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドで MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）が使用されている場合は、Catalyst 6500 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは互いに独立して動作します。両方の機能をスイッチ上で同時にイネーブルに設定できます。
- スイッチに許可されているマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチに許可されているアドレス エントリの最大数は 1000 です。

MLD スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングは、スイッチ上でグローバルにディセーブルにされており、すべての VLAN でイネーブルに設定されています。MLD スヌーピングがグローバルにディセーブルに設定されていると、すべての VLAN でもディセーブルになります。MLD スヌーピングをグローバルにイネーブルに設定すると、VLAN 設定がグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルト状態（イネーブル）の VLAN インターフェイス上でだけイネーブルになります。

MLD スヌーピングは VLAN 単位、または VLAN の範囲を基準にイネーブルまたはディセーブルに設定できますが、グローバルにディセーブルにすると、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合は、VLAN スヌーピングをイネーブルまたはディセーブルのどちらにも設定できます。

スイッチ上で MLD スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping**	スイッチ上で MLD スヌーピングをグローバルにイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 5	**reload**	オペレーティング システムをリロードします。

スイッチ上で MLD スヌーピングをグローバルにディセーブルにするには、**no ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用します。

VLAN で MLD スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

（注） IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）が使用されている場合は、Catalyst 6500 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping**	スイッチ上で MLD スヌーピングをグローバルにイネーブルにします。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id*	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 **（注）** VLAN スヌーピングをイネーブルにするには、MLD スヌーピングをグローバルにイネーブルにする必要があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN インターフェイスで MLD スヌーピングをディセーブルにするには、指定された VLAN 番号に対して **no ipv6 mld snooping vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

スタティック マルチキャスト グループの設定

ホストまたはレイヤ 2 ポートは、通常はマルチキャスト グループにダイナミックに参加しますが、IPv6 マルチキャスト アドレスと VLAN のメンバー ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **static** *ipv6_multicast_address* **interface** *interface-id*	マルチキャスト グループのメンバーとして、レイヤ 2 ポートをマルチキャスト グループにスタティックに設定します。 • *vlan-id* には、マルチキャスト グループの VLAN ID を指定します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *ipv6_multicast_address* は、128 ビット グループ IPv6 アドレスです。アドレスは、RFC 2373 で指定された形式にします。 • *interface-id* にはメンバー ポートを指定します。物理インターフェイスまたはポート チャネル（1 ～ 48）を指定できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping multicast-address user** or **show ipv6 mld snooping multicast-address vlan** *vlan-id* **user**	スタティック メンバー ポートおよび IPv6 アドレスを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

マルチキャスト グループからレイヤ 2 ポートを削除するには、**no ipv6 mld snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。すべてのメンバー ポートがグループから削除されると、グループは削除されます。

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet0/1
Switch(config)# end
```

マルチキャスト ルータ ポートの設定

MLD スヌーピングは MLD クエリーと PIMv6 クエリーを通じてルータ ポートを学習しますが、コマンドライン インターフェイス（CLI）を使用してマルチキャスト ルータ ポートを VLAN に追加することもできます。マルチキャスト ルータ ポートを追加する（マルチキャスト ルータにスタティック接続を追加する）場合は、スイッチ上で **ipv6 mld snooping vlan mrouter** グローバル コンフィギュレーション コマンドを使用します。

（注） マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id*	マルチキャスト ルータの VLAN ID とインターフェイスをマルチキャスト ルータに指定します。 • 指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping mrouter** [**vlan** *vlan-id*]	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN からマルチキャスト ルータ ポートを削除する場合は、**no ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト ルータ ポートを VLAN 200 に追加する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet0/2
Switch(config)# exit
```

MLD 即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出すると、即座にそのポートをマルチキャスト グループから削除します。即時脱退機能を使用するのは、VLAN の各ポートにレシーバーが 1 つ存在する場合だけです。同一ポート上のマルチキャスト グループに複数のクライアントが存在する場合は、VLAN 内で即時脱退をイネーブルに設定しないでください。

MLDv1 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **immediate-leave**	VLAN インターフェイス上で MLD 即時脱退をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping vlan** *vlan-id*	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN 上で MLD 即時脱退をディセーブルにするには、**no ipv6 mld snooping vlan** *vlan-id* **immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit
```

MLD スヌーピング クエリーの設定

即時脱退がイネーブルに設定されていない状態でポートが MLD Done メッセージを受信した場合、スイッチはポート上で MASQ を生成し、Done メッセージを送信した IPv6 マルチキャスト アドレスに送信します。送信される MASQ の数、およびスイッチがポートをマルチキャスト グループから削除するまでの応答待機時間を任意に設定できます。

スイッチまたは VLAN に対して MLD スヌーピング クエリーの特性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping robustness-variable** *value*	（任意）スイッチが、一般クエリーに応答しないリスナー（ポート）を削除するまでに送信されるクエリーの数を設定します。指定できる範囲は 1 ～ 3 で、デフォルトは 2 です。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value*	（任意）ロバストネス変数を VLAN ベースで設定します。これにより、MLD レポート応答がない場合に、マルチキャスト アドレスの期限が切れるまでに MLD スヌーピングが送信する一般クエリーの数が決まります。指定できる範囲は 1 ～ 3 で、デフォルトは 0 です。0 に設定した場合、グローバルなロバストネス変数値が使用されます。
ステップ 4	**ipv6 mld snooping last-listener-query-count** *count*	（任意）MLD クライアントが期限切れになるまでにスイッチが送信する MASQ の数を設定します。指定できる範囲は 1 ～ 7 で、デフォルトは 2 です。クエリーは 1 秒間隔で送信されます。
ステップ 5	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-count** *count*	（任意）最終リスナー クエリー カウントを VLAN 単位で設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ～ 7 です。デフォルト値は 0 です。0 に設定した場合、グローバル カウント値が使用されます。クエリーは 1 秒間隔で送信されます。
ステップ 6	**ipv6 mld snooping last-listener-query-interval** *interval*	（任意）スイッチがポートをマルチキャスト グループから削除する前に、MASQ 送信後に応答を待機する最大時間を設定します。指定できる範囲は 100 ～ 32,768 ミリ秒です。デフォルト値は 1000（1 秒）です。
ステップ 7	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-interval** *interval*	（任意）最終リスナー クエリー インターバルを VLAN 単位で設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 0 ～ 32,768 ミリ秒です。デフォルト値は 0 です。0 に設定した場合、グローバル最終リスナー クエリー インターバルが使用されます。
ステップ 8	**ipv6 mld snooping tcn query solicit**	（任意）Topology Change Notification（TCN; トポロジー変更通知）送信請求をイネーブルにします。これは受信を要求したポートにだけマルチキャスト データを送信する前に、設定された数のクエリーが送信される間、IPv6 マルチキャスト トラフィックすべてが VLAN にフラッディングされることを意味します。デフォルトは、TCN がディセーブルです。
ステップ 9	**ipv6 mld snooping tcn flood query count** *count*	（任意）TCN がイネーブルの場合、送信される TCN クエリーの数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	**show ipv6 mld snooping querier** [**vlan** *vlan-id*]	（任意）スイッチまたは VLAN の MLD スヌーピング クエリア情報を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、MLD スヌーピング グローバル ロバストネス変数を 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

次に、VLAN の MLD スヌーピング最終リスナー クエリー カウントを 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit
```

次に、MLD スヌーピング最終リスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
```

MLD リスナー メッセージ抑制のディセーブル化

MLD スヌーピング リスナー メッセージ抑制は、デフォルトでイネーブルにされています。この機能がイネーブルになると、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートだけを転送します。メッセージ抑制がディセーブルに設定されている場合は、複数の MLD レポートがマルチキャスト ルータに転送される可能性があります。

MLD リスナー メッセージ抑制をディセーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ipv6 mld snooping listener-message-suppression**	MLD メッセージ抑制をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping**	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD メッセージ抑制を再びイネーブルに設定するには、**ipv6 mld snooping listener-message-suppression** グローバル コンフィギュレーション コマンドを使用します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの MLD スヌーピング情報を表示できます。MLD スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

MLD スヌーピング情報を表示するには、表 38-2 に示す、1 つまたは複数の特権 EXEC コマンドを使用します。

表 38-2　MLD スヌーピング情報を表示するためのコマンド

コマンド	目的
show ipv6 mld snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。 （任意）単一の VLAN に関する情報を表示するには、**vlan** *vlan-id* を使用します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習された、または手動で設定されたマルチキャスト ルータ インターフェイスに関する情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらはダイナミックに学習されるインターフェイスです。 （任意）単一の VLAN に関する情報を表示するには、**vlan** *vlan-id* を使用します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意）単一の VLAN の情報を表示するには、**vlan** *vlan-id* を使用します。VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping multicast-address [**vlan** *vlan-id*] [**count** | **dynamic** | **user**]	スイッチまたは VLAN の、すべての IPv6 マルチキャスト アドレス情報または特定の IPv6 マルチキャスト アドレス情報を表示します。 • スイッチまたは VLAN のグループ カウントを表示するには、**count** を入力します。 • スイッチまたは VLAN の MLD スヌーピング学習グループ情報を表示するには、**dynamic** を入力します。 • スイッチまたは VLAN の MLD スヌーピング ユーザ定義グループ情報を表示するには、**user** を入力します。
show ipv6 mld snooping multicast-address vlan *vlan-id* [*ipv6-multicast-address*]	指定された VLAN および IPv6 マルチキャスト アドレスに対する MLD スヌーピングを表示します。

CHAPTER 39

IPv6 ACL の設定

Cisco ME 3400E イーサネット アクセス スイッチがメトロ IP アクセス イメージを実行している場合、ACL と呼ばれる IP Version 4（IPv4）を作成して適用する場合と同じ方法で、IPv6 Access Control List（ACL; アクセス コントロール リスト）を作成し、それらをインターフェイスに適用して、IP Version 6（IPv6）トラフィックをフィルタリングできます。また、入力ルータ ACL を作成して適用することで、レイヤ 3 管理トラフィックをフィルタできます。

（注） IPv6 を使用するには、スイッチにデュアル IPv4 および IPv6 Switch Database Management（SDM; スイッチ データベース管理）テンプレートを設定しておく必要があります。**sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan}** グローバル コンフィギュレーション コマンドを入力し、テンプレートを選択します。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、第 7 章「SDM テンプレートの設定」を参照してください。
- スイッチの IPv6 の詳細については、第 37 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。
- スイッチの ACL の詳細については、第 32 章「ACL によるネットワーク セキュリティの設定」を参照してください。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、または手順に記載された Cisco IOS のマニュアルを参照してください。

この章の内容は次のとおりです。

- 「IPv6 ACL の概要」（P.39-2）
- 「IPv6 ACL の設定」（P.39-3）
- 「IPv6 ACL の表示」（P.39-8）

IPv6 ACL の概要

メトロ IP アクセス イメージを実行しているスイッチは、次の 2 種類の IPv6 ACL をサポートしています。

- IPv6 ルータ ACL は、レイヤ 3 インターフェイスの発信または着信トラフィックでサポートされています。これらはルーテッド ポート、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、またはレイヤ 3 EtherChannel です。IPv6 ルータ ACL は、ルーテッド IPv6 パケットにだけ適用されます。
- IPv6 ポート ACL は、レイヤ 2 インターフェイスの受信トラフィックでだけサポートされています。IPv6 ポート ACL はインターフェイスに入るすべての IPv6 パケットに適用されます。

スイッチは、IPv6 トラフィックの VLAN ACL（VLAN マップ）をサポートしていません。

サポートされていない IPv6 ACL を設定すると、エラー メッセージが表示され、設定は無効となります。

（注）　スイッチでの IPv4 ACL のサポートの詳細については、第 32 章「ACL によるネットワーク セキュリティの設定」を参照してください。

IPv4 および IPv6 ACL の両方をインターフェイスに適用できます。

IPv4 ACL と同様に、IPv6 ポート ACL は、ルータ ACL より優先されます。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信したルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、パケットはポート ACL によってフィルタリングされます。発信するルーティング IPv6 パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。

（注）　*いずれか*のポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL がパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

ここでは、スイッチの IPv6 ACL の特性の一部について説明します。

- 「サポートされている ACL の機能」（P.39-2）
- 「IPv6 ACL の制限事項」（P.39-3）

サポートされている ACL の機能

スイッチの IPv6 ACL には次の 3 つの特性があります。

- 分割されたフレーム（IPv4 の **fragments** キーワード）はサポートされていません。
- IPv4 でサポートされている統計情報は IPv6 ACL でサポートされます。
- スイッチでハードウェアの領域が不足している場合、ACL に関連付けられているパケットは CPU に転送され、ACL はソフトウェアで適用されます。
- ホップバイホップ オプションによるルーテッド パケットまたはブリッジド パケットでは、IPv6 ACL はソフトウェアで適用されます。

- ロギングは ACL に対してサポートされていますがポート ACL に対してはサポートされていません。
- スイッチでは、全 prefix-length 範囲の IPv6 アドレス照合をサポートしています。

IPv6 ACL の制限事項

IPv4 では、標準番号および拡張番号付き IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 では、名前付き ACL だけがサポートされています。

スイッチでは、Cisco IOS がサポートする多くの IPv6 ACL がサポートされていますが、次の例外があります。

- スイッチでは、**flowlabel**、**routing header**、および **undetermined-transport** の各キーワードでの照合はサポートされていません。
- スイッチでは、再帰 ACL（**reflect** キーワード）はサポートされていません。
- このリリースでは、IPv6 の ポート ACL およびルータ ACL はサポートされていません。また VLAN ACL（VLAN マップ）はサポートされていません。
- スイッチは、IPv6 フレームに MAC ベース ACL を適用しません。
- IPv6 ポート ACL をレイヤ 2 EtherChannel に適用できません。
- スイッチは、出力ポート ACL をサポートしていません。
- ACL を設定する場合、プラットフォームでサポートされているかどうかに関係なく、ACL に入力するキーワードに制限はありません。ACL をハードウェア転送（物理ポートまたは SVI）が必要なインターフェイスに適用する場合、スイッチは ACL がインターフェイスでサポートできるかどうかを確認します。サポートされない場合、ACL 付加は拒否されます。
- ACL がインターフェイスに適用され、サポートされていないキーワードで Access Control Entry（ACE; アクセス制御エントリ）を追加する場合、スイッチは付加 ACL への ACE 追加を許可しません。

IPv6 ACL の設定

IPv6 ACL を設定する前に、デュアル IPv4 および IPv6 SDM テンプレートのいずれかを選択する必要があります。

IPv6 トラフィックをフィルタリングするには、次の手順を実行します。

ステップ 1　IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

ステップ 2　トラフィックをブロック（deny）または許可（permit）するよう、IPv6 ACL を設定します。

ステップ 3　IPv6 ACL をインターフェイスに適用します。ルータ ACL には、ACL が適用される レイヤ 3 インターフェイスに IPv6 アドレスを設定する必要もあります。

- 「IPv6 ACL のデフォルト設定」（P.39-4）
- 「他の機能およびスイッチとの相互作用」（P.39-4）
- 「IPv6 ACL の作成」（P.39-4）
- 「インターフェイスへの IPv6 ACL の適用」（P.39-7）

IPv6 ACL のデフォルト設定

IPv6 ACL は設定も適用もされません。

他の機能およびスイッチとの相互作用

IPv6 ACL を設定すると、他の機能またはスイッチの特性に関して次のような相互作用があります。

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーが Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）キューに送信され、フレームに対して ICMP の Unreachable メッセージが生成されます。
- ポート ACL によりブリッジド フレームがドロップされると、フレームはブリッジされません。
- スイッチで IPv4 および IPv6 ACL を作成でき、IPv4 および IPv6 ACL を同じインターフェイスに適用できます。それぞれの ACL には一意な名前を指定する必要があります。すでに設定されている名前を使用しようとすると、エラーメッセージが表示されます。

  IPv4 および IPv6 ACL を作成し、IPv4 または IPv6 ACL を同じレイヤ 2 またはレイヤ 3 インターフェイスに付加する場合は、異なるコマンドを使用します。誤ったコマンドを使用して ACL を付加（IPv4 コマンドを使用して IPv6 ACL に付加など）すると、エラー メッセージが表示されます。
- MAC ACL は、IPv6 フレームのフィルタリングに使用できません。MAC ACL がフィルタリングできるのは、非 IP フレームだけです。
- ハードウェア メモリが満杯の場合、追加で設定された ACL については、パケットが CPU に転送され、ACL がソフトウェアで適用されます。

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 access-list** *access-list-name*	名前を使用して IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3a	{**deny** | **permit**} *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	**deny** または **permit** を入力して、条件が一致する場合にパケットを拒否するか許可するかを指定します。次に、条件を示します。 • *protocol* に、インターネット プロトコルの名前または番号 **ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、または **udp**、または IPv6 プロトコルの番号を示す整数 0 ～ 255 を入力します。 **（注）** ICMP、TCP、および UDP の具体的なパラメータについては、ステップ 3b ～ 3d を参照してください。 • *source-ipv6-prefix*/*prefix-length* または *destination-ipv6-prefix*/*prefix-length* は、deny または permit 条件を設定するネットワークの送信元または宛先 IPv6 ネットワークまたはクラスで、16 進数で 16 ビットの値を指定し、コロンで囲んで指定します。 • IPv6 プレフィックス ::/0 の省略形として **any** と入力します。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、deny または permit 条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力し、16 進数で 16 ビットの値を指定し、コロンで囲んで指定します。 • （任意）*operator* には、指定したプロトコルの送信元または宛先ポートを比較するオペランドを指定します。オペランドは、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range** です。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。*destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 • （任意）*port-number* は 0 ～ 65535 の 10 進数または TCP または UDP ポートの名前です。TCP をフィルタリングする場合にだけ TCP ポート名を使用できます。UDP をフィルタリングする場合にだけ UDP ポート名を使用できます。 • （任意）**dscp** *value* を入力して、各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント（DSCP）値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）**fragments** を入力して、初期状態でないフラグメントをチェックします。プロトコルが **ipv6** である場合にだけ、このキーワードが表示されます。 • （任意）**log** を入力して、エントリに一致するパケットに関するロギング メッセージをコンソールに送信します。**log-input** を入力して、ログ エントリに入力インターフェイスを含めるようにします。ロギングは、ルータ ACL にだけサポートされています。 • （任意）**routing** を入力して、ルーティングされる IPv6 パケットを指定します。 • （任意）**sequence** *value* を入力して、アクセス リスト文のシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • （任意）**time-range** *name* を入力して、許可または拒否文に適用する時間範囲を指定します。

	コマンド	目的
ステップ 3b	{**deny** | **permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**rst**] [**routing**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。ステップ 3a で説明するパラメータと同じパラメータを使用しますが、次に示すパラメータが追加されています。 • **ack** *:* ACK ビット設定。 • **established** *:* 確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • **fin**：終了したビット設定。送信者からのデータはありません。 • **neq** {*port* | *protocol*} *:* 指定のポート番号上にないパケットだけを照合します。 • **psh**：PSH ビット設定。 • **range** {*port* | *protocol*}：指定のポート番号の範囲内にあるパケットだけを照合します。 • **rst**：RST ビット設定。 • **syn**：SYN ビット設定。 • **urg** *:* URG ビット設定。
ステップ 3c	{**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] **[log]** [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**] [**sequence** *value*] [**time-range** *name*]	（任意）UDP アクセス リストおよびアクセス条件を定義します。 UDP の場合は、**udp** を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[*operator* [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前とします。UDP の場合、パラメータ **established** は無効です。
ステップ 3d	{**deny** | **permit**} **icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dscp** *value*] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 ICMP の場合は、**icmp** を入力します。ICMP パラメータはステップ 3a の IP プロトコルで説明されているパラメータと同じですが、ICMP メッセージ タイプとコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプを使用してフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-code*：ICMP メッセージ コード タイプを使用してフィルタリングされた ICMP パケットをフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-message*：ICMP メッセージ タイプ名または ICMP メッセージのタイプおよびコード名を使用して、ICMP パケットをフィルタリングします。ICMP メッセージ タイプ名およびコード名を確認するには、「?」キーを使用するか、このリリースのコマンド リファレンスを参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show ipv6 access-list**	アクセス リストの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

no {**deny** | **permit**} IPv6 アクセス リスト コンフィギュレーション コマンドとキーワードを使用して、拒否または許可条件を指定のアクセス リストから削除します。

次の例では、CISCO という名前の IPv6 アクセス リストを設定します。リストの最初の拒否エントリは、5000 より大きい宛先 TCP ポート番号を持ったすべてのパケットを拒否します。2 番目の拒否エントリは、5000 未満の送信元 UDP ポート番号を持ったパケットを拒否します。また、この 2 番目の拒否エントリは、すべての一致をコンソールに表示します。リストの最初の許可エントリは、すべての ICMP パケットを許可します。リストの 2 番目の許可エントリは、他のすべてのトラフィックを許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 アクセス リストの末尾にあるので、この 2 番目の許可エントリが必要となります。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

インターフェイスへの IPv6 ACL の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。ACL は、レイヤ 3 インターフェイスの発信または着信トラフィックに、あるいはレイヤ 2 インターフェイスの着信トラフィックに適用できます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL）またはレイヤ 3 インターフェイス（ルータ ACLS）を特定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport**	ルータ ACL を適用する場合、インターフェイスをレイヤ 2 モード（デフォルト）からレイヤ 3 モードに変更します。
ステップ 4	**ipv6 address** *ipv6-address*	レイヤ 3 インターフェイス（ルータ ACL）に IPv6 アドレスを設定します。 **（注）** このコマンドは、レイヤ 2 インターフェイス、またはインターフェイスに IPv6 アドレスが明示的に設定されている場合は必要ありません。
ステップ 5	**ipv6 traffic-filter** *access-list-name* {**in** | **out**}	アクセス リストをインターフェイスの受信または発信トラフィックに適用します。 **（注）** **out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	アクセス リストの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

no ipv6 traffic-filter *access-list-name* インターフェイス コンフィギュレーション コマンドを使用して、アクセス リストをインターフェイスから削除します。

次の例では、アクセス リスト *Cisco* をレイヤ 3 インターフェイス上の発信トラフィックに適用する方法を示します。

```
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

IPv6 ACL の表示

表 39-1 の 1 つまたは複数の特権 EXEC コマンドを使用して、設定されているすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

表 39-1　IPv6 アクセス リストの情報を表示するためのコマンド

コマンド	目的
show access-lists	スイッチで設定されるすべてのアクセス リストを表示します。
show ipv6 access-list [*access-list-name*]	設定されたすべての IPv6 アクセス リストまたは名前で指定されたアクセス リストを表示します。

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定されているすべてのアクセス リストが表示されます。

```
Switch #show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定されている IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30

IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```

CHAPTER 40

HSRP の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチで Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）を使用する方法について説明します。HSRP は、IP トラフィック ルーティングに冗長性を提供し、1 台のルータのアベイラビリティに依存しないルーティングを実現します。HSRP をサポートするには、スイッチでメトロ IP アクセス イメージが稼動している必要があります。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのスイッチ コマンド リファレンス、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* Release 12.2』を参照してください。

- 「HSRP の概要」（P.40-1）
- 「HSRP の設定」（P.40-5）
- 「HSRP 設定の表示」（P.40-12）

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE（米国電気電子学会）802 LAN 上の IP ホスト ファースト ホップに冗長性を確保しネットワークのアベイラビリティを高めるシスコの標準方式です。HSRP を使用すると、特定のルータのアベイラビリティに依存せず IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合せることで、1 台の仮想ルータ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させることができます。ネットワークまたはセグメント上に HSRP を設定すると、仮想 Media Access Control（MAC; メディア アクセス制御）アドレス、および設定されたルータ グループ間で共有される IP アドレスを使用できるようになり、HSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは実際には存在しません。相互にバックアップ機能を提供するように設定されている複数のルータの共通のターゲットとなるルータです。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御するルータです。

（注） HSRP グループ内のルータには、スイッチのルーテッド ポートや Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRP は、ネットワーク上のホストからの IP トラフィックに冗長性を提供することで、ネットワークのアベイラビリティを高めます。アクティブ ルータは、ルータ インターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイ ルータは、アクティブ ルータが故障した場合、または設定条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

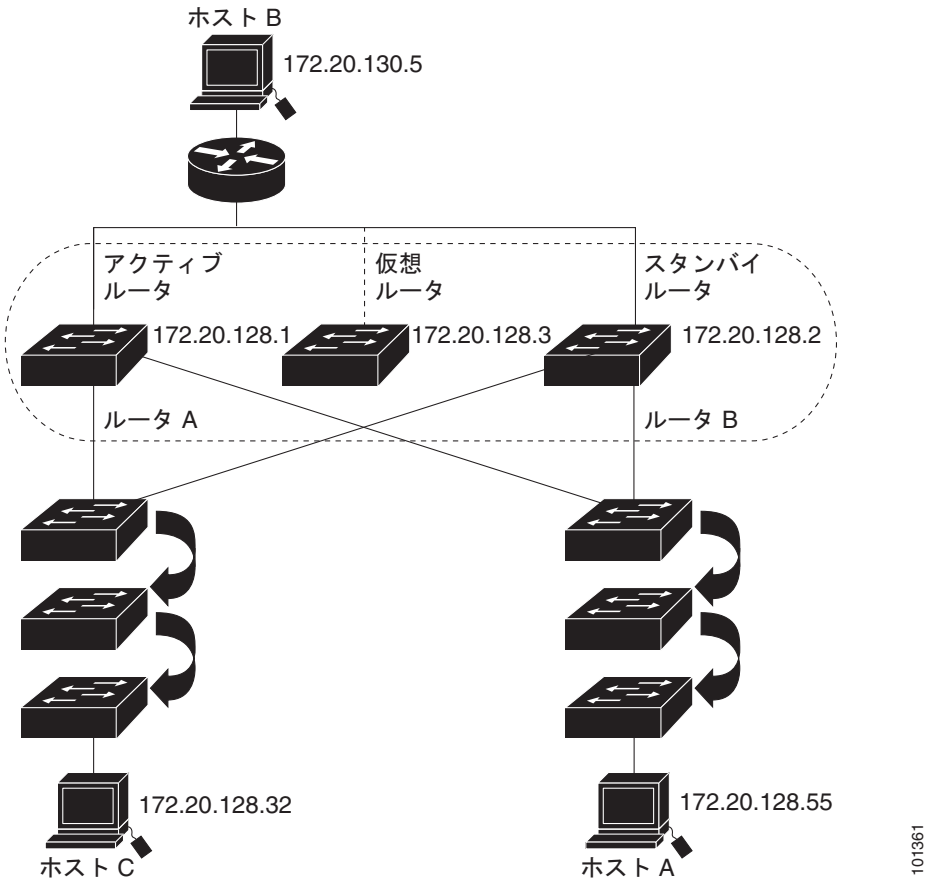
HSRP は、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。HSRP をネットワーク セグメントに設定すると、HSRP は仮想 MAC アドレスと IP アドレスを 1 つずつ提供します。このアドレスは、HSRP が動作するルータ インターフェイス グループ内のルータ インターフェイス間で共有できます。プロトコルによってアクティブ ルータとして選択されたルータは、グループの MAC アドレス宛てのパケットを受信し、ルーティングします。*n* 台のルータで HSRP が稼動している場合、*n +1* 個の IP アドレスおよび MAC アドレスが割り当てられます。

指定されたアクティブ ルータの故障を HSRP が検出すると、選択されているスタンバイ ルータがホット スタンバイ グループの MAC アドレスおよび IP アドレスの制御を引き継ぎます。この時点で新しいスタンバイ ルータも選択されます。HSRP が稼動しているデバイスは、マルチキャスト UDP ベースの hello パケットを送受信することにより、ルータ障害の検出、アクティブ ルータおよびスタンバイ ルータの指定を行います。インターフェイスに HSRP が設定されている場合、そのインターフェイスでは Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）のリダイレクト メッセージがデフォルトでディセーブルとなっています。

レイヤ 3 で動作するスイッチ間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。そのためには、インターフェイスに設定するホット スタンバイ コマンド グループごとにグループ番号を指定します。たとえば、スイッチ 1 のインターフェイスをアクティブ ルータ、スイッチ 2 のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

図 40-1 に、HSRP 用に設定されたネットワークのセグメントを示します。各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。ルータ A の IP アドレスをネットワーク上のホストに設定する代わりに、デフォルト ルータである仮想ルータの IP アドレスを設定します。ホスト C からホスト B にパケットが送信される場合、ホスト C は仮想ルータの MAC アドレスにパケットを送信します。何らかの理由により、ルータ A がパケットの転送を停止すると、ルータ B が仮想 IP アドレスおよび仮想 MAC アドレスに応答してアクティブ ルータとなり、アクティブ ルータの作業を行います。ホスト C は引き続き仮想ルータの IP アドレスを使用し、ホスト B 宛てのパケットをアドレッシングします。ルータ B はそのパケットを受信し、ホスト B に送信します。ルータ B は HSRP の機能を使用し、ルータ A が動作を再開するまで、ホスト B のセグメント上のユーザと通信する必要があるホスト C のセグメント上のユーザに連続的にサービスを提供します。また、ホスト A セグメントとホスト B の間で、引き続き通常のパケット処理機能を実行します。

図 40-1　HSRP の一般的な構成



HSRP のバージョン

スイッチでサポートされている HSRP のバージョンは次のとおりです。

- HSRPv1：HSRP のバージョン 1。これが HSRP のデフォルト バージョンです。機能は次のとおりです。
  - HSRP グループ番号は、0 ～ 255 の範囲で指定できます。
  - HSRPv1 では、hello パケットの送信にマルチキャスト アドレス 224.0.0.2 が使用されますが、これは Cisco Group Management Protocol（CGMP）の脱退処理と競合する可能性があります。HSRPv1 と CGMP は相互に排他的で、同時には使用できません。
- HSRPv2：HSRP のバージョン 2。HSRPv2 の機能は次のとおりです。
  - HSRPv2 では、HSRP グループ番号とサブインターフェイスの VLAN ID を一致させるため、グループ番号として 0 ～ 4095 の値、MAC アドレスとして 0000.0C9F.F000 ～ 0000.0C9F.FFFF の値をそれぞれ使用できます。
  - HSRPv2 では、hello パケットの送信にマルチキャスト アドレス 224.0.0.102 が使用されます。HSRPv2 と CGMP の脱退処理は相互に排他的ではないため、同時にイネーブルにできます。
  - HSRPv2 のパケット形式は HSRPv1 とは異なります。

    HSRPv1 を実行しているスイッチでは、hello パケットを送信した物理ルータを特定できません。これはルータの送信元 MAC アドレスが仮想 MAC アドレスであることに起因します。

HSRPv2 のパケット形式は HSRPv1 とは異なります。HSRPv2 パケットには、Type Length Value（TLV）形式が使用され、パケットを送信した物理ルータの MAC アドレスが 6 バイトの識別子フィールドに格納されます。

HSRPv1 を実行しているインターフェイスが HSRPv2 パケットを取得した場合、このタイプ フィールドは無視されます。

HSRPv2 と HSRPv1 は相互に排他的です。同じインターフェイス上では、HSRPv2 と HSRPv1 を同時に使用できません。

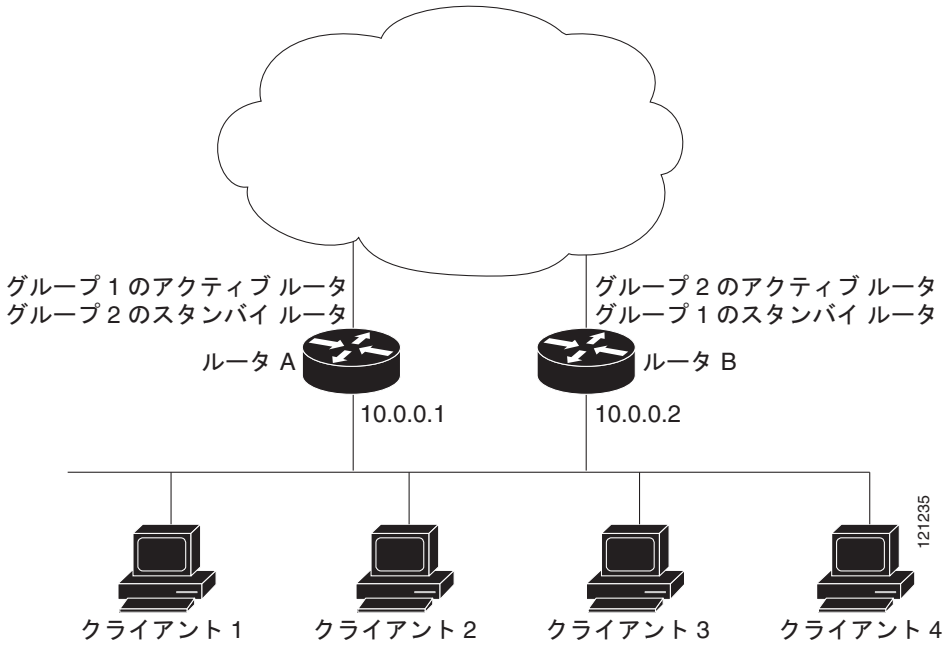
Multiple HSRP

スイッチでは、HSRP の拡張機能である Multiple HSRP（MHSRP）がサポートされています。これにより 2 つ以上の HSRP グループ間でロード シェアリングが行えます。MHSRP を設定すると、ホスト ネットワークからサーバ ネットワークまで、ロード バランシングを実現して複数のスタンバイ グループ（およびパス）を使用できます。図 40-2 では、半数のクライアントがルータ A として設定され、もう半数のクライアントがルータ B として設定されています。それと同時に、ルータ A およびルータ B に対する設定により、2 つの HSRP グループが確立されています。グループ 1 では、ルータ A に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータになり、ルータ B がスタンバイ ルータとなります。グループ 2 では、ルータ B に最高のプライオリティが割り当てられているので、ルータ B がデフォルトのアクティブ ルータになり、ルータ A がスタンバイ ルータとなります。通常の運用では、この 2 つのルータが IP トラフィック負荷を分担します。一方のルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータのパケット転送機能を引き継ぎます。

設定手順の例については、「MHSRP の設定」（P.40-10）を参照してください。

（注）　MHSRP では、障害が発生したルータが再び稼動状態へ戻った場合にプリエンプトが発生してロード シェアリングが復元されるように、**standby preempt** インターフェイス コンフィギュレーション コマンドを HSRP インターフェイスで入力する必要があります。

図 40-2　MHSRP ロード シェアリング



HSRP の設定

- 「HSRP のデフォルト設定」（P.40-5）
- 「HSRP 設定時の注意事項」（P.40-6）
- 「HSRP のイネーブル化」（P.40-6）
- 「HSRP のプライオリティの設定」（P.40-8）
- 「MHSRP の設定」（P.40-10）
- 「HSRP 認証およびタイマーの設定」（P.40-11）
- 「ICMP リダイレクト メッセージの HSRP サポートのイネーブル化」（P.40-12）

HSRP のデフォルト設定

表 40-1 は、HSRP のデフォルト設定をまとめたものです。

表 40-1　HSRP のデフォルト設定

機能	デフォルト設定
HSRP バージョン	バージョン 1
HSRP グループ	設定なし
スタンバイ グループ番号	0
スタンバイ MAC アドレス	システムへの割り当て：0000.0c07.acXX（*XX* は HSRP グループ番号）
スタンバイ プライオリティ	100

表 40-1　HSRP のデフォルト設定 （続き）

機能	デフォルト設定
スタンバイ遅延	0（遅延なし）
スタンバイでのインターフェイス プライオリティの追跡	10
スタンバイ hello 時間	3 秒
スタンバイ ホールドタイム	10 秒

HSRP 設定時の注意事項

- HSRP を設定できる VLAN インターフェイスまたはルーティング インターフェイスは合わせて 32 個までです。
- 以下の手順では、次のレイヤ 3 インターフェイスのうちいずれか 1 つを指定する必要があります。
  - ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。
  - SVI：**interface vlan** *vlan_id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
  - レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイスです。詳細については、「レイヤ 3 EtherChannel の設定」（P.35-14）を参照してください。
- すべてのレイヤ 3 インターフェイスに IP アドレスを割り当てる必要があります。「レイヤ 3 インターフェイスの設定」（P.10-27）を参照してください。
- HSRPv1 が設定されているインターフェイスとは異なるインターフェイスに HSRPv2 を設定する場合、HSRPv2 と HSRPv1 を同一のスイッチ上に設定できます。
- HSRP グループのバージョンは、そのグループの番号が 256 未満である場合に限って HSRPv2 から HSRPv1 に変更できます。
- インターフェイス上で HSRP のバージョンを変更すると、新しい仮想 MAC アドレスが割り当てられるため、各 HSRP グループはリセットされます。

HSRP のイネーブル化

standby ip インターフェイス コンフィギュレーション コマンドを実行すると、設定されたインターフェイスで HSRP がアクティブになります。IP アドレスを指定すると、その IP アドレスがホット スタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなければ、スタンバイ機能によってアドレスが学習されます。指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。

standby ip コマンドがインターフェイス上でイネーブルに設定され、プロキシ Address Resolution Protocol（ARP; アドレス解決プロトコル）がイネーブルの場合、インターフェイスのホット スタンバイ ステートがアクティブになると、プロキシ ARP 要求に対する応答は、ホット スタンバイ グループの MAC アドレスを使用して実行されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

レイヤ 3 インターフェイス上で HSRP を作成する場合、またはイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 4	**no switchport**	必要であれば、ポート上でレイヤ 2 スイッチングをディセーブルにし、レイヤ 3 インターフェイスをイネーブルにします。
ステップ 5	**standby version** {**1** | **2**}	（任意）インターフェイスに HSRP バージョンを設定します。 • 1：HSRPv1 を選択する場合に指定します。 • 2：HSRPv2 を選択する場合に指定します。 このコマンドを入力しないか、またはキーワードを指定しない場合、そのインターフェイスではデフォルト バージョンの HSRP である HSRP v1 が実行されます。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 で、デフォルト値は 0 です。HSRP グループが 1 つだけであれば、グループ番号を指定する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホット スタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：指定した IP アドレスが、セカンダリ ホット スタンバイ ルータ インターフェイスの IP アドレスとなります。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show standby** [*interface-id* [*group*]]	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

HSRP をディセーブルにする場合は、**no standby** [*group-number*] **ip** [*ip-address*] インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイスのグループ 1 で HSRP をアクティブにする例を示します。ホット スタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。

（注）　これは、HSRP をイネーブルにするために最低限必要な手順です。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```

HSRP のプライオリティの設定

standby priority、**standby preempt**、および **standby track** の各インターフェイス コンフィギュレーション コマンドはいずれも、アクティブ ルータとスタンバイ ルータ、および新しいアクティブ ルータが処理を引き継いだ場合の動作を検索する際の手掛かりとなる特性を設定するためのものです。

HSRP プライオリティを設定するときの注意事項は、次のとおりです。

- プライオリティを割り当てると、アクティブ ルータおよびスタンバイ ルータを選択できるようになります。プリエンプトがイネーブルの場合は、プライオリティが最高のルータがアクティブ ルータになります。プライオリティが同じであれば、現在のアクティブ ルータがそのまま使用されます。
- 最も大きな値（1 ～ 255）が、最高のプライオリティ（アクティブ ルータになる可能性が最も高い）を表します。
- プライオリティ、プリエンプト、またはその両方を設定するときは、少なくとも 1 つのキーワード（**priority**、**preempt**、または両方）を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティはダイナミックに変更されます。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホット スタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。この機能は、HSRP 用に設定されていないインターフェイスを追跡する場合に有効です。追跡対象のインターフェイスが故障すると、追跡が設定されていたデバイスのホット スタンバイ プライオリティが 10 減少します。追跡対象でないインターフェイスの場合は、そのステートが変わっても、設定済みデバイスのホット スタンバイ プライオリティは変わりません。ホット スタンバイ用に設定されたインターフェイスごとに、追跡するインターフェイスのリストを個別に設定できます。
- **standby track** *interface-priority* インターフェイス コンフィギュレーション コマンドを使用すると、追跡対象のインターフェイスがダウンした場合のホット スタンバイ プライオリティの減少幅を指定できます。インターフェイスが稼動状態に戻ると、プライオリティは同じ分だけ増加します。
- *interface-priority* の値が設定されている場合、複数の追跡対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。プライオリティ値が設定されていない追跡対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- インターフェイスに対しルーティングを初めてイネーブルにした時点では、完全なルーティング テーブルは存在しません。preempt に設定されたインターフェイスはアクティブ ルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティング テーブルを更新できるように遅延時間を設定します。

インターフェイスに HSRP プライオリティ特性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**standby** [*group-number*] **priority** *priority* [**preempt** [**delay** *delay*]]	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 で、デフォルト値は 100 です。最も大きな値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号を指定します。 • （任意）**preempt**：ローカル ルータのプライオリティがアクティブ ルータよりも高い場合、そのローカル ルータがアクティブ ルータとして制御を行います。 • （任意）**delay**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** *delay*]	ルータを **preempt** に設定します（つまりローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、そのローカル ルータがアクティブ ルータとして制御を行います）。 • （任意）*group-number*：コマンドが適用されるグループ番号を指定します。 • （任意）**priority**：グループ プライオリティを設定または変更する場合に入力します。指定できる値の範囲は 1 ～ 255 で、デフォルト値は 100 です。 • （任意）**delay**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 6	**standby** [*group-number*] **track** *type number* [*interface-priority*]	他のインターフェイスを追跡するようにインターフェイスを設定します。この設定により、他のインターフェイスの 1 つがダウンした場合は、そのデバイスのホット スタンバイ プライオリティが減少します。 • （任意）*group-number*：コマンドが適用されるグループ番号を指定します。 • *type*：追跡対象のインターフェイス タイプを（インターフェイス番号とともに）入力します。 • *number*：追跡対象のインターフェイス番号を（インターフェイス タイプとともに）入力します。 • （任意）*interface-priority*：インターフェイスがダウンした場合、または稼動状態に戻った場合に、ルータのホット スタンバイ プライオリティを減少または増加させる幅を入力します。デフォルト値は 10 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

プライオリティ、プリエンプト、および遅延の値をデフォルト値に戻すには、**no standby** [*group-number*] **priority** *priority* [**preempt** [**delay** *delay*]] および **no standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** *delay*] の各インターフェイス コンフィギュレーション コマンドを使用します。

追跡を解除するには、**no standby** [*group-number*] **track** *type number* [*interface-priority*] インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートがアクティブになり、IP アドレスおよびプライオリティ 120（デフォルト値よりも高いプライオリティ）が設定されます。アクティブ ルータになるまでの待機時間は 300 秒（5 分間）です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
```

MHSRP の設定

MHSRP およびロード バランシングをイネーブルにするには、グループのアクティブ ルータとして 2 つのルータを設定し、仮想ルータをスタンバイ ルータとして設定します。次は、図 40-2 の MHSRP 設定をイネーブルにする例です。障害が発生したルータが稼動状態へ戻った場合にプリエンプトを発生させてロード バランシングが復元されるよう、**standby preempt** インターフェイス コンフィギュレーション コマンドをそれぞれの HSRP インターフェイスで入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。ルータ A の HSRP インターフェイスの IP アドレスは 10.0.0.1、グループ 1 スタンバイ プライオリティは 110 です（デフォルトは 100）。ルータ B の HSRP インターフェイスの IP アドレスは 10.0.0.2、グループ 2 スタンバイ プライオリティは 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

ルータ A の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
```

```
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

HSRP 認証およびタイマーの設定

必要であれば、HSRP 認証文字列を設定できるほか、hello 時間インターバルやホールドタイムを変更することもできます。

これらのアトリビュートを設定するときの注意事項は次のとおりです。

- 認証文字列はすべての HSRP メッセージに暗号化されずに送信されます。相互運用できるように、接続されたすべてのルータおよびアクセス サーバに同じ認証文字列を設定する必要があります。認証文字列が一致しないと、HSRP が設定された他のルータから、指定されたホット スタンバイ IP アドレスおよびタイマー値を取得することができません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を取得できます。アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。
- 同じホット スタンバイ グループに属するルータにはすべて、同じタイマー値を使用する必要があります。通常、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスに HSRP の認証とタイマーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、認証を設定する HSRP インターフェイスを入力します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**standby** [*group-number*] **authentication** *string*	（任意）**authentication** *string*：すべての HSRP メッセージで伝達される文字列を入力します。認証文字列として指定できる文字数は最大 8 文字です。デフォルトの文字列は **cisco** です。 （任意）*group-number*：コマンドが適用されるグループ番号を指定します。
ステップ 5	**standby** [*group-number*] **timers** *hellotime holdtime*	（任意）hello パケット インターバル、およびアクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 • *group-number*：コマンドが適用されるグループ番号を指定します。 • *hellotime*：hello インターバルを秒単位で指定します。指定できる範囲は 1 ～ 255 秒で、デフォルトは 3 秒です。 • *holdtime*：アクティブ ルータまたはスタンバイ ルータのダウンが宣言されるまでの時間を秒単位で指定します。指定できる範囲は 1 ～ 255 秒で、デフォルトは 10 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

認証文字列を削除する場合は、**no standby** [*group-number*] **authentication** *string* インターフェイス コンフィギュレーション コマンドを使用します。タイマーをデフォルト値に戻す場合は、**no standby** [*group-number*] **timers** *hellotime holdtime* インターフェイス コンフィギュレーション コマンドを使用します。

次に、グループ 1 のホット スタンバイ ルータを相互運用させるために必要な認証文字列として、*word* を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、hello パケット インターバルが 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

ICMP リダイレクト メッセージは、HSRP が設定されたインターフェイス上で自動的にイネーブルになります。この機能により、HSRP を介した発信 ICMP リダイレクト メッセージがフィルタリングされます。その際、ネクスト ホップ IP アドレスが HSRP 仮想 IP アドレスに変更される場合があります。ICMP は、メッセージ パケットにより IP 処理に関するエラーなどの情報がレポートされるネットワーク レイヤ インターネット プロトコルです。ICMP は、エラー パケットをホストに送信するなどの診断機能も備えています。

スイッチで HSRP が実行されている場合、ホストでは HSRP グループ内のルータのインターフェイス（または実際の）MAC アドレスが検出されないようにしてください。ICMP によってホストがルータの実際の MAC アドレスへリダイレクトされて、そのルータに障害が発生した場合、ホストからのパケットは消失します。

詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* を参照してください。

HSRP 設定の表示

HSRP 設定を表示するには、特権 EXEC モードで次のコマンドを実行します。

show standby [*interface-id* [*group*]] [**brief**] [**detail**]

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイスの HSRP グループに関する HSRP 情報を表示できます。HSRP 情報の概要と詳細のどちらを表示するかを指定することもできます。デフォルト表示は **detail** です。HSRP グループが多数ある場合、修飾子を指定しないで **show standby** コマンドを使用すると、正確に表示されないことがあります。

次に、**show standby** 特権 EXEC コマンドを実行して、2 つのスタンバイ グループ（グループ 1 およびグループ 100）の HSRP 情報を表示する例を示します。

```
Switch# show standby
VLAN1 - Group 1
   Local state is Standby, priority 105, may preempt
   Hellotime 3 holdtime 10
   Next hello sent in 00:00:02.182
   Hot standby IP address is 172.20.128.3 configured
   Active router is 172.20.128.1 expires in 00:00:09
   Standby router is local
   Standby virtual mac address is 0000.0c07.ac01
   Name is bbb
VLAN1 - Group 100
   Local state is Active, priority 105, may preempt
   Hellotime 3 holdtime 10
   Next hello sent in 00:00:02.262
   Hot standby IP address is 172.20.138.51 configured
   Active router is local
   Standby router is unknown expired
   Standby virtual mac address is 0000.0c07.ac64
   Name is test
```

CHAPTER 41

Cisco IOS IP SLA 動作の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにおける Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）および IETF Two-Way Active Measurement Protocol（TWAMP; 双方向アクティブ測定プロトコル）の使用方法について説明します。Cisco IP SLA は、シスコのお客様が IP アプリケーションおよび IP サービスの IP サービス レベルを分析し、ネットワーク パフォーマンスを測定できるようにするための機能で、Cisco IOS ソフトウェアの一部として組み込まれています。分析には、継続的かつ信頼性の高い確実な方法でトラフィックが生成されるアクティブ トラフィック モニタリングを使用します。Cisco IOS IP SLA を使用することで、サービス プロバイダーのカスタマーは、サービス レベル契約を評価してから提供できる一方、企業のお客様は、サービス レベルおよび外部委託しているサービス レベル契約を検証し、ネットワーク パフォーマンスを把握できます。Cisco IOS IP SLA を使用すると、ネットワーク アセスメントや QoS（Quality Of Service）の検証が可能で、新しいサービスの導入やネットワークに関するトラブルシューティングも容易になります。

（注） Cisco IP SLA の全機能を使用できるのは、メトロ IP アクセスまたはメトロ アクセス イメージが実行されているスイッチ上に限られます。ME 2400 など、メトロ ベース イメージが実行されているスイッチは IP SLA レスポンダ機能しかサポートしていないため、Cisco IP SLA の全機能をサポートしている別のテバイスを使用して設定する必要があります。

TWAMP は、このプロトコルをサポートする 2 つのデバイス間でのラウンドトリップ ネットワーク パフォーマンスの測定に関する規格を定めたものです。Cisco IOS リリース 12.2(52)SE 以降では、Cisco ME 3400E イーサネット アクセス スイッチ上に TWAMP を実装できます。

IP SLA の詳細については、次の URL にある『*Cisco IOS IP SLAs Configuration Guide*』*Release 12.4T* を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

構文の詳細については、次の URL にあるコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

この章で説明する内容は、次のとおりです。

- 「Cisco IOS IP SLA の概要」（P.41-2）
- 「IP SLA 動作の設定」（P.41-6）
- 「IP SLA 動作のモニタリング」（P.41-13）
- 「TWAMP の概要」（P.41-14）
- 「TWAMP の設定」（P.41-15）

Cisco IOS IP SLA の概要

Cisco IOS IP SLA では、ネットワーク全体にデータを送信することで、複数のネットワーク間または複数のネットワーク パス間のパフォーマンスが測定されます。また、ネットワーク データおよび IP サービスのシミュレーションが行われ、ネットワーク パフォーマンスに関する情報がリアルタイムで収集されます。Cisco IOS IP SLA では、Cisco IOS デバイス間のトラフィック、または Cisco IOS デバイスからリモート IP デバイス（ネットワーク アプリケーション サーバなど）へのトラフィックが生成され、その解析が行われます。さまざまな Cisco IOS IP SLA 動作によって得られた測定結果は、トラブルシューティング、問題の分析、ネットワーク トポロジの設計などに利用できます。

実行される Cisco IOS IP SLA 動作の内容に応じて、シスコ製デバイス内部ではネットワーク パフォーマンスに関するさまざまな統計情報がモニタされ、Command-Line Interface（CLI; コマンドライン インターフェイス）および Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）の MIB に格納されます。IP SLA パケットには、送信元 IP アドレス、宛先 IP アドレス、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）/TCP ポートの番号、Type Of Service（ToS; タイプ オブ サービス）バイト（Differentiated Services Code Point [DSCP; DiffServ コード ポイント] ビット、IP プレフィクス ビットなど）、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing/Forwarding Instance（VRF; ルーティング/フォワーディング インスタンス）、URL Web アドレスなど、IP レイヤおよびアプリケーション レイヤのさまざまな設定可能オプションを指定できます。

Cisco IP SLA はレイヤ 2 転送には依存しないため、異種ネットワーク間でエンドツーエンド動作を設定することで、エンド ユーザが経験する可能性が高いメトリックを最大限反映させられます。IP SLA では、次のような独自のパフォーマンス メトリックが収集されます。

- 遅延（往復および一方向）
- ジッタ（方向性あり）
- パケット損失（方向性あり）
- パケット シーケンス（パケット順序）
- パス（ホップ単位）
- 接続性（方向性あり）
- サーバまたは Web サイトのダウンロード時間

Cisco IOS IP SLA は、SNMP によるアクセスが可能であるため、CiscoWorks Internetwork Performance Monitor（IPM; インターネットワーク パフォーマンス モニタ）やサードパーティ（シスコ パートナー）製パフォーマンス管理製品などのパフォーマンス モニタリング アプリケーションでも使用できます。Cisco IOS IP SLA を使用するネットワーク管理製品の詳細については、次の URL を参照してください。

http://www.cisco.com/go/ipsla

IP SLA には次のような特長があります。

- サービスレベル契約のモニタリング、評価、および検証が実行できる。
- ネットワーク パフォーマンス モニタリングを実行できる。
  - ネットワーク内のジッタ、遅延、パケット損失を測定できる。
  - 継続的かつ信頼性の高い確実な評価を実行できる。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに十分なものかどうかを検証できる。
- 予防的な検証を目的としたエッジ間におけるネットワーク可用性のモニタリングと、ネットワーク リソースの接続性テストを実行できる（リモート サイトから業務上の重要データを格納するために使用する NFS サーバのネットワーク可用性を確認するなど）。

- 整合性と信頼性を兼ね備えた測定結果を基にネットワーク動作に関するトラブルシューティングを実行できる。またそれによって、問題点を即座に特定しトラブルシューティングの所要時間を短縮できる。
- Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）によるパフォーマンス モニタリングおよびネットワーク検証を実行できる（スイッチが MPLS をサポートしている場合）。

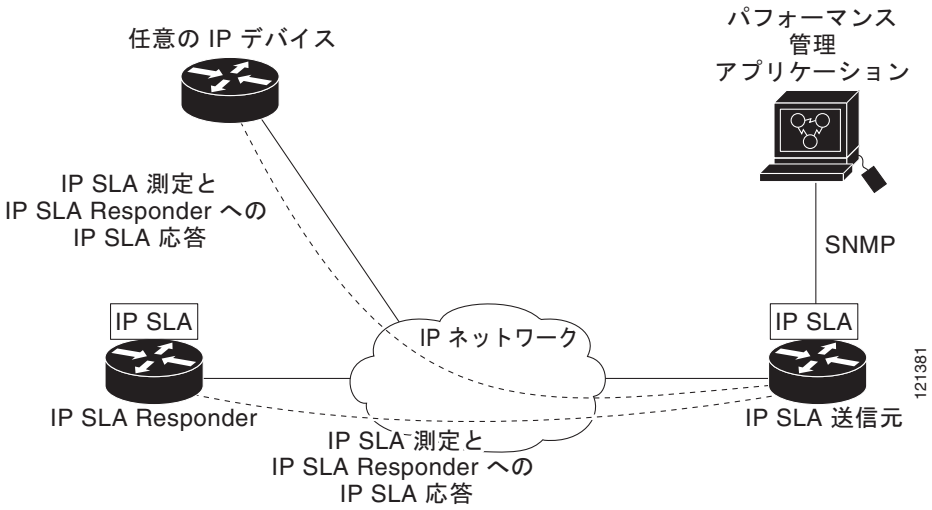
ここでは、次の IP SLA 機能について説明します。

- 「Cisco IOS IP SLA を使用したネットワーク パフォーマンスの測定」（P.41-3）
- 「IP SLA レスポンダと IP SLA 制御プロトコル」（P.41-4）
- 「IP SLA に対する応答時間の算出」（P.41-4）
- 「IP SLA 動作のスケジューリング」（P.41-5）
- 「IP SLA 動作のしきい値のモニタリング」（P.41-6）

Cisco IOS IP SLA を使用したネットワーク パフォーマンスの測定

IP SLA を使用すると、物理プローブを導入することなく、コア、分散、エッジなど、ネットワーク内にある任意のエリア間のパフォーマンスをモニタできます。2 つのネットワーキング デバイス間におけるネットワーク パフォーマンスを測定する際には、それに使用するトラフィックが生成されます。図 41-1 は、生成されたパケットが送信元デバイスから宛先デバイスに送信された場合に、IP SLA がどのように開始されるかを示したものです。パケットを受信した宛先デバイスは、IP SLA 動作のタイプに応じて、タイムスタンプ情報を返します。送信元ではそれを基にしてパフォーマンス メトリックの値が算出されます。IP SLA 動作によるネットワーク測定は、UDP など特定のプロトコルを使用して、ネットワーク内の送信元デバイスから宛先デバイスへ向けて実行されます。

図 41-1　　Cisco IOS IP SLA 動作



IP SLA ネットワーク パフォーマンス測定を実施する手順は次のとおりです。

1. 必要に応じて IP SLA レスポンダをイネーブルにします。
2. 目的の IP SLA 動作タイプを設定します。
3. 指定した動作タイプに対して使用できるオプションを設定します。

4. 必要に応じて、しきい値条件を設定します。
5. 動作の実行をスケジューリングしたあと、その動作を一定時間実行して統計情報を収集します。
6. Cisco IOS CLI または Network Management System（NMS; ネットワーク管理システム）から SNMP を使用して動作の結果を表示し、その内容を分析します。

各 IP SLA 動作の詳細については、次の URL にある『*Cisco IOS IP SLAs Configuration Guide*』の該当箇所を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

（注）　スイッチは、ゲートキーパー登録遅延動作測定を使用した IP SLA Voice over IP（VoIP）サービス レベルをサポートしていません。IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用して、動作タイプがソフトウェア イメージでサポートされているかどうかを確認してください。

IP SLA レスポンダと IP SLA 制御プロトコル

IP SLA レスポンダは、宛先のシスコ製デバイスに組み込まれているコンポーネントです。システムではこれを使用することで、IP SLA 要求パケットの到達を待ち、受信した時点でそれに応答します。レスポンダを使用すると、専用のプローブを使用することなく、正確な測定を実行できます。レスポンダは、Cisco IOS IP SLA 制御プロトコルに基づいた、受信および応答するポートを通知するためのメカニズムを備えています。宛先の IP SLA レスポンダに対する送信元として使用できるのは、Cisco IOS デバイスだけです。

（注）　IP SLA レスポンダには、Catalyst 2960 スイッチや Cisco ME 2400 スイッチ、メトロ ベース イメージが実行される Cisco ME 3400 スイッチなどの Cisco IOS レイヤ 2 レスポンダ設定可能スイッチを使用できます。レスポンダは、IP SLA の全機能をサポートする必要はありません。

図 41-1 には、IP ネットワークにおける Cisco IOS IP SLA レスポンダの配置場所が示してあります。レスポンダは、IP SLA 動作により送信された制御プロトコル メッセージを特定のポート上で受信します。コントロール メッセージを受信すると、指定された UDP ポートまたは TCP ポートが、指定された時間にわたってイネーブルになります。レスポンダはイネーブルになっている間に、要求を受け取り、それに対する応答を行います。IP SLA パケットに応答するか、指定した時間が超過すると、ポートがディセーブルになります。コントロール メッセージに対しては、より一層のセキュリティ対策として、MD5 認証を使用できます。

宛先デバイス上のレスポンダは、すべての IP SLA 動作に対してイネーブルにする必要はありません。たとえば、宛先ルータですでに使用できるサービス（Telnet や HTTP など）に対しては、レスポンダは不要です。シスコ製以外のデバイス上では IP SLA レスポンダは設定できません。また Cisco IOS IP SLA から動作パケットを送信できるのは、こうしたデバイスに固有のサービスに対してだけです。

IP SLA に対する応答時間の算出

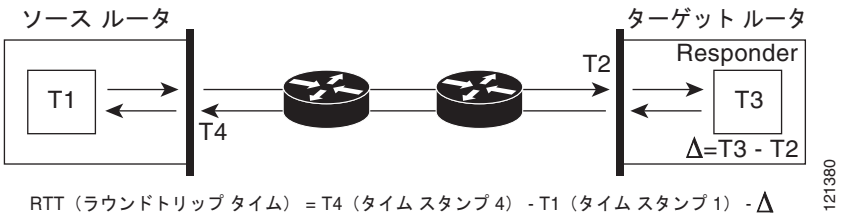
スイッチおよびルータでは、より優先度の高い処理がある場合、受信パケットの処理に数十ミリ秒程度かかることがあります。こうした遅延は応答時間に影響を与えます。これは、テスト パケットへの応答が、キューの中で処理されるのを待機している場合があるためです。このような場合、応答時間には実際のネットワーク遅延が正確には反映されません。IP SLA を使用すると、宛先デバイスだけでなく

送信元デバイスでも、これらの処理遅延が最小限に抑えられるため（レスポンダが使用されている場合）、実際のラウンドトリップ時間を特定できます。IP SLA のテスト パケットでは、処理遅延を最小限に留めるための手段としてタイムスタンプが使用されます。

IP SLA レスポンダがイネーブルの場合、宛先デバイスでは、まずパケットがインターフェイスに到達した時点でタイムスタンプが割り込みレベルで記録され、その後パケットが送出された時点でも再びタイムスタンプが記録されます。処理時間は記録されません。このタイムスタンプは、サブミリ秒（ms）単位で設定されます。

図 41-2 は、レスポンダが動作するしくみを表したものです。ここでは、ラウンドトリップ時間の計算に 4 つのタイムスタンプが使用されています。レスポンダの機能がイネーブルになっている宛先ルータでは、タイムスタンプ 3（TS3）からタイムスタンプ 2（TS2）を差し引いて、テスト パケットの処理に要した時間 Δ （デルタ）が算出されます。次に、全ラウンドトリップ時間からこの Δ の値が差し引かれます。送信元ルータ上でも IP SLA によりこれと同じ原理が適用されます。送信元ルータでは正確を期すため、受信時のタイムスタンプ 4（TS4）が割り込みレベルで記録されています。

図 41-2　Cisco IOS IP SLA レスポンダのタイムスタンプ



宛先デバイスで 2 つのタイムスタンプを記録すると、一方向遅延、ジッタ、方向性を持つパケット損失などを追跡できるという利点もあります。ネットワーク動作はその多くが非同期であるため、こうした統計情報は非常に重要です。ただし、一方向遅延を測定するためには、送信元ルータと宛先ルータが同一のクロック ソースに同期するように、双方のルータに Network Time Protocol（NTP; ネットワーク タイム プロトコル）を設定する必要があります。一方向ジッタを測定する場合は、クロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合は、統計情報の取得およびエラー情報の収集が開始される日時をスケジューリングする必要があります。動作は、ただちに開始されるようにスケジューリングできるほか、特定の月、日、および時刻に開始されるようスケジューリングすることもできます。一定期間をおいて動作が開始されるように設定する場合は、*保留*オプションを使用できます。この保留オプションとは、SNMP を介して認識できる動作の内部状態のことです。保留状態は、トリガされるのを待機しているリアクション（しきい値）動作に対しても使用できます。単独の IP SLA 動作をスケジューリングすることも、一度に複数の動作をスケジューリングすることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB から単一のコマンドを使用して複数の IP SLA 動作をスケジューリングできます。これらの動作を複数回にわたり均等に分散して実行するようにスケジューリングすると、IP SLA のモニタリング トラフィックの量を制御できます。このように IP SLA 動作を分散して実行すると、CPU の利用率を最小限に抑制できるため、ネットワークのスケーラビリティが向上します。

IP SLA の複数動作スケジューリング機能に関する詳細については、次の URL にある『*Cisco IOS IP SLAs Configuration Guide*』の「IP SLAs—Multiple Operation Scheduling」を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA 動作のしきい値のモニタリング

サービス レベル契約の適切なモニタリングをサポートするためには、違反があった場合にそれを即在に通知するメカニズムが必要です。IP SLA では、次のような状況でトリガされる SNMP トラップを送信できます。

- 接続の切断
- タイムアウト
- ラウンドトリップ時間のしきい値
- 平均ジッタのしきい値
- 一方向パケット損失
- 一方向ジッタ
- 一方向 Mean Opinion Score（MOS; 平均オピニオン評点）
- 一方向遅延

IP SLA のしきい値が超過した場合にも、別の IP SLA 動作をトリガしてより詳しい分析を行えます。たとえば、動作の頻度を高めたり、ICMP パス エコー動作または ICMP パス ジッタ動作を開始してトラブルシューティングを行ったりします。

しきい値のタイプや設定レベルは、決定する際に煩雑な作業を伴う場合があるうえ、ネットワーク内で使用している IP サービスのタイプにも依存します。Cisco IOS IP SLA 動作でしきい値を使用する詳しい方法については、次の URL にある『Cisco IOS IP SLAs Configuration Guide』の「IP SLAs—Proactive Threshold Monitoring」を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA 動作の設定

ここで説明する設定情報は、使用可能なすべての動作を網羅したものではありません。詳細な設定情報については、『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。ここでは、レスポンダの設定、UDP ジッタ動作の設定（レスポンダが必要）、ICMP エコー動作の設定（レスポンダは不要）など、具体例として取り上げるいくつかの動作の設定について説明します。その他の動作の設定に関する詳細については、次の URL にある『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

ここでは、次の情報について説明します。

- 「デフォルト設定」（P.41-6）
- 「設定時の注意事項」（P.41-7）
- 「IP SLA レスポンダの設定」（P.41-8）
- 「UDP ジッタ動作による IP サービス レベルの分析」（P.41-8）
- 「ICMP エコー動作による IP サービス レベルの分析」（P.41-11）

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA コマンドの詳細については、次の URL にあるコマンド リファレンス『*Cisco IOS IP SLAs Command Reference*』*Release 12.4T* を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

詳細な説明および設定手順については、次の URL にある『*Cisco IOS IP SLAs Configuration Guide*』*Release 12.4T* を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

このガイドで説明されている IP SLA コマンドや IP SLA 動作の中には、スイッチ上でサポートされていないものも含まれます。スイッチでは、複数動作スケジューリング機能や、しきい値の予防的モニタリングのほか、UDP ジッタ、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッタ、FTP、DNS、DHCP などを使用することにより、IP サービス レベルの分析を行えます。スイッチは、ゲートキーパー登録遅延動作測定を使用した IP SLA VoIP サービス レベルをサポートしていません。

IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用して、動作タイプがソフトウェア イメージでサポートされているかどうかを確認してください。次に、このコマンドの出力例を示します。

```
Switch# show ip sla application
        IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0

        Supported Operation Types
Type of Operation to Perform: 802.1agEcho
Type of Operation to Perform: 802.1agJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho

IP SLAs low memory water mark: 21741224
```

IP SLA レスポンダの設定

IP SLA レスポンダは、Catalyst 2960 スイッチや Cisco ME 2400 スイッチ、メトロ ベース イメージが実行される Cisco ME 3400 スイッチなど、Cisco IOS ソフトウェア ベースのデバイス上に限って使用できます。これらのデバイスには、IP SLA 機能を部分的にサポートする一部のレイヤ 2 スイッチも含まれます。宛先デバイス（動作のターゲット）上で IP SLA レスポンダを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla responder** {**tcp-connect** | **udp-echo**} **ipaddress** *ip-address* **port** *port-number*	スイッチを IP SLA レスポンダとして設定します。 キーワードの意味は次のとおりです。 • **tcp-connect**：レスポンダの TCP 接続動作をイネーブルにします。 • **udp-echo**：レスポンダの UDP エコー動作または UDP ジッタ動作をイネーブルにします。 • **ipaddress** *ip-address*：宛先 IP アドレスを入力します。 • **port** *port-number*：宛先のポート番号を入力します。 **（注）** IP アドレスおよびポート番号は、対象の IP SLA 動作用に送信元デバイス上で設定されたものと同じであることが必要です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip sla responder**	デバイス上の IP SLA レスポンダの設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA レスポンダをディセーブルにする場合は、**no ip sla responder** グローバル コンフィギュレーション コマンドを入力します。次に、デバイスを IP SLA の UDP ジッタ動作用のレスポンダとして設定する例を示します。手順については以下で説明します。

```
Switch(config)# ip sla responder udp-echo 172.29.139.134 5000
```

UDP ジッタ動作による IP サービス レベルの分析

ジッタとは、パケット間遅延のばらつきのことです。送信元から宛先へ複数のパケットが 10 ミリ秒間隔で連続的に送信される場合、ネットワークが正常に動作していれば、宛先ではそれらのパケットが 10 ミリ秒間隔で受信されます。しかし、ネットワーク内で遅延（キューイング、代替ルート経由での転送など）が発生すると、パケットの到達間隔が 10 ミリ秒より長くなったり短くなったりすることがあります。パケットの到達間隔が 10 ミリ秒より長い場合、ジッタ値は正となります。パケットが 12 ミリ秒間隔で到達した場合、ジッタ値は +2、パケットが 8 ミリ秒間隔で到達した場合ジッタ値は -2 となります。遅延に影響されやすいネットワークの場合、ジッタ値は 0 となることが理想的で、正の値になることは好ましくありません。

ジッタのモニタリング以外にも、多目的なデータ収集動作として、IP SLA の UDP ジッタ動作を使用できます。送信元と動作ターゲットとの間で送受信されるシーケンス情報やタイムスタンプは、IP SLA で生成されるパケットにより搬送されます。UDP ジッタ動作では、これらの情報に基づいて、次のようなデータが測定されます。

- 方向別ジッタ（送信元から宛先および宛先から送信元）
- 方向別パケット損失

- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均ラウンドトリップ時間）

データの送信および受信に使用するパスは異なる場合があるため（非対称）、方向別のデータを使用することで、ネットワーク内の輻輳などの問題点がある場所をより迅速に特定できます。

UDP ジッタ動作では、疑似的な UDP トラフィックが生成され、大量の UDP パケットが送信されます。各パケットは、サイズが指定され、送信元ルータから宛先ルータへ指定された時間間隔（ミリ秒単位）で送信されます。さらにこうしたパケットの送信が、指定された時間間隔で繰り返し実行されます。デフォルトでは、ペイロード サイズが 10 バイトのパケット フレームが 10 ミリ秒間隔で計 10 個生成され、60 秒ごとにこの動作が繰り返し実行されます。これらの各パラメータを設定することにより、目的の IP サービスを的確にシミュレーションできます。

一方向遅延を正確に測定するには、送信元と宛先デバイスとの間に、NTP などによる時刻同期が必要です。一方向ジッタおよび一方向パケット損失の測定には、時刻同期は不要です。送信元デバイスと宛先デバイスとの間で時刻が同期していない場合、一方向ジッタおよび一方向パケット損失に関するデータは取得できますが、UDP ジッタ動作による一方向遅延の測定では、値 *0* が返されます。

（注） 送信元デバイス上で UDP ジッタ動作を設定する場合は、あらかじめ宛先デバイス（動作のターゲット）上で IP SLA レスポンダをイネーブルにしておく必要があります。

送信元デバイス上で UDP ジッタ動作を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]	IP SLA 動作を UDP ジッタ動作として設定し、UDP ジッタ コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先の IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先のポート番号を、1 ～ 65535 の範囲で指定します。 • （任意）**source-ip** {*ip-address* | *hostname*}：送信元の IP アドレスまたはホスト名を指定します。送信元の IP アドレスまたはホスト名を指定しない場合は、宛先に最も近い IP アドレスが IP SLA によって選択されます。 • （任意）**source-port** *port-number*：送信元のポート番号を、1 ～ 65535 の範囲で指定します。ポート番号を指定しない場合は、使用可能なポートが IP SLA によって選択されます。 • （任意）**control**：IP SLA レスポンダへの IP SLA コントロール メッセージの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA レスポンダとの接続を確立するため、IP SLA コントロール メッセージが宛先デバイスに送信されます。 • （任意）**num-packets** *number-of-packets*：生成するパケットの数を入力します。指定できる範囲は 1 ～ 6000 で、デフォルト値は 10 です。 • （任意）**interval** *inter-packet-interval*：パケットの送信間隔をミリ秒単位で入力します。指定できる範囲は 1 ～ 6000 で、デフォルト値は 20 ミリ秒です。
ステップ 4	**frequency** *seconds*	（任意）指定された IP SLA 動作を繰り返し実行する周期を設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。

	コマンド	目的
ステップ 5	**exit**	UDP ジッタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip sla monitor schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]	個々の IP SLA 動作に対してスケジューリング パラメータを設定します。 • *operation-number* : Response Time Reporter（RTR）エントリ番号を入力します。 •（任意）**life** : 動作を無制限（**forever**）または特定の*秒*数（seconds）実行するかを設定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time** : 情報収集を開始する動作の時間を入力します。 – 特定の時間に開始するには、時間、分、秒（24 時間式）および日付を入力します。月を指定しない場合、現在の月がデフォルトとして設定されます。 – 開始時間を選択するまで情報を収集しないように選択するには **pending** を入力します。 – 動作を即座に開始するには **now** を入力します。 – 入力した時間が経過した後に動作を開始するには、**after** *hh:mm:ss* を入力します。 •（任意）**ageout** *seconds* : 情報をアクティブに収集していない場合に動作をメモリに保存しておく秒数を入力します。指定できる範囲は 0 ～ 2073600 秒で、デフォルトは 0 秒（無期限に保持）です。 •（任意）**recurring** : 動作が毎日自動的に実行されるよう設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip sla configuration** [*operation-number*]	（任意）すべての IP SLA 動作または特定の動作のすべてのデフォルト値を含む、設定値を表示します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA 動作をディセーブルにするには、no **ip sla** *operation-number* グローバル コンフィギュレーション コマンドを入力します。次に、IP SLA の UDP ジッタ動作を設定する方法の例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
```

```
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

ICMP エコー動作による IP サービス レベルの分析

ICMP エコー動作では、シスコ製デバイスと、IP を使用する任意のデバイスとの、エンドツーエンドの応答時間が測定されます。応答時間は、宛先へ ICMP エコー要求メッセージを送信してから ICMP エコー応答を受信するまでの所要時間を測定して算出されます。送信元 IP SLA デバイスと宛先 IP デバイスの間の応答時間を測定する際、多くのお客様が、ICMP ベースの IP SLA 動作、社内 ping テスト、または ping ベースの専用プローブを使用しています。IP SLA の ICMP エコー動作は、ICMP ping テストと同じ仕様に準拠しているため、応答時間の測定結果は、どちらの方法を使用しても同じです。

（注） ICMP エコー動作では、IP SLA レスポンダをイネーブルにする必要はありません。

送信元デバイス上で ICMP エコー動作を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-id*]	IP SLA 動作を ICMP エコー動作として設定し、ICMP エコー コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先の IP アドレスまたはホスト名を指定します。 • （任意）**source-ip** {*ip-address* | *hostname*}：送信元の IP アドレスまたはホスト名を指定します。送信元の IP アドレスまたはホスト名を指定しない場合は、宛先に最も近い IP アドレスが IP SLA によって選択されます。 • （任意）**source-interface** *interface-id*：この動作に使用する送信元のインターフェイスを指定します。
ステップ 4	**frequency** *seconds*	（任意）指定された IP SLA 動作を繰り返し実行する周期を設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 5	**exit**	UDP ジッタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]	個々の IP SLA 動作に対してスケジューリング パラメータを設定します。 • *operation-number*：Response Time Reporter（RTR）エントリ番号を入力します。 •（任意）**life**：動作を無制限（**forever**）または特定の*秒*数（seconds）実行するかを設定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time**：情報収集を開始する動作の時間を入力します。 – 特定の時間に開始するには、時間、分、秒（24 時間式）および日付を入力します。月を指定しない場合、現在の月がデフォルトとして設定されます。 – 開始時間を選択するまで情報を収集しないように選択するには **pending** を入力します。 – 動作を即座に開始するには **now** を入力します。 – 入力した時間が経過した後に動作を開始する場合は、**after** *hh:mm:ss* を入力します。 •（任意）**ageout** *seconds*：情報をアクティブに収集していない場合に動作をメモリに保存しておく秒数を入力します。指定できる範囲は 0 ～ 2073600 秒で、デフォルトは 0 秒（無期限に保持）です。 •（任意）**recurring**：動作が毎日自動的に実行されるよう設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip sla configuration** [*operation-number*]	（任意）すべての IP SLA 動作または特定の動作のすべてのデフォルト値を含む、設定値を表示します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA 動作をディセーブルにするには、**no ip sla** *operation-number* グローバル コンフィギュレーション コマンドを入力します。次に、IP SLA の ICMP エコー動作を設定する方法の例を示します。

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
```

```
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

IP SLA 動作のモニタリング

IP SLA 動作の設定および結果を表示するときは、表 41-1 に示すユーザ EXE コマンドまたは特権 EXEC コマンドを使用します。

表 41-1　IP SLA 動作のモニタリング

コマンド	目的
show ip sla application	Cisco IOS IP SLA に関するグローバル情報を表示します。
show ip sla authentication	IP SLA の認証情報を表示します。
show ip sla configuration [*entry-number*]	すべての IP SLA 動作または特定の動作のすべてのデフォルト値を含む、設定値を表示します。
show ip sla enhanced-history {**collection-statistics** | **distribution statistics**} [*entry-number*]	収集された履歴バケットに関する拡張履歴統計情報、またはすべての IP SLA 動作あるいは特定の IP SLA 動作に関する分散統計情報を表示します。
show ip sla ethernet-monitor configuration [*entry-number*]	IP SLA 自動イーサネット設定を表示します。
show ip sla group schedule [*schedule-entry-number*]	IP SLA グループ スケジューリング設定およびその詳細を表示します。
show ip sla history [*entry-number* | **full** | **tabular**]	すべての IP SLA 動作について収集された履歴を表示します。
show ip sla mpls-lsp-monitor {**collection-statistics** | **configuration** | **ldp operational-state** | **scan-queue** | **summary** [*entry-number*] | **neighbors**}	MPLS Label Switched Path（LSP; ラベル スイッチド パス）ヘルス モニタ動作を表示します。
show ip sla reaction-configuration [*entry-number*]	すべての IP SLA 動作または特定の動作について、事前に設定したしきい値のモニタリング設定を表示します。
show ip sla reaction-trigger [*entry-number*]	すべての IP SLA 動作または特定の動作に関する反応トリガ情報を表示します。
show ip sla responder	IP SLA レスポンダに関する情報を表示します。
show ip sla statistics [*entry-number* | **aggregated** | **details**]	現在または集約された操作ステータスおよび統計情報を表示します。

TWAMP の概要

TWAMP は、関連する 2 つのプロトコルで構成されます。パフォーマンス測定セッションを開始するときは、TWAMP 制御プロトコルを使用します。パフォーマンス測定プローブを送受信するときは、TWAMP テスト プロトコルを使用します。TWAMP は、制御クライアントおよびセッション センダを 1 つのデバイス上に配置し、サーバおよびセッション リフレクタをもう 1 つのデバイス上に配置するという簡単なネットワーク アーキテクチャにより導入できます。

Cisco IOS ソフトウェアでの TWAMP 実装では基本的な設定がサポートされています。図 41-3 は配置例を示したものです。

図 41-4 は、TWAMP を構成する 4 つの論理エンティティの模式図です。

図 41-3　　TWAMP の導入

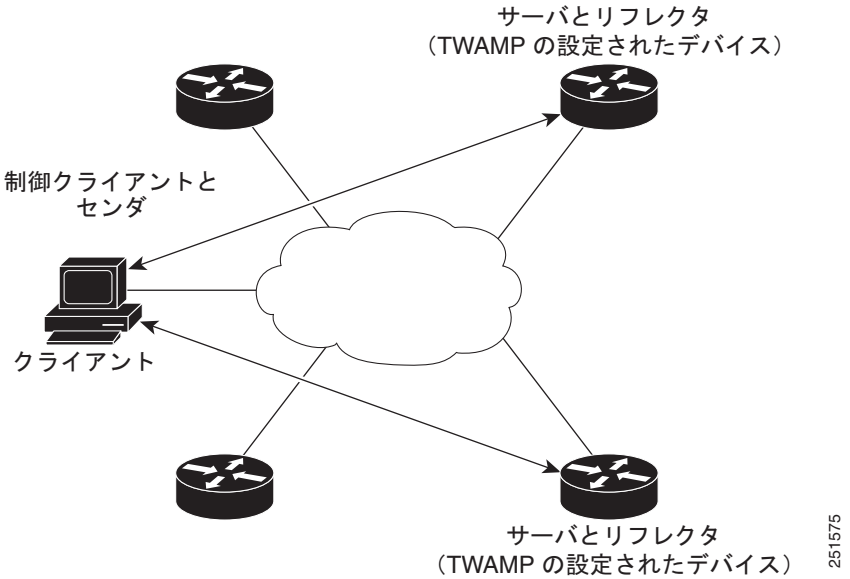
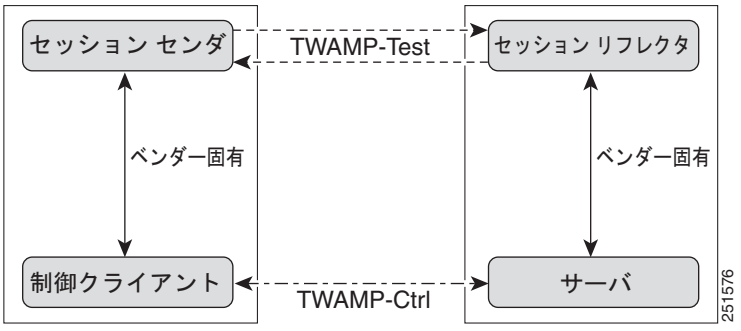


図 41-4　　TWAMP のアーキテクチャ



このプロトコルでは、各エンティティはそれぞれ独立していますが、それらの役割を 1 つのデバイス上に論理的にマージできます。

TWAMP の設定

- 「TWAMP サーバの設定」（P.41-15）
- 「TWAMP リフレクタの設定」（P.41-16）
- 「TWAMP に関するトラブルシューティング」（P.41-16）

TWAMP サーバの設定

TWAMP のサーバ機能とリフレクタ機能は、同一のデバイス上に設定できます。

（注）　スイッチでは、TWAMP のサーバ機能およびリフレクタ機能はサポートされていません。

TWAMP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla server twamp**	スイッチを TWAMP サーバとして設定し、TWAMP コンフィギュレーション モードを開始します。
ステップ 3	**port** *port-number*	（任意）TWAMP サーバにおいて接続要求および制御要求をリスンするために使用するポートを指定します。パフォーマンス プローブが送信されるポートのネゴシエーションも、このポートにより行われます。このポートには、IANA ウェルノウン ポート ポートなど、他のアプリケーションにより使用されているポートは指定できません。デフォルトはポート 862 です。
ステップ 4	**timer inactivity** *seconds*	（任意）セッションが終了することなく非アクティブ状態を継続できる最長時間を秒単位で設定します。指定できる範囲は、1 ～ 6000 秒です。デフォルト値は 900 秒です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip sla standards**	（任意）スイッチ上でサポートされている IP SLA の規格を表示します。
ステップ 7	**show ip sla twamp connection requests**	（任意）TWAMP 接続の数および発信元を表示します。
ステップ 8	**show ip sla twamp connection detail**	（任意）接続 ID、クライアントの IP アドレスとポート番号、TWAMP 接続のモードとステータス、およびテスト要求の数を表示します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA TWAMP サーバをディセーブルにする場合は、**no ip sla server twamp** グローバル コンフィギュレーション コマンドを入力します。次に、スイッチを IP SLA TWAMP サーバとして設定する方法の例を示します。

```
Switch(config)# ip sla server twamp
Switch(config-twamp-srvr)# port 9000
Switch(config-twamp-srvr)# timer inactivity 300
```

TWAMP リフレクタの設定

TWAMP のサーバ機能とリフレクタ機能は、同一のデバイス上に設定できます。

TWAMP リフレクタを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla responder twamp**	スイッチを TWAMP レスポンダとして設定し、TWAMP コンフィギュレーション モードを開始します。
ステップ 3	**timeout** *seconds*	（任意）セッションが終了することなく非アクティブ状態を継続できる最長時間を秒単位で設定します。指定できる範囲は 1 ～ 604800 秒です。デフォルト値は 900 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip sla twamp session** [**source-ip** *ip-address* **source-port** *port-number*]	（任意）指定したクライアントに対する TWAMP テストの結果を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA TWAMP リフレクタをディセーブルにする場合は、**no ip sla responder twamp** グローバル コンフィギュレーション コマンドを入力します。次に、スイッチを IP SLA TWAMP リフレクタとして設定する方法の例を示します。

```
Switch(config)# ip sla responder twamp
Switch(config-twamp-srvr)# timeout 300
```

TWAMP に関するトラブルシューティング

TWAMP セッションに関するトラブルシューティングを行う場合は、次のコマンドを使用します。

debug ip sla error twamp [**connection source-ip** *ip-address* | **control** {**reflector** | **server**} | **session source-ip** *ip-address*]

debug ip sla trace twamp [**connection source-ip** *ip-address* | **control** {**reflector** | **server**} | **session source-ip** *ip-address*]

CHAPTER 42

拡張オブジェクト トラッキングの設定

この章では、Cisco ME 3400E スイッチに拡張オブジェクト トラッキングを設定する方法について説明します。この機能は、Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）のトラッキング メカニズムに対する優れた代替手段を提供するものであり、この機能を使用すれば、インターフェイスのライン プロトコル ステートを追跡できます。あるインターフェイスのライン プロトコル ステートがダウンした場合、そのインターフェイスの HSRP プライオリティが下がり、高いプライオリティを持つ別の HSRP デバイスがアクティブになります。拡張オブジェクト トラッキング機能により、HSRP からトラッキング メカニズムが分離され、個別の独立したトラッキング プロセスが生成されます。このプロセスは HSRP 以外のプロセスで使用できます。また、この機能により、インターフェイス ライン プロトコル ステートに加えて、他のオブジェクトも追跡できます。

HSRP や Gateway Local Balancing Protocol（GLBP）などのクライアント プロセスは、オブジェクトを追跡する対象を登録し、追跡対象オブジェクトのステートが変化したら通知するように要求できます。この機能を使用することにより、ルーティング システムのアベイラビリティおよび回復速度が向上し、停止回数および停止時間が減少します。

拡張オブジェクト トラッキングおよびその設定に使用するコマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541be.html

この章で説明する内容は、次のとおりです。

- 「拡張オブジェクト トラッキングの概要」（P.42-1）
- 「拡張オブジェクト トラッキング機能の設定」（P.42-2）
- 「拡張オブジェクト トラッキングのモニタリング」（P.42-13）

拡張オブジェクト トラッキングの概要

各追跡対象オブジェクトには、トラッキング CLI（コマンドライン インターフェイス）で指定される一意の番号があります。クライアント プロセスでは、この番号を使用して特定のオブジェクトを追跡します。トラッキング プロセスでは、追跡対象オブジェクトに値の変更がないかどうかを定期的にポーリングし、（アップ値またはダウン値など）変化があれば登録されているクライアント プロセスに送信します。ただちに通知する場合と、指定された時間遅延後に送信する場合があります。同じオブジェクトを複数のクライアントが追跡して、オブジェクトのステートが変化した場合にそれぞれ異なるアクションを実行できます。

複数のオブジェクトを組み合せて 1 つのリストにして追跡することもできます。このリストの状態を判定するには、ウェイトしきい値またはパーセントしきい値を使用します。オブジェクトの組み合せには、ブール ロジックを使用できます。「AND」ブール関数を使用する追跡リストでは、リスト内の各

オブジェクトがアップ ステートでないと追跡対象オブジェクトはアップになりません。「OR」ブール関数を使用する追跡リストでは、リスト内の 1 つのオブジェクトだけがアップ ステートであれば追跡対象オブジェクトはアップになります。

拡張オブジェクト トラッキング機能の設定

- 「デフォルト設定」（P.42-2）
- 「インターフェイス ライン プロトコルまたは IP ルーティング ステートの追跡」（P.42-2）
- 「追跡リストの設定」（P.42-3）
- 「HSRP オブジェクト トラッキングの設定」（P.42-7）
- 「他のトラッキング特性の設定」（P.42-8）
- 「IP SLA オブジェクト トラッキングの設定」（P.42-9）
- 「スタティック ルーティング サポートの設定」（P.42-10）

デフォルト設定

いかなるオブジェクト トラッキングのタイプも設定されていません

インターフェイス ライン プロトコルまたは IP ルーティング ステートの追跡

インターフェイス ライン プロトコル ステートまたはインターフェイス IP ルーティング ステートのいずれかを追跡できます。IP ルーティング ステートを追跡する場合、そのオブジェクトをアップにするには次の 3 つの条件が必要です。

- IP ルーティングがインターフェイス上でイネーブルおよびアクティブである必要があります。
- インターフェイス ライン プロトコル ステートがアップである必要があります。
- インターフェイス IP アドレスが既知である必要があります。

これら 3 つの条件がすべて満たされていない場合、IP ルーティング ステートはダウンします。

インターフェイスのライン プロトコル ステートまたは IP ルーティング ステートを追跡するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-number* **interface** *interface-id* **line-protocol**	（任意）インターフェイスのライン プロトコル ステートを追跡するためのトラッキング リストを作成して、トラッキング コンフィギュレーション モードを開始します。 • *object-number*：追加対象オブジェクトを識別します。指定できる範囲は 1 ～ 500 です。 • **interface** *interface-id*：追跡されたインターフェイスです。
ステップ 3	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追加対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 5	**track** *object-number* **interface** *interface-id* **ip routing**	（任意）インターフェイスの IP ルーティング ステートを追跡するためのトラッキング リストを作成して、トラッキング コンフィギュレーション モードを開始します。IP ルート トラッキングでは、ルーティング テーブル内の IP ルートおよびインターフェイスの IP パケット ルーティング機能を追跡します。 • *object-number*：追加対象オブジェクトを識別します。指定できる範囲は 1 ～ 500 です。 • **interface** *interface-id*：追跡されたインターフェイスです。
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追加対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track** *object-number*	指定されたオブジェクトが追跡されていることを確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス ライン プロトコル ステートのトラッキングを設定して、その設定を確認する例を示します。

```
Switch(config)# track 33 interface gigabitethernet0/1 line-protocol
Switch(config-track)# end
Switch# show track 33
Track 33
  Interface GigabitEthernet0/1 line-protocol
  Line protocol is Down (hw down)
    1 change, last change 00:18:28
```

追跡リストの設定

オブジェクトの追跡リストは、ブール式、ウェイトしきい値、またはパーセントしきい値を使用して設定できます。追跡リストには、1 つまたは複数のオブジェクトが含まれます。オブジェクトが存在していないと、追跡リストに追加できません。

- 演算を指定するのにブール式を設定するときは、「AND」または「OR」演算子のどちらかを使用します。
- 追跡リスト ステートをウェイトしきい値を使用して測定するときは、追跡リスト内の各オブジェクトに重み番号を割り当てます。追跡リストのステートは、このしきい値に合致したかどうかで判別されます。各オブジェクトのステートは、すべてのオブジェクトの合計重みと各オブジェクトのしきい値の重みを比較して判別されます。
- 追跡リスト ステートをパーセントしきい値を使用して測定するときは、追跡リスト内の各オブジェクトにパーセントしきい値を割り当てます。各オブジェクトのステートは、各オブジェクトに割り当てられたパーセント値とリストを比較して判別されます。

ブール式を使用した追跡リストの設定

ブール式を使用して追跡リストを設定すると、「AND」または「OR」演算子を使用した演算が可能になります。たとえば、「AND」演算子を使用して 2 つのインターフェイスを追跡するとき、*up* は両方のインターフェイスがアップであることを意味し、*down* はいずれかのインターフェイスがダウンであることを意味します。

ブール式を使用してオブジェクトの追跡リストを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *track-number* **list boolean** {**and** | **or**}	追跡リストのオブジェクトを設定して、トラッキング コンフィギュレーション モードを開始します。*track-number* に指定できる値は 1 ～ 500 です。 • **boolean**：ブール式に基づいて追跡リストのステートを指定します。 • **and**：すべてのオブジェクトがアップであればリストはアップで、1 つまたは複数のオブジェクトがダウンであればリストはダウンであることを指定します。 • **or**：1 つのオブジェクトがアップであればリストはアップで、すべてのオブジェクトがダウンであればリストはダウンであることを指定します。
ステップ 3	**object** *object-number* [**not**]	追跡されるオブジェクトを指定します。指定できる範囲は 1 ～ 500 です。キーワード **not** は、オブジェクトのステートを否定します。これは、オブジェクトがアップである場合に、追跡リストはそのオブジェクトをダウンとして検出することを意味します。 **（注）**　オブジェクトが存在していないと、追跡リストに追加できません。
ステップ 4	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追加対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show track** *object-number*	指定されたオブジェクトが追跡されていることを確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

追跡リストを削除する場合は、**no track** *track-number* グローバル コンフィギュレーション コマンドを使用します。

次に、AND ブール式を使用して追跡リスト 4 を設定する例を示します。リストには 2 つのオブジェクトが含まれ、そのうち 1 つは否定されます。リストがアップである場合は、オブジェクト 2 がダウンであることを検出しています。

```
Switch(config)# track 4 list boolean and
Switch(config-track)# object 1
Switch(config-track)# object 2 not
Switch(config-track)# exit
```

ウェイトしきい値を使用した追跡リストの設定

ウェイトしきい値により追跡するには、オブジェクトの追跡リストを設定し、しきい値として重みが使用されることを指定して、リストの各オブジェクトに重み値を設定します。各オブジェクトのステートは、アップであるすべてのオブジェクトの合計重みと各オブジェクトのしきい値の重みを比較して判別されます。

ウェイトしきい値のリストには、ブール式の「NOT」演算子を使用できません。

ウェイトしきい値を使用してオブジェクトの追跡リストを設定し、各オブジェクトの重みを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *track-number* **list threshold weight**	追跡リストのオブジェクトを設定して、トラッキング コンフィギュレーション モードを開始します。*track-number* に指定できる値は 1 ～ 500 です。 • **threshold**：しきい値に基づいて追跡リストのステートを指定します。 • **weight**：しきい値が重みに基づくことを指定します。
ステップ 3	**object** *object-number* [**weight** *weight-number*]	追跡されるオブジェクトを指定します。指定できる範囲は 1 ～ 500 です。任意の **weight** *weight-number* は、オブジェクトのしきい値の重みを指定します。指定できる範囲は 1 ～ 255 です。 **（注）**　オブジェクトが存在していないと、追跡リストに追加できません。
ステップ 4	**threshold weight** {**up** *number* | [**down** *number*]}	しきい値の重みを指定します。 • **up** *number*：指定できる範囲は、1 ～ 255 です。 • **down** *number*：（任意）指定できる範囲は、**up** *number* で選択された数により異なります。**up** *number* を 25 に設定した場合、down number の範囲は 0 ～ 24 となります。
ステップ 5	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追加対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show track** *object-number*	指定されたオブジェクトが追跡されていることを確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

追跡リストを削除する場合は、**no track** *track-number* グローバル コンフィギュレーション コマンドを使用します。

次に、ウェイトしきい値により追跡する追跡リスト 4 を設定する例を示します。オブジェクト 1 およびオブジェクト 2 がダウンである場合、オブジェクト 3 が up 30 というしきい値を満たすため、追跡リスト 4 はアップになります。ただし、オブジェクト 3 がダウンである場合、しきい値の重みを満たすには、オブジェクト 1 および オブジェクト 2 の両方がアップである必要があります。

```
Switch(config)# track 4 list threshold weight
Switch(config-track)# object 1 weight 15
Switch(config-track)# object 2 weight 20
Switch(config-track)# object 3 weight 30
Switch(config-track)# threshold weight up 30 down 10
Switch(config-track)# exit
```

この設定は、オブジェクト 1 およびオブジェクト 2 が 2 つの小さな帯域幅の接続を、オブジェクト 3 が大きな帯域幅の接続を表す場合に有効です。設定された **down 10** の値は、追跡対象オブジェクトが一度アップになると、しきい値が 10 以下になるまでダウンしないということを意味します。この例の場合、10 以下はすべての接続がダウンすることを意味します。

パーセントしきい値を使用した追跡リストの設定

パーセントしきい値を使用して追跡するには、オブジェクトの追跡リストを設定し、しきい値としてパーセントを使用することを指定して、リスト内のすべてのオブジェクトにパーセント値を指定します。リストのステートは、各オブジェクトに割り当てられたパーセント値とリストを比較して判別されます。

パーセントしきい値のリストには、ブール式の「NOT」演算子を使用できません。

パーセントしきい値を使用してオブジェクトの追跡リストを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *track-number* **list threshold percentage**	追跡リストのオブジェクトを設定して、トラッキング コンフィギュレーション モードを開始します。*track-number* に指定できる値は 1 ～ 500 です。 • **threshold**：しきい値に基づいて追跡リストのステートを指定します。 • **percentage**：しきい値がパーセントに基づくことを指定します。
ステップ 3	**object** *object-number*	追跡されるオブジェクトを指定します。指定できる範囲は 1 ～ 500 です。 **（注）**　オブジェクトが存在していないと、追跡リストに追加できません。
ステップ 4	**threshold percentage** {**up** *number* | [**down** *number*]}	しきい値のパーセンテージを指定します。 • **up** *number*：指定できる範囲は、1 ～ 100 です。 • **down** *number*：（任意）指定できる範囲は、**up** *number* で選択された数により異なります。**up** *number* を 25 に設定した場合、down number の範囲は 0 ～ 24 となります。
ステップ 5	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追加対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show track** *object-number*	指定されたオブジェクトが追跡されていることを確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

追跡リストを削除する場合は、**no track** *track-number* グローバル コンフィギュレーション コマンドを使用します。

次に、3 つのオブジェクトを持つ追跡リスト 4 および指定されたパーセント値を設定して、リストのステートを判定する例を示します。

```
Switch(config)# track 4 list threshold percentage
Switch(config-track)# object 1
Switch(config-track)# object 2
Switch(config-track)# object 3
Switch(config-track)# threshold percentage up 51 down 10
Switch(config-track)# exit
```

HSRP オブジェクト トラッキングの設定

特定のオブジェクトを追跡し、そのオブジェクトのステートに基づいて HSRP プライオリティを変更するようスタンバイ HSRP グループを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-number* {**interface** *interface-id* {**line-protocol** | **ip routing**} | *ip route ip-address/prefix-length* {**metric threshold** | **reachability**} | **list** {**boolean** {**and** | **or**}} | {**threshold** {**weight** | **percentage**}}}	（任意）設定されたステートを追跡するためのトラッキング リストを作成して、トラッキング コンフィギュレーション モードを開始します。 • *object-number* に指定できる範囲は 1 ～ 500 です。 • 追跡するインターフェイスを選択するには、**interface** *interface-id* を入力します。 • インターフェイス ライン プロトコル ステートを追跡するには、**line-protocol** を入力し、インターフェイス IP ルーティング ステートを追跡するには、**ip routing** を入力します。 • IP ルートのステートを追跡するには、**ip route** *ip-address/prefix-length* を入力します。 • しきい値のメトリックを追跡するには、**metric threshold** を入力し、ルートが到達可能かどうかを追跡するには、**reachability** を入力します。 デフォルトの up しきい値は 254、デフォルトの down しきい値は 255 です。 • リスト内の一連のオブジェクトを追跡するには、**list** を入力します。リストはこれまでのページの説明に従って設定してください。 – **boolean** については、「ブール式を使用した追跡リストの設定」（P.42-4）を参照してください。 – **threshold weight** については、「ウェイトしきい値を使用した追跡リストの設定」（P.42-5）を参照してください。 – **threshold percentage** については、「パーセントしきい値を使用した追跡リストの設定」（P.42-6）を参照してください。 **（注）**　追跡するインターフェイスごとにこの手順を繰り返してください。
ステップ 3	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 で、デフォルト値は 0 です。HSRP グループが 1 つだけであれば、グループ番号を指定する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホット スタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスとなるように指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 6	**standby** [*group-number*] **track** *object-number* [**decrement** [*priority-decrement*]]	特定のオブジェクトを追跡して、そのオブジェクトのステートに基づいてホット スタンバイ プライオリティを変更するよう HSRP を設定します。 • （任意）*group-number*：トラッキングが適用されるグループ番号を入力します。 • *object-number*：追跡対象のオブジェクト番号を入力します。指定できる範囲は 1 ～ 500 で、デフォルトは 1 です。 • （任意）**decrement** *priority-decrement*：追跡対象オブジェクトがダウンした場合、または稼動状態に戻った場合に、ルータのホット スタンバイ プライオリティを減少または増加させる幅を指定します。指定できる範囲は 1 ～ 255 で、デフォルトは 10 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show standby**	スタンバイ ルータの IP アドレスおよびトラッキング ステートを確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

他のトラッキング特性の設定

拡張オブジェクト トラッキングは、他の特性を追跡する場合にも使用できます。

- **track ip route reachability** グローバル コンフィギュレーション コマンドを使用すると、IP ルートの到達可能性を追跡できます。
- **track ip route metric threshold** グローバル コンフィギュレーション コマンドを使用すると、ルートがしきい値を越えているか下回っているかを判別できます。
- **track resolution** グローバル コンフィギュレーション コマンドを使用すると、ルーティング プロトコルのメトリック解決のデフォルト値を変更できます。
- **track timer** グローバル コンフィギュレーション コマンドを使用すると、トラッキング プロセスで追跡対象オブジェクトを定期的にポーリングするよう設定できます。

拡張オブジェクト トラッキングの設定を確認する場合は、**show track** 特権 EXEC コマンドを使用します。

拡張オブジェクト トラッキングおよびその設定に使用するコマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541be.html

IP SLA オブジェクト トラッキングの設定

Cisco IOS IP Service Level Agreement（IP SLA）は、ネットワーク パフォーマンスの測定および診断ツールであり、ネットワーク パフォーマンスを測定するためのトラフィックを生成することによって、アクティブ モニタリングが使用されます。Cisco IP SLA の動作により、ネットワークのトラブルシューティング、設計、および分析に利用可能なリアルタイムのメトリックが収集されます。

スイッチ上の Cisco IP SLA の詳細については、第 41 章「Cisco IOS IP SLA 動作の設定」を参照してください。IP SLA のコマンドについては、次の URL にある、『*Cisco IOS IP SLAs Command Reference*』*Release 12.4T* を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

IP SLA のオブジェクト トラッキングの動作により、クライアントは、IP SLA オブジェクトからの出力を追跡し、その情報を使用してアクションをトリガーできます。すべての IP SLA の動作により、*OK* や *OverThreshold* などの SNMP 動作のリターンコード値が保持されます。この値はトラッキング プロセスによって解釈されます。ステートと到達可能性という、IP SLA の動作の 2 つの面を追跡できます。ステートについては、リターン コードが OK の場合、追跡ステートはアップの状態であり、リターン コードが OK でない場合は、追跡ステートはダウンの状態です。到達可能性については、リターン コードが OK または OverThreshold の場合、到達可能性はアップの状態であり、OK でない場合は、到達可能性はダウンの状態です。

IP SLA 動作のステートまたは IP SLA IP ホストの到達可能性を追跡するには、特権 EXEC モードで、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-number* **rtr** *operation-number* **state**	IP SLA 動作のステートを追跡するには、トラッキング コンフィギュレーション モードを開始します。 • *object-number* に指定できる範囲は 1 ～ 500 です。 • *operation-number* に指定できる範囲は 1 ～ 2147483647 です。
ステップ 3	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追加対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**track** *object-number* **rtr** *operation-number* **reachability**	IP SLA IP ホストの到達可能性を追跡するには、トラッキング コンフィギュレーション モードを開始します。 • *object-number* に指定できる範囲は 1 ～ 500 です。 • *operation-number* に指定できる範囲は 1 ～ 2147483647 です。
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}	（任意）追加対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track** *object-number*	設定を確認するためのトラッキング情報を表示します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、IP SLA ステート トラッキングを設定および表示する例を示します。

```
Switch(config)# track 2 200 state
Switch(config)# end
Switch# show track 2
Track 2
  Response Time Reporter 1 state
```

```
  State is Down
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (millisecs) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

次に、ルートが到達可能であるかどうかを示す出力の例を示します。

```
Switch(config)# track 3 500 reachability
Switch(config)# end
Switch# show track 3
Track 3
  Response Time Reporter 1 reachability
  Reachability is Up
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (millisecs) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

スタティック ルーティング サポートの設定

拡張オブジェクト トラッキングを使用したスタティック ルーティング サポートは、スイッチが、ICMP ping によって、事前に設定されたスタティック ルートまたは DHCP ルートがダウンしたタイミングを特定することを可能にする機能を備えています。トラッキングをイネーブルにすると、システムによってルートのステートが追跡され、そのステートが変わるとクライアントに対して通知が行われます。スタティック ルート オブジェクト トラッキングでは、Cisco IP SLA が使用され、プライマリ ゲートウェイへの接続のステートを監視するための ICMP ping が生成されます。

- スイッチ上の Cisco IP SLA サポートの詳細については、第 41 章「Cisco IOS IP SLA 動作の設定」を参照してください。
- スタティック ルート オブジェクト トラッキングの詳細については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

スタティック ルート オブジェクト トラッキングを設定するには、次の手順を実行します。

ステップ 1　スタティック ルーティングまたは DHCP のプライマリ インターフェイスを設定します。

ステップ 2　プライマリ インターフェイスを使用して IP アドレスに対する ping を実行するための IP SLA エージェントと、そのエージェントのステートを監視するための追跡オブジェクトを設定します。

ステップ 3　セカンダリ インターフェイスを使用して、デフォルト スタティック デフォルト ルートを設定します。このルートは、プライマリ ルートが削除された場合にだけ使用されます。

プライマリ インターフェイスの設定

スタティック ルーティングのプライマリ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	プライマリまたはセカンダリ インターフェイスを選択して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**description** *string*	インターフェイスに対して説明を追加します。
ステップ 4	**ip address** *ip-address mask* **[secondary]**	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

DHCP のプライマリ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	プライマリまたはセカンダリ インターフェイスを選択して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**description** *string*	インターフェイスに対して説明を追加します。
ステップ 4	**ip dhcp client route track** *number*	追加したルートを指定した追跡番号に関連付けるには、DCHP クライアントを設定します。有効な番号は 1 ～ 500 です。
ステップ 5	**ip address dhcp**	イーサネット インターフェイス上で DHCP から IP アドレスを取得します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

Cisco IP SLAs Monitoring Agent および追跡オブジェクトの設定

Cisco IP SLA を使用したネットワーク モニタリングを設定するには、特権 EXEC モードで次の手順を実行します。

ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	Cisco IP SLA 動作の設定を開始して、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	**icmp-echo** {*destination-ip-address* | *destination hostname* [**source- ipaddr** {*ip-address* | *hostname* **source-interface** *interface-id*]	Cisco IP SLA のエンドツーエンド ICMP エコー要求時間動作を設定し、IP SLA ICMP エコー コンフィギュレーション モードを開始します。
ステップ 4	**timeout** *milliseconds*	動作が、その要求パケットからの応答を待機する時間を設定します。
ステップ 5	**frequency** *seconds*	動作がネットワークに送信されるレートを設定します。
ステップ 6	**threshold** *milliseconds*	リアクション イベントを生成し、動作の履歴情報を保存する上昇しきい値（ヒステリシス）を設定します。
ステップ 7	**exit**	IP SLA ICMP エコー コンフィギュレーション モードを終了します。

ステップ 8	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] **start-time** *time* | **pending** | **now** | **after** *time*] [**ageout** *seconds*] [**recurring**]	単一の IP SLA 動作のスケジューリング パラメータを設定します。
ステップ 9	**track** *object-number* **rtr** *operation-number* { {**state** | **reachability**}	Cisco IOS IP SLA 動作のステートを追跡し、トラッキング コンフィギュレーション モードを開始します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show track** *object-number*	設定を確認するためのトラッキング情報を表示します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング ポリシーおよびデフォルト ルートの設定

オブジェクト トラッキングを使用してスタティック ルーティングをバックアップするルーティング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。この手順で使用するコマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number*	拡張 IP アクセス リストを定義します。任意の特性を設定します。
ステップ 3	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]	ルートマップ コンフィギュレーション モードを開始し、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配信するための条件を定義します。
ステップ 4	**match ip address** {*access-list number* | *access-list name*}	標準または拡張アクセス リストによって許可されるか、あるいは、パケット上のポリシー ルーティングを実行する、宛先ネットワーク番号アドレスを持つルートを配信します。複数の番号または名前を入力できます。
ステップ 5	**set ip next-hop dynamic dhcp**	DHCP ネットワーク専用です。DHCP によって直近に学習されたゲートウェイへのネクスト ホップを設定します。
ステップ 6	**set interface** *interface-id*	スタティック ルーティング ネットワーク専用です。ポリシー ルーティング用のルート マップの match 文を渡す出力パケットの送信先を示します。
ステップ 7	**exit**	ルートマップ コンフィギュレーション モードを終了します。
ステップ 8	**ip local policy route-map** *map-tag*	ローカル ポリシー ルーティング用に使用するルート マップを特定します。
ステップ 9	**ip route** *prefix mask* {*ip-address* | { *interface-id* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *track-number*] [*tag tag*]	スタティック ルーティング ネットワーク専用です。スタティック ルートを確立します。 **track** *track-number* を入力すると、設定された追跡オブジェクトがアップの場合にだけスタティック ルートがインストールされるように指定されます。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip route track table**	IP ルート追跡テーブルに関する情報を表示します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定例については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

拡張オブジェクト トラッキングのモニタリング

拡張オブジェクト トラッキングの情報を表示するには、表 42-1 に示す特権 EXEC コマンドまたはユーザ EXEC コマンドを使用します。

表 42-1　トラッキング情報を表示するためのコマンド

コマンド	目的
show ip route track table	IP ルート追跡テーブルに関する情報を表示します。
show track [*object-number*]	すべてのトラッキング リストまたは指定したリストに関する情報を表示します。
show track brief	トラッキング情報出力を 1 行表示します。
show track interface [**brief**]	追跡対象のインターフェイス オブジェクトに関する情報を表示します。
show track ip [*object-number*] [**brief**] **route**	追跡対象の IP ルート オブジェクトに関する情報を表示します。
show track resolution	追跡対象のパラメータの解決を表示します。
show track timers	追跡対象のポーリング インターバル タイマーを表示します。

CHAPTER 43

イーサネット OAM、CFM、および E-LMI の設定

イーサネットの Operations, Administration, and Maintenance（OAM; 運用、管理および保守）はイーサネット ネットワークの設置、モニタ、およびトラブルシューティングのためのプロトコルで、総体的な Ethernet インフラストラクチャのコンテキストの中で管理機能を向上します。Cisco ME 3400E スイッチは IEEE 802.1ag Connectivity Fault Management（CFM）、Ethernet Local Management Interface（E-LMI）、および IEEE 802.3ah イーサネット OAM ディスカバリ、リンク モニタリング、リモート障害検知、およびリモート ループバックをサポートします。また、CFM の IP Service Level Agreement（SLA; サービス レベル契約）、および ITU-T Y.1731 障害管理もサポートします。イーサネット OAM マネージャは、CFM、E-LMI、および OAM のうち 2 つのプロトコル間のインターワーキングを制御します。

この章では、CFM、E-LMI、およびイーサネット OAM プロトコルの設定に関する情報について説明します。批准された CFM 802.1ag 標準（ドラフト 8.1）と Cisco IOS のスイッチでサポートされている前回のバージョン（ドラフト 1.0）との違いを定義します。また、このリリースでの CFM ITU-TY.1731 障害管理サポートの設定に関する情報について説明します。

イーサネット OAM、CFM、E-LMI、および Y.1731 のコマンドおよび設定の詳細については、次の URL の『*Cisco IOS Carrier Ethernet Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/12_2sr/ce_12_2sr_book.html

この章で使用するコマンドの構文の詳細については、このリリースのコマンド リファレンスおよび次の URL にある『*Cisco IOS Carrier Ethernet Command Reference*』を参照してください。
http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_book.html

この章の内容は次のとおりです。

- 「イーサネット CFM の概要」（P.43-2）
- 「イーサネット CFM の設定」（P.43-7）
- 「Y.1731 障害管理の設定」（P.43-24）
- 「イーサネット CFM 情報の管理および表示」（P.43-29）
- 「イーサネット OAM プロトコルの概要」（P.43-31）
- 「イーサネット OAM のセット アップおよび設定」（P.43-32）
- 「イーサネット OAM プロトコル情報の表示」（P.43-41）
- 「イーサネット ループバックのイネーブル化」（P.43-42）
- 「E-LMI の概要」（P.43-46）
- 「E-LMI の設定」（P.43-47）
- 「E-LMI および OAM マネージャの情報の表示」（P.43-53）
- 「イーサネット CFM とイーサネット OAM の相互作用」（P.43-54）

イーサネット CFM の概要

イーサネット CFM は、革新的な接続モニタリング、障害確認、および障害分離を含む、エンドツーエンド、サービスインスタンス単位（VLAN 単位）、およびイーサネット レイヤの OAM プロトコルです。エンドツーエンドは、Provider Edge から Provider Edge（PE-to-PE）デバイス、または Customer Edge から Customer Edge（CE-to-CE）デバイスのいずれでも可能です。IEEE 802.1ag により指定されているように、イーサネット CFM は、イーサネット ネットワークのレイヤ 2 ping、レイヤ 2 traceroute、およびエンドツーエンド接続確認の標準です。

ここでは、イーサネット CFM に関する次の概念について説明します。

- 「CFM ドメイン」（P.43-2）
- 「メンテナンス アソシエーションとメンテナンス ポイント」（P.43-3）
- 「CFM メッセージ」（P.43-5）
- 「クロスチェック機能およびスタティック リモート MEP」（P.43-5）
- 「SNMP トラップと障害アラーム」（P.43-6）
- 「設定エラー リスト」（P.43-6）
- 「CFM バージョンの相互運用性」（P.43-6）
- 「CFM の IP SLAs サポート」（P.43-7）

CFM ドメイン

CFM のメンテナンス ドメインは、ネットワーク上の管理スペースで、単一のエンティティによって所有および操作され、ドメインの内部にある一連のポートにより定義されますが、その境界上に存在します。一意のメンテナンス レベル（0 ～ 7）を割り当てて、ドメイン間の階層関係を定義します。ドメインが大きくなるほど、レベルが高くなります。たとえば図 43-1 に示すように、サービス プロバイダーのドメインはオペレータのドメインよりも大きくなり、オペレータ ドメインのメンテナンス レベルが 3 または 4 の場合でも、メンテナンス レベルは 6 となる場合があります。

図 43-2 に示すように、許可されていない複数のエンティティによる管理が必要となるため、ドメインを交差または重複できません。ドメインを接触またはネスト（外側のドメインがネストされたドメインよりも高いメンテナンス レベルである場合）することはできます。ネスティング ドメインは、サービス プロバイダーがイーサネット サービスの提供に関して、1 つまたは複数のオペレータと契約している場合に便利です。各オペレータには、独自のメンテナンス ドメインがあり、サービス プロバイダー ドメインはオペレータ ドメインの上位集合となります。ネスティング ドメインのメンテナンス レベルは、管理組織間で伝達される必要があります。CFM は、ドメイン単位で、メッセージの交換および操作の実行を行います。

図 43-1　CFM メンテナンス ドメイン

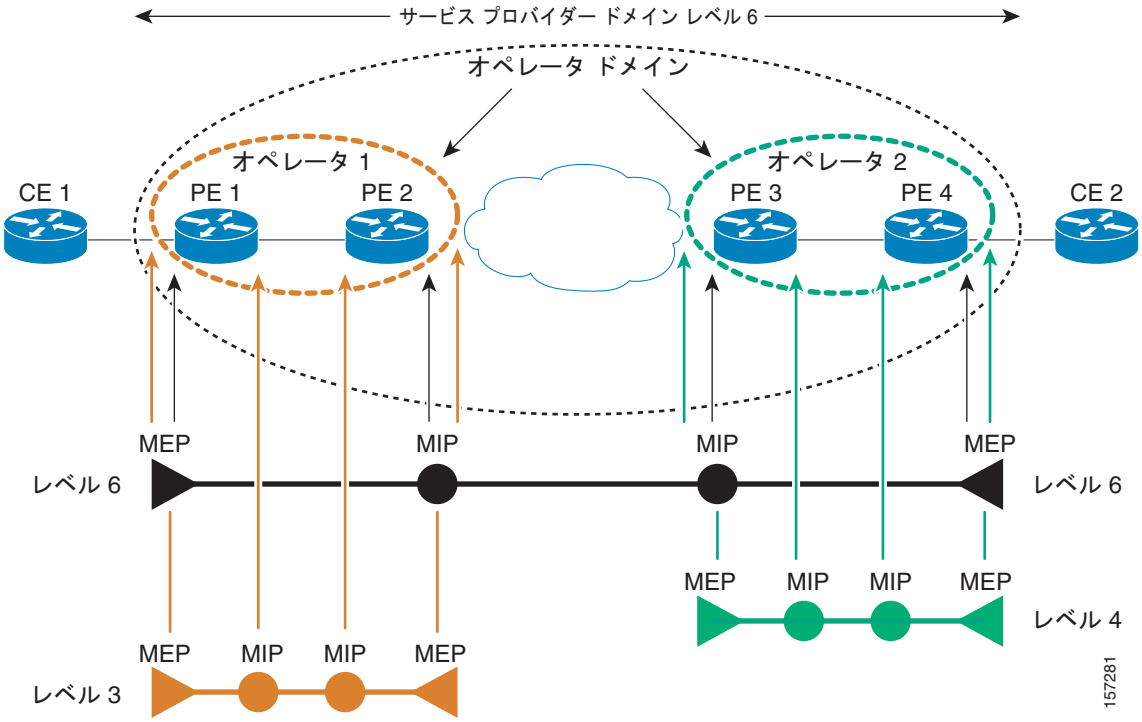
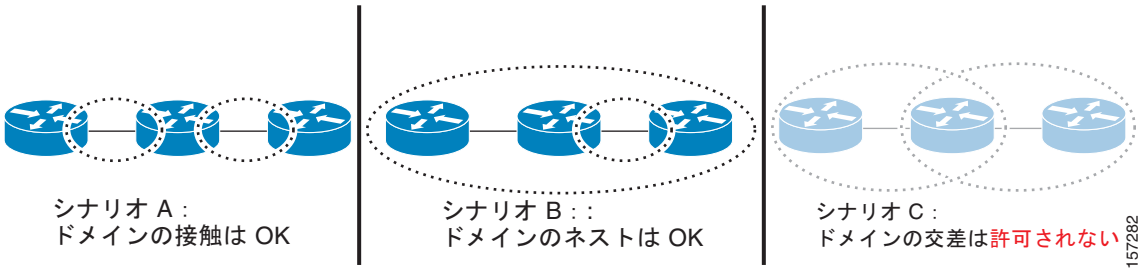


図 43-2　許可されるドメイン関係



メンテナンス アソシエーションとメンテナンス ポイント

Maintenance Association（MA; メンテナンス アソシエーション）により、メンテナンス ドメイン内で一意に識別できるサービスが識別されます。CFM プロトコルは、メンテナンス アソシエーション内で動作します。メンテナンス ポイントとは、メンテナンス ドメイン内で CFM に参加するインターフェイス上の境界点です。メンテナンス ポイントでは、下位レベルのフレームをすべて廃棄して、上位レベルのフレームをすべて転送します。メンテナンス ポイントは 2 種類あります。

- Maintenance End Point（MEP）は、ドメイン エッジにあるポイントで、境界を定義して、CFM メッセージをこれらの境界内に制限します。*外側向き* MEP または*ダウン* MEP は（ポートに接続された）ワイヤ側を介して通信します。*内側向き* MEP または*アップ* MEP はワイヤ側ではなく、リレー機能側を介して通信します。

（注）　CFM ドラフト 1 では、内側向き MEP および外側向き MEP について説明しています。CFM ドラフト 8.1 ではそれぞれ、アップ MEP およびダウン MEP について説明しています。このマニュアルでは、説明に CFM 8.1 の用語を使用しています。

CFM ドラフト 1 は、ポート単位または VLAN 単位でアップ MEP だけをサポートしていました。CFM 802.1ag は、ポート MEP だけではなく、VLAN 単位でアップ MEP およびダウン MEP をサポートしています。これらは、VLAN に関連付けられていないタグなしダウン MEP です。ポート MEP は 1 つのホップを保護するよう設定されており、CFM を介してリンク状態を監視します。ポート MEP が指定した間隔で、そのピア（スタティック リモート MEP）からの cc メッセージを受信していない場合、ポートは稼動ダウン ステートになります。その場合、CFM および OAM パケットだけが通過し、その他のデータと制御パケットは廃棄されます。

- アップ MEP では、リレー機能により CFM フレームを送受信します。ワイヤ側から送信され、レベルが自身のレベル以下であるすべての CFM フレームが廃棄されますが、ダウン MEP に向かうトラフィックは廃棄されません。リレー側からの CFM フレームの場合、レベルが自身のレベルと同じフレームは処理され、下位レベルのフレームは廃棄されます。MEP では、リレー側またはワイヤ側のいずれから受信したかにかかわらず、上位レベルのすべての CFM フレームを透過的に転送します。MEP が設定されているポートが STP でブロックされても、MEP はリレー機能を使用して CFM メッセージを送受信できます。CFM は、プロバイダー メンテナンス レベル（UPE ツー UPE）で稼動し、特にアップ MEP と User Network Interface（UNI; ユーザ ネットワーク インターフェイス）で連携します。

（注）　CFM および OAM マネージャとの関係における UNI は、UNI のポート タイプとは異なります。CFM UNI は、UNI、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）または Network Node Interface（NNI; ネットワーク ノード インターフェイス）のいずれのポート タイプにも設定できます。スイッチにより、すべての着信 CFM メッセージは 1 秒当たり 500 フレームの固定速度でレート制限されます。CFM ドラフト 1 では、コントロール プレーンのセキュリティ機能により、着信 CFM メッセージが UNI ポート タイプおよび ENI ポート タイプでだけレート制限されています。

- ダウン MEP は、MEP が設定されているポートに接続されたワイヤを介して CFM フレームを送受信します。MEP は、リレー側から送信され、レベルが自身のレベル以下であるすべての CFM フレームを廃棄します。ワイヤ側からの CFM フレームの場合、レベルが自身のレベルと同じ CFM フレームはすべて処理され、下位レベルの CFM フレームは廃棄されます。ただし、他の下位レベル ダウン MEP に向かうトラフィックは廃棄されません。MEP では、リレー側またはワイヤ側のいずれから受信したかにかかわらず、上位レベルのすべての CFM フレームを透過的に転送します。

- Maintenance Intermediate Point（MIP）は境界ではなくドメインの内部にあり、traceroute およびループバック メッセージにトリガーされた場合に限り、CFM に応答します。MIP は、MEP および別の MIP から受信した CFM フレームを転送し、リレー側またはワイヤ側のいずれから受信したかにかかわらず、（MIP フィルタリングがイネーブルになっていない限り）下位レベルの CFM フレームをすべて廃棄し、上位レベルおよび下位レベルの CFM フレームをすべて転送します。MIP フィルタリングがイネーブルになっている場合、MIP により CFM フレームは下位レベルで廃棄されます。MIP はまた Continuity Check Message（CCM; CC メッセージ）をカタログし、転送しますが、それらには応答しません。

  CFM の初版では、MIP フィルタリングは常にイネーブルになっていました。ドラフト 8.1 では、MIP フィルタリングはデフォルトでディセーブルになっていますが、イネーブルまたはディセーブルに設定できます。MIP フィルタリングがディセーブルになっている場合、すべての CFM フレームが転送されます。

MIP を手動で設定するか、MIP を自動作成するようスイッチを設定できます。MIP のない MEP を設定できます。設定に矛盾がある場合、自動作成された MIP よりも手動作成された MIP が優先されます。

MEP が設定されたポートが Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）でブロックされている場合、MIP はワイヤ側およびリレー側両方からの CFM メッセージを受信でき、それに応答する場合がありますが、CFM メッセージは転送できません。この点が CFM ドラフト 1 とは異なります。ドラフト 1 では STP でブロックされたポートでは CFM メッセージの送受信はできません。

CFM メッセージ

CFM は、EtherType または（マルチキャスト メッセージの場合は）MAC アドレスにより区別される標準のイーサネット フレームを使用します。すべての CFM メッセージは、メンテナンス ドメインおよび Service-Provider VLAN（S-VLAN）に限定されます。サポート対象の CFM メッセージは、次のとおりです。

- Continuity Check（CC）メッセージ : MEP 間で定期的に交換されるマルチキャスト ハートビート メッセージで、これにより、MEP はドメイン内の他の MEP を検出でき、MIP は MEP を検出できます。CC メッセージは、ドメインまたは VLAN に設定されます。CCM をイネーブルにするには **continuity-check** イーサネット サービス コンフィギュレーション コマンドを入力します。

  スイッチのデフォルト Continuity Check Message（CCM）間隔は 10 秒です。**continuity-check interval** イーサネット サービス モード コマンドを入力して、この間隔を 100 ミリ秒、1 秒、1 分、または 10 分に設定できます。CCM の速度が速くなると CPU により負荷が掛かるため、100 ミリ秒間隔で多数の MEP を稼動する設定はお勧めしません。

- ループバック メッセージ : 管理者要求で MEP により伝送されるユニキャスト またはマルチキャスト フレームで、宛先が到達可能かどうかを示して、特定のメンテナンス ポイントへの接続を確認します。ループバック メッセージは、Internet Control Message Protocol（ICMP）ping メッセージと同様です。**ping ethernet** 特権 EXEC コマンドを参照してください。

- Traceroute メッセージ : 管理者要求で MEP により伝送されるマルチキャスト フレームで、宛先 MEP へのパス（ホップバイホップ）を追跡します。Traceroute メッセージは、概念上 UDP traceroute メッセージと同様です。**traceroute ethernet** 特権 EXEC コマンドを参照してください。

クロスチェック機能およびスタティック リモート MEP

クロスチェック機能は、ダイナミックに設定された MEP （クロスチェック メッセージにより）とサービスに予測される MEP（設定により）間でのタイマー駆動型のポストプロビジョニング サービス確認です。この機能では、マルチポイント サービスのすべてのエンドポイントが動作可能であることを確認します。クロスチェック機能は 1 回だけ実行され、CLI（コマンドライン インターフェイス）から開始されます。

CFM 802.1ag はまた、スタティック リモート MEP またはスタティック RMEP チェックをサポートします。1 回だけ実行されるクロスチェック機能とは異なり、設定されたスタティック RMEP は実行を連続してチェックします。スタティック RMEP チェックを設定するには、**continuity-check static rmep** イーサネット CFM サービス モード コマンドを入力します。

SNMP トラップと障害アラーム

MEP により、CC トラップとクロスチェック トラップの 2 種類の SNMP トラップが生成されます。サポート対象の CC トラップは、MEP アップ、MEP ダウン、クロスコネクト（サービス ID が VLAN に一致ない）、ループ、および設定エラーです。クロスチェック トラップは、サービス アップ、MEP 不明（予測された MEP がダウン）、および不明な MEP です。

障害アラームは、CFM で障害が検出された場合に、システム管理者に注意を促すための非送信請求通知です。CFM ドラフト 1 では、障害アラームは障害が検出されると即座に送信されました。CFM 802.1ag では、SNMP トラップまたは syslog メッセージをトリガーするアラームのプライオリティ レベルを設定できます。また、障害アラーム送信までの遅延時間およびアラームのリセットまでの時間も設定できます。

設定エラー リスト

CFM 802.1ag の CFM 設定エラーは、MEP 設定中に検出された設定ミスまたは 余分なコンフィギュレーション コマンドの場合があります。これらは、メンテナンス アソシエーションが重複した結果発生する場合があります。たとえば、インターフェイスで VLAN リストと MEP とのメンテナンス アソシエーションを作成すると、MEP が設定されていない同じ VLAN に関連付けられた他のメンテナンス アソシエーションが上位に存在する場合、リーク エラーが発生するおそれがあります。説明たけを目的とした設定エラー リストは、**show ethernet cfm errors configuration** 特権 EXEC コマンドを入力して表示できます。

CFM バージョンの相互運用性

Cisco CFM ドラフト 1 から IEEE 標準化 802.1ag CFM にネットワークをアップグレードするお客様は、同時にすべての機器をアップグレードするとは限りません。これにより Cisco CFM ドラフト 1 および IEEE 標準化 CFM デバイスがネットワークに混在する可能性があります。CFM エリアは、Cisco CFM ドラフト 1 ソフトウェアを実行しているネットワーク上のリージョンです。内部エリア ブリッジはすべて CFM ドラフト 1 を実行するシスコ製デバイスで、外部エリア ブリッジは IEEE 標準化 802.1ag CFM を実行するデバイス（シスコまたはサードパーティ製のデバイス）です。

これらのエリアのエッジにあるデバイスで、メッセージ変換を行います。（CFM メッセージがデバイスのあるポートで終端するような）異なるエリアにまたがらないメンテナンス ドメインを変換する必要はありません。そのポートは、受信時と同じメッセージ形式で応答できるためです。ただし、2 つのエリアをまたぐメンテナンス ドメインの場合は、デバイスで CFM メッセージを適切に変換してから、他のエリアに送信する必要があります。

CFM エリアのネットワークを設計する場合は、次の注意事項に従ってください。

- できる限り、CFM バージョンが同じデバイスのグループにします。
- CFM クラスタ間の境界の数と変換に必要なデバイスの数を最小限に抑えます。
- 1 つのセグメントに異なるバージョンの CFM を混在させてはいけません。

ネットワークで両方のバージョンの CFM が使用される場合、**ethernet cfm version cisco** インターフェイス コンフィギュレーション コマンドを入力して、ドラフト 1 デバイスに接続されている CFM 802.1ag ポートでの変換をイネーブルにできます。

（注）　CFM ドラフト 1 を実行しており、CFM 802.1ag をサポートするソフトウェア バージョンにアップグレードする場合、スイッチにより ドラフト 1 の設定が自動的に標準に転送されます。

CFM の IP SLAs サポート

スイッチでは、イーサネット レイヤ ネットワーク パフォーマンス メトリックを収集できる機能を備えた IP Service Level Agreement（SLA; サービス レベル契約）が付いた CFM がサポートされます。IP SLA CFM 動作に使用できる統計測定値として、ラウンドトリップ時間、ジッタ（インターパケット遅延差異）、およびパケット損失があります。複数の IP SLAs 動作をスケジューリングし、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップ通知および syslog メッセージを使用して、しきい値超過の予防のため監視できます。

IP SLA の詳細については、第 41 章「Cisco IOS IP SLA 動作の設定」を参照してください。

IP SLA と CFM を統合し、CFM MEP 間でイーサネット データ フレームを送受信してイーサネット レイヤ統計測定値を収集します。発信元 MEP および宛先 MEP 間のパフォーマンスが測定されます。IP レイヤだけのパフォーマンス メトリックを実現するその他の IP SLA 動作とは異なり、CFM のある IP SLA はレイヤ 2 のパフォーマンス メトリックを実現します。

個々のイーサネット ping またはジッタ動作は手動で設定できます。ある指定のメンテナンス ドメインおよび VLAN のすべての MEP について CFM データベースを照会する、IP SLA 自動イーサネット動作を設定することもできます。この動作により、検出された MEP に基づいて自動的に個々のイーサネット ping またはジッタ動作が作成されます。

IP SLA はシスコの独自機能であるため、CFM ドラフト 1 と CFM 802.1ag の間の相互運用性は、スイッチにより自動的に処理されます。

CFM のある IP SLA 動作の詳細については、次の URL にある *IP SLA for Metro-Ethernet* フィーチャ モジュールを参照してください。

http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a00807d72f5.html

イーサネット CFM の設定

イーサネット CFM の設定には、CFM ドメインの設定が必要です。クロスチェック、リモート MEP、ポート MEP、SNMP トラップ、および障害アラームなどその他の CFM 機能を任意に設定し、イネーブルにできます。CFM ドラフト 1 と異なるコンフィギュレーション コマンドおよび手順がある点に注意してください。

- 「イーサネット CFM のデフォルト設定」（P.43-8）
- 「イーサネット CFM 設定時の注意事項」（P.43-8）
- 「CFM ドメインの設定」（P.43-9）
- 「イーサネット CFM クロスチェックの設定」（P.43-12）
- 「スタティック リモート MEP の設定」（P.43-13）
- 「ポート MEP の設定」（P.43-14）
- 「SNMP トラップの設定」（P.43-15）
- 「障害アラームの設定」（P.43-16）
- 「IP SLA CFM 動作の設定」（P.43-17）

イーサネット CFM のデフォルト設定

CFM はグローバルにディセーブルです。

CFM がグローバルにイネーブルの場合、CFM はすべてのインターフェイスでイネーブルになっています。

ポートは、フロー ポイント（MIP/MEP）、トランスペアレント ポート、またはディセーブル（CFM ディセーブル）として設定できます。デフォルトでは、ポートは MEP、MIP、またはディセーブルとして設定されるまでは、トランスペアレント ポートです。

MEP または MIP は設定されていません。

MEP サービスを設定する場合、方向を設定しないと、デフォルト値はアップ（内側向き）になります。

イーサネット CFM 設定時の注意事項

- CFM はルーテッド ポートまたはレイヤ 3 EtherChannel ではサポートされておらず、設定できません。
- CFM は EtherChannel ポート チャネルでサポートされています。EtherChannel ポート チャネルを MEP または MIP として設定できます。ただし、CFM は EtherChannel に属する個々のポートではサポートされておらず、CFM ポートを EtherChannel グループには追加できません。
- ポート MEP は、レイヤ 2 EtherChannel または EtherChannel に属するポートではサポートされていません。
- CFM は、VLAN インターフェイスでは設定できません。
- CFM はトランク ポート、アクセス ポート、および 802.1Q トンネル ポートでサポートされていますが、次の例外があります。
  - MEP として設定されているトランク ポートは、許可 VLAN に属している必要があります。
  - MEP として設定されているアクセス ポートは、ネイティブ VLAN に属している必要があります。
- CFM および VLAN の変換を同時にスイッチで設定できます。
- CFM は、プライベート VLAN ポートではサポートされません。
- REP ポートまたは FlexLink ポートもサービス（VLAN）MEP または MIP として設定できますが、ポート MEP としては設定できません。
- CFM は STP を稼動するポートでサポートされています。
- インターフェイス上の任意のサービス（VLAN）MEP より下位にあるポート MEP を設定する必要があります。
- 802.1Q（QinQ）トンネル ポートは CFM アップ MEP またはポート MEP として設定できます。ME 3400E スイッチ上で、選ばれた QinQ ポートで MEP を設定することもできます。
- QinQ ポートはダウン MEP または MIP としては設定できません。ポートを MIP として設定できますが、traceroute ではアクティブでない、または見えません。QinQ インターフェイスで受信されたポート MEP フレームはトンネリングされず、ローカルに処理されます。
- QinQ ポートで、入力ドラフト 1 トラフィックは、CFM バージョンを変換したり、考慮せずにトンネリングされます。
- ネイティブ VLAN を S-VLAN または C-VLAN として使用しても、トンネル モードは設定できません。
- QinQ ポート上のポート MEP の場合は、**vlan dot1q tag native** グローバル コンフィギュレーション コマンドを入力してネイティブ VLAN フレームでタギングをイネーブルにしないでください。

- 802.1Q トンネル ポートに入るタグ付きまたはタグなし 802.1ag CFM パケットを設定しないでください。
- トランク ポートに入る 2 重タグ 802.1ag CFM パケットを設定しないでください。

CFM ドメインの設定

イーサネット CFM ドメインを設定する、ドメインを VLAN に接続するサービスを設定する、または MEP の役割を果たすポートを設定するには、特権 EXEC モードで次の手順を実行します。また、任意のコマンドを入力して Continuity Check など他のパラメータを設定できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm ieee**	CFM バージョンを IEEE 802.1ag として設定します。
ステップ 3	**ethernet cfm global**	スイッチ上でイーサネット CFM をグローバルにイネーブルにします。
ステップ 4	**ethernet cfm traceroute cache** [**size** *entries* | **hold-time** *minutes*]	（任意）CFM traceroute キャッシュを設定します。最大キャッシュ サイズまたはホールド タイムを設定できます。 • （任意）**size** には、キャッシュ サイズをエントリ ライン数で入力します。指定できる範囲は 1 ～ 4095 で、デフォルトは 100 ラインです。 • （任意）**hold-time** には、最大キャッシュ ホールド タイム（分）を入力します。指定できる範囲は 1 ～ 65535 で、デフォルトは 100 分です。
ステップ 5	**ethernet cfm mip auto-create level** *level-id* **vlan** *vlan-id*	（任意）指定のレベルで特定のメンテナンス アソシエーションと関連付けられていない VLAN IDS の MIP を自動作成するようスイッチを設定します。指定できるレベルの範囲は 0 ～ 7 です。 **（注）** MIP が監視する必要がある VLAN についてだけ MIP 自動作成を設定します。すべての VLAN を設定すると、CPU とメモリを大量に消費します。
ステップ 6	**ethernet cfm mip filter**	（任意）MIP フィルタリングをイネーブルにします。下位レベルのすべての CFM フレームが廃棄されることを意味します。デフォルトはディセーブルです。
ステップ 7	**ethernet cfm domain** *domain-name* **level** *level-id*	CFM ドメインを定義して、ドメイン レベルを設定し、ドメインで ethernet-cfm コンフィギュレーション モードを開始します。メンテナンス レベルに指定できる数の範囲は 0 ～ 7 です。
ステップ 8	**id** {*mac-address domain_number* | **dns** *name* | **null**}	（任意）メンテナンス ドメイン ID を割り当てます。 • *mac-address domain_number* : MAC アドレスとドメイン番号を入力します。番号は、0 ～ 65535 です。 • **dns** *name* : DNS name ストリングを入力します。名前は最大 43 文字です。 • **null** : ドメイン名は割り当てません。

	コマンド	目的
ステップ 9	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	ドメインに関連付けるカスタマー サービス Maintenance Association（MA; メンテナンス アソシエーション）名、番号、または VPN ID、VLAN ID、またはポート MEP を定義し、ethernet-cfm-service コンフィギュレーション モードを開始します。 • *ma-name*：MAID を識別する 100 文字以下の文字列 • *ma-number*：0 ～ 65535 の値 • *vpn-id vpn*：*ma-name* として VPN ID を入力します。 • **vlan** *vlan-id*：指定できる VLAN の範囲は 1 ～ 4094 です。同じレベルの複数のドメインに同じ VLAN ID は使用できません。 • （任意）**direction down**：サービスの方向をダウンに指定します。 • **port**：VLAN と関連付けられていないタグなしダウン MEP である、ポート MEP を設定します。
ステップ 10	**continuity-check**	CC メッセージの送受信をイネーブルにします。
ステップ 11	**continuity-check interval** *value*	（任意）CC メッセージを送信する間隔を設定します。指定できる値は 100 ミリ秒、1 秒、10 秒、1 分、10 分です。デフォルトは 10 秒です。 **（注）** CCM の速度が速くなると CPU により負荷が掛かるため、100 ミリ秒間隔で多数の MEP を稼動する設定はお勧めしません。
ステップ 12	**continuity-check loss-threshold** *threshold-value*	（任意）MEP がダウンであると宣言する前に、不在着信にする CC メッセージの数を設定します。指定できる範囲は 2 ～ 255 です。デフォルトは 3 です。
ステップ 13	**maximum meps** *value*	（任意）ネットワーク上で許可される MEP の最大数を設定します。指定できる範囲は 1 ～ 65535 です。デフォルトは 100 です。
ステップ 14	**sender-id** {**chassis** | **none**}	（任意）近接デバイスのタイプ、長さ、および値を含むアトリビュートである、送信者の ID TLV を指定します。 • **chassis**：シャーシ ID（ホスト名）を送信します。 • **none**：送信者 ID に情報を指定しません。
ステップ 15	**mip auto-create** [**lower-mep-only** | **none**]	（任意）サービスの MIP の自動作成を設定します。 • **lower-mep-only**：次に低いアクティブ レベルにある別のドメインにサービスの MEP がある場合だけ MIP を作成します。 • **none** ：MIP は自動作成されません。
ステップ 16	**exit**	ethernet-cfm コンフィギュレーション モードに戻ります。
ステップ 17	**mip auto-create** [**lower-mep-only**]	（任意）ドメインの MIP の自動作成を設定します。 • **lower-mep-only**：次に低いアクティブ レベルにある別のドメインにサービスの MEP がある場合だけ MIP を作成します。

	コマンド	目的
ステップ 18	**mep archive-hold-time** *minutes*	（任意）不明のメンテナンス エンド ポイントからのデータが、消去されるまで保有される時間（分）を設定します。指定できる範囲は 1 ～ 65535 で、デフォルトは 100 分です。
ステップ 19	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 20	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	**switchport mode trunk**	（任意）ポートをトランク ポートとして設定します。
ステップ 22	**ethernet cfm mip level** *level-id*	（任意）インターフェイスのカスタマー レベルまたはサービス プロバイダー レベルの MIP を設定します。指定できる MIP レベルの範囲は 0 ～ 7 です。 （注）　**ethernet cfm mip auto-create** グローバル コンフィギュレーション コマンド、または **mip auto-create** ethernet-cfm コンフィギュレーション モードあるいは ethernet-cfm-srv コンフィギュレーション モードを開始している場合は、この手順は不要です。
ステップ 23	**ethernet cfm mep domain** *domain-name* **mpid** *identifier* {**vlan** *vlan-id* | **port**}	ドメインのメンテナンス エンド ポイントを設定し、ethernet cfm mep モードを開始します。 • **domain** *domain-name*：作成したドメインの名前を指定します。 • **mpid** *identifier*：メンテナンス エンド ポイント ID を入力します。ID は VLAN（サービス インスタンス）ごとに一意でなければなりません。指定できる範囲は 1 ～ 8191 です。 • **vlan** *vlan-id*：サービス プロバイダーの VLAN ID を単一の VLAN-ID（1 ～ 4094）、ハイフンで区切られた VLAN-ID の範囲、またはカンマで区切られた一連の VLAN ID として入力します。 • **port**：ポート MEP を設定します。
ステップ 24	**coS** *value*	（任意）メッセージとともに送信する Class of Service（CoS; サービス クラス）の値を指定します。指定できる範囲は 0 ～ 7 です。
ステップ 25	**end**	特権 EXEC モードに戻ります。
ステップ 26	**show ethernet cfm maintenance-points** {**local** | **remote**}	設定を確認します。
ステップ 27	**show ethernet cfm errors [configuration]**	（任意）設定エラー リストを表示します。
ステップ 28	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定を削除する場合、またはデフォルト設定に戻すには、コマンドの **no** 形式を使用します。

これは、基本 CFM 設定の例です。

```
Switch(config)# ethernet cfm ieee
Switch(config)# ethernet cfm global
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service test vlan 5
```

```
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ethernet cfm mep domain abc mpid 222 vlan 5
Switch(config-if-ecfm-mep)# exit
```

イーサネット CFM クロスチェックの設定

イーサネット CFM クロスチェックを設定するには、特権 EXEC モードで次の手順を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm mep crosscheck start-delay** *delay*	クロスチェックが開始される前に、デバイスでリモート MEP がアップするのを待機する時間（秒）を設定します。指定できる範囲は 1 ～ 65535 秒で、デフォルトは 30 秒です。
ステップ 3	**ethernet cfm domain** *domain-name* **level** *level-id*	CFM ドメインを定義して、ドメイン レベルを設定し、ドメインで ethernet-cfm コンフィギュレーション モードを開始します。メンテナンス レベルに指定できる数の範囲は 0 ～ 7 です。
ステップ 4	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id*}	ドメインに関連付けるカスタマー サービス メンテナンス アソシエーション名、番号、または VPN ID、および VLAN ID を定義し、ethernet-cfm-service コンフィギュレーション モードを開始します。 • *ma-name* : MAID を識別する 100 文字以下の文字列 • *ma-number* : 0 ～ 65535 の値 • *vpn-id vpn* : *ma-name* として VPN ID を入力します。 • **vlan** *vlan-id* : 指定できる VLAN の範囲は 1 ～ 4094 です。同じレベルの複数のドメインに同じ VLAN ID は使用できません。
ステップ 5	**mep mpid** *identifier*	ドメインおよびサービスの MEP メンテナンス エンド ポイント ID を定義します。指定できる範囲は 1 ～ 8191 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**ethernet cfm mep crosscheck** {**enable** | **disable**} **domain** *domain-name* {**vlan** {*vlan-id* | **any**} | **port**}	ドメインの 1 つまたは複数の VLAN またはポート MEP の CFM クロスチェックをイネーブルまたはディセーブルにします。 • **domain** *domain-name* : 作成したドメインの名前を指定します。 • **vlan** {*vlan-id* | **any**} : サービス プロバイダーの VLAN ID を単一の VLAN ID（1 ～ 4094）、ハイフンで区切られた VLAN ID の範囲、またはカンマで区切られた一連の VLAN ID として入力します。任意の VLAN には **any** を入力します。 • **port** : ポート MEP を識別します。

	コマンド	目的
ステップ 8	**show ethernet cfm maintenance-points remote crosscheck**	設定を確認します。
ステップ 9	**show ethernet cfm errors** [**configuration**]	CFM クロスチェックをイネーブルにし、クロスチェック動作の結果を表示してからこのコマンドを入力します。設定エラー リストを表示するにはキーワード **configuration** を入力します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定を削除する場合、またはデフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

スタティック リモート MEP の設定

イーサネット CFM スタティック リモート MEP を設定するには、特権 EXEC モードで次の手順を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm domain** *domain-name* **level** *level-id*	CFM ドメインを定義して、ドメイン レベルを設定し、ドメインで ethernet-cfm コンフィギュレーション モードを開始します。メンテナンス レベルに指定できる数の範囲は 0 ～ 7 です。
ステップ 3	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	ドメインに関連付けるカスタマー サービス メンテナンス アソシエーション名または番号、あるいは VPN ID、および VLAN ID、またはピアを定義し、ethernet-cfm-service コンフィギュレーション モードを開始します。 • *ma-name*：MAID を識別する 100 文字以下の文字列 • *ma-number*：0 ～ 65535 の値 • *vpn-id*：VPN ID を *ma-name* として入力します。 • **vlan** *vlan-id*：指定できる VLAN の範囲は 1 ～ 4094 です。同じレベルの複数のドメインに同じ VLAN ID は使用できません。 • （任意）**direction down**：サービスの方向をダウンに指定します。 • **port**：VLAN と関連付けられていないタグなしダウン MEP である、ポート MEP を設定します。
ステップ 4	**continuity-check**	CC メッセージの送受信をイネーブルにします。
ステップ 5	**mep mpid** *identifier*	スタティック リモート メンテナンス エンド ポイント ID を定義します。指定できる範囲は 1 ～ 8191 です。
ステップ 6	**continuity-check static rmep**	MEP リストで設定されているリモート MEP からの着信 CCM のチェックをイネーブルにします。
ステップ 7	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	**show ethernet cfm maintenance-points remote static**	設定を確認します。
ステップ 9	**show ethernet cfm errors** [**configuration**]	CFM クロスチェックをイネーブルにし、クロスチェック動作の結果を表示してからこのコマンドを入力します。設定エラー リストを表示するにはキーワード **configuration** を入力します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定を削除する場合、またはデフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

ポート MEP の設定

ポート MEP は VLAN に関連付けられていないダウン MEP で、タグなしフレームを使用して CFM メッセージを伝達します。ポート MEP を 2 つの接続されたインターフェイス上で設定します。ポート MEP は常にネイティブ VLAN MEP より下位レベルのドメインで設定されます。

イーサネット CFM ポート MEP を設定するには、特権 EXEC モードで次の手順を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm domain** *domain-name* **level** *level-id*	CFM ドメインを定義して、ドメイン レベルを設定し、ドメインで ethernet-cfm コンフィギュレーション モードを開始します。メンテナンス レベルに指定できる数の範囲は 0 ～ 7 です。
ステップ 3	**service** {*ma-name* | *ma-number* | *vpn-id*} **port**	ドメインに関連付けるカスタマー サービス メンテナンス アソシエーション名、番号、または VPN ID を定義し、ポート MEP を定義して、ethernet-cfm-service コンフィギュレーション モードを開始します。 • *ma-name* : MAID を識別する 100 文字以下の文字列 • *ma-number* : 0 ～ 65535 の値 • *vpn-id vpn* : *ma-name* として VPN ID を入力します。
ステップ 4	**mep mpid** *identifier*	ドメインおよびサービスのスタティック リモート メンテナンス エンド ポイント ID を定義します。指定できる範囲は 1 ～ 8191 です。
ステップ 5	**continuity-check**	CC メッセージの送受信をイネーブルにします。
ステップ 6	**continuity-check interval** *value*	（任意）CC メッセージを送信する間隔を設定します。指定できる値は 100 ミリ秒、1 秒、10 秒、1 分、10 分です。デフォルトは 10 秒です。 **（注）** CCM の速度が速くなると CPU により負荷が掛かるため、100 ミリ秒間隔で多数の MEP を稼動する設定はお勧めしません。
ステップ 7	**continuity-check loss-threshold** *threshold-value*	（任意）MEP がダウンであると宣言する前に、不在着信にする CC メッセージの数を設定します。指定できる範囲は 2 ～ 255 です。デフォルトは 3 です。

	コマンド	目的
ステップ 8	**continuity-check static rmep**	MEP リストで設定されているリモート MEP からの着信 CCM のチェックをイネーブルにします。
ステップ 9	**exit**	ethernet-cfm コンフィギュレーション モードに戻ります。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**interface** *interface-id*	ポート MEP インターフェイスを識別し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**ethernet cfm mep domain** *domain-name* **mpid** *identifier* **port**	インターフェイスをドメインのポート MEP として設定します。 • **domain** *domain-name*：作成したドメインの名前を指定します。 • **mpid** *identifier*：メンテナンス エンド ポイント ID を入力します。ID は VLAN（サービス インスタンス）ごとに一意でなければなりません。指定できる範囲は 1 ～ 8191 です。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show ethernet cfm maintenance-points remote static**	設定を確認します。
ステップ 15	**show ethernet cfm errors** [**configuration**]	CFM クロスチェックをイネーブルにし、クロスチェック動作の結果を表示してからこのコマンドを入力します。設定エラー リストを表示するにはキーワード **configuration** を入力します。
ステップ 16	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定を削除する場合、またはデフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

これはポート MEP 設定のサンプルです。

```
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service PORTMEP port
Switch(config-ecfm-srv)# mep mpid 222
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# continuity-check static rmep
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ethernet cfm mep domain abc mpid 111 port
Switch(config-if)# end
```

SNMP トラップの設定

イーサネット CFM のトラップを設定するには、特権 EXEC モードで次の手順を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]	（任意）イーサネット CFM cc トラップをイネーブルにします。

	コマンド	目的
ステップ 3	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown**] [**mep-missing**] [**service-up**]	（任意）イーサネット CFM クロスチェック トラップをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定を削除する場合、またはデフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

障害アラームの設定

イーサネット CFM 障害アラームを設定するには、特権 EXEC モードで次の手順を行います。別のグローバル コンフィギュレーション モードまたはイーサネット CFM インターフェイス MEP モードのいずれかで障害アラームを設定できる点に注意してください。矛盾が発生した場合は、インターフェイス MEP モード設定が優先されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm alarm notification** {**all** | **error-xcon** | **mac-remote-error-xcon** | **none** | **remote-error-xcon** | **xcon**}	指定の障害について、イーサネット CFM 障害アラーム通知をグローバルにイネーブルにします。 • **all**：すべての障害を報告します。 • **error-xcon**：エラーおよび接続障害だけ報告します。 • **mac-remote-error-xcon**：MAC アドレス、リモート、エラー、接続に関する障害だけ報告します。 • **none**：障害を報告しません。 • **remote-error-xcon**：リモート、エラー、接続に関する障害だけ報告します。 • **xcon**：接続障害だけ報告します。
ステップ 3	**ethernet cfm alarm delay** *value*	（任意）CFM 障害アラームが送信されるまでの遅延時間を設定します。指定できる範囲は 2500 ～ 10000 ミリ秒です。デフォルトは 2500 ミリ秒です。
ステップ 4	**ethernet cfm alarm reset** *value*	（任意）CFM 障害アラームがリセットされるまでの時間を指定します。指定できる範囲は 2500 ～ 10000 ミリ秒です。デフォルトは 10000 ミリ秒です。
ステップ 5	**ethernet cfm logging alarm ieee**	アラームのシステム ロギング メッセージを生成するようスイッチを設定します。
ステップ 6	**interface** *interface-id*	（任意）設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 7	**ethernet cfm mep domain** *domain-name* **mpid** *identifier* **vlan** *vlan-id*	ドメインのメンテナンス エンド ポイントを設定し、ethernet cfm interface mep モードを開始します。 • **domain** *domain-name*：作成したドメインの名前を指定します。 • **mpid** *identifier*：メンテナンス エンド ポイント ID を入力します。ID は VLAN（サービス インスタンス）ごとに一意でなければなりません。指定できる範囲は 1 ～ 8191 です。 • **vlan** *vlan-id*：サービス プロバイダーの VLAN ID を単一の VLAN-ID（1 ～ 4094）、ハイフンで区切られた VLAN-ID の範囲、またはカンマで区切られた一連の VLAN ID として入力します。
ステップ 8	**ethernet cfm alarm notification** {**all** | **error-xcon** | **mac-remote-error-xcon** | **none** | **remote-error-xcon** | **xcon**}	（任意）インターフェイス上の指定の障害について、イーサネット CFM 障害アラーム通知をイネーブルにします。 **（注）** イーサネット CFM インターフェイス MEP アラーム設定は、グローバル設定より優先されます。
ステップ 9	**ethernet cfm alarm** {**delay** *value* | **reset** *value*}	（任意）アラーム遅延時間またはリセット時間を設定します。 **（注）** イーサネット CFM インターフェイス MEP アラーム設定は、グローバル設定より優先されます。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定を削除する場合、またはデフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

IP SLA CFM 動作の設定

IP SLA イーサネット ping またはジッタ エコー動作を手動で個々に設定したり、エンドポイント ディスカバリで IP SLA イーサネット動作を設定できます。複数のオペレーション スケジューリングを設定することもできます。一方向の遅延統計情報を正確に入手するには、エンドポイント スイッチのクロックを同期させる必要があります。スイッチが同じクロック ソースに同期するよう、Network Time Protocol（NTP; ネットワーク タイム プロトコル）でエンドポイント スイッチを設定できます。

IP SLA イーサネット動作の設定の詳細については、次の URL にある *IP SLA for Metro-Ethernet* フィーチャ モジュールを参照してください。
http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a00807d72f5.html

IP SLA 動作の設定の詳細については、次の URL にある『*Cisco IOS IP SLAs Configuration Guide*』*Release 12.4T* を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA コマンドの詳細については、次の URL にあるコマンド リファレンスを参照してください。
http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a008049739b.html

この章の内容は、次のとおりです。

- 「IP SLA CFM プローブまたはジッタ動作の手動設定」（P.43-18）
- 「エンドポイント ディスカバリによる IP SLA 動作の設定」（P.43-20）

IP SLA CFM プローブまたはジッタ動作の手動設定

IP SLA イーサネット エコー（ping）動作またはジッタ動作を手動設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla** *operation-number*	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	**ethernet echo mpid** *identifier* **domain** *domain-name* **vlan** *vlan-id* または **ethernet jitter mpid** *identifier* **domain** *domain-name* **vlan** *vlan-id* [**interval** *interpacket-interval*] [**num-frames** *number-of frames transmitted*]	IP SLA 動作をエコー（ping）動作またはジッタ動作として設定し、IP SLA イーサネット エコー コンフィギュレーション モードを開始します。 • ping 動作には **echo** を、ジッタ動作には **jitter** を入力します。 • **mpid** *identifier* には、MEP の識別子を入力します。ID は VLAN（サービス インスタンス）ごとに一意でなければなりません。指定できる範囲は 1 ～ 8191 です。 • **domain** *domain-name* には、CFM ドメイン名を入力します。 • **vlan** *vlan-id* に指定できる VLAN 範囲は 1 ～ 4095 です。 • （任意：ジッタの場合だけ）ジッタ パケットの送信の間に **interval** を入力します。 • （任意：ジッタの場合だけ）**num-frames** および送信するフレーム数を入力します。
ステップ 4	**cos** *cos-value*	（任意）動作のサービス値のクラスを設定します。
ステップ 5	**frequency** *seconds*	（任意）IP SLA 動作が繰り返される比率を設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 6	**history** *history-parameter*	（任意）IP SLA 動作の統計履歴情報を収集するパラメータを指定します。
ステップ 7	**owner** *owner-id*	（任意）IP SLA 動作の SNMP オーナーを設定します。
ステップ 8	**request-data-size** *bytes*	（任意）IP SLA 要求パケットのプロトコル データ サイズを指定します。指定できる範囲は、0 から使用中のプロトコルで許可されている最大サイズで、デフォルト値は 66 バイトです。
ステップ 9	**tag** *text*	（任意）IP SLA 動作のユーザ指定の ID を作成します。

	コマンド	目的
ステップ 10	**threshold** *milliseconds*	（任意）ネットワーク モニタリング統計情報を計算する場合は、上位しきい値をミリ秒（ms）で指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 5000 です。
ステップ 11	**timeout** *milliseconds*	（任意）IP SLA 動作がその要求パケットからの応答を待つ時間をミリ秒で指定します。指定できる範囲は 0 ～ 604800000 です。デフォルトは 5000 です。
ステップ 12	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**ip sla schedule** *operation-number* [**ageout** *seconds*] [**life** {**forever** | *seconds*}] [**recurring**] [**start-time** {*hh:mm* {*:ss*} [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]	IP SLA 動作の時間パラメータをスケジューリングします。 • *operation-number*：IP SLA 動作番号を入力します。 • （任意）**ageout** *seconds*：情報をアクティブに収集していない場合に動作をメモリに保存しておく秒数を入力します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒です。 • （任意）**life**：動作を無制限（**forever**）または特定の*秒*数（seconds）実行するかを設定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 • （任意）**recurring**：毎日自動的にスケジューリングするようプローブを設定します。 • （任意）**start-time**：情報収集を開始する動作の時間を入力します。 – 特定の時間に開始するには、時間、分、秒（24 時間式）および日付を入力します。 – 開始時間を選択するまで情報を収集しないように選択するには **pending** を入力します。 – 動作を即座に開始するには **now** を入力します。 – 入力した時間が経過した後に動作を開始するには、**after** *hh:mm:ss* を入力します。
ステップ 14	**end**	特権 EXEC モードに戻ります。
ステップ 15	**show ip sla configuration** [*operation-number*]	設定済み IP SLA 動作を示します。
ステップ 16	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA 動作を削除するには、no **ip sla** *operation-number* グローバル コンフィギュレーション コマンドを入力します。

エンドポイント ディスカバリによる IP SLA 動作の設定

IP SLA を使用してドメインの CFM エンドポイントおよび VLAN ID を自動的に検出するには、特権 EXEC モードで次の手順を実行します。検出されたエンドポイントへの ping 動作またはジッタ動作を設定できます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sla ethernet-monitor** *operation-number*	IP SLA 自動イーサネット動作の設定を開始し、IP SLA イーサネット モニタ コンフィギュレーション モードを開始します。
ステップ 3	**type echo domain** *domain-name* **vlan** *vlan-id* [**exclude-mpids** *mp-ids*] または **type jitter domain** *domain-name* **vlan** *vlan-id* [**exclude-mpids** *mp-ids*] [**interval** *interpacket-interval*] [**num-frames** *number-of frames transmitted*]	自動イーサネット動作をエコー（ping）動作またはジッタ動作として設定し、IP SLA イーサネット エコー コンフィギュレーション モードを開始します。 • ping 操作には **type echo** を、ジッタ操作には **type jitter** を入力します。 • **mpid** *identifier* には、MEP の識別子を入力します。指定できる範囲は 1 ～ 8191 です。 • **domain** *domain-name* には、CFM ドメイン名を入力します。 • **vlan** *vlan-id* に指定できる VLAN 範囲は 1 ～ 4095 です。 • （任意）指定の MEP の識別子を除外するには **exclude-mpids** *mp-ids* を入力します。 • （任意：ジッタの場合だけ）ジッタ パケットの送信の間に **interval** を入力します。 • （任意：ジッタの場合だけ）**num-frames** および送信するフレーム数を入力します。
ステップ 4	**cos** *cos-value*	（任意）動作のサービス値のクラスを設定します。
ステップ 5	**owner** *owner-id*	（任意）IP SLA 動作の SNMP オーナーを設定します。
ステップ 6	**request-data-size** *bytes*	（任意）IP SLA 要求パケットのプロトコル データ サイズを指定します。指定できる範囲は、0 から使用中のプロトコルで許可されている最大サイズで、デフォルト値は 66 バイトです。
ステップ 7	**tag** *text*	（任意）IP SLA 動作のユーザ指定の ID を作成します。
ステップ 8	**threshold** *milliseconds*	（任意）ネットワーク モニタリング統計情報を計算する場合は、上位しきい値をミリ秒で指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 5000 です。
ステップ 9	**timeout** *milliseconds*	（任意）IP SLA 操作がその要求パケットからの応答を待つ時間をミリ秒で指定します。指定できる範囲は 0 ～ 604800000 です。デフォルトは 5000 です。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 11	**ip sla schedule** *operation-number* [**ageout** *seconds*] [**life** {**forever** | *seconds*}] [**recurring**] [**start-time** {*hh:mm* {*:ss*} [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]	IP SLA 動作の時間パラメータをスケジューリングします。 • *operation-number*：IP SLA 動作番号を入力します。 • （任意）**ageout** *seconds*：情報をアクティブに収集していない場合に動作をメモリに保存しておく秒数を入力します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒です。 • （任意）**life**：動作を無制限（**forever**）または特定の*秒数*（seconds）実行するかを設定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 • （任意）**recurring**：毎日自動的にスケジューリングするようプローブを設定します。 • （任意）**start-time**：情報収集を開始する動作の時間を入力します。 – 特定の時間に開始するには、時間、分、秒（24 時間式）および日付を入力します。 – 開始時間を選択するまで情報を収集しないように選択するには **pending** を入力します。 – 動作を即座に開始するには **now** を入力します。 – 入力した時間が経過した後に動作を開始するには、**after** *hh:mm:ss* を入力します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip sla configuration** [*operation-number*]	設定済み IP SLA 動作を示します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA 動作を削除するには、**no ip sla** *operation-number* グローバル コンフィギュレーション コマンドを入力します。

CFM ITU-T Y.1731 障害管理の概要

ITU-T Y.1731 機能は、大規模ネットワークのサービス プロバイダーの障害およびパフォーマンスを管理する新しい CFM 機能を実現します。スイッチは、障害の検出、確認、および分離を行う Ethernet Alarm Indication Signal（ETH-AIS; イーサネット アラーム表示信号）、Ethernet Remote Defect Indication（ETH-RDI; イーサネット リモート障害表示）、Ethernet Locked Signal（ETH-LCK; イーサネットロック信号）、Ethernet Multicast Loopback Message（MCAST-LBM; イーサネット マルチキャスト ループバック メッセージ）の各機能をサポートしています。

- 「Y.1731 の用語」（P.43-22）
- 「アラーム表示信号」（P.43-22）
- 「イーサネット リモート障害表示」（P.43-23）
- 「イーサネット ロック信号」（P.43-23）
- 「マルチキャスト イーサネット ループバック」（P.43-23）

Y.1731 の用語

- サーバ MEP：サーバ レイヤ終端機能およびサーバまたはイーサネット最適化機能を組み合せたものです。この場合、サーバ レイヤ終端機能は、サーバ レイヤに固有の OAM メカニズムを実行することが前提になっています。サポートされているメカニズムは、リンクアップ、リンクダウン、および 802.3ah です。
- サーバ レイヤ：障害状態を検出できる仮想 MEP レイヤです。
- 障害状態
  - Loss of Continuity（LOC; 連続性の損失）：MEP がピア MEP からの CCM フレームの受信を停止した。
  - マージ失敗：MEP は（MEP レベルと一致する）正しいメンテナンス レベルの CCM フレームを受信したが、メンテナンス ID が誤っている。
  - 予期しない MEP：MEP は（MEP レベルと一致する）正しいメンテナンス レベルの CCM フレームを受信し、メンテナンス ID も正しいが、予期しない MEP ID であった。
  - 予期しないメンテナンス レベル：MEP はメンテナンス レベルが正しくない CCM フレームを受信した。
  - 予期しない時間：MEP は正しいメンテナンス レベル、正しいメンテナンス ID、正しい MEP ID の CCM フレームを受信したが、転送時間フィールドが異なっている。
- 信号障害：MEP は障害状態を検出すると、信号障害状態を宣言する。
- Alarm Indication Signal（AIS; アラーム表示信号）状況：MEP は AIS フレームを受信した。
- Remote Defect Indication（RDI; リモート障害表示）状況：MEP は RDI フィールドが設定された CCM フレームを受信した。
- Locked Signal（LCK; ロック信号）状況：MEP は LCK フレームを受信した。

アラーム表示信号

Ethernet Alarm Indication Signal（ETH-AIS; イーサネット アラーム表示信号）を使用して、障害が *server*（サブ）レイヤで検出された後にアラームを抑制します。このレイヤは、障害状態を検出できる仮想 MEP レイヤです。障害状態には、信号障害状態、AIS 状態、または LCK 状態があります。

（注） 設定が許可されていても、STP を実行しているネットワークで AIS を設定しないでください。STP の設定により AIS が中断またはリダイレクションされる場合があります。

MEP またはサービス MEP（SMEP）により特定のメンテナンス アソシエーション レベルで接続障害が検出されると、AIS フレームは、クライアント メンテナンス アソシエーション レベルで検出された障害とは逆方向にマルチキャストされます。AIS フレーム転送頻度は、AIS 転送時間に基づいています。最初の AIS フレームは常に、障害状態が検出された直後に送信されます。わずか数個の VLAN のネットワークでは、最初の AIS フレームがエラー検出直後に送信されるよう、転送時間を 1 秒に設定することを推奨します。1 秒の転送時間によるネットワークへの負荷を避けるため、複数（最大 4094 個）の VLAN のネットワークでは、間隔を 60 秒に設定することを推奨します。

ETH-AIS 情報を持つフレームを受信する MEP は、障害状態またはアラームを抑制する必要があるピア MEP のセットにより特定のサーバを判断できません。したがって、この MEP は、すべてのピア MEP が接続されているかいないかにかかわらず、それらのアラームを抑制します。

MEP は AIS フレームを受信すると Entity Group（MEG）レベルがそれ自体の MEG と一致するかその AIS フレームを検査し、AIS 障害状態を検出します（MEG は 802.1ag のメンテナンス アソシエーションの Y.1731 用語です）。障害状態検出の後、AIS 転送時間の 3.5 倍の間隔が経過しても AIS フレームが受信されないと、MEP は AIS 障害状態をクリアします。たとえば、AIS タイマーが 60 秒に設定されている場合、AIS タイマーは 60 秒の 3.5 倍である 210 秒後に切れます。

すべてのエラー状態がクリアされた状態で有効な CCM が受信されるか、AIS 期間タイマーが切れる（デフォルト時間は 60 秒）と、AIS 状態が終了します。

イーサネット リモート障害表示

Ethernet OAM Continuity Check（ETH-CC; イーサネット OAM Continuity Check）転送がイネーブルにされると、Ethernet Remote Defect Indication（ETH-RDI; イーサネット リモート障害表示）機能が CFM CC メッセージのビットを使用して障害状態を MEP ピアに通知します。ETH-RDI 機能については、MEP MEG レベル、ETH-CC 転送時間、および ETH-CC フレーム プライオリティを設定する必要があります。ETH-RDI では MIP を設定する必要はありません。

MEP が ETH-RDI 情報を持つフレームを受信する場合、そのピア MEP が障害状態になったことが判断され、障害状態の間 RDI ファイルが CCM フレームに設定されます。障害状態がクリアされると、MEP は RDI フィールドをクリアします。

MEP は CCM フレームを受信すると、その MEG レベルが同じになるようその CCM フレームを検査し、RDI フィールドが設定されると、RDI 状態が検出されます。ポイントツーポイント イーサネット接続の場合、MEP は、RDI フィールドがクリアされたそのピア MEP からの最初のフレームを受信すると、RDI 状態をクリアできます。ただし、マルチポイント イーサネット接続の場合、MEP は、送信している MEP が障害状態を検出した手段となるピア MEP の関連サブセットを判断できません。MEP は、RDI フィールドがクリアされた CCM フレームをピア MEP 全体のリストから受信した後に RDI 状態をクリアできます。

イーサネット ロック信号

Ethernet Locked Signal（ETH-LCK; イーサネット ロック信号）機能は、サーバ MEP の管理ロックおよびトラフィックを予想している MEP に転送中のデータ トラフィックの割り込みを通知します。ETH-LCK 情報を持つフレームを受信する MEP は、障害状態と管理ロックを区別できます。ETH-LCK はループバック情報（ローカル、リモートポート ループバック、VLAN 単位のループバック、ターミナル ループバック）に依存しています。ETH-LCK のデフォルト タイマーは 60 秒で、デフォルト レベルは MIP レベルです。

MEP が管理ロックされている場合は、AIS 転送時間と同じである、LCK 転送時間に基づいて、そのピア MEP と反対方向に LCK フレームが送信されます。最初の LCK フレームは、管理処理または診断処理の直後に送信されます。

LCK フレームを受信する MEP により、メンテナンス レベルがその設定したメンテナンス レベルと一致していることが確認され、LCK 状態が検出されます。LCK 転送時間の 3.5 倍の時間が経過しても LCK フレームが受信されないと、MEP は LCK 状態をクリアします。

マルチキャスト イーサネット ループバック

Multicast Ethernet Loopback（ETH-LB; マルチキャスト イーサネット ループバック）機能は、MEP のピア MEP で MEP の双方向接続を確認するオンデマンド OAM 機能です。**ping** 特権 EXEC コマンドを入力して MEP でこの機能が起動されると、MEP は ETH-LB 要求情報を持つマルチキャスト フレー

ムを同じ MEG のピア MEP に送信します。MEP は、指定した時間内にそのピア MEP から ETH-LB 応答情報を持つユニキャスト フレームを受信することになります。ETH-LB 要求情報を持つマルチキャスト フレームを受信する MEP によりフレームが検証され、応答情報を持つフレームが転送されます。

マルチキャスト ETH-LB を設定するには、MEP の MEG レベルおよび ETH-LB 要求を持つマルチキャスト フレームのプライオリティを設定します。ETH-LB 要求情報を持つマルチキャスト フレームは、常に不適当な廃棄とマークされます。MIP を設定する必要はありません。

MEP は、オンデマンドでマルチキャスト LB メッセージ フレームを送信します。マルチキャスト LBM フレーム送信後、MEP は 5 秒以内に LB 応答フレームを受信することになります。

MEP が有効な LBM フレームを受信すると、LB 応答フレームが生成され、0 ～ 1 秒のランダムな遅延があった後に、要求された MEP に送信されます。フレームが有効かどうかは、MEG レベルが正しいかどうかによって判断されます。

MEP がマルチキャスト LBM フレームを送信し、5 秒以内に LB 応答フレームを受信する場合、LB 応答フレームは有効です。

Y.1731 障害管理の設定

Y.1731 障害管理を設定するには、CFM をイネーブルにし、参加しているインターフェイスで MIP を設定する必要があります。AIS メッセージは、MIP が設定されたインターフェイスでだけ生成されます。

- 「デフォルト Y.1731 設定」（P.43-24）
- 「ETH-AIS の設定」（P.43-24）
- 「ETH-LCK の設定」（P.43-26）
- 「マルチキャスト イーサネット ループバックの使用」（P.43-29）

デフォルト Y.1731 設定

CFM がイネーブルにされている場合、ETH-AIS および ETH-LCK はデフォルトでイネーブルにされています。

ETH-AIS または ETH-LCK を設定する場合、ETH-AIS または ETH-LCK を操作する前に CFM を設定する必要があります。

CC メッセージがイネーブルにされると、ETH-RDI が自動的に設定されます。

ETH-AIS の設定

スイッチ上でイーサネット AIS を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm ais link-status global**	config-ais-link-cfm モードを開始して、AIS 固有の SMEP コマンドを設定します。

	コマンド	目的
ステップ 3	**level** *level-id* または **disable**	SMEP で転送された AIS フレームを送信する場合のメンテナンス レベルを設定します。指定できる範囲は 0 ～ 7 です。 または ETH-AIS フレームの生成をディセーブルにします。
ステップ 4	**period** *value*	SMEP AIS 転送時間の間隔を設定します。許容値は 1 秒または 60 秒です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ethernet cfm domain** *domain-name* **level** *level-id*	CFM ドメインを定義して、ドメイン レベルを設定し、ドメインで ethernet-cfm コンフィギュレーション モードを開始します。メンテナンス レベルに指定できる数の範囲は 0 ～ 7 です。
ステップ 7	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	ドメインに関連付けるカスタマー サービス Maintenance Association（MA; メンテナンス アソシエーション）名または番号、または VLAN ID あるいは VPN ID を定義し、ethernet-cfm-service コンフィギュレーション モードを開始します。 • *ma-name*：MAID を識別する 100 文字以下の文字列 • *ma-number*：0 ～ 65535 の値 • *vpn-id*：VPN ID を *ma-name* として入力します。 • **vlan** *vlan-id*：指定できる VLAN の範囲は 1 ～ 4094 です。同じレベルの複数のドメインに同じ VLAN ID は使用できません。 • （任意）**direction down**：サービスの方向をダウンに指定します。 • **port**：VLAN と関連付けられていないタグなしダウン MEP である、ポート MEP を設定します。
ステップ 8	**ais level** *level-id*	（任意）MEP で転送された AIS フレームを送信する場合のメンテナンス レベルを設定します。指定できる範囲は 0 ～ 7 です。
ステップ 9	**ais period** *value*	（任意）MEP AIS 転送時間の間隔を設定します。許容値は 1 秒または 60 秒です。
ステップ 10	**ais expiry-threshold** *value*	（任意）MA の期限切れになろうとしているしきい値を整数で設定します。指定できる範囲は 2 ～ 255 です。デフォルトは 3.5 です。
ステップ 11	**no ais suppress-alarms**	（任意）AIS メッセージ受信後に MEP が AIS 障害状態になると、冗長アラームの抑制が無効にされます。
ステップ 12	**exit**	ethernet-cfm コンフィギュレーション モードに戻ります。
ステップ 13	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *interface-id*	インターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	[**no**] **ethernet cfm ais link-status**	インターフェイス上の SMEP からの AIS フレームの送信をイネーブルまたはディセーブルにします。

	コマンド	目的
ステップ 16	**ethernet cfm ais link-status period** *value*	インターフェイス上で SMEP により生成された ETH-AIS 転送時間を設定します。許容値は 1 秒または 60 秒です。
ステップ 17	**ethernet cfm ais link-status level** *level-id*	インターフェイス上で SMEP で転送された AIS フレームを送信する場合のメンテナンス レベルを設定します。指定できる範囲は 0 ～ 7 です。
ステップ 18	**end**	特権 EXEC モードに戻ります。
ステップ 19	**show ethernet cfm smep** [**interface** *interface-id*]	設定を確認します。
ステップ 20	**show ethernet cfm error**	受信 ETH-AIS フレームおよびその他のエラーを表示します。
ステップ 21	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻る、または設定を削除するには、コマンドの **no** 形式を使用します。ETH-AIS フレームの生成をディセーブルにするには、**disable** config-ais-link-cfm モード コマンドを入力します。

次に、イーサネット AIS がイネーブルにされたときの **show ethernet cfm smep** コマンドの出力例を示します。

```
Switch# show ethernet cfm smep
SMEP Settings:
--------------
Interface: GigabitEthernet0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```

ETH-LCK の設定

スイッチ上でイーサネット ロック信号を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm lck link-status global**	config-lck-link-cfm モードを開始して、SMEP LCK コマンドを設定します。
ステップ 3	**level** *level-id* または **disable**	SMEP で転送された ETH-LCK フレームを送信する場合のメンテナンス レベルを設定します。指定できる範囲は 0 ～ 7 です。 または ETH-LCK フレームの生成をディセーブルにします。
ステップ 4	**period** *value*	SMEP ETH-LCK フレーム転送時間の間隔を設定します。許容値は 1 秒または 60 秒です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**ethernet cfm domain** *domain-name* **level** *level-id*	CFM ドメインを定義して、ドメイン レベルを設定し、ドメインで ethernet-cfm コンフィギュレーション モードを開始します。メンテナンス レベルに指定できる数の範囲は 0 ～ 7 です。
ステップ 7	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	ドメインに関連付けるカスタマー サービス メンテナンス アソシエーション名または番号、または VLAN ID あるいは VPN ID を定義し、ethernet-cfm-service コンフィギュレーション モードを開始します。 • *ma-name*：MAID を識別する 100 文字以下の文字列 • *ma-number*：0 ～ 65535 の値 • *vpn-id*：VPN ID を *ma-name* として入力します。 • **vlan** *vlan-id*：指定できる VLAN の範囲は 1 ～ 4094 です。同じレベルの複数のドメインに同じ VLAN ID は使用できません。 •（任意）**direction down**：サービスの方向をダウンに指定します。 • **port**：VLAN と関連付けられていないタグなしダウン MEP である、ポート MEP を設定します。
ステップ 8	**lck level** *level-id*	（任意）MEP で送信された ETH-LCK フレームを送信する場合のメンテナンス レベルを設定します。指定できる範囲は 0 ～ 7 です。
ステップ 9	**lck period** *value*	（任意）MEP ETH-LCK フレーム転送時間の間隔を設定します。許容値は 1 秒または 60 秒です。
ステップ 10	**lck expiry-threshold** *value*	（任意）MA の期限切れになろうとしているしきい値を設定します。指定できる範囲は 2 ～ 255 です。デフォルトは 3.5 です。
ステップ 11	**exit**	ethernet-cfm コンフィギュレーション モードに戻ります。
ステップ 12	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**interface** *interface-id*	インターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	[**no**] **ethernet cfm lck link-status**	インターフェイス上の SMEP からの ETH-LCK フレームの送信をイネーブルまたはディセーブルにします。
ステップ 15	**ethernet cfm lck link-status period** *value*	インターフェイス上で SMEP により生成された ETH-LCK 転送時間を設定します。許容値は 1 秒または 60 秒です。
ステップ 16	**ethernet cfm lck link-status level** *level-id*	インターフェイス上で SMEP で送信された ETH-LCK フレームを送信する場合のメンテナンス レベルを設定します。指定できる範囲は 0 ～ 7 です。
ステップ 17	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 18	**ethernet cfm lck start mpid** *local-mpid* **domain** *domain-name* **vlan** *vlan-id* [**drop l2-bpdu**]	（任意）MEP を LCK 状態にします。 • **mpid** *local-mpid* **domain** *domain-name* **vlan** *vlan-id* は MEP を識別します。 • （任意）**drop l2-bpdu** はスイッチがすべてのデータ フレーム、すべてのレイヤ 3 制御トラフィック、およびすべてのレイヤ 2 BPDU を廃棄するよう指定します。ただし、その MEP の CFM フレームは廃棄しません。このオプションを入力しないと、スイッチによりデータ フレームおよびレイヤ 3 制御フレームだけ廃棄されます。
ステップ 19	**ethernet cfm lck start interface** *interface-id* **direction** {**up** | **down**} [**drop l2-bpdu**]	（任意）インターフェイスを LCK 状態にします。 • **interface** *interface-id*：LCK 状態にするインターフェイスを指定します。 • **direction inward**：LCK はリレー方向を向いています。つまり、スイッチ内にあります。 • **direction outward**：LCK はワイヤ方向を向いています。 • （任意）**drop l2-bpdu** は CFM フレームを除くすべてのレイヤ 2 BPDU、すべてのデータ フレーム、およびすべてのレイヤ 3 制御トラフィックがその MEP に対して廃棄されるよう指定します。このオプションを入力しないと、データ フレームおよびレイヤ 3 制御フレームだけ廃棄されます。
ステップ 20	**show ethernet cfm smep** [**interface** *interface-id*]	設定を確認します。
ステップ 21	**show ethernet cfm error**	受信 ETH-LCK フレームを表示します。
ステップ 22	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MEP を LCK 状態から出すには、**ethernet cfm lck stop mpid** *local-mpid* **domain** *domain-name* **vlan** *vlan-id* 特権 EXEC コマンドを入力します。インターフェイスを LCK 状態から出すには、**ethernet cfm lck start interface** *interface-id* **direction** {**inward** | **outward**} 特権 EXEC コマンドを入力します。

次に、イーサネット LCK がイネーブルにされたときの **show ethernet cfm smep** コマンドの出力例を示します。

```
Switch# show ethernet cfm smep
SMEP Settings:
--------------
Interface: GigabitEthernet0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```

マルチキャスト イーサネット ループバックの使用

この例にあるように、MEP の双方向接続を確認するには、**ping** 特権 EXEC コマンドを使用できます。

```
Switch# ping ethernet multicast domain CD vlan 10
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 0180.c200.0037, timeout is 5 seconds:
Reply to Multicast request via interface FastEthernet1/0/3, from 001a.a17e.f880, 8 ms
Total Loopback Responses received: 1
```

イーサネット CFM 情報の管理および表示

これらの表で特権 EXEC コマンドを使用すると、イーサネット CFM 情報をクリアできます。

表 43-1　CFM 情報のクリア

コマンド	目的
clear ethernet cfm ais domain *domain-name* **mpid** *id* {**vlan** *vlan-id* | **port**}	AIS 障害状態から一致するドメインおよび VLAN ID を備えた MEP をクリアします。
clear ethernet cfm ais link-status interface *interface-id*	AIS 障害状態から SMEP をクリアします。
clear ethernet cfm error	AIS を含む、すべての CFM エラー状態をクリアします。

表 43-2 に記載された特権 EXEC コマンドを使用すると、イーサネット CFM 情報を表示できます。

表 43-2　CFM 情報の表示

コマンド	目的
show ethernet cfm domain brief	CFM ドメイン情報または簡単なドメイン情報を表示します。
show ethernet cfm errors [configuration | domain-id]	デバイスが最後にリセットされてから、またはログが最後にクリアされてからデバイスにロギングされた CFM cc エラー状態を表示します。CFM クロスチェックがイネーブルにされている場合、CFM クロスチェック動作の結果を表示します。
show ethernet cfm maintenance-points local [detail | domain | interface | level | mep | mip]	デバイスに設定されたメンテナンス ポイントを表示します。
show ethernet cfm maintenance-points remote [crosscheck | detail | domain | static]	リモート メンテナンス ポイントのドメインまたはレベル、もしくは CFM データベースの詳細についての表示情報を表示します。
show ethernet cfm mpdb	MIP CC データベースの項目に関する情報を表示します。
show ethernet cfm smep [**interface** *interface-id*]	イーサネット CFM SMEP 情報を表示します。
show ethernet cfm traceroute-cache	traceroute キャッシュの内容を表示します。
show platform cfm	プラットフォームごとの CFM 情報を表示します。

次に、**show ethernet cfm domain brief** コマンドの出力例を示します。

```
Switch# show ethernet cfm domain brief
Domain Name                                Index Level Services Archive(min)
level5                                         1     5        1     100
level3                                         2     3        1     100
test                                           3     3        3     100
```

```
name                                          4     3        1     100
test1                                         5     2        1     100
lck                                           6     1        1     100Total Services : 1
```

次に、**show ethernet cfm errors** コマンドの出力例を示します。

```
Switch# show ethernet cfm errors
-------------------------------------------------------------------------------
MPID Domain Id                                Mac Address     Type   Id  Lvl
     MAName                                   Reason                 Age
-------------------------------------------------------------------------------
6307 level3                                   0021.d7ee.fe80  Vlan   7    3
     vlan7                                    Receive RDI            5s
```

次に、**show ethernet cfm maintenance-points local detail** コマンドの出力例を示します。

```
Switch# show ethernet cfm maintenance-points local detail
Local MEPs:
----------
MPID: 7307
DomainName: level3
Level: 3
Direction: Up
Vlan: 7
Interface: Gi0/3
CC-Status: Enabled
CC Loss Threshold: 3
MAC: 0021.d7ef.0700
LCK-Status: Enabled
LCK Period: 60000(ms)
LCK Expiry Threshold: 3.5
Level to transmit LCK: Default
Defect Condition: No Defect
presentRDI: FALSE
AIS-Status: Enabled
AIS Period: 60000(ms)
AIS Expiry Threshold: 3.5
Level to transmit AIS: Default
Suppress Alarm configuration: Enabled
Suppressing Alarms: No


MIP Settings:
-------------
Local MIPs:
* = MIP Manually Configured
-------------------------------------------------------------------------------
 Level Port           MacAddress     SrvcInst   Type    Id
-------------------------------------------------------------------------------
*5     Gi0/3          0021.d7ef.0700 N/A        Vlan    2,7
```

次に、**how ethernet cfm traceroute** コマンドの出力例を示します。

```
Switch# show ethernet cfm traceroute
Current Cache-size: 0 Hops
Max Cache-size: 100 Hops
Hold-time: 100 Minutes
```

表 43-3 に記載された特権 EXEC コマンドを使用すると、IP SLA イーサネット CFM 情報を表示できます。

表 43-3　IP SLA CFM 情報の表示

コマンド	目的
show ip sla configuration [*entry-number*]	すべての IP SLA 動作または特定の動作のすべてのデフォルト値を含む、設定値を表示します。
show ip sla ethernet-monitor configuration [*entry-number*]	IP SLA 自動イーサネット動作の設定を表示します。
show ip sla statistics [*entry-number* | **aggregated** | **details**]	現在または集約された操作ステータスおよび統計情報を表示します。

イーサネット OAM プロトコルの概要

メトロ イーサネット ネットワークおよびイーサネット WAN の設置、モニタ、およびトラブルシューティングのためのイーサネット OAM プロトコルは、OSI モデルのデータ リンク層のオプション サブレイヤを使用します。通常のリンク動作では、イーサネット OAM を必要としません。イーサネット OAM は、ネットワークまたはネットワークの一部（指定されたインターフェイス）の、全二重ポイントツーポイントまたはエミュレートされたポイントツーポイント イーサネット リンク上に実装できます。

OAM Protocol Data Unit（PDU; プロトコル データ ユニット）と呼ばれる OAM フレームは、低速プロトコル宛先 MAC アドレス（0180.c200.0002）を使用します。これらは MAC サブレイヤで代行受信され、イーサネット ネットワーク内の複数のホップには伝播されません。イーサネット OAM は比較的低速なプロトコル（最大伝送速度が毎秒 10 フレーム）であるため、通常動作にはほとんど影響を及ぼしません。ただし、リンク モニタリングをイネーブルにした場合、CPU はエラー カウンタを頻繁にポーリングする必要があるため、必要な CPU サイクル数はポーリングする必要があるインターフェイス数に比例します。

イーサネット OAM は、主に次の 2 つのコンポーネントで構成されます。

- OAM クライアントは、リンク上でイーサネット OAM を確立、管理して、OAM サブレイヤをイネーブル化および設定します。OAM ディスカバリ フェーズで、OAM クライアントはリモート ピアから受信した OAM PDU をモニタして、OAM 機能をイネーブル化します。ディスカバリ フェーズのあと、OAM クライアントは OAM PDU に対する応答規則および OAM リモート ループバック モードを管理します。
- OAM サブレイヤは、上位 MAC サブレイヤと下位 MAC サブレイヤに対して、2 つの標準 IEEE 802.3 MAC サービス インターフェイスを提供します。OAM クライアントの専用インターフェイスとして機能し、OAM 制御情報および PDU をクライアントとの間で送受信します。次のコンポーネントで構成されます。
  - 制御ブロックは、OAM クライアントとその他の OAM サブレイヤ内部ブロックとの間にインターフェイスを提供します。
  - マルチプレクサは、MAC クライアントからのフレーム、制御ブロック、およびパーサーを管理して、制御ブロックからの OAM PDU およびパーサーからのループバック フレームを下位レイヤに渡します。
  - パーサーは、フレームを OAM PDU、MAC クライアント フレーム、またはループバック フレームに分類して、適切なエンティティに送信します。具体的には、OAM PDU を制御ブロックに、MAC クライアント フレームを上位サブレイヤに、ループバック フレームをマルチプレクサに送信します。

OAM 機能

次の OAM 機能は、IEEE 802.3ah で定義されています。

- ディスカバリでは、ネットワーク内のデバイスおよびその OAM 機能を識別します。定期的に OAM PDU を使用して、OAM モード、設定、および機能、PDU 構成、プラットフォーム ID をアドバタイズします。オプションのフェーズにより、ローカル ステーションはピアの OAM エンティティの設定を許可または拒否できます。
- リンク モニタリングでは、さまざまな状況でのリンク障害を検出し、表示します。リンク上で問題を検出すると、イベント通知 OAM PDU を使用して、リモート OAM デバイスに通知します。エラー イベントには、シンボル エラー数、フレーム エラー数、指定フレーム数内のフレーム エラー数、または指定時間内のエラー秒数が設定されたしきい値を超過した場合などがあります。
- リモート障害表示では、OAM エンティティの質が徐々に劣化していることを、次の状況を伝達することによりピアに伝えます。Link Fault は信号損失を意味し、Dying Gasp は回復不能な状況を意味し、Critical Event は指定されていないベンダー固有のクリティカル イベントを意味します。スイッチは、Link Fault または Critical Event OAM PDU を受信および処理できますが、生成できません。Dying Gasp OAM PDU は生成でき、イーサネット OAM がディセーブル化されたとき、インターフェイスがシャット ダウンされたとき、インターフェイスが error-disabled ステートになったとき、またはスイッチがリロードしたときに示されます。また、電源喪失に基づいた Dying Gasp PDU に対応します。
- リモート ループバック モードは、設置またはトラブルシューティング時のリモート ピアとのリンク品質を確認します。このモードでは、スイッチが OAM PDU ではないフレームを受信すると、同一ポート上にそのフレームを送り返します。ユーザからは、リンクがアップ状態に見えます。戻されたループバック確認応答を使用して、遅延、ジッタ、およびスループットをテストできます。

（注） 接続をテストし、リモート デバイスが到達可能になるようにする別の方法には、イーサネット ループバックの設定があります。「イーサネット ループバックのイネーブル化」（P.43-42）を参照してください。

OAM メッセージ

イーサネット OAM メッセージまたは PDU は標準長のタグなしのイーサネット フレーム（64 ～ 1518 バイト）です。これらは複数のホップには伝播されず、最大伝送速度は毎秒 10 OAM PDU です。メッセージ タイプには、情報、イベント通知、ループバック制御、またはベンダー固有 OAM PDU があります。

イーサネット OAM のセット アップおよび設定

- 「イーサネット OAM のデフォルト設定」（P.43-33）
- 「イーサネット OAM 設定時の注意事項」（P.43-33）
- 「インターフェイス上でのイーサネット OAM のイネーブル化」（P.43-33）
- 「イーサネット OAM リモート ループバックのイネーブル化」（P.43-34）
- 「イーサネット OAM リンク モニタリングの設定」（P.43-35）
- 「イーサネット OAM リモート障害表示の設定」（P.43-38）
- 「イーサネット OAM テンプレートの設定」（P.43-39）

イーサネット OAM のデフォルト設定

イーサネット OAM は、すべてのインターフェイス上でディセーブルです。

インターフェイスでイーサネット OAM がイネーブルになると、リンク モニタリングが自動的にオンになります。

リモート ループバックはディセーブルです。

イーサネット OAM テンプレートは設定されていません。

イーサネット OAM 設定時の注意事項

- スイッチは、Cyclic Redundancy Code（CDC）エラーを伴って送信された出力フレームのモニタリングをサポートしていません。スイッチでは、**ethernet oam link-monitor transmit crc** インターフェイス コンフィギュレーション コマンドまたはテンプレートコンフィギュレーション コマンドを表示できますが、サポートしません。これらのコマンドは受け入れられますが、インターフェイスに適用されません。
- リモート障害表示では、スイッチは Link Fault または Critical Event OAM PDU を生成しません。ただし、リンク パートナーからこれらの PDU を受信した場合は、処理します。イーサネット OAM がディセーブル化されたとき、インターフェイスがシャット ダウンされたとき、インターフェイスが error-disabled ステートになったとき、またはスイッチがリロードしたとき、スイッチは Dying Gasp OAM PDU の生成と受信をサポートします。また、スイッチは電源喪失に基づいた Dying Gasp PDU を生成し、受信できます。PDU には、PDU が送信された理由を示す原因コードが含まれています。
- スイッチは、EtherChannel に属するポート上のイーサネット OAM をサポートしません。

インターフェイス上でのイーサネット OAM のイネーブル化

インターフェイス上でイーサネット OAM をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを OAM インターフェイスとして設定するように定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ethernet oam**	インターフェイス上でイーサネット OAM をイネーブルにします。

	コマンド	目的
ステップ 4	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *seconds* | **mode** {**active** | **passive**} | **timeout** *seconds*]	次のオプションの OAM パラメータを設定できます。 • （任意）**max-rate** *oampdus* を入力して、送信される OAM PDU の 1 秒あたりの最大数を設定します。指定できる範囲は 1 ～ 10 です。 • （任意）**min-rate** *seconds* を入力して、1 秒あたり 1 つの OAM PDU が送信されるときの最小伝送速度を設定します。指定できる範囲は 1 ～ 10 です。 • （任意）**mode active** を入力して、OAM クライアント モードをアクティブに設定します。 • （任意）**mode passive** を入力して、OAM クライアント モードをパッシブに設定します。 **（注）** トラフィックが通過する 2 つのインターフェイス上でイーサネット OAM モードがイネーブルの場合、少なくとも 1 つのインターフェイスはアクティブ モードである必要があります。 • （任意）**timeout** *seconds* を入力して、OAM クライアントのタイムアウト時間を設定します。指定できる範囲は 2 ～ 30 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ethernet oam status** [**interface** *interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイス上でイーサネット OAM をディセーブルにするには、**no ethernet oam** インターフェイス コンフィギュレーション コマンドを入力します。

イーサネット OAM リモート ループバックのイネーブル化

ローカル OAM クライアントが OAM リモート ループバック動作を開始するには、インターフェイス上でイーサネット OAM リモート ループバックをイネーブルにする必要があります。この設定が変更されると、ローカル OAM クライアントはリモート ピアと設定情報を交換します。リモート ループバックは、デフォルトでディセーブルです。

リモート ループバックには、次の制限事項があります。

- Internet Group Management Protocol（IGMP）パケットは、ループバックされません。
- ISL ポートまたは EthrerChannel に属するポート上では、イーサネット OAM リモート ループバックを設定できません。
- ダイナミック ARP インスペクションがイネーブルな場合、ARP パケットまたはリバース ARP パケットはループも廃棄もされません。

インターフェイス上でイーサネット OAM リモート ループバックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを OAM インターフェイスとして設定するように定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ethernet oam remote-loopback** {**supported** | **timeout** *seconds*}	インターフェイス上でイーサネット リモート ループバックをイネーブルにするか、またはループバック タイムアウト時間を設定します。 • **supported** を入力して、リモート ループバックをイネーブルにします。 • **timeout** *seconds* を入力して、リモート ループバック タイムアウト時間を設定します。指定できる範囲は 1 ～ 10 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**ethernet oam remote-loopback** {**start** | **stop**} {**interface** *interface-id*}	インターフェイス上でイーサネット OAM リモート ループバックをオンまたはオフにします。
ステップ 6	**show ethernet oam status** [**interface** *interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

リモート ループバック サポートをディセーブルにするか、またはタイムアウト設定を削除するには、**no ethernet oam remote-loopback** {**supported** | **timeout**} インターフェイス コンフィギュレーション コマンドを使用します。

イーサネット OAM リンク モニタリングの設定

リンク モニタリング機能では、高しきい値および低しきい値を設定できます。高しきい値が設定されていない場合、デフォルト値は **none** です（高しきい値が未設定）。低しきい値が設定されていない場合、デフォルト値は高しきい値よりも低い値になります。

インターフェイス上でイーサネット OAM リンク モニタリングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ethernet oam link-monitor supported**	インターフェイスでリンク モニタリングのサポートをイネーブルにします。これはデフォルト設定です。 このコマンドを入力する必要があるのは、事前に **no ethernet oam link-monitor supported** コマンドが入力され、ディセーブルになっている場合だけです。

	コマンド	目的
ステップ 4	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols* | **none**} | **low** {*low-symbols*}} | **window** *symbols*} **（注）** 高しきい値と低しきい値の両方を設定するときは、この手順を繰り返します。	（任意）エラー シンボル期間リンク イベントをトリガーするエラー シンボル期間の高しきい値および低しきい値を設定します。 • **threshold high** *high-symbols* を入力して、高しきい値をシンボル数で設定します。指定できる範囲は 1 ～ 65535 です。デフォルトは **none** です。 • **threshold high none** を入力して、高しきい値（設定されていた場合）をディセーブルにします。これはデフォルト設定です。 • **threshold low** *low-symbols* を入力して、低しきい値をシンボル数で設定します。指定できる範囲は 0 ～ 65535 です。この値は、高しきい値より小さな値である必要があります。 • **window** *symbols* を入力して、ポーリング期間のウィンドウ サイズ（シンボル数）を設定します。指定できる範囲は 1 ～ 65535 シンボルです。
ステップ 5	**ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} **（注）** 高しきい値と低しきい値の両方を設定するときは、この手順を繰り返します。	（任意）エラー フレームのリンク イベントをトリガーするエラー フレームの高しきい値および低しきい値を設定します。 • **threshold high** *high-frames* を入力して、高しきい値をフレーム数で設定します。指定できる範囲は 1 ～ 65535 です。デフォルトは **none** です。 • **threshold high none** を入力して、高しきい値（設定されていた場合）をディセーブルにします。これはデフォルト設定です。 • **threshold low** *low-frames* を入力して、低しきい値をフレーム数で設定します。指定できる範囲は 0 ～ 65535 です。デフォルトは 1 です。 • **window** *milliseconds* を入力して、エラー フレームがカウントされるウィンドウおよび時間を設定します。指定できる範囲は 10 ～ 600 で、ミリ秒単位で、100 の倍数になります。デフォルトは 100 です。

	コマンド	目的
ステップ 6	**ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*} **（注）** 高しきい値と低しきい値の両方を設定するときは、この手順を繰り返します。	（任意）エラー フレーム期間リンク イベントをトリガーするエラーフレーム期間の高しきい値および低しきい値を設定します。 • **threshold high** *high-frames* を入力して、高しきい値をフレーム数で設定します。指定できる範囲は 1 ～ 65535 です。デフォルトは **none** です。 • **threshold high none** を入力して、高しきい値（設定されていた場合）をディセーブルにします。これはデフォルト設定です。 • **threshold low** *low-frames* を入力して、低しきい値をフレーム数で設定します。指定できる範囲は 0 ～ 65535 です。デフォルトは 1 です。 • **window** *frames* を入力して、ポーリング ウィンドウ サイズをフレーム数で設定します。指定できる範囲は 1 ～ 65535 で、各値は 10000 フレームの倍数になります。デフォルトは 1000 です。
ステップ 7	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} **（注）** 高しきい値と低しきい値の両方を設定するときは、この手順を繰り返します。	（任意）エラー フレーム秒リンク イベントをトリガーするエラーフレーム秒の高しきい値および低しきい値を設定します。 • **threshold high** *high-frames* を入力して、エラー フレーム秒の高しきい値を秒数で設定します。指定できる範囲は 1 ～ 900 です。デフォルトは none です。 • **threshold high none** を入力して、高しきい値（設定されていた場合）をディセーブルにします。これはデフォルト設定です。 • **threshold low** *low-frames* を入力して、低しきい値をフレーム数で設定します。指定できる範囲は 1 ～ 900 です。デフォルトは 1 です。 • **window** *frames* を入力して、ポーリング ウィンドウ サイズをミリ秒数で設定します。指定できる範囲は 100 ～ 9000 で、各値は 100 ミリ秒の倍数になります。デフォルトは 1000 です。
ステップ 8	**ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} **（注）** 高しきい値と低しきい値の両方を設定するときは、この手順を繰り返します。	（任意）一定期間、CRC エラーを伴って受信される入力フレームのモニタリング用のしきい値を設定します。 • **threshold high** *high-frames* を入力して、CRC エラーを伴って受信されるフレーム数の高しきい値を設定します。指定できる範囲は 1 ～ 65535 フレームです。 • **threshold high none** を入力して、高しきい値をディセーブルにします。 • **threshold low** *low-frames* を入力して、低しきい値をフレーム数で設定します。指定できる範囲は 0 ～ 65535 です。デフォルトは 1 です。 • **window** *milliseconds* を入力して、CRC エラーがカウントされるウィンドウおよび時間を設定します。指定できる範囲は 10 ～ 1800 で、ミリ秒単位で、100 の倍数になります。デフォルトは 100 です。

	コマンド	目的
ステップ 9	[**no**] **ethernet link-monitor on**	（任意）インターフェイス上のリンクモニタリング動作を開始または停止（**no** キーワードの使用時）します。リンク モニタリング動作は、サポートがイネーブルであれば自動的に開始されます。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ethernet oam status** [**interface** *interface-id*]	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ethernet oam link-monitor transmit-crc {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} コマンドは、スイッチで表示され、入力も可能ですが、サポートされていません。設定をディセーブルにするには、このコマンドの **no** 形式を使用します。しきい値設定をディセーブルにするには、各コマンドで **no** 形式を使用します。

イーサネット OAM リモート障害表示の設定

高しきい値を超過した場合、リモート リンクがダウンした場合、リモート デバイスがリブートされた場合、またはリモート デバイスのインターフェイス上でイーサネット OAM がディセーブルな場合、インターフェイス上で error-disable アクションが実行されるように設定できます。

インターフェイス上でイーサネット OAM リモート障害表示アクションをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ethernet oam remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action error-disable-interface**	インターフェイス上でイーサネット OAM リモート障害アクションを設定します。次のいずれかの条件でインターフェイスをディセーブルにするよう設定できます。 • **critical-event** を選択すると、指定されていないクリティカル イベントが発生した場合にインターフェイスをシャット ダウンします。 • イーサネット OAM がディセーブル化されたとき、またはインターフェイスが error-disabled ステートになったとき、**dying-gasp** を選択し、インターフェイスをシャットダウンします。 • **link-fault** を選択すると、レシーバーが信号損失を検出した場合にインターフェイスをシャット ダウンします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ethernet oam status** [**interface** *interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチは Link Fault または Critical Event OAM PDU を生成しません。ただし、リンク パートナーからこれらの PDU を受信した場合は、処理します。イーサネット OAM がディセーブル化されたとき、インターフェイスがシャット ダウンされたとき、インターフェイスが error-disabled ステートになったとき、またはスイッチがリロードしたとき、スイッチは原因コードを備えた Dying Gasp OAM PDU の送受信をサポートします。また、電源喪失に基づいた Dying Gasp PDU に対応でき、生成できます。リモート障害表示アクションをディセーブルにするには、**no ethernet remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action** コマンドを入力します。

イーサネット OAM テンプレートの設定

テンプレートを作成すると、複数のイーサネット OAM インターフェイス上で共通のオプション セットを設定できます。テンプレートは、フレーム エラー、フレーム期間エラー、フレーム秒エラー、受信 CRC エラー、およびシンボル期間エラー、しきい値をモニタするよう設定できます。またテンプレートを、高しきい値を超過した場合に error-disabled ステートにするようにも設定できます。これらの手順は任意で、順序を変えて実行したり、繰り返して別のオプションを設定したりできます。

イーサネット OAM テンプレートを設定して、それをインターフェイスに関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**template** *template-name*	テンプレートを作成し、テンプレート コンフィギュレーション モードを開始します。
ステップ 3	**ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	（任意）一定期間、CRC エラーを伴って受信される入力フレームのモニタリング用のしきい値を設定します。 • **threshold high** *high-frames* を入力して、CRC エラーを伴って受信されるフレーム数の高しきい値を設定します。指定できる範囲は 1 ～ 65535 フレームです。 • **threshold high none** を入力して、高しきい値をディセーブルにします。 • **threshold low** *low-frames* を入力して、低しきい値をフレーム数で設定します。指定できる範囲は 0 ～ 65535 です。デフォルトは 1 です。 • **window** *milliseconds* を入力して、CRC エラーがカウントされるウィンドウおよび時間を設定します。指定できる範囲は 10 ～ 1800 で、ミリ秒単位で、100 の倍数になります。デフォルトは 100 です。

	コマンド	目的
ステップ 4	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols* | **none**} | **low** {*low-symbols*}} | **window** *symbols*}	（任意）エラー シンボル期間リンク イベントをトリガーするエラー シンボル期間の高しきい値および低しきい値を設定します。 • **threshold high** *high-symbols* を入力して、高しきい値をシンボル数で設定します。指定できる範囲は 1 ～ 65535 です。 • **threshold high none** を入力して、高しきい値をディセーブルにします。 • **threshold low** *low-symbols* を入力して、低しきい値をシンボル数で設定します。指定できる範囲は 0 ～ 65535 です。この値は、高しきい値より小さな値である必要があります。 • **window** *symbols* を入力して、ポーリング期間のウィンドウ サイズ（シンボル数）を設定します。指定できる範囲は 1 ～ 65535 シンボルです。
ステップ 5	**ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	（任意）エラー フレームのリンク イベントをトリガーするエラー フレームの高しきい値および低しきい値を設定します。 • **threshold high** *high-frames* を入力して、高しきい値をフレーム数で設定します。指定できる範囲は 1 ～ 65535 です。高しきい値を入力する必要があります。 • **threshold high none** を入力して、高しきい値をディセーブルにします。 • **threshold low** *low-frames* を入力して、低しきい値をフレーム数で設定します。指定できる範囲は 0 ～ 65535 です。デフォルトは 1 です。 • **window** *milliseconds* を入力して、エラー フレームがカウントされるウィンドウおよび時間を設定します。指定できる範囲は 10 ～ 600 で、ミリ秒単位で、100 の倍数になります。デフォルトは 100 です。
ステップ 6	**ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*}	（任意）エラー フレーム期間リンク イベントをトリガーするエラーフレーム期間の高しきい値および低しきい値を設定します。 • **threshold high** *high-frames* を入力して、高しきい値をフレーム数で設定します。指定できる範囲は 1 ～ 65535 です。高しきい値を入力する必要があります。 • **threshold high none** を入力して、高しきい値をディセーブルにします。 • **threshold low** *low-frames* を入力して、低しきい値をフレーム数で設定します。指定できる範囲は 0 ～ 65535 です。デフォルトは 1 です。 • **window** *frames* を入力して、ポーリング ウィンドウ サイズをフレーム数で設定します。指定できる範囲は 1 ～ 65535 で、各値は 10000 フレームの倍数になります。デフォルトは 1000 です。

	コマンド	目的
ステップ 7	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-seconds* | **none**} | **low** {*low-seconds*}} | **window** *milliseconds*}	（任意）エラー フレーム秒リンク イベントをトリガーするフレーム秒の高しきい値および低しきい値を設定します。 • **threshold high** *high-seconds* を入力して、高しきい値をシンボル数で設定します。指定できる範囲は 1 ～ 900 です。高しきい値を入力する必要があります。 • **threshold high none** を入力して、高しきい値をディセーブルにします。 • **threshold low** *low-frames* を入力して、低しきい値をフレーム数で設定します。指定できる範囲は 1 ～ 900 です。デフォルトは 1 です。 • **window** *frames* を入力して、ポーリング ウィンドウ サイズをフレーム数で設定します。指定できる範囲は 100 ～ 9000 で、各値は 100 ミリ秒の倍数になります。デフォルトは 1000 です。
ステップ 8	**ethernet oam link-monitor high threshold action error-disable-interface**	（任意）エラーが高しきい値を超過した場合に、インターフェイスを error disabled ステートにするようスイッチを設定します。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *interface-id*	イーサネット OAM インターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**source-template** *template-name*	テンプレートを関連付けて、設定されたオプションをインターフェイスに適用します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ethernet oam status** [**interface** *interface-id*]	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチは、CRC エラーを伴う出力フレームのモニタリングをサポートしていません。**ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} コマンドは、スイッチで表示され、入力も可能ですが、サポートされていません。テンプレートからオプションを削除するには、各コマンドの **no** 形式を使用します。送信元テンプレートの関連付けを削除するには、**no source-template** *template-name* を使用します。

イーサネット OAM プロトコル情報の表示

表 43-4 に記載された特権 EXEC コマンドを使用すると、イーサネット OAM プロトコル情報を表示できます。

表 43-4　イーサネット OAM プロトコル情報の表示

コマンド	目的
show ethernet oam discovery [**interface** *interface-id*]	すべてのイーサネット OAM インターフェイスまたは指定されたインターフェイスのディスカバリ情報を表示します。
show ethernet oam statistics [**interface** *interface-id*]	イーサネット OAM パケットの詳細情報を表示します。

表 43-4　イーサネット OAM プロトコル情報の表示

コマンド	目的
show ethernet oam status [**interface** *interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスのイーサネット OAM 設定を表示します。
show ethernet oam summary	スイッチ上のアクティブなイーサネット OAM セッションを表示します。

イーサネット ループバックのイネーブル化

サービス プロバイダーは、ポート単位および VLAN 単位のイーサネット ループバックを使用して、初期起動時の接続のテスト、スループットのテスト、および両方向の Quality of Service（QoS）のテストができます。スイッチでは、次の 2 種類のループバックがサポートされています。

- ファシリティ ループバックにより、トラフィックのポート単位または VLAN 単位のループバックが可能になります。複数のスイッチ間の接続をテストする場合のイーサネット OAM リモート ループバックへの代替方法になります（「イーサネット OAM リモート ループバックのイネーブル化」（P.43-34）を参照）。MAC 宛先アドレスおよび送信元アドレスを交換（スワップ）し、パケットをテスト ヘッドおよびテスト スイッチ間の複数のスイッチ間で送受信できます。

  ポート単位のファシリティ ループバックによりポートはループバック状態になり、通常のトラフィックについてリンクはアップになりますが、ライン プロトコルはダウンです。スイッチにより、すべての受信トラフィックはループバックされます。

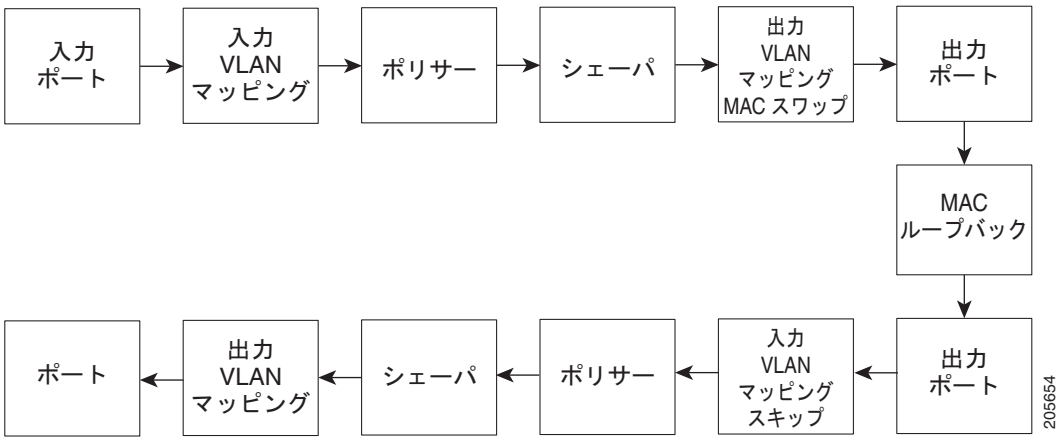
  キーワード **vlan** *vlan-list* を入力してポート単位、VLAN 単位のループバックを設定する場合、ポートのその他の VLAN では引き続きトラフィックが正常にスイッチされるため、処理を中断させずにループバック テストできます。

- ターミナル ループバックにより、両方向の完全パス QoS をテストできます。ターミナル ループバックによりポートは、リンクがアップに見える状態になりますが、実際はリンクは外部でダウンになっており、パケットは送信されません。ポートの設定変更は、ループバックされているトラフィックに即座に影響を与えます。

  ターミナル ループバックでは、ループバックされるトラフィックはフォワーディング パスを 2 回通過します。MAC スワップが設定されていない場合、ループバックされたマルチキャストまたはブロードキャスト トラフィックは、その VLAN でフラッディングされます。パケットは他のポートから 2 回、1 回は入力パケットから、もう 1 回はループバック パケットから出てゆきます。図 43-3 を参照してください。

  スイッチ 1 つにつきターミナル ループバックは 1 回だけ設定できます。

図 43-3　ターミナル ループバック パケットの流れ



デフォルトでは、ループバックは設定されません。

イーサネット ループバックには次の特性があります。

- イーサネット ループバックは、VLAN またはポート チャネルではなく、物理ポートでだけ設定できます。
- ポート 1 つにつきループバックを 1 つ設定でき、スイッチ 1 つにつきループバックを 2 つまで設定できます。
- スイッチ 1 つにつきターミナル ループバックは 1 回だけ設定できます。
- ポートは、シャットダウンやスイッチ ポートからルーテッド ポートへの交換などのポート イベント後にループバックを終了します。
- キーワード **vlan** *vlan-list* を入力して VLAN ループバックを設定する場合、VLAN はどのポートにも転送されない内部 VLAN へトンネリングされます。トンネリングは出力ポートで終了するため、ユーザには透過的です。
- VLAN ループバックは、非トランク インターフェイスではサポートされていません。
- ターミナル ループバックは、ルーテッド インターフェイスではサポートされていません。
- SPAN とループバックは同じスイッチで同時に設定できません。ループバックが設定されている任意のポートに SPAN を設定しようとすると、エラー メッセージを受信します。
- ポートが Flex Link ポート、あるいは EtherChannel に属している場合は、ループバック状態にはできません。ループバックがアクティブな場合、ポートを Flex Link または EtherChannel に追加できません。
- ポート ループバックは、VLAN マッピング機能とハードウェア リソースを共有します。ループバックを設定しようとするとき、VLAN マッピング設定のために十分な TCAM リソースが使用できない場合、エラー メッセージを受信し、設定は許可されません。

インターフェイス上でイーサネット ファシリティ ループバックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的
ステップ 3	**ethernet loopback facility** [**vlan** *vlan-list*] [**mac-address** {**swap** | **copy**}] [**timeout** {*seconds* | **none**}] **supported**	イーサネット ファシリティ ループバックをインターフェイスで設定します。キーワードの意味は次のとおりです。 • （任意）処理を中断させずにループバック テストを行う VLAN ループバックを設定するには、**vlan** *vlan-list* を入力します。ポート上のその他の VLAN では、引き続きトラフィックがスイッチされます。 • （任意）ループバック処理のため MAC 宛先アドレスおよび発信元アドレスをスワップするようスイッチを設定するには、**mac-address swap** を入力します。 • （任意）ループバック処理のため MAC 宛先アドレスおよび発信元アドレスをコピーするようスイッチを設定するには、**mac-address copy** を入力します。これは、**mac-address** オプションが設定されていない場合のデフォルト動作です。 • ループバック タイムアウト時間を設定するには **timeout** *seconds* を入力します。指定できる範囲は 5 ～ 300 秒です。デフォルトは 60 秒です。 • （任意）タイムアウトしないようループバックを設定するには、**timeout none** を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**ethernet loopback** {**start** *interface-id* | **stop** {*interface-id* | **all**}	インターフェイスでイーサネット ループバックをオンにする（**start**）か、インターフェイスまたはすべてのインターフェイスでイーサネット ループバックをオフ（**stop**）にします。 **（注）** コマンドを入力してループバックを開始すると、これはポートまたは VLAN 上の浸入ループバックであり、パケットを渡すことができないというメッセージを受信します。コマンドを確認する必要があります。
ステップ 6	**show ethernet loopback** [*interface-id*] **show interface** *interface-id*, **show interface status**, **show log**	スイッチまたはインターフェイスの設定を確認します。 ループバックがインターフェイスで稼動中（開始された）ことを確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスのアクティブ ループバック セッションを停止する、またはすべてのアクティブ ループバック セッションを停止するには、**ethernet loopback stop** {*interface-id* | **all**} 特権 EXEC コマンドを入力します。イーサネット ファシリティ ループバック設定を削除するには、**no ethernet loopback** インターフェイス コンフィギュレーション コマンドを入力します。

次に、MAC 宛先アドレスおよび発信元アドレスをスワップし、タイムアウトせず、ループバック プロセスを開始するようイーサネット ループバックを設定する方法の例を示します。ループバックを開始する前にコマンドを確認する必要があります。

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback facility mac-address swap timeout none supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
This is an intrusive loopback.
```

```
Therefore, while you test Ethernet connectivity,
you will be unable to pass traffic across that link.
Proceed with Local Loopback?[confirm]
```

This is the output from the **show ethernet loopback** privileged EXEC command for the previous configuration:

```
Switch# show ethernet loopback
======================================
Loopback Session 0  : Interface Gi0/1
Direction           : facility
Type                : port
Status              : configured
MAC Mode            : swap
Time out            : none.
```

インターフェイス上でイーサネット ターミナル ループバックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ethernet loopback terminal** [**mac-address** {**swap** | **copy**}] [**timeout** {*seconds* | **none**}] **supported**	イーサネット ターミナル ループバックを設定し、インターフェイスで QoS をテストします。キーワードの意味は次のとおりです。 • （任意）ループバック処理のため MAC 宛先アドレスおよび発信元アドレスをスワップするようスイッチを設定するには、**mac-address swap** を入力します。 • （任意）ループバック処理のため MAC 宛先アドレスおよび発信元アドレスをコピーするようスイッチを設定するには、**mac-address copy** を入力します。これは、**mac-address** オプションが設定されていない場合のデフォルト動作です。 • ループバック タイムアウト時間を設定するには **timeout** *seconds* を入力します。指定できる範囲は 5 ～ 300 秒です。デフォルトは 60 秒です。 • （任意）タイムアウトしないようループバックを設定するには、**timeout none** を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**ethernet loopback** {**start** | **stop**} {*interface-id*}	インターフェイス上でイーサネット ループバックをオン（**start**）またはオフ（**stop**）にします。 **（注）** ルーテッド インターフェイスでターミナル ループバックを開始しようとすると、エラー メッセージを受信し、ループバックを開始できません。
ステップ 6	**show ethernet loopback** [*interface-id*] **show interface** *interface-id*, **show interface status**, **show log**	スイッチまたはインターフェイスの設定を確認します。 ループバックがインターフェイスで稼動中（開始された）ことを確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

イーサネット ターミナル設定をディセーブルにするには、**no ethernet loopback** インターフェイス コンフィギュレーション コマンドを入力します。

次に、インターフェイスで QoS をテストし、MAC 宛先アドレスおよび発信元アドレスをスワップし、30 秒後にタイムアウトし、ループバック プロセスを開始するようイーサネット ターミナル ループバックを設定する方法の例を示します。

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback terminal mac-address swap timeout 30 supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
```

E-LMI の概要

Ethernet Local Management Interface（E-LMI）は、CE デバイスと PE デバイス間のプロトコルです。PE-CE UNI リンクでだけ稼動し、CE ポートで利用可能なイーサネット サービスの接続ステータスおよび設定パラメータを CE デバイスに 通知します。E-LMI は、プロバイダー ネットワーク内で稼動して、OAM ステータスを収集する CFM などの OAM プロトコルと相互運用します。CFM は、プロバイダー メンテナンス レベル（アップ MFP と UNI で連携する UPE ツー UPE）で稼動します。E-LMI は OAM Ethernet Infrastructure に依存して、CFM ドメイン上の Ethernet Virtual Connection（EVC）のエンドツーエンドのステータスに関して、CFM と相互作用します。

任意の 2 つの OAM プロトコル間の相互作用効率を向上させる OAM マネージャは CFM と E-LMI 間の相互作用を処理します。インターフェイスは単一方向で、スイッチの UPE 側の OAM マネージャから E-LMI に対してだけ実行されます。OAM プロトコルから変更に関する通知を受信すると、その情報は E-LMI からの要求または OAM にトリガーされることにより、交換されます。次のタイプの情報が、リレーされます。

- EVC の名前および使用可能なステータス
- リモート UNI の名前およびステータス
- リモート UNI カウント

EVC、サービス VLAN、（各 CE ツー PE リンクの）UNI ID、および UNI のカウントとアトリビュートを設定できます。所定の S-VLAN ドメインのアクティブ UNI 数またはリモート UNI ID のいかなる変更に関しても OAM マネージャに通知するよう CFM を設定する必要があります。

スイッチは、CE デバイスとしても PE デバイスとしても設定できます。

E-LMI の OAM マネージャとの相互作用

CE 側では、E-LMI と OAM マネージャとの相互作用は必要ありません。UPE 側では、OAM マネージャがメトロ ネットワーク内で稼動する OAM プロトコル（この場合は CFM）から収集されたデータを、E-LMI スイッチにリレーする抽象的レイヤを定義します。情報のフローは単一方向（OAM マネージャから E-LMI への）ですが、次のいずれかの方法でトリガーされます。

- E-LMI からの要求によりトリガーされる同期データ フロー
- CFM からリモート UNI 数の変更についての通知を受信した場合に、OAM マネージャによりトリガーされる非同期データ フロー

このデータには、次の内容が含まれます。

- EVC の名前および使用可能ステータス（アクティブ、非アクティブ、部分的なアクティブ、または定義なし）

- リモート UNI の名前およびステータス（アップ、切断、管理上のダウン、過剰な FCS 障害、または到達不可能）
- リモート UNI カウント（予想される UNI の総数およびアクティブ UNI の実数）

非同期更新は、アクティブ UNI 数が変更された場合にだけトリガーされます。

CFM の OAM マネージャとの相互作用

所定の S-VLAN またはドメインのアクティブ UNI 数またはリモート UNI ID が変更された場合、CFM は非同期で OAM マネージャに通知します。アクティブ UNI 数が変更されると、EVC ステータスが変更される場合（または、されない場合）があります。OAM マネージャは、アクティブ UNI 数および関連する UNI の総数により、EVC ステータスを算出します。

（注）　クロスチェックがディセーブルの場合、UNI 数が変更されても SNMP トラップは送信されません。

E-LMI の設定

E-LMI と CFM とを連携させるには、EVC、Ethernet Service Instance（EFP）、および E-LMI カスタマーの VLAN マッピングを設定します。ほとんどの設定は、CE デバイスと接続するインターフェイス上の PE スイッチで行われます。CE スイッチでは、接続インターフェイス上で E-LMI をイネーブルにすることだけが必要です。メトロ ネットワークの両側の PE デバイスでは、EVC 定義など 一部の OAM パラメータを設定する必要があることに注意してください。

ここでは、次の情報について説明します。

- 「E-LMI のデフォルト設定」（P.43-47）
- 「E-LMI および OAM マネージャ設定時の注意事項」（P.43-48）
- 「OAM マネージャの設定」（P.43-48）
- 「E-LMI のイネーブル化」（P.43-51）
- 「イーサネット OAM マネージャの設定例」（P.43-52）

E-LMI のデフォルト設定

イーサネット LMI は、デフォルトでグローバルにディセーブルにされています。イネーブルの場合、スイッチは、デフォルトで PE モードです。

ethernet lmi global グローバル コンフィギュレーション コマンドを入力して、E-LMI をグローバルにイネーブルにすると、すべてのインターフェイス上で自動的にイネーブルになります。また、グローバル設定の上書きに関してインターフェイス単位で E-LMI をイネーブルまたはディセーブルにすることもできます。最後に入力された E-LMI コマンドが優先されます。

EVC、EFP サービス インスタンス、または UNI は定義されていません。

UNI バンドリング サービスは、多重化に組み込まれています。

E-LMI および OAM マネージャ設定時の注意事項

OAM マネージャは基礎となる要素で、2 つの相互作用する OAM プロトコル（この場合、CFM および E-LMI）が必要です。OAM が動作するには、接続の PE 側で、CFM および E-LMI が稼動している必要があります。

- E-LMI は、ルーテッド ポート、EtherChannel ポート チャネル、または EtherChannel、プライベート VLAN ポート、もしくは IEEE 802.1Q トンネル ポートに属するポートではサポートされていません。
- E-LMI は、VLAN インターフェイスでは設定できません。
- E-LMI をグローバルに、またはインターフェイス上でイネーブルにすると、デフォルトでは、スイッチは PE モードです。**ethernet lmi ce** グローバル コンフィギュレーション コマンドを入力して、スイッチまたはインターフェイスを CE モードでイネーブルにする必要があります。
- スイッチが CE デバイスとして設定されている場合、**service instance** および **ethernet uni** インターフェイス コマンドは表示されますが、サポートされません。

OAM マネージャの設定

PE スイッチ上で OAM マネージャを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm domain** *domain-name* **level** *level-id*	CFM ドメインを定義して、ドメイン レベルを設定し、ドメインで ethernet-cfm コンフィギュレーション モードを開始します。メンテナンス レベルに指定できる数の範囲は 0 ～ 7 です。
ステップ 3	**service** *csi-id* **vlan** *vlan-id*	メンテナンス ドメイン内の普遍的に一意の CSI および VLAN ID を定義します。 • *csi-id* : CSI を識別する 100 文字以下の文字列 • *vlan-id* : 指定できる VLAN の範囲は 1 ～ 4095 です。同じレベルの複数のドメインに同じ VLAN ID は使用できません。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ethernet evc** *evc-id*	Ethernet Virtual Connection（evc; イーサネット バーチャル コネクション）を定義して、evc コンフィギュレーション モードを開始します。識別子は、最大 100 文字長まで設定できます。
ステップ 6	**oam protocol cfm svlan** *vlan-id* **domain** *domain-name*	EVC OAM プロトコルを CFM として設定し、ステップ 2 および 3 で設定された CFM ドメインのメンテナンス レベルの Service Provider VLAN-ID（S-VLAN-ID）を識別します。 **（注）** CFM ドメインが存在しない場合、コマンドは拒否され、エラー メッセージが表示されます。

	コマンド	目的
ステップ 7	**uni count** *value*	（任意）EVC の UNI カウントを設定します。指定できる範囲は 2 ～ 1024 です。デフォルトは 2 です。 このコマンドを入力しない場合、デフォルトのポイントツーポイント サービスになります。値を 2 に入力した場合、ポイントツーマルチポイント サービスを選択することもできます。値を 3 以上に設定した場合、サービスはポイントツーマルチポイントになります。 **（注）** ドメイン内のメンテナンス エンド ポイントの適切な数値を認識する必要があります。実際のエンド ポイントの数より大きい値を入力した場合、すべてのエンド ポイントがアップである場合でも、UNI ステータスは一部アクティブと表示されます。また、実際のエンド ポイントの数より小さい uni count 値を入力した場合、エンド ポイントの一部がアップでない場合でも、ステータスはアクティブと表示される場合があります。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	OAM マネージャでモニタリングする他の CFM ドメインに関して、ステップ 2 ～ 5 を繰り返します。	
ステップ 10	**interface** *interface-id*	CE デバイスに接続される物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**service instance** *efp-identifier* **ethernet** [*evc-id*]	インターフェイス上で EFP を設定して、イーサネット サービス コンフィギュレーション モードを開始します。 • EFP 識別子は、インターフェイスごとのサービス識別子で、VLAN にはマッピングしません。指定できる EFP 識別子の範囲は 1 ～ 4967295 です。 • （任意）*evc-id* を入力して、EVC を EFP に接続します。
ステップ 12	**ethernet lmi ce-vlan map** {*vlan-id* | **any** | **default** | **untagged**}	特定の UNI で E-LMI カスタマー の VLAN/EVC マッピングを設定します。キーワードの意味は次のとおりです。 • **vlan** *vlan-id* には、カスタマーの VLAN ID または 単一の VLAN ID（1 ～ 4094）としてマッピングする ID、ハイフンで区切られた VLAN ID、またはカンマで区切られた一連の VLAN ID を入力します。 • すべての VLAN（タグなしまたは 1 ～ 4094）をマッピングするには、**any** を入力します。 • デフォルトの EFP をマッピングする場合は、**default** を入力します。**default** キーワードを使用できるのは、サービス インスタンスが VLAN または VLAN のグループにマッピング済みの場合に限ります。 • タグなしの VLAN をマッピングするには、**untagged** を入力します。
ステップ 13	**exit**	インターフェイス コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 14	**ethernet uni id** *name*	イーサネット UNI ID を設定します。名前は、所定のカスタマー サービス インスタンスの一部であるすべての UNI で一意である必要があり、最大で 64 文字長まで設定できます。ポートで UNI ID が設定されている場合、この ID は、所定の MEP 用に明示的に設定された名前ではない限り、ポート上で設定されるすべての MEP のデフォルト名として使用されます。 **（注）** このコマンドは、CE デバイスに直接接続されているすべてのポート上で必要です。指定された ID がデバイス上で一意でない場合、エラー メッセージが表示されます。
ステップ 15	**ethernet uni** {**bundle** [**all-to-one**] | **multiplex**}	（任意）UNI バンドリング アトリビュートを設定します。 • **bundle** <cr> を入力した場合、UNI は多重化なしのバンドリング（EVC は 1 つだけで、1 つまたは複数の VLAN がその EVC にマッピングされる）をサポートします。 • **bundle all-to-one** を入力した場合、UNI は単一の EVC をサポートし、すべての VLAN はその EVC にマッピングされます。 • **multiplex** を入力した場合、UNI はバンドリングなしの多重化をサポートします（1 つまたは複数の EVC で単一の VLAN が各 EVC にマッピングされる）。 バンドリング アトリビュートを設定しない場合、デフォルトの多重化と連携するバンドリングとなります（1 つまたは複数の EVC で、1 つまたは複数の VLAN が各 EVC にマッピングされる）。
ステップ 16	**end**	特権 EXEC モードに戻ります。
ステップ 17	**show ethernet service evc** {**detail** | **id** *evc-id* | **interface** *interface-id*}	設定を確認します。
ステップ 18	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EVC、EFP、または UNI ID を削除するか、またはデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

（注） UNI サービス タイプ、EVC、EFP、または CE-VLAN を設定、またはその設定を変更、削除する場合、すべての設定で、その設定が一致している（UNI サービス タイプが EVC または EFP および CE-VLAN 設定に）ことを確認します。一致しない場合、その設定は拒否されます。

E-LMI のイネーブル化

E-LMI をグローバルに、またはインターフェイス上でイネーブルにし、スイッチを PE または CE デバイスとして設定できます。スイッチまたはインターフェイスで E-LMI をイネーブルにするには、特権 EXEC モードで次の手順を実行します。グローバル コマンドとインターフェイス コマンドの順序により設定が決定されることに注意してください。最後に入力されたコマンドが優先されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet lmi global**	すべてのインターフェイス上で E-LMI をグローバルにイネーブルにします。デフォルトでは、スイッチは PE デバイスです。
ステップ 3	**ethernet lmi ce**	（任意）スイッチを E-LMI CE デバイスとして設定します。
ステップ 4	**interface** *interface-id*	インターフェイスを E-LMI インターフェイスとして設定するように定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ethernet lmi interface**	インターフェイス上で E-LMI を設定します。グローバルにイネーブルにした E-LMI は、特定のインターフェイス上でディセーブルにしない限り、すべてのインターフェイスでイネーブルになります。グローバルにディセーブルに設定されている E-LMI は、このコマンドを使用して特定のインターフェイス上でイネーブルにできます。
ステップ 6	**ethernet lmi** {**n391** *value* | **n393** *value* | **t391** *value*| **t392** *value*}	UNI に E-LMI パラメータを設定します。 キーワードの意味は次のとおりです。 • **n391** *value*：カスタマー機器のイベント カウンタを設定します。カウンタは、UNI およびすべての Ethernet Virtual Connection（EVC）のステータスをポーリングします。指定できる範囲は 1 ～ 65000 で、デフォルトは 360 です。 • **n393** *value*：メトロ イーサネット ネットワークのイベント カウンタを設定します。指定できる範囲は 1 ～ 10 で、デフォルトは 4 です。 • **t391** *value*：カスタマー機器のポーリング タイマーを設定します。ポーリング タイマーはステータス問い合せを送信し、ステータス メッセージが受信されない場合、エラーを記録します。指定できる範囲は 5 ～ 30 秒で、デフォルトは 10 秒です。 • **t392** *value*：メトロ イーサネット ネットワークのポーリング確認タイマー、または受信したステータス照会を確認するタイマーを設定します。指定できる範囲は、5 ～ 30 秒です。または、0 を入力すると、タイマーはディセーブルになります。デフォルトは 15 秒です。 **（注）** **t392** キーワードは、スイッチが CE モードの場合にはサポートされません。
ステップ 7	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	**show ethernet lmi evc**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

E-LMI をグローバルにディセーブルにするには、**no ethernet lmi** グローバル コンフィギュレーション コマンドを使用します。インターフェイス上で E-LMI をディセーブルにするか、またはタイマーをデフォルト設定に戻すには、キーワードを指定する **ethernet lmi** インターフェイス コンフィギュレーション コマンドの **no** 形式を使用します。

ステータス要求ポールから CE に送信された情報を表示するには、**show ethernet lmi** コマンドを使用します。デバイスの現在のステータスを示すには、**show ethernet service** コマンドを使用します。

イーサネット OAM マネージャの設定例

次に、PE デバイスおよび CE デバイス上の CFM および E-LMI を OAM マネージャとともに設定する単純な例を示します。スイッチは、PE デバイスとしても CE デバイスとしても設定できます。

PE デバイスの設定

次に、PE デバイス上での OAM マネージャ、CFM、E-LMI の設定例を示します。

```
Switch# config t
Switch(config)# ethernet cfm domain Top level 7
Switch(config)# ethernet cfm domain Provider level 4
Switch(config-ether-cfm)# service customer_1 vlan 101
Switch(config-ether-cfm)# mep crosscheck mpid 404 vlan 101
Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm domain Operator_level 2
Switch(config-ether-cfm)# service operator_1 vlan 101
Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm enable
Switch(config)# ethernet evc test1
Switch(config-evc)# oam protocol cfm svlan 101 domain Provider
Switch(config-evc)# exit
Switch(config)# ethernet evc 101
Switch(config-evc)# uni count 3
Switch(config-evc)# oam protocol cfm svlan 101 domain Operator
Switch(config-evc)# exit
Switch(config)# ethernet lmi global
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 200 vlan 200
Switch(config-if)# service instance 101 ethernet test1
Switch(config-if-srv)# ethernet lmi ce-vlan map 101
Switch(config-if-srv)# exit
Switch(config-if)# exit
Switch(config)# ethernet cfm cc enable level 2-4 vlan 101
Switch(config)# exit
```

CE デバイスの設定

次に、CE デバイス上で E-LMI を設定するのに必要なコマンドの例を示します。スイッチは、CE デバイスとして設定できます。この例では E-LMI はグローバルにイネーブルになりますが、特定のインターフェイス上でだけイネーブルにすることもできます。ただし、**ethernet lmi ce** グローバル コンフィギュレーション コマンドを入力しない場合、インターフェイスはデフォルトで PE モードになります。

```
Switch# config t
Switch(config)# ethernet lmi global
Switch(config)# ethernet lmi ce
Switch(config)# exit
```

（注）　E-LMI を機能させるには、PE デバイスで使用される VLAN を CE デバイスでも作成する必要があります。CE デバイス上で **vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力して、VLAN を作成します。この場合、*vlan-ids* は PE デバイスのものと一致します。**switchport trunk allowed vlan** *vlan-ids* インターフェイス コンフィギュレーションコマンドを入力して、これらの VLAN を許可 VLAN として設定します。許可 VLAN は、トランキング モードにある場合にタグ付き形式のトラフィックで送受信できます。

E-LMI および OAM マネージャの情報の表示

表 43-5 の特権 EXEC コマンドを使用すると、E-LMI または OAM マネージャの情報を表示できます。

表 43-5　E-LMI および OAM マネージャの情報の表示

コマンド	目的
show ethernet lmi evc [**detail** *evc-id* [**interface** *interface-id*] | **map interface** *type number*]	ステータス要求ポールから CE に送信された E-LMI EVC に関する詳細情報を表示します。
show ethernet lmi parameters interface *interface-id*	ステータス要求ポールから CE に送信されたイーサネット LMI インターフェイス パラメータを表示します。
show ethernet lmi statistics interface *interface-id*	ステータス要求ポールから CE に送信されたイーサネット LMI インターフェイスの統計情報を表示します。
show ethernet lmi uni map interface [*interface-id*]	ステータス要求ポールから CE に送信された E-LMI UNI VLAN マップに関する情報を表示します。
show ethernet service evc {**detail** | **id** *evc-id* | **interface** *interface-id*}	指定された EVC CSI または設定されたすべてのサービス インスタンスの詳細を表示します。
show ethernet service instance {**detail** | **id** *efp-identifier* **interface** *interface-id* | **interface** *interface-id*}	指定された EFP に関連する情報を表示します。
show ethernet service interface [*interface-id*] [**detail**]	OAM マネージャ インターフェイスの情報を表示します。

イーサネット CFM とイーサネット OAM の相互作用

CFM とイーサネット OAM 間の相互作用のため、OAM マネージャ インフラストラクチャも設定できます。イーサネット OAM プロトコルが CFM MEP が設定されたインターフェイスで稼動している場合、イーサネット OAM により CFM にインターフェイスの状態が通知されます。イーサネット OAM から CFM プロトコルへの単一方向に相互作用し、交換される唯一の情報はユーザ ネットワーク インターフェイス ポートのステータスです。

これらの状況が発生した場合、イーサネット OAM プロトコルにより CFM が通知されます。

- エラーしきい値は、ローカル インターフェイスで交差します。

  CFM は、Port StatusType Length Value（TLV）の *Local_Excessive_Errors* のポート ステータスを送信することで、通知に応答します。

- イーサネット OAM は、エラーしきい値がリモート エンドポイントで超過していることを示す OAMPDU をリモート側から受信します。

  CFM は、Port Status TLV の *Remote_Excessive_Errors* のポート ステータスを送信することで、通知に応答します。

- ローカル ポートはループバック モードに設定されています。

  CFM は Port Status TLV の Test のポート ステータスを送信することで応答します。

- リモート ポートはループバック モードに設定されています。

  CFM は Port Status TLV の Test のポート ステータスを送信することで応答します。

ここでは、次の情報について説明します。

- 「イーサネット OAM の CFM との相互作用の設定」（P.43-54）
- 「イーサネット OAM および CFM 設定の例」（P.43-56）

CFM およびイーサネット OAM の相互作用の詳細については、次の URL の Ethernet Connectivity Fault Management フィーチャ モジュールを参照してください。

http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a008066fcb8.html

イーサネット OAM の CFM との相互作用の設定

イーサネット OAM を CFM とともに動作させるには、Ethernet Virtual Circuit（EVC）および OAM マネージャを設定し、EVC を CFM と関連付ける必要があります。OAM マネージャとの相互作用には、アップ MEP を使用する必要があります。

（注）　UNI サービス タイプ、EVC、イーサネット サービス インスタンス、または CE-VLAN を設定、またはその設定を変更、削除する場合、すべての設定で、UNI サービス タイプが EVC 設定と一致しており、イーサネット サービス インスタンスが CE-VLAN 設定と一致していることを確認します。それらのペアが一致しない場合、設定は拒否されます。

OAM マネージャの設定

PE デバイス上で OAM マネージャを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ethernet cfm domain** *domain-name* **level** *level-id*	CFM ドメインを定義して、ドメイン レベルを設定し、ドメインで ethernet-cfm コンフィギュレーション モードを開始します。メンテナンス レベルに指定できる数の範囲は 0 ～ 7 です。
ステップ 3	**service** *csi-id* **vlan** *vlan-id*	メンテナンス ドメイン内の普遍的に一意の CSI および VLAN ID を定義します。 • *csi-id* : CSI を識別する 100 文字以下の文字列 • *vlan-id* : 指定できる VLAN の範囲は 1 ～ 4095 です。同じレベルの複数のドメインに同じ VLAN ID は使用できません。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ethernet evc** *evc-id*	EVC を定義して、EVC コンフィギュレーション モードを開始します。
ステップ 6	**oam protocol cfm svlan** *vlan-id* **domain** *domain-name*	EVC OAM プロトコルを CFM として設定し、ステップ 2 および 3 で設定された CFM ドメインのメンテナンス レベルの Service Provider VLAN-ID（S-VLAN-ID）を識別します。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	OAM マネージャでモニタリングする他の CFM ドメインを定義するには、ステップ 2 ～ 7 を繰り返します。	
ステップ 9	**ethernet cfm enable**	CFM をグローバルにイネーブルにします。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

イーサネット OAM のイネーブル化

インターフェイス上でイーサネット OAM をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイスをイーサネット OAM インターフェイスとして設定するように定義して、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *seconds* | **mode** {**active** | **passive**} | **timeout** *seconds*]	インターフェイス上でイーサネット OAM をイネーブルにします。 • （任意）**max-rate** *oampdus* を入力して、OAM PDU を送信する最大レート（1 秒単位）を設定します。指定できる範囲は 1 ～ 10 PDU/ 秒です。デフォルトは 10 です。 • （任意）**min-rate** *seconds* を入力して最大レートを秒数で入力します。指定できる範囲は 1 ～ 10 秒です。 • （任意）OAM クライアントを **mode** as **active** *or* **passive** として設定します。デフォルト値は **active** です。 • （任意）**timeout** *seconds* を入力して、デバイスにより OAM ピアが動作不能と宣言され、そのステート マシンがリセットされてから経過する時間を設定します。指定できる範囲は 2 ～ 30 秒で、デフォルトは 5 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 6	**show ethernet cfm maintenance points remote**	（任意）イーサネット OAM で報告されているポート ステートを表示します。

イーサネット OAM および CFM 設定の例

次に、サンプルのサービス プロバイダー ネットワークでのイーサネット OAM と CFM 間のインターワーキングの設定例を示します。PE スイッチは各エンド ポイントで CE スイッチに接続されています。CE スイッチおよび PE スイッチ間で CFM、E-LMI、およびイーサネット OAM を設定する必要があります。

CE スイッチ 1（CE1）の設定

```
Switch# config t
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport trunk allowed vlan 10
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# exit
```

PE スイッチ 1（PE1）の設定

```
Switch# config t
Switch(config)# interface gigabitethernet0/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 100 vlan 10
Switch(config-if)# ethernet uni id 2004-20
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# service instance 10 ethernet BLUE
Switch(config-if-srv)# ethernet lmi ce-vlan map 10
```

```
Switch(config-if-srv)# exit
```

PE スイッチ 2（PE2）の設定

```
Switch# config t
Switch(config)# interface gigabitethernet1/20
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 101 vlan 10
Switch(config-if)# ethernet uni id 2004-20
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# service instance 10 ethernet BLUE
Switch(config-if-srv)# ethernet lmi ce-vlan map 10
Switch(config-if-srv)# exit
```

CE スイッチ 2（CE2）の設定

```
Switch# config t
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport trunk allowed vlan 10
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# exit
```

次に、設定の PE スイッチ ポート ステータスを表示する出力の例を示します。ポート ステータスは両方のスイッチで *UP* と表示されています。

スイッチ PE1：

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
101 * 4     0015.633f.6900 10   UP          Gi0/1         27       blue
```

スイッチ PE2：

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
100 * 4     0012.00a3.3780 10   UP          Gi0/1         8        blue
Total Remote MEPs: 1
```

次に、CE1（または PE1）でリモート ループバックを開始する場合の出力例を示します。リモート PE スイッチのポート ステートは *Test* と表示され、リモート CE スイッチは error-disable モードになります。

```
Switch# ethernet oam remote-loopback start interface gigabitEthernet 0/1
This is a intrusive loopback.
Therefore, while you test Ethernet OAM MAC connectivity,
you will be unable to pass traffic across that link.
Proceed with Remote Loopback? [confirm]
```

スイッチ PE1：

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
101 * 4     0015.633f.6900 10   UP        Gi0/1         27       blue
```

スイッチ PE2：

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
100 * 4     0012.00a3.3780 10   TEST      Gi1/1/1         8        blue
Total Remote MEPs: 1
```

さらに、PE1 に接続する CE1 インターフェイス をシャットダウンすると、リモート PE2 ポートの PortState は *Down* と表示されます。

CHAPTER 44

IP マルチキャスト ルーティングの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに IP マルチキャスト ルーティングを設定する方法について説明します。IP マルチキャストは、ネットワークのリソースをより効率的に使用する方法です。特に、音声やビデオなど、帯域幅を消費するサービスに効果があります。IP マルチキャスト ルーティングを使用すると、ホスト（送信元）は IP *マルチキャスト グループ アドレス*と呼ばれる特殊な形式の IP アドレスを使用し、IP ネットワーク内の任意の場所にあるホスト（レシーバー）のグループにパケットを送信できます。送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、マルチキャスト グループのメンバーに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。グループのメンバーであるかどうかに関係なく、すべてのホストはグループに送信できます。ただし、そのメッセージを受信できるのは、グループのメンバーだけです。

この機能を使用するには、スイッチでメトロ IP アクセス イメージが稼動している必要があります。

（注） この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』*Release 12.2* を参照してください。

この章で説明する内容は、次のとおりです。

- 「シスコの IP マルチキャスト ルーティングの実装の概要」（P.44-1）
- 「IP マルチキャスト ルーティングの設定」（P.44-9）
- 「高度な PIM 機能の設定」（P.44-36）
- 「オプションの IGMP 機能の設定」（P.44-39）
- 「オプションのマルチキャスト ルーティング機能の設定」（P.44-45）
- 「IP マルチキャスト ルーティングのモニタおよびメンテナンス」（P.44-48）

Multicast Source Discovery Protocol（MSDP）の設定の詳細については、第 45 章「MSDP の設定」を参照してください。

シスコの IP マルチキャスト ルーティングの実装の概要

スイッチは IP マルチキャスト ルーティングを実装するため、次のプロトコルをサポートしています。

- Internet Group Management Protocol（IGMP）は、LAN のホストおよび LAN のルータ（およびマルチレイヤ スイッチ）間で使用され、ホストがメンバーとして属するマルチキャスト グループを追跡します。

- Protocol-Independent Multicast（PIM）プロトコルは、ルータおよびマルチレイヤ スイッチ間で使用され、相互に転送されるマルチキャスト パケット、および直接接続された LAN に転送されるマルチキャスト パケットを追跡します。

IPv4 マルチキャスト標準に従って、MAC 宛先マルチキャスト アドレスは 0100:5e で始まり、IP アドレスの末尾の 23 ビットが付加されます。Cisco ME スイッチ上では、スイッチのマルチキャスト アドレスに一致しないマルチキャスト パケットは、次のように処理されます。

- マルチキャスト IP アドレスおよびユニキャスト MAC アドレスを含むパケットである場合は、ソフトウェア内で転送されます。これは、レガシー デバイス上の一部のプロトコルがマルチキャスト IP アドレスとユニキャスト MAC アドレスを併用するために起こります。
- マルチキャスト IP アドレスおよび一致しない MAC アドレスを含むパケットである場合は、廃棄されます。

ここでは、次の情報について説明します。

- 「IGMP の概要」（P.44-2）
- 「PIM の概要」（P.44-3）

IGMP の概要

IP マルチキャスティングに参加するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ スイッチで IGMP が動作している必要があります。このプロトコルは、クエリアおよびホストの役割を定義します。

- クエリアは、指定されたマルチキャスト グループに属するネットワーク デバイスを検出するためのクエリー メッセージを送信するネットワーク デバイスです。
- ホストは、クエリアにホスト メンバシップを通知するためのレポート メッセージ（クエリー メッセージに応答するメッセージ）を送信するレシーバーです。

同じ送信元からマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは IGMP メッセージを使用して、マルチキャスト グループに参加したり、脱退したりします。

グループのメンバーであるかどうかに関係なく、すべてのホストはグループに送信できます。ただし、そのメッセージを受信できるのは、グループのメンバーだけです。マルチキャスト グループのメンバシップはダイナミックです。ホストはいつでもグループに参加、また脱退できます。マルチキャスト グループの場所またはメンバー数に制限はありません。ホストは一度に複数のマルチキャストのメンバーになることができます。マルチキャスト グループのアクティブ状態および所属メンバーは、グループや時間によって変化し、マルチキャスト グループを長時間または短時間アクティブにすることもできます。グループのメンバシップはいつでも変更可能です。メンバーを含むグループにアクティビティがない場合もあります。

IP マルチキャスト トラフィックには、グループ アドレス（クラス D アドレス）が使用されます。クラス D アドレスの上位ビットは 1110 です。したがって、ホスト グループのアドレスは 224.0.0.0 ～ 239.255.255.255 の範囲となります。224.0.0.0 ～ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために確保されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは、次に示す IP マルチキャスト グループ アドレスを使用して送信されます。

- IGMP 汎用クエリアは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象グループの IP アドレスを宛先とします。
- IGMP グループ メンバシップ レポートは、レポート対象グループの IP アドレスを宛先とします。

- IGMPv2（IGMP バージョン 2）Leave メッセージは、アドレス 224.0.0.2（サブネット上のすべてのマルチキャスト ルータ）を宛先とします。古いホスト IP スタックの中には、Leave メッセージの宛先がすべてのルータのアドレスでなく、グループの IP アドレスであるものがあります。

IGMP バージョン 1

IGMPv1（IGMP バージョン 1）には主にクエリー応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤ スイッチは、ローカル サブネット上のどのマルチキャスト グループがアクティブであるか（マルチキャスト グループに関係するホストが 1 台または複数存在するか）を判別できます。IGMPv1 では別のプロセスを使用して、ホストをマルチキャスト グループに参加および脱退させることができます。詳細については、RFC 1112 を参照してください。

IGMP バージョン 2

IGMPv2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退遅延を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。また、この作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もルータに追加されます。詳細については、RFC 2236 を参照してください。

PIM の概要

PIM は*プロトコルに依存しないマルチキャスト*と呼ばれます。ユニキャスト ルーティング テーブルを読み込むために使用されるユニキャスト ルーティング プロトコルに関係なく、PIM はこのテーブルの情報を使用してマルチキャスト転送を実行します。マルチキャスト ルーティング テーブルは個別に維持されません。

PIM は、RFC 2362『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』で定義されています。次に示す Internet Engineering Task Force（IETF）インターネット ドラフトを参照してください。

- 『*Protocol Independent Multicast (PIM): Motivation and Architecture*』
- 『*Protocol Independent Multicast (PIM), Dense Mode Protocol Specification*』
- 『*Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*』
- 『*draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2*』
- 『*draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode*』

ここでは、PIM に関する次の内容について説明します。

- 「PIM のバージョン」（P.44-4）
- 「PIM のモード」（P.44-4）
- 「PIM スタブ ルーティング」（P.44-5）
- 「IGMP ヘルパー」（P.44-6）
- 「自動 RP」（P.44-6）
- 「BSR」（P.44-7）
- 「マルチキャスト転送およびリバース パス チェック」（P.44-7）

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ Rendezvous Point（RP; ランデブー ポイント）を持つアクティブな RP が 1 つ存在します。この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- Bootstrap Router（BSR; ブートストラップ ルータ）はフォールトトレラントな、自動化された RP ディスカバリ メカニズム、および配信メカニズムを提供します。これらのメカニズムにより、ルータおよびマルチレイヤ スイッチはグループ /RP マッピングをダイナミックに取得できます。
- Sparse Mode（SM; 希薄モード）および Dense Mode（DM; 稠密モード）は、インターフェイスではなく、グループに関するプロパティです。SM または DM のいずれか一方だけでなく、SM-DM（sparse-dense モード）を使用してください。
- PIM の Join メッセージおよび Prune メッセージを使用すると、複数のアドレス ファミリーを柔軟に符号化できます。
- 現在および今後の機能オプションを符号化するため、クエリー パケットではなく、より柔軟な hello パケット形式を使用しています。
- RP への登録メッセージが境界ルータによって送信されるか、あるいは指定ルータによって送信されるかは、メッセージ自身が指定します。
- PIM パケットは IGMP パケット内に格納されず、独立したパケットとして処理されます。

PIM のモード

PIM は Dense Mode（DM; 稠密モード）、Sparse Mode（SM; 希薄モード）、または PIM Sparse-Dense Mode（SM-DM）のいずれかのモードで動作します。PIM DM-SM では、sparse グループと dense グループの両方が同時に処理されます。

PIM DM

PIM DM では、送信元に基づくマルチキャスト配信ツリーが構築されます。DM の場合、PIM DM のルータまたはマルチレイヤ スイッチは、他のすべてのルータまたはマルチレイヤ スイッチで常にグループ宛てのマルチキャスト パケットが転送されると想定しています。直接接続されたメンバーまたは PIM ネイバが存在しない場合、PIM DM デバイスがマルチキャスト パケットを受信すると、Prune メッセージが送信元に送信され、不要なマルチキャスト トラフィックが停止されます。このプルーニング済みブランチ上のこのルータまたはスイッチでは、後続のマルチキャスト パケットがフラッディングしません。レシーバーを含まないブランチが配信ツリーからプルーニングされ、レシーバーを含むブランチだけが存続するためです。

プルーニング済みのツリー内ブランチのレシーバーがマルチキャスト グループに新規に参加すると、PIM DM デバイスは新しいレシーバーを検出し、配信ツリーの送信元方向にすぐに接合メッセージを送信します。アップストリームの PIM DM デバイスが接合メッセージを受信すると、受信したデバイスは接合メッセージが着信したインターフェイスをすぐに転送ステートにし、マルチキャスト トラフィックのレシーバーへの転送を開始します。

PIM SM

PIM SM は共有ツリーおよび Shortest-Path-Trees（SPT）を使用し、マルチキャスト トラフィックをネットワーク内のマルチキャスト レシーバーに配信します。PIM SM の場合、ルータまたはマルチレイヤ スイッチは、トラフィックに関する明示的な要求（Join メッセージ）がないかぎり、他のルータまたはスイッチではグループ宛てのパケットが転送されないと想定します。IGMP を使用してホストが

マルチキャスト グループに参加すると、直接接続された PIM SM デバイスは、RP と呼ばれるルートに向けて PIM Join メッセージを送信します。この Join メッセージはルートに向かってルータを順次移動しながら、共有ツリーのブランチを作成します。

RP はマルチキャスト レシーバーを追跡します。また、送信元の先頭ホップ ルータ（*Designated Router（指定ルータ）*[DR]）から受信した登録メッセージを使用して送信元を登録し、送信元からレシーバーへの共有ツリー パスを完成させます。共有ツリーを使用する場合、送信元は RP にトラフィックを送信し、これらのトラフィックをすべてのレシーバーに到達させるようにする必要があります。

マルチキャスト グループ トラフィックをプルーニングする場合は、Prune メッセージが配信ツリーの上方向に送信されます。この結果、明示的な Join メッセージによって作成された共有ツリーまたは SPT のブランチが不要になった場合、これらを解除することが可能となります。

PIM スタブ ルーティング

PIM のスタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの使用状況を低減させます。

PIM スタブ ルーティングを使用するネットワークでは、ユーザへの IP トラフィックが使用可能な唯一のルートは、PIM スタブ ルーティングが設定されているスイッチ経由のルートです。PIM 受動インターフェイスは VLAN などのレイヤ 2 アクセス ドメイン、または他の レイヤ 2 デバイスに接続されているインターフェイスに接続されます。レイヤ 2 アクセス ドメインでは、直接接続されたマルチキャスト（IGMP）レシーバーおよび送信元だけが許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

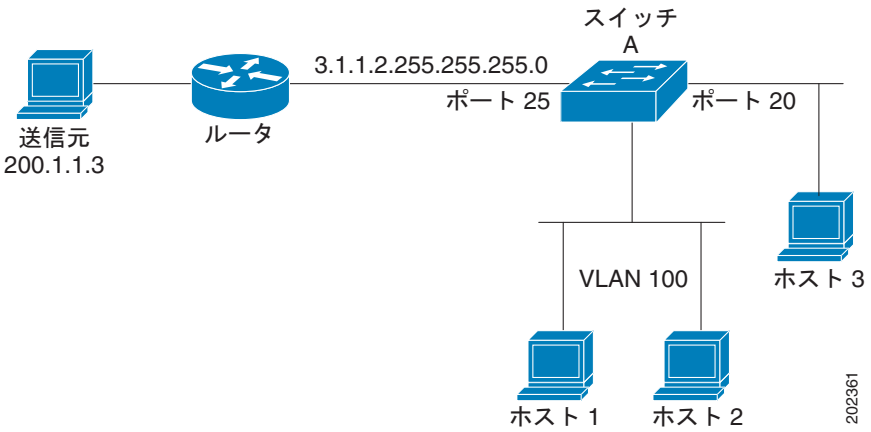
PIM スタブ ルーティングを使用している場合は、分散ルータおよびリモート ルータが IP マルチキャスト ルーティングを使用するように設定して、スイッチだけを PIM スタブ ルータとして設定します。スイッチは、分散ルータ間の伝送トラフィックはルーティングしません。また、スイッチ上のルーティングされたアップリンク ポートの設定も必要です。スイッチのアップリンク ポートは SVI では使用できません。SVI アップリンク ポートの PIM が必要な場合は、IP サービス機能セットへのアップグレードが必要です。

スイッチで PIM スタブ ルーティングを設定する場合は、EIGRP スタブ ルーティングも設定する必要があります。詳細については、「EIGRP スタブ ルーティングの設定」（P.36-43）を参照してください。

冗長 PIM スタブ ルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合は、冗長トポロジーが存在します。PIM メッセージはブロックされ、PIM アサート ルータおよび指定ルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけをサポートします。非冗長トポロジーを使用することで、PIM 受動インターフェイスはアクセス ドメイン内で唯一のインターフェイスおよび指定ルータであると想定します。

図 44-1 では、スイッチ A のルーテッド アップリンク ポート 25 がルータに接続されており、VLAN 100 インターフェイスおよびホスト 3 では PIM スタブ ルーティングがイネーブルに設定されています。このコンフィギュレーションでは、直接接続されたホストがマルチキャスト送信元である 200.1.1.3 からトラフィックを受信できます。詳細については、「PIM スタブ ルーティングの設定」（P.44-13）を参照してください。

図 44-1　PIM スタブ ルータ コンフィギュレーション



IGMP ヘルパー

PIM スタブ ルーティングによって、ルーテッド トラフィックがエンド ユーザの近くに移動し、ネットワーク トラフィックを低減します。また、スタブ ルータ（スイッチ）に IGMP ヘルパー機能を持たせることでも、トラフィックを低減できます。

igmp helper help-address インターフェイス コンフィギュレーション コマンドを使用してスタブ ルータ（スイッチ）を設定し、スイッチによるネクストホップ インターフェイスへのレポート送信をイネーブルに設定できます。ダウンストリーム ルータに直接接続されていないホストは、アップストリーム ネットワークの送信元のマルチキャスト グループに参加できます。この機能が設定されていると、マルチキャスト ストリームに参加したいホストからの IGMP パケットは、アップストリームのネクストホップ デバイスへ転送されます。アップストリームのセントラル ルータがヘルパー IGMP レポート または Leave を受信すると、そのグループの発信インターフェイス リストからインターフェイスを追加または削除します。

ip igmp helper-address コマンドの構文および使用方法の詳細については、『*Cisco IOS IP and IP Routing Command Reference*』*Release 12.1* を参照してください。

自動 RP

この独自の機能により、ネットワーク内のルータまたはマルチレイヤ スイッチごとに RP 情報を手動で設定する必要がなくなります。自動 RP を機能させるには、シスコのルータまたはマルチレイヤ スイッチをマッピング エージェントとして設定します。マッピング エージェントは IP マルチキャストを使用して、候補 RP アナウンスメントを受信する候補 RP として設定可能なネットワーク内のルータまたはスイッチを取得します。候補 RP はマルチキャスト RP アナウンス メッセージを特定のグループまたはグループ範囲に定期的に送信し、それらが使用可能であることをアナウンスします。

マッピング エージェントはこれらの候補 RP アナウンスメントをリスニングし、この情報を使用して、グループ /RP マッピング キャッシュにエントリを作成します。受信されたグループ /RP 範囲に対して複数の候補 RP が RP アナウンスメントを送信した場合でも、この範囲には 1 つのマッピング キャッシュ エントリだけが作成されます。RP アナウンス メッセージ着信時に、マッピング エージェントは IP アドレスが最大であるルータまたはスイッチをアクティブ RP として選択し、この RP アドレスをグループ /RP マッピング キャッシュ内に保存します。

マッピング エージェントは、グループ /RP マッピング キャッシュの内容を定期的にマルチキャストします。このため、すべてのルータおよびスイッチで、サポート対象のグループに使用される RP が自動的に検出されます。ルータまたはスイッチが RP ディスカバリ メッセージの受信に失敗し、グループ /RP マッピング情報が期限切れになると、ルータまたはスイッチは、**ip pim rp-address** グローバル コ

ンフィギュレーション コマンドによって定義された、スタティックに設定された RP に切り替わります。スタティックに設定された RP が存在しない場合、ルータまたはスイッチはグループの動作を DM に変更します。

複数の RP がさまざまなグループ範囲として、または互いのホット バックアップとして機能します。

BSR

PIMv2 BSR は、グループ /RP マッピング情報をネットワーク内のすべての PIM ルータおよびマルチレイヤ スイッチに配信する別の方法です。これにより、ネットワーク内のルータまたはスイッチごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ /RP マッピング情報を配信する代わりに、特殊な BSR メッセージをホップバイホップでフラッディングしてマッピング情報を配信します。

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよびスイッチから選択されます。選択メカニズムは、ブリッジングされた LAN で使用されるルートブリッジ選択メカニズムに似ています。BSR の選択の基準は、ネットワークを経由してホップバイホップで送信される BSR メッセージに格納されている、デバイスの BSR プライオリティです。各 BSR デバイスは BSR メッセージを調べ、自身の BSR プライオリティよりも BSR プライオリティが同等以上で、BSR IP アドレスが大きなメッセージだけを、すべてのインターフェイスから転送します。この方法によって、BSR が選択されます。

選択された BSR は、Time to Live（TTL; 存続可能時間）値が 1 である BSR メッセージを送信します。隣接する PIMv2 ルータまたはマルチレイヤ スイッチは BSR メッセージを受信し、TTL 値が 1 である他のすべてのインターフェイス（メッセージを受信したインターフェイスを除く）にマルチキャストします。この方法により、BSR メッセージは PIM ドメイン内をホップバイホップで移動します。BSR メッセージには現在の BSR の IP アドレスが格納されているため、候補 RP はフラッディング メカニズムを使用し、どのデバイスが選択された BSR であるかを自動的に認識します。

候補 RP は候補 RP アドバタイズを送信し、対象となるグループ範囲を BSR に指示します。この情報は、ローカルな候補 RP キャッシュに格納されます。BSR はドメイン内の他のすべての PIM デバイスに、BSR メッセージ内のこのキャッシュの内容を定期的にアドバタイズします。これらのメッセージはネットワークをホップバイホップで移動し、すべてのルータおよびスイッチに送信されます。BSR メッセージ内の RP 情報は、到達したルータおよびスイッチのローカルな RP キャッシュに格納されます。すべてのルータおよびスイッチには一般的な RP ハッシュ アルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

マルチキャスト転送およびリバース パス チェック

ユニキャスト ルーティングの場合、ルータおよびマルチレイヤ スイッチは、送信元から IP パケットの宛先アドレス フィールドに IP アドレスが格納されている宛先ホストへ、ネットワーク内の単一のパスに沿ってトラフィックを送信します。パス上の各ルータおよびスイッチはユニキャスト ルーティング テーブル内の宛先アドレスを参照し、指定されたインターフェイスを経由して、宛先方向のネクストホップへパケットを転送します。そのあと、パケット内の宛先 IP アドレスを使用して、ユニキャスト転送判断を行います。

マルチキャスティングの場合、送信元は IP パケットの宛先アドレス フィールドに格納された、マルチキャスト グループ アドレスで表されるホストの任意のグループにトラフィックを送信します。着信マルチキャスト パケットの転送または、廃棄を決定するため、ルータまたはマルチレイヤ スイッチで、パケットに対する Reverse Path Forwarding（RPF）チェックを実行します（図 44-2 を参照）。

1. ルータまたはマルチレイヤ スイッチは着信したマルチキャスト パケットの送信元アドレスを調べ、リバース パス上のインターフェイスに着信したパケットを送信元に戻すかどうかを決定します。

2. パケットが送信元に逆戻りするインターフェイスに着信した場合、RPF チェックは成功し、発信インターフェイス リスト内のすべてのインターフェイス（ルータのすべてのインターフェイスとは限りません）にパケットが転送されます。

3. RPF チェックに失敗した場合、パケットは廃棄されます。

一部のマルチキャスト ルーティング プロトコルでは、マルチキャスト ルーティング テーブルは個別に維持され、RPF チェックに使用されます。ただし、PIM では RPF チェックを実行するためにユニキャスト ルーティング テーブルが使用されます。

図 44-2 に送信元 151.10.3.21 からのマルチキャスト パケットを受信するポート 2 を示します。表 44-1 は、送信元へのリバース パス上にあるポートは、ポート 2 ではなくポート 1 であることを示しています。RPF チェックが失敗したため、マルチレイヤ スイッチはパケットを破棄します。送信元 151.10.3.21 からの別のマルチキャスト パケットは、ポート 1 に着信します。ルーティング テーブルにより、このポートは送信元へのリバース パス上にあることがわかります。RPF チェックに合格したため、パケットは発信ポート リスト内のすべてのポートに転送されます。

図 44-2　　RPF チェック

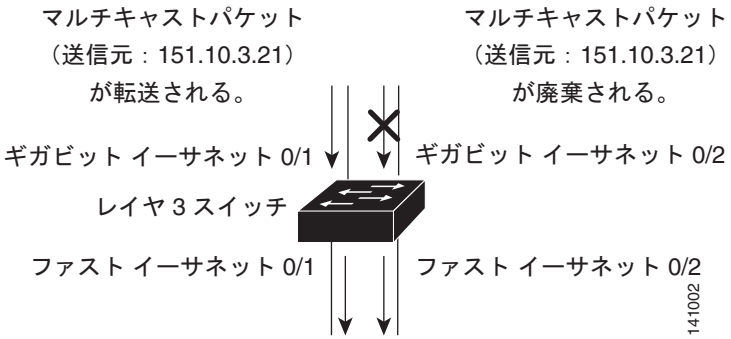


表 44-1　　RPF チェックのルーティング テーブル例

ネットワーク	ポート
151.10.0.0/16	ギガビット イーサネット 0/1
198.14.32.0/32	ファスト イーサネット 0/1
204.1.16.0/24	ファスト イーサネット 0/2

PIM は送信元ツリーと RP でルーティングされた共有ツリーを使用して、データグラムを転送します（「PIM DM」（P.44-4）および「PIM SM」（P.44-4）を参照）。RPF チェックは、それぞれ異なる方法で実行されます。

- PIM ルータまたはマルチレイヤ スイッチが送信元ツリー ステートである場合（つまり（S,G）エントリがマルチキャスト ルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤ スイッチが共有ツリー ステートである場合（および送信元ツリー ステートが明示されていない場合）、（メンバーがグループに参加している場合は既知である）RP アドレスについて RPF チェックが実行されます。

PIM SM は RPF 参照機能を使用し、Join メッセージおよび Prune メッセージを送信する必要があるかどうかを判断します。

- （S,G）Join メッセージ（送信元ツリー ステート）は送信元に向け送信されます。
- （*,G）Join メッセージ（共有ツリー ステート）は RP に向け送信されます。

DM PIM では送信元ツリーだけが使用され、上記のように RPF が使用されます。

IP マルチキャスト ルーティングの設定

- 「マルチキャスト ルーティングのデフォルト設定」（P.44-9）
- 「マルチキャスト ルーティング設定時の注意事項」（P.44-9）
- 「基本的なマルチキャスト ルーティングの設定」（P.44-11）（必須）
- 「PIM スタブ ルーティングの設定」（P.44-13）（任意）
- 「Source-Specific Multicast の設定」（P.44-15）
- 「Source Specific Multicast マッピングの設定」（P.44-18）
- 「RP の設定」（P.44-24）（インターフェイスが SM-DM モードで、グループを sparse（希薄）グループとして扱う場合に必須）
- 「自動 RP および BSR の使用法」（P.44-34）（他社製の PIMv2 デバイスをシスコ製 PIM v1 デバイスと相互運用する場合に必須）
- 「RP マッピング情報のモニタ」（P.44-35）（任意）
- 「PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング」（P.44-35）（任意）

マルチキャスト ルーティングのデフォルト設定

表 44-2 に、マルチキャスト ルーティングのデフォルト設定を示します。

表 44-2　マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	全インターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM RP アドレス	設定なし。
PIM ドメイン境界	ディセーブル。
PIM マルチキャスト境界	なし
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 キロビット / 秒
PIM ルータ クエリー メッセージ インターバル	30 秒

マルチキャスト ルーティング設定時の注意事項

- 「PIMv1 および PIMv2 の相互運用性」（P.44-10）
- 「自動 RP および BSR 設定時の注意事項」（P.44-10）

PIMv1 および PIMv2 の相互運用性

シスコの PIMv2 実装機能を使用すると、バージョン 1 とバージョン 2 間での相互運用性および変換が可能となります。ただし、若干の問題が発生する場合もあります。

PIMv2 に付加的にアップグレードできます。PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤ スイッチに設定できます。内部的には、共有メディア ネットワーク上のすべてのルータおよびマルチレイヤ スイッチで同じ PIM バージョンを実行する必要があります。したがって、PIMv2 デバイスが PIMv1 デバイスを検出した場合は、バージョン 1 デバイスがシャットダウンするかアップグレードされるまで、バージョン 2 デバイスはバージョン 1 にダウングレードされます。

PIMv2 は BSR を使用して各グループ プレフィクスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ スイッチにアナウンスします。自動 RP 機能を組み合せることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。ただし、自動 RP は PIMv1 から独立している、スタンドアロンのシスコ独自のプロトコルで、PIMv2 は IETF 標準の追跡プロトコルです。したがって、PIMv2 の使用を推奨します。BSR メカニズムは、シスコのルータおよびマルチレイヤ スイッチ上の自動 RP と相互運用します。詳細については、「自動 RP および BSR 設定時の注意事項」（P.44-10）を参照してください。

PIMv2 デバイスを PIMv1 デバイスと相互運用させる場合は、自動 RP を事前に導入しておく必要があります。自動 RP マッピング エージェントでもある PIMv2 BSR は、自動 RP で選択された RP を自動的にアドバタイズします。つまり、自動 RP によって、グループ内のルータまたはマルチレイヤごとに 1 つの RP が設定されます。ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 と PIMv2 が混在する領域内の DM グループは、特殊な設定を行わなくても自動的に相互運用します。

PIMv1 の自動 RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に SM グループを設定できます。すべての PIMv2 デバイスで PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。PIMv2 への変換を簡単に行うための推奨事項は次のとおりです。

- 領域全体で自動 RP を使用します。
- 領域全体で SM-DM を設定します。

自動 RP がまだ PIMv1 領域に設定されていない場合は、自動 RP を設定してください。詳細については、「自動 RP の設定」（P.44-26）を参照してください。

自動 RP および BSR 設定時の注意事項

PIMv2 は 2 つの方法で使用できます。1 つはバージョン 2 をネットワーク内で排他的に使用する方法、もう 1 つは PIM バージョンの混在環境を採用してバージョン 2 に移行する方法です。

- 使用しているネットワークがすべてシスコ ルータおよびマルチレイヤ スイッチである場合は、自動 RP または BSR のいずれかを使用できます。
- ネットワークに他社製のルータがある場合は、BSR を使用する必要があります。
- シスコの PIMv1 および PIMv2 ルータとマルチレイヤ スイッチ、および他社製のルータがある場合は、自動 RP と BSR の両方を使用する必要があります。ネットワークに他のベンダー製のルータが含まれる場合には、シスコの PIMv2 デバイス上に自動 RP マッピング エージェントと BSR を設定します。BSR と他社製の PIMv2 デバイス間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。

- ブートストラップ メッセージはホップバイホップで送信されるため、PIMv1 デバイスの場合、これらのメッセージはネットワーク内の一部のルータおよびマルチレイヤ スイッチに到達しません。このため、ネットワーク内に PIMv1 デバイスがあり、シスコ ルータおよびマルチレイヤ スイッチだけが存在する場合は、自動 RP を使用してください。
- ネットワーク内に他社製のルータが存在する場合は、シスコ PIMv2 ルータまたはマルチレイヤ スイッチに自動 RP マッピング エージェントおよび BSR を設定します。BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 デバイスを、自動 RP マッピング エージェントと BSR の両方に設定してください。詳細については、「自動 RP および BSR の使用法」（P.44-34）を参照してください。

基本的なマルチキャスト ルーティングの設定

IP マルチキャスト ルーティングをイネーブルにし、PIM バージョンおよび PIM モードを設定する必要があります。これにより、ソフトウェアはマルチキャスト パケットを転送し、スイッチがそのマルチキャスト ルーティング テーブルを読み込むことができます。

（注）　IP マルチキャストをイネーブルにするには、スイッチでメトロ IP アクセス イメージが稼動している必要があります。

インターフェイスは PIM DM、SM、または SM-DM のいずれかに設定できます。スイッチはモード設定に従って、マルチキャスト ルーティング テーブルを読み込み、直接接続された LAN から受信したマルチキャスト パケットを転送します。IP マルチキャスト ルーティングを実行するには、インターフェイスに対して、これらの PIM モードのいずれかをイネーブルにする必要があります。インターフェイスで PIM をイネーブルにすると、同じインターフェイス上で IGMP 処理もイネーブルになります。

（注）　複数のインターフェイス上で PIM をイネーブルにした場合に、そのほとんどのインターフェイスが発信インターフェイス リストになく、IGMP スヌーピングがディセーブルになっている場合、余分で不要なレプリケーションによって発信インターフェイスはマルチキャスト トラフィックの回線速度を維持できない場合があります。

マルチキャスト ルーティング テーブルへのパケット読み込みでは、DM インターフェイスは常にテーブルに追加されます。SM インターフェイスがテーブルに追加されるのは、ダウンストリーム デバイスから定期的な Join メッセージを受信した場合、またはインターフェイスに直接接続されたメンバーが存在する場合に限ります。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。認識している RP がなければ、パケットは DM 方式でフラッディングされます。特定の送信元からのマルチキャスト トラフィックが十分であれば、レシーバーの先頭ホップ ルータからその送信元に Join メッセージが送信され、送信元を基点とする配信ツリーが構築されます。

デフォルトでは、マルチキャスト ルーティングはディセーブルとなっており、モードは設定されていません。この手順は必須です。

IP マルチキャストをイネーブルにし、PIM バージョンおよび PIM モードを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip multicast-routing distributed**	IP マルチキャストによる分散スイッチングをイネーブルにします。
ステップ 3	**interface** *interface-id*	マルチキャスト ルーティングをイネーブルにするレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN（仮想 LAN）インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。詳細については、「レイヤ 3 インターフェイスの設定」（P.10-27）を参照してください。
ステップ 4	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 5	**ip pim version** [**1** | **2**]	インターフェイスに PIM バージョンを設定します。 デフォルトでは、バージョン 2 がイネーブルです（推奨設定）。 PIMv2 モードのインターフェイスに PIMv1 ネイバが存在する場合、インターフェイスは自動的に PIMv1 モードにダウングレードされます。バージョン 1 のすべてのネイバがシャットダウンするかアップグレードされると、インターフェイスはバージョン 2 モードに戻ります。 詳細については、「PIMv1 および PIMv2 の相互運用性」（P.44-10）を参照してください。

	コマンド	目的
ステップ 6	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}	インターフェイスで PIM モードをイネーブルにします。 デフォルトで、モードは設定されていません。 キーワードの意味は次のとおりです。 • **dense-mode**：DM 動作をイネーブルにします。 • **sparse-mode**：SM 動作をイネーブルにします。SM を設定する場合は、RP も設定する必要があります。詳細については、「RP の設定」（P.44-24）を参照してください。 • **sparse-dense-mode**：グループが属するモードでインターフェイスが処理されます。DM-SM 設定を推奨します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

マルチキャスティングをディセーブルにするには、**no ip multicast-routing distributed** グローバル コンフィギュレーション コマンドを使用します。デフォルトの PIM バージョンに戻すには、**no ip pim version** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで PIM をディセーブルにするには、**no ip pim** インターフェイス コンフィギュレーション コマンドを使用します。

PIM スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。サポート対象のインターフェイスは、アップリンク PIM インターフェイスと PIM 受動インターフェイスの 2 種類です。PIM 受動モードが設定されたルーテッド インターフェイスは、PIM 制御トラフィックの通過または転送を許可しません。通過および転送されるのは IGMP トラフィックだけです。

PIM スタブ ルーティング設定時の注意事項

- PIM スタブ ルーティングの設定前には、スタブ ルータとセントラル ルータの両方に IP マルチキャスト ルーティングが設定されている必要があります。また、スタブ ルータのアップリンク インターフェイスに PIM モード（dense-mode、sparse-mode、または dense-sparse-mode）が設定されている必要があります。
- PIM スタブ ルータはディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト（EIGRP）スタブ ルーティングでは、この動作が強制されます。PIM スタブ ルーティングの動作をユニキャスト スタブ ルーティングが支援するように設定する必要があります。詳細については、「EIGRP スタブ ルーティングの設定」（P.36-43）を参照してください。
- レイヤ 2 アクセス ドメインでは、直接接続されたマルチキャスト（IGMP）レシーバーおよび送信元だけが許可されます。アクセス ドメインでは PIM プロトコルはサポートされません。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。

PIM スタブ ルーティングのイネーブル化

インターフェイス上で PIM スタブ ルーティングをイネーブルに設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	PIM スタブ ルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim passive**	インターフェイスで PIM スタブ機能を設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip pim interface**	各インターフェイスでイネーブルになっている PIM スタブを表示します。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスで PIM スタブ ルーティングをディセーブルにするには、**no ip pim passive** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、IP マルチキャスト ルーティングがイネーブルに設定されて、スイッチ A の PIM アップリンク ポート 25 が **spare-dense-mode** がイネーブルに設定されたルーテッド アップリンク ポートとして設定されています。図 44-1 では、VLAN 100 インターフェイスおよびギガビット イーサネット ポート 20 で PIM スタブ ルーティングがイネーブルに設定されています。

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet0/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/20
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/20
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

各インターフェイスで PIM スタブがイネーブルに設定されていることを確認するには、**show ip pim interface** 特権 EXEC コマンドを使用します。

```
Switch# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet0/20 v2/P 0 30 1 10.1.1.1
```

これらの特権 EXEC コマンドを使用して、PIM スタブ コンフィギュレーションおよびステータスの情報を表示します。

- **show ip pim interface** を実行すると、各インターフェイスでイネーブルに設定されている PIM スタブを表示します。
- **show ip igmp detail** を実行すると、特定のマルチキャスト送信元グループに参加した対象クライアントを表示します。
- **show ip igmp mroute** を実行すると、送信元から対象クライアントにマルチキャスト ストリームが転送されることを確認します。

Source-Specific Multicast の設定

ここでは、Source-Specific Multicast（SSM）の設定方法を説明します。ここで説明する SSM コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』の「IP Multicast Routing Commands」の章を参照してください。この章で言及する他のコマンドについては、コマンド リファレンス マスター インデックス（オンライン検索）を使用して、該当するマニュアルを検索してください。

SSM 機能は IP マルチキャストの拡張機能です。この機能を使用すると、レシーバーに転送されるデータグラム トラフィックは、レシーバーが明示的に参加しているマルチキャスト送信元からのトラフィックだけになります。SSM に設定されたマルチキャスト グループでは、SSM 配信ツリー（共有ツリーは存在しない）だけが作成されます。

SSM コンポーネントの概要

SSM は、1 対多のアプリケーション（ブロードキャスト アプリケーション）のサポートに最適なデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの実装の中核をなすネットワーキング テクノロジーです。このスイッチは、SSM の実装に対応する次のコンポーネントをサポートしています。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）

  PIM-SSM は、SSM の実装をサポートするルーティング プロトコルであり、PIM Sparse Mode（PIM-SM）に基づいています。

- Internet Group Management Protocol version 3（IGMPv3）

  IGMPv3 で SSM を実行するには、シスコ IOS ルータ、アプリケーションが稼動しているホスト、およびアプリケーション自体が SSM をサポートしている必要があります。

Internet Standard Multicast と SSM の相違点

インターネットの現行の IP マルチキャスト インフラストラクチャや多くの企業のイントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。これらのプロトコルには、Internet Standard Multicast（ISM）サービス モデルの限界があります。たとえば、ISM を使用すると、ネットワークは、アクティブにマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。

ISM サービスは、任意の送信元から、マルチキャスト ホスト グループと呼ばれるレシーバーのグループへの IP データグラムの配信によって構成されます。マルチキャスト ホスト グループへのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス S と、IP 宛先アドレスとしてのマルチキャスト グループ アドレス G のデータグラムで構成されます。システムは、ホスト グループのメンバーになることによりこのトラフィックを受信します。

ホスト グループのメンバシップに必要なのは、IGMP version 1、2 または 3 によるホスト グループのシグナリングだけです。SSM では、データグラムの配信は（S, G）チャネルに基づいて行われています。SSM と ISM のいずれでも、送信元になるのにシグナリングは不要です。ただし、SSM では、レシーバーは特定の送信元からのトラフィックを受信する、または受信しないために、（S, G）チャネルへの参加または脱退を行う必要があります。つまり、レシーバーは参加している（S, G）チャネルからのトラフィックだけを受信できます。一方 ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを知る必要はありません。推奨されているチャネル参加シグナリングの標準的な方法では、IGMP include モード メンバシップ レポートを使用しています。ただし、このレポートをサポートしているのは IGMP version 3 だけです。

SSM IP アドレスの範囲

SSM 配信モデルを、IP マルチキャストのグループ アドレス範囲の設定済みのサブセットに適用することにより、SSM ISM サービスを一緒に使用できます。Cisco IOS ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 までの IP マルチキャスト アドレス範囲で SSM を設定できます。SSM 範囲が定義されている場合、既存の IP マルチキャスト レシーバー アプリケーションは、SSM 範囲内のアドレスを使おうとしてもトラフィックを受信できません（ただし、明示的な（S, G）チャネル参加を使用するようアプリケーションが変更されている場合を除く）。

SSM の動作

IIP マルチキャスト サービスが PIM-SM に基づいている設立されているネットワークは、SSM サービスをサポートできます。SSM サービスだけが必要とされている場合は、ドメイン間の PIM-SM に必要な全プロトコル範囲（たとえば、MSDP、自動 RP、またはブートストラップ ルータ [BSR]）が存在しない場合も、単独で SSM をネットワークに配置できます。

PIM-SM 用に設定されているネットワークに SSM を配置する場合、ラストホップ ルータだけが SSM をサポートします。レシーバーに直接接続されていないルータは、SSM のサポートが不要です。一般的には、ラストホップ以外のルータは、SSM 範囲内では PIM-SM だけを実行します。SSM 範囲内の MSDP シグナリング、登録、または PIM-SM 共有ツリーの動作を抑制するには、他のアクセス制御設定が必要である場合があります。

SSM 範囲を設定し、イネーブルにするには、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用します。この設定による影響は次のとおりです。

- SSM 範囲内のグループは、IGMPv3 include モード メンバシップ レポートを通じて（S, G）チャネルに参加できます。
- SSM アドレス範囲内の PIM 動作は PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、PIM（S, G）の Join および Prune メッセージだけがルータによって生成され、（S, G）の Rendezvous Point Tree（RPT）や（*, G）RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視または拒否されます。着信 PIM 登録メッセージは register-stop メッセージで即座に応答されます。ラストホップ ルータ以外では、PIM-SSM は PIM-SM との下位互換性があります。したがって、ラストホップ以外のルータは SSM グループで PIM-SM を実行できます（たとえば、まだ SSM をサポートしていない場合など）。
- SSM 範囲内の MSDP Source-Active（SA）メッセージは、受け入れ、生成、転送のいずれも実行されません。

IGMPv3 ホスト シグナリング

IGMPv3 では、ホストはマルチキャスト グループのラストホップ ルータへメンバシップ シグナルを送信します。ホストは、グループ メンバシップのシグナル送信時に、送信元に対するフィルタリング機能を使用できます。ホストは、いくつかの特定の送信元を除く、すべての送信元からグループへのトラフィックを受信する（exclude モード）、または、特定の送信元からグループへのトラフィックだけを受信する（include モード）といういずれかのシグナルを送信できます。

IGMPv3 は、ISM および SSM の両方で動作できます。ISM では、exclude モードおよび include モードの両方のレポートを適用できます。SSM では、ラストホップ ルータは include モードのレポートだけを受け入れることができます。exclude モードのレポートは無視されます。

設定時の注意事項

SSM 範囲のレガシー アプリケーションに関する制約

ネットワーク内の SSM 以前の既存のアプリケーションは、(S, G）チャネル参加をサポートするように変更されない限り、SSM 範囲では機能しません。そのため、既存のアプリケーションが指定された SSM 範囲内のアドレスを使用している場合、ネットワークで SSM をイネーブルに設定すると問題が発生することがあります。

アドレス管理に関する制約

レイヤ 2 のスイッチング メカニズムとともに SSM を使用する場合、ある程度のアドレス管理が必要になります。Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）はグループ固有のフィリタリングだけをサポートしています。(S, G）チャネル固有のフィルタリングはサポートしません。スイッチド ネットワーク内の異なるレシーバーが、同じグループを共有している異なる（S, G）チャネルを要求した場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーもすべての（S, G）チャネル トラフィックを受信し、不要なトラフィックは入力時に除外します。SSM は、独立した多くのアプリケーションで SSM 範囲内のグループ アドレスを再利用できるため、このような状況はスイッチド ネットワークのトラフィック フィルタリング機能を低下させる可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲の単一アドレスが異なるアプリケーション間で再利用される可能性を低減することが重要です。たとえば、TV チャネル セットを提供するアプリケーション サービスは、SSM を使用している場合であっても、各 TV（S, G）チャネルに異なるグループを使用する必要があります。この設定により、同一アプリケーション内の異なるチャネルへの複数のレシーバーには、レイヤ 2 スイッチを含むネットワークではトラフィック エイリアシングが発生しなくなります。

IGMP スヌーピングおよび CGMP の制限

IGMPv3 で使用される新しいメンバシップ レポート メッセージは、古い IGMP スヌーピング スイッチでは正しく認識されない場合があります。

IGMP のスイッチング問題に関する詳細（特に CGMP について）は、「Configuring IP Multicast Routing」の章の Configuring IGMP Version 3 を参照してください。

ステート維持の制限

PIM-SSM では、インターフェイス上に適切な（S, G）参加が存在する場合、ラストホップ ルータは定期的に（S, G）Join メッセージを送信します。そのため、レシーバーが（S, G）参加を送信する限り、送信元が長時間（またはまったく）トラフィックを送信しなくても、レシーバーから送信元への Shortest Path Tree（SPT; 最短パスツリー）ステートは維持されます。

これは、送信元がトラフィックを送信していて、レシーバーがグループに参加している場合だけ（S, G）ステートが維持される PIM-SM とは対照的です。PIM-SM において、送信元からのトラフィック送信が途絶えてから 3 分を超えると、（S, G）ステートが削除され、再確立されるのはその送信元からのパケットが RPT を通じてサイド到着した場合だけです。PIM-SSM は送信元がアクティブであることをレシーバーに通知するメカニズムがないため、レシーバーがチャネルからの受信を要求している限り、ネットワークは PIM-SSM の（S, G）ステートを維持する必要があります。

SSM の設定

SSM を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**ip pim ssm** [**default** | **range** *access-list*]	IP マルチキャスト アドレスの SSM 範囲を定義します。
ステップ 2	**interface** type number	IGMPv3 がイネーブルに設定可能なホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim** {**sparse-mode** | **sparse-dense-mode**}	インターフェイスで PIM をイネーブルにします。**sparse mode** または **sparse-dense mode** のいずれかを使用する必要があります。
ステップ 4	**ip igmp version 3**	このインターフェイスに対して IGMPv3 をイネーブルにします。IGMP のバージョンは、デフォルトではバージョン 2 に設定されます。

SSM のモニタリング

SSM を監視するには、表 44-3 のコマンドを使用します。

表 44-3　SSM のモニタリング

コマンド	目的
show ip igmp groups detail	IGMPv3 による（S, G）チャネル参加を表示します。
show ip mroute	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートを受信したかどうかを表示します。

Source Specific Multicast マッピングの設定

Source Specific Multicast（SSM）マッピング機能は、管理上または技術上の理由からエンド システムにおける SSM のサポートが不可能または不要である場合、SSM 移行をサポートします。SSM マッピングを使用して、IGMPv3 をサポートしないレガシー STB へのビデオ配信や、IGMPv3 ホスト スタックを使用しないアプリケーションに SSM を活用できます。

ここでは、次の内容について説明します。

- 「設定時の注意事項および制限事項」（P.44-19）
- 「SSM マッピングの概要」（P.44-19）
- 「SSM マッピングの設定」（P.44-21）
- 「SSM マッピングのモニタリング」（P.44-23）

設定時の注意事項および制限事項

SSM マッピング設定時の注意事項を次に示します。

- SSM マッピングを設定する前に、IP マルチキャスト ルーティングおよび PIM Sparce Mode（SM; 希薄モード）をイネーブルに設定し、SSM を設定します。IP マルチキャスト ルーティングおよび PIM SM のイネーブル化の詳細については、「マルチキャスト ルーティングのデフォルト設定」（P.44-9）を参照してください。
- スタティック SSM マッピングを設定する場合は、事前に Access Control List（ACL; アクセス コントロール リスト）を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。ACL の設定の詳細については、第 32 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- SSM マッピングと DNS ルックアップを設定し使用する前には、稼動中の DNS サーバにレコードを追加できなければなりません。稼動中の DNS サーバがない場合は、インストールする必要があります。

  Cisco Network Registrar などの製品を使用できます。詳細は、次の URL を参照してください。

  http://www.cisco.com/warp/public/cc/pd/nemnsw/nerr/index.shtml

SSM マッピングには次のような制約があります。

- SSM マッピング機能は、完全な SSM のすべての利点を受けられるわけではありません。SSM マッピングは、ホストからグループ参加を取得し、このグループを 1 つ以上の送信元に関連付けられたアプリケーションと関連付けるため、各グループで 1 つのアプリケーションしかサポートできません。完全な SSM アプリケーションは、SSM マッピングと同様に同じグループを共有できます。
- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合、ラスト ホップ ルータの IGMPv3 をイネーブルに設定する場合は注意が必要です。SSM マッピングと IGMPv3 の両方をイネーブルに設定し、ホストが既に IGMPv3 をサポートしている（SSM は未サポート）場合、ホストは IGMPv3 グループ レポートを送信します。SSM マッピングはこれらの IGMPv3 グループ レポートはサポートしないため、ルータはこれらのレポートと送信元を正しく関連付けることができません。

SSM マッピングの概要

典型的な STB 配置では、各 TV チャネルは独立した 1 つの IP マルチキャスト グループを使用します。また、TV チャネルを送信するサーバ ホストも 1 つです。単一のサーバは複数の TV チャネルを送信できますが、各チャネルの送信先は別のグループとなります。このようなネットワーク環境で、ルータが特定のグループへの IGMpv1 または ICMPv2 メンバシップ レポートを受信した場合、レポートの送信先はマルチキャスト グループに関連付けられている TV チャネルの既知の TV サーバとなります。

SSM マッピングが設定されている環境で、ルータが特定のグループへの IGMPv1 または IGMPv2 メンバシップ レポートを受信した場合、ルータはこのレポートを、このグループに関連付けられている既知の送信元の 1 つ以上のチャネル メンバシップに変換します。

ルータがグループへの IGMPv1 または IGMPv2 メンバシップ レポートを受信した場合、ルータは SSM マッピングを使用してそのグループの 1 つ以上の送信元 IP アドレスを決定します。SSM マッピングはメンバシップ レポートを IGMPv3 レポートに変換し、IGMPv3 レポートを受信した場合と同様に続行します。その後、ルータが IGMPv1 または IGMPv2 メンバシップ レポートを受信し、グループの SSM マッピングが同じである限り、PIM join を送信し、このグループに参加し続けます。

ラスト ホップ ルータは、SSM マッピングを使用して、ルータのスティックに設定されたテーブルまたは DNS サーバを通じて送信元アドレスを決定できます。スタティックに設定されたテーブルまたは DNS マッピングが変更された場合、参加しているグループに関連付けられた現在の送信元からルータは脱退します。

SSM マッピングの詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

スタティック SSM マッピング

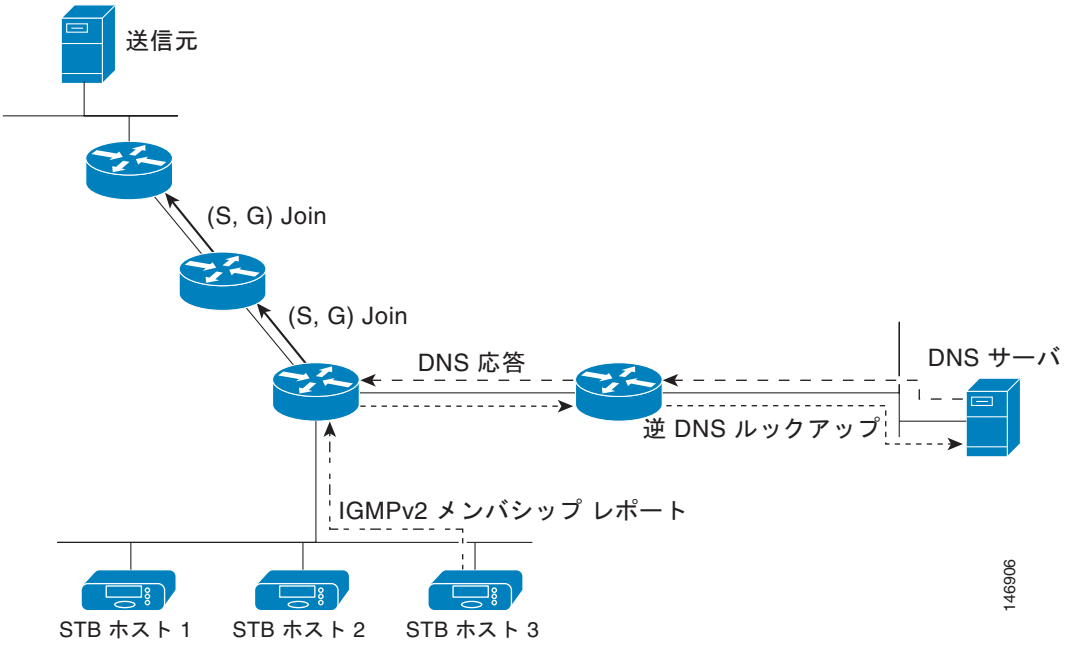
スタティック SSM マッピングでは、グループに送信している送信元を決定するためにスタティック マップを使用するよう、ラスト ホップ ルータを設定できます。スタティック SSM マッピングでは、グループ範囲の定義のために ACL を設定する必要があります。その後、**ip igmp static ssm-map** グローバル コンフィギュレーション コマンドを使用して、ACL に許可されたグループを送信元にマッピングできます。

DNS が不要、または DNS マッピングをローカルで上書きする場合、小規模ネットワークでスタティック SSM マッピングを設定できます。設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用して、ラスト ホップ ルータが逆 DNS ルックアップを実行するよう設定し、グループに送信する送信元を決定できます。DNS ベースの SSM マッピングが設定されると、ルータはグループ アドレスを含むドメイン名を構築し、DNS の逆ルックアップを実行します。ルータは IP アドレス リソース レコードを検索し、グループに関連付けられた送信元アドレスとして使用します。SSM マッピングは、グループごとに最大 20 の送信元をサポートしています。ルータは、グループに設定されているすべての送信元に参加します（図 44-3 を参照）。

図 44-3　DNS ベースの SSM マッピング



ラスト ホップ ルータが、グループに対して複数の送信元に参加することを可能にする SSM マッピング メカニズムによって、TV ブロードキャストの送信元に冗長性を持たせることができます。このコンテキストでは、ラスト ホップ ルータは SSM マッピングを使用して同じ TV チャネルの 2 つのビデオ送信元に同時に参加することで、冗長性を実現します。ただし、ラスト ホップ ルータによるビデオ トラフィックの重複を防ぐため、ビデオ送信元はサーバ側でスイッチオーバー メカニズムを使用する必

要があります。単一のビデオ送信元がアクティブ、もう一つのバックアップ ビデオ送信元はパッシブになります。パッシブな送信元は、アクティブな送信元の障害が検知されるまで待機し、障害が検知されるとビデオ トラフィックを TV チャネルに送信します。これによって、サーバ側のスイッチオーバー メカニズムにより常に 1 つのサーバだけがビデオ トラフィックを TV チャネルに送信することとなります。

G1、G2、G3、G4 を含むグループの 1 つ以上の送信元アドレスを検索するには、次の DNS レコードを DNS サーバで設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout]IN A source-address-1
    IN A source-address-2
    IN A source-address-n
```

DNS リソース レコードの設定に関する詳細は、DNS サーバのマニュアルを参照してください。SSM マッピングに関する詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

SSM マッピングの設定

- 「スタティック SSM マッピングの設定」（P.44-21）（必須）
- 「DNS ベースの SSM ルーティングの設定」（P.44-22）（必須）
- 「SSM マッピングを使用したスタティック トラフィック転送の設定」（P.44-23）（任意）

スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp ssm-map enable**	設定された SSM 範囲のグループに対する SSM マッピングをイネーブルに設定します。 **（注）** デフォルトでは、このコマンドにより DNS ベースの SSM マッピングがイネーブルになります。
ステップ 3	**no ip igmp ssm-map query dns**	（任意）DNS ベースの SSM マッピングをディセーブルにします。 **（注）** スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、**ip igmp ssm-map** グローバル コンフィギュレーション コマンドにより DNS ベースの SSM マッピングがイネーブルに設定されます。

	コマンド	目的
ステップ 4	**ip igmp ssm-map static** *access-list source-address*	スタティック SSM マッピングを設定します。 *access-list* に入力した ACL は、*source-address* に入力した送信元 IP アドレスにマッピングするグループを定義します。 **（注）** スタティック SSM マッピングを追加で設定することもできます。追加の SSM マッピングが設定されている場合、SSM 範囲に含まれるグループへの IGMPv1 または IGMPv2 メンバシップ レポートをルータが受信すると、スイッチは、設定されている各 **ip igmp ssm-map static** コマンドを使用して、グループに関連付けられた送信元アドレスを決定します。スイッチは、グループごとに最大 20 の送信元を関連付けます。
ステップ 5	必要に応じて、ステップ 4 を繰り返し、追加のスタティック SSM マッピングを設定します。	
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピング設定の例については、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

DNS ベースの SSM ルーティングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバ ゾーンを作成するか、既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用しているルータが、その DNS を他の目的でも使用している場合は、通常設定の DNS を使用する必要があります。ルータで使用されている DNS 実装が、DNS ベースの SSM マッピングだけである場合、ルート ゾーンが空であるか、自身を指すルートゾーンを含むフォールス DNS セットアップを設定できます。

DNS ベースの SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp ssm-map enable**	設定された SSM 範囲のグループに対する SSM マッピングをイネーブルに設定します。
ステップ 3	**ip igmp ssm-map query dns**	（任意）DNS ベースの SSM マッピングをイネーブルに設定します。 デフォルトでは、**ip igmp ssm-map** コマンドにより DNS ベースの SSM マッピングがイネーブルに設定されます。このコマンドの **no** 形式を使用した場合だけ、実行コンフィギュレーションに保存されます。 **（注）** DNS ベースの SSM マッピングがディセーブルに設定されている場合、DNS ベースの SSM マッピングを再度イネーブルに設定するには、このコマンドを使用します。
ステップ 4	**ip domain multicast** *domain-prefix*	（任意）スイッチが DNS ベースの SSM マッピングで使用するドメイン プレフィクスを変更します。 デフォルトでは、スイッチは *ip-addr.arpa* ドメイン プレフィクスを使用します。

	コマンド	目的
ステップ 5	**ip name-server** ***server-address1*** [*server-address2... server-address6*]	1 つまたは複数のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。
ステップ 6	必要に応じて、ステップ 5 を繰り返し、追加の DNS サーバを設定し、冗長性を実現します。	—
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングを使用したスタティック トラフィック転送の設定

SSM マッピングを使用したスタティック トラフィック転送で、特定のグループに SSM トラフィックをスタティックに転送できます。

SSM マッピングによるスタティック トラフィック転送を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number*	SSM マッピングを使用して、マルチキャスト グループへトラフィックをスタティックに転送するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 **（注）** SSM マッピングを使用したトラフィックのスタティック転送は、DNS ベースの SSM マッピングまたはスタティックに設定された SSM マッピングのいずれかで動作します。
ステップ 3	**ip igmp static-group** ***group-address*** **source ssm-map**	インターフェイスから（S, G）チャネルをスタティックに転送するよう SSM マッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する場合に使用します。チャネルの送信元のアドレスを決定するには、DNS ベースの SSM マッピングを使用します。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングのモニタリング

SSM マッピングを監視するには、表 44-4 の特権 EXEC コマンドを使用します。

表 44-4　SSM マッピングのモニタリングに使用するコマンド

コマンド	目的
show ip igmp ssm-mapping	SSM マッピングについての情報を表示します。
show ip igmp ssm-mapping *group-address*	SSM マッピングが特定のグループに使用する送信元を表示します。
show ip igmp groups [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]	ルータに直接接続されているレシーバー、および IGMP によって取得されたレシーバーのマルチキャスト グループを表示します。

表 44-4　SSM マッピングのモニタリングに使用するコマンド

コマンド	目的
show host	デフォルトのドメイン名、名前検索サービスの方式、ネーム サーバ ホストのリスト、およびキャッシュに保存されているホスト名とアドレスのリストを表示します。
debug ip igmp *group-address*	送受信した IGMP パケット、および IGMP ホスト関連のイベントを表示します。

SSM マッピングのモニタリングの例については、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html#wp1047772

RP の設定

インターフェイスが SM-DM で、グループを sparse グループとして扱う場合には、RP を設定する必要があります。ここに記載するいくつかの方法を使用できます。

- 「マルチキャスト グループへの RP の手動割り当て」（P.44-24）
- 「自動 RP の設定」（P.44-26）（PIMv1 から独立した、スタンドアロンのシスコ独自のプロトコル）
- 「PIMv2 BSR の設定」（P.44-30）（Internet Engineering Task Force [IETF; インターネット技術特別調査委員会] 標準の追跡プロトコル）

動作中の PIM バージョン、およびネットワーク内のルータ タイプに応じて、自動 RP、BSR、またはこれらを組み合せて使用できます。詳細については、「PIMv1 および PIMv2 の相互運用性」（P.44-10）および「自動 RP および BSR 設定時の注意事項」（P.44-10）を参照してください。

マルチキャスト グループへの RP の手動割り当て

ここでは、RP を手動で割り当てる方法について説明します。ダイナミック メカニズム（自動 RP や BSR など）を使用してグループの RP を取得する場合、RP を手動で割り当てる必要はありません。

マルチキャスト トラフィックの送信側は、送信元の先頭ホップ ルータ（指定ルータ）から受信して RP に転送される Register メッセージを通し、自身の存在をアナウンスします。マルチキャスト パケットの受信側は RP を使用し、マルチキャスト グループに参加します。この場合は、明示的な Join メッセージが使用されます。RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの「*合流地点*」として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤ スイッチはグループを dense として処理し、DM PIM 技術を使用します。

RP のアドレスを手動で設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-address** *ip-address* [*access-list-number*] [**override**]	PIM RP のアドレスを設定します。 デフォルトで、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤ スイッチ（RP を含む）で、RP の IP アドレスを設定する必要があります。グループに RP が設定されていない場合、スイッチはグループを dense として処理し、DM PIM 技術を使用します。 1 台の PIM デバイスを、複数のグループの RP にできます。1 つの PIM ドメイン内で一度に使用できる RP アドレスは 1 つだけです。アクセス リスト条件により、デバイスがどのグループの RP であるかを指定します。 • *ip-address* には、RP のユニキャスト アドレスをドット付き 10 進表記で入力します。 • （任意）*access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • （任意）キーワード **override** を指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、RP が使用されるマルチキャスト グループのアドレスを入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RP アドレスを削除するには、**no ip pim rp-address** *ip-address* [*access-list-number*] [**override**] グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト グループ 225.2.2.2 の場合にだけ、RP のアドレスを 147.106.6.22 に設定する例を示します。

```
Switch(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Switch(config)# ip pim rp-address 147.106.6.22 1
```

自動 RP の設定

自動 RP は IP マルチキャストを使用し、グループ/RP マッピングを PIM ネットワーク内のすべてのシスコ ルータおよびマルチレイヤ スイッチに自動配信します。自動 RP には次の利点があります。

- ネットワーク内で複数の RP を使用し、複数のグループ範囲を処理する作業が簡単になります。
- 複数の RP 間で負荷を分散し、グループに参加するホストの場所に従って RP を配置できます。
- PIM ネットワーク内のすべてのルータおよびマルチレイヤ スイッチで矛盾が発生しなくなり、手動による RP 設定が不要になります。この結果、接続問題を引き起こす要因が取り除かれます。

（注）　PIM を SM または SM-DM に設定し、自動 RP を設定しない場合は、RP を手動で設定する必要があります（「マルチキャスト グループへの RP の手動割り当て」（P.44-24）を参照）。

（注）　ルーテッド インターフェイスが SM に設定されていると、すべてのデバイスが自動 RP グループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。

ここでは、自動 RP を設定する方法について説明します。

- 「新規インターネットワークでの自動 RP の設定」（P.44-26）（任意）
- 「既存の SM クラウドへの自動 RP の追加」（P.44-26）（任意）
- 「問題のある RP への Join メッセージの送信禁止」（P.44-28）（任意）
- 「着信 RP アナウンスメント メッセージのフィルタリング」（P.44-29）（任意）

概要については、「自動 RP」（P.44-6）を参照してください。

新規インターネットワークでの自動 RP の設定

新規インターネットワーク内に自動 RP を設定している場合は、すべてのインターフェイスが SM-DM に設定されるため、デフォルトの RP は不要です。「既存の SM クラウドへの自動 RP の追加」（P.44-26）に記載された手順に従ってください。ただし、PIM ルータをローカル グループの RP として設定する場合は、ステップ 3 を省略してください。

既存の SM クラウドへの自動 RP の追加

ここでは、最初に自動 RP を既存の SM クラウドに導入し、既存のマルチキャスト インフラストラクチャができるだけ破壊されないようにする方法について説明します。

既存の SM クラウドに自動 RP を導入するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**show running-config**	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを確認します。RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって設定済みです。 SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自動 RP によってダイナミックに検出された RP は、スタティックに設定された RP よりも優先されます。ローカル グループ用に 2 番目の RP を使用することもできます。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*	別の PIM デバイスをローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイス タイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • **scope** *ttl* には、ホップの TTL 値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。 • **group-list** *access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval** *seconds* には、アナウンスメント メッセージを送信する頻度を指定します。デフォルトは 60 秒です。指定できる範囲は 1 ～ 16383 です。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。

	コマンド	目的
ステップ 5	**ip pim send-rp-discovery scope** *ttl*	接続が中断される可能性がないスイッチを検索し、RP マッピング エージェントの役割を割り当てます。 **scope** *ttl* には、ホップの TTL 値を指定し、RP ディスカバリ パケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾（グループ/RP 範囲の重複など）を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
	show ip pim rp mapping	関連するマルチキャスト ルーティング エントリとともに保管されているアクティブな RP を表示します。
	show ip pim rp	ルーティング テーブルのキャッシュに保管されている情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

候補 RP として設定された PIM デバイスを解除するには、**no ip pim send-rp-announce** *interface-id* グローバル コンフィギュレーション コマンドを使用します。RP マッピング エージェントとして設定されたスイッチを解除するには、**no ip pim send-rp-discovery** グローバル コンフィギュレーション コマンドを使用します。

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスメントを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセス リスト 5 には、このスイッチが RP として機能するグループが記述されています。

```
Switch(config)# ip pim send-rp-announce gigabitethernet0/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

問題のある RP への Join メッセージの送信禁止

ip pim accept-rp コマンドがネットワーク全体に設定されているかどうかを判別するには、**show running-config** 特権 EXEC コマンドを使用します。**ip pim accept-rp** コマンドが設定されていないデバイスがある場合は、あとでこの問題を解決できます。ルータまたはマルチレイヤ スイッチが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新規にアドバタイズされる RP を許可する必要があります。

自動 RP によってアドバタイズされるすべての RP を許可し、他のすべての RP をデフォルトで拒否するには、**ip pim accept-rp auto-rp** グローバル コンフィギュレーション コマンドを使用します。この手順は任意です。

すべてのインターフェイスが SM の場合は、デフォルト設定の RP を使用し、既知のグループ 224.0.1.39 および 224.0.1.40 をサポートします。自動 RP はこれら 2 つの既知のグループを使用し、RP マッピング情報を収集、配信します。**ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定してください。

```
Switch(config)# ip pim accept-rp 172.10.20.1 1
Switch(config)# access-list 1 permit 224.0.1.39
Switch(config)# access-list 1 permit 224.0.1.40
```

着信 RP アナウンスメント メッセージのフィルタリング

マッピング エージェントにコンフィギュレーション コマンドを追加すると、故意に不正設定されたルータが候補 RP として動作し問題を引き起こさないようにできます。

着信 RP アナウンスメント メッセージをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-announce-filter rp-list** *access-list-number* **group-list** *access-list-number*	着信 RP アナウンスメント メッセージをフィルタリングします。 ネットワーク内のマッピング エージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべての着信 RP アナウンスメント メッセージがデフォルトで許可されます。 **rp-list** *access-list-number* を指定する場合は、候補 RP アドレスのアクセス リストを設定します。アクセス リストが許可されている場合は、**group-list** *access-list-number* 変数で指定されたグループ範囲に対してアクセス リストを使用できます。この変数を省略すると、すべてのマルチキャスト グループにフィルタが適用されます。 複数のマッピング エージェントを使用する場合は、グループ/RP マッピング情報に矛盾が生じないようにするため、すべてのマッピング エージェント間でフィルタを統一する必要があります。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンスメント（rp-list Access Control List [ACL; アクセス コントロール リスト]）がマッピング エージェントによって許可されるかを指定するアクセス リストを作成します。 • 許可または拒否するマルチキャスト グループの範囲を指定するアクセス リスト（グループリスト ACL）を作成します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

着信 RP アナウンスメント メッセージに関するフィルタを削除するには、**no ip pim rp-announce-filter rp-list** *access-list-number* [**group-list** *access-list-number*] グローバル コンフィギュレーション コマンドを使用します。

次に、候補 RP アナウンスメントが不正な候補 RP から許可されないようにするために使用される自動 RP マッピング エージェントの設定例を示します。

```
Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config)# access-list 10 permit host 172.16.5.1
Switch(config)# access-list 10 permit host 172.16.2.1
Switch(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Switch(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

この例では、マッピング エージェントは 2 つのデバイス（172.16.5.1 および 172.16.2.1）からの候補 RP アナウンスだけを許可します。マッピング エージェントは 2 つのデバイスからの候補 RP アナウンスメントのうち、グループ範囲が 224.0.0.0 ～ 239.255.255.255 であるマルチキャスト グループ宛てのアナウンスメントだけを許可します。マッピング エージェントは、ネットワーク内の他のデバイスからの候補 RP アナウンスメントを許可しません。さらに、候補 RP アナウンスメントが 239.0.0.0 ～ 239.255.255.255 の範囲のグループに宛てたものである場合、マッピング エージェントは 172.16.5.1 または 172.16.2.1 からの候補 RP アナウンスメントを許可しません。この範囲は、管理の有効範囲付きアドレス範囲です。

PIMv2 BSR の設定

ここでは、PIMv2 ネットワークでの BSR の設定方法について説明します。

- 「PIM ドメイン境界の定義」（P.44-30）（任意）
- 「IP マルチキャスト境界の定義」（P.44-31）（任意）
- 「候補 BSR の設定」（P.44-32）（任意）
- 「候補 RP の設定」（P.44-33）（任意）

概要については、「BSR」（P.44-7）を参照してください。

PIM ドメイン境界の定義

IP マルチキャストの普及に伴い、PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する場合が増えています。これらの 2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していないことが多いため、PIMv2 BSR メッセージがドメインの内外に流れないようにする必要があります。これらメッセージのドメイン境界通過を許可すると、通常の BSR 選択メカニズムに悪影響が及んだり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズが共存し、間違ったドメイン内で RP が選択されたりすることがあります。

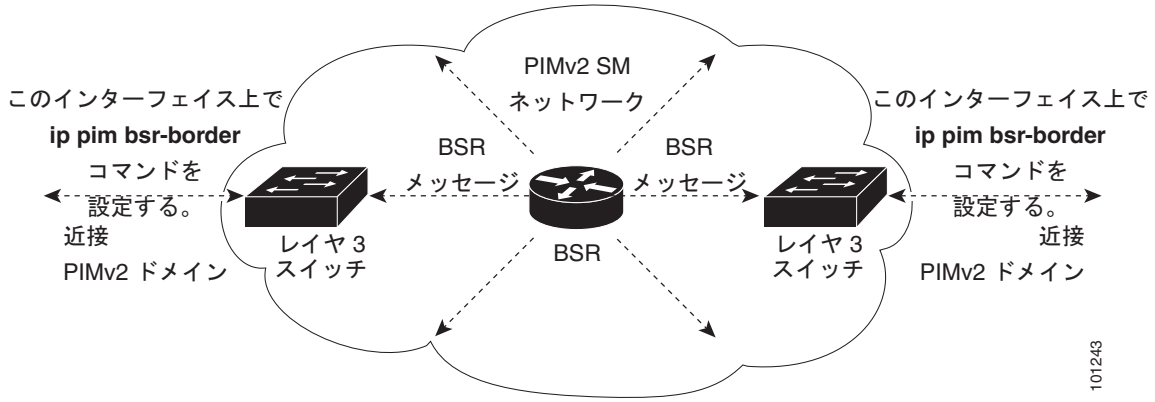
PIM ドメイン境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**ip pim bsr-border**	PIM ドメイン用の PIM ブートストラップ メッセージ境界を定義します。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。このコマンドを実行すると、スイッチは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指示されます（図 44-4 を参照）。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM 境界を削除するには、**no ip pim bsr-border** インターフェイス コンフィギュレーション コマンドを使用します。

図 44-4　PIMv2 BSR メッセージの抑制



IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセス リストを作成します。

マルチキャスト境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **deny** *source* [*source-wildcard*]	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。 • *source* には、自動 RP 情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 3	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5	**ip multicast boundary** *access-list-number*	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

境界を削除するには、**no ip multicast boundary** インターフェイス コンフィギュレーション コマンドを使用します。

次に、自動 RP 情報を拒否する IP マルチキャスト境界のコンフィギュレーション例の一部を示します。

```
Switch(config)# access-list 1 deny 224.0.1.39
Switch(config)# access-list 1 deny 224.0.1.40
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip multicast boundary 1
```

候補 BSR の設定

候補 BSR を、1 つまたは複数設定できます。候補 BSR として機能するデバイスは、他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。

スイッチを候補 BSR として設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*]	候補 BSR となるようにスイッチを設定します。 • *interface-id* には、スイッチを候補 BSR に設定するときに BSR アドレスの取得元となる、スイッチ上のインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必要があります。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • *hash-mask-length* には、ハッシュ機能を呼び出す前に、グループ アドレスとの AND 条件となるマスク長（最大 32 ビット）を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。 • （任意）*priority* を指定するときは、0 ～ 255 の数値を入力します。プライオリティの大きな BSR が優先されます。このプライオリティ値が同じである場合は、大きな IP アドレスを持つデバイスが BSR として選択されます。デフォルト値は 0 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

候補 BSR として設定されたデバイスを解除するには、**no ip pim bsr-candidate** グローバル コンフィギュレーション コマンドを使用します。

次に、候補 BSR の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip address 172.21.24.18 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip pim bsr-candidate gigabitethernet0/2 30 10
```

候補 RP の設定

候補 RP を、1 つまたは複数設定できます。BSR と同様、RP は他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。RP は IP マルチキャスト アドレス スペース全体、またはその一部を処理します。候補 RP は候補 RP アドバタイズを BSR に送信します。RP となるデバイスを決定するときは、次の可能性を考慮してください。

- 自動 RP だけが使用されているシスコ ルータおよびマルチレイヤ スイッチで構成されるネットワークでは、すべてのデバイスを RP として設定できます。
- シスコの PIMv2 ルータおよびマルチレイヤ スイッチと、他のベンダーのルータだけで構成されるネットワークでは、すべてのデバイスを RP として使用できます。
- シスコの PIMv1 ルータ、PIMv2 ルータ、および他のベンダーのルータで構成されるネットワークでは、シスコ PIMv2 ルータおよびマルチレイヤ スイッチを RP として設定できます。

スイッチが自身を PIMv2 候補 RP として BSR にアドバタイズするよう設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*]	候補 RP となるようにスイッチを設定します。 • *interface-id* には、対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • （任意）**group-list** *access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。group-list を指定しない場合は、スイッチはすべてのグループの候補 RP となります。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

候補 RP として設定されたデバイスを解除するには、**no ip pim rp-candidate** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチが自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするよう設定する例を示します。標準アクセス リスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループ プレフィクスが指定されます。この RP は、プレフィクスが 239 であるグループを処理します。

```
Switch(config)# ip pim rp-candidate gigabitethernet0/2 group-list 4
Switch(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

自動 RP および BSR の使用法

ネットワーク上のルータがすべてシスコ製デバイスである（他のベンダー製のルータが存在しない）場合には、BSR を設定する必要はありません。PIMv1 と PIMv2 が両方とも動作しているネットワークに、自動 RP を設定します。

シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 ルータまたはマルチレイヤ スイッチを、自動 RP マッピング エージェントと BSR の両方に設定してください。

BSR を 1 つまたは複数使用する必要がある場合は、次の推奨事項に従ってください。

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。詳細については、「自動 RP の設定」（P.44-26）および「候補 BSR の設定」（P.44-32）を参照してください。
- グループ プレフィクスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループ プレフィクスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。PIMv1 および PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループ プレフィクスが処理されるように設定します。このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

グループ /RP マッピングの一貫性を確認するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**show ip pim rp** [[*group-name* | *group-address*] | **mapping**]	任意のシスコ製デバイスに関して、使用可能な RP マッピングを表示します。 • （任意）*group-name* を指定するときは、RP を表示するグループの名前を指定します。 • （任意）*group-address* を指定するときは、RP を表示するグループのアドレスを指定します。 • （任意）シスコ製デバイスによって認識されている（設定されている、または自動 RP によって取得されている）すべてのグループ /RP マッピングを表示するには、キーワード **mapping** を使用します。
ステップ 2	**show ip pim rp-hash** *group*	PIMv2 ルータまたはマルチレイヤ スイッチ上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。 *group* には、RP 情報を表示するグループ アドレスを入力します。

RP マッピング情報のモニタ

RP マッピング情報をモニタするには、特権 EXEC モードで次のコマンドを使用します。

- **show ip pim bsr**：現在選択されている BSR の情報を表示します。
- **show ip pim rp-hash** *group*：指定グループに選択されている RP を表示します。
- **show ip pim rp** [*group-name* | *group-address* | **mapping**]：スイッチが RP を取得する方法（BSR 経由か、または自動 RP メカニズムによるか）を表示します。

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

PIMv1 および PIMv2 間の相互運用性に関する問題を解決するには、次の点を順にチェックします。

1. **show ip pim rp-hash** 特権 EXEC コマンドを使用して RP マッピングを確認し、すべてのシステムが同じグループの同じ RP に同意していることを確認します。
2. DR と RP の各バージョン間の相互運用性を確認し、RP が DR と適切に相互作用していることを確認します（この場合は、登録停止に応答し、カプセル化が解除されたデータ パケットをレジスタから転送します）。

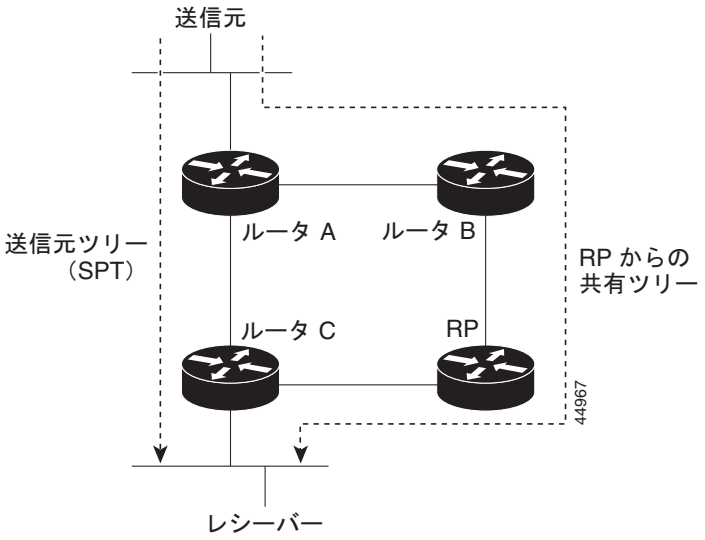
高度な PIM 機能の設定

- 「PIM 共有ツリーおよび送信元ツリーの概要」（P.44-36）
- 「PIM SPT 使用の延期」（P.44-37）（任意）
- 「PIM ルータクエリー メッセージ インターバルの変更」（P.44-38）（任意）

PIM 共有ツリーおよび送信元ツリーの概要

デフォルトでは、グループのメンバーで受信されるデータは、RP でルーティングされた単一のデータ配信ツリーを経由して、送信側からグループに送られます。図 44-5 に、このタイプの共有配信ツリーを示します。送信側からのデータは、共有ツリーに参加しているグループ メンバーに配信するため、RP にアドバタイズされます。

図 44-5　　共有ツリーおよび送信元ツリー（SPT）



データ レートによって保証されている場合は、送信元でルーティングされるデータ配信ツリーを、共有ツリーのリーフ ルータ（ダウンストリーム接続がないルータ）で使用できます。このタイプの配信ツリーは、SPT または送信元ツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

1. レシーバーがグループに参加します。リーフ ルータ C は Join メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して Register メッセージに格納し、RP に送信します。
4. RP はデータをルータ C に向けて共有ツリーの下方向に転送し、送信元に向けて Join メッセージを送信します。この時点で、データはルータ C に 2 回着信する可能性があります（カプセル化されたデータ、およびネイティブ状態のデータ）。
5. データがネイティブ状態（カプセル化されていない状態）で着信すると、RP は Register 停止メッセージをルータ A に送信します。

6. デフォルトでは、最初のデータ パケット受信時に、ルータ C が Join メッセージを送信元に送信するよう要求します。
7. （S,G）に関するデータを受信すると、ルータ C は送信元宛の Prune メッセージを共有ツリーの上方向に送信します。
8. RP は（S,G）の発信インターフェイスからルータ C へのリンクを削除します。RP は送信元に向けて Prune メッセージを送信します。

Join および Prune メッセージが送信元および RP に送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP へのパス上にある各 PIM デバイスで処理されます。Register メッセージおよび Register 停止メッセージはホップバイホップで送信されません。これらのメッセージは、送信元に直接接続された指定ルータで送信され、グループの RP で受信されます。

グループに送信する複数の送信元で、共有ツリーが使用されます。

共有ツリー上に存在するように、PIM デバイスを設定できます。詳細については、「PIM SPT 使用の延期」（P.44-37）を参照してください。

PIM SPT 使用の延期

最初のデータ パケットが最終ホップ ルータ（図 44-5 のルータ C）に着信すると、共有ツリーから送信元ツリーへと変更されます。この変更が生じるのは、**ip pim spt-threshold** グローバル コンフィギュレーション コマンドによってタイミングが制御されるためです。

SPT には共有ツリーよりも多くのメモリが必要ですが、遅延が短縮されます。SPT の使用を延期することもできます。リーフ ルータを SPT にすぐ移動せず、トラフィックがしきい値に最初に到達したあとで移動するように指定できます。

PIM リーフ ルータが、指定グループの SPT に参加する時期を設定できます。送信元の送信速度が指定速度（キロビット/秒）以上の場合、マルチレイヤ スイッチは PIM Join メッセージを送信元に向けて送信し、送信元ツリー（SPT）を構築します。送信元からのトラフィック速度がしきい値を下回ると、リーフ ルータは共有ツリーに再び切り替わり、Prune メッセージを送信元に送信します。

SPT しきい値を適用するグループを指定するには、グループ リスト（標準アクセス リスト）を使用します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。

マルチキャスト ルーティングが送信元ツリーから SPT に切り替わる上限値となるトラフィック速度のしきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。 • *access-list-number* の範囲は 1 ～ 99 です。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、しきい値が適用されるマルチキャスト グループを指定します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 3	**ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list-number*]	SPT に移行する上限値となるしきい値を指定します。 • *kbps* を指定するときは、トラフィック速度をキロビット/秒で指定します。デフォルト値は 0 キロビット/秒です。 **（注）** 有効範囲は 0 ～ 4294967 ですが、スイッチ ハードウェアの制限により、0 キロビット/秒以外は無効です。 • **infinity** を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。 • （任意）**group-list** *access-list-number* を指定するときは、ステップ 2 で作成したアクセス リストを指定します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip pim spt-threshold** {*kbps* | **infinity**} グローバル コンフィギュレーション コマンドを使用します。

PIM ルータクエリー メッセージ インターバルの変更

PIM ルータおよびマルチレイヤ スイッチでは、各 LAN セグメント（サブネット）の DR になるデバイスを判別するため、PIM ルータクエリー メッセージが送信されます。DR は、直接接続された LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。

PIM DM 動作では、IGMPv1 が使用中の場合だけ、DR は意味を持ちます。IGMPv1 には IGMP クエリア選択プロセスがないため、選択された DR は IGMP クエリアとして機能します。PIM SM 動作では、マルチキャスト送信元に直接接続されたデバイスが DR になります。DR は PIM Register メッセージを送信し、送信元からのマルチキャスト トラフィックを共有ツリーの下方向へ転送する必要があることを RP に通知します。この場合、DR は最大の IP アドレスを持つデバイスです。

ルータクエリー メッセージ インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip pim query-interval** *seconds*	スイッチが PIM ルータクエリー メッセージを送信する頻度を設定します。 デフォルトは 30 秒です。指定できる範囲は 1 ～ 65535 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no ip pim query-interval** [*seconds*] インターフェイス コンフィギュレーション コマンドを使用します。

オプションの IGMP 機能の設定

- 「IGMP のデフォルト設定」（P.44-39）
- 「グループのメンバーとしてのスイッチの設定」（P.44-40）（任意）
- 「IP マルチキャスト グループへのアクセスの制御」（P.44-41）（任意）
- 「IGMP バージョンの変更」（P.44-42）（任意）
- 「IGMP ホストクエリー メッセージ インターバルの変更」（P.44-42）（任意）
- 「IGMPv2 の IGMP クエリー タイムアウトの変更」（P.44-43）（任意）
- 「IGMPv2 の最大クエリー応答時間の変更」（P.44-44）（任意）
- 「スタティックに接続されたメンバーとしてのスイッチの設定」（P.44-44）（任意）

IGMP のデフォルト設定

表 44-5 に、IGMP のデフォルト設定を示します。

表 44-5　IGMP のデフォルト設定

機能	デフォルト設定
マルチキャスト グループのメンバーとしてのマルチレイヤ スイッチ	グループ メンバシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを許可
IGMP バージョン	すべてのインターフェイスでバージョン 2
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
スタティックに接続されたメンバーとしてのマルチレイヤ スイッチ	ディセーブル。

グループのメンバーとしてのスイッチの設定

スイッチをマルチキャスト グループのメンバーとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理しているすべてのマルチキャスト対応ルータおよびマルチレイヤ スイッチがマルチキャスト グループのメンバーである場合、グループに ping を送信すると、これらのすべてのデバイスが応答します。デバイスは、所属グループにアドレス指定された IGMP エコー要求パケットに応答します。もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。

注意　この手順を実行すると、グループ アドレス用のデータ トラフィックがすべて CPU に送られるため、CPU のパフォーマンスが低下する場合があります。

スイッチがグループのメンバーになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp join-group** *group-address*	マルチキャスト グループに参加するスイッチを設定します。 デフォルトでは、グループのメンバシップは定義されていません。 *group-address* には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

グループ内のメンバシップを取り消すには、**no ip igmp join-group** *group-address* インターフェイス コンフィギュレーション コマンドを使用します。

次に、マルチキャスト グループ 255.2.2.2 へのスイッチの参加を許可する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp join-group 255.2.2.2
```

IP マルチキャスト グループへのアクセスの制御

スイッチは IGMP ホストクエリー メッセージを送信し、接続されたローカル ネットワーク上のメンバーが属しているマルチキャスト グループを判別します。次に、スイッチは、マルチキャスト グループにアドレス指定されたすべてのパケットをこれらのグループ メンバーに転送します。インターフェイスごとにフィルタを適用し、インターフェイスで処理されるサブネット上のホストが参加可能なマルチキャスト グループを制限できます。

インターフェイスで許可されるマルチキャスト グループをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp access-group** *access-list-number*	インターフェイスで処理されるサブネット上のホストが参加できるマルチキャスト グループを指定します。 デフォルトでは、インターフェイスのすべてのグループが許可されています。 *access-list-number* には、IP 標準アクセス リスト番号を指定します。指定できる範囲は 1 ～ 99 です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。 • *access-list-number* には、ステップ 3 で作成したアクセス リストを指定します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、サブネット上のホストが参加できるマルチキャスト グループを指定します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスでグループをディセーブルにするには、**no ip igmp access-group** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに接続されたホストが、グループ 255.2.2.2 にだけ参加できるように設定する例を示します。

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# ip igmp access-group 1
```

IGMP バージョンの変更

スイッチでは、IGMP クエリー タイムアウトや最大クエリー応答時間などの機能を使用できる IGMP バージョン 2 がデフォルトで使用されます。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。スイッチは、バージョン 1 システムを自動的には検出しないため、バージョン 1 へのスイッチングも行われません。バージョン 2 ルータまたはスイッチは、常に IGMPv1 ホストと正常に動作するため、バージョン 1 とバージョン 2 のホストをサブネット上で混在させることができます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

IGMP バージョンを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp version** {**1** | **2**}	スイッチで使用する IGMP バージョンを指定します。 **（注）** バージョン 1 に変更すると、**ip igmp query-interval** または **ip igmp query-max-response-time** の各インターフェイス コンフィギュレーション コマンドを設定できません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no ip igmp version** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP ホストクエリー メッセージ インターバルの変更

スイッチは、IGMP ホストクエリー メッセージを定期的に送信し、接続されたネットワーク上にあるマルチキャスト グループを検出します。これらのメッセージは、Time To Live（TTL）値が 1 のすべてのホスト マルチキャスト グループ（224.0.0.1）に送信されます。スイッチはホストクエリー メッセージを送信し、ネットワーク内のメンバシップに関する情報を更新します。クエリーをいくつか実行

したあとで、マルチキャスト グループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカル ネットワークへのマルチキャスト パケット転送が停止され、Prune メッセージが送信元のアップストリーム方向へ送信されます。

スイッチは LAN（サブネット）用の PIM DR を選択します。DR は、IP アドレスが最大である、IGMPv2 用のルータまたはマルチレイヤ スイッチです。IGMPv1 の場合、DR は LAN 上で動作するマルチキャスト ルーティング プロトコルに従って選択されます。DR は、LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。

ホストクエリー インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp query-interval** *seconds*	DR が IGMP ホストクエリー メッセージを送信する頻度を設定します。 デフォルトでは、DR は IGMP ホストクエリー メッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。指定できる範囲は 1 ～ 65535 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp query-interval** インターフェイス コンフィギュレーション コマンドを使用します。

IGMPv2 の IGMP クエリー タイムアウトの変更

IGMPv2 を使用している場合、スイッチがインターフェイスのクエリアとして引き継ぐまでの時間を指定できます。デフォルトでは、スイッチは **ip igmp query-interval** インターフェイス コンフィギュレーション コマンドによって制御されるクエリー インターバルの 2 倍の時間だけ待機します。この時間を経過しても、スイッチがクエリーを受信しない場合は、スイッチがクエリアになります。

クエリー インターバルを設定するには、**show ip igmp interface** *interface-id* 特権 EXEC コマンドを入力します。

IGMP クエリー タイムアウトを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**ip igmp querier-timeout** *seconds*	IGMP クエリー タイムアウトを指定します。 デフォルトは 60 秒です（クエリー インターバルの 2 倍）。指定できる範囲は 60 ～ 300 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp querier-timeout** インターフェイス コンフィギュレーション コマンドを使用します。

IGMPv2 の最大クエリー応答時間の変更

IGMPv2 を使用している場合は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。スイッチは最大クエリー応答時間を使用し、LAN 上に直接接続されたグループ メンバーが存在しないことを短時間で検出します。値を小さくすると、グループのプルーニング速度が向上します。

最大クエリー応答時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp query-max-response-time** *seconds*	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルトは 10 秒です。指定できる範囲は 1 ～ 25 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを使用します。

スタティックに接続されたメンバーとしてのスイッチの設定

ネットワーク セグメント上にグループ メンバーが存在しなかったり、ホストで IGMP を使用してグループ メンバシップを報告できないにもかかわらず、そのネットワーク セグメントにマルチキャスト トラフィックを送り込むことが必要な場合もあります。マルチキャスト トラフィックをネットワーク セグメントに送り込む方法は次のとおりです。

- **ip igmp join-group** インターフェイス コンフィギュレーション コマンドを使用します。この方法の場合、スイッチはマルチキャスト パケットの転送だけでなく、受信も行います。マルチキャスト パケットを受信する場合は、高速スイッチングを実行できません。

- **ip igmp static-group** インターフェイス コンフィギュレーション コマンドを使用します。この方法の場合、スイッチはパケットそのものを受信せず、転送だけを実行します。この方法を使用すると、高速スイッチングが可能です。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに *L*（ローカル）フラグが付かないことからも明らかなように、スイッチ自体はメンバーではありません。

スタティックに接続されたグループのメンバーになるように（および高速スイッチングできるように）スイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp static-group** *group-address*	スイッチをスタティックに接続されたグループのメンバーとして設定します。 デフォルトでは、この機能はディセーブルです。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

グループのメンバーとして設定されたスイッチを解除するには、**no ip igmp static-group** *group-address* インターフェイス コンフィギュレーション コマンドを使用します。

オプションのマルチキャスト ルーティング機能の設定

- 「sdr リスナー サポート機能の設定」（P.44-45）（任意）：MBONE マルチメディア コンファレンス セッションおよびセット アップ
- 「IP マルチキャスト境界の設定」（P.44-47）（任意）：帯域幅の利用率を制御

sdr リスナー サポート機能の設定

MBONE は、相互接続された、IP マルチキャスト トラフィックの転送が可能なインターネット ルータおよびホストの小さなサブセットです。その他のマルチメディア コンテンツも、通常は MBONE を通してブロードキャストされます。マルチメディア セッションに参加する前に、このセッションで使用されているマルチメディア グループ アドレス、ポート、セッションがアクティブになる時期、およびワークステーションで必要となるアプリケーションの種類（音声、ビデオなど）を把握する必要があります。この情報は、MBONE Session Directory バージョン 2（sdr）ツールによって提供されます。このフリーウェア アプリケーションは WWW 上の複数のサイト（http://www.video.ja.net/mice/index.html など）からダウンロードできます。

SDR は、Session Announcement Protocol（SAP）マルチキャスト パケット用の既知のマルチキャスト グループ アドレスおよびポートを、SAP クライアントからリスニングするマルチキャスト アプリケーションです（SAP クライアントは、会議セッションをアナウンスします）。これらの SAP パケットに

は、セッションの説明、セッションがアクティブな期間、IP マルチキャスト グループ アドレス、メディア形式、担当者、およびアドバタイズされたマルチメディア セッションに関するその他の情報が格納されます。SAP パケットの情報は、SDR Session Announcement ウィンドウに表示されます。

sdr リスナー サポート機能のイネーブル化

デフォルトでは、スイッチでセッション ディレクトリのアドバタイズはリスニングされません。

スイッチがインターフェイスのデフォルトのセッション ディレクトリ グループ（224.2.127.254）に参加し、セッション ディレクトリ アドバタイズをリスニングできるようにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	sdr に対してイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip sdr listen**	sdr リスナー サポート機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

sdr サポート機能をディセーブルにするには、**no ip sdr listen** インターフェイス コンフィギュレーション コマンドを使用します。

sdr キャッシュ エントリの存在期間の制限

デフォルトでは、エントリは sdr キャッシュから削除されません。送信元が SAP 情報のアドバタイズを停止した場合に、古いアドバタイズが無駄に保持されないようにするため、エントリがアクティブである期間を制限できます。

sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sdr cache-timeout** *minutes*	sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限します。 デフォルトでは、エントリはキャッシュから削除されません。 *minutes* に指定できる範囲は 1 ～ 4294967295 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no ip sdr cache-timeout** グローバル コンフィギュレーション コマンドを使用します。キャッシュ全体を削除するには、**clear ip sdr** 特権 EXEC コマンドを使用します。

セッション ディレクトリ キャッシュを表示するには、**show ip sdr** 特権 EXEC コマンドを使用します。

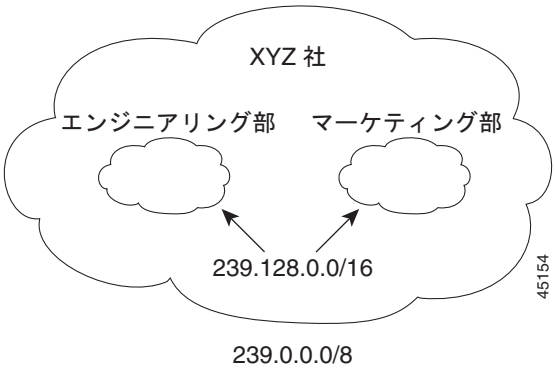
IP マルチキャスト境界の設定

管理の有効範囲付き境界を使用し、ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限できます。この方法では、「*管理の有効範囲付きアドレス*」と呼ばれる特殊なマルチキャスト アドレス範囲が境界のメカニズムとして使用されます。管理の有効範囲付き境界をルーテッド インターフェイスに設定すると、マルチキャスト グループ アドレスがこの範囲内にあるマルチキャスト トラフィックは、このインターフェイスに出入りできません。この結果、このアドレス範囲内のマルチキャスト トラフィックに対するファイアウォール機能が提供されます。

（注） マルチキャスト境界および TTL しきい値は、マルチキャスト ドメインの有効範囲を制御しますが、TTL しきい値はこのスイッチでサポートされていません。ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限するには、TTL しきい値でなくマルチキャスト境界を使用する必要があります。

図 44-6 に、XYZ 社が自社ネットワーク周辺にあるすべてのルーテッド インターフェイス上で、管理の有効範囲付き境界をマルチキャスト アドレス範囲 239.0.0.0/8 に設定した例を示します。この境界では、239.0.0.0 ～ 239.255.255.255 の範囲のマルチキャスト トラフィックはネットワークに入ったり、外へ出ることができません。同様に、エンジニアリング部およびマーケティング部では、各自のネットワークの周辺で、管理の有効範囲付き境界を 239.128.0.0/16 に設定しました。この境界では、239.128.0.0 ～ 239.128.255.255 の範囲のマルチキャスト トラフィックは、それぞれのネットワークに入ったり、外部に出ることができません。

図 44-6　　管理の有効範囲付き境界



マルチキャスト グループ アドレスに対して、ルーテッド インターフェイス上に管理の有効範囲付き境界を定義できます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。この境界が定義されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過できません。この境界を使用すると、異なる管理ドメイン内で同じマルチキャスト グループ アドレスを再利用できます。

IANA は、マルチキャスト アドレス範囲 239.0.0.0 ～ 239.255.255.255 を管理の有効範囲付きアドレスとして指定しました。このアドレス範囲は、異なる組織によって管理されたドメイン内で再利用できます。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

管理の有効範囲付き境界を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 3	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5	**ip multicast boundary** *access-list-number*	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

境界を削除するには、**no ip multicast boundary** インターフェイス コンフィギュレーション コマンドを使用します。

次に、すべての管理の有効範囲付きアドレスに対して境界を設定する例を示します。

```
Switch(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Switch(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip multicast boundary 1
```

IP マルチキャスト ルーティングのモニタおよびメンテナンス

- 「キャッシュ、テーブル、およびデータベースのクリア」（P.44-49）
- 「システムおよびネットワーク統計情報の表示」（P.44-49）
- 「IP マルチキャスト ルーティングのモニタ」（P.44-50）

キャッシュ、テーブル、およびデータベースのクリア

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定のキャッシュ、テーブル、またはデータベースの内容が無効である場合、または無効である可能性がある場合は、これらをクリアする必要があります。

表 44-6 に示す特権 EXEC コマンドのいずれかを使用すると、IP マルチキャストのキャッシュ、テーブル、データベースをクリアできます。

表 44-6　キャッシュ、テーブル、およびデータベースをクリアするためのコマンド

コマンド	目的
clear ip igmp group [*group-name* | *group-address* | *interface*]	IGMP キャッシュのエントリを削除します。
clear ip mroute {* | *group* [*source*]}	IP マルチキャスト ルーティング テーブルのエントリを削除します。
clear ip pim auto-rp *rp-address*	自動 RP キャッシュをクリアします。
clear ip sdr [*group-address* | “*session-name*”]	Session Directory Protocol バージョン 2 キャッシュ（sdr キャッシュ エントリ）を削除します。

システムおよびネットワーク統計情報の表示

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注）　このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの利用率を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらには、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティング パスを検出することもできます。

表 44-7 に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 44-7　システムおよびネットワーク統計情報を表示するためのコマンド

コマンド	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレスに ICMP エコー要求を送信します。
show ip igmp groups [*group-name* | *group-address* | *type number*]	スイッチに直接接続されている、IGMP によって取得されたマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	インターフェイスのマルチキャスト関連情報を表示します。
show ip mcache [*group* [*source*]]	IP 高速スイッチング キャッシュの内容を表示します。
show ip mpacket [*source-address* | *name*] [*group-address* | *name*] [**detail**]	回覧用キャッシュヘッダー バッファの内容を表示します。
show ip mroute [*group-name* | *group-address*] [*source*] [**summary**] [**count**] [**active** *kbps*]	IP マルチキャスト ルーティング テーブルの内容を表示します。
show ip pim interface [*type number*] [**count**]	PIM 用に設定されたインターフェイスの情報を表示します。
show ip pim neighbor [*type number*]	スイッチによって検出された PIM ネイバのリストを示します。
show ip pim rp [*group-name* | *group-address*]	SM マルチキャスト グループに関連付けられた RP ルータを表示します。

表 44-7　システムおよびネットワーク統計情報を表示するためのコマンド （続き）

コマンド	目的
show ip rpf {*source-address* | *name*}	スイッチの RPF の実行方法（ユニキャスト ルーティング テーブル、またはスタティック マルチキャスト ルーティングのいずれか）を表示します。
show ip sdr [*group* | “*session-name*” | **detail**]	Session Directory Protocol バージョン 2 のキャッシュを表示します。

IP マルチキャスト ルーティングのモニタ

表 44-8 に示す特権 EXEC コマンドを使用すると、IP マルチキャスト ルータ、パケット、パスをモニタできます。

表 44-8　IP マルチキャスト ルーティングをモニタするためのコマンド

コマンド	目的
mrinfo [*hostname* | *address*] [*source-address* | *interface*]	マルチキャスト ルータまたはマルチレイヤ スイッチとピアリングする近接マルチキャスト デバイスに関して、マルチキャスト ルータまたはマルチレイヤ スイッチをクエリーします。
mstat *source* [*destination*] [*group*]	IP マルチキャスト パケット速度および損失情報を表示します。
mtrace *source* [*destination*] [*group*]	指定されたグループのマルチキャスト配信ツリーに対して、送信元から宛先ブランチへのパスをトレースします。

CHAPTER 45

MSDP の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチに Multicast Source Discovery Protocol（MSDP）を設定する方法について説明します。MSDP によって、複数の Protocol-Independent Multicast Sparse-Mode（PIM-SM）ドメインが接続されます。

このソフトウェア リリースでは、MSDP と連携して動作する Multicast Border Gateway Protocol（MBGP）がサポートされていないため、MSDP は完全にはサポートされていません。ただし、MBGP が動作していない場合、MSDP と連携して動作するデフォルト ピアを作成できます。

この機能を使用するには、スイッチでメトロ IP アクセス イメージが稼動している必要があります。

（注） この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』*Release 12.2* を参照してください。

この章で説明する内容は、次のとおりです。

- 「MSDP の概要」（P.45-1）
- 「MSDP の設定」（P.45-3）
- 「MSDP のモニタおよびメンテナンス」（P.45-17）

MSDP の概要

MSDP を使用すると、さまざまなドメイン内のすべての Rendezvous Point（RP; ランデブー ポイント）に、グループのマルチキャスト送信元を通知できます。各 PIM-SM ドメインでは独自の RP が使用され、他のドメインの RP には依存しません。RP は Transmission Control Protocol（TCP）を通じて MSDP を実行し、他のドメイン内のマルチキャスト送信元を検出します。

PIM-SM ドメイン内の RP は、他のドメイン内の MSDP 対応デバイスと MSDP ピアリング関係にあります。ピアリング関係は TCP 接続を通じて発生します。交換されるのは、主にマルチキャスト グループを送信する送信元のリストです。RP 間の TCP 接続は、基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送信元のパスが確立されます。

このトポロジの目的は、ドメインから、他のドメイン内のマルチキャスト送信元を検出することです。マルチキャスト送信元がレシーバーのあるドメインを対象としている場合、マルチキャスト データは PIM-SM の通常の送信元ツリー構築メカニズムを通じて配信されます。MSDP は、グループを送信する送信元のアナウンスにも使用されます。これらのアナウンスは、ドメインの RP で発信する必要があります。

MSDP のドメイン間動作は、Border Gateway Protocol（BGP）または MBGP に大きく依存します。ドメイン内の RP（インターネットへのアナウンス対象であるグローバル グループを送信する送信元用の RP）で、MSDP を実行してください。

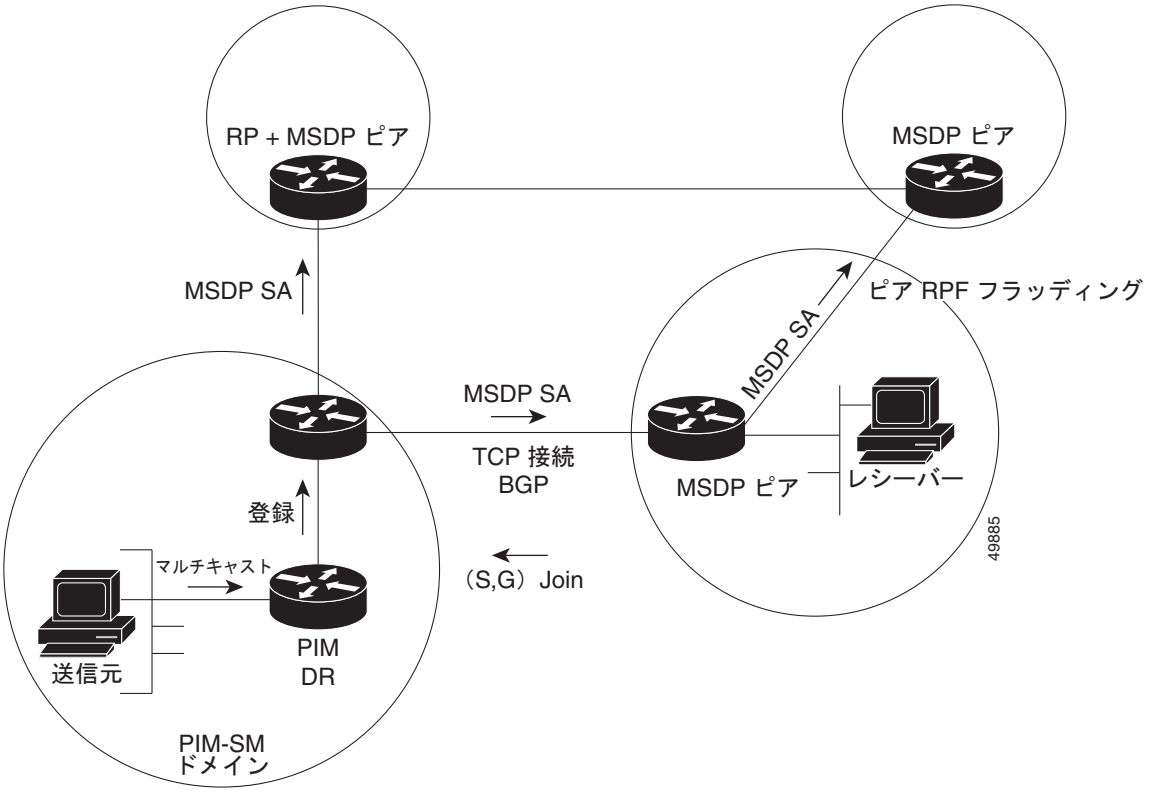
MSDP の動作

図 45-1 に、2 つの MSDP ピア間での MSDP の動作を示します。PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。MSDP が設定されている場合は、次のシーケンスが発生します。

送信元が最初のマルチキャスト パケットを送信すると、送信元に直接接続された先頭ホップ ルータ（*指定ルータ*または RP）によって RP に PIM Register メッセージが送信されます。RP は Register メッセージを使用し、アクティブな送信元を登録したり、ローカル ドメイン内の共有ツリーの下方向にマルチキャスト パケットを転送します。MSDP が設定されている場合は、Source-Active（SA）メッセージもすべての MSDP ピアに転送されます。送信元、送信元からの送信先であるグループ、および RP のアドレスまたは発信元 ID（RP アドレスとして使用されるインターフェイスの IP アドレス）が設定されている場合は、SA メッセージによってこれらが識別されます。

各 MSDP ピアは SA メッセージを発信元の RP から受信および転送し、ピア Reverse-Path Forwarding（RPF）フラッディングを実現します。MSDP デバイスは、BGP または MBGP ルーティング テーブルを調べ、どのピアが SA メッセージの発信元 RP へのネクスト ホップであるかを検出します。このようなピアは *RPF ピア*と呼ばれます。MSDP デバイスでは、RPF ピア以外のすべての MSDP ピアにメッセージが転送されます。BGP および MBGP がサポートされていない場合に MSDP を設定する方法については、「デフォルトの MSDP ピアの設定」（P.45-4）を参照してください。

図 45-1　　RP ピア間で動作する MSDP



MSDP ピアは、非 RPF ピアから発信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージを廃棄します。それ以外の場合、その MSDP ピアはすべての MSDP ピアにメッセージを転送します。

ドメインの RP ピアは MSDP ピアから SA メッセージを受信します。この RP が SA メッセージに記述されているグループへの Join 要求を持ち、空でない発信インターフェイス リストに（*,G）エントリが含まれている場合、そのグループはドメインの対象となり、RP から送信元方向に（S,G）Join メッセージが送信されます。（S,G）Join メッセージが送信元の DR に到達すると、送信元からリモート ドメイン内の RP への送信元ツリーのブランチが構築されます。この結果、マルチキャスト トラフィックを送信元から送信元ツリーを経由して RP へ、そしてリモート ドメイン内の共有ツリーを下ってレシーバーへと送信できます。

MSDP の利点

MSDP には次の利点があります。

- 共有されたマルチキャスト配信ツリーが分割され、共有ツリーがドメインに対してローカルになるように設定できます。ローカル メンバーはローカル ツリーに加わります。共有ツリーへの Join メッセージをドメイン外へ送信する必要はありません。
- PIM SM ドメインは独自の RP だけを信頼するため、他のドメインの RP に対する信頼度が低下します。このため、送信元の情報がドメイン外部に漏れないようにすることができ、セキュリティが高まります。
- レシーバーだけが配置されているドメインは、グループ メンバーシップをグローバルにアドバタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャスト ルーティング テーブル ステートが不要になり、コストが削減されます。

MSDP の設定

- 「MSDP のデフォルト設定」（P.45-3）
- 「デフォルトの MSDP ピアの設定」（P.45-4）（必須）
- 「SA ステートのキャッシング」（P.45-6）（任意）
- 「MSDP ピアからの送信元情報の要求」（P.45-8）（任意）
- 「スイッチから発信される送信元情報の制御」（P.45-8）（任意）
- 「スイッチで転送される送信元情報の制御」（P.45-11）（任意）
- 「スイッチで受信される送信元情報の制御」（P.45-13）（任意）
- 「MSDP メッシュ グループの設定」（P.45-15）（任意）
- 「MSDP ピアのシャットダウン」（P.45-15）（任意）
- 「MSDP への境界 PIM DM 領域の追加」（P.45-16）（任意）
- 「RP アドレス以外の発信元アドレスの設定」（P.45-17）（任意）

MSDP のデフォルト設定

MSDP はイネーブルになっていません。デフォルトの MSDP ピアはありません。

デフォルトの MSDP ピアの設定

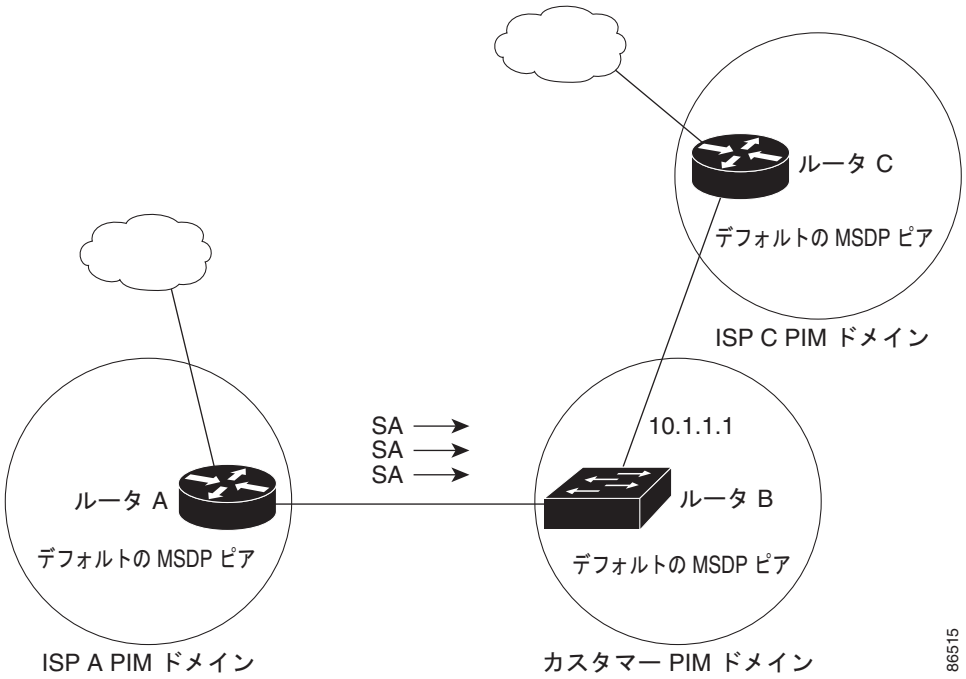
このソフトウェア リリースでは、BGP および MBGP がサポートされていないため、**ip msdp peer** グローバル コンフィギュレーション コマンドを使用してローカル スイッチに MSDP ピアを設定できません。その代わり、デフォルトの MSDP ピアを定義し、そこから送信されるスイッチのすべての SA メッセージを受信できます（そのためには、**ip msdp default-peer** グローバル コンフィギュレーション コマンドを使用します）。デフォルトの MSDP ピアは、事前に設定しておく必要があります。スイッチで MSDP ピアによる BGP または MBGP ピアリングが行われない場合は、デフォルトの MSDP ピアを設定します。単一の MSDP ピアが設定されている場合、スイッチでは常にそのピアからのすべての SA メッセージが受信されます。

図 45-2 に、デフォルトの MSDP ピアを使用できるネットワークを示します。図 45-2 では、スイッチ B を所有するカスタマーが、2 つの Internet Service Provider（ISP; インターネット サービス プロバイダー）に接続されています。一方の ISP はルータ A、もう一方の ISP はルータ C を所有しています。これらの ISP 間で、BGP または MBGP は動作していません。ISP のドメイン内、または他のドメイン内の送信元を学習するため、カスタマー サイトのスイッチ B はルータ A をデフォルトの MSDP ピアとして識別します。スイッチ B はルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、受信するのはルータ A からの SA メッセージ、またはルータ C からの SA メッセージだけです。ルータ A がコンフィギュレーション ファイルの最初に記述されている場合、ルータ A が動作していれば、ルータ A が使用されます。ルータ A が動作していない場合だけ、スイッチ B はルータ C からの SA メッセージを受信します。これが、プレフィクス リストがない場合のデフォルトの動作です。

プレフィクス リストを指定すると、ピアはリスト内のプレフィクス専用のデフォルト ピアになります。プレフィクス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。プレフィクス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアだけです（このピアにルータが接続されていて、ピアがアクティブの場合に限ります）。最初に設定されたデフォルト ピアに障害が発生した場合、またはこのピアが正常に接続されていない場合は、2 番めに設定されているピアがアクティブなデフォルト ピアになります。以下同様に処理されます。

通常、ISP はプレフィクス リストを使用して、カスタマーのルータから受信するプレフィクスを定義します。

図 45-2　デフォルトの MSDP ピア ネットワーク



デフォルトの MSDP ピアを指定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp default-peer** *ip-address* | *name* [**prefix-list** *list*]	すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。 • *ip-address* | *name* には、MSDP デフォルト ピアの IP アドレスまたは Domain Name System（DNS; ドメイン ネーム システム）サーバ名を入力します。 • （任意）**prefix-list** *list* を指定する場合は、リスト内のプレフィクス専用のデフォルト ピアとなるピアを指定するリスト名を入力します。プレフィクス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 キーワード **prefix-list** を指定して **ip msdp default-peer** コマンドを複数入力すると、複数の RP プレフィクスに対してすべてのデフォルト ピアが同時に使用されます。この構文は通常、スタブ サイト クラウドに接続されたサービス プロバイダー クラウドで使用されます。 キーワード **prefix-list** を指定せずに **ip msdp default-peer** コマンドを複数入力すると、単一のアクティブ ピアですべての SA メッセージが受信されます。このピアに障害がある場合は、次の設定済みデフォルト ピアですべての SA メッセージが受信されます。この構文は通常、スタブ サイトで使用されます。

	コマンド	目的
ステップ 3	**ip prefix-list** *name* [**description** *string*] | **seq** *number* {**permit** | **deny**} *network length*	（任意）ステップ 2 で指定された名前を使用し、プレフィクス リストを作成します。 • （任意）**description** *string* を指定する場合は、このプレフィクス リストを説明する 80 文字以下のテキストを入力します。 • **seq** *number* には、エントリのシーケンス番号を入力します。指定できる範囲は 1 ～ 4294967294 です。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。 • キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *network length* には、許可または拒否されているネットワークの番号およびネットワーク マスク長（ビット単位）を指定します。
ステップ 4	**ip msdp description** {*peer-name* | *peer-address*} *text*	（任意）設定内で、または **show** コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。 デフォルトでは、MSDP ピアに説明は関連付けられていません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト ピアを削除するには、**no ip msdp default-peer** *ip-address* | *name* グローバル コンフィギュレーション コマンドを使用します。

次に、図 45-2 のルータ A およびルータ C の設定の一部を示します。それぞれの ISP には、デフォルト ピア（BGP または MBGP 以外）を使用する複数のカスタマーが存在します（図 45-2 のカスタマーと同様）。この場合、両方の ISP で類似した設定となります。つまり、両方の ISP では、対応するプレフィクス リストで SA が許可されている場合、デフォルト ピアからの SA だけが受信されます。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

SA ステートのキャッシング

デフォルトでは、スイッチで受信された SA メッセージ内の送信元とグループのペアは、キャッシュに格納されません。また、MSDP SA 情報が転送される場合、この情報はメモリに格納されません。したがって、ローカル RP で SA メッセージが受信された直後にメンバーがグループに加入した場合、次の SA メッセージによって送信元に関する情報が取得されるまでそのメンバーは待機する必要があります。この遅延は加入遅延と呼ばれます。

メモリを消費して送信元情報の遅延を短縮する場合は、SA メッセージをキャッシュに格納するようにスイッチを設定できます。

送信元とグループのペアのキャッシングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp cache-sa-state** [**list** *access-list-number*]	送信元とグループのペアのキャッシングをイネーブルにします（SA ステートを作成します）。アクセス リストを通過したこれらのペアがキャッシュに格納されます。 **list** *access-list-number* を指定する場合、範囲は 100 ～ 199 です。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 100 ～ 199 です。ステップ 2 で作成した番号と同じ値を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注）　このコマンドの代わりに、**ip msdp sa-request** グローバル コンフィギュレーション コマンドを使用できます。代替コマンドを使用すると、グループの新しいメンバーがアクティブになった場合に、SA 要求メッセージがスイッチから MSDP ピアに送信されます。詳細については、次のセクションを参照してください。

デフォルト設定（SA ステートが作成されていない状態）に戻すには、**no ip msdp cache-sa-state** グローバル コンフィギュレーション コマンドを使用します。

次に、グループ 224.2.0.0/16 への送信元である 171.69.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
Switch(config)# ip msdp cache-sa-state 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

MSDP ピアからの送信元情報の要求

ローカル RP では、SA 要求を送信し、指定されたグループに対するすべてのアクティブな送信元の要求をすぐに取得できます。デフォルトでは、新しいメンバーがグループに加入してマルチキャスト トラフィックを受信する必要が生じた場合、スイッチは MSDP ピアに SA 要求メッセージを送信しません。新しいメンバーは次の定期的な SA メッセージを受信する必要があります。

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバーが学習する必要がある場合は、新しいメンバーがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。ピアは SA キャッシュ内の情報に応答します。ピアにキャッシュが設定されていない場合、このコマンドを実行しても何も起こりません。この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバーがグループに加入し、マルチキャスト トラフィックを受信する必要が生じた場合、MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp sa-request** {*ip-address* | *name*}	指定された MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定します。 *ip-address* | *name* を指定する場合は、グループの新しいメンバーがアクティブになるときにローカル スイッチの SA メッセージの要求元になる MSDP ピアの IP アドレス、または名前を入力します。 SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip msdp sa-request** {*ip-address* | *name*} グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

スイッチから発信される送信元情報の制御

スイッチから発信されるマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元（送信元ベース）
- 送信元情報のレシーバー（要求元認識ベース）

詳細については、「送信元の再配信」（P.45-9）および「SA 要求メッセージのフィルタリング」（P.45-10）を参照してください。

送信元の再配信

SA メッセージは、送信元が登録されている RP で発信されます。デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。送信元が登録されている場合は、RP に *A フラグ*が設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA に格納されてアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp redistribute** [**list** *access-list-name*] [**asn** *aspath-access-list-number*] [**route-map** *map*]	SA メッセージに格納されてアドバタイズされる、マルチキャスト ルーティング テーブル内の（S,G）エントリを設定します。 デフォルトでは、ローカル ドメイン内の送信元だけがアドバタイズされます。 • （任意）**list** *access-list-name* を指定するときは、IP 標準または IP 拡張アクセス リストの名前または番号を入力します。標準アクセス リストの範囲は 1 ～ 99、拡張アクセス リストの範囲は 100 ～ 199 です。アクセス リストによって、アドバタイズされるローカルな送信元、および送信されるグループが制御されます。 • （任意）**asn** *aspath-access-list-number* を指定する場合は、1 ～ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は **ip as-path access-list** コマンドでも設定する必要があります。 • （任意）**route-map** *map* を指定する場合は、1 ～ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は **ip as-path access-list** コマンドでも設定する必要があります。 アクセス リストまたは自律システム パス アクセス リストに従って、（S,G）ペアがアドバタイズされます。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。
	または	または
	access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、標準アクセス リストの範囲は 1 ～ 99、拡張アクセス リストの範囲は 100 ～ 199 を入力します。ステップ 2 で作成した番号と同じ値を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

フィルタを削除するには、**no ip msdp redistribute** グローバル コンフィギュレーション コマンドを使用します。

SA 要求メッセージのフィルタリング

デフォルトでは、SA 情報をキャッシングしているスイッチだけが、SA 要求に応答します。このようなスイッチでは、デフォルトで MSDP ピアからのすべての SA 要求メッセージが採用され、アクティブな送信元の IP アドレスが取得されます。

ただし、MSDP ピアからの SA 要求をすべて無視するように、スイッチを設定できます。標準アクセス リストに記述されたグループのピアからの SA 要求メッセージだけを採用することもできます。アクセス リスト内のグループが指定された場合は、そのグループのピアからの SA 要求メッセージが受信されます。他のグループのピアからの他のメッセージは、すべて無視されます。

これらの方法のいずれかを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp filter-sa-request** *ip-address* | *name* または **ip msdp filter-sa-request** {*ip-address* | *name*} **list** *access-list-number*	指定された MSDP ピアからの SA 要求メッセージをすべてフィルタリングします。 または 標準アクセス リストを通過したグループに対して、指定された MSDP ピアからの SA 要求メッセージをフィルタリングします。アクセス リストには、複数のグループ アドレスが記述されています。access-list-number の範囲は 1 ～ 99 です。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip msdp filter-sa-request** {*ip-address* | *name*} グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.2.2 の MSDP ピアからの SA 要求メッセージをフィルタリングするように、スイッチを設定する例を示します。ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージはアクセス リスト 1 を通過して、受信されます。その他のすべてのメッセージは無視されます。

```
Switch(config)# ip msdp filter sa-request 171.69.2.2 list 1
Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

スイッチで転送される送信元情報の制御

デフォルトでは、スイッチで受信されたすべての SA メッセージが、すべての MSDP ピアに転送されます。ただし、フィルタリングするか、または Time To Live（TTL）値を設定し、発信メッセージがピアに転送されないようにできます。次のセクションでは、この方法について説明します。

フィルタの使用法

フィルタを作成すると、次のいずれかの処理を実行できます。

- すべての送信元とグループのペアのフィルタリング
- 特定の送信元とグループのペアだけが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致基準に基づくフィルタリング

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp sa-filter out** *ip-address* | *name*	指定された MSDP ピアへの SA メッセージをフィルタリングします。
	または	または
	ip msdp sa-filter out {*ip-address* | *name*} **list** *access-list-number*	IP 拡張アクセス リストを通過する、指定されたピア宛ての SA メッセージだけを通過させます。拡張アクセス リスト *access-list-number* の範囲は 100 ～ 199 です。 **list** と **route-map** の両方のキーワードを使用すると、すべての条件が true である場合に、発信 SA メッセージ内のすべての（S,G）ペアが通過します。
	または	または
	ip msdp sa-filter out {*ip-address* | *name*} **route-map** *map-tag*	ルート マップ *map-tag* 内の一致基準を満たす、指定された MSDP ピア宛の SA メッセージを通過させます。 すべての一致基準が true の場合、ルート マップに **permit** が指定されていれば、ルートはフィルタを通過します。**deny** が指定されていれば、ルートはフィルタリングされます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	（任意）IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

フィルタを削除するには、**no ip msdp sa-filter out** {*ip-address* | *name*} [**list** *access-list-number*] [**route-map** *map-tag*] グローバル コンフィギュレーション コマンドを使用します。

次に、アクセス リスト 100 を通過する（S,G）ペアだけが SA メッセージに格納され、*switch.cisco.com* という名前のピアに転送されるように設定する例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter out switch.cisco.com list 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。IP ヘッダー TTL 値が *ttl* 引数以上であるマルチキャスト パケットだけが、指定された MSDP ピアに送信されます。たとえば、内部トラフィックの TTL 値を 8 に制限できます。他のグループを外部に送信する場合は、これらのパケットの TTL を 8 より大きく設定して送信する必要があります。

TTL しきい値を確立するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp ttl-threshold** {*ip-address* | *name*} *ttl*	指定された MSDP ピア宛ての最初の SA メッセージにカプセル化されるマルチキャスト データを制限します。 • *ip-address* | *name* を指定する場合は、TTL の制限が適用される MSDP ピアの IP アドレスまたは名前を入力します。 • *ttl* には、TTL 値を入力します。デフォルトは 0 です。この場合、すべてのマルチキャスト データ パケットは、TTL がなくなるまでピアに転送されます。指定できる範囲は 0 ～ 255 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip msdp ttl-threshold** {*ip-address* | *name*} グローバル コンフィギュレーション コマンドを使用します。

スイッチで受信される送信元情報の制御

デフォルトでは、スイッチは、MSDP の RPF ピアによって送信されたすべての SA メッセージを受信します。ただし、着信 SA メッセージをフィルタリングし、MSDP ピアから受信する送信元情報を制御できます。つまり、特定の着信 SA メッセージを受信しないようにスイッチを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージのフィルタリング
- 特定の送信元とグループのペアが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致基準に基づくフィルタリング

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp sa-filter in** *ip-address* | *name* または **ip msdp sa-filter in** {*ip-address* | *name*} **list** *access-list-number* または **ip msdp sa-filter in** {*ip-address* | *name*} **route-map** *map-tag*	指定された MSDP ピアからの SA メッセージをすべてフィルタリングします。 または IP 拡張アクセス リストを通過する、指定されたピアからの SA メッセージだけを通過させます。拡張アクセス リスト *access-list-number* の範囲は 100 ～ 199 です。 **list** と **route-map** の両方のキーワードを使用すると、すべての条件が true である場合に、着信 SA メッセージ内のすべての（S,G）ペアが通過します。 または ルート マップ *map-tag* 内の一致基準を満たす、指定された MSDP ピアからの SA メッセージを通過させます。 すべての一致基準が true の場合、ルート マップに **permit** が指定されていれば、ルートはフィルタを通過します。**deny** が指定されていれば、ルートはフィルタリングされます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	（任意）IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • キーワード **deny** を指定すると、条件が一致した場合にアクセスが拒否されます。キーワード **permit** を指定すると、条件が一致した場合にアクセスが許可されます。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を入れます。 アクセス リストの末尾には、すべてに適用される暗黙の拒否文が常に存在することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

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

フィルタを削除するには、**no ip msdp sa-filter in** {*ip-address* | *name*} [**list** *access-list-number*] [**route-map** *map-tag*] グローバル コンフィギュレーション コマンドを使用します。

次に、*switch.cisco.com* という名前のピアからのすべての SA メッセージをフィルタリングする例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter in switch.cisco.com
```

MSDP メッシュ グループの設定

MSDP メッシュ グループは、MSDP によって完全なメッシュ型に相互接続された MSDP スピーカーのグループです。メッシュ グループ内のピアから受信された SA メッセージは、同じメッシュ グループ内の他のピアに転送されません。したがって、SA メッセージのフラッディングが削減され、ピア RPF フラッディングが簡素化されます。ドメイン内に複数の RP がある場合は、**ip msdp mesh-group** グローバル コンフィギュレーション コマンドを使用します。特に、ドメインにわたって SA メッセージを送信する場合に使用します。単一のスイッチに複数のメッシュ グループを（異なる名前で）設定できます。

メッシュ グループを作成するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp mesh-group** *name* {*ip-address* | *name*}	MSDP メッシュ グループを設定するには、そのメッシュ グループに属する MSDP ピアを指定します。 デフォルトでは、MSDP ピアはメッシュ グループに属しません。 • *name* には、メッシュ グループの名前を入力します。 • *ip-address* | *name* には、メッシュ グループのメンバーになる MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 6		グループ内の MSDP ピアごとに、この手順を繰り返します。

メッシュ グループから MSDP ピアを削除するには、**no ip msdp mesh-group** *name* {*ip-address* | *name*} グローバル コンフィギュレーション コマンドを使用します。

MSDP ピアのシャットダウン

複数の MSDP コマンドが設定された単一のピアをアクティブにしない場合は、ピアをシャットダウンしてから、あとで起動できます。ピアがシャットダウンすると、TCP 接続が終了し、再起動されません。ピアの設定情報を保持したまま、MSDP セッションをシャットダウンすることもできます。

ピアをシャットダウンするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp shutdown** {*peer-name* | *peer address*}	設定情報を保持したまま、指定された MSDP ピアを管理上のシャットダウン状態にします。 *peer-name* | *peer address* を指定する場合は、シャットダウンする MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ピアを再起動するには、**no ip msdp shutdown** {*peer-name* | *peer address*} グローバル コンフィギュレーション コマンドを使用します。TCP 接続が再確立されます。

MSDP への境界 PIM DM 領域の追加

Dense-Mode（DM; dense [密] モード）領域と PIM SM 領域の境界となるスイッチに MSDP を設定します。デフォルトでは、DM 領域のアクティブな送信元は MSDP に参加しません。

（注）　**ip msdp border sa-address** グローバル コンフィギュレーション コマンドの使用は推奨できません。DM ドメイン内の送信元が SM ドメイン内の RP にプロキシ登録されるように SM ドメイン内の境界ルータを設定し、標準 MSDP 手順でこれらの送信元をアドバタイズするように SM ドメインを設定してください。

DM 領域でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp border sa-address** *interface-id*	DM 領域内のアクティブな送信元に関する SA メッセージを送信するように、DM 領域と SM 領域の境界スイッチを設定します。 *interface-id* には、SA メッセージ内の RP アドレスとして使用される、IP アドレスの配信元となるインターフェイスを指定します。 インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。
ステップ 3	**ip msdp redistribute** [**list** *access-list-name*] [**asn** *aspath-access-list-number*] [**route-map** *map*]	SA メッセージに格納されてアドバタイズされる、マルチキャスト ルーティング テーブル内の（S,G）エントリを設定します。 詳細については、「送信元の再配信」（P.45-9）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ip msdp originator-id グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。**ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

デフォルト設定（DM 領域内のアクティブな送信元が MSDP に参加しない設定）に戻すには、**no ip msdp border sa-address** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

RP アドレス以外の発信元アドレスの設定

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用する場合は、送信元 ID を変更します。次のいずれかの場合に送信元 ID を変更できます。

- MSDP メッシュ グループ内の複数のスイッチ上で、ローカルな RP を設定する場合
- PIM SM ドメインと DM ドメインの境界となるスイッチがある場合。サイトの DM ドメインの境界となるスイッチがあり、SM がその外部で使用されている場合は、DM の送信元を外部に通知する必要があります。このスイッチは RP でないため、SA メッセージで使用される RP アドレスはありません。したがって、このコマンドではインターフェイスのアドレスを指定し、RP アドレスを提供します。

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp originator-id** *interface-id*	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。 *interface-id* には、ローカル スイッチのインターフェイスを指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ip msdp border sa-address と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスによって RP アドレスが決まります。

この方法で RP アドレスが取得されないようにするには、**no ip msdp originator-id** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

MSDP のモニタおよびメンテナンス

MSDP SA メッセージ、ピア、ステート、またはピア ステータスをモニタするには、表 45-1 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 45-1　MSDP のモニタおよびメンテナンスのためのコマンド

コマンド	目的
debug ip msdp [*peer-address* | *name*] [**detail**] [**routes**]	MSDP アクティビティをデバッグします。
debug ip msdp resets	MSDP ピアのリセット原因をデバッグします。
show ip msdp count [*autonomous-system-number*]	SA メッセージに格納され、各自律システムから発信された送信元およびグループの個数を表示します。**ip msdp cache-sa-state** コマンドは、このコマンドによって出力が生成されるように設定する必要があります。
show ip msdp peer [*peer-address* | *name*]	MSDP ピアに関する詳細情報を表示します。
show ip msdp sa-cache [*group-address* | *source-address* | *group-name* | *source-name*] [*autonomous-system-number*]	MSDP ピアから学習した（S,G）ステートを表示します。
show ip msdp summary	MSDP ピア ステータスおよび SA メッセージ数を表示します。

MSDP 接続、統計情報、または SA キャッシュ エントリをクリアするには、表 45-2 に示す特権 EXEC コマンドを使用します。

表 45-2　MSDP 接続、統計情報、または SA キャッシュ エントリをクリアするためのコマンド

コマンド	目的
clear ip msdp peer *peer-address* | *name*	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。
clear ip msdp statistics [*peer-address* | *name*]	セッションをリセットせずに、1 つまたはすべての MSDP ピア統計情報カウンタをクリアします。
clear ip msdp sa-cache [*group-address* | *name*]	すべてのエントリの SA キャッシュ エントリ、特定のグループのすべての送信元、または特定の送信元とグループのペアのすべてのエントリをクリアします。

CHAPTER 46

トラブルシューティング

この章では、Cisco IOS ソフトウェアに関連する、Cisco ME 3400E スイッチのソフトウェア問題を特定し、解決する方法について説明します。

問題の特定および解決には、CLI（コマンドライン インターフェイス）を使用できます。

ハードウェアに関連するその他のトラブルシューティング情報は、ハードウェア インストレーション ガイドで提供されます。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、および『*Cisco IOS Command Summary*』*Release 12.2* を参照してください。

- 「ソフトウェアの障害からの回復」（P.46-2）
- 「パスワードを忘れた場合の回復」（P.46-3）

（注） 回復手順を実行するには、スイッチを直接操作しなければなりません。

- 「自動ネゴシエーションの不一致の防止」（P.46-8）
- 「SFP モジュールのセキュリティと識別」（P.46-8）
- 「SFP モジュール ステータスのモニタリング」（P.46-9）
- 「温度のモニタリング」（P.46-9）
- 「ping の使用」（P.46-10）
- 「レイヤ 2 traceroute の使用」（P.46-13）
- 「IP traceroute の使用」（P.46-15）
- 「TDR の使用」（P.46-16）
- 「debug コマンドの使用」（P.46-17）
- 「show platform forward コマンドの使用例」（P.46-19）
- 「crashinfo ファイルの使用」（P.46-21）
- 「オンボード障害ロギングの使用」（P.46-21）

ソフトウェアの障害からの回復

アップグレード時にスイッチ ソフトウェアで障害が発生する状況としては、スイッチに誤ったファイルをダウンロードした場合、およびイメージ ファイルを削除した場合が考えられます。いずれの場合にも、スイッチは Power-on Self-Test（POST; 電源投入時セルフテスト）をパスしなくなり、接続ができなくなります。

次の手順ではブートローダ コマンドおよび TFTP を使用し、イメージ ファイルが壊れた状況、またはイメージ ファイルを間違えた状況からの回復を図ります。ここで紹介する回復手順を実行するには、スイッチを直接操作する必要があります。

ステップ 1　PC 上で、Cisco.com から tar 形式のソフトウェア イメージ ファイル（*image_filename.tar*）をダウンロードします。

Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルで格納されます。Cisco.com 上のソフトウェア イメージ ファイルの検索方法については、リリース ノートを参照してください。

ステップ 2　tar ファイルから bin ファイルを抽出します。

- Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して bin ファイルを特定し、抽出します。
- UNIX を使用している場合は、次の手順に従ってください。

1. **tar -tvf** <*image_filename.tar*> UNIX コマンドを使用して、tar ファイルの内容を表示します。

```
switch% tar -tvf image_filename.tar
```

2. **tar -xvf** <*image_filename.tar*> <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルを特定し、抽出します。

```
switch% tar -xvf image_filename.tar image_filename.bin
x image_filename/image_filename.bin, 3970586 bytes, 7756 tape blocks
```

3. **ls -l** <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。

```
switch% ls -l image_filename.bin
-rw-r--r--   1 boba      3970586 Apr 21 12:00 image_filename/image_filename.bin
```

ステップ 3　PC をスイッチのイーサネット管理ポートに接続します。

ステップ 4　スイッチの電源コードを取り外します。

ステップ 5　**Mode** ボタンを押しながら、電源コードを再度スイッチに接続します。

ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、**Mode** ボタンを放します。ソフトウェアに関する数行分の情報と指示が表示されます。

```
The system has been interrupted prior to initializing the flash file system.The
following commands will initialize the flash file system, and finish loading the
operating system software#

flash_init
boot
```

ステップ 6　フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

ステップ 7　イーサネット管理ポートを経由して、スイッチを TFTP サーバに接続します。

ステップ 8　TFTP を使用し、ファイル転送を開始します。

a.　TFTP サーバの IP アドレスを指定します。

```
switch: set ip_addr ip_address/mask
```

b. デフォルトのルータを指定します。

```
switch: set default_router ip_address
```

ステップ 9　ソフトウェア イメージを TFTP サーバからスイッチにコピーします。

```
switch: copy tftp://ip_address/filesystem:/source-file-url flash:image_filename.bin
```

ステップ 10　新規にダウンロードされた Cisco IOS イメージを起動します。

```
switch: boot flash:image_filename.bin
```

ステップ 11　**archive download-sw** 特権 EXEC コマンドを使用して、スイッチまたはスイッチ スタックにソフトウェア イメージをダウンロードします。

ステップ 12　**reload** 特権 EXEC コマンドを使用して、スイッチを再起動し、新規ソフトウェア イメージが適切に動作していることを確認します。

ステップ 13　スイッチから、flash:*image_filename.bin* ファイルを削除します。

パスワードを忘れた場合の回復

スイッチのデフォルト設定では、エンドユーザは、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを失くした状態から回復できます。

（注）　これらのスイッチでは、エンドユーザがデフォルト設定に戻すことに同意するだけでパスワードをリセットできます。それにより、システム管理者はこの機能の一部をディセーブルにできます。パスワード回復がディセーブルの場合に、エンド ユーザがパスワードをリセットしようとすると、回復プロセス中にこれを示すステータス メッセージが表示されます。

パスワード回復のディセーブル化では、未許可のユーザによるコンフィギュレーション ファイルへのアクセスを防止することにより、コンフィギュレーション ファイルのセキュリティを確保します。

Cisco ME スイッチのブート ローダでは、パスワード回復目的の自動ブート シーケンスを停止するのに、ブレーク キー検出を使用します。

（注）　ブレーク キーの文字は、オペレーティング システムにより異なります。

UNIX を実行する SUN ワーク ステーションでは、Ctrl-C がブレーク キーとなります。

Windows XP または 2000 を実行する PC では、Ctrl-Break がブレーク キーとなります。Cisco TAC では、一般的なオペレーティング システムのブレーク キーおよびブレーク キーをサポートしないそれらの端末エミュレータのために代わりとなるブレーク キー シーケンスについて、リストとして提供しています。このリストについては、http://www.cisco.com/warp/public/701/61.html#how-to にアクセスしてください。

ここでは、スイッチのパスワードを忘れた場合の回復手順について説明します。

- 「パスワード回復がイネーブルになっている場合の手順」（P.46-4）
- 「パスワード回復がディセーブルになっている場合の手順」（P.46-6）

パスワード回復をイネーブルまたはディセーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

スイッチのパスワードを忘れた場合は、次の手順に従ってください。

ステップ 1　端末エミュレーション ソフトウェアが稼動している端末または PC をスイッチのコンソール ポートに接続します。

ステップ 2　エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 3　スイッチの電源を切ります。

スイッチに電源コードを再接続します。

ステップ 4　スイッチは、POST を実行してから、自動ブート プロセスを開始します。ブート ローダは、ブート アップ シーケンス中にユーザにブレーク キーの文字を求めるプロンプトを表示します（次の例を参照）。

```
***** The system will autoboot in 5 seconds *****

Send a break key to prevent autobooting.
```

システムが自動ブートを行うというメッセージを受信してから 5 秒以内にコンソール ターミナルにブレーク キーを入力する必要があります。システム LED は、ブレーク キーを受け入れるまでグリーンで点滅します。システム LED は、ブレーク キーを受け入れると、スイッチがブートされるまで消灯します。

ソフトウェアに関する数行分の情報と指示が表示され、パスワード回復手順がディセーブルになっていないかどうかが通知されます。

- 次のような開始のメッセージが表示された場合

```
The system has been interrupted, or encountered an error during initializion of the
flash filesystem. The following commands will initialize the flash filesystem, and
finish loading the operating system software:

flash_init
load_helper
boot
```

「パスワード回復がイネーブルになっている場合の手順」（P.46-4）に進んで、その手順を実行します。

- 次のような開始のメッセージが表示された場合

```
The password-recovery mechanism has been triggered, but is currently disabled.
```

「パスワード回復がディセーブルになっている場合の手順」（P.46-6）に進んで、その手順を実行します。

ステップ 5　パスワードが回復したら、スイッチをリロードします。

```
Switch> reload
Proceed with reload? [confirm] y
```

パスワード回復がイネーブルになっている場合の手順

パスワード回復メカニズムがイネーブルになっている場合は、次のメッセージが表示されます。

```
The system has been interrupted, or encountered an error during initializion of the flash
filesystem. The following commands will initialize the flash filesystem, and finish
loading the operating system software:

flash_init
load_helper
boot
```

ステップ 1　フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

ステップ 2　コンソール ポートの速度を 9600 以外に設定していた場合は、9600 にリセットされています。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合せて変更します。

ステップ 3　ヘルパー ファイルのロード

```
switch: load_helper
```

ステップ 4　フラッシュ メモリの内容を表示します。

```
switch: dir flash:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
   13  drwx         192   Mar 01 1993 22:30:48 image-name-mz.122-50-EX
   11  -rwx        5825   Mar 01 1993 22:31:59  config.text
   18  -rwx         720   Mar 01 1993 02:21:30  vlan.dat

16128000 bytes total (10003456 bytes free)
```

ステップ 5　コンフィギュレーション ファイルの名前を config.text.old に変更します。

このファイルには、パスワード定義が格納されています。

```
switch: rename flash:config.text flash:config.text.old
```

ステップ 6　システムを起動します。

```
switch: boot
```

Setup プログラムを起動するように求められます。プロンプトに **N** を入力します。

```
Continue with the configuration dialog? [yes/no]: N
```

ステップ 7　スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
```

ステップ 8　コンフィギュレーション ファイルを元の名前に戻します。

```
Switch# rename flash:config.text.old flash:config.text
```

ステップ 9　コンフィギュレーション ファイルをメモリにコピーします。

```
Switch# copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
```

確認を求めるプロンプトに、**Return** キーを押して応答します。

コンフィギュレーション ファイルがリロードされ、パスワードの変更が可能となります。

ステップ 10　グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 11　パスワードを変更します。

```
Switch (config)# enable secret password
```

シークレット パスワードは 1 ～ 25 文字の英数字です。数字から開始でき、大文字と小文字は区別されます。スペースも使用できますが、先頭のスペースは無視されます。

ステップ 12　特権 EXEC モードに戻ります。

```
Switch (config)# exit
Switch#
```

ステップ 13　実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Switch# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。

（注）　上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン ステートになることがあります。**show running-config** 特権 EXEC コマンドを入力することにより、このインターフェイスを識別できます。インターフェイスを再びイネーブルにするには、**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力し、シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コンフィギュレーション モードの状態で、**no shutdown** コマンドを入力します。

ステップ 14　スイッチをリロードします。

```
Switch# reload
```

パスワード回復がディセーブルになっている場合の手順

パスワード回復メカニズムがディセーブルの場合、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

注意　スイッチをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合せて、バックアップ スイッチと VLAN コンフィギュレーション ファイルの有無を確認してください。

（注）　パスワード回復のディセーブル化では、未許可ユーザによるコンフィギュレーション ファイルへのアクセスを防止することにより、コンフィギュレーション ファイルのセキュリティを実現します。

- **n**（no）を入力すると、**ブレーク キー**が押されていなかった場合のように、通常の起動プロセスが継続されます。ブート ローダ プロンプトにアクセスできないため、新しいパスワードは入力できません。次のメッセージが表示されます。

```
Press Enter to continue........
```

- **y**（yes）を入力すると、フラッシュ メモリ内のコンフィギュレーション ファイルおよび VLAN データベース ファイルが削除されます。デフォルト設定がロードされたら、パスワードをリセットできます。

ステップ 1　パスワード回復手順の継続を選択すると、既存の設定が失われます。

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

ステップ 2　ヘルパー ファイルのロード

```
Switch: load_helper
```

ステップ 3　フラッシュ メモリの内容を表示します。

```
switch: dir flash:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
13  drwx         192   Mar 01 1993 22:30:48 image-name-mz.122-50-SE

16128000 bytes total (10003456 bytes free)
```

ステップ 4　システムを起動します。

```
Switch: boot
```

Setup プログラムを起動するように求められます。パスワード回復手順を継続するには、プロンプトに **N** を入力します。

```
Continue with the configuration dialog? [yes/no]: N
```

ステップ 5　スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
```

ステップ 6　グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 7　パスワードを変更します。

```
Switch (config)# enable secret password
```

シークレット パスワードは 1 ～ 25 文字の英数字です。数字から開始でき、大文字と小文字は区別されます。スペースも使用できますが、先頭のスペースは無視されます。

ステップ 8　特権 EXEC モードに戻ります。

```
Switch (config)# exit
Switch#
```

ステップ 9　実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Switch# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。

（注）　上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン ステートになることがあります。**show running-config** 特権 EXEC コマンドを入力することにより、このインターフェイスを識別できます。インターフェイスを再びイネーブルにするには、**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力し、シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コンフィギュレーション モードの状態で、**no shutdown** コマンドを入力します。

ステップ 10　ここでスイッチを再設定する必要があります。バックアップ スイッチと VLAN コンフィギュレーション ファイルがシステム管理者によって利用できるようになっている場合は、それらを利用します。

自動ネゴシエーションの不一致の防止

IEEE（米国電気電子学会）802.3ab 自動ネゴシエーション プロトコルは、スイッチの速度（SFP モジュール ポートを除く 10 Mbps、100 Mbps、1000 Mbps）およびデュプレックス（半二重または全二重）に関する設定を管理します。このプロトコルでは、状況によって設定の不一致が生じ、その結果、パフォーマンスの低下を招くことがあります。設定の不一致は、次の状況下で発生します。

- 手動で設定した速度またはデュプレックス パラメータが、接続先ポートの手動で設定された速度またはデュプレックス パラメータと異なる。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている。

スイッチのパフォーマンスを最大限に高めてリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。

（注）　接続先装置が自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定を一致させます。速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

SFP モジュールのセキュリティと識別

シスコの Small Form-Factor Pluggable（SFP）モジュールに搭載されているシリアル EEPROM（電気的に消去可能でプログラミング可能な ROM）には、モジュールのシリアル番号、ベンダーの名前と ID、固有のセキュリティ コード、Cyclic Redundancy Check（CRC; 巡回冗長検査）が格納されています。SFP モジュールがスイッチに搭載されると、スイッチのソフトウェアが EEPROM を読み取り、シリアル番号とベンダーの名前、ベンダー ID を検証して、セキュリティ コードと CRC を再計算します。シリアル番号、ベンダーの名前またはベンダー ID、セキュリティ コード、CRC のいずれかが無効である場合は、セキュリティ エラー メッセージが生成され、そのインターフェイスは errordisable エラーディセーブル ステートになります。

（注）　セキュリティ エラー メッセージでは、GBIC_SECURITY ファシリティが参照されます。スイッチは SFP モジュールをサポートしますが、GBIC（ギガビット インターフェイス コンバータ）モジュールをサポートしません。エラー メッセージ テキストでは GBIC インターフェイスおよびモジュールが参照されますが、セキュリティ メッセージが実際に参照するのは SFP モジュールおよびモジュール インターフェイスです。エラー メッセージの詳細については、このリリースに対応するシステム メッセージ ガイドを参照してください。

シスコ製品以外の SFP モジュールを使用している場合は、スイッチから SFP モジュールを取り外し、シスコ製のモジュールと交換してください。シスコ製の SFP モジュールを取り付けたあと、**errdisable recovery cause gbic-invalid** グローバル コンフィギュレーション コマンドを使用してポートのステータスを検証し、errdisable ステートから回復するためのタイム インターバルを開始します。タイム インターバルが経過すると、スイッチはそのインターフェイスを errdisable ステートから復帰させ、再起動します。**errdisable recovery** コマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

モジュールがシスコ製の SFP モジュールとして識別されたにもかかわらず、システムがベンダーデータ情報を読み取ってその情報が正確かどうかを確認できない場合は、SFP モジュールによってエラー メッセージが生成されます。この場合は、SFP モジュールを取り外して、取り付け直す必要があります。それでも障害が発生する場合は、SFP モジュールに障害がある可能性があります。

SFP モジュール ステータスのモニタリング

show interfaces transceiver 特権 EXEC コマンドを使用して、SFP モジュールの物理上および動作上のステータスをチェックできます。このコマンドは、特定のインターフェイス上にある SFP モジュールの温度や電流などの動作上のステータス、およびアラーム ステータスを表示します。また、SFP モジュールの速度およびデュプレックス設定をチェックするのにこのコマンドを使用できます。詳細については、このリリースのコマンド リファレンスに記載された **show interfaces transceiver** コマンドの説明を参照してください。

温度のモニタリング

Cisco ME スイッチは、温度状態をモニタリングします。スイッチでは温度情報が使用されてファンも制御されます。温度の値は、スイッチ内の温度です（外部温度ではありません）。温度が OK か不正かを確認するには、**show env temperature** 特権 EXEC コマンドを使用します。

show env all コマンドは、温度の値、ステート、およびしきい値を表示します。

次の例では、**show env temperature** コマンドの出力を示します。

```
Switch# show env temperature
TEMPERATURE is OK
```

次の例では、**show env all** コマンドの出力を示します。

```
Switch# show env all
FAN PS 1 is OK
FAN PS 2 is OK
TEMPERATURE is OK
Temperature Value: 23 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 66 Degree Celsius
Red Threshold    : 74 Degree Celsius
POWER SUPPLY 1 is DC OK
```

```
POWER SUPPLY 2 is DC OK

ALARM CONTACT 1 is not asserted
ALARM CONTACT 2 is not asserted
ALARM CONTACT 3 is not asserted
ALARM CONTACT 4 is not asserted
```

詳細については、このリリースのコマンド リファレンスを参照してください。

ping の使用

ここでは、次の情報について説明します。

- 「ping の概要」（P.46-10）
- 「ping の使用」（P.46-10）

ping の概要

Cisco ME スイッチは、リモート ホストへの接続テストに使用できる IP packet internet groper（ping）をサポートしています。ping は、アドレスにエコー要求パケットを送信し、応答を待ちます。

また、Cisco ME スイッチでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）または Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）で受信された ping 応答パケットをデフォルトで廃棄する Control Plane Security 機能も提供します。ただし、スイッチから UNI または ENI に接続されたホストへの正常な ping の実行方式も利用できます。

Control Plane Security は、Network Node Interface（NNI; ネットワーク ノード インターフェイス）からまたは NNI への ping 応答パケットを廃棄しません。また、NNI に接続されたホストからまたはホストへの ping をイネーブルにするのに、特別な設定は必要ありません。

ping の使用

ネットワーク上の別のデバイスに対してスイッチから ping を実行するには、特権 EXEC モードで **ping** コマンドを使用します。

コマンド	目的
ping [*host* | *address*]	ホスト名や IP ネットワーク アドレスを指定して、リモート ホストに ping を実行します。 **（注）** **ping** コマンドでは他のプロトコル キーワードを指定することもできますが、このリリースではサポートされていません。

（注） ping は、IEEE 802.1Q トンネル ポートとして設定されている UNI または ENI ではサポートされません。ping は、すべてのソフトウェア イメージの NNI 上でサポートされます。

UNI または ENI に接続されたホストへの ping の実行に関して、各種オプションを提供するスイッチでは、次のソフトウェア イメージが使用可能であることに留意してください。

- IP ルーティングをサポートするメトロ IP アクセス イメージ
- メトロ アクセス イメージ

次のセクションは、アクセス ポートおよびトランク ポートの両方に適用されます。

すべてのソフトウェア バージョン

Cisco ME スイッチのすべてのソフトウェア イメージでは、レイヤ 3 サービス ポリシーを使用して、スイッチから UNI または ENI に接続されたホストへの ping をイネーブルにできます。

（注）　メトロ IP アクセス イメージが稼動するスイッチの場合、IP ルーティングはデフォルトでイネーブルではなく、レイヤ 3 サービス ポリシーを使用するためにイネーブルにする必要はありません。

次に、可能な設定の一例を示します。

```
switch# configure terminal
switch(config)# access list 101 permit ip any any
switch(config)# class-map match-any ping-class
switch(config-cmap)# match access-group 101
switch(config-cmap)# exit
switch(config)# policy-map ping-policy
switch(config-pmap)# class ping-class
switch(config-pmap-c)# police 1000000
switch(config-pmap-c)# exit
switch(config-pmap)# exit
switch(config)# int fa0/1
switch(config-if)# service-policy input ping-policy
switch(config-if)# switchport access vlan 2
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# int vlan 2
switch(config-if)# ip address 192.168.1.1 255.255.255.0
switch(config-if)# end
switch# ping 192.168.1.2
```

メトロ IP アクセス イメージ

スイッチでメトロ IP アクセス イメージが稼動している場合は、次のいずれかの方法を使用できます。

- UNI または ENI にレイヤ 3 サービス ポリシーを適用する
- IP ルーティングをグローバルにイネーブルにして、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）からの ping を実行する。
- IP ルーティングをイネーブルにして、ルーテッド ポートからの ping を実行する。

レイヤ 3 サービス ポリシーを UNI または ENI に追加する設定例については、「すべてのソフトウェア バージョン」のセクションを参照してください。

IP ルーティングの使用および SVI またはルーテッド ポートからの ping 実行の例については、次のセクションを参照してください。

IP ルーティングおよび SVI

IP ルーティングは、スイッチでメトロ IP アクセス イメージが稼動する場合にだけサポートされます。

この設定を使用すると、IP ルーティングおよび SVI から UNI または ENI に接続されたホストへの ping をイネーブルにできます。

```
Switch# configure terminal
Switch(config)# ip routing
Switch(config)# int fa0/1
Switch(config-if)# switchport access vlan 2
Switch(config-if)# no shutdown
Switch(config-if)# int vlan 2
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# end
Switch# ping 192.168.1.2
```

この設定を使用すると、スイッチから IP アドレスが 192.168.1.2 であるホストへの ping を実行できます。

IP ルーティングおよびルーテッド ポート

この設定を使用すると、IP ルーティングをイネーブルにして、スイッチポートをルーテッド ポートに変更し、スイッチから接続ホストへの ping を許可できます。

```
switch# configure terminal
switch(config)# int fa0/1
switch(config-if)# no switchport
switch(config-if)# ip address 192.168.1.1 255.255.255.0
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# ip routing
switch(config)# end
switch# ping 192.168.1.2
```

ping 応答

この応答は、通常のホストへの正常な ping です。

```
Switch# ping 72.20.52.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

異常な ping の場合、次のメッセージが表示されます。

```
Switch# ping 72.20.52.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
. . . . .

Success rate is 0 percent (0/5)
```

要約

ping を実行する際は、次の注意事項に留意してください。

- IP ルーティングは、メトロ IP アクセス イメージが稼動している場合に限り使用可能で、デフォルトではディセーブルに設定されています。
- スイッチから各種 IP サブネットワーク内のホストに ping を実行するには、サブネット間のルーティングを行うよう IP ルーティングを設定する必要があり、宛先に対するスタティック ルートも適切となります。IP ルーティングをイネーブルにする場合、または設定する必要がある場合は、第 36 章「IP ユニキャスト ルーティングの設定」を参照してください。

- すべてのソフトウェア バージョンはレイヤ 3 サービス ポリシーを使用して、UNI または ENI と接続されたホストからまたはホストへの ping を許可します。ポリシー マップの詳細については、「入力ポリシーおよび出力ポリシー」（P.34-4）を参照してください。

スイッチでメトロ IP アクセス イメージが稼動している場合、次のいずれかの方法を使用して UNI または ENI に接続されたホストに ping を実行します。

- レイヤ 3 サービス ポリシーを使用して、UNI または ENI と接続されたホストからまたはホストへの ping を許可します。
- **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、IP ルーティングをグローバルにイネーブルにし、ポートをルーテッド ポートとして設定します。
- IP ルーティングをグローバルにイネーブルにし、作成した SVI に IP アドレスを割り当てます。SVI の詳細については、「スイッチ仮想インターフェイス」（P.10-6）を参照してください。

ping セッションを終了するには、**Ctrl**、**Shift**、および **6** のキーを同時に押してから放し、次に **X** キーを押します。

レイヤ 2 traceroute の使用

- 「レイヤ 2 traceroute の概要」（P.46-13）
- 「レイヤ 2 traceroute の使用上の注意事項」（P.46-13）
- 「物理パスの表示」（P.46-14）

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能により、パケットが通過する送信元デバイスから宛先デバイスへの物理パスをスイッチが識別できます。レイヤ 2 traceroute は、ユニキャスト送信元および宛先 MAC アドレスだけをサポートしています。パスにあるスイッチの MAC アドレス テーブルを使用してパスを検索します。スイッチがレイヤ 2 traceroute に対応していないデバイスをパス上に検出した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

（注）　レイヤ 2 traceroute は、NNI 上でだけ使用できます。

スイッチは、送信元デバイスから宛先デバイスへのパスだけを識別できます。パケットが通過する送信元ホストから送信元デバイスへのパス、あるいは宛先デバイスから宛先ホストへのパスは識別できません。

レイヤ 2 traceroute の使用上の注意事項

- Cisco Discovery Protocol（CDP; シスコ検出プロトコル）は、ネットワークの全デバイスでイネーブルになっていなければなりません。レイヤ 2 traceroute を適切に機能させるには、CDP をディセーブルにしないでください。

（注）　デフォルトでは、CDP は NNI 上でイネーブルに設定されています。ENI の CDP はイネーブルに設定できますが、UNI は CDP をサポートしません。

レイヤ 2 traceroute をサポートするスイッチのリストについては、「レイヤ 2 traceroute の使用上の注意事項」（P.46-13）を参照してください。物理パス内のデバイスが CDP にトランスペアレントの場合、スイッチはこれらのデバイスを通過するパスを識別できません。CDP のイネーブル化の詳細については、第 24 章「CDP の設定」を参照してください。

- **ping** 特権 EXEC コマンドを使用して接続をテストできる場合、スイッチは他のスイッチから到達可能です。物理パス内の全スイッチは、互いに到達可能でなければなりません。
- パス内で識別できるホップ数は最大で 10 です。
- 送信元デバイスから宛先デバイスへの物理パス上にないスイッチに、**traceroute mac** または **traceroute mac ip** の各特権 EXEC コマンドを入力できます。パス内の全スイッチは、このスイッチから到達可能でなければなりません。
- 指定された送信元および宛先 MAC アドレスが同じ VLAN に属している場合、**traceroute mac** コマンド出力は、レイヤ 2 パスだけを表示します。異なる VLAN に属する送信元および宛先 MAC アドレスを指定した場合、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- マルチキャスト送信元 MAC アドレスまたはマルチキャスト宛先 MAC アドレスを指定した場合、パスは識別されず、エラー メッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN にある場合、送信元および宛先 MAC アドレス両方の属する VLAN を指定する必要があります。VLAN が指定されないと、パスは識別されず、エラー メッセージが表示されます。
- 指定された送信元および宛先 IP アドレスが同じサブネットに属している場合、**traceroute mac ip** コマンド出力は、レイヤ 2 パスを表示します。IP アドレスを指定すると、スイッチは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用して IP アドレスと対応する MAC アドレスおよび VLAN ID を対応付けます。
  - 指定の IP アドレスの ARP のエントリが存在していた場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
  - ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスが解決されないと、パスは識別されず、エラー メッセージが表示されます。
- 複数のデバイスがハブを通じて 1 つのポートに接続されている場合（たとえば複数の CDP ネイバーが 1 つのポートで検出される場合）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

物理パスの表示

パケットが通過する送信元デバイスから宛先デバイスへのパスは、次のいずれかの特権 EXEC コマンドを使用して表示できます。

- **tracetroute mac** [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]
- **tracetroute mac ip** {*source-ip-address* | *source-hostname*}{*destination-ip-address* | *destination-hostname*} [**detail**]

（注）　レイヤ 2 traceroute は、NNI 上でだけ使用できます。

詳細については、このリリースのコマンド リファレンスを参照してください。

IP traceroute の使用

- 「IP traceroute の概要」（P.46-15）
- 「IP traceroute の実行」（P.46-15）

IP traceroute の概要

IP traceroute を使用すると、パケットがネットワークを通過するパスをホップ単位で識別できます。コマンド出力では、トラフィックが宛先までに通過する、ルータなどのネットワーク レイヤ（レイヤ 3）デバイスがすべて表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先として参加できますが、**traceroute** コマンド出力にホップとして表示されるかは不明です。スイッチが traceroute の宛先である場合、出力では、最終宛先として表示されます。中間スイッチは、同じ VLAN のポート間でパケットのブリッジングだけを行っている場合、出力では表示されません。ただし、中間スイッチが特定のパケットをルーティングしているマルチレイヤ スイッチである場合、出力ではこのスイッチをホップとして表示します。

ルータおよびサーバが特定の戻りメッセージを生成するには、**traceroute** 特権 EXEC コマンドで IP ヘッダーの Time To Live（TTL）フィールドを使用します。traceroute は、TTL フィールドを 1 に設定した状態で User Datagram Protocol（UDP）データグラムを宛先ホストに送信することで開始されます。ルータは 1 または 0 の TTL 値を検出すると、データグラムを廃棄して、送信元に Internet Control Message Protocol（ICMP）time-to-live-exceeded メッセージを送ります。traceroute は、このメッセージの送信元アドレスを調べることにより、最初のホップのアドレスを検出します。

次のホップを識別するために、traceroute は TTL 値を 2 に設定した UDP パケットを送信します。最初のルータは、TTL フィールドを 1 減らして、次のルータにデータグラムを送信します。次のルータでは、TTL 値が 1 であるパケットを確認して、データグラムを廃棄し、送信元に time-to-live-exceeded メッセージを返します。このプロセスは、データグラムが宛先ホストに到達するのに十分な TTL 値に増分されるまで（または最大 TTL 値になるまで）、続けられます。

データグラムが宛先に到達したことを学習するために、traceroute は、データグラムの UDP の宛先ポート番号を宛先ホストが使用しないような非常に大きい値に設定します。ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛てのデータグラムを受信すると、送信元に ICMP *ポート到達不能*エラーを送信します。ポート到達不能エラー以外のすべてのエラーは、中間ホップから送信されるため、ポート到達不能エラーを受信することは、このメッセージが宛先ポートから送信されたことを意味します。

IP traceroute の実行

パケットがネットワークを通過するパスを追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
traceroute ip *host*	パケットがネットワークを通過するパスを追跡します。

（注）　**traceroute** 特権 EXEC コマンドには他のプロトコル キーワードを指定することもできますが、このリリースではサポートされていません。

次に、IP ホストに **traceroute** を実行する例を示します。

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

  1 172.2.52.1 0 msec 0 msec 4 msec
  2 172.2.1.203 12 msec 8 msec 0 msec
  3 171.9.16.6 4 msec 0 msec 0 msec
  4 171.9.4.5 0 msec 4 msec 0 msec
  5 171.9.121.34 0 msec 4 msec 4 msec
  6 171.9.15.9 120 msec 132 msec 128 msec
  7 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

この表示では、ホップ カウント、ルータの IP アドレス、および送信される 3 つのプローブそれぞれのラウンドトリップ時間（ミリ秒）を示しています。

表 46-1　traceroute 出力表示文字

文字	説明
*	プローブがタイムアウトです。
?	パケット タイプが不明です。
A	管理上、到達不可能です。通常、この出力はアクセス リストがトラフィックをブロックしていることを意味します。
H	ホストが到達不可能です。
N	ネットワークが到達不可能です。
P	プロトコルが到達不可能です。
Q	送信元がクエンチです。
U	ポートが到達不可能です。

進行中の追跡を終了するには、エスケープ シーケンス（デフォルトは **Ctrl-^ X**）を入力します。**Ctrl**、**Shift**、**6** の各キーを同時に押してから放し、次に **X** キーを押します。

TDR の使用

- 「TDR の概要」（P.46-16）
- 「TDR の実行および結果の表示」（P.46-17）

TDR の概要

Time Domain Reflector（TDR; タイム ドメイン反射率計）機能を使用すると、ケーブル配線の問題を診断および解決できます。TDR を実行すると、ローカル デバイスによってケーブルを通して信号が送信され、返された信号と最初の信号が比較されます。

Cisco ME スイッチ上では、TDR は銅線イーサネット 10/100 ポート、または RJ-45 コネクタにより 10/100/100 ポートとして設定されたデュアルパーパス ポート上でだけサポートされます。

TDR では、次のケーブル配線の問題を検出できます。

- ツイストペア ワイヤのオープン、破損、切断：ワイヤが、リモート デバイスのワイヤに接続されていません。
- ツイストペア ワイヤのショート：ワイヤが相互に接触しているか、リモート デバイスのワイヤと接触しています。たとえば、ツイストペアの 1 本のワイヤが別のワイヤにはんだ付けされていると、ツイストペアはショートします。

ツイストペア ワイヤの片方がオープンである場合、TDR では、オープンであるワイヤの長さを検出できます。

次の状況では、TDR を使用してケーブル配線の問題を診断して解決します。

- スイッチの交換
- 配線クローゼットの設定
- リンクを確立できない場合、または適切に動作していない場合の、2 つのデバイス間における接続のトラブルシューティング

TDR の実行および結果の表示

TDR を実行するには、**test cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを入力します。

結果を表示するには、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを入力します。表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。

（注） TDR は、銅線のイーサネット 10/100 ポートまたは RJ-45 コネクタを使用して 10/100/100 ポートとして設定されたデュアルパーパス ポート上でだけサポートされます。

debug コマンドの使用

- 「特定の機能に関するデバッグのイネーブル化」（P.46-18）
- 「全システム診断のイネーブル化」（P.46-18）
- 「デバッグおよびエラー メッセージ出力のリダイレクト」（P.46-18）

注意 デバッグ出力には、CPU プロセスで高いプライオリティが割り当てられるので、システムが使用不能になる可能性があります。このため、**debug** コマンドは、特定の問題のトラブルシューティングを行う場合やシスコのテクニカル サポート スタッフによるトラブルシューティング セッション中に限って使用するようにください。**debug** コマンドは、ネットワーク トラフィック量が少ない、またはユーザ数が少ない時間帯に使用してください。このような時間帯を選んでデバッグを実行すると、**debug** コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。

（注） 特定の **debug** コマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

特定の機能に関するデバッグのイネーブル化

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。たとえば、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）に対するデバッグをイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# debug span-session
```

このコマンドの **no** 形式が入力されるまで、スイッチは出力の生成を続けます。

debug コマンドをイネーブルにしても出力が表示されない場合は、次の可能性を検討してください。

- スイッチが適切に設定されていないため、モニタ対象のトラフィック タイプが生成されない可能性があります。**show running-config** コマンドを使用し、コンフィギュレーションをチェックしてください。
- スイッチが正しく設定されていても、デバッグがイネーブルになっている特定の間は、モニタ対象のトラフィック タイプが生成されない場合もあります。デバッグを行う機能に応じて TCP/IP **ping** コマンドなどを使用し、ネットワーク トラフィックを生成します。

SPAN のデバッグをディセーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# no debug span-session
```

あるいは、特権 EXEC モードで、このコマンドの **undebug** 形式を入力することもできます。

```
Switch# undebug span-session
```

各デバッグ オプションのステートを表示するには、イネーブル モードで次のコマンドを入力します。

```
Switch# show debugging
```

全システム診断のイネーブル化

全システム診断をイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# debug all
```

注意　デバッグの出力は他のネットワーク トラフィックよりも優先され、また、**debug all** 特権 EXEC コマンドを実行すると他の **debug** コマンドよりも大量の出力が生成されるため、スイッチのパフォーマンスが大幅に低下したり、使用できなくなることがあります。**debug** コマンドは、なるべく対象を特定して使用してください。

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。**no debug all** コマンドを使用すると簡単に、誤って **debug** コマンドがイネーブルのままの状態にならないようにできます。

デバッグおよびエラー メッセージ出力のリダイレクト

デフォルトでは、ネットワーク サーバは **debug** コマンドの出力やシステム エラー メッセージをコンソールに送信します。このデフォルトを使用する場合は、コンソール ポートに接続する代わりに仮想端末接続を使用し、デバッグ出力をモニタできます。

宛先として使用できるのは、コンソール、仮想端末、内部バッファ、Syslog サーバが動作している UNIX ホストなどです。Syslog 形式は、4.3 Berkeley Standard Distribution（BSD）UNIX およびその派生 OS と互換性があります。

（注）　デバッグの宛先によって、システムのオーバーヘッドが変わることに注意してください。ロギング メッセージをコンソールに送信すると、大きなオーバーヘッドが発生しますが、仮想端末に出力すれば、オーバーヘッドは小さくなります。Syslog サーバに出力すると、オーバーヘッドはさらに小さくなります。最もオーバーヘッドが小さいのは、内部バッファへの出力です。

システム メッセージのロギングに関する詳細については、第 29 章「システム メッセージ ロギングの設定」を参照してください。

show platform forward コマンドの使用例

show platform forward 特権 EXEC コマンドの出力から、システムを介してインターフェイスに入るパケットの転送結果に関して、有用な情報がいくつか得られます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポート マップ、ビットマップ、および出力側の情報が表示されます。

（注）　**show platform forward** コマンドの構文および使用方法の詳細については、このリリースのスイッチ コマンド リファレンスを参照してください。

このコマンドで出力される情報のほとんどは、主に、スイッチの Application Specific Integrated Circuit（ASIC; 特定用途向け IC）に関する詳細情報を利用するテクニカル サポート担当者に役立ちます。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

次に、VLAN 5 内のギガビット イーサネット ポート 1 に入るパケットが未知の MAC アドレスにアドレッシングされる場合の **show platform forward** コマンドの出力例を示します。パケットは VLAN 5 内のその他のすべてのポートに対してフラッディングされなければなりません。

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2
udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000      01FFA   03000000
L2Local  80_00050002_00020002-00_00000000_00000000      00C71   0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

=========================================
Egress:Asic 2, switch 1
Output Packets:

-----------------------------------------
Packet 1
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000      01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/1    0005 0001.0001.0001  0002.0002.0002

-----------------------------------------
Packet 2
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000      01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
```

```
Gi0/2    0005 0001.0001.0001  0002.0002.0002

-----------------------------------------
<output truncated>
-----------------------------------------
Packet 10
 Lookup                   Key-Used                     Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000
Packet dropped due to failed DEJA_VU Check on Gi0/2
```

次に、VLAN 5 内のギガビット イーサネット ポート 1 に着信するパケットを、VLAN 上の別のポートで学習済みのアドレスに送信した場合の出力例を示します。パケットは、アドレスを学習済みのポートから転送する必要があります。

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                   Key-Used                     Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050009_43A80145-00_00000000_00000000     00086   02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003

=========================================
Egress:Asic 3, switch 1
Output Packets:


-----------------------------------------
Packet 1
 Lookup                   Key-Used                     Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0005 0001.0001.0001  0009.43A8.0145
```

次に、VLAN 5 内のギガビット イーサネット ポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが不明である場合の出力例を示します。デフォルト ルートが設定されていないため、パケットは廃棄されます。

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                   Key-Used                     Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_0D020202     010F0   01880290
L3Scndr  12_0D020202_0D010101-00_40000014_000A0000     034E0   000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000
```

次に、VLAN 5 内のギガビット イーサネット ポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが IP ルーティング テーブル内の IP アドレスに設定されている場合の出力例を示します。パケットはルーティング テーブルの指定どおりに転送されます。

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
Global Port Number:24, Asic Number:5
```

```
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_10010A05_0A010505-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_10010A05     010F0   01880290
L3Scndr  12_10010A05_0A010505-00_40000014_000A0000     01D28   30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

========================================
Egress:Asic 3, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0007 XXXX.XXXX.0246  0009.43A8.0147
```

crashinfo ファイルの使用

crashinfo ファイルには、シスコのテクニカル サポート スタッフが Cisco IOS イメージの障害（クラッシュ）の原因となる問題をデバッグするときに役立つ情報が保存されています。スイッチでは障害が発生すると、コンソールにクラッシュ情報を書き込みます。また、（システム障害ではない）障害後の Cisco IOS イメージの起動時にはファイルが作成されます。

ファイル内の情報には、障害が発生した Cisco IOS イメージの名前やバージョン、プロセッサ レジスタのリスト、およびスタック トレースが含まれます。この情報をシスコのテクニカル サポート スタッフに提供するには、**show tech-support** 特権 EXEC コマンドを使用します。

すべての crashinfo ファイルは、フラッシュ ファイル システム内の次のディレクトリに保管されます。

flash:/crashinfo/crashinfo_*n*（*n* はシーケンス番号）

新たに作成される crashinfo ファイルごとに、既存のシーケンス番号よりも大きなシーケンス番号が使用されるため、シーケンス番号が最大であるファイルに最新の障害が記述されます。スイッチにはリアルタイム クロックがないため、タイムスタンプの代わりにバージョン番号が使用されます。ファイル作成時に使用されるファイル名は変更できません。ただし、ファイルが作成されたあとに、**rename** 特権 EXEC コマンドを使用して名前を変更することもできますが、**show tech-support** 特権 EXEC コマンドを実行しても、名前が変更されたファイルの内容は表示されません。crashinfo ファイルを削除するには、**delete** 特権 EXEC コマンドを使用します。

最新の crashinfo ファイル（つまり、ファイル名の末尾のシーケンス番号が最大であるファイル）を表示するには、**show tech-support** 特権 EXEC コマンドを使用します。**more** や **copy** 特権 EXEC コマンドなど、ファイルをコピーまたは表示するコマンドを使用し、ファイルにアクセスすることもできます。

オンボード障害ロギングの使用

On-Board-Failure Logging（OBFL; オンボード障害ロギング）機能を使用すると、スイッチに関する情報を収集できます。この情報には、稼動時間、温度、電圧に関する情報が含まれており、シスコのテクニカルサポートの担当者がスイッチに関する問題のトラブルシューティングを行うのに役立ちます。

ここでは、次の情報について説明します。

- 「OBFL の概要」（P.46-22）
- 「OBFL の設定」（P.46-22）
- 「OBFL 情報の表示」（P.46-23）

OBFL の概要

デフォルトでは、OBFL は有効になっています。スイッチおよび Small Form-Factor Pluggable（SFP）モジュールに関する情報を収集します。スイッチは、この情報をフラッシュメモリに保存します。

- CLI コマンド：スイッチで入力されている OBFL CLI コマンド
- 環境データ：Product Identification（PID）、Version Identification（VID）、シリアル番号など、スイッチおよびすべての接続デバイスに関する Unique Device Identifier（UDI）情報
- メッセージ：スイッチで生成されたハードウェア関連のシステム メッセージの記録
- 温度：スイッチの温度
- 稼動時間データ：スイッチが起動する時間、スイッチが再起動する理由、最後に再起動して以降スイッチが稼動している時間
- 電圧：スイッチのシステム電圧

（注）　Cisco ME 3400EG-2CS-A スイッチでは、電圧のモニタリングをサポートしていません。

システムクロックを手動で設定する、または Network Time Protocol（NTP）を使用して設定する必要があります。

スイッチが稼動している場合、**show logging onboard** 特権 EXEC コマンドを使用して OBFL データを取得できます。スイッチに障害が発生した場合は、シスコのテクニカル サポートに連絡し、データの取得方法について問い合せてください。

OBFL 対応のスイッチが再起動になると、新しいデータのログが開始する際に 10 分の遅延が発生します。

OBFL の設定

OBFL をイネーブルに設定するには、**hw-module module logging onboard** [**message level** *level*] グローバル コンフィギュレーション コマンドを使用します。パラメータ **message level** *level* を使用して、スイッチが生成し、フラッシュメモリに保存するハードウェア関連メッセージの重大度を指定します。

OBFL データをローカル ネットワークまたは特定のファイル システムにコピーするには、**copy logging onboard module 1** *destination* 特権 EXEC コマンドを使用します。

注意　OBFL をイネーブルにしたまま、フラッシュ メモリに保存したデータを削除しないでください。

OBFL をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。OBLF はデフォルトでイネーブルに設定されています。イネーブルにする必要があるのはディセーブルになった場合だけです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hw-module module** [*slot-number*] **logging onboard** [**message** *level*]	スイッチ上で OBFL をイネーブルに設定します。 任意で、次のパラメータを設定できます。 • （任意）*slot-number*：スロット番号は常に 1 で、ME-3400E には関連しません。 • （任意）**message** *level*：生成され、保存されるメッセージの重大度を指定します。指定できる範囲は 1 ～ 7 です。1 が最も高い重大度です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy logging onboard module** [*slot-number*] *destination*	（任意）OBFL データをローカル ネットワークまたは特定のファイル システムにコピーします。 • （任意）*slot-number*：スロット番号は常に 1 で、ME-3400E には関連しません。 • *destination*：宛先オプションの詳細は、**copy logging onboard module** コマンドを参照してください。
ステップ 5	**show logging onboard**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

OBFL をディセーブルにするには、**no hw-module module 1 logging onboard** [**message** *level*] global configuration コマンドを使用します。

稼動時間情報および CLI コマンド情報を除く、フラッシュ メモリ内の OBFL データをすべてクリアするには、**clear logging onboard** 特権 EXEC コマンドを使用します。

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

OBFL 情報の表示

OBFL 情報を表示するには、表 46-2 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

（注）　OBFL 対応のスイッチが再起動になると、新しいデータのログが開始する際に 10 分の遅延が発生します。

表 46-2　OBFL 情報を表示するためのコマンド

コマンド	目的
show logging onboard clilog	スイッチ上に入力された OBFL CLI コマンドを表示します。
show logging onboard environment	PID、VID、シリアル番号など、スタンドアロンのスイッチおよび接続されているすべての FRU デバイスの UDI 情報を表示します。

表 46-2　OBFL 情報を表示するためのコマンド （続き）

コマンド	目的
show logging onboard message	スイッチによって生成されたハードウェア関連メッセージが表示されます。
show logging onboard temperature	スイッチの温度を表示します。
show logging onboard uptime	スイッチが起動する時間、スイッチが再起動する理由、最後に再起動して以降スイッチが稼動している時間を表示します。
show logging onboard voltage	スイッチのシステム電圧を表示します。

次の例では、show logging onboard コマンドの出力を示します。

```
Switch# show logging onboard clilog
----------------------------------------------------------------------------------
CLI LOGGING SUMMARY INFORMATION
----------------------------------------------------------------------------------
COUNT COMMAND
----------------------------------------------------------------------------------
    1 hw-module module logging onboard
    1 hw-module module logging onboard message level 7
    4 show logging onboard
    1 show logging onboard message
    1 show logging onboard summary
----------------------------------------------------------------------------------

Switch# show logging onboard temp
----------------------------------------------------------------------------------
TEMPERATURE SUMMARY INFORMATION
----------------------------------------------------------------------------------
Number of sensors          : 1
Sampling frequency         : 5 minutes
Maximum time of storage    : 720 minutes
----------------------------------------------------------------------------------
Sensor                            |   ID  | Maximum Temperature 0C
----------------------------------------------------------------------------------
System                              1     41
---------------------------------------
Temp                          Sensor ID
0C     1
---------------------------------------
No historical data to display
---------------------------------------

Switch# show logging onboard uptime
----------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
----------------------------------------------------------------------------------
First customer power on : 93/03/01 00:06:06
Total uptime            :   0 years  20 weeks   4 days   6 hours  20 minutes
Total downtime          :   0 years   0 weeks   0 days   0 hours   0 minutes
Number of resets        : 90
Number of slot changes  : 0
Current reset reason    : 0x0
Current reset timestamp : 93/03/01 00:05:43
Current slot            : 1
Current uptime          :   0 years   0 weeks   2 days   6 hours   0 minutes
----------------------------------------------------------------------------------
Reset  |        |
Reason | Count  |
----------------------------------------------------------------------------------
```

```
No historical data to display
-------------------------------------------------------------------------------

Switch# show logging onboard voltage
-------------------------------------------------------------------------------------------------
VOLTAGE SUMMARY INFORMATION
-------------------------------------------------------------------------------------------------
Number of sensors          : 6
Sampling frequency         : 1 minutes
Maximum time of storage    : 720 minutes
-------------------------------------------------------------------------------------------------
Sensor                            |   ID   | Maximum Voltage
-------------------------------------------------------------------------------------------------
12.00V                              0      12.567
1.25V                               2       1.258
3.30V                               3       3.305
2.50V                               4       2.517
1.80V                               5       1.825
1.50V                               6       1.508
-------------------------------------------------------------------------------------------------
Nominal Range                         Sensor ID

-------------------------------------------------------------------------------------------------
No historical data to display
-------------------------------------------------------------------------------------------------
```

表 46-2 のコマンド使用例、OBFL データの例については、このリリースに対応するコマンド リファレンスを参照してください。

CHAPTER 47

オンライン診断の設定

この章では、Cisco ME 3400E スイッチへのオンライン診断の設定方法について説明します。

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

- 「オンライン診断の概要」（P.47-1）
- 「オンライン診断の設定」（P.47-2）
- 「オンライン診断テストの実行」（P.47-6）

オンライン診断の概要

オンライン診断を使用すれば、スイッチが稼動中のネットワークに接続されている間でも、スイッチのハードウェア機能をテストおよび確認できます。オンライン診断には、各種ハードウェア コンポーネントを監視し、データ パスおよび制御信号を確認するための、パケット スイッチング テストが含まれます。

オンライン診断では、次の領域における問題が検出されます。

- ハードウェア コンポーネント
- インターフェイス（イーサネット ポートなど）
- はんだ接合

表 47-1 に、診断テストの ID および名前を示します。テスト アトリビュートについては、**show diagnostic content** 特権 EXEC コマンドからの出力を参照してください。

表 47-1　　診断テスト

テスト ID 番号	テスト名
1	TestPortAsicStackPortLoopback
2	TestPortAsicLoopback
3	TestPortAsicCam
4	TestPortAsicRingLoopback
5	TestMicRingLoopback
6	TestPortAsicMem

オンライン診断は、オンデマンド診断、スケジューリング診断、またはヘルス モニタリング診断に分類されます。

- オンデマンド診断は、CLI から実行されます。
- スケジューリング診断は、ユーザが指定したインターバル、またはスイッチが稼動中のネットワークに接続されている間の指定された時間で実行されます。
- ヘルス モニタリングはバックグラウンドで実行されます。

オンライン診断の設定

診断モニタリングをイネーブルにする前に、障害しきい値およびテストの実行インターバルを設定する必要があります。

- 「スケジューリング オンライン診断」（P.47-2）
- 「ヘルス モニタリング診断テストの設定」（P.47-4）

スケジューリング オンライン診断

オンライン診断をスケジューリングして、指定した時刻、日単位、週単位、または月単位のスケジュールで実行できます。スケジューリングを削除する場合は、このコマンドの **no** 形式を使用します。このコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

オンライン診断をスケジューリングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**diagnostic schedule test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}	特定の日付時刻でオンデマンド診断テストをスケジューリングします。 テストのスケジューリングを指定する場合、次のオプションを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前。表 47-1 を参照してください。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号。表 47-1 を参照してください。 • *test-id-range*：ハイフンやカンマで区切られたテスト ID 番号の範囲。 • **all**：すべての診断テスト。 • **basic**：基本的なオンデマンド診断テスト。 • **non-disruptive**：ノンディスラプティブ ヘルス モニタリング テスト。 次の期間でテストをスケジューリングできます。 • 日単位：**daily** *hh*:*mm* パラメータを使用します。 • 特定の日付時刻：**on** *mm dd yyyy hh*:*mm* パラメータを使用します。 • 週単位：**weekly** *day-of-week hh*:*mm* パラメータを使用します。
ステップ 3	**show diagnostic** {**content** | **schedule**}	設定されたオンライン診断テストおよびスケジュールを確認します。 • 設定されたオンライン診断を表示するには、**show diagnostic content** を入力します。 • オンライン診断テストのスケジュールを表示するには、**show diagnostic schedule** を入力します。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Use the **no diagnostic schedule test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*} global configuration command to remove the scheduled tests.

次に、特定の日付時刻に診断テストをスケジューリングし、そのスケジュールを確認する例を示します。

```
Switch(config)# diagnostic schedule test 1 on Dec 4 2008 10:22
Switch(config)# end
Switch# show diagnostic schedule
Current Time = 10:21:24 UTC Thu Dec 4 2008

Diagnostic:

Schedule #1:
        To be run on December 4 2008 10:22
        Test ID(s) to be executed: 1.
```

スケジューリングされた時間になると、スイッチによってテストが実行されます。

```
Switch# #
Dec  4 10:21:59.492: %DIAG-6-SCHED_RUNNING: : Performing Scheduled Online Diagnostic...
Dec  4 10:21:59.492: %DIAG-6-TEST_RUNNING: : Running TestPortAsicStackPortLoopback{ID=1} ..
Dec  4 10:22:00.498: %DIAG-6-TEST_OK: : TestPortAsicStackPortLoopback{ID=1} has completed
successfully
Dec  4 10:22:00.498: %DIAG-6-SCHED_COMPLETE: : Scheduled Online Diagnostic is completed
```

詳細については、このリリースのコマンド リファレンスにおける **diagnostic schedule test** コマンドの「Examples」を参照してください。

ヘルス モニタリング診断テストの設定

ヘルス モニタリング診断テストは、稼動中のネットワークにスイッチが接続している間に設定できます。各ヘルス モニタリング テストの実行インターバルを設定したり、テストが失敗した場合に Syslog メッセージを生成するようにスイッチをイネーブルにしたり、特定のテストをイネーブルにしたりできます。

デフォルトでは、ヘルス モリタリングはディセーブルに設定されています。イネーブルにすると、テストが失敗したときに、スイッチによって Syslog メッセージが生成されます。

ヘルス モニタリング診断テストを設定およびイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**diagnostic monitor interval test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*	指定したテストのヘルス モニタリング インターバルを設定します。 次のパラメータを使用してテストを指定します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前。表 47-1 を参照してください。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号。表 47-1 を参照してください。 • *test-id-range*：ハイフンやカンマで区切られたテスト ID 番号の範囲。 • **all**：すべての診断テスト。 インターバルを指定する場合、次のパラメータを設定します。 • *hh:mm:ss*：時間、分、または秒単位でのモニタリング インターバル。*hh* に指定できる範囲は 0 ～ 24 で、*mm* および *ss* に指定できる範囲は 0 ～ 60 です。 • *milliseconds*：ミリ秒（ms）単位でのモニタリング インターバル。指定できる範囲は 0 ～ 999 です。 • *day*：日数単位でのモニタリング インターバル。指定できる範囲は 0 ～ 20 です。
ステップ 3	**diagnostic monitor syslog**	（任意）ヘルス モニタリング テストが失敗したときに Syslog メッセージを生成するようにスイッチを設定します。

	コマンド	目的
ステップ 4	**diagnostic monitor threshold test** {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count*	（任意）ヘルス モニタリング テストの障害しきい値を設定します。 次のパラメータを使用してテストを指定します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前。表 47-1 を参照してください。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号。表 47-1 を参照してください。 • *test-id-range*：ハイフンやカンマで区切られたテスト ID 番号の範囲。 • **all**：すべての診断テスト。 障害しきい値 *count* に指定できる範囲は 0 ～ 99 です。
ステップ 5	**diagnostic monitor test** {*name* | *test-id* | *test-id-range* | **all**}	指定したヘルス モニタリング テストをイネーブルにします。 次のパラメータを使用してテストを指定します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前。表 47-1 を参照してください。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号。表 47-1 を参照してください。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号。 • **all**：すべての診断テスト。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show diagnostic** {**content** | **post** | **result** | **schedule** | **status** | **switch**}	オンライン診断テストの結果およびサポートされるテスト スイートを表示します。詳細については、「オンライン診断テストおよび結果の表示」（P.47-7）を参照してください。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

診断テストをディセーブルにし、デフォルト設定に戻すには、次のコマンドを使用します。

- オンライン診断テストをディセーブルにするには、**no diagnostic monitor test** {*name* | *test-id* | *test-id-range* | **all**} グローバル コンフィギュレーション コマンドを使用します。
- デフォルトのヘルス モニタリング インターバルに戻すには、**no diagnostic monitor interval test** {*name* | *test-id* | *test-id-range* | **all**} グローバル コンフィギュレーション コマンドを使用します。
- ヘルス モニタリング テストが失敗しても Syslog メッセージを生成しないようにスイッチを設定するには、**no diagnostic monitor syslog** グローバル コンフィギュレーション コマンドを使用します。
- デフォルトの障害しきい値に戻すには、**no diagnostic monitor threshold test** {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count* グローバル コンフィギュレーション コマンドを使用します。

次に、ヘルス モニタリング テストの設定例を示します。

```
Switch(config)# diagnostic monitor threshold test 1 failure count 50
Switch(config)# diagnostic monitor interval test TestPortAsicRingLoopback
```

オンライン診断テストの実行

オンライン診断を設定した後は、手動で診断テストを開始したり、テスト結果を表示したりできます。また、スイッチに対して設定されたテスト、およびすでに実行されているテストも表示できます。

- 「オンライン診断テストの開始」（P.47-6）
- 「オンライン診断テストおよび結果の表示」（P.47-7）

オンライン診断テストの開始

スイッチ上で実行されるように診断テストを設定したら、**diagnostic start** 特権 EXEC コマンドを使用して、診断テストを開始します。

（注）　テストを開始した後は、そのテスト プロセスを停止できません。

コマンド	目的
diagnostic start test {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**}	診断テストを開始します。 次のパラメータを使用してテストを指定します。 • *name*：テストの名前を入力します。テスト ID リストを表示するには、**show diagnostic content** 特権 EXEC コマンドを使用します。表 47-1 を参照してください。 • *test-id*：テストの ID 番号を入力します。テスト ID リストを表示するには、**show diagnostic content** 特権 EXEC コマンドを使用します。表 47-1 を参照してください。 • *test-id-range*：コンマおよびハイフンによって区切られた整数を使って、テスト ID の範囲を入力します。詳細については、このリリースのコマンド リファレンスに記載された **diagnostic start** コマンドの説明を参照してください。 • **all**：すべてのテストを実行するときは、このキーワードを使用します。 • **basic**：基本的なテスト スイートを実行するときは、このキーワードを使用します。 • **non-disruptive**：ノンディスラプティブ テスト スイートを実行するときは、このキーワードを使用します。

次に、テスト名を使用して診断テストを開始する例を示します。

```
Switch# diagnostic start test TestPortAsicRingLoopback
```

次に、ノンディスラプティブ診断テストを開始する例を示します。

```
Switch# diagnostic start test non-disruptive
Switch#
*Mar  3 19:34:02.680: %DIAG-6-TEST_RUNNING: : Running TestPortAsicStackPortLoopback{ID=1} ..
*Mar  3 19:34:03.687: %DIAG-6-TEST_OK: : TestPortAsicStackPortLoopback{ID=1} has completed
successfully
```

次に、すべての基本的な診断テストを開始する例を示します。

```
Switch# diagnostic start test all
```

オンライン診断テストおよび結果の表示

表 47-2 に記載された特権 EXEC **show** コマンドを使用することによって、設定されているオンライン診断テストを表示し、テスト結果を確認できます。

表 47-2　診断テストの設定および結果用コマンド

コマンド	目的
show diagnostic content	スイッチに対して設定されたオンライン診断を表示します。
show diagnostic status	実行中の診断テストを表示します。
show diagnostic result [**detail** | **test** {*name* | *test-id* | *test-id-range* | **all** [**detail**]}]	指定したオンライン診断テストの結果を表示します。
show diagnostic switch [**detail**]	オンライン診断テストの結果を表示します。
show diagnostic schedule	オンライン診断テストのスケジュールを表示します。
show diagnostic post	POST 結果を表示します （出力は、**show post** コマンドの出力と同じです)。

次の例では、**show diagnostic result** コマンドの出力を示します。

```
Switch# show diagnostic result

:   SerialNo : FOC1225U4CY

  Overall diagnostic result: PASS

  Test results: (. = Pass, F = Fail, U = Untested)

    1) TestPortAsicStackPortLoopback ---> .
    2) TestPortAsicLoopback ------------> U
    3) TestPortAsicCam -----------------> U
    4) TestPortAsicRingLoopback --------> U
    5) TestMicRingLoopback -------------> U
    6) TestPortAsicMem -----------------> U
```

次の例では、**show diagnostic post** コマンドの出力を示します。

```
Switch# show diagnostic post
Stored system POST messages:

Switch 1
---------

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC interface Loopback Tests : Begin
POST: CPU MIC interface Loopback Tests : End, Status Passed

POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed

POST: Thermal, Fan Tests : Begin
POST: Thermal, Fan Tests : End, Status Passed

POST: PortASIC CAM Subsystem Tests : Begin
```

```
POST: PortASIC CAM Subsystem Tests : End, Status Passed

POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

POST: EMAC Loopback Tests : Begin
POST: EMAC Loopback Tests : End, Status Passed
```

他の **show diagnostic** コマンドの出力例については、このリリースのコマンド リファレンスにおける **show diagnostic** コマンドの「Examples」を参照してください。

APPENDIX A

サポートされている MIB

この付録では、このリリースでサポートされている Cisco ME 3400E イーサネット アクセス スイッチの MIB（管理情報ベース）を示します。具体的な内容は次のとおりです。

- 「MIB リスト」（P.A-1）
- 「FTP による MIB ファイルへのアクセス」（P.A-3）

MIB リスト

- BRIDGE-MIB（RFC1493）

（注） BRIDGE-MIB は単一 VLAN（仮想 LAN）のコンテキストをサポートします。デフォルトでは、設定済みコミュニティ ストリングを使用した SNMP メッセージには常に VLAN 1 の情報が記載されています。たとえば VLAN x といった他の VLAN の BRIDGE-MIB 情報を取得するには、SNMP メッセージのこのコミュニティ ストリングである「設定済みのコミュニティ ストリング @x」を使用します。

- CISCO-CABLE-DIAG-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DHCP-SNOOPING-MIB
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-ERR-DISABLE-MIB
- CISCO-ETHER-CFM-MIB
- CISCO-ETHERNET-ACCESS-MIB
- CISCO-FLASH-MIB（すべてのスイッチのフラッシュ メモリは着脱式フラッシュ メモリとしてモデル化されています）

- CISCO-FTP-CLIENT-MIB
- CISCO-HSRP-MIB

（注）　レイヤ 3 MIB は、スイッチ上でメトロ IP アクセス イメージが稼動している場合に限りサポートされます。

- CISCO-HSRP-EXT-MIB（一部サポート）
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO-IPSLA-ETHERNET-MIB

（注）　スイッチ上でメトロ IP アクセス イメージが稼動している場合に限りサポートされます。

- CISCO-L2L3-INTERFACE-CONFIG-MIB
- CISCO-LAG-MIB
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NAC-NAD-MIB
- CISCO-PAE-MIB
- CISCO-PAGP-MIB
- CISCO-PING-MIB
- CISCO-PORT-QOS-MIB（cportQosStats Table では、スイッチの設定によってオクテットおよびパケット カウンタから値が戻されます）
- CISCO-PRODUCTS-MIB
- CISCO-PROCESS-MIB
- CISCO-RTTMON-MIB
- CISCO-SMI-MIB
- CISCO-STACKMAKER-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SYSLOG-MIB
- CISCO-TC-MIB
- CISCO-TCP-MIB
- CISCO-UDLDP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- IEEE8021-PAE-MIB

- IEEE8023-LAG-MIB
- IF-MIB（VLAN の入力/出力カウンタはサポートされていません）
- IGMP-MIB
- INET-ADDRESS-MIB
- IPMROUTE-MIB
- LLDP MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TCP-MIB
- OLD-CISCO-TS-MIB
- PIM-MIB
- RFC1213-MIB（機能は CISCO-RFC1213-CAPABILITY.my で指定されているエージェント機能によります）
- RFC1253-MIB（OSPF-MIB）
- RMON-MIB
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- TCP-MIB
- UDP-MIB

（注） 特定のシスコ製品およびリリースの MIB サポートの詳細については、次の URL の MIB Locator ツールにアクセスしてください。
http://tools.cisco.com/ITDIT/MIBS/MainServlet

FTP による MIB ファイルへのアクセス

各 MIB ファイルを入手する手順は、次のとおりです。

ステップ 1　FTP（ファイル転送プロトコル）クライアントが passive モードになっていることを確認します。

（注） 一部の FTP クライアントは passive モードをサポートしていません。

ステップ 2　FTP を使用してサーバ **ftp.cisco.com** にアクセスします。

ステップ 3　ユーザ名 **anonymous** を使用してログインします。

ステップ 4　パスワードが要求されたら、E メールのユーザ名を入力します。

ステップ 5　`ftp>` プロンプトで、ディレクトリを **/pub/mibs/v1** および **/pub/mibs/v2** に変更します。

ステップ 6　**get** *MIB_filename* コマンドを使用して、MIB ファイルのコピーを入手します。

APPENDIX B

Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作

この付録では、Cisco ME 3400E イーサネット アクセス スイッチ のフラッシュ ファイル システムの操作方法、コンフィギュレーション ファイルのコピー方法、およびスイッチにソフトウェア イメージをアーカイブ（アップロードおよびダウンロード）する方法について説明します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのスイッチ コマンド リファレンス、および『*Cisco IOS Configuration Fundamentals Command Reference*』*Release 12.2* を参照してください。

この付録で説明する内容は、次のとおりです。

- 「フラッシュ ファイル システムの操作」（P.B-1）
- 「コンフィギュレーション ファイルの操作」（P.B-8）
- 「ソフトウェア イメージの操作」（P.B-23）

フラッシュ ファイル システムの操作

フラッシュ ファイル システムは、ファイルを格納できる単一のフラッシュ デバイスです。また、ソフトウェア イメージおよびコンフィギュレーション ファイルの管理に役立つコマンドもいくつか用意されています。スイッチのデフォルトのフラッシュ ファイル システムは *flash:* です。

ここでは、次の設定情報について説明します。

- 「使用可能なファイル システムの表示」（P.B-2）
- 「デフォルトのファイル システムの設定」（P.B-3）
- 「ファイル システム上のファイルに関する情報の表示」（P.B-3）
- 「ディレクトリの作成および削除」（P.B-4）
- 「ファイルのコピー」（P.B-4）
- 「ファイルの削除」（P.B-5）
- 「tar ファイルの作成、表示、および抽出」（P.B-6）
- 「ファイルの内容の表示」（P.B-8）

使用可能なファイル システムの表示

スイッチで使用可能なファイル システムを表示する場合は、**show file systems** 特権 EXEC コマンドを使用します（次の例を参照）。

```
Switch# show file systems
File Systems:
     Size(b)     Free(b)      Type  Flags   Prefixes
*   15998976     5135872     flash     rw   flash:
           -           -    opaque     rw   bs:
           -           -    opaque     rw   vb:
      524288      520138     nvram     rw   nvram:
           -           -   network     rw   tftp:
           -           -    opaque     rw   null:
           -           -    opaque     rw   system:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
```

表 B-1　show file systems フィールドの説明

フィールド	値
Size（b）	ファイル システムのメモリ サイズ（バイト単位）です。
Free（b）	ファイル システムの空きメモリ サイズ（バイト単位）です。
Type	ファイル システムのタイプです。 **flash**：このファイル システムはフラッシュ メモリ デバイス用です。 **nvram**：このファイル システムは NVRAM（不揮発性 RAM）デバイス用です。 **opaque**：このファイル システムはローカルに生成された *pseudo* ファイル システム（*system* など）、または brimux などのダウンロード インターフェイスです。 **unknown**：タイプが不明なファイル システムです。
Flags	ファイル システムの権限です。 **ro**：読み取り専用です。 **rw**：読み取り / 書き込みです。 **wo**：書き込み専用です。
Prefixes	ファイル システムのエイリアスです。 **flash**：フラッシュ ファイル システムです。 **nvram**：NVRAM です。 **null**：コピーの null 宛先です。リモート ファイルを null にコピーし、そのサイズを判別できます。 **rcp**：Remote Copy Protocol（RCP; リモート コピー プロトコル）ネットワーク サーバです。 **system**：実行コンフィギュレーションを含むシステム メモリの内容が格納されています。 **tftp**：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）ネットワーク サーバです。 **xmodem**：XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。 **ymodem**：YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。

デフォルトのファイル システムの設定

cd *filesystem:* 特権 EXEC コマンドを使用すると、システムにおけるデフォルト ファイル システムとして使用されるファイル システムまたはディレクトリを指定できます。デフォルト ファイル システムを設定すると、引数 *filesystem:* を使用するコマンドで、その引数の指定を省略できます。たとえば、オプションの引数 *filesystem:* を持つすべての特権 EXEC コマンドに対しは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは *flash:* です。

cd コマンドで指定された現在のデフォルト ファイル システムを表示する場合は、**pwd** 特権 EXEC コマンドを使用します。

ファイル システム上のファイルに関する情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコンフィギュレーション ファイルが格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマンドで使用できます。

ファイル システム上のファイルに関する情報を表示する場合は、表 B-2 に示すいずれかの特権 EXEC コマンドを使用します。

表 B-2　ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [**/all**] [*filesystem***:**][*filename*]	ファイル システムの上にあるファイルのリストを表示します。
show file systems	ファイル システムの各ファイルに関する詳細を表示します。
show file information *file-url*	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイルの記述子のリストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用すると、別のユーザによってファイルが開かれているかどうかを確認できます。

ディレクトリの変更と作業ディレクトリの表示

ディレクトリの変更および作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 システム ボード フラッシュ デバイスの場合は、*filesystem***:** に **flash:** を指定します。
ステップ 2	**cd new_configs**	目的のディレクトリに変更します。 *new_configs* という名前のディレクトリに変更する方法については、コマンド例を参照してください。
ステップ 3	**pwd**	作業ディレクトリを表示します。

ディレクトリの作成および削除

ディレクトリを作成および削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 システム ボード フラッシュ デバイスの場合は、*filesystem***:** に **flash:** を指定します。
ステップ 2	**mkdir old_configs**	新しいディレクトリを作成します。 *old_configs* という名前のディレクトリを作成する方法については、コマンド例を参照してください。 ディレクトリ名は、大文字と小文字が区別されます。 スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。
ステップ 3	**dir** *filesystem***:**	設定を確認します。

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除する場合は、**delete /force/recursive** *filesystem***:/***file-url* 特権 EXEC コマンドを使用します。

名前で指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除する場合は、キーワード **/recursive** を使用します。ディレクトリ内のファイルごとに表示される削除確認のプロンプトを省略する場合は、キーワード **/force** を使用します。この場合、削除プロセスの中でプロンプトが表示されるのは開始時の一度だけです。**archive download-sw** コマンドによってインストールされたあと不要になった古いソフトウェア イメージを削除する場合は、/force **および /recursive** の各キーワードを使用します。

システム ボード フラッシュ デバイスの場合は、*filesystem* に **flash:** を指定します。*file-url* には、削除するディレクトリの名前を入力します。ディレクトリ内のすべてのファイルおよびそのディレクトリが削除されます。

注意　ファイルおよびディレクトリを削除すると、その内容を回復できません。

ファイルのコピー

コピー元からコピー先にファイルをコピーするには、**copy** *source-url destination-url* 特権 EXEC コマンドを使用します。コピー元およびコピー先の URL には、**running-config** キーワード ショートカットおよび **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドを実行すると、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存され、システム初期化中のコンフィギュレーションとして使用されます。

また、XMODERN プロトコルや YMODERN プロトコルが使用されているネットワーク マシンのファイルの場合は、特殊なファイル システム（**xmodem:**、**ymodem:**）からコピーすることもできます。

ネットワーク ファイル システムの URL には、**ftp:**、**rcp:**、および **tftp:** を使用できます。それぞれを使用する場合の構文は次のとおりです。

- FTP（ファイル転送プロトコル）：**ftp:**[[*//username* [**:***password*]**@***location*]*/directory*]*/filename*

- RCP：**rcp:**[[*//username@location*]*/directory*]*/filename*
- TFTP：**tftp:**[[*//location*]*/directory*]*/filename*

さらに、Secure Copy Protocol（SCP）により、スイッチ設定またはスイッチ イメージ ファイルをセキュアな認証方法でコピーできます。SCP は、Secure Shell（SSH; セキュア シェル）を使用します。SSH は、Berkeley r-tool をセキュアにしたアプリケーションおよびプロトコルです。「SCP のためのスイッチの設定」（P.8-42）を参照してください。

（注） SCP の設定方法および確認方法の詳細については、次の URL にある『*Cisco IOS New Features, Cisco IOS*』*Release 12.2* の「Secure Copy Protocol」の章を参照してください。
http://cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b18.html

ローカルな書き込み可能ファイル システムには flash: などがあります。

コピー元とコピー先の組み合せによっては、無効となる場合もあります。特に、次に示す組み合せの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同一のデバイスへ（たとえば **copy flash: flash:** コマンドは無効）

コンフィギュレーション ファイルに対する **copy** コマンドの具体的な使用例については、「コンフィギュレーション ファイルの操作」（P.B-8）を参照してください。

新しいバージョンをダウンロード、または既存のバージョンをアップロードして、ソフトウェア イメージをコピーする場合は、**archive download-sw** 特権 EXEC コマンドまたは **archive upload-sw** 特権 EXEC コマンドを使用します。詳細については、「ソフトウェア イメージの操作」（P.B-23）を参照してください。

ファイルの削除

フラッシュ メモリ デバイス上の不要になったファイルは、永続的に削除できます。指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、**delete** [**/force**] [**/recursive**] [*filesystem***:**]*/file-url* 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、キーワード **/recursive** を使用します。ディレクトリ内のファイルごとに表示される削除確認のプロンプトを省略する場合は、キーワード **/force** を使用します。この場合、削除プロセスの中でプロンプトが表示されるのは開始時の一度だけです。**archive download-sw** コマンドによってインストールされたあと不要になった古いソフトウェア イメージを削除する場合は、/force **および /recursive** の各キーワードを使用します。

*filesystem***:** オプションが省略された場合、スイッチでは **cd** コマンドにより指定されたデフォルト デバイスが使用されます。*file-url* には、削除するファイルのパス（ディレクトリ）および名前を指定します。

ファイルを削除しようとすると、削除確認のプロンプトが表示されます。

注意 ファイルが削除された場合、その内容を回復できません。

次に、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する例を示します。

```
Switch# delete myconfig
```

tar ファイルの作成、表示、および抽出

tar ファイルを作成し、そこにファイルを書き込んだり、tar ファイル内のファイルをリスト表示したり、tar ファイルからファイルを抽出したりできます（次の各セクションを参照）。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするときは、**copy** 特権 EXEC コマンドや **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** 特権 EXEC コマンドおよび **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

tar ファイルの作成

tar ファイルを作成し、そこにファイルを書き込む場合は、次の特権 EXEC コマンドを使用します。

archive tar/create *destination-url* **flash:**/*file-url*

destination-url には、ローカル ファイル システムまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカルのフラッシュ ファイル システムの場合、構文は次のとおりです。
  flash:
- FTP の場合、構文は次のとおりです。
  ftp:[[//*username*[**:***password*]**@***location*]/*directory]*/*tar-filename***.tar**
- RCP の場合、構文は次のとおりです。
  rcp:[[//*username***@***location*]/*directory*]/*tar-filename***.tar**
- TFTP の場合、構文は次のとおりです。
  tftp:[[//*location*]/*directory*]/*tar-filename***.tar**

*tar-filename***.tar** は、作成する tar ファイルです。

flash:/*file-url* には、新しい tar ファイルの作成元になるローカルなフラッシュ ファイル システム上の場所を指定します。送信元ディレクトリ内に格納されているオプションのファイルまたはディレクトリのリストを指定し、それらを新しい tar ファイルに書き込むこともできます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

次の例では、tar ファイルを作成する方法を示します。次のコマンドを実行すると、ローカルなフラッシュ デバイスの *new-configs* ディレクトリの内容が、172.20.10.30 にある TFTP サーバ上のファイル *saved.tar* に書き込まれます。

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

tar ファイルの内容の表示

画面に tar ファイルの内容を表示するには、次の特権 EXEC コマンドを使用します。

archive tar/table *source-url*

source-url には、ローカルまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカルのフラッシュ ファイル システムの場合、構文は次のとおりです。
  flash:
- FTP の場合、構文は次のとおりです。
  ftp:[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar**

- RCP の場合、構文は次のとおりです。
  rcp:[[*//username@location*]*/directory*]*/tar-filename*.**tar**
- TFTP の場合、構文は次のとおりです。
  tftp:[[*//location*]*/directory*]*/tar-filename*.**tar**

tar-filename.**tar** は、表示する tar ファイルです。

次に、フラッシュ メモリ内にあるスイッチ tar ファイルの内容を表示する例を示します。

```
Switch# archive tar /table flash:image-name.tar
info (219 bytes)
image-name/ (directory)
image-name/html/ (directory)
image-name/html/foo.html (0 bytes)
image-name/image-name.bin (4527884 bytes)
image-name/info (346 bytes)
info (110 bytes)
```

tar ファイルの抽出

tar ファイルをフラッシュ ファイル システム上のディレクトリに抽出するには、次の特権 EXEC コマンドを使用します。

archive tar/xtract *source-url* **flash:**/*file-url* [*dir/file...*]

source-url には、ローカル ファイル システムの送信元 URL のエイリアスを指定します。次のオプションがサポートされています。

- ローカルのフラッシュ ファイル システムの場合、構文は次のとおりです。
  flash:
- FTP の場合、構文は次のとおりです。
  ftp:[[*//username*[**:***password*]**@***location*]*/directory*]*/tar-filename*.**tar**
- RCP の場合、構文は次のとおりです。
  rcp:[[*//username@location*]*/directory*]*/tar-filename*.**tar**
- TFTP の場合、構文は次のとおりです。
  tftp:[[*//location*]*/directory*]*/tar-filename*.**tar**

tar-filename.**tar** には、ファイルの抽出元の tar ファイルを指定します。

flash:/*file-url* [*dir/file...*] には、tar ファイルが抽出されるローカル フラッシュ ファイル システムの場所を指定します。tar ファイルから抽出されるファイルまたはディレクトリのオプション リストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

次に、172.20.10.30 の TFTP サーバ上にある tar ファイルの内容を抽出する例を示します。このコマンドは、*new-configs* ディレクトリだけを、ローカル フラッシュ ファイル システムのルート（root）ディレクトリに抽出します。*saved.tar* ファイルの残りのファイルは無視されます。

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

ファイルの内容の表示

リモート ファイル システム上のファイルなど、読み取り可能ファイルの内容を表示するには、**more** [**/ascii** | **/binary** | **/ebcdic**] *file-url* 特権 EXEC コマンドを使用します。

次に、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示する例を示します。

```
Switch# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

コンフィギュレーション ファイルの操作

ここでは、コンフィギュレーション ファイルの作成、ロード、メンテナンスの手順について説明します。

コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力されるコマンドが格納されています。基本的なコンフィギュレーション ファイルを作成する場合は、**setup** プログラムを使用するか、または **setup** 特権 EXEC コマンドを使用します。詳細については、第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」を参照してください。

コンフィギュレーション ファイルは、TFTP、FTP、または RCP サーバから、スイッチの実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにコピー（*ダウンロード*）できます。この操作が必要となるのは、次のいずれかの場合です。

- バックアップ コンフィギュレーション ファイルを復元する場合
- 別のスイッチのコンフィギュレーション ファイルを使用する場合。たとえば、ネットワークに別のスイッチを追加し、それを元のスイッチと同じ設定にできます。ファイルを新しいスイッチにコピーし、目的の部分を変更すれば、ファイル全体を作成し直す必要はなくなります。
- すべてのスイッチのコンフィギュレーションが同じになるように、ネットワーク内のすべてのスイッチに同じコンフィギュレーション コマンドをロードする場合

スイッチからファイル サーバにコンフィギュレーション ファイルをコピー（*アップロード*）するには、TFTP、FTP、または RCP を使用します。あとでサーバから元のコンフィギュレーション ファイルを復元できるようにするため、現在のコンフィギュレーション ファイルをサーバにバックアップしてから、内容を変更してください。

使用するプロトコルは、使用中のサーバのタイプによって異なります。FTP や RCP のトランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが高速化され、データがより確実に伝送されます。こうした優れた動作は、FTP および RCP がコネクション型の TCP/IP スタックに基づいて構築され、実際に TCP/IP スタックが使用されることで実現されるものです。

ここでは、次の設定情報について説明します。

- 「コンフィギュレーション ファイルの作成および使用に関する注意事項」（P.B-9）
- 「コンフィギュレーション ファイルのタイプおよび場所」（P.B-9）
- 「テキスト エディタによるコンフィギュレーション ファイルの作成」（P.B-10）
- 「TFTP によるコンフィギュレーション ファイルのコピー」（P.B-10）

- 「FTP によるコンフィギュレーション ファイルのコピー」（P.B-12）
- 「RCP によるコンフィギュレーション ファイルのコピー」（P.B-15）
- 「設定情報の消去」（P.B-19）
- 「コンフィギュレーションの置換とロールバック」（P.B-19）

コンフィギュレーション ファイルの作成および使用に関する注意事項

コンフィギュレーション ファイルを作成しておくと、スイッチの設定が容易になります。コンフィギュレーション ファイルには、1 台または複数台のスイッチを設定する場合に必要となるコマンドの一部、またはすべてを格納できます。たとえば、同じハードウェア コンフィギュレーションを持つ複数のスイッチに、同じコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- スイッチの初期設定を行う場合は、コンソール ポートを介して接続してください。コンソール ポートに直接接続せずに、ネットワーク接続を介してスイッチにアクセスすると、設定の一部が変更され（スイッチの IP アドレスの変更やポートのディセーブル化など）、スイッチとの接続が切断される場合があります。
- スイッチにパスワードが設定されていない場合は、**enable secret** *secret-password* グローバル コンフィギュレーション コマンドを使用して、パスワードを設定してください。

（注）　**copy** {**ftp:** | **rcp:** | **tftp:**} **system:running-config** 特権 EXEC コマンドを実行すると、コマンド ラインからコマンドを入力した場合と同じように、スイッチ上のコンフィギュレーション ファイルをロードできます。既存の実行コンフィギュレーションは、コマンドを追加するまで消去されません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内のコマンドの一部を置き換えたり、無効にしたりはできません。この場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが混在するコンフィギュレーション ファイルが作成され、コピーされたコンフィギュレーション ファイルが優先されます。

コンフィギュレーション ファイルの内容を、サーバに格納されているファイルのコピーと全く同じ状態に戻すには、（**copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** 特権 EXEC コマンドを使用して）そのコンフィギュレーション ファイルをスタートアップ コンフィギュレーションに直接コピーし、スイッチをリロードします。

コンフィギュレーション ファイルのタイプおよび場所

スタートアップ コンフィギュレーション ファイルは、システムの起動時にソフトウェアの設定を行うためのものです。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が格納されています。この 2 つのコンフィギュレーション ファイルは、別々に用意できます。たとえば、コンフィギュレーション ファイルを一時的に設定を変更する必要がある場合が発生したとします。このような場合、実行コンフィギュレーションを変更したあとに **copy running-config startup-config** 特権 EXEC コマンドによる設定の保存を行わないようにします。

実行コンフィギュレーションは DRAM に保存されますが、スタートアップ コンフィギュレーションはフラッシュ メモリの NVRAM セクションに格納されます。

テキスト エディタによるコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成するときは、システムが適切に応答できるように、コマンドを論理的に並べる必要があります。これは、コンフィギュレーション ファイルを作成する 1 つの方法です。

ステップ 1　スイッチからサーバに既存のコンフィギュレーションをコピーします。

詳細については、「TFTP によるコンフィギュレーション ファイルのダウンロード」（P.B-11）、「FTP によるコンフィギュレーション ファイルのダウンロード」（P.B-13）、または「RCP によるコンフィギュレーション ファイルのダウンロード」（P.B-17）を参照してください。

ステップ 2　UNIX の vi または emacs、PC のメモ帳などのテキスト エディタでコンフィギュレーション ファイルを開きます。

ステップ 3　目的のコマンドが格納されたコンフィギュレーション ファイルの一部を抽出し、新しいファイルに保存します。

ステップ 4　コンフィギュレーション ファイルをサーバ内の適切な場所にコピーします。たとえば、ファイルをワークステーションの TFTP ディレクトリ（UNIX ワークステーションの場合は通常 /tftpboot）にコピーします。

ステップ 5　ファイルに関する権限が world-read に設定されていることを確認します。

TFTP によるコンフィギュレーション ファイルのコピー

スイッチの設定には、作成したコンフィギュレーション ファイル、別のスイッチからダウンロードしたコンフィギュレーション ファイル、または TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用できます。コンフィギュレーション ファイルは、TFTP サーバにコピー（アップロード）すれば、そこで保管できます。

ここでは、次の設定情報について説明します。

- 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-10）
- 「TFTP によるコンフィギュレーション ファイルのダウンロード」（P.B-11）
- 「TFTP によるコンフィギュレーション ファイルのアップロード」（P.B-12）

TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能するワークステーションが、適切に設定されていることを確認します。Sun ワークステーションで、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

（注）　/etc/inetd.conf ファイルおよび /etc/services ファイルを変更したら、inetd デーモンを再起動する必要があります。このデーモンを再起動する場合は、inetd プロセスをいったん終了して再起動するか、**fastboot** コマンド（SunOS 4.x の場合）または **reboot** コマンド（Solaris 2.x または SunOS 5.x の場合）を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが格納されていることを確認します。ルータでサブネット間トラフィックのルーティングを実行しない場合は、スイッチおよび TFTP サーバを同じサブネット内に配置する必要があります。**ping** コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするコンフィギュレーション ファイルが、TFTP サーバ上の正しいディレクトリ内にあることを確認します（UNIX ワークステーションの場合は通常 /tftpboot）。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。
- コンフィギュレーション ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* には、サーバにアップロードするときに使用するファイルの名前を指定します。
- アップロード処理中にサーバ上の既存ファイル（空のファイルを作成する必要がある場合は空のファイルを含む）を上書きするときは、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードされたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

ステップ 1　コンフィギュレーション ファイルをワークステーション上の適切な TFTP ディレクトリにコピーします。

ステップ 2　「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-10）を参照し、TFTP サーバが適切に設定されていることを確認します。

ステップ 3　コンソール ポートまたは Telnet セッションを介してスイッチにログインします。

ステップ 4　TFTP サーバからコンフィギュレーション ファイルをダウンロードし、スイッチを設定します。

TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイルの名前を指定します。

次に示すいずれかの特権 EXEC コマンドを使用します。

- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **system:running-config**
- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **nvram:startup-config**

目的のコンフィギュレーション ファイルがダウンロードされ、1 行ごとに解析が行われると同時にコマンドが実行されます。

次に、IP アドレス 172.16.2.155 上にあるファイル *tokyo-confg* を基にソフトウェアを設定する例を示します。

```
Switch# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

TFTP によるコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして格納するには、次の手順を実行します。

ステップ 1　「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-10）を参照し、TFTP サーバが適切に設定されていることを確認します。

ステップ 2　コンソール ポートまたは Telnet セッションを介してスイッチにログインします。

ステップ 3　スイッチのコンフィギュレーションを TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名、およびアップロード先でのファイル名を指定します。

次に示すいずれかの特権 EXEC コマンドを使用します。

- **copy system:running-config tftp:**[[[*//location*]*/directory*]*/filename*]
- **copy nvram:startup-config tftp:**[[[*//location*]*/directory*]*/filename*]

ファイルが TFTP サーバにアップロードされます。

次に、スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードする例を示します。

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [OK]
```

FTP によるコンフィギュレーション ファイルのコピー

コンフィギュレーション ファイルは、FTP サーバとの間でコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードをクライアントからサーバに送信する必要があります。

FTP を使用してコンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内で最初にある有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- 匿名。

スイッチは、次のリスト内で最初にある有効なパスワードを送信します。

- **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）。
- スイッチは、*username@switchname.domain* という名前のパスワードを生成します。変数 *username* は現在のセッションに関連付けられているユーザ名、*switchname* は設定されているホスト名、*domain* はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定する場合は、**ip ftp username** コマンドおよび **ip ftp password** コマンドを使用します。コピー操作の際にユーザ名だけを指定する場合は、**copy** コマンド内にそのユーザ名を指定します。

サーバにディレクトリ構造がある場合は、ユーザ名に関連付けられたサーバ上のディレクトリが、コンフィギュレーション ファイルの書き込み先またはコピー先となります。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリに置かれている場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、FTP サーバのマニュアルを参照してください。

ここでは、次の設定情報について説明します。

- 「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-13）
- 「FTP によるコンフィギュレーション ファイルのダウンロード」（P.B-13）
- 「FTP によるコンフィギュレーション ファイルのアップロード」（P.B-14）

FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが格納されていることを確認します。ルータでサブネット間トラフィックのルーティングを実行しない場合は、スイッチおよび FTP サーバを同じサブネット内に配置する必要があります。**ping** コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしている場合、または有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用されていることを確認します。**show users** 特権 EXEC コマンドを使用すると、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのコピー処理中に **ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して、新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしている場合、有効なユーザ名があれば、そのユーザ名が使用されるため、FTP ユーザ名を設定する必要はありません。特定のコピー操作にだけ使用するユーザ名を指定する場合は、**copy** コマンド内にそのユーザ名を指定します。
- コンフィギュレーション ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、FTP サーバを適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-13）を参照し、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。

	コマンド	目的
ステップ 3	**configure terminal**	スイッチで、グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを無効にする場合だけです（ステップ 4、5、6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] **system:running-config** または **copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] **nvram:startup-config**	FTP を使用して、ネットワーク サーバにあるコンフィギュレーション ファイルを実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-confg* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上の *netadmin1* ディレクトリからコピーし、それらのコマンドをスイッチ上にロードして実行する例を示します。

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。IP アドレスが 172.16.101.101 であるリモート サーバ上の *netadmin1* ディレクトリから、スイッチのスタートアップ コンフィギュレーションへ、コンフィギュレーション ファイル *host2-confg* がコピーされます。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-13）を参照し、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを無効にする場合だけです（ステップ 4、5、6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy system:running-config ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] または **copy nvram:startup-config ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]	FTP を使用して、スイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定した場所に格納します。

次に、実行コンフィギュレーション ファイル *switch2-confg* を、IP アドレスが 172.16.101.101 であるリモート ホスト上の *netadmin1* ディレクトリにコピーする例を示します。

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-confg
Write file switch2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをコピーし、サーバに格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

RCP によるコンフィギュレーション ファイルのコピー

リモート ホストとスイッチの間でのコンフィギュレーション ファイルのダウンロード、アップロード、およびコピーは、RCP を使用して行うこともできます。コネクションレス型プロトコルの UDP を使用する TFTP とは異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーするためには、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合には、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザが行うのは、リモート シェル（rsh）をサポートするサーバへのアクセスだけです （ほとんどの UNIX システムでは rsh がサポートされています）。ファイルは特定の場所から別の場所にコピーされるため、コピー元ファイルの読み取り権限およびコピー先ファイルへの書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとにリモート ユーザ名をクライアントからサーバに送信する必要があります。コンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初にある有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet 経由でルータに接続され、**username** コマンドを介して認証された場合、スイッチ ソフトウェアからはリモート ユーザ名として Telnet ユーザ名が送信されます。
- スイッチのホスト名。

RCP コピー要求が正常に処理されるには、ネットワーク サーバにリモート ユーザ名用のアカウントを定義する必要があります。サーバにディレクトリ構造がある場合は、リモート ユーザ名に関連付けられたサーバ上のディレクトリが、コンフィギュレーション ファイルの書き込み先またはコピー先となります。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、そのユーザの名前をリモート ユーザ名として指定します。

ここでは、次の設定情報について説明します。

- 「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-16）
- 「RCP によるコンフィギュレーション ファイルのダウンロード」（P.B-17）
- 「RCP によるコンフィギュレーション ファイルのアップロード」（P.B-18）

RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能するワークステーションで、リモート シェル（rsh）がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが格納されていることを確認します。ルータでサブネット間トラフィックのルーティングを実行しない場合は、スイッチおよびサーバを同じサブネット内に配置する必要があります。**ping** コマンドを使用して、RCP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしている場合、または有効なユーザ名がない場合は、RCP ダウンロードに使用するユーザ名が現在の RCP ユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用すると、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのコピー処理中に **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用し、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしている場合、有効なユーザ名があれば、そのユーザ名が使用されるため、RCP ユーザ名を設定する必要はありません。特定のコピー操作にだけ使用するユーザ名を指定する場合は、**copy** コマンド内にそのユーザ名を指定します。

- ファイルを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、RCP サーバを適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザの .rhosts ファイルにエントリを追加する必要があります。たとえば、スイッチに次のコンフィギュレーション行が含まれていると仮定します。

```
hostname Switch1
ip rcmd remote-username User0
```

このスイッチの IP アドレスを *Switch1.company.com* に変換するためには、RCP サーバ上の User0 用の .rhosts ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-16）を参照し、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を無効にする場合だけです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **system:running-config** または **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **nvram:startup-config**	RCP を使用して、ネットワーク サーバにあるコンフィギュレーション ファイルを実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-confg* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上の *netadmin1* ディレクトリからコピーし、それらのコマンドをスイッチ上にロードして実行する例を示します。

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。IP アドレスが 172.16.101.101 であるリモート サーバ上の *netadmin1* ディレクトリから、コンフィギュレーション ファイル *host2-confg* がスイッチのスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-16）を参照し、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を無効にする場合だけです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy system:running-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] or **copy nvram:startup-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]	RCP を使用して、コンフィギュレーション ファイルをスイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコピーします。

次に、実行コンフィギュレーション ファイル *switch2-confg* を、IP アドレスが 172.16.101.101 であるリモート ホスト上の *netadmin1* ディレクトリにコピーする例を示します。

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-confg
Write file switch-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバに格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
```

```
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

設定情報の消去

スタートアップ コンフィギュレーションから設定情報を消去できます。スタートアップ コンフィギュレーションを使用せずにスイッチを再起動すると、スイッチはセットアップ プログラム状態になり、新しい設定でスイッチを再設定できます。

スタートアップ コンフィギュレーション ファイルの消去

スタートアップ コンフィギュレーション ファイルの内容を消去する場合は、**erase nvram:** または **erase startup-config** 特権 EXEC コマンドを使用します。

注意　いったん削除されたスタートアップ コンフィギュレーション ファイルは復元できません。

格納されたコンフィギュレーション ファイルの削除

保存された設定をフラッシュ メモリから削除する場合は、**delete flash:***filename* 特権 EXEC コマンドを使用します。**file prompt** グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削除する前に削除確認のプロンプトが表示されます。デフォルトでは、スイッチは、破壊的なファイル操作に関する確認をプロンプトで要求します。**file prompt** コマンドの詳細については、『*Cisco IOS Command Reference*』*Release 12.2* を参照してください。

注意　いったん削除されたファイルは復元できません。

コンフィギュレーションの置換とロールバック

コンフィギュレーションの置換とロールバック機能を使用すると、実行コンフィギュレーションを、保存されている Cisco IOS コンフィギュレーション ファイルに置き換えることができます。ロールバック機能は、以前のコンフィギュレーションにロールバックする場合に使用します。

ここでは、次の情報について説明します。

- 「コンフィギュレーションの置換とロールバックの概要」（P.B-19）
- 「コンフィギュレーションの置換とロールバックに関する注意事項」（P.B-21）
- 「コンフィギュレーション アーカイブの設定」（P.B-21）
- 「コンフィギュレーションの置換処理またはロールバック処理の実行」（P.B-22）

コンフィギュレーションの置換とロールバックの概要

- 「コンフィギュレーションのアーカイブ」（P.B-20）
- 「コンフィギュレーションの置換」（P.B-20）

- 「コンフィギュレーションのロールバック」（P.B-21）

コンフィギュレーションのアーカイブ

コンフィギュレーション アーカイブ機能は、コンフィギュレーション ファイルのアーカイブを保管、整理、および管理するためのメカニズムを備えています。**configure replace** 特権 EXEC コマンドを使用すれば、コンフィギュレーションのより高度なロールバックが可能です。また、**copy running-config** *destination-url* 特権 EXEC コマンドを使用すれば、実行コンフィギュレーションのコピーを保存することもできます。これにより、置換ファイルをローカルまたはリモートに保管できます。ただし、この方法ではファイルを自動管理できません。コンフィギュレーションの置換とロールバック機能では、実行コンフィギュレーションのコピーがコンフィギュレーション アーカイブに自動で保存されます。

archive config 特権 EXEC コマンドを使用すると、コンフィギュレーションをコンフィギュレーション アーカイブに保存できます。その際、標準的な場所が保存先として使用され、ファイルが保存されるたびにファイル名のプレフィクスとしてバージョン番号（およびオプションのタイムスタンプ）が連番形式で自動的に追加されます。また、アーカイブに保持される実行コンフィギュレーションのバージョンの数も指定できます。保存されているファイル数が上限に達した場合、最新のファイルが保存された時点で、最も古いファイルが自動的に削除されます。**show archive** 特権 EXEC コマンドを使用すると、コンフィギュレーション アーカイブに保存されている全コンフィギュレーション ファイルについての情報を表示できます。

Cisco IOS のコンフィギュレーション アーカイブは、FTP、HTTP、RCP、TFTP のどのファイル システム内でも配置でき、そこで保管されるコンフィギュレーション ファイルは **configure replace** コマンドを使って使用できます。

コンフィギュレーションの置換

configure replace 特権 EXEC コマンドを使用すると、実行コンフィギュレーションを、保存されているコンフィギュレーション ファイルに置き換えることができます。**configure replace** コマンドを入力すると、実行コンフィギュレーションと、指定した置換用コンフィギュレーションとが比較され、それらの差分が生成されます。コンフィギュレーションの置換は、この差分に基づいて行われます。コンフィギュレーションの置換処理は通常、3 パス以内で完了します。また、ループ動作を回避するために、最大 5 パスまでしか実行されません。

copy *source-url* **running-config** 特権 EXEC コマンドを使用すると、保管されているコンフィギュレーション ファイルを実行コンフィギュレーションにコピーできます。**configure replace** *target-url* 特権 EXEC コマンドの代わりにこのコマンドを使用する場合は、次のような違いがあることに注意してください。

- **copy** *source-url* **running-config** コマンドによって実行されるのはマージ処理です。コピー元のファイルに含まれるコマンドおよび実行コンフィギュレーションに含まれるコマンドはどちらもすべて保存されます。このコマンドを実行した場合、実行コンフィギュレーションのコマンドは、コピー元のファイルに含まれていないものであっても削除されません。それに対して、**configure replace** *target-url* コマンドを実行した場合、実行コンフィギュレーションのコマンドのうち、置換用ファイルに含まれていないものは削除され、実行コンフィギュレーション内に存在しないコマンドは追加されます。
- **copy** *source-url* **running-config** コマンドでは、コンフィギュレーション ファイルの一部分をコピー元ファイルとして使用できます。**configure replace** replace *target-url* コマンドの場合は、置換用のファイルとして 1 つのコンフィギュレーション ファイル全体を使用する必要があります。

コンフィギュレーションのロールバック

configure replace コマンドを使用すると、コンフィギュレーションを前回保存した以降に変更された内容をロールバックすることもできます。コンフィギュレーション ロールバック機能では、適用されている特定の変更内容に基づいてロールバック処理を行うのではなく、保存されているコンフィギュレーション ファイルを基にして特定のコンフィギュレーションに戻します。

コンフィギュレーション ロールバック機能を使用するときは、コンフィギュレーションの内容を変更する前に実行コンフィギュレーションを保存しておく必要があります。コンフィギュレーションの内容を変更した場合は、**configure replace** *target-url* コマンドを使用すれば、保存されているコンフィギュレーション ファイルを基に変更内容をロールバックできます。

ロールバック用コンフィギュレーションには、保存されている任意のコンフィギュレーション ファイルを指定できます。一部のロールバック モデルとは異なり、ロールバックの回数に制限はありません。

コンフィギュレーションの置換とロールバックに関する注意事項

- スイッチのメモリに、2 つのコンフィギュレーション ファイル（実行コンフィギュレーションと保存されている置換用コンフィギュレーション）の合計サイズを超える空き容量があることを確認してください。空き容量が不足していると、コンフィギュレーションの置換は正常に実行されません。
- またスイッチのメモリに、コンフィギュレーションの置換コマンドやロールバック コマンドを実行する十分な空き容量があることも確認してください。
- ネットワーキング デバイスの物理コンポーネント（物理インターフェイスなど）を対象とする一部のコンフィギュレーション コマンドは、実行コンフィギュレーションに追加することも、実行コンフィギュレーションから削除することもできません。
  - **interface** *interface-id* コマンドに指定されたインターフェイスが実際にデバイス上に存在する場合、コンフィギュレーションの置換処理では、このコマンド行を実行コンフィギュレーションから削除できません。
  - **interface** *interface-id* コマンド行に指定されたインターフェイスが実際にはデバイス上に存在しない場合、このコマンド行を実行コンフィギュレーションに追加できません。
- **configure replace** コマンドを使用するときは、実行コンフィギュレーションに対する置換用コンフィギュレーション ファイルとして、保存されているコンフィギュレーションを指定する必要があります。置換用ファイルは、Cisco IOS デバイスにより生成された完全なコンフィギュレーション（**copy running-config** *destination-url* コマンドにより生成されたコンフィギュレーションなど）であることが必要です。

（注）　置換用コンフィギュレーション ファイルを外部で生成する場合、そのファイルは Cisco IOS デバイスにより生成されるファイルのフォーマットに準拠している必要があります。

コンフィギュレーション アーカイブの設定

configure replace コマンドは、必ずしもコンフィギュレーション アーカイブや **archive config** コマンドと併用する必要はありませんが、コンフィギュレーション ロールバックを実行する場合には非常に有用なコマンドです。**archive config** コマンドを使用するときは、事前にコンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**archive**	アーカイブ コンフィギュレーション モードを開始します。
ステップ 3	**path** *url*	コンフィギュレーション アーカイブに保存するファイルの場所およびファイル名のプレフィクスを指定します。
ステップ 4	**maximum** *number*	（任意）コンフィギュレーション アーカイブに保存する実行コンフィギュレーションのアーカイブ ファイルの最大数を設定します。 *number*：コンフィギュレーション アーカイブに保存する実行コンフィギュレーションのアーカイブ ファイルの最大数を指定します。有効な値は 1 ～ 14 です。デフォルト値は 10 です。 **（注）** このコマンドを使用するには、**path** アーカイブ コンフィギュレーション コマンドを入力して、コンフィギュレーション アーカイブに保存されるファイルの場所およびファイル名のプレフィクスをあらかじめ指定しておく必要があります。
ステップ 5	**time-period** *minutes*	（任意）コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する時間間隔を設定します。 *minutes*：コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する時間間隔を分単位で指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

コンフィギュレーションの置換処理またはロールバック処理の実行

実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルに置換するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**archive config**	（任意）実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。 **（注）** このコマンドを使用する前に **path** アーカイブ コンフィギュレーション コマンドを入力します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3		実行コンフィギュレーションに対して必要な変更を行います。
ステップ 4	**exit**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**configure replace** *target-url* [**list**] [**force**] [**time** *seconds*] [**nolock**]	実行コンフィギュレーションを保存されているコンフィギュレーション ファイルに置換します。 *target-url*：ステップ 2 で **archive config** 特権 EXEC コマンドを使用して作成したコンフィギュレーション ファイルなど、実行コンフィギュレーションと置換する保存済みコンフィギュレーション ファイルの URL（ファイル システムからアクセス可能な URL）を指定します。 **list**：コンフィギュレーションの置換処理における各パスでソフトウェア パーサーにより適用されるコマンド エントリをリスト表示します。パスの合計数も表示されます。 **force**：実行コンフィギュレーションを保存されているコンフィギュレーション ファイルに置換する際、確認のプロンプトが表示されないようにします。 **time** *seconds*：実行コンフィギュレーション ファイルの置換を確定する **configure confirm** コマンドを入力するまでの制限時間（秒単位）を指定します。指定した時間内に **configure confirm** コマンドを入力しないと、コンフィギュレーションの置換処理は自動的に停止します （つまり、実行コンフィギュレーションが **configure replace** コマンドを入力する前まで存在していたコンフィギュレーションに戻ります）。 **（注）** **time** *seconds* コマンドライン オプションを使用する場合は、コンフィギュレーション アーカイブを事前にイネーブルにしておく必要があります。 **nolock**：コンフィギュレーションの置換処理中に他のユーザが実行コンフィギュレーションを変更できないようにするための実行コンフィギュレーションのロックをディセーブルにします。
ステップ 6	**configure confirm**	（任意）実行コンフィギュレーションを保存されているコンフィギュレーション ファイルで置換することを確定します。 **（注）** このコマンドを使用するのは、**configure replace** コマンドで **time** *seconds* キーワードおよび引数を指定した場合だけです。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ソフトウェア イメージの操作

ここでは、システム ソフトウェア、Cisco IOS コード、および組み込みデバイス マネージャ ソフトウェアが含まれるソフトウェア イメージ ファイルをアーカイブ（ダウンロードおよびアップロード）する方法について説明します。

（注） ソフトウェア イメージ ファイルをダウンロードおよびアップロードするときは、**copy** 特権 EXEC コマンドや **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** 特権 EXEC コマンドおよび **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

スイッチ ソフトウェアをアップグレードするには、TFTP サーバ、FTP サーバ、または RCP サーバからスイッチ イメージ ファイルをダウンロードします。TFTP サーバを使用したスイッチのアップグレードに関する詳細については、リリース ノートを参照してください。

現在のイメージを新しいイメージに置き換えたり、ダウンロード後に現在のイメージをフラッシュ メモリに保管したりできます。

スイッチ イメージ ファイルをバックアップするときは、それを TFTP サーバ、FTP サーバ、または RCP サーバにアップロードします。アップロードされたこのイメージは、それ以降同じスイッチや同じタイプの別のスイッチにダウンロードできます。

使用するプロトコルは、使用しているサーバのタイプによって異なります。FTP や RCP のトランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが高速化され、データがより確実に伝送されます。こうした優れた動作は、FTP および RCP がコネクション型の TCP/IP スタックに基づいて構築され、実際に TCP/IP スタックが使用されることで実現されるものです。

ここでは、次の設定情報について説明します。

- 「スイッチ上のイメージの場所」（P.B-24）
- 「サーバまたは Cisco.com 上のイメージの tar ファイル形式」（P.B-24）
- 「TFTP によるイメージ ファイルのコピー」（P.B-25）
- 「FTP によるイメージ ファイルのコピー」（P.B-28）
- 「RCP によるイメージ ファイルのコピー」（P.B-33）

（注）　ソフトウェア イメージ、およびサポートされているアップグレード パスのリストについては、スイッチのリリース ノートを参照してください。

スイッチ上のイメージの場所

Cisco IOS イメージは、バージョン番号を表すディレクトリ内の *.bin* ファイルとして格納されます。サブディレクトリには、Web 管理用のファイルが格納されます。イメージはシステム ボードのフラッシュ メモリ（flash:）に格納されます。

show version 特権 EXEC コマンドを使用すると、スイッチ上で現在動作しているソフトウェア バージョンを参照できます。画面上で、`System image file is...` で始まる行を調べます。この行には、イメージが格納されているフラッシュ メモリ内のディレクトリ名が表示されます。

フラッシュ メモリ内に格納したその他のソフトウェア イメージのディレクトリ名を参照する場合には、**dir** *filesystem*: 特権 EXEC コマンドを使用することもできます。

サーバまたは Cisco.com 上のイメージの tar ファイル形式

サーバ上にあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは tar ファイル形式で提供され、次のファイルが含まれます。

- tar ファイルの目次の役割を持つ *info* ファイル
- Cisco IOS イメージなど、他のイメージやファイルが格納された 1 つまたは複数のサブディレクトリ

次に、info ファイルに含まれている情報の一部を表示する例を示します。表 B-3 は、この情報に関する詳細をまとめたものです。

```
version_suffix: image-name
version_directory: image-name
image_system_type_id: 0x00000000
image_name: image-name .bin
ios_image_file_size: 4526592
```

```
total_image_file_size: 4526592
image_feature: LAYER_2|MIN_DRAM_MEG=64
image_family: family
stacking_number: 1.11
board_ids: 0x00000029
info_end:
```

（注）　stacking_number フィールドは無視してください。このフィールドはスイッチには適用されません。

表 B-3　　info ファイルの説明

フィールド	説明
version_suffix	Cisco IOS イメージ バージョン ストリングのサフィックスです。
version_directory	Cisco IOS イメージおよび HTML サブディレクトリがインストールされるディレクトリです。
image_name	tar ファイル内の Cisco IOS イメージの名前です。
ios_image_file_size	tar ファイル内の Cisco IOS イメージのサイズです。このサイズは、Cisco IOS イメージだけを保持するために必要なフラッシュ メモリの概略値です。
total_image_file_size	tar ファイル内の全イメージ（Cisco IOS イメージおよび Web 管理ファイル）のサイズです。このサイズは、これらのファイルを保持するために必要なフラッシュ メモリの概略値です。
image_feature	イメージの主な機能に関する説明です。
image_min_dram	このイメージを実行するために必要な DRAM の最小サイズです。
image_family	ソフトウェアをインストールできる製品ファミリーに関する説明です。

TFTP によるイメージ ファイルのコピー

スイッチ イメージは、TFTP サーバからダウンロードしたり、スイッチから TFTP サーバにアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きできるだけでなく、必要であればダウンロード後も現在のイメージを保持できます。

スイッチ イメージ ファイルをバックアップするときは、それをサーバにアップロードします。アップロードされたこのイメージは、それ以降同じスイッチや同じタイプの別のスイッチにダウンロードできます。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするときは、**copy** 特権 EXEC コマンドや **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** 特権 EXEC コマンドおよび **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-26）
- 「TFTP によるイメージ ファイルのダウンロード」（P.B-26）
- 「TFTP によるイメージ ファイルのアップロード」（P.B-28）

TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能するワークステーションが、適切に設定されていることを確認します。Sun ワークステーションで、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

  /etc/services ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```

  （注）　/etc/inetd.conf ファイルおよび /etc/services ファイルを変更したら、inetd デーモンを再起動する必要があります。このデーモンを再起動する場合は、inetd プロセスをいったん終了して再起動するか、**fastboot** コマンド（SunOS 4.x の場合）または **reboot** コマンド（Solaris 2.x または SunOS 5.x の場合）を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが格納されていることを確認します。ルータでサブネット間トラフィックのルーティングを実行しない場合は、スイッチおよび TFTP サーバを同じサブネット内に配置する必要があります。**ping** コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするイメージが、TFTP サーバ上の正しいディレクトリ内にあることを確認します（UNIX ワークステーションの場合は通常 /tftpboot）。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。
- イメージ ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* には、イメージをサーバへアップロードするときに使用するファイルの名前を指定します。
- アップロード処理中にサーバ上の既存ファイル（空のファイルを作成する必要がある場合は空のファイルを含む）を上書きするときは、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードしたら、現在のイメージをそのイメージ ファイルに置き換えることも、現在のイメージを保持することもできます。

TFTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードで次のステップ 1 ～ 3 を実行します。現在のイメージを保持する場合は、ステップ 3 に進んでください。

	コマンド	目的
ステップ 1		イメージをワークステーション上の適切な TFTP ディレクトリにコピーします。TFTP サーバが適切に設定されていることを確認します（「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-26）を参照）。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。

	コマンド	目的
ステップ 3	**archive download-sw /overwrite /reload tftp:**[[*//location*]/*directory*]/*image-name*.**tar**	TFTP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージに上書きします。 • オプション **/overwrite** を指定すると、フラッシュ メモリ内のソフトウェア イメージが、ダウンロードされたイメージで上書きされます。 • オプション **/reload** を指定すると、設定が変更されて保存されなかった場合を除き、イメージのダウンロード後にシステムがリロードされます。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。
ステップ 4	**archive download-sw /leave-old-sw /reload tftp:**[[*//location*]/*directory*]/*image-name*.**tar**	TFTP サーバからスイッチにイメージ ファイルをダウンロードする一方、現在のイメージを保持します。 • オプション **/leave-old-sw** を指定すると、ダウンロード後も古いソフトウェア バージョンが保持されます。 • オプション **/reload** を指定すると、設定が変更されて保存されなかった場合を除き、イメージのダウンロード後にシステムがリロードされます。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切かどうか、および DRAM サイズは十分かどうかが検証されます。問題がある場合、プロセスは中断し、エラーが報告されます。オプション **/overwrite** を指定した場合は、ダウンロード アルゴリズムによって、フラッシュ デバイス上の既存のイメージが、新しいイメージと同じであるかどうかに関係なく削除され、新しいイメージがダウンロードされたあと、ソフトウェアがリロードされます。

（注） フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きするには、オプション **/overwrite** を指定する必要があります。

/leave-old-sw を指定した場合は、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在のイメージを保持しようとすると、ダウンロード プロセスが停止してエラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス（flash:）にインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新しいディレクトリに格納されます。また、新規にインストールされたイメージを示すように BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いイメージが保持されるようにした場合は（キーワード **/leave-old-sw** を指定した場合は）、**delete /force/recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力すれば、そのイメージを削除できます。システム ボード フラッシュ デバイスの場合は、*filesystem* に **flash:** を指定します。*file-url* には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびそのディレクトリが削除されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるため、イメージの名前は変更しないでください。

TFTP によるイメージ ファイルのアップロード

イメージは、スイッチから TFTP サーバにアップロードできます。このイメージは、あとでこのスイッチや同じタイプの別のスイッチにダウンロードできます。

アップロード機能は、組み込みデバイス マネージャに関連する Web 管理ページが、既存イメージとともにインストールされている場合に限り使用してください。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		TFTP サーバが適切に設定されていることを確認します（「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-26）を参照）。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。
ステップ 3	**archive upload-sw tftp:**[[*//location*]*/directory*]*/image-name*.**tar**	現在動作中のスイッチ イメージを TFTP サーバにアップロードします。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、アップロードするソフトウェア イメージのディレクトリ（任意）と名前を指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。*image-name*.**tar** には、サーバに格納されるソフトウェア イメージの名前を指定します。

archive upload-sw 特権 EXEC コマンドを使用すると、info ファイル、Cisco IOS イメージ ファイル、Web 管理ファイルの順にアップロードすることで、サーバ上にイメージ ファイルを作成できます。これらのファイルがアップロードされると、アップロード アルゴリズムによって tar 形式のファイルが作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるため、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのコピー

スイッチ イメージは、FTP サーバからダウンロードしたり、スイッチから FTP サーバにアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きできるだけでなく、必要であればダウンロード後も現在のイメージを保持できます。

スイッチ イメージ ファイルをバックアップするときは、それをサーバにアップロードします。アップロードされたこのイメージは、それ以降同じスイッチや同じタイプの別のスイッチにダウンロードできます。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするときは、**copy** 特権 EXEC コマンドや **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** 特権 EXEC コマンドおよび **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-29）
- 「FTP によるイメージ ファイルのダウンロード」（P.B-30）
- 「FTP によるイメージ ファイルのアップロード」（P.B-32）

FTP によるイメージ ファイルのダウンロードまたはアップロードの準備

イメージ ファイルは、FTP サーバとの間でコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードをクライアントからサーバに送信する必要があります。FTP を使用してスイッチからサーバにイメージ ファイルをコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初にある有効なユーザ名を送信します。

- **archive download-sw** 特権 EXEC コマンドまたは **archive upload-sw** 特権 EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- 匿名。

スイッチは、次のリスト内で最初にある有効なパスワードを送信します。

- **archive download-sw** 特権 EXEC コマンドまたは **archive upload-sw** 特権 EXEC コマンドで指定されたパスワード（パスワードが指定されている場合）。
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）。
- スイッチは、*username@switchname.domain* という名前のパスワードを生成します。変数 *username* は現在のセッションに関連付けられているユーザ名、*switchname* は設定されているホスト名、*domain* はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定する場合は、**ip ftp username** コマンドおよび **ip ftp password** コマンドを使用します。この処理のためだけにユーザ名を指定するときは、**archive download-sw** 特権 EXEC コマンドまたは **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。

サーバにディレクトリ構造がある場合は、ユーザ名に関連付けられたサーバ上のディレクトリが、イメージ ファイルの書き込み先またはコピー先となります。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

FTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが格納されていることを確認します。ルータでサブネット間トラフィックのルーティングを実行しない場合は、スイッチおよび FTP サーバを同じサブネット内に配置する必要があります。**ping** コマンドを使用して、FTP サーバへの接続をチェックします。

- コンソールまたは Telnet セッションを介してスイッチにアクセスしている場合、または有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用されていることを確認します。**show users** 特権 EXEC コマンドを使用すると、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して、新しい FTP ユーザ名を作成します。新しい名前は、すべてのアーカイブ処理において使用されます。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしている場合、有効なユーザ名があれば、そのユーザ名が使用されるため、FTP ユーザ名を設定する必要はありません。ユーザ名をこの処理のためにだけ指定するには、**archive download-sw** 特権 EXEC コマンドまたは **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。
- イメージ ファイルを FTP サーバにアップロードするときは、スイッチ上のユーザからの書き込み要求が許可されるように、FTP サーバを適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードしたら、現在のイメージをそのイメージ ファイルに置き換えることも、現在のイメージを保持することもできます。

FTP サーバから新しいイメージをダウンロードし、既存のイメージを上書きするには、特権 EXEC モードで次のステップ 1 ～ 7 を実行します。現在のイメージを保持する場合は、ステップ 7 に進んでください。

	コマンド	目的
ステップ 1		「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-29）を参照し、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを無効にする場合だけです（ステップ 4、5、6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/image-name*.**tar**	FTP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージを上書きします。 • オプション **/overwrite** を指定すると、フラッシュ メモリ内のソフトウェア イメージが、ダウンロードされたイメージで上書きされます。 • オプション **/reload** を指定すると、設定が変更されて保存されなかった場合を除き、イメージのダウンロード後にシステムがリロードされます。 • *//username*[**:***password*] には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられている必要があります。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-29）を参照してください。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • *directory/image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。
ステップ 8	**archive download-sw /leave-old-sw /reload ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/image-name*.**tar**	FTP サーバからスイッチにイメージ ファイルをダウンロードする一方、現在のイメージを保持します。 • オプション **/leave-old-sw** を指定すると、ダウンロード後も古いソフトウェア バージョンが保持されます。 • オプション **/reload** を指定すると、設定が変更されて保存されなかった場合を除き、イメージのダウンロード後にシステムがリロードされます。 • *//username*[**:***password*] には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-29）を参照してください。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • *directory/image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切かどうか、および DRAM サイズは十分かどうかが検証されます。問題がある場合、プロセスは中断し、エラーが報告されます。オプション **/overwrite** を指定した場合は、ダウンロード アルゴリズムによって、フラッシュ デバイス上の既存のイメージが、新しいイメージと同じであるかどうかに関係なく削除され、新しいイメージがダウンロードされたあと、ソフトウェアがリロードされます。

（注）　フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きするには、オプション **/overwrite** を指定する必要があります。

/leave-old-sw を指定した場合は、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に現在のイメージを保持しようとすると、ダウンロード プロセスが停止してエラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス（flash:）にインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新しいディレクトリに格納されます。また、新規にインストールされたイメージを示すように BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いイメージが保持されるようにした場合は（キーワード **/leave-old-sw** を指定した場合は）、**delete /force/recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力すれば、そのイメージを削除できます。システム ボード フラッシュ デバイスの場合は、*filesystem* に **flash:** を指定します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびそのディレクトリが削除されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるため、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのアップロード

イメージは、スイッチから FTP サーバにアップロードできます。このイメージは、あとでこのスイッチや同じタイプの別のスイッチにダウンロードできます。

アップロード機能は、組み込みデバイス マネージャに関連する Web 管理ページが、既存イメージとともにインストールされている場合に限り使用してください。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-13）を参照し、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを無効にする場合だけです（ステップ 4、5、6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。

	コマンド	目的
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**archive upload-sw** **ftp:**[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*image-name*.**tar**	現在動作中のスイッチ イメージを FTP サーバにアップロードします。 • *//username***:***password* には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-29）を参照してください。 • *@location* には、FTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、アップロードするソフトウェア イメージのディレクトリ（任意）と名前を指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。*image-name*.**tar** には、サーバに格納されるソフトウェア イメージの名前を指定します。

archive upload-sw コマンドを使用すると、info ファイル、Cisco IOS イメージ ファイル、Web 管理ファイルの順にアップロードすることで、サーバ上にイメージ ファイルを作成できます。これらのファイルがアップロードされると、アップロード アルゴリズムによって tar 形式のファイルが作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるため、イメージの名前は変更しないでください。

RCP によるイメージ ファイルのコピー

スイッチ イメージは、RCP サーバからダウンロードしたり、スイッチから RCP サーバにアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きできるだけでなく、必要であればダウンロード後も現在のイメージを保持できます。

スイッチ イメージ ファイルをバックアップするときは、それをサーバにアップロードします。アップロードされたこのイメージは、それ以降同じスイッチや同じタイプの別のスイッチにダウンロードできます。

（注）　ソフトウェア イメージ ファイルをダウンロードおよびアップロードするときは、**copy** 特権 EXEC コマンドや **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** 特権 EXEC コマンドおよび **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-34）
- 「RCP によるイメージ ファイルのダウンロード」（P.B-35）
- 「RCP によるイメージ ファイルのアップロード」（P.B-37）

RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

リモート ホストとスイッチの間でのコンフィギュレーション ファイルのダウンロード、アップロード、およびコピーは、RCP を使用して行うこともできます。コネクションレス型プロトコルの UDP を使用する TFTP とは異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーするためには、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合には、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザが行うのは、リモート シェル（rsh）をサポートするサーバへのアクセスだけです （ほとんどの UNIX システムでは rsh がサポートされています）。ファイルは特定の場所から別の場所にコピーされるため、コピー元ファイルの読み取り権限およびコピー先ファイルへの書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとにリモート ユーザ名をクライアントからサーバに送信する必要があります。RCP を使用してスイッチからサーバにイメージをコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初にある有効なユーザ名を送信します。

- **archive download-sw** 特権 EXEC コマンドまたは **archive upload-sw** 特権 EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet 経由でルータに接続され、**username** コマンドを介して認証された場合、スイッチ ソフトウェアからはリモート ユーザ名として Telnet ユーザ名が送信されます。
- スイッチのホスト名。

RCP コピー要求を正常に実行するためには、ネットワーク サーバにリモート ユーザ名のアカウントを定義する必要があります。サーバにディレクトリ構造がある場合は、リモート ユーザ名に関連付けられたサーバ上のディレクトリが、イメージ ファイルの書き込み先またはコピー先となります。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能するワークステーションで、リモート シェル（rsh）がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが格納されていることを確認します。ルータでサブネット間トラフィックのルーティングを実行しない場合は、スイッチおよびサーバを同じサブネット内に配置する必要があります。**ping** コマンドを使用して、RCP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしている場合、または有効なユーザ名がない場合は、RCP ダウンロードに使用するユーザ名が現在の RCP ユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用すると、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのアーカイブ処理中に **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用して、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしている場合、有効なユーザ名があれば、このユーザ名が使用されるため、RCP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定するときは、**archive download-sw** 特権 EXEC コマンドまたは **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。

- イメージ ファイルを RCP サーバにアップロードするときは、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、RCP サーバを適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザの .rhosts ファイルにエントリを追加する必要があります。たとえば、スイッチに次のコンフィギュレーション行が含まれていると仮定します。

```
hostname Switch1
ip rcmd remote-username User0
```

このスイッチの IP アドレスを *Switch1.company.com* に変換するためには、RCP サーバ上の User0 用の .rhosts ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードしたら、現在のイメージをそのイメージ ファイルに置き換えることも、現在のイメージを保持することもできます。

RCP サーバから新しいイメージをダウンロードし、既存のイメージを上書きするときは、特権 EXEC モードで次のステップ 1 ～ 6 を実行します。現在のイメージを保持する場合は、ステップ 6 に進んでください。

	コマンド	目的
ステップ 1		「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-34）を参照し、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を無効にする場合だけです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**archive download-sw /overwrite /reload rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	RCP サーバからスイッチにイメージ ファイルをダウンロードし、現在のイメージを上書きします。 • オプション **/overwrite** を指定すると、フラッシュ メモリ内のソフトウェア イメージが、ダウンロードされたイメージで上書きされます。 • オプション **/reload** を指定すると、設定が変更されて保存されなかった場合を除き、イメージのダウンロード後にシステムがリロードされます。 • *//username* には、ユーザ名を指定します。RCP コピー要求を正常に実行するためには、ネットワーク サーバにリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-34）を参照してください。 • *@location* には、RCP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。
ステップ 7	**archive download-sw /leave-old-sw /reload rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	FTP サーバからスイッチにイメージ ファイルをダウンロードする一方で、現在のイメージを保持します。 • オプション **/leave-old-sw** を指定すると、ダウンロード後も古いソフトウェア バージョンが保持されます。 • オプション **/reload** を指定すると、設定が変更されて保存されなかった場合を除き、イメージのダウンロード後にシステムがリロードされます。 • *//username* には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバにリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-34）を参照してください。 • *@location* には、RCP サーバの IP アドレスを指定します。 • */directory*]/*image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切かどうか、および DRAM サイズは十分かどうかが検証されます。問題がある場合、プロセスは中断し、エラーが報告されます。オプション **/overwrite** を指定した場合は、ダウンロード アルゴリズムによって、フラッシュ デバイス上の既存のイメージが、新しいイメージと同じであるかどうかに関係なく削除され、新しいイメージがダウンロードされたあと、ソフトウェアがリロードされます。

（注）　フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きするには、オプション **/overwrite** を指定する必要があります。

/leave-old-sw を指定した場合は、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に現在のイメージを保持しようとすると、ダウンロード プロセスが停止してエラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス（flash:）にインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新しいディレクトリに格納されます。また、新規にインストールされたイメージを示すように BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いソフトウェアが保持されるようにした場合は（**/leave-old-sw** キーワードを指定した場合は）**delete /force/recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力すれば、そのソフトウェアを削除できます。システム ボード フラッシュ デバイスの場合は、*filesystem* に **flash:** を指定します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびそのディレクトリが削除されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるため、イメージの名前は変更しないでください。

RCP によるイメージ ファイルのアップロード

イメージは、スイッチから RCP サーバにアップロードできます。このイメージは、あとでこのスイッチや同じタイプの別のスイッチにダウンロードできます。

アップロード機能は、組み込みデバイス マネージャに関連付けられている Web 管理ページが、既存イメージとともにインストールされている場合に限り使用してください。

イメージを RCP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-34）を参照し、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介してスイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を無効にする場合だけです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**archive upload-sw rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	現在動作中のスイッチ イメージを RCP サーバにアップロードします。 • *//username* には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバにリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.B-34）を参照してください。 • *@location* には、RCP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、アップロードするソフトウェア イメージのディレクトリ（任意）と名前を指定します。ディレクトリおよびイメージの名前は大文字と小文字が区別されます。 • *image-name*.**tar** は、サーバに保存するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを使用すると、info ファイル、Cisco IOS イメージ ファイル、Web 管理ファイルの順にアップロードすることで、サーバ上にイメージ ファイルを作成できます。これらのファイルがアップロードされると、アップロード アルゴリズムによって tar 形式のファイルが作成されます。

注意　ダウンロードおよびアップロード アルゴリズムを適切に動作させるため、イメージの名前は変更しないでください。

APPENDIX C

Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド

この付録では、Cisco Metro Ethernet (ME) 3400E イーサネット アクセス スイッチのプロンプトに疑問符（?）を入力したときに表示される CLI（コマンドライン インターフェイス）コマンドの中で、テストされていないか、またはハードウェアの制限により、このリリースでサポートされていないものをいくつか示します。このリストに記載されていないものもあります。サポートされていないコマンドは、ソフトウェア機能およびコマンド モード別にリストされています。

アクセス コントロール リスト

サポートされていない特権 EXEC コマンド

access-enable [**host**] [**timeout** *minutes*]

access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*] [**timeout** *minutes*]

clear access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*]

サポートされていないグローバル コンフィギュレーション コマンド

access-list rate-limit *acl-index* {*precedence* | **mask** *prec-mask*}

access-list dynamic extended

ARP コマンド

サポートされていないグローバル コンフィギュレーション コマンド

arp *ip-address hardware-address* **smds**

arp *ip-address hardware-address* **srp-a**

arp *ip-address hardware-address* **srp-b**

サポートされていないインターフェイス コンフィギュレーション コマンド

arp probe

ip probe proxy

ブートローダ コマンド

サポートされていないユーザ EXEC コマンド

verify

サポートされていないグローバル コンフィギュレーション コマンド

ブート バッファサイズ

デバッグ コマンド

debug dot1x feature

debug platform cli-redirection main

debug platform configuration

debug qos

Embedded Event Manager

サポートされていない特権 EXEC コマンド

event manager update user policy [*policy-filename* | *group* [*group name expression*]] | *repository* [*url location*]

次のコマンドに対して、パラメータはサポートされていません。

event manager run [*policy name*] |<*paramater1*>|... <***paramater15***>|

サポートされていないグローバル コンフィギュレーション コマンド

no event manager directory user repository [*url location*]

event manager applet [*applet-name*] maxrun

サポートされていない Applet コンフィギュレーション モードのコマンド

no event interface name [*interface-name*] **parameter** [*counter-name*] entry-val [*entry counter value*] **entry-op** {*gt* | *ge* | *eq* | *ne* |*lt* | *le*} [**entry-type {increment | rate | value**] [**exit-val** [*exit value*] **exit-op** {*gt* | *ge* | *eq* | *ne* |*lt* | *le*} **exit-type { increment | rate | value}**][**average-factor <average-factor-value>**]

no trigger

tag

HSRP

サポートされていないグローバル コンフィギュレーション コマンド

interface Async

interface BVI

interface Dialer

interface Group-Async

interface Lex

interface Multilink

interface Virtual-Template

interface Virtual-Tokenring

サポートされていないインターフェイス コンフィギュレーション コマンド

mtu

standby mac-refresh *seconds*

standby use-bia

IEEE 802.1x

サポートされていないグローバル コンフィギュレーション コマンド

dot1x critical

サポートされていないインターフェイス コンフィギュレーション コマンド

dot1x auth-fail

dot1x control-direction

dot1x critical

dot1x host-mode multi-domain

dot1x mac-auth-bypass

dot1x pae

（注）　スイッチは、IEEE 802.1x MAC 認証バイパスまたはゲスト VLAN 機能をサポートしていません。

サポートされていない特権 EXEC コマンド

clear dot1x

clear eap sessions

show eap

サポートされていないグローバル コンフィギュレーション コマンド

dot1x critical {**eapol** | **recovery delay** ***ms***}

サポートされていないインターフェイス コンフィギュレーション コマンド

dot1x auth-fail {**max-attempts** *number*| **vlan** *vlan-id*}

dot1x control-direction {both | in}

dot1x critical [**recovery action reinitialize** | **vlan** *vlan-id*}

dot1x control-direction {both | in}

dot1x mac-auth-bypass

dot1x mac-reauth-req

dot1x pae

dot1x timeout rate-limit period

IGMP スヌーピング コマンド

サポートされていないグローバル コンフィギュレーション コマンド

ip igmp snooping source-only-learning

インターフェイス コマンド

サポートされていない特権 EXEC コマンド

show interfaces [*interface-id* | **vlan** *vlan-id*] [**crb** | **fair-queue** | **irb** | **mac-accounting** | **precedence** | **irb** | **random-detect** | **rate-limit** | **shape**]

サポートされていないグローバル コンフィギュレーション コマンド

interface tunnel

サポートされていないインターフェイス コンフィギュレーション コマンド

transmit-interface *type number*

IP マルチキャスト ルーティング

サポートされていない特権 EXEC コマンド

clear ip rtp header-compression [*type number*]

clear ip dvmrp route コマンド

debug ip dvmrp コマンド

debug ip packet コマンドを実行すると、スイッチの CPU で受信されるパケットが表示されます。ハードウェアでスイッチングされるパケットは表示されません。

debug ip mcache コマンドは、スイッチの CPU で受信されるパケットに影響します。ハードウェアでスイッチングされるパケットは表示されません。

debug ip mpacket [**detail**] [*access-list-number* [*group-name-or-address*] コマンドは、スイッチの CPU で受信されるパケットにだけ影響します。ほとんどのマルチキャスト パケットはハードウェアでスイッチングされるため、このコマンドは、パケットが CPU に転送されることがわかっている場合だけ使用してください。

debug ip pim atm

show frame-relay ip rtp header-compression [**interface** *type number*]

show ip dvmrp route コマンド

show ip mcache コマンドを実行すると、スイッチの CPU に送信されるパケット用のキャッシュ内のエントリが表示されます。ほとんどのマルチキャスト パケットは CPU の関与を受けずにハードウェアでスイッチングされるため、このコマンドを使用しても、マルチキャスト パケット情報は表示されません。

show ip mpacket コマンドはサポートされていますが、スイッチの CPU で受信されるパケットに対してだけ効果があります。ルートがハードウェアによってスイッチングされる場合、このコマンドは効果がありません。CPU はパケットを受信せず、パケット情報が表示されないためです。

show ip pim vc [*group-address* | *name*] [*type number*]

show ip rtp header-compression [*type number*] [**detail**]

サポートされていないグローバル コンフィギュレーション コマンド

すべての **ip dvmrp** コマンド

ip multicast-routing vrf *vrf-name*

ip pim accept-rp {*address* | **auto-rp**} [*group-access-list-number*]

ip pim message-interval *seconds*

ip pim register-rate-limit

サポートされていないインターフェイス コンフィギュレーション コマンド

frame-relay ip rtp header-compression [**active** | **passive**]

frame-relay map ip *ip-address dlci* [**broadcast**] **compress**

frame-relay map ip *ip-address dlci* **rtp header-compression** [**active** | **passive**]

すべての **ip dvmrp** コマンド

ip igmp helper-address *ip-address*

ip multicast helper-map {*group-address* | **broadcast**} {*broadcast-address* | *multicast-address*} *extended-access-list-number*

ip multicast rate-limit {**in** | **out**} [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*] *kbps*

ip multicast ttl-threshold *ttl-value*（代わりに **ip multicast boundary** *access-list-number* インターフェイス コンフィギュレーション コマンドを使用）

ip multicast use-functional

ip pim minimum-vc-rate *pps*

ip pim multipoint-signalling

ip pim nbma-mode

ip pim vc-count *number*

ip rtp compression-connections *number*

ip rtp header-compression [**passive**]

IP ユニキャスト ルーティング

サポートされていない特権 EXEC コマンドまたはユーザ EXEC コマンド

clear ip accounting [**checkpoint**]

clear ip bgp *address* flap-statistics

clear ip bgp prefix-list

debug ip cef stats

show cef [**drop** | **not-cef-switched**]

show ip accounting [**checkpoint**] [**output-packets** | **access-violations**]

show ip bgp dampened-paths

show ip bgp inconsistent-as

show ip bgp regexp *regular expression*

show ip prefix-list *regular expression*

show ipv6

サポートされていないグローバル コンフィギュレーション コマンド

ip accounting-list ***ip-address wildcard***

ip as-path access-list

ip accounting-transits *count*

ip cef accounting [**per-prefix**] [**non-recursive**]

ip cef traffic-statistics [**load-interval** *seconds*] [**update-rate** *seconds*]]

ip flow-aggregation

ip flow-cache

ip flow-export

ip gratuitous-arps

ip local

ip prefix-list

ip reflexive-list

router egp

router-isis

router iso-igrp

router mobile

router odr

router static

サポートされていないインターフェイス コンフィギュレーション コマンド

dampening

ip load-sharing [**per-packet**]

ip accounting

ip load-sharing [**per-packet**]

ip mtu *bytes*

ip ospf dead-interval minimal hello-multiplier *multiplier*

ip verify

ip unnumbered *type number*

すべての **ip security** コマンド

サポートされていない BGP ルータ コンフィギュレーション コマンド

address-family vpnv4

default-information originate

neighbor advertise-map

neighbor allowas-in

neighbor default-originate

neighbor description

network backdoor

table-map

サポートされていない VPN コンフィギュレーション コマンド

すべて

サポートされていないルート マップ コマンド

match route-type（ポリシー ベース ルーティング [PBR]）

set as-path {**tag** | **prepend** *as-path-string*}

set automatic-tag

set dampening *half-life reuse suppress max-suppress-time*

set default interface *interface-id* [*interface-id.....*]

set interface *interface-id* [*interface-id.....*]

set ip default next-hop *ip-address* [*ip-address.....*]

set ip destination *ip-address mask*

set ip precedence *value*

set ip *qos-group*

set metric-type internal

set origin

set metric-type internal

set tag *tag-value*

MAC アドレス

サポートされていない特権 EXEC コマンド

show mac-address-table

show mac-address-table address

show mac-address-table aging-time

show mac-address-table count

show mac-address-table dynamic

show mac-address-table interface

show mac-address-table multicaset

show mac-address-table notification

show mac-address-table static

show mac-address-table vlan

show mac address-table multicast

（注）　VLAN のレイヤ 2 マルチキャスト アドレス テーブルのエントリを表示するには、**show ip igmp snooping groups** 特権 EXEC コマンドを使用します。

サポートされていないグローバル コンフィギュレーション コマンド

mac-address-table aging-time

mac-address-table notification

mac-address-table static

その他

サポートされていないユーザ EXEC コマンド

verify

サポートされていない特権 EXEC コマンド

archive config

file verify auto

remote command all

show archive config

show archive log
show cable-diagnostics prbs
show power inline
test cable-diagnostics prbs

サポートされていないグローバル コンフィギュレーション コマンド

exception crashinfo
errdisable detect cause dhcp-rate-limit
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause unicast flood
l2protocol-tunnel global drop-threshold
memory reserve critical
power inline consumption default *wattage*
service compress-config
stack-mac persistent timer
track *object-number* **rtr**

サポートされていない show platform コマンド

show platform ip unicast vrf {**compaction** | **tcam-label**}
show platform ipv6 unicast
show platform tb

MSDP

サポートされていない特権 EXEC コマンド

show access-expression
show exception
show location
show pm LINE
show smf [*interface-id*]
show subscriber-policy [*policy-number*]
show template [*template-name*]

サポートされていないグローバル コンフィギュレーション コマンド

ip msdp default-peer *ip-address* | *name* [**prefix-list** *list*]（BGP/MBGP がサポートされていないため、このコマンドの代わりに **ip msdp peer** コマンドを使用）

NetFlow

サポートされていないグローバル コンフィギュレーション コマンド

ip flow-aggregation cache

ip flow-cache entries

ip flow-export

QoS

サポートされていないグローバル コンフィギュレーション コマンド

priority-list

サポートされていないインターフェイス コンフィギュレーション コマンド

priority-group

サポートされていない policy-map Class Police Configuration Mode コマンド

conform-color *class-map* **police configuration**

RADIUS

サポートされていないグローバル コンフィギュレーション コマンド

aaa authentication *feature* **default enable**

aaa authentication *feature* **default line**

aaa nas port extended

authentication command bounce-port ignore

authentication command disable-port ignore

radius-server attribute nas-port

radius-server configure

radius-server extended-portnames

SNMP

サポートされていないグローバル コンフィギュレーション コマンド

snmp-server enable informs

snmp-server ifindex persist

スパニングツリー

サポートされていないグローバル コンフィギュレーション コマンド

spanning-tree pathcost method {long | short}

spanning-tree transmit hold-count

サポートされていないインターフェイス コンフィギュレーション コマンド

spanning-tree stack-port

ストーム制御

（注）　コマンドライン インターフェイスでは表示されますが、既存のブロードキャスト ストーム ディセーブル機能が小さなフレームを正しく制御できるので、小さなフレームのしきい値をスイッチに設定するコマンドは必要ありません。

サポートされていないグローバル コンフィギュレーション コマンド

errdisable detect cause small-frame

errdisable recovery cause small-frame

サポートされていないインターフェイス コンフィギュレーション コマンド

small-frame violation rate

VLAN

サポートされていないグローバル コンフィギュレーション コマンド

vlan internal allocation policy {ascending | descending}

サポートされていないユーザ EXEC コマンド

show running-config vlan

show vlan ifindex

vlan database

サポートされていない VLAN データベース コマンド

vtp

vlan

INDEX

数字

2 重タグ パケット
  IEEE 802.1Q トンネリング 14-3
  レイヤ 2 プロトコル トンネリング 14-16
802.1X 許可ステートのポート 9-4
802.1X 無許可ステートのポート 9-4

A

ABR 36-26
access-class コマンド 32-19
ACE
  IP 32-2
  イーサネット 32-2
  定義 32-2
ACL
  ACE 32-2
  any キーワード 32-12, 34-41
  host キーワード 32-12, 34-41
  IP
    暗黙の拒否 32-9, 32-14, 32-16
    一致条件 32-7
    作成 32-7
    マスクの省略 32-9
    未定義 32-20
  IPv4
    一致条件 32-7
    インターフェイスへの適用 32-19
    作成 32-7
    サポートされていない機能 32-7
    端末回線、設定 32-18
    名前付き 32-14
    番号 32-8
  IPv6
    一致条件 39-3
    インターフェイスへの適用 39-7
    サポートされていない機能 39-3
    サポート対象 39-2
    制限事項 39-3
    設定 39-3, 39-4
    他の機能との相互作用 39-4
    名前付き 39-3
    表示 39-8
    優先順位 39-2
MAC 拡張 32-27
QoS 34-11
QoS に関するトラフィックの分類 34-39
VLAN マップ
  設定 32-30
  設定時の注意事項 32-30
エントリの並べ替え 32-14
拡張 IPv4
  一致条件 32-7
  作成 32-10
コメント 32-18
コンパイル 32-22
サポート 1-9
サポートされていない機能
  IPv6 39-3
サポートされていない機能、IPv4 32-7
サポート対象のタイプ 32-2
時間範囲 32-16
照合 32-7, 32-20
定義 32-1, 32-7
適用

IPv6 インターフェイスへの 39-7
QoS 34-11
インターフェイス 32-19, 39-7
時間範囲 32-16
スイッチド パケット 32-38
マルチキャスト パケット 32-40
ルーテッド パケット 32-39
名前 39-4
名前付き
IPv6 39-3
名前付き、IPv4 32-14
ハードウェアおよびソフトウェアでの処理 32-20
ハードウェアでのサポート 32-20
標準 IPv4
一致条件 32-7
作成 32-9
ポート 32-2, 39-2
モニタリング 32-40, 39-8
優先順位 32-2
ルータ 32-2, 39-2
ルータ ACL と VLAN マップの設定時の注意事項 32-37
ルータ ACL を VLAN マップと組み合せて使用する方法 32-37
例 32-22
レイヤ 4 情報 32-38
ログ メッセージ 32-8
ACL による分類、QoS 34-11
ARP
カプセル化 36-10
スタティック キャッシュの設定 36-8
設定 36-8
定義 1-4, 5-31, 36-8
テーブル
アドレス解決 5-31
管理 5-31
ASBR 36-26
AS パス フィルタ、BGP 36-57

B

bandwidth remaining percent コマンド 34-32
bandwidth コマンド
CBWFQ 34-28
police コマンド 34-32
QoS、設定 34-67
QoS、説明 34-30
Berkeley r-tools の代替機能 8-42
BGP
CIDR 36-63
clear コマンド 36-66
show コマンド 36-66
イネーブル化 36-50
コミュニティ フィルタリング 36-59
サポート 1-11
集約アドレス 36-63
集約ルート、設定 36-63
スーパーネット 36-63
セッションのリセット 36-52
説明 36-47
デフォルト設定 36-48, 36-80
ネイバー、タイプ 36-50
ネイバーの設定 36-61
バージョン 4 36-47
パス選択 36-54
ピア、設定 36-61
プレフィクス フィルタリング 36-58
マルチ VRF CE によるルーティング セッション 36-96
マルチパス サポート 36-54
モニタリング 36-66
ルーティング ドメイン連合 36-63
ルート ダンプニング 36-65
ルート マップ 36-56
ルート リフレクタ 36-64
BPDU
errdisable ステート 17-3
RSTP フォーマット 16-12

フィルタリング 17-3
BPDU ガード
イネーブル化 17-8
サポート 1-6
説明 17-3
ディセーブル化 17-9
BPDU フィルタリング
イネーブル化 17-9
サポート 1-6
説明 17-3
ディセーブル化 17-10
broadcast storm-control コマンド 23-4
bulkstat object-list 30-19
bulkstat schema 30-20

C

CBWFQ
bandwidth コマンド 34-30, 34-67
QoS スケジューリング 34-28
設定時の注意事項 34-67
CDP
LLDP による定義 25-1
アップデート 24-2
イネーブル化とディセーブル化
インターフェイス 24-4
スイッチ 24-3
概要 24-1
サポート 1-4
設定 24-2
説明 24-1
タイマーおよびホールドタイム、設定 24-2
デフォルト設定 24-2
モニタリング 24-5
ルーティング デバイスでのディセーブル化 24-3 ～ 24-4
レイヤ 2 プロトコル トンネリング 14-13
CEF
IPv6 37-19
イネーブル化 36-102
定義 36-101
CFM
Continuity Check メッセージ 43-5
EtherChannel のサポート 43-8
EtherChannel ポート チャネル 43-8
IEEE 802.1ag 43-2
IP SLA の PING またはジッタの手動設定 43-18
IP SLA のサポート 43-7
MEP アップ 43-4
MEP ダウン 43-4
OAM マネージャ 43-47
SNMP トラップ 43-6
traceroute メッセージ 43-5
UNI 43-4
Y.1731
説明 43-21
イーサネット OAM、設定 43-54
イーサネット OAM との相互作用 43-54
エンドポイント ディスカバリによる IP SLA 43-20
クロスチェック 43-5
クロスチェックの設定 43-12
障害アラーム
設定 43-16
定義 43-6
障害アラームの設定 43-16
消去 43-29
スタティック RMEP、設定 43-13
スタティック RMEP チェック 43-5
スタティック リモート MEP の設定 43-13
設定エラー 43-6
設定時の注意事項 43-8
その他の機能 43-8
定義 43-2
デフォルト設定 43-8
ドラフト 1 43-4
ドラフト 8.1 43-4
トンネル 43-8
ネットワークの設定 43-9

ネットワーク パフォーマンスの測定 43-7
バージョンの相互運用性 43-6
ポート MEP、設定 43-14
ポート MEP の設定 43-14
メッセージ
Continuity Check 43-5
traceroute 43-5
ループバック 43-5
メッセージ タイプ 43-5
メンテナンス アソシエーション 43-3
メンテナンス ドメイン 43-2
メンテナンス ポイント 43-3
モニタリング 43-29, 43-30
リモート MEP 43-5
ループバック メッセージ 43-5
CIDR 36-63
Cisco Configuration Engine 1-3
Cisco Data Collection MIB 30-2
Cisco IOS IP SLA 41-2
Cisco IOS ファイル システム
「IFS」を参照
Cisco Process MIB 30-2
CiscoWorks 2000 1-4, 30-4
CISP 9-10
CIST リージョナル ルート
「MSTP」を参照
CIST ルート
「MSTP」を参照
class-map コマンド 34-3
CLI
エラー メッセージ 2-4
コマンド出力のフィルタリング 2-8
コマンドの no 形式と default 形式 2-3
コマンドの省略形 2-3
コマンド モード 2-1
説明 1-3
ヘルプ システムの概要 2-3
編集機能
イネーブル化とディセーブル化 2-6
折り返し機能 2-7
キーストロークによる編集 2-6
履歴
コマンドの呼び出し方法 2-5
説明 2-4
ディセーブル化 2-5
バッファ サイズの変更 2-4
CLNS
「ISO CLNS」を参照
CNS
Configuration Engine
configID、deviceID、ホスト名 4-3
Configuration Service 4-2
Event Service 4-3
説明 4-1
アップグレード 4-14
組み込み型エージェント
イベント エージェントのイネーブル化 4-7
コンフィギュレーション エージェントのイネーブル化 4-9
自動設定のイネーブル化 4-7
説明 4-5
config.text 3-18
configure terminal コマンド 10-9
Connectivity Fault Management
「CFM」を参照
CoS
値 34-6
分類 34-8
CPU しきい値通知 30-22
CPU しきい値テーブル 30-2, 30-22
CPU の過負荷、保護 33-1
CPU 保護 33-4
CPU ポリシング機能 33-6
CPU 利用率の統計情報 30-22
crashinfo ファイル 46-21
C-VLAN 14-8

D

default コマンド 2-3
description コマンド 10-26
DHCP
  DHCP for IPv6
    「DHCPv6」を参照
DHCPv6
  DHCPv6 サーバ機能のイネーブル化 37-16
  クライアント機能のイネーブル化 37-18
  設定時の注意事項 37-15
  説明 37-6
  デフォルト設定 37-15
DHCP オブジェクト トラッキング、プライマリ インターフェイスの設定 42-11
DHCP オプション 82
  回線 ID サブオプション 20-5
  概要 20-3
  設定時の注意事項 20-8
  デフォルト設定 20-8
  転送アドレス、指定 20-10
  パケット形式、サブオプション
    回線 ID 20-5
    リモート ID 20-5
  表示 20-15
  ヘルパー アドレス 20-10
  リモート ID サブオプション 20-5
DHCP サーバによるポートベース アドレスの割り当て
  イネーブル化 20-17
  設定時の注意事項 20-16
  説明 20-16
  デフォルト設定 20-16
  表示 20-19
  予約アドレス 20-17
DHCP スヌーピング
  エッジ スイッチからの信頼できないパケットの取得 20-3, 20-12
  オプション 82 データ挿入 20-3
  信頼できないインターフェイス 20-2
  信頼できないメッセージ 20-2
  信頼できるインターフェイス 20-2
  設定時の注意事項 20-8
  デフォルト設定 20-8
  バインディング データベース
    「DCHP スヌーピング バインディング データベース」を参照
  バインディング テーブルの表示 20-15
  プライベート VLAN 20-14
  メッセージ交換プロセス 20-4
DHCP スヌーピング バインディング データベース
  イネーブル化 20-14
  エージェント統計情報の消去 20-15
  エントリ 20-6
  削除
    データベース エージェント 20-15
    バインディング 20-15
    バインディング ファイル 20-15
  設定 20-14
  設定時の注意事項 20-9
  説明 20-6
  データベースの更新 20-15
  デフォルト設定 20-8
  バインディング 20-6
  バインディング エントリ、表示 20-15
  バインディングの追加 20-14
  バインディング ファイル
    形式 20-7
    場所 20-6
  表示 20-15
    ステータスと統計情報 20-15
    バインディング エントリ 20-15
  リセット
    タイムアウト値 20-15
    遅延値 20-15
DHCP スヌーピング バインディング テーブル
  「DCHP スヌーピング バインディング データベース」を参照
DHCP バインディング データベース

「DCHP スヌーピング バインディング データベース」を参照
DHCP バインディング テーブル
「DCHP スヌーピング バインディング データベース」を参照
DHCP ベースの自動設定
BOOTP との関係 3-3
概要 3-3
クライアント要求メッセージの交換 3-4
サポート 1-4
設定
DNS 3-8
TFTP サーバ 3-7
クライアント側 3-3
サーバ側 3-6
リレー デバイス 3-8
リース オプション
IP アドレス情報 3-6
コンフィギュレーション ファイルの受信 3-7
リレーのサポート 1-4, 1-11
例 3-10
DHCP ベースの自動設定とイメージ アップデート
概要 3-5 ～ 3-6
設定 3-12 ～ 3-15
DHCP、リレー エージェントのイネーブル化 20-10
DiffServ コード ポイント
「DSCP」を参照
Diffusing アップデート アルゴリズム（DUAL） 36-38
distribute-list コマンド 36-114
DNS
DHCP ベースの自動設定 3-8
IPv6 37-4
概要 5-15
サポート 1-4
設定 5-16
設定の表示 5-17
デフォルト設定 5-16
DNS ベースの SSM マッピング 44-20, 44-22
DoM
サポートされているトランシーバの表示 10-32
Dos 攻撃、回避 33-1
dot1q-tunnel スイッチポート モード 12-16
DRP
IPv6 37-4
設定 37-12
説明 37-4
DSCP
値 34-6
急送型転送 34-9
クラス セレクタ 34-9
デフォルト サービス 34-9
分類 34-9
保証型転送 34-9
DUAL 有限状態マシン、EIGRP 36-38
Dynamic Host Configuration Protocol
「DHCP ベースの自動設定」を参照

E

EBGP 36-46
EEM 3.2 31-5
EIGRP
インターフェイス パラメータ、設定 36-41
コンポーネント 36-38
サポート 1-11
スタブ ルーティング 36-43
設定 36-40
定義 36-38
デフォルト設定 36-39
認証 36-42
モニタリング 36-45
EIGRP IPv6 37-7
elin ロケーション 25-3
E-LMI
CE デバイスの設定 43-51, 43-53
OAM マネージャ 43-46
PE デバイスの設定 43-51, 43-52
イネーブル化 43-51

情報 43-46
設定時の注意事項 43-48
定義 43-46
デフォルト設定 43-47
モニタリング 43-53
Enhanced IGRP
「EIGRP」を参照
ENI
設定 10-18
説明 10-2
プロトコル制御パケット 33-1
EtherChannel
802.3ad、説明 35-6
LACP
システム プライオリティ 35-20
ステータスの表示 35-22
説明 35-6
他の機能との相互作用 35-7
ポート プライオリティ 35-21
ホットスタンバイ ポート 35-19
モード 35-6
PAgP
Catalyst 1900 との互換性 35-18
学習方式およびプライオリティの設定 35-18
サポート 1-2
集約ポート ラーナー 35-18
ステータスの表示 35-22
説明 35-4
他の機能との相互作用 35-5
モード 35-5
サポート 1-2
自動作成 35-4, 35-6
ステータスの表示 35-22
設定
レイヤ 2 インターフェイス 35-12
レイヤ 3 物理インターフェイス 35-15
レイヤ 3 ポートチャネル論理インターフェイス 35-14
設定時の注意事項 35-10
説明 35-2
相互作用
STP 35-10
VLAN 35-11
チャネル グループ
番号付け 35-3
物理インターフェイスと論理インターフェイスのバインド 35-3
デフォルト設定 35-10
転送方式 35-7, 35-17
ポート グループ 10-7
ポートチャネル インターフェイス
説明 35-3
番号付け 35-3
レイヤ 3 インターフェイス 36-3
ロード ジランシング 35-7, 35-17
論理インターフェイス、説明 35-3
EtherChannel ガード
イネーブル化 17-10
説明 17-4
ディセーブル化 17-11
Ethernet Link Management Interface
「E-LMI」を参照
Ethernet Virtual Connection
「EVC」を参照
EUI 37-3
EVC
CFM ドメイン 43-46
設定 43-48
Extended Universal Identifier
「EUI」を参照
Extensible Authentication Protocol over LAN 9-1

F

Fa0 ポート
「イーサネット管理ポート」を参照
fastethernet0 ポート
「イーサネット管理ポート」を参照

FIB 36-101
Flex Link
VLAN 19-2
VLAN ロード バランシングの設定 19-12
設定 19-10
設定時の注意事項 19-9
説明 19-1
デフォルト設定 19-8
モニタリング 19-15
優先 VLAN の設定 19-13
リンク ロード バランシング 19-2
Flex Link マルチキャスト高速コンバージェンス 19-3
FTP
MIB ファイルへのアクセス A-3
イメージ ファイル
アップロード B-32
サーバの準備 B-29
ダウンロード B-30
古いイメージの削除 B-32
コンフィギュレーション ファイル
アップロード B-14
概要 B-12
サーバの準備 B-13
ダウンロード B-13

G

get-bulk-request 動作 30-3
get-next-request 動作 30-3, 30-5
get-request 動作 30-3, 30-4, 30-5
get-response 動作 30-4

H

hello タイム
MSTP 16-24
STP 15-22
HP OpenView 1-4
HSRP
ICMP リダイレクト メッセージのサポート 40-12
オブジェクト トラッキング 42-7
概要 40-1
コマンド スイッチの冗長性 1-6
設定 40-5
設定時の注意事項 40-6
タイマー 40-11
定義 40-1
デフォルト設定 40-5
トラッキング 40-8
認証ストリング 40-11
プライオリティ 40-8
モニタリング 40-12
ルーティングの冗長性 1-11
HTTP（S）、IPv6 37-8

I

IBPG 36-46
ICMP
IPv6 37-4
time-to-live-exceeded メッセージ 46-15
traceroute 46-15
サポート 1-11
到達不能と ACL 32-21
到達不能メッセージ 32-19
到達不能メッセージと IPv6 39-4
リダイレクト メッセージ 36-11
ICMP PING
概要 46-10
実行 46-10
ICMP Router Discovery Protocol
「IRDP」を参照
ICMPv6 37-4
ICMP エコー動作
IP SLA 41-11
設定 41-11
IDS アプライアンス
入力 RSPAN 27-21

入力 SPAN 27-14
IEEE 802.1ag 43-2
IEEE 802.1D
「STP」を参照
IEEE 802.1Q
カプセル化 12-15
設定に関する制限事項 12-16
その他の機能を含むトンネル ポート 14-6
タグなしトラフィック用ネイティブ VLAN 12-20
トランク ポート 10-4
トンネリング
説明 14-2
他の機能との互換性 14-6
デフォルト 14-4
IEEE 802.1s
「MSTP」を参照
IEEE 802.1w
「RSTP」を参照
IEEE 802.1x
「ポートベース認証」を参照
IEEE 802.1 トンネリングによる ISL トランキング 14-5
IEEE 802.3ad
「EtherChannel」を参照
IEEE 802.3ah イーサネット OAM ディスカバリ 43-1
IEEE 802.3Z フロー制御 10-24
ifIndex 値、SNMP 30-6
IFS 1-4
IGMP
Join メッセージ 22-3
概要 44-2
キャッシュ エントリの削除 44-49
クエリー 22-4
グループの表示 44-49
グループへのアクセスの制御 44-41
高速スイッチング 44-45
サポート 1-3
サポート対象バージョン 22-2
スイッチの設定
グループのメンバー 44-40
スタティックに接続されたメンバー 44-44
設定可能な Leave タイマー、説明 22-6
設定可能な Leave タイマー、手順 22-10
脱退処理、イネーブル化 22-10, 38-9
デフォルト設定 44-39
バージョン 1
説明 44-3
バージョン 2 への変更 44-42
バージョン 2
クエリー タイムアウト 44-43
グループのプルーニング 44-44
最大クエリー応答時間 44-44
説明 44-3
バージョン 1 への変更 44-42
フラッディングされたマルチキャスト トラフィック
インターフェイスでのディセーブル化 22-13
クエリー請求 22-12
グローバル Leave 22-12
フラッディング時間の制御 22-11
フラッディング モードからの回復 22-12
ホストクエリー インターバル、変更 44-42
マルチキャスト グループからの脱退 22-5
マルチキャスト グループへの加入 22-3
マルチキャストの到達可能性 44-40
レポート抑制
説明 22-6
ディセーブル化 22-15, 38-11
IGMP Leave タイマー、設定 22-10
IGMP グループ
最大数の設定 22-28
フィルタリングの設定 22-29
IGMP スヌーピング
VLAN 設定 22-8
アドレスのエイリアス 22-2
イネーブル化とディセーブル化 22-7, 38-6
クエリア
設定 22-13
設定時の注意事項 22-13
グローバル コンフィギュレーション 22-7

サポート 1-3
サポート対象バージョン 22-2
設定 22-7
即時脱退 22-6
定義 22-1
デフォルト設定 22-7, 38-5, 38-6
モニタリング 22-15, 38-12
IGMP スロットリング
設定 22-29
説明 22-26
デフォルト設定 22-26
表示 22-30
IGMP の設定可能な Leave タイマー 22-6
IGMP フィルタリング
サポート 1-3
設定 22-27
説明 22-25
デフォルト設定 22-26
モニタリング 22-31
IGMP プロファイル
コンフィギュレーション モード 22-27
設定 22-27
適用 22-28
IGMP ヘルパー 44-6
IGP 36-25
interfaces range macro コマンド 10-11
interface コマンド 10-9
Interior Gateway Protocol
「IGP」を参照
Intermediate System-to-Intermediate System
「IS-IS」を参照
IP ACL
QoS 分類 34-11
暗黙の拒否 32-9, 32-14
名前付き 32-14
マスクの省略 32-9
未定義 32-20
ip cef distributed コマンド 36-102
ip igmp profile コマンド 22-27
IP precedence
値 34-6
分類 34-9
IP SLA
CFM エンドポイント ディスカバリ 43-20
CFM の PING またはジッタの手動設定 43-18
ICMP エコー動作 41-11
SNMP サポート 41-2
UDP ジッタ動作 41-8
応答時間 41-5
オブジェクト トラッキング 42-9
オブジェクト トラッキングの設定 42-9
コントロール プロトコル 41-4
サポート対象のメトリック 41-2
しきい値のモニタリング 41-6
スケジューリング 41-5
設定時の注意事項 41-7
追跡オブジェクト モニタリング エージェント、設定 42-11
追跡ステート 42-9
定義 41-1
デフォルト設定 41-6
動作 41-3
到達可能性トラッキング 42-9
特長 41-2
ネットワーク パフォーマンスの測定 41-3
複数動作スケジューリング 41-5
モニタリング 41-13
レスポンダ
イネーブル化 41-8
説明 41-4
IP traceroute
概要 46-15
実行 46-15
IPv4 ACL
インターフェイスへの適用 32-19
拡張、作成 32-10
名前付き 32-14
標準、作成 32-9

IPv6
ACL
一致条件 39-3
サポート対象 39-2
制限事項 39-3
表示 39-8
ポート 39-2
優先順位 39-2
ルータ 39-2
CEFv6 37-19
Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 37-7
ルータ ID 37-7
ICMP 37-4
OSPF 37-7
SDM テンプレート 7-2, 38-1, 39-1
アドレス 37-2
アドレスの形式 37-2
アドレスの割り当て 37-10
アプリケーション 37-5
機能の制限事項 37-9
近隣探索 37-4
サポートされていない機能 37-8
サポート対象の機能 37-2
自動設定 37-5
スイッチの制限事項 37-9
スタティック ルートの概要 37-6
ステートレス自動設定 37-5
定義 37-1
デフォルト設定 37-10
デフォルト ルータ プリファレンス（DRP） 37-4
パス MTU ディカバリ 37-4
フォワーディング 37-10
IPv6 トラフィック、フィルタリング 39-3
IP アドレス
128 ビット 37-2
IPv6 37-2
IP ルーティング 36-4
MAC アドレスとの対応付け 36-8
クラス 36-5
検出 5-31
デフォルト設定 36-4
モニタリング 36-18
IP サービス レベル契約
「IP SLA」を参照
IP サービス レベル、分析 41-1
IP 情報
デフォルト設定 3-3
割り当て
DHCP ベースの自動設定の使用 3-3
手動 3-15
IP ソース ガード
802.1x 20-23
DHCP スヌーピング 20-20
EtherChannels 20-23
TCAM エントリ 20-23
VRF 20-23
イネーブル化 20-23, 20-24
スタティック バインディング
削除 20-24
追加 20-23, 20-24
スタティック ホスト 20-24
設定時の注意事項 20-22
説明 20-20
送信元 IP アドレスのフィルタリング 20-20
送信元の IP アドレスおよび MAC アドレスのフィルタリング 20-21
ディセーブル化 20-24
デフォルト設定 20-22
トランク インターフェイス 20-22
バインディング設定
自動 20-20
手動 20-20
バインディング テーブル 20-20
表示
設定 20-30
バインディング 20-30
フィルタリング

送信元 IP アドレス 20-20
送信元の IP アドレスおよび MAC アドレス 20-21
プライベート VLAN 20-23
ポート セキュリティ 20-23
ルーテッド ポート 20-22
IP ダイレクト ブロードキャスト 36-14
IP パケット、分類 34-6
IP ブロードキャスト アドレス 36-16
IP プロトコル
ルーティング 1-11
IP ポート セキュリティ、スタティック ホストの
PVLAN ホスト ポート 20-28
レイヤ 2 アクセス ポート 20-24
IP マルチキャスト ルーティング
IGMP スヌーピング 22-1
MBONE
sdr キャッシュ エントリの削除 44-49
sdr キャッシュ エントリの存在期間の制限 44-46
sdr キャッシュの表示 44-50
sdr リスナー サポート機能のイネーブル化 44-46
Session Directory（sdr）ツール、説明 44-45
会議セッション アナウンスメント用の SAP パケット 44-45
説明 44-45
PIMv1 と PIMv2 の相互運用性 44-10
Reverse Path Forwarding（RPF） 44-7
RP
PIMv2 BSR の設定 44-30
自動 RP および BSR の使用 44-34
自動 RP の設定 44-26
手動による割り当て 44-24
マッピング情報のモニタリング 44-35
アドレス
すべてのシステム 44-2
すべてのマルチキャスト ルータ 44-3
ホスト グループ アドレス範囲 44-2
イネーブル化
PIM モード 44-13
マルチキャスト転送 44-12
管理の有効範囲付き境界、説明 44-47
グループ /RP マッピング
BSR 44-7
自動 RP 44-6
シスコの実装 44-1
自動 RP
BSR との併用 44-34
新しいインターネットワーク内での設定 44-26
概要 44-6
既存の sparse（希薄）モード クラウドへの追加 44-26
キャッシュのクリア 44-49
候補 RP スプーフィングの禁止 44-29
設定時の注意事項 44-10
着信 RP アナウンスメント メッセージのフィルタリング 44-29
特長 44-26
問題のある RP への Join メッセージの送信禁止 44-28
設定
IP マルチキャスト境界 44-47
基本的なマルチキャスト ルーティング 44-11
デフォルト設定 44-9
統計情報の表示、システムおよびネットワーク 44-49
ブートストラップ ルータ
IP マルチキャスト境界の定義 44-31
PIM ドメイン境界の定義 44-30
概要 44-7
候補 BSR の設定 44-32
候補 RP の設定 44-33
自動 RP との併用 44-34
設定時の注意事項 44-10
マルチキャスト転送、説明 44-7
モニタリング
デバイスのピアリング 44-50
パケットの速度および損失 44-50
パスのトレース 44-50

ルーティング テーブル
削除 44-49
表示 44-49
「IGMP」も参照
「PIM」を参照
IP ユニキャスト ルーティング
ARP 36-8
EtherChannel レイヤ 3 インターフェイス 36-3
IGP 36-25
IPv6 37-2
IP アドレス指定
クラス 36-5
設定 36-4
IRDP 36-12
MAC アドレスと IP アドレス 36-8
SVI 36-3
UDP 36-15
VLAN 間 36-2
アドレス解決 36-8
イネーブル化 36-19
管理ディスタンス 36-104, 36-115
逆アドレス解決 36-8
クラスレス ルーティング 36-6
再配布 36-106
サブネット ゼロ 36-6
サブネット マスク 36-5
受動インターフェイス 36-113
スーパーネット 36-6
スタティック ルーティング 36-2
スタティック ルートの設定 36-103
設定手順 36-3
ダイナミック ルーティング 36-3
ダイレクト ブロードキャスト 36-14
ディセーブル化 36-19
デフォルト
アドレス指定の設定 36-4
ゲートウェイ 36-11
ネットワーク 36-105
ルーティング 36-2
ルート 36-105
認証鍵 36-116
ブロードキャスト
アドレス 36-16
ストーム 36-14
パケット 36-13
フラッディング 36-17
プロキシ ARP 36-8
ルーテッド ポート 36-3
レイヤ 3 インターフェイス 36-3
レイヤ 3 インターフェイスへの IP アドレスの割り当て 36-5
「BGP」も参照
「EIGRP」も参照
「IS-IS」も参照
「OSPF」も参照
「RIP」も参照
IP ルーティング
イネーブル化 36-19
インターフェイスの接続 10-8
ディセーブル化 36-19
IP ルート、モニタリング 36-117
IRDP
サポート 1-11
設定 36-12
定義 36-12
IS-IS
show コマンド 36-77
アドレス 36-67
エリア ルーティング 36-67
サポート 1-11
システム ルーティング 36-67
デフォルト設定 36-69
モニタリング 36-77
ISO CLNS
clear コマンド 36-77
NET 36-67
NSAP 36-67
OSI 標準 36-67

ダイナミック ルーティング プロトコル 36-67
モニタリング 36-77
ISO IGRP
エリア ルーティング 36-67
システム ルーティング 36-67
ITU-T Y.1731
「Y.1731」を参照

J

Join メッセージ、IGMP 22-3

K

KDC
説明 8-32
「Kerberos」も参照
keepalive コマンド 10-18
Kerberos
KDC 8-32
TGT 8-34
暗号化ソフトウェア イメージ 8-32
サーバ 8-34
サポート 1-8
証明書 8-32
信頼のおけるサード パーティとしてのスイッチ 8-32
設定 8-35
設定例 8-32
説明 8-32
チケット 8-32
動作 8-34
認証の取得
KDC 8-35
境界スイッチ 8-35
ネットワーク サービス 8-35
用語 8-33
レルム 8-34

L

l2protocol-tunnel コマンド 14-19
LACP
「EtherChannel」を参照
レイヤ 2 プロトコル トンネリング 14-15
LDAP 4-2
Lightweight Directory Access Protocol
「LDAP」を参照
LLDP
イネーブル化とディセーブル化
グローバルな 25-4
概要 25-1
サポート対象の TLV 25-2
設定 25-3
デフォルト設定 25-3
特性 25-4
タイマーおよびホールドタイム、設定 25-4
ディセーブル化とイネーブル化
インターフェイス 25-5
モニタリングとメンテナンス 25-7
LLDP-MED
TLV の設定 25-6
概要 25-1, 25-2
サポート対象の TLV 25-2
設定 25-3
モニタリングとメンテナンス 25-7
LLDP メディア拡張
「LLDP-MED」を参照

M

MAC アドレス
ACL 32-27
IP アドレスとの対応付け 36-8
IP 送信元バインディング テーブルでの表示 20-30
VLAN 上での学習のディセーブル化 5-30
VLAN との対応付け 5-20
アドレス テーブルの作成 5-20

エージング タイム 5-21
検出 5-31
スタティック
許可 5-29, 5-30
削除 5-28
追加 5-28
特性 5-27
廃棄 5-29
ダイナミック
学習 5-20
削除 5-22
デフォルト設定 5-21
表示 5-31
MAC アドレス通知、サポート 1-12
MAC アドレステーブル移行更新
設定 19-13
設定時の注意事項 19-9
説明 19-7
デフォルト設定 19-9
モニタリング 19-15
MAC アドレスと VLAN のマッピング 12-24
MAC アドレスの学習、VLAN 上でのディセーブル化 5-30
MAC 拡張アクセス リスト
QoS 用の設定 34-42
作成 32-27
定義 32-27
レイヤ 2 インターフェイスへの適用 32-28
match コマンド、QoS
注意事項 34-43
分類 34-3, 34-8
maximum-paths コマンド 36-54, 36-103
ME 34000EG-2CS スイッチのポリシング機能 33-4
ME 3400E-24TS スイッチのポリシング機能 33-4
ME 3400EG-12CS スイッチのポリシング機能 33-4
media-type コマンド 10-22
MEP
STP 43-5
定義 43-3
MHSRP 40-4
MIB
FTP によるファイルへのアクセス A-3
SNMP との相互作用 30-4
概要 30-1
サポート対象 A-1
ファイルの場所 A-3
MIP
STP 43-5
定義 43-4
MQC
設定手順 34-3
プロセス 34-3
MSDP
dense（稠密）モード領域
SA メッセージの送信 45-16
発信元アドレスの指定 45-17
MSDP 接続および統計情報のクリア 45-18
SA メッセージ
TTL によるデータの制限 45-13
アドバタイズされる送信元の制限 45-9
キャッシュ エントリの削除 45-18
キャッシング 45-6
着信 SA メッセージのフィルタリング 45-14
定義 45-2
ピアからの SA メッセージのフィルタリング 45-10
ピアへの SA メッセージのフィルタリング 45-12
モニタリング 45-18
概要 45-1
加入遅延、定義 45-6
サポート 1-11
送信元情報の制御
スイッチから転送された 45-11
スイッチから発信された 45-8
スイッチで受信した 45-13
デフォルト設定 45-3
特長 45-3

発信元アドレス、変更 45-17
ピア
シャットダウン 45-15
送信元情報の要求 45-8
デフォルトの設定 45-4
ピアリング関係、概要 45-1
モニタリング 45-17
ピア RPF フラッディング 45-2
フィルタリング
着信 SA メッセージ 45-14
ピアからの SA 要求メッセージ 45-10
ピアへの SA メッセージ 45-12
メッシュ グループ
設定 45-15
定義 45-15
MSTP
802.1D との相互運用性
移行プロセスの再起動 16-28
説明 16-9
BPDU ガード
イネーブル化 17-8
説明 17-3
BPDU フィルタリング
イネーブル化 17-9
説明 17-3
CIST、説明 16-3
CIST リージョナル ルート 16-5
CIST ルート 16-5
CST
定義 16-3
リージョン間の動作 16-4
EtherChannel ガード
イネーブル化 17-10
説明 17-4
IEEE 802.1s
実装 16-7
ポート役割命名の変更 16-7
IST
定義 16-3
マスター 16-3
リージョン内の動作 16-3
MST リージョン
CIST 16-3
IST 16-3
サポート対象のスパニングツリー インスタンス 16-2
設定 16-16
説明 16-2
ホップ カウント メカニズム 16-6
PortFast
イネーブル化 17-6
説明 17-2
PortFast 対応インターフェイスのシャットダウン 17-3
VLAN と MST インスタンスのマッピング 16-17
インターフェイス ステート、ブロッキングからフォワーディング 17-2
オプション機能のデフォルト設定 17-6
概要 16-2
拡張システム ID
セカンダリ ルート スイッチへの影響 16-19
予期せぬ動作 16-18
ルート スイッチへの影響 16-18
境界ポート
設定時の注意事項 16-16
説明 16-6
サポート対象のインスタンス 15-11
サポート対象のオプション機能 1-6
ステータスの表示 16-29
ステータス、表示 16-29
設定
hello タイム 16-24
MST リージョン 16-16
高速コンバージェンスのためのリンク タイプ 16-26
最大エージング タイム 16-25
最大ホップ カウント 16-25
スイッチ プライオリティ 16-23
セカンダリ ルート スイッチ 16-19

転送遅延時間 16-24
ネイバー タイプ 16-27
パス コスト 16-22
ポート プライオリティ 16-20
ルート スイッチ 16-18
設定時の注意事項 16-15, 17-6
デフォルト設定 16-15
モード間の相互運用性と互換性 15-11
モードのイネーブル化 16-16
ルート ガード
イネーブル化 17-11
説明 17-4
ルート スイッチ
拡張システム ID の影響 16-18
設定 16-18
予期せぬ動作 16-18
ルート スイッチとしての選択の防止 17-4
ループ ガード
イネーブル化 17-12
説明 17-5
Multicast Source Discovery Protocol
「MSDP」を参照
multicast storm-control コマンド 23-4
Multiple HSRP
「MHSRP」を参照
Multiple VPN Routing/Forwarding、カスタマー エッジ デバイス
「マルチ VRF CE」を参照
MVR
IGMPv3 22-20
アドレスのエイリアス 22-20
インターフェイスの設定 22-22
グローバル パラメータの設定 22-20
サポート 1-3
サンプル アプリケーション 22-17
スイッチ スタック 22-19
設定時の注意事項 22-20
説明 22-17
デフォルト設定 22-19
マルチキャスト TV アプリケーション 22-17
モード 22-21
モニタリング 22-25
MVRoT、注意事項 22-20
MVR over trunk port
「MVRoT」を参照

N

NameSpace Mapper
「NSM」を参照
NEAT
概要 9-10
設定 9-25
NNI
設定 10-18
説明 10-2
プロトコル制御パケット 33-1
no switchport コマンド 10-5
not-so-stubby areas
「NSSA」を参照
no コマンド 2-3
NSAP、ISO IGRP アドレスとして 36-67
NSF 認識
BGP 36-50
EIGRP 36-40
IS-IS 36-69
OSPF 36-28
NSM 4-3
NSSA、OSPF 36-33
NTP
アクセスの制限
アクセス グループの作成 5-8
インターフェイス単位での NTP サービスのディセーブル化 5-10
アソシエーション
サーバ 5-5
定義 5-2
認証 5-4

ピア 5-5
ブロードキャスト メッセージのイネーブル化 5-7
概要 5-2
サポート 1-4
時刻
サービス 5-2
同期化 5-2
ストラタム 5-2
設定の表示 5-11
送信元の IP アドレス、設定 5-10
デバイスの同期化 5-5
デフォルト設定 5-4

O

OAM
機能 43-32
クライアント 43-31
サブレイヤ 43-31
OAM PDU 43-33
OAM プロトコル データ ユニット 43-31
OAM マネージャ
CFM 43-47
CFM およびイーサネット OAM 43-54
E-LMI 43-46
設定 43-48, 43-55
設定時の注意事項 43-48
モニタリング 43-53
用途 43-46
OBFL
設定 46-22
説明 46-22
表示 46-23
Open Shortest Path First
「OSPF」を参照
OSPF
IPv6 37-7
LSA グループ ペーシング 36-36
インターフェイス パラメータ、設定 36-29
エリア パラメータ、設定 36-33
仮想リンク 36-34
経路集約 36-34
サポート 1-11
設定 36-28
説明 36-25
デフォルト設定
設定 36-27
メトリック 36-35
ルート 36-34
ネットワーク タイプ、設定 36-32
モニタリング 36-37
ルータ ID 36-36

P

PAgP
「EtherChannel」を参照
レイヤ 2 プロトコル トンネリング 14-15
PBR
イネーブル化 36-111
定義 36-109
ポリシーベース ルーティングの の高速スイッチング 36-113
ローカル ポリシーベース ルーティング 36-113
PE/CE ルーティング、設定 36-96
Per-VLAN Spanning-Tree Plus
「PVST+」を参照
PIM
dense（稠密）モード
RPF チェック 44-8
概要 44-4
ランデブー ポイント（RP）、説明 44-5
sparse（希薄）モード
Join メッセージと共有ツリー 44-4
RPF チェック 44-8
概要 44-4
プルーニング メッセージ 44-5

SPT、使用の延期 44-37
概要 44-3
共有ツリーと送信元ツリー、概要 44-36
サポート 1-1, 1-11
スタブ ルーティング
イネーブル化 44-14
概要 44-5
設定時の注意事項 44-13
デフォルト設定 44-9
ネイバーの表示 44-49
バージョン
v2 の改善点 44-4
相互運用性 44-10
相互運用性の問題点に関するトラブルシューティング 44-35
モードのイネーブル化 44-13
ルータクエリー メッセージ インターバル、変更 44-38
PING
概要 46-10
実行 46-10
police aggregate コマンド 34-57
policer aggregate コマンド 34-54
police コマンド、個別のポリシング機能 34-48, 34-63
policy-map コマンド 34-3
PortFast
イネーブル化 17-6
サポート 1-6
説明 17-2
priority コマンド 34-21
QoS スケジューリング 34-28
完全プライオリティ キューイング 34-32
完全プライオリティ キューイングの設定 34-71
Protocol Independent Multicast プロトコル
「PIM」を参照
PVST+
802.1Q トランクの相互運用性 15-11
サポート対象のインスタンス 15-11
説明 15-10

Q

QinQ
「IEEE 802.1Q トンネリング」を参照
QoS
CBWFQ 34-30
CBWFQ、設定 34-67
CPU 生成トラフィック
QoS グループ番号の設定 34-13
キュー制限の設定 34-75
出力のリマーキング 34-6
出力ポリシーの分類基準の設定 34-6
IP パケットの分類 34-6
match コマンド 34-8
MQC 34-1
WTD 34-34
親子階層 34-14, 34-29
概要 34-1
完全プライオリティ キューイング 34-32
基本的なモデル 34-2
キュー サイズ 34-34
クラスベース シェーピング、説明 34-29
クラス マップ、設定 34-43
クラス マップ、設定時の注意事項 34-43
サポート 1-9
サポート対象のテーブル マップ 34-16
事前設定 34-37
集約ポリシング機能 34-19
出力ポリシー マップ
設定 34-66
説明 34-5
初期設定の例 34-85
スケジューリング 34-27
CBWFQ 34-28
トラフィック シェーピング 34-28
プライオリティ キューイング 34-28
設定
IP ACL 34-39
IP ACL による分類 34-39

MAC ACL 34-42
WTD 34-75, 34-76
完全プライオリティ キューイング 34-71
キュー サイズ 34-34
クラスベース シェーピング 34-69
クラス マップ 34-43, 34-44
個別のポリシング 34-48, 34-63
個別のポリシング機能 34-49
サービス ポリシー 34-47
集約ポリシング機能 34-54
出力ポリシー マップ 34-65
テーブル マップ 34-46
プライオリティ キュー 34-71
ポート シェーピング 34-70
マーキングを含む入力ポリシー マップ 34-58
無条件のプライオリティ ポリシング 34-73
要件 34-37
設定時の注意事項
CBWFQ 34-67
WTD 34-75
一般 34-37
クラスベース シェーピング 34-68
クラス マップ 34-43
個別のポリシング機能 34-48
集約ポリシング機能 34-54
出力ポリシー マップ 34-65
入力ポリシー マップ 34-47
マーキング 34-58
無条件のプライオリティ ポリシング 34-73
設定例
カスタマーの追加 34-87
キューイングパラメータまたはスケジューリング パラメータの変更 34-88
クラスの追加または削除 34-90
設定済み動作の追加または削除 34-89
分類基準の追加または削除 34-87
テーブル マップ 34-15
テスト 34-84
デフォルト設定 34-37
トラフィック シェーピング、説明 34-28
入力ポリシー マップ
設定 34-47
説明 34-5
パケット分類 34-2
パケット ポリシング 34-2
パケット マーキング 34-22
輻輳回避 34-2, 34-34
輻輳管理 34-2, 34-27
プライオリティ ポリシング、説明 34-21
分類
ACL 検索 34-11
CoS 値に基づく 34-8
DSCP に基づく 34-9
IP precedence に基づく 34-9
QoS グループに基づく 34-12
VLAN ID に基づく 34-13, 34-60
基準 34-6
クラス マップ、説明 34-7
比較 34-11
フレームとパケット 34-7
ポリシー マップ、説明 34-17
ポート シェーピング、説明 34-29
ポート単位 VLAN 単位 の階層型ポリシー マップ
説明 34-13
ポリシー マップ
インターフェイスへの付加 34-20
統計情報の表示 34-84
付加 34-47
ポリシング
個別 34-17
集約 34-19
説明 34-2, 34-16
プライオリティ 34-21
ポリシング機能
設定 34-50, 34-56, 34-73
説明 34-16
ポリシングを含むプライオリティ マーキング、説明 34-32
34-2

無条件のプライオリティ ポリシング 34-32
レイヤ 2 パケットの分類 34-6
レイヤ 3 パケットの分類 34-6
QoS グループ
説明 34-5, 34-12
分類 34-12, 34-13, 34-60
QoS 情報、表示 34-83
Quality Of Service
「QoS」を参照
queue-limit コマンド、QoS 34-34, 34-35, 34-75

R

RADIUS
AAA サーバ グループの定義 8-25
アトリビュート
ベンダ固有 8-29
ベンダ独自仕様 8-30
概要 8-18
サーバの特定 8-20
サーバのロード バランシング 8-31
サポート 1-8
推奨するネットワーク環境 8-18
設定
アカウンティング 8-28
通信、グローバル 8-21, 8-29
通信、サーバ単位 8-20, 8-21
認可 8-27
認証 8-23
複数の UDP ポート 8-21
設定の表示 8-32
デフォルト設定 8-20
動作 8-19
方式リスト、定義 8-20
ユーザがアクセスするサービスの追跡 8-28
ユーザへのサービスの制限 8-27
Rapid Per-VLAN Spanning-Tree plus
「Rapid PVST+」を参照
Rapid PVST+
802.1Q トランクの相互運用性 15-11
サポート対象のインスタンス 15-11
説明 15-10
RARP 36-8
RCP
イメージ ファイル
アップロード B-37
サーバの準備 B-34
ダウンロード B-35
古いイメージの削除 B-37
コンフィギュレーション ファイル
アップロード B-18
概要 B-15
サーバの準備 B-16
ダウンロード B-17
Remote Authentication Dial-In User Service
「RADIUS」を参照
REP
SNMP トラップ、設定 18-14
STP 18-6
VLAN のロード バランシング 18-4
VLAN ブロッキング 18-13
VLAN ロード バランシングのトリガー 18-5
インターフェイスの設定 18-10
エージング タイマー 18-8
オープン セグメント 18-2
管理 VLAN 18-9
管理 VLAN、設定 18-9
コンバージェンス 18-4
サポート対象のインターフェイス 18-1
手動プリエンプション、設定 18-14
セカンダリ エッジ ポート 18-4
セグメント 18-1
特性 18-2
設定時の注意事項 18-7
デフォルト設定 18-7
ネイバーのオフセット番号 18-4
プライマリ エッジ ポート 18-4
プリエンプション遅延時間 18-5

ポート 18-6
モニタリング 18-15
リンク完全性の検証 18-3
リング セグメント 18-2
RFC
1112、IP マルチキャストと IGMP 22-2
1157、SNMPv1 30-2
1305、NTP 5-2
1587、NSSA 36-26
1757、RMON 28-2
1901、SNMPv2C 30-2
1902 ～ 1907、SNMPv2 30-2
2236、IP マルチキャストと IGMP 22-2
2273 ～ 2275、SNMPv3 30-2
2475、DSCP 34-10
2597、AF Per-Hop Behavior 34-10
2598、EF 34-10
RIP
IPv6 37-6
アドバタイズメント 36-20
サポート 1-11
サマリー アドレス 36-24
設定 36-21
説明 36-20
デフォルト設定 36-20
認証 36-23
ホップ カウント 36-20
RMON
アラームおよびイベントのイネーブル化 28-3
概要 28-1
サポート 1-12
サポート対象のグループ 28-2
ステータスの表示 28-6
デフォルト設定 28-3
統計情報
グループ イーサネットの収集 28-5
グループ履歴の収集 28-5
route-map コマンド 36-112
Routing Information Protocol
「RIP」を参照
RSPAN
VLAN ベース 27-6
宛先ポート 27-7
概要 1-12, 27-1
受信トラフィック 27-4
ステータスの表示 27-24
セッション
作成 27-18
送信元トラフィックの特定の VLAN への制限 27-23
定義 27-3
入力トラフィックがイネーブル 27-21
モニタ対象ポートの指定 27-18
セッションの制限 27-10
設定時の注意事項 27-17
送信トラフィック 27-5
送信元ポート 27-5
他の機能との相互作用 27-8
定義 27-2
デフォルト設定 27-9
特性 27-8
モニタ対象ポート 27-5
モニタリング ポート 27-7
RSPAN VLAN、UNI VLAN 12-13
RSTP
802.1D との相互運用性
移行プロセスの再起動 16-28
説明 16-9
トポロジの変更 16-14
BPDU
処理 16-13
フォーマット 16-12
「MSTP」も参照
アクティブ トポロジ 16-10
概要 16-9
高速コンバージェンス
エッジ ポートと PortFast 16-10
説明 16-10

ポイントツーポイント リンク 16-10, 16-26
ルート ポート 16-10
指定スイッチ、定義 16-10
指定ポート、定義 16-10
提案合意ハンドシェイク プロセス 16-10
ポートの役割
説明 16-9
同期化 16-12
ルート ポート、定義 16-9

S

SCP
SSH 8-42
設定 8-42
「SCP」を参照
SDM
説明 7-1
テンプレート
数 7-1
設定 7-5
SDM テンプレート
設定 7-3
設定時の注意事項 7-4
タイプ 7-1
デフォルト 7-1
デュアル IPv4/IPv6 7-2
レイヤ 2 7-1
Secure Copy Protocol
service-policy コマンド
使用 34-47
注意事項 34-66
ポリシー マップの付加 34-4
set-request 動作 30-5
set コマンド
QoS マーキング 34-22
注意事項 34-58
SFP
ステータスのモニタリング 1-12, 10-32, 46-9
ステータス、表示 1-12
セキュリティと識別 46-8
shape average コマンド、QoS 34-28, 34-29, 34-68
show access-lists hw-summary コマンド 32-21
show cdp traffic コマンド 24-5
show configuration コマンド 10-26
show forward コマンド 46-19
show interfaces switchport 19-4
show interfaces コマンド 10-21, 10-26
show l2protocol コマンド 14-20, 14-21, 14-22
show lldp traffic コマンド 25-8
show platform forward コマンド 46-19
show running-config コマンド
ACL の表示 32-19, 32-20, 32-32, 32-34
インターフェイスの説明 10-26
show コマンドおよび more コマンドの出力、フィルタリング 2-8
shutdown コマンド、インターフェイス 10-33
SMNP トラップ、CFM 43-6
SNAP 24-1
SNMP
CPU しきい値通知の設定 30-17
ifIndex 値 30-6
IP SLA 41-2
MIB
サポート対象 A-1
場所 A-3
MIB 変数へのアクセス 30-4
NMS への syslog メッセージの制限 29-10
TFTP サーバのアクセス制限 30-18
インフォーム
trap キーワード 30-13
イネーブル化 30-17
説明 30-5
ディセーブル化 30-17
トラップとの違い 30-5
エージェント
説明 30-4
ディセーブル化 30-8

エンジン ID 30-8
概要 30-1, 30-4
グループ 30-8, 30-10
コミュニティ ストリング
概要 30-4
設定 30-9
サポート対象のバージョン 30-2
システム コンタクトおよびロケーション 30-18
ステータス、表示 30-24
セキュリティ レベル 30-3
設定例 30-22
帯域内管理 1-5
通知 30-5
デフォルト設定 30-7
トラップ
MACアドレス通知のイネーブル化 5-22, 5-24, 5-26
イネーブル化 30-13
インフォームとの違い 30-5
概要 30-1, 30-5
説明 30-4, 30-5
タイプ 30-14
ディセーブル化 30-17
トラップ マネージャ、設定 30-15
認証レベル 30-12
ホスト 30-8
マネージャの機能 1-4, 30-3
ユーザ 30-8, 30-10
SNMPv1 30-2
SNMPv2C 30-2
SNMPv3 30-3
SNMP と syslog、IPv6 37-7
SNMP トラップ
REP 18-14
Source-Specific Multicast
「SSM」を参照
SPAN
VLAN ベース 27-6
宛先ポート 27-7
概要 1-12, 27-1
受信トラフィック 27-4
ステータスの表示 27-24
セッション
宛先（モニタリング）ポートの削除 27-13
作成 27-11
送信元トラフィックの特定の VLAN への制限 27-16
定義 27-3
入力転送の設定 27-15, 27-22
入力トラフィックがイネーブル 27-14
モニタ対象ポートの指定 27-11
セッションの制限 27-10
設定時の注意事項 27-10
送信トラフィック 27-5
送信元ポート 27-5
他の機能との相互作用 27-8
デフォルト設定 27-9
トラフィック 27-4
ポート、制限 23-11
モニタ対象ポート 27-5
モニタリング ポート 27-7
SRR、サポート 1-10
SSH
暗号化ソフトウェア イメージ 8-37
暗号化方式 8-38
設定 8-39
説明 1-5, 8-38
ユーザ認証方式、サポート対象 8-38
SSM
CGMP の制限事項 44-17
IGMPv3 44-15
IGMPv3 ホスト シグナリング 44-17
IGMP スヌーピング 44-17
IP アドレス範囲 44-16
PIM 44-15
アドレス管理上の制限 44-17
インターネット標準マルチキャストとの違い 44-15
コンポーネント 44-15

状態の維持に関する制限事項 44-17
設定 44-15, 44-18
設定時の注意事項 44-17
動作 44-16
モニタリング 44-18
SSM マッピング
DNS ベース 44-20, 44-22
概要 44-19
スタティック 44-20, 44-21
スタティック トラフィック転送 44-23
制限 44-19
設定 44-18, 44-21
設定時の注意事項 44-19
定義 44-18
モニタリング 44-23
standby ip コマンド 40-6
STP
802.1Q トランクでの制約 15-11
BPDU ガード
イネーブル化 17-8
説明 17-3
ディセーブル化 17-9
BPDU フィルタリング
イネーブル化 17-9
説明 17-3
ディセーブル化 17-10
BPDU メッセージ交換 15-3
EtherChannel ガード
イネーブル化 17-10
説明 17-4
ディセーブル化 17-11
IEEE 802.1D とブリッジ ID 15-4
IEEE 802.1D とマルチキャスト アドレス 15-9
IEEE 802.1t と VLAN ID 15-4
PortFast
イネーブル化 17-6
説明 17-2
REP 18-6
インターフェイス ステート
概要 15-5
学習 15-7
ディセーブル化 15-8
フォワーディング 15-6, 15-7
ブロッキング 15-6
リスニング 15-7
インターフェイス ステート、ブロッキングからフォワーディング 17-2
オプション機能のデフォルト設定 17-6
下位 BPDU 15-3
概要 15-2
カウンタ、クリア 15-25
拡張システム ID
概要 15-4
セカンダリ ルート スイッチに対する影響 15-18
予期せぬ動作 15-17
ルート スイッチへの影響 15-16
キープアライブ メッセージ 15-3
サポート対象のインスタンス 15-11
サポート対象のオプション機能 1-6
サポート対象の機能 1-6
サポート対象のプロトコル 15-10
サポート対象のモード 15-10
指定スイッチ、定義 15-4
指定ポート、定義 15-4
冗長接続 15-9
ステータスの表示 15-24
ステータス、表示 15-24
設定
hello タイム 15-22
最大エージング タイム 15-24
スイッチ プライオリティ 15-21
スパニングツリー モード 15-14
セカンダリ ルート スイッチ 15-18
転送遅延時間 15-23
パス コスト 15-20
ポート プライオリティ 15-18
ルート スイッチ 15-16

設定時の注意事項 15-13, 17-6
タイマー、説明 15-22
ディセーブル化 15-16
デフォルト設定 15-12
パス コスト 12-22, 12-23
ポート プライオリティ 12-21
マルチキャスト アドレス、影響 15-9
モード間の相互運用性と互換性 15-11
優位 BPDU 15-3
ルート ガード
イネーブル化 17-11
説明 17-4
ルート スイッチ
拡張システム ID の影響 15-4, 15-16
設定 15-16
選択 15-3
予期せぬ動作 15-17
ルート スイッチとしての選択の防止 17-4
ルート ポート、定義 15-4
ループ ガード
イネーブル化 17-12
説明 17-5
レイヤ 2 プロトコル トンネリング 14-13
ロード シェアリング
概要 12-20
パス コストの使用 12-22
ポート プライオリティの使用 12-21
SunNet Manager 1-4
SVI
IP ユニキャスト ルーティング 36-3
VLAN 間ルーティング 12-2
VLAN の接続 10-8
定義 10-6
ルータ ACL 32-4
S-VLAN 14-8
switchport backup interface 19-4, 19-5
switchport block multicast コマンド 23-8
switchport block unicast コマンド 23-8
switchport mode dot1q-tunnel コマンド 14-7
switchport protected コマンド 23-6
switchport コマンド 10-16
syslog
「システム メッセージ ロギング」を参照
System-to-Intermediate System Protocol
「IS-IS」を参照

T

TACACS+
アカウンティング、定義 8-11
概要 8-10
サーバの特定 8-13
サポート 1-8
設定
アカウンティング 8-16
認可 8-16
認証鍵 8-13
ログイン認証 8-14
設定の表示 8-17
デフォルト設定 8-13
動作 8-12
認可、定義 8-11
認証、定義 8-11
ユーザがアクセスするサービスの追跡 8-16
ユーザへのサービスの制限 8-16
tar ファイル
イメージ ファイル形式 B-24
作成 B-6
抽出 B-7
内容の表示 B-6
TCL スクリプト、組み込みイベント マネージャによる登録と定義 31-7
TDR 1-12
Telnet
管理インターフェイスへのアクセス 2-9
接続数 1-5
パスワードの設定 8-6
Terminal Access Controller Access Control System Plus

「TACACS+」を参照
TFTP
イメージ ファイル
アップロード B-28
サーバの準備 B-26
削除 B-27
ダウンロード B-26
コンフィギュレーション ファイル
アップロード B-12
サーバの準備 B-10
ダウンロード B-11
サーバのアクセス制限 30-18
自動設定の場合 3-7
ベース ディレクトリのコンフィギュレーション ファイル 3-7
TFTP サーバ 1-4
time-range コマンド 32-16
TLV
LLDP 25-2
LLDP-MED 25-2
定義 25-1
traceroute コマンド 46-15
「IP traceroute」も参照
traceroute、レイヤ 2
1 つのポートに複数のデバイス 46-14
ARP 46-14
CDP 46-13
IP アドレスとサブネット 46-14
MAC アドレスと VLAN 46-14
使用上の注意事項 46-13
説明 46-13
ブロードキャスト トラフィック 46-13
マルチキャスト トラフィック 46-14
ユニキャスト トラフィック 46-13

U

UDLD
イネーブル化
インターフェイス単位 26-5
グローバルな 26-5
インターフェイスのリセット 26-6
エコーを用いた検出メカニズム 26-2
概要 26-1
近接データベース 26-2
サポート 1-6
ステータス、表示 26-7
設定時の注意事項 26-4
ディセーブル化
インターフェイス単位 26-5
グローバルな 26-5
光ファイバ インターフェイス 26-5
デフォルト設定 26-4
リンク検出メカニズム 26-1
レイヤ 2 プロトコル トンネリング 14-16
UDLD によりディセーブル化されたインターフェイスのリセット 26-6
UDP
定義 36-15
データグラム 36-17
フォワーディング 36-15
UDP ジッタ、設定 41-9
UDP ジッタ動作、IP SLA 41-8
UDP、設定 36-15
UN-ENI VLAN
定義 12-6
UNI
設定 10-18
説明 10-2
プロトコル制御パケット 33-1
unicast storm control コマンド 23-4
UNI VLAN
RSPAN VLAN 12-13
設定 12-14
設定時の注意事項 12-13
プライベート VLAN 12-13
UNIX syslog サーバ
サポート対象のファシリティ 29-13

デーモンの設定 29-12
メッセージ ロギングの設定 29-12
UNI コミュニティ VLAN 12-6
UNI 独立 VLAN 12-6
UNI、リモート（CFM） 43-47

V

VLAN
RSPAN による送信元トラフィックの制限 27-23
SPAN による送信元トラフィックの制限 27-16
STP と 802.1Q トランク 15-11
SVI による接続 10-8
UNI 12-6
UNI コミュニティ 12-6
UNI 独立 12-6
VLAN 間トラフィック 12-2
拡張範囲 12-1
機能 1-7
サービス プロバイダー ネットワーク内のカスタマー番号 14-3
サポート数 1-7
サポート対象 12-3
図 12-2
スタティックアクセス ポート 12-11
スパニングツリー インスタンス 12-3, 12-9
設定 12-1
設定時の注意事項 12-8
設定時の注意事項、標準範囲 VLAN 12-8
説明 10-3, 12-1
ダイナミック アドレスの有効期間 15-10
追加 12-9
デフォルト設定 12-7
トランク上で許可 12-18
内部 12-9
ネイティブ、設定 12-20
パラメータ 12-3
表示 12-15
標準範囲 12-1, 12-3
変更 12-9
ポート メンバシップ モード 12-4
マルチキャスト 22-17
vlan.dat ファイル 12-3
VLAN 1
最小化 12-19
トランク ポート上でのディセーブル化 12-19
VLAN ACL
「VLAN マップ」を参照
vlan dot1q tag native コマンド 14-5
VLAN ID
検出 5-31
サービス プロバイダー 14-9
VLAN ID 変換
「VLAN マッピング」を参照
VLAN 間ルーティング 1-11, 36-2
VLAN クエリー プロトコル
「VQP」を参照
vlan グローバル コンフィギュレーション コマンド 12-7, 12-9
VLAN コンフィギュレーション モード 2-2
VLAN データベース
VLAN 設定の保存 12-10
VLAN の保存 12-3
VLAN トランク 12-15
VLAN フィルタリングと SPAN 27-6
VLAN ブロッキング、REP 18-13
VLAN マッピング
1 対 1 14-8
1 対 1、設定 14-10
従来の QinQ 14-8
従来の Q-in-Q、設定 14-11
設定 14-10
設定時の注意事項 14-10
説明 14-8
選択的 QinQ 14-8
選択的 Q-in-Q、設定 14-12
タイプ 14-8
デフォルト 14-9

トランク ポート上での設定 14-10
VLAN マップ
ACL および VLAN マップの例 32-32
一般的な使用方法 32-35
サーバへのアクセス拒否の例 32-36
削除 32-34
作成 32-32
サポート 1-9
設定 32-30
設定時の注意事項 32-30
定義 32-2, 32-5
適用 32-34
パケットの拒否および許可 32-32
表示 32-41
ルータ ACL との組み合せ 32-40
ワイヤリング クローゼットの構成例 32-35
VLAN マップ エントリ、順序 32-31
VLAN マネジメント ポリシー サーバ
「VMPS」を参照
VLAN メンバシップ
確認 12-28
モード 12-5
VLAN ループバック
定義 43-42
VLAN ロード バランシング
Flex Link 19-2
Flex Link の設定に関する注意事項 19-9
REP 18-4
トリガー 18-5
VLAN 割り当て（vlan-assignment）の応答、VMPS 12-25
VMPS
VLAN への MAC アドレスのマッピング 12-24
管理 12-29
再確認間隔、変更 12-28
再試行回数、変更 12-29
設定時の注意事項 12-26
設定例 12-30
説明 12-24
ダイナミック ポート メンバシップ
再確認 12-28
説明 12-25
トラブルシューティング 12-30
デフォルト設定 12-26
メンバシップの再確認 12-28
モニタリング 12-29
VPN
サービス プロバイダー ネットワーク内 36-88
フォワーディング 36-90
ルーティングの設定 36-95
ルート 1-19, 36-89
VQP 1-7, 12-24
VRF
定義 36-90
テーブル 1-18, 36-88
VRF テーブル
「VRF」を参照
VRF 認識サービス
ARP 36-93
ftp 36-95
HSRP 36-94
PING 36-93
SNMP 36-93
syslog 36-94
tftp 36-95
traceroute 36-95
設定 36-92
VTP レイヤ 2 プロトコル トンネリング 14-13

W

WTD
サポート 1-10
設定 34-75, 34-76
設定時の注意事項 34-75
説明 34-34

Y

Y.1731
- ETH-AIS
  - イーサネット アラーム 信号機能（ETH-AIS） 43-22
  - 設定 43-24
- ETH-LCK 43-23
  - 設定 43-26
- ETH-RDI 43-23
- 説明 43-21
- デフォルト設定 43-24
- マルチキャスト ETH-LB 43-23
- マルチキャスト イーサネット ループバック 43-29
- 用語 43-22

あ

アカウンティング
- IEEE 802.1x 9-5, 9-23
- RADIUS 8-28
- TACACS+ 8-11, 8-16

アクセス拒否（access-denied）の応答、VMPS 12-25

アクセス グループ
- インターフェイスへの IPv4 ACL の適用 32-19
- レイヤ 2 32-20
- レイヤ 3 32-20

アクセス コントロール エントリ
- 「ACE」を参照

アクセス ポート
- 定義 10-4
- レイヤ 2 プロトコル トンネリング 14-17

アクセス リスト
- 「ACL」を参照

アクティブ トラフィック モニタリング、IP SLA 41-1

アクティブ リンク 19-2, 19-4, 19-5, 19-6

アクティブ ルータ 40-1

アップグレード、CNS による 4-14

アップグレード、ソフトウェア イメージ
- 「ダウンロード」を参照

アップロード
- イメージ ファイル
  - FTP の使用 B-32
  - RCP の使用 B-37
  - TFTP の使用 B-28
  - 準備 B-26, B-29, B-34
  - 目的 B-24
- コンフィギュレーション ファイル
  - FTP の使用 B-14
  - RCP の使用 B-18
  - TFTP の使用 B-12
  - 準備 B-10, B-13, B-16
  - 目的 B-8

宛先 IP アドレスベース転送、EtherChannel 35-8

宛先 MAC アドレス転送、EtherChannel 35-7

宛先アドレス
- IPv6 ACL 39-5

宛先のアドレス、IPv4 ACL 内 32-11

アドバタイズメント
- CDP 24-1
- LLDP 25-1
- RIP 36-20

アトリビュート、RADIUS
- ベンダ固有 8-29
- ベンダ独自仕様 8-30

アドレス
- IPv6 37-2
- MAC アドレス テーブルの表示 5-31
- MAC、検出 5-31
- スタティック
  - 追加と削除 5-27
  - 定義 5-19
- ダイナミック
  - エージング タイムの変更 5-21
  - 学習 5-20
  - 削除 5-22
  - 定義 5-19
  - デフォルトの有効期間 15-9

有効期間の短縮 15-9
マルチキャスト
STP アドレス管理 15-9
グループ アドレス範囲 44-2
アドレス解決 5-31, 36-8
アドレス解決プロトコル
「ARP」を参照
アドレスのエイリアス 22-2
アベイラビリティ、機能 1-6
アラーム、RMON 28-3
暗号化ソフトウェア イメージ
Kerberos 8-32
SSH 8-37
暗号化、パスワードの 8-3
安全なリモート接続 8-38

い

イーサネット OAM 43-32
CFM との相互作用 43-54
CFM による設定 43-54
イネーブル化 43-33, 43-55
設定時の注意事項 43-33
ディスカバリ 43-32
デフォルト設定 43-33
テンプレート 43-39
プロトコル
定義 43-31
モニタリング 43-41
マネージャ 43-1
メッセージ 43-32
リモート障害表示 43-32, 43-38
リモート ループバック 43-32, 43-34
リンク モニタリング 43-32, 43-35
イーサネット OAM プロトコル 43-1
イーサネット OAM プロトコルによる CFM 通知 43-54
イーサネット VLAN
追加 12-9
デフォルト値と範囲 12-8
変更 12-9
イーサネット インフラストラクチャ 43-1
イーサネット管理ポート
TFTP 10-15
サポートされていない機能 10-15
サポート対象の機能 10-15
指定 10-15
設定 10-15
説明 10-6, 10-13
デフォルト設定 10-14
ネットワーク管理 10-6, 10-13
ルーティング 10-14
ルーティング プロトコル 10-14
イーサネット管理ポート、内部
サポートされていない機能 10-15
ルーティング 10-14
ルーティング プロトコル 10-14
イーサネット ターミナル ループバック 34-84
イーサネットの運用、管理および保守
「イーサネット OAM」を参照
イーサネット リモート障害表示（ETH-RDI） 43-23
イーサネット ループバック
特性 43-43
イーサネット ロック信号（ETH-LCK） 43-23
一括統計情報
オブジェクト リスト、設定 30-19
オブジェクト リスト、説明 30-6
スキーマ、設定 30-19
スキーマ、説明 30-6
定義 30-6
転送 30-20
ファイル 30-7
一般クエリー 19-5
イネーブル シークレット パスワード 8-3
イネーブル パスワード 8-3
イベント、RMON 28-3
イベント ディテクタ、組み込みイベント マネージャ 31-3
インターネット グループ管理プロトコル

「IGMP」を参照
インターネット制御メッセージ プロトコル
「ICMP」を参照
インターネット プロトコル バージョン 6
「IPv6」を参照
インターフェイス
カウンタ、クリア 10-32
管理 1-3
記述名、追加 10-26
再起動 10-33
サポート対象 10-8
シャットダウン 10-33
情報の表示 10-31
ステータス 10-31
設定
速度 10-19
手順 10-9
デュプレックス モード 10-19
設定時の注意事項、デュプレックスと速度 10-19
説明 10-26
タイプ 10-1
名前の指定 10-26
範囲 10-10
範囲マクロ 10-11
番号 10-9
物理、識別 10-8, 10-9
フロー制御 10-24
モニタリング 10-31
インターフェイス コンフィギュレーション モード 2-2
インターフェイス タイプ 10-9
ENI 10-2
NNI 10-2
UNI 10-2
インターフェイスの設定、REP 18-10
インターフェイス ラインプロトコル ステートの追跡 42-2

え

エージング タイマー、REP 18-8
エージング タイム
MAC アドレス テーブル 5-21
最大
MSTP 16-25
STP 15-24
短縮
MSTP 16-24
STP 15-9, 15-23
エリア境界ルータ
「ABR」を参照
エリア ルーティング
IS-IS 36-67
ISO IGRP 36-67

お

応答時間、IP SLA による測定 41-5
オブジェクト トラッキング
HSRP 42-7
IP SLA 42-9
IP SLA、設定 42-9
モニタリング 42-13
オプション、管理 1-3
重み付きテール ドロップ
「WTD」を参照
親ポリシー、QoS 34-14, 34-29
オンボード障害ロギング
「OBFL」を参照
オンライン診断
概要 47-1
説明 47-1
テストの実行 47-6

か

外部 BGP

「EBGP」を参照
回復手順 46-1
外部ネイバー、BGP 36-50
カウンタ、インターフェイスのクリア 10-32
鍵発行局
「KDC」を参照
拡張オブジェクト トラッキング
DHCP プライマリ インターフェイス 42-11
HSRP 42-7
IP SLA 42-9
IP SLA によるネットワーク モニタリング 42-11
IP ルーティング ステート 42-2
コマンド 42-1
スタティック ルート プライマリ インターフェイス 42-11
追跡リスト 42-3
定義 42-1
バックアップ スタティック ルーティング 42-12
ラインプロトコル ステート 42-2
ルーティング ポリシー、設定 42-12
拡張システム ID
MSTP 16-18
STP 15-4, 15-16
拡張ネットワーク インターフェイス
「ENI」を参照
拡張範囲 VLAN
定義 12-1
内部 VLAN ID にる作成 12-12
カスタマー エッジ デバイス 1-19, 36-89
仮想ルータ 40-1, 40-2
簡易ネットワーク管理プロトコル
「SNMP」を参照
環境変数、機能 3-22
環境変数、組み込みイベント マネージャ 31-5
完全プライオリティ キューイング 34-71
QoS 34-32
設定 34-71
設定時の注意事項 34-71
定義 34-32
管理 VLAN
REP、設定 18-9
管理 VLAN、REP 18-9
管理アクセス
帯域外コンソール ポート接続 1-5
帯域内
CLI セッション 1-5
SNMP 1-5
管理オプション
CLI 2-1
CNS 4-1
概要 1-3
管理機能 1-4
管理ディスタンス
OSPF 36-35
定義 36-115
ルーティング プロトコルのデフォルト 36-104

き

キープアライブ メッセージ 15-3
キープアライブ メッセージ、デフォルト 10-18
起動
起動プロセス 3-1
手動 3-19
特定のイメージ 3-20
ブート ローダ、起動 3-2
機能、非互換 23-11
逆アドレス解決 36-8
逆アドレス解決プロトコル
「RARP」を参照
キュー サイズ、QoS、管理 34-34
急送型転送、DSCP 34-9
キューの帯域幅とキュー サイズ、関係 34-36
共通セッション ID
「個別セッション ID」を参照 9-11
許可 VLAN リスト 12-18
許可デバイスの最大数、ポートベース認証 9-14
近隣探索、IPv6 37-4

近隣探索 / 回復、EIGRP 36-38

く

グ 14-15
クエリー、IGMP 22-4
クエリー請求、IGMP 22-12
組み込みイベント マネージャ
3.2 31-5
TCL スクリプトの登録と定義 31-7
アプレットの登録と定義 31-6
イベント ディテクタ 31-3
概要 31-1
環境変数 31-5
情報の表示 31-8
処理 31-4
設定 31-1, 31-6
ポリシー 31-4
クライアント情報シグナリング プロトコル
「CISP」を参照
クライアント プロセス、追跡 42-1
クラス セレクタ、DSCP 34-9
クラス ベース均等化キューイング
「CBWFQ」を参照
クラスベース シェーピング
QoS 34-29
設定 34-68
設定時の注意事項 34-68
クラスベース プライオリティ キューイング、QoS 34-21
クラス マップ
match-all オプション 34-8
match-any オプション 34-8
クラス マップ、QoS
設定 34-43, 34-44
説明 34-7
クラスレス ドメイン間ルーティング
「CIDR」を参照
クラスレス ルーティング 36-6
クリア、インターフェイス 10-32
グローバル Leave、IGMP 22-12
グローバル コンフィギュレーション モード 2-2
クロスチェック、CFM 43-5, 43-12
クロック
「システム クロック」を参照

け

経路集約、OSPF 36-34
ケーブル、単方向リンクのモニタリング 26-1
権限レベル
回線に対するデフォルトの変更 8-9
概要 8-2, 8-7
コマンドの設定 8-8
終了 8-9
ログイン 8-9

こ

構成例
ネットワーク 1-16
高速コンバージェンス 16-10, 19-3
高速スパニング ツリー プロトコル
「RSTP」を参照
固定学習 23-9
個別セッション ID 9-11
個別のポリシング機能
設定 34-48
設定時の注意事項 34-48
子ポリシー、QoS 34-14, 34-29
コマンド
no と default 2-3
省略形 2-3
コマンド、権限レベルの設定 8-8
コマンド入力時のエラー メッセージ 2-4
コマンドの省略形 2-3
コマンド マクロ
グローバル パラメータ値の適用 11-4

作成 11-3
設定時の注意事項 11-2
定義 11-1
デフォルト設定 11-2
トレース 11-2
パラメータ値の適用 11-4
表示 11-5
マクロの適用 11-4
コマンド モード 2-1
コマンドライン インターフェイス
「CLI」を参照
コミュニティ VLAN 13-2, 13-3
コミュニティ ストリング
概要 30-4
設定 30-9
コミュニティ ポート 13-3
コミュニティ リスト、BGP 36-60
コンソール ポート、接続 2-9
コントロール プレーンのセキュリティ
制御パケット 33-2
設定 33-7
ポリシング 33-2
ポリシング機能 33-4
モニタリング 33-8
用途 33-1
コントロール プロトコル、IP SLA 41-4
コンバージェンス
REP 18-4
コンフィギュレーション設定、保存 3-16
コンフィギュレーションの置換 B-19
コンフィギュレーションのロールバック B-19, B-20
コンフィギュレーション ファイル
DHCP による取得 3-9
TFTP サーバのアクセス制限 30-18, 30-19, 30-20, 30-22
アーカイブ B-20
アップロード
FTP の使用 B-14
RCP の使用 B-18
TFTP の使用 B-12
準備 B-10, B-13, B-16
目的 B-8
格納されているコンフィギュレーションの削除 B-19
コピー時の無効な組み合せ B-5
作成および使用に関する注意事項 B-9
システム コンタクトおよびロケーション情報 30-18
実行コンフィギュレーションの置換 B-19, B-20
実行コンフィギュレーションのロールバック B-19, B-21
スタートアップ コンフィギュレーションの消去 B-19
説明 B-8
タイプと場所 B-9
ダウンロード
FTP の使用 B-13
RCP の使用 B-17
TFTP の使用 B-11
自動 3-18
準備 B-10, B-13, B-16
目的 B-8
置換およびロールバックに関する注意事項 B-21
テキスト エディタによる作成 B-10
デフォルト名 3-18
パスワード回復をディセーブルにする場合の考慮事項 8-5
ファイル名の指定 3-19

さ

サービス クラス
「CoS」を参照
サービス プロバイダー ネットワーク
EtherChannel のレイヤ 2 プロトコル トンネリン 14-15
レイヤ 2 プロトコル 14-14
サービスプロバイダー ネットワーク
IEEE 802.1Q トンネリング 14-2

カスタマー VLAN 14-3
サービス プロバイダー ネットワーク、MSTP と RSTP 16-1
再確認間隔、VMPS、変更 12-28
再確認、ダイナミック VLAN メンバシップの 12-28
在庫管理 TLV 25-6
再試行回数、VMPS、変更 12-29
最大エージング タイム
MSTP 16-25
STP 15-24
最大ホップ カウント、MSTP 16-25
最適化、システム リソース 7-1
サブドメイン、プライベート VLAN 13-1
サブネット ゼロ 36-6
サブネット マスク 36-5

し

シーケンス番号、ログ メッセージの 29-8
シェイプド ラウンド ロビン
「SRR」を参照
時間範囲、ACL 32-16
しきい値、トラフィック レベル 23-2
しきい値の重み、追跡リスト内の 42-5
しきい値のパーセント、追跡リスト内の 42-6
しきい値のモニタリング、IP SLA 41-6
時刻
「NTP」および「システム クロック」を参照
シスコ エクスプレス フォワーディング
「CEF」を参照
シスコ検出プロトコル
「CDP」を参照
システム MTU
IEEE 802.1Q トンネリング 14-6
IS-IS LSP 36-72
システム クロック
概要 5-2
設定
手動 5-11
タイム ゾーン 5-12
夏時間 5-13
日時の表示 5-12
「NTP」も参照
システム プロンプト、デフォルト設定 5-15
システム名
手動設定 5-15
デフォルト設定 5-15
「DNS」も参照
システム メッセージ ロギング
level キーワード、説明 29-9
syslog 機能 1-12
UNIX syslog サーバ
サポート対象のファシリティ 29-13
デーモンの設定 29-12
ロギング ファシリティの設定 29-12
イネーブル化 29-4
エラー メッセージの重大度の定義 29-8
概要 29-1
シーケンス番号、イネーブル化とディセーブル化 29-8
出力先デバイスの設定 29-5
設定の表示 29-13
タイム スタンプ、イネーブル化とディセーブル化 29-7
ディセーブル化 29-4
デフォルト設定 29-3
ファシリティ キーワード、説明 29-13
メッセージの形式 29-2
メッセージの制限 29-10
ログ メッセージの同期化 29-6
システム リソース、最適化 7-1
システム ルーティング
IS-IS 36-67
ISO IGRP 36-67
実行コンフィギュレーション
置換 B-19, B-20
ロールバック B-19, B-21
実行コンフィギュレーション、保存 3-16
自動 RP、説明 44-6

自動イネーブル化 9-10
自動検知、ポート速度 1-2
自動設定 3-3
自動ネゴシエーション
インターフェイス設定時の注意事項 10-20
デュプレックス モード 1-2
不一致 46-8
シャットダウンしきい値、レイヤ 2 プロトコル パケットの 14-17
重大度、システム メッセージに対する定義 29-8
集約アドレス、BGP 36-63
集約可能なグローバル ユニキャスト アドレス 37-3
集約ポート
「EtherChannel」を参照
集約ポリシング機能
設定 34-54
設定時の注意事項 34-54
説明 34-19
出力ポリシー 34-6
出力ポリシー マップ
設定 34-65
設定時の注意事項 34-65
統計情報の表示 34-84
分類基準 34-5
受動インターフェイス
OSPF 36-35
設定 36-113
手動プリエンプション、REP、設定 18-14
準備状態チェック
ポートベース認証
設定 9-14
説明 9-7, 9-14
消去
イーサネット CFM 43-29
照合、IPv4 ACL 32-7
照合による分類、QoS 34-8
使用上の注意事項
レイヤ 2 traceroute 46-13
冗長性
EtherChannel 35-3
HSRP 40-1
STP
パス コスト 12-22
バックボーン 15-9
ポート プライオリティ 12-21
初期設定
デフォルト 1-13
自律システム、BGP 内 36-50
自律システム境界ルータ
「ASBR」を参照
診断スケジュール コマンド 47-3
侵入検知システム
「IDS アプライアンス」を参照
信頼できるタイム ソース、説明 5-2
信頼できるトランスポート プロトコル、EIGRP 36-38

す

スイッチ仮想インターフェイス
「SVI」を参照
スイッチ コンソール ポート 1-5
スイッチ ソフトウェアの機能 1-1
スイッチ データベース管理
「SDM」を参照
スイッチド パケット、ACL 32-38
スイッチド ポート 10-4
スイッチド ポート アナライザ
「SPAN」を参照
スイッチ プライオリティ
MSTP 16-23
STP 15-21
スーパーネット 36-6
スケジューリング、IP SLA 動作 41-5
スケジューリング、QoS 34-27
スケジューリング、リロード 3-22
スタートアップ コンフィギュレーション
起動
手動 3-19

特定のイメージ 3-20
コンフィギュレーション ファイル
自動ダウンロード 3-18
ファイル名の指定 3-19
消去 B-19
デフォルトのブート コンフィギュレーション 3-18
スタティック IP ルーティング 1-11
スタティック MAC アドレス指定 1-9
スタティック SSM マッピング 44-20, 44-21
スタティック VLAN メンバシップ 12-2
スタティック アクセス ポート
VLAN 割り当て 12-11
定義 10-4, 12-5
スタティック アドレス
「アドレス」を参照
スタティック トラフィック転送 44-23
スタティック ルーティング 36-2
スタティック ルート
概要 37-6
スタティック ルート、設定 36-103
スタティック ルートのプライマリ インターフェイス、設定 42-11
スタブ エリア、OSPF 36-33
スタブ ルーティング、EIGRP 36-43
スタンバイ タイマー、HSRP 40-11
スタンバイ リンク 19-2
スタンバイ ルータ 40-1
ストーム制御
サポート 1-3
しきい値 23-1
設定 23-3
説明 23-1
ディセーブル化 23-5
表示 23-18
ストラタム、NTP 5-2
スヌーピング、IGMP 22-1
スパニング ツリーとネイティブ VLAN 12-16
スパニング ツリー プロトコル
「STP」を参照

せ

制御パケット
コントロール プレーンのセキュリティ 33-2
廃棄およびレート制限 33-2
制限、アクセスの
NTP サービス 5-8
RADIUS 8-17
TACACS+ 8-10
概要 8-1
パスワードと権限レベル 8-2
成功（success）の応答、VMPS 12-25
生成、IGMP レポート 19-4
セカンダリ VLAN 13-2
セカンダリ エッジ ポート、REP 18-4
セキュア MAC アドレス
最大数 23-9
削除 23-14
タイプ 23-9
セキュア シェル
「SSH」を参照
セキュア ポート、設定 23-8
セキュリティ機能 1-7
セキュリティ、ポート 23-8
設計、ネットワーク、例 1-16
接続、安全なリモート 8-38
接続に関する問題点 46-10, 46-13, 46-15
設定可能 Leave タイマー、IGMP 22-6
設定時の注意事項
CBWFQ 34-67
CFM 43-8
EtherChannel 35-10
HSRP 40-6
OAM マネージャ 43-48
PIM スタブ ルーティング 44-13
QoS、一般 34-37
QoS クラス マップ 34-43
REP 18-7
SSM 44-17

SSM マッピング 44-19
UNI VLAN 12-13
VLAN 12-8
VLAN マッピング 14-10
WTD 34-75
イーサネット OAM 43-33
完全プライオリティ キューイング 34-71
クラスベース シェーピング 34-68
個別のポリシング機能 34-48
集約ポリシング機能 34-54
出力ポリシー マップ 34-65
入力ポリシー マップ 34-47
ポート セキュリティ 23-11
ポート単位 VLAN 単位 QoS 34-60
ポリシー マップのマーキング 34-58
マルチ VRF CE 36-91
無条件のプライオリティ ポリシング 34-73
リンクステート トラッキング 35-24
ロールバックと置換 B-21
設定、初期
デフォルト 1-13
設定、ポートベース認証の違反モード 9-15 ～ 9-16
設定例
QoS
カスタマーの追加 34-87
キューイングパラメータまたはスケジューリング パラメータの変更 34-88
クラスの追加または削除 34-90
初期 34-85
設定済み動作の追加または削除 34-89
分類基準の追加または削除 34-87
ポリシー マップ 34-84

そ

送信元 IP アドレスベース転送、EtherChannel 35-8
送信元 MAC アドレス転送、EtherChannel 35-7
送信元 / 宛先 IP アドレスベース転送、EtherChannel 35-8
送信元 / 宛先 MAC アドレス転送、EtherChannel 35-8
送信元アドレス
IPv6 ACL 39-5
送信元のアドレス、IPv4 ACL 内 32-11
即時脱退、IGMP
イネーブル化 22-10, 38-9
設定時の注意事項 22-10
説明 22-6
速度、インターフェイスに対する設定 10-19
ソフトウェア イメージ
tar ファイル形式、説明 B-24
回復手順 46-2
フラッシュ内の場所 B-24
リロードのスケジューリング 3-23
「ダウンロード」および「アップロード」も参照
ソフトウェア障害、XMODEM による回復手順 46-2
存続可能時間 36-17

た

ターミナル ループバック
定義 43-42
帯域幅、QoS、設定 34-67
ダイナミック ARP インスペクション
ARP ACL と DHCP スヌーピング エントリのプライオリティ 21-4
ARP キャッシュ ポイズニング 21-1
ARP スプーフィング攻撃 21-1
ARP パケットのレート制限
errdisable ステート 21-4
設定 21-11
説明 21-4
ARP 要求、説明 21-1
DHCP スヌーピング バインディング データベース 21-2
Dos 攻撃、回避 21-11
man-in-the middle 攻撃、説明 21-2
インターフェイスの信頼状態 21-3
機能 21-2

消去
統計情報 21-16
ログ バッファ 21-16
設定
DHCP 環境 21-7
着信 ARP パケットのレート制限 21-4, 21-11
非 DHCP 環境の ACL 21-9
ログ バッファ 21-14
設定時の注意事項 21-6
説明 21-1
妥当性チェック、実行 21-13
デフォルト設定 21-5
統計情報
消去 21-16
表示 21-16
ネットワーク セキュリティの問題とインターフェイスの信頼状態 21-3
廃棄されたパケットのロギング、説明 21-5
表示
ARP ACL 21-15
信頼状態とレート制限 21-16
設定および動作ステート 21-16
統計情報 21-16
ログ バッファ 21-16
レート制限を超過した場合の errdisable ステート 21-4
ログ バッファ
消去 21-16
設定 21-14
表示 21-16
ダイナミック アクセス ポート
設定 12-27
定義 10-4
特性 12-5
ダイナミック アドレス
「アドレス」を参照
ダイナミック ポート VLAN メンバシップ
再確認 12-28
接続タイプ 12-27
説明 12-25
トラブルシューティング 12-30
ダイナミック ルーティング
ISO CLNS 36-67
プロトコル 36-3
タイム スタンプ、ログ メッセージの 29-7
タイム ゾーン 5-12
タイム ドメイン反射率計
「TDR」を参照
ダイレクト ユニキャスト要求 1-4
ダウンロード
イメージ ファイル
FTP の使用 B-30
RCP の使用 B-35
TFTP の使用 B-26
準備 B-26, B-29, B-34
デバイス マネージャまたは Network Assistant の使用 B-23
古いイメージの削除 B-27
目的 B-24
コンフィギュレーション ファイル
FTP の使用 B-13
RCP の使用 B-17
TFTP の使用 B-11
準備 B-10, B-13, B-16
目的 B-8
タグ付きパケット
IEEE 802.1Q 14-4
レイヤ 2 プロトコル 14-13
単方向リンク検出プロトコル
「UDLD」を参照
端末回線、パスワードの設定 8-6

つ

ツイストペア イーサネット、単方向リンク検出 26-1
追跡、IP ルーティング ステート 42-2
追跡、オブジェクト 42-1
追跡ステート、IP SLA の追跡 42-9
追跡対象オブジェクト

しきい値の重み 42-5
しきい値のパーセント 42-6
ブール式 42-4
追跡リスト
設定 42-3
タイプ 42-3

て

定期的なデータの収集および転送のメカニズム 30-6
ディスカバリ、イーサネット OAM 43-32
ディレクトリ
作業ディレクトリの表示 B-3
作成と削除 B-4
変更 B-3
データ収集、一括統計情報 30-21
テーブル マップ
QoS、設定 34-46
QoS マーキング 34-22
説明 34-15
タイプ 34-16
デフォルト アクション 34-15
デジタル オプティカル モニタリング
「DoM」を参照
デバイス ディスカバリ プロトコル 24-1, 25-1
デバッグ
エラー メッセージ出力のリダイレクト 46-18
コマンドを使用した 46-17
全システム診断のイネーブル化 46-18
特定の機能に対するイネーブル化 46-18
デフォルト
ポリシング機能の設定
ENI と UNI 33-4
NNI 33-6
デフォルト アクション、テーブル マップ 34-15
デフォルト ゲートウェイ 3-15, 36-11
デフォルト サービス、DSCP 34-9
デフォルト設定
BGP 36-48, 36-80
CDP 24-2
CFM 43-8
DHCP 20-8
DHCP オプション 82 20-8
DHCP スヌーピング 20-8
DHCP スヌーピング バインディング データベース 20-8
DNS 5-16
EIGRP 36-39
E-LMI と OAM 43-47
EtherChannel 35-10
Flex Link 19-8
HSRP 40-5
IEEE 802.1Q トンネリング 14-4
IEEE 802.1x 9-13
IGMP 44-39
IGMP スヌーピング 22-7, 38-5, 38-6
IGMP スロットリング 22-26
IGMP フィルタリング 22-26
IP SLA 41-6
IPv6 37-10
IP アドレス指定、IP ルーティング 36-4
IP ソース ガード 20-22
IP マルチキャスト ルーティング 44-9
IS-IS 36-69
LLDP 25-3
MAC アドレス テーブル 5-21
MAC アドレステーブル移行更新 19-9
MSDP 45-3
MSTP 16-15
MVR 22-19
NTP 5-4
OSPF 36-27
PIM 44-9
QoS 34-37
RADIUS 8-20
REP 18-7
RIP 36-20
RMON 28-3
RSPAN 27-9

SDM テンプレート 7-4
SNMP 30-7
SPAN 27-9
STP 15-12
TACACS+ 8-13
UDLD 26-4
VLAN 12-7
VLAN マッピング 14-9
VLAN、レイヤ 2 イーサネット インターフェイス 12-17
VMPS 12-26
Y.1731 43-24
イーサネット OAM 43-33
オプションのスパニングツリー設定 17-6
起動 3-18
システム名とシステム プロンプト 5-15
システム メッセージ ロギング 29-3
ダイナミック ARP インスペクション 21-5
デフォルト スイッチ情報 3-3
パスワードと権限レベル 8-2
バナー 5-17
プライベート VLAN 13-7
マルチ VRF CE 36-90
レイヤ 2 インターフェイス 10-16
レイヤ 2 プロトコル トンネリング 14-17
デフォルト テンプレート 7-1
デフォルト ネットワーク 36-105
デフォルト ルータ プリファレンス
「DRP」を参照
デフォルト ルーティング 36-2
デフォルト ルート 36-105
デュアル IPv4/IPv6 テンプレート 7-2, 37-6
デュアルパーパス ポート
LED 10-7
タイプの設定 10-22
定義 10-7
デフォルト 10-22
デフォルトのポート タイプ 10-7
フレーム サイズ 10-22
デュアル プロトコル スタック
IPv4 と IPv6 37-6
SDM テンプレートのサポート 37-6
デュプレックス モード、設定 10-19
電源管理 TLV 25-6
転送情報ベース
「FIB」を参照
転送遅延時間
MSTP 16-24
STP 15-23
テンプレート
SDM 7-2
イーサネット OAM 43-39

と

等価コスト ルーティング 1-11, 36-103
同期、BGP 36-50
統計情報
802.1x 9-27
CDP 24-5
IP マルチキャスト ルーティング 44-49
LLDP 25-7
LLDP-MED 25-7
OSPF 36-37
RMON グループ イーサネット 28-5
RMON グループ履歴 28-5
SNMP 入出力 30-24
インターフェイス 10-31
到達可能性、IP SLA IP ホストの追跡 42-9
独立 VLAN 13-2, 13-3
独立ポート 13-3
都市ロケーション 25-2
特権 EXEC モード 2-2
ドメイン、ISO IGRP ルーティング 36-67
ドメイン ネーム システム
「DNS」を参照
ドメイン名、DNS 5-15
トラッキング プロセス 42-1

トラップ
MAC アドレス通知の設定 5-22, 5-24, 5-26
イネーブル化 5-22, 5-24, 5-26, 30-13
概要 30-1, 30-5
通知タイプ 30-14
定義 30-4
マネージャの設定 30-13
トラップドア メカニズム 3-2
トラフィック
フラッディングのブロック 23-7
分割された 32-5
分割された IPv6 トラフィック 39-2
分割されていない 32-5
トラフィック クラス、定義 34-3
トラフィック シェーピング
QoS スケジューリング 34-28
QoS トラフィック制御 34-28
トラフィックの優先処理
「QoS」を参照
トラフィック分類、一般値 34-11
トラフィック ポリシー、要素 34-3
トラフィック マーキング 34-22
トラフィック抑制 23-1
トラブルシューティング
CiscoWorks 30-4
debug コマンドを使用した 46-17
PIMv1 と PIMv2 の相互運用性の問題点 44-35
PING 46-10
SFP のセキュリティと識別 46-8
show forward コマンド 46-19
traceroute を使用した 46-15
クラッシュ情報の表示 46-21
システム メッセージ ロギングの使用 29-1
接続に関する問題点 46-10, 46-13, 46-15
単方向リンクの検出 26-1
パケット転送の設定 46-19
トランキング カプセル化 1-7
トランク
許可 VLAN リスト 12-18
タグなしトラフィック用ネイティブ VLAN 12-20
パラレル 12-22
ロード シェアリング
STP パス コストの設定 12-22
STP ポート プライオリティの使用 12-21
トランク フェールオーバー
「リンクステート トラッキング」を参照
トランク ポート
設定 12-18
定義 10-4, 12-5
トンネリング
IEEE 802.1Q 14-2
定義 14-1
レイヤ 2 プロトコル 14-14
トンネル ポート
IEEE 802.1Q、設定 14-7
説明 10-5, 14-2
他の機能との非互換性 14-6
定義 12-5

な

内部 BGP
「IBGP」を参照
内部ネイバー、BGP 36-50
夏時間 5-13
名前付き IPv4 ACL 32-14
名前付き IPv6 ACL 39-3
並べ替え、ACL エントリ 32-14

に

入力ポリシー マップ
設定 34-47
設定時の注意事項 34-47
統計情報の表示 34-84
分類基準 34-5
入力ポリシー マップのマーキングの設定 34-58
認可

RADIUS 8-27
TACACS+ 8-11, 8-16
認証
AAA でのローカル モード 8-36
EIGRP 36-42
HSRP 40-11
NTP アソシエーション 5-4
RADIUS
鍵 8-21
ログイン 8-23
TACACS+
鍵 8-13
定義 8-11
ログイン 8-14
「ポートベース認証」を参照
認証鍵、ルーティング プロトコル 36-116
認証マネージャ
個別セッション ID 9-11

ね

ネイティブ VLAN
IEEE 802.1Q トンネリング 14-4
設定 12-20
デフォルト 12-20
ネイバー、BGP 36-61
ネイバーのオフセット番号、REP 18-4
ネットワーク エッジ アクセス トポロジ
「NEAT」を参照
ネットワーク管理
CDP 24-1
RMON 28-1
SNMP 30-1
ネットワーク タイム プロトコル
「NTP」を参照
ネットワーク ノード インターフェイス
「NNI」を参照
ネットワーク パフォーマンス、IP SLA による測定 41-3
ネットワーク ポリシー TLV 25-6

の

ノンストップ フォワーディング認識
「NSF 認識」を参照

は

バーチャル プライベート ネットワーク
「VPN」を参照
ハードウェア制限とレイヤ 3 インターフェイス 10-28
廃棄しきい値、レイヤ 2 プロトコル パケットの 14-17
バインディング
DHCP スヌーピング データベース 20-6
IP ソース ガード 20-20
バインディング データベース
DHCP スヌーピング
「DCHP スヌーピング バインディング データベース」を参照
バインディング テーブル、DHCP スヌーピング
「DCHP スヌーピング バインディング データベース」を参照
パケット分類
定義 34-6
トラフィックの組織化 34-2
パケット ポリシング、QoS 34-2
パケット マーキング
設定 34-58
定義 34-22
パス MTU ディカバリ 37-4
パス コスト
MSTP 16-22
STP 15-20
パスワード
暗号化 8-3
回復 46-3
回復のディセーブル化 8-5
概要 8-1

セキュリティ 1-8
設定
Telnet 8-6
イネーブル化 8-3
イネーブル シークレット 8-3
ユーザ名 8-7
デフォルト設定 8-2
バックアップ インターフェイス
「Flex Link」を参照
バックアップ スタティック ルーティング、設定 42-12
バックアップ リンク 19-2
バナー
設定
MoTD ログイン 5-18
ログイン 5-19
デフォルト設定 5-17
表示のタイミング 5-17
パフォーマンスの特長 1-2
パラレル パス、ルーティング テーブル内 36-103
範囲
インターフェイス 10-10
マクロ 10-11

ひ

非 IP トラフィックのフィルタリング 32-27
ピア、BGP 36-61
光ファイバ、単方向リンクの検出 26-1
非互換、機能 23-11
非対称リンク、IEEE 802.1Q トンネリング 14-4
非トランキング モード 12-16
標準範囲 VLAN
設定 12-7
定義 12-1
特性 12-3

ふ

ファイル
crashinfo
説明 46-21
内容の表示 46-21
場所 46-21
tar
イメージ ファイル形式 B-24
作成 B-6
抽出 B-7
内容の表示 B-6
コピー B-4
削除 B-5
内容の表示 B-8
ファイル システム
使用可能なファイル システムの表示 B-2
デフォルトの設定 B-3
ネットワーク ファイルシステムの名前 B-4
ファイル情報の表示 B-3
ローカル ファイル システムの名前 B-1
不一致、自動ネゴシエーション 46-8
フィルタ、IP
「ACL」を参照、IP
フィルタリング
IPv6 トラフィック 39-3, 39-7
show コマンドおよび more コマンドの出力 2-8
VLAN 32-30
非 IP トラフィック 32-27
フィルタリング、show コマンドおよび more コマンドの出力 2-8
ブートストラップ ルータ（BSR）、説明 44-7
ブート ローダ
アクセス 3-21
環境変数 3-21
説明 3-2
トラップドア メカニズム 3-2
プロンプト 3-21
ブール式、追跡リスト内の 42-4
複数動作スケジューリング、IP SLA 41-5
輻輳回避、QoS 34-2, 34-34
輻輳管理、QoS 34-2, 34-27

物理ポート 10-4
プライオリティ
HSRP 40-8
プライオリティ キュー
QoS スケジューリング 34-28
設定 34-71
説明 34-32
プライオリティ ポリシング、説明 34-21
プライベート VLAN
IP アドレス指定 13-4
SVI 13-6
UNI VLAN 12-13
エンド ステーション アクセス 13-3
コミュニティ VLAN 13-2, 13-3
コミュニティ ポート 13-3
サブドメイン 13-1
セカンダリ VLAN 13-2
設定 13-10
設定作業 13-6
設定時の注意事項 13-7, 13-9
デフォルト設定 13-7
特長 13-1
独立 VLAN 13-2, 13-3
独立ポート 13-3
トラフィック 13-5
複数のスイッチにまたがる 13-4
プライマリ VLAN 13-2, 13-3
プロミスキャス ポート 13-2
ポート
コミュニティ 13-3
設定時の注意事項 13-9
説明 12-5
独立 13-3
プロミスキャス 13-2
プロミスキャス ポートの設定 13-13
ホスト ポートの設定 13-12
マッピング 13-15
モニタリング 13-16
プライマリ VLAN 13-2, 13-3
プライマリ インターフェイス、オブジェクト トラッキングの、DHCP、設定 42-11
プライマリ インターフェイス、スタティック ルートの、設定 42-11
プライマリ エッジ ポート、REP 18-4
プライマリ リンク 19-2
フラッシュ デバイス、番号 B-1
フラッディング トラフィック、ブロック 23-7
プリエンプション遅延時間、REP 18-5
プリエンプション遅延、デフォルト設定 19-8
プリエンプション、デフォルト設定 19-8
プレフィクス リスト、BGP 36-58
フロー制御 1-2, 10-24
ブロードキャスト ストーム 23-1, 36-14
ブロードキャスト パケット
ダイレクト 36-13
フラッディングされた 36-13
ブロードキャスト フラッディング 36-17
プロキシ ARP
IP ルーティングがディセーブルの場合 36-11
設定 36-10
定義 36-8
プロキシ レポート 19-4
ブロック、パケット 23-7
プロトコル依存モジュール、EIGRP 36-39
プロトコル制御パケット 33-1
プロバイダー エッジ デバイス 1-19, 36-89
プロミスキャス ポート
設定 13-13
定義 13-2
分析用トラフィックのミラーリング 27-1
分類
ACL 検索に基づく 34-11
QoS グループ 34-12
QoS 比較 34-11
パケット ヘッダ 34-6
ポート単位 VLAN 単位 34-13, 34-60

へ

ベストエフォート型のパケット配信 34-1
ヘルプ、コマンドラインに関する 2-3
編集機能
　イネーブル化とディセーブル化 2-6
　折り返し機能 2-7
　使用されるキーストローク 2-6

ほ

防止、不正アクセスの 8-1
ボーダー ゲートウェイ プロトコル
　「BGP」を参照
ポート
　IEEE 802.1Q トンネル 12-5
　REP 18-6
　VLAN 割り当て 12-11
　アクセス 10-4
　スイッチ 10-4
　スタティック アクセス 12-5, 12-11
　セキュア 23-8
　ダイナミック アクセス 12-5
　デュアルパーパス 10-7
　トランク 12-5, 12-15
　ブロッキング 23-7
　保護 23-5
　ルーテッド 10-5
ポート ACL
　タイプ 32-3
　定義 32-2
ポート シェーピング
　設定 34-69
　説明 34-29
ポート シャットダウン（port-shutdown）の応答、VMPS 12-25
ポート集約プロトコル
　「EtherChannel」を参照
ポート セキュリティ
　イネーブル化 23-17
　違反 23-10
　エージング 23-15
　固定学習 23-9
　設定 23-12
　設定時の注意事項 23-11
　説明 23-8
　その他の機能との互換性 23-11
　デフォルト設定 23-10
　トランク ポート 23-13
　表示 23-18
　プライベート VLAN 23-17
ポート タイプ 10-2
ポート単位 VLAN 単位ポリシー マップ、設定時の注意事項 34-60
ポート単位 VLAN 単位ポリシング 34-13, 34-60
ポート単位ファシリティ ループバック
　定義 43-42
ポートチャネル
　「EtherChannel」を参照
ポート プライオリティ
　MSTP 16-20
　STP 15-18
ポート ブロッキング 1-3, 23-7
ポートベース認証
　EAPOL 開始フレーム 9-3
　EAP 応答 / アイデンティティ フレーム 9-3
　EAP 要求 / アイデンティティ フレーム 9-3
　VLAN 割り当て
　　AAA 認証 9-16
　　設定作業 9-9
　　説明 9-8
　　特性 9-8
　アカウンティング 9-5
　開始とメッセージ交換 9-3
　各ポートの許可デバイスの最大数 9-14
　カプセル化 9-3
　クライアント、定義 9-2
　準備状態チェック

設定 9-14
説明 9-7, 9-14
スイッチ
RADIUS クライアント 9-3
プロキシとしての 9-3
スイッチ サプリカント
概要 9-10
設定 9-25
設定
802.1x 認証 9-16
RADIUS サーバ 9-18
違反モード 9-8, 9-15 ～ 9-16
手動によるクライアントの再認証 9-19
スイッチからクライアントへの再送信時間 9-20
スイッチからクライアントへのフレーム再送信時間 9-21
スイッチ上の RADIUS サーバ パラメータ 9-17
待機時間 9-19
定期的再認証 9-18
ホスト モード 9-22
設定時の注意事項 9-13
説明 9-1
デバイスの役割 9-2
デフォルト設定 9-13
デフォルト値へのリセット 9-23
統計情報の表示 9-27
統計情報、表示 9-27
認証サーバ
RADIUS サーバ 9-3
定義 9-3
複数ホスト モード、説明 9-6
方式リスト 9-16
ポート
許可および無許可 9-4
許可ステートと dot1x port-control コマンド 9-4
ポート セキュリティ
説明 9-7
相互作用 9-7
複数ホスト モード 9-6
ホスト モード 9-6
ユーザ分散
概要 9-9
注意事項 9-9
ポート メンバシップ モード、VLAN 12-4
保護ポート 23-5
保証型転送、DSCP 34-9
ホスト、ダイナミック ポート上での上限 12-30
ホスト ポート
種類 13-3
設定 13-12
ホットスタンバイ ルータ プロトコル
「HSRP」を参照
ポリシーベース ルーティング
「PBR」を参照
ポリシー マップ
出力
設定 34-65
説明 34-4
設定例 34-84
説明 34-17
入力
設定 34-47
説明 34-4
付加 34-4, 34-47
ポリシーマップ マーキング、設定時の注意事項 34-58
ポリシング
QoS 34-16
出力ポリシー マップへのプライオリティ ポリシングの適用 34-21
説明 34-2
入力ポリシー マップへの個別ポリシングの適用 34-17
入力ポリシー マップへの集約ポリシングの適用 34-19
ポリシング機能
説明 34-2
複数のトラフィック クラスの設定 34-54

ポリシング機能の設定
ENI と UNI のデフォルト 33-4
NNI のデフォルト 33-6
ポリシングを含むプライオリティ
コマンド 34-22
設定 34-73
説明 34-32

ま

マーキング
集約ポリシング機能のアクション 34-54
説明 34-2, 34-16
マクロ
「コマンド マクロ」を参照
マルチ VRF CE
サポート 1-12
設定 36-90
設定時の注意事項 36-91
設定例 36-97
定義 1-18, 36-88
デフォルト設定 36-90
ネットワーク コンポーネント 36-90
パケット転送処理 36-90
表示 36-101
モニタリング 36-101
マルチキャスト TV アプリケーション 22-17
マルチキャスト VLAN 22-17
マルチキャスト VLAN レジストレーション
「MVR」を参照
マルチキャスト イーサネット ループバック（ETH-LB） 43-23
マルチキャスト イーサネット ループバック、使用 43-29
マルチキャスト グループ
スタティックな加入 22-9, 38-8
即時脱退 22-6
脱退 22-5
マルチキャスト ストーム 23-1
マルチキャスト パケット
ACL 32-40
マルチキャスト ルータ インターフェイス、モニタリング 22-16, 38-12
マルチキャスト ルータ ポート 19-3, 19-5
マルチキャスト ルータ ポート、追加 22-8, 38-8

む

無条件のプライオリティ ポリシング
設定時の注意事項 34-73
ポリシングを含むプライオリティ 34-32
無条件のポリシングを含むプライオリティ、QoS 34-28

め

メッセージ
イーサネット OAM 43-32
バナーを使用してユーザに送信 5-17
メトリック、BGP 内 36-55
メトリック変換、ルーティング プロトコル間 36-109
メトロ タグ 14-3
メンテナンス エンド ポイント
「MEP」を参照
メンテナンス中間ポイント
「MIP」を参照
メンバシップ モード、VLAN ポート 12-5

も

モジュール番号 10-9
モジュラ QoS コマンドライン インターフェイス
「MQC」を参照
モニタリング
BGP 36-66
CDP 24-5
CEF 36-102
EIGRP 36-45

E-LMI 43-53
Flex Link 19-15
HSRP 40-12
IEEE 802.1Q トンネリング 14-24
IGMP
スヌーピング 22-15, 38-12
フィルタ 22-31
IP
アドレス テーブル 36-18
マルチキャスト ルーティング 44-48
ルート 36-117
IP SLA 動作 41-13
IPv4 ACL 設定 32-40
IPv6 ACL の設定 39-8
IS-IS 36-77
ISO CLNS 36-77
MAC アドレステーブル移行更新 19-15
MSDP ピア 45-17
MVR 22-25
OAM マネージャ 43-53
OSPF 36-37
QoS 34-83
REP 18-15
RP マッピング情報 44-35
SA メッセージ 45-17
SFP
ステータス 10-32
SFP ステータス 1-12, 46-9
SSM マッピング 44-23
VLAN 12-15
フィルタ 32-41
マップ 32-41
VMPS 12-29
アクセス グループ 32-40
イーサネット CFM 43-29, 43-30
イーサネット OAM 43-41
イーサネット OAM プロトコル 43-41
インターフェイス 10-31
オブジェクト トラッキング 42-13
機能 1-12
コントロール プレーンのセキュリティ 33-8
スイッチ間のトラフィック フロー 28-1
速度とデュプレックス モード 10-21
単方向リンクのケーブル 26-1
トラフィック抑制 23-18
トンネリング 14-24
プライベート VLAN 13-16
プローブによる分析用トラフィックのミラーリング 27-2
ポート
ブロッキング 23-18
保護 23-18
マルチ VRF CE 36-101
マルチキャスト ルータ インターフェイス 22-16, 38-12
レイヤ 2 プロトコル トンネリング 14-24

ゆ

有効期間、短縮 15-9
ユーザ EXEC モード 2-2
ユーザ データグラム プロトコル
「UDP」を参照
ユーザ ネットワーク インターフェイス
「UNI」を参照
ユーザ名ベースの認証 8-7
ユニキャスト MAC アドレス フィルタリング
CPU パケット 5-28
スタティック アドレスの追加 5-29
設定時の注意事項 5-28
説明 5-28
ブロードキャスト MAC アドレス 5-28
マルチキャスト アドレス 5-28
ルータ MAC アドレス 5-28
ユニキャスト ストーム 23-1
ユニキャスト トラフィック、ブロック 23-7

よ

予約アドレス、DHCP プール内の　20-17

ら

ライン コンフィギュレーション モード　2-2

り

リーク、IGMP レポート　19-4
リセット、BGP 内　36-52
リモート SPAN　27-2
　「RSPAN」を参照
リモート コピー プロトコル
　「RCP」を参照
リモート障害表示　43-32
リモート障害表示、イーサネット OAM　43-38
リモート ネットワーク モニタリング
　「RMON」を参照
リモート ループバック、イーサネット OAM　43-32, 43-34
履歴
　コマンドの呼び出し方法　2-5
　説明　2-4
　ディセーブル化　2-5
　バッファ サイズの変更　2-4
履歴テーブル、syslog メッセージのレベルと数　29-10
リロード、ソフトウェア　3-22
リンク完全性、REP による検証　18-3
リンク集約制御プロトコル
　「EtherChannel」を参照
リンク障害、単方向リンクでの検出　16-8
リンク冗長性
　「Flex Link」を参照
リンクステート アドバタイズメント（LSA）　36-33
リンクステート トラッキング
　設定　35-24
　設定時の注意事項　35-24
　説明　35-22
リンク、単方向　26-1
リンク モニタリング、イーサネット OAM　43-32, 43-35
リンク レイヤ検出プロトコル
　「CDP」を参照
リンク ローカル ホスト アドレス　37-3
隣接関係テーブル、CEF　36-102

る

ルータ ACL
　タイプ　32-4
　定義　32-2
ルータ ID、OSPF　36-36
ルーティング
　IPv6 トラフィック　37-2
　情報の再配布　36-106
　スタティック　36-2
　ダイナミック　36-3
　デフォルト　36-2
ルーティング ドメイン連合、BGP　36-63
ルーティング プロトコルの管理ディスタンス　36-104
ルーテッド パケット、ACL　32-39
ルーテッド ポート
　IP アドレス　10-27, 36-3
　設定　36-3
　定義　10-5
ルート ガード
　イネーブル化　17-11
　サポート　1-6
　説明　17-4
ルート計算タイマー、OSPF　36-35
ルート スイッチ
　MSTP　16-18
　STP　15-16
ルート選択、BGP　36-54
ルート ターゲット、VPN　36-90
ルート ダンプニング、BGP　36-65

ルート マップ
BGP 36-56
ポリシーベース ルーティング 36-110
ルート リフレクタ、BGP 36-64
ループ ガード
イネーブル化 17-12
サポート 1-6
説明 17-5

れ

例
ネットワーク構成 1-16
レイヤ 2 traceroute
1 つのポートに複数のデバイス 46-14
ARP 46-14
CDP 46-13
IP アドレスとサブネット 46-14
MAC アドレスと VLAN 46-14
使用上の注意事項 46-13
説明 46-13
ブロードキャスト トラフィック 46-13
マルチキャスト トラフィック 46-14
ユニキャスト トラフィック 46-13
レイヤ 2 インターフェイス、デフォルト設定 10-16
レイヤ 2 テンプレート 7-1
レイヤ 2 パケット、分類 34-6
レイヤ 2 プロトコル トンネリング
EtherChannel 用の設定 14-20
設定 14-16
注意事項 14-18
定義 14-14
デフォルト設定 14-17
レイヤ 2 プロトコル パケット、およびコントロール プレーンのセキュリティ 33-2
レイヤ 3 インターフェイス
IPv4 アドレスおよび IPv6 アドレスの割り当て 37-13
IPv6 アドレスの割り当て 37-11
IP アドレスの割り当て 36-5
タイプ 36-3
レイヤ 2 モードからの変更 36-5, 36-94
レイヤ 3 機能 1-11
レート制限しきい値、CPU 保護 33-7
レジリエント イーサネット プロトコル
「REP」を参照
レスポンダ、IP SLA
イネーブル化 41-8
説明 41-4
レポート抑制、IGMP
説明 22-6
ディセーブル化 22-15, 38-11

ろ

ローカル SPAN 27-2
ロード バランシング 40-4
ログイン認証
RADIUS 8-23
TACACS+ 8-14
ログイン バナー 5-17
ログ メッセージ
「システム メッセージ ロギング」を参照
ログ メッセージ、ACL 32-8
ロケーション TLV 25-2, 25-6